Firepower Management Center 구성 가이드, 버전 6.7

초판: 2020년 11월 2일

최종 변경: 2020년 11월 18일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

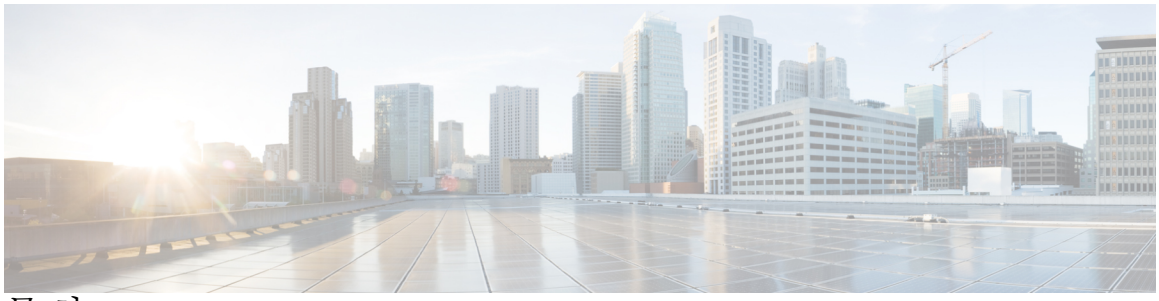
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. 모든 권리 보유.



목 차

장 1

Firepower 시작하기 1

- 빠른 시작: 기본 설정 2
  - 물리적 어플라이언스에서 초기 설정 설치 및 수행 2
  - 가상 어플라이언스 구축 3
  - 최초 로그인 3
  - 기본 정책 및 구성 설정 5
- Firepower 디바이스 7
  - Firepower 7000/8000 시리즈 디바이스 판매 종료 7
- Firepower 기능 8
  - 어플라이언스 및 시스템 관리 기능 8
    - 플랫폼별 고가용성 및 확장성 기능 10
  - 잠재적 위협 탐지, 방지 및 처리 기능 11
  - 외부 툴과 통합 12
- FMC 검색 13
  - 웹 인터페이스 메뉴 옵션 검색 13
- 도메인 전환 Firepower Management Center 14
- 상황 메뉴 14
- Firepower 온라인 도움말, 방법 및 문서 16
  - FMC 구축에 대한 최상위 문서 목록 페이지 17
  - 문서 내 라이선스 설명 19
  - 문서 내 지원 디바이스 설명 19
  - 문서 내 액세스 설명 19
- Firepower System IP 주소 규칙 19
- 추가 리소스 20

Firepower 시작 기록 20

부 I: 사용자 어카운트 23

장 2 **Firepower System**에 로그인 25

Firepower System 사용자 어카운트 25

Firepower System 유저 인터페이스 27

웹 인터페이스 고려 사항 29

세션 시간 초과 30

Firepower Management Center 웹 인터페이스 로그인 30

SSO를 사용한 FMC 웹 인터페이스 로그인 31

7000 또는 8000 Series 디바이스의 웹 인터페이스에 로그인 33

CAC 크리덴셜로 Firepower Management Center에 로그인 33

CAC 크리덴셜을 사용하여 7000 또는 8000 Series 디바이스에 로그인 34

FMC Command Line Interface에 로그인 35

7000/8000 시리즈, ASA FirePOWER, NGIPSv 디바이스에서 CLI에 로그인 36

마지막 로그인 보기 37

Firepower System 웹 인터페이스에서 로그아웃 37

Firepower 시스템 로그인 기록 38

장 3 사용자 환경설정 지정 39

사용자 환경설정 소개 39

비밀번호 변경 39

만료된 비밀번호 변경 40

웹 인터페이스 모양 변경 40

홈 페이지 지정 41

이벤트 보기 구성 41

이벤트 보기 환경 설정 42

파일 다운로드 환경설정 43

기본 시간대 44

기본 워크플로 46

기본 표준 시간대 설정 46
기본 대시보드 지정 47
사용자 환경 설정 지정 기록 48

장 4

FMC의 사용자 계정 49
FMC 사용자 계정 정보 49
내부 및 외부, 그리고 SSO 사용자 49
웹 인터페이스 및 CLI 액세스 50
사용자 역할 50
사용자 암호 52
FMC용 사용자 계정 지침 및 제한 사항 54
FMC 사용자 계정 요구 사항 및 사전 요건 55
내부 사용자 추가 55
외부 인증 구성 57
외부 인증 정보 58
LDAP 정보 58
RADIUS 정보 59
FMC에 대한 LDAP 외부 인증 개체 추가 59
FMC에 대한 RADIUS 외부 인증 개체 추가 66
FMC 사용자에 대한 외부 인증 활성화 71
LADP로 CAC(Common Access Card) 인증 구성 72
SAML SSO(Single Sign-On) 구성 74
SAML SSO(Single Sign-On) 74
FMC에 대한 SSO 지침 74
SSO 사용자 계정 75
SSO 사용자에 대한 사용자 역할 매핑 76
FMC에서 SSO(Single Sign-On) 활성화 77
Okta로 SSO(Single Sign-On) 구성 78
Okta 조직 검토 78
Okta를 위한 FMC 서비스 제공자 애플리케이션 구성 79
Okta SSO용 FMC 구성 81

Okta에 대한 사용자 역할 매핑 구성 FMC 82
Okta IdP에서 사용자 역할 매핑 구성 83
Okta 사용자 역할 매핑 예 85
OneLogin으로 SSO(Single Sign-On) 구성 90
OneLogin 하위 도메인 검토 91
OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성 91
OneLogin SSO용 FMC 구성 93
FMC에서 OneLogin 사용자 역할 매핑 구성 94
OneLogin IdP에서 사용자 역할 매핑 구성 95
OneLogin 사용자 역할 매핑 예 98
Azure AD로 SSO(Single Sign-On, 단일 인증) 구성 103
Azure 테넌트 검토 104
Azure용 FMC 서비스 제공자 애플리케이션 구성 104
Azure SSO용 FMC 구성 106
FMC에서 Azure에 대한 사용자 역할 매핑 구성 108
Azure IdP에서 사용자 역할 매핑 구성 108
Azure 사용자 역할 매핑 예 111
PingID로 SSO(Single Sign-On) 구성 116
PingID PingOne for Customers 환경 검토 117
PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정 117
PingID PingOne for Customers을 사용하여 SSO용 FMC을 구성합니다. 119
SAML 2.0 규정준수 SSO 제공자로 SSO(Single Sign-On) 구성 120
SSO ID 제공자 및 SSO 페더레이션을 숙지합니다. 121
SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성 122
SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성 123
SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정 125
SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정 126
웹 인터페이스의 사용자 역할 맞춤화 127
맞춤형 사용자 역할 생성 127
사용자 역할 비활성화 129
사용자 역할 확대 활성화 130

확대 대상 역할 설정 130
확대를 위한 맞춤형 사용자 역할 구성 131
사용자 역할 확대 132
LDAP 인증 연결 문제 해결 132
FMC 사용자 계정 히스토리 134

장 5 디바이스 사용자 계정 135
디바이스 사용자 계정 정보 135
내부 및 외부 사용자 135
CLI 액세스 136
CLI 사용자 역할 136
디바이스의 사용자 계정에 대한 요구 사항 및 사전 요건 136
디바이스 사용자 계정을 위한 지침 및 제한 사항 137
CLI에서 내부 사용자 추가 137
FTD에 대한 외부 인증 구성 139
FTD 외부 인증 정보 139
LDAP 정보 140
RADIUS 정보 141
FTD에 대한 LDAP 외부 인증 개체 추가 141
FTD에 대한 RADIUS 외부 인증 개체 추가 146
FTD 디바이스 사용자에 대한 외부 인증 활성화 151
LDAP 인증 연결 문제 해결 152
디바이스용 사용자 계정 기록 154

부 II: **Firepower System Management** 155

장 6 **Firepower System** 라이선싱 157
Firepower 라이선스 정보 157
라이선싱 요구 사항 및 사전 요건 158
Firepower Management Center 라이선스 요구 사항 158
Firepower Management Center Virtual 라이선스 158

평가판 라이선스 주의 사항 159
모든 디바이스 라이선싱 159
제품 라이선스 등록 포털 159
Firepower 기능에 대한 서비스 서브스크립션(클래식 라이선싱) 160
기본 라이선스 유형 및 제한 사항 160
보호 라이선스 162
제어 라이선스 163
클래식 디바이스에 대한 URL 필터링 라이선스 163
클래식 디바이스에 대한 악성코드 라이선스 164
7000 및 8000 시리즈 디바이스에 대한 VPN 라이선스 165
디바이스 스택 및 고가용성 쌍의 기본 라이선스 165
기본 라이선스 보기 165
라이선스 키를 식별합니다. 166
기본 라이선스 생성 및 추가 Firepower Management Center 167
FTD 디바이스에서 사용할 클래식 라이선스를 변환하는 방법 168
디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당 170
라이선스 만료 171
이 가이드의 기타 라이선싱 정보 174
Firepower 라이선싱 관련 추가 정보 176
Cisco 지원 진단 176
Cisco 지원 진단 등록 변경 177
라이선싱 기록 177

장 7

시스템 업데이트 179
Firepower 업데이트 정보 179
시스템 업데이트 요구 사항 및 사전 요건 180
Firepower 업데이트에 대한 가이드라인 및 제한 사항 180
Firepower System 소프트웨어 업그레이드 181
VDB 수동 업데이트 182
GeoDB(지리위치 데이터베이스) 업데이트 183
GeoDB 수동 업데이트(인터넷 연결) 184

GeoDB 수동 업데이트(인터넷 연결 없음) 185
GeoDB 업데이트 예약 185
침입 규칙 업데이트 186
침입 규칙 일회성 수동 업데이트 187
침입 규칙 일회성 자동 업데이트 188
반복 되는 침입 규칙 업데이트 구성 189
로컬 침입 규칙 가져오기 모범 사례 190
로컬 침입 규칙 가져오기 191
규칙 업데이트 로그 192
침입 규칙 업데이트 로그 테이블 192
침입 규칙 업데이트 로그 보기 193
침입 규칙의 필드에 로그를 업데이트합니다. 193
침입 규칙 업데이트 가져오기 로그 세부 정보 보기 195
에어-갭(Air-Gapped) 구축 유지 관리 196
시스템 업데이트 히스토리 197

장 8
백업 및 복원 203
백업 및 복원 정보 203
백업 및 복구 요구 사항 205
백업 및 복원 지침 및 제한 사항 206
Firepower 4100/9300에 대한 구성 가져오기/내보내기 지침 207
백업 및 복원을 위한 모범 사례 208
Firepower 어플라이언스 백업 211
FMC 백업 212
FMC에서 디바이스 백업 213
FXOS 구성 파일 내보내기 215
7000/8000 시리즈 디바이스 로컬 백업 216
백업 프로파일 생성 217
Firepower 어플라이언스 복구 218
백업에서 FMC 복원 219
백업에서 FTD 복구: Firepower 1000/2100 및 ASA-5500-X 시리즈 220

백업에서 FTD 복원: Firepower 4100/9300 섀시 223
구성 파일 가져오기 226
백업에서 FTD 복원: FTDv 228
백업에서 7000/8000 시리즈 디바이스 복구 230
백업 및 원격 스토리지 관리 231
백업 스토리지 위치 233
백업 및 복원 기록 234

장 9
구성 가져오기 및 내보내기 237
컨피그레이션 가져오기/내보내기 정보 237
가져오기/내보내기를 지원하는 구성 237
구성 가져오기/내보내기에 대한 특별 고려 사항 238
구성 가져오기/내보내기 요구 사항 및 사전 요건 239
컨피그레이션 내보내기 240
컨피그레이션 가져오기 240
가져오기 충돌 해결 241

장 10
작업 예약 245
작업 예약 관련 정보 245
작업 스케줄링 요구 사항 및 사전 요건 246
반복 작업 구성 246
예약 백업 248
FMC 백업 예약 248
원격 디바이스 백업 예약 249
로컬 7000 및 8000 Series 디바이스 백업 예약 250
CRL(Certificate Revocation List) 다운로드 구성 250
정책 구축 자동화 251
Nmap 스캔 자동화 253
Nmap 스캔 예약 253
보고서 생성 자동화 254
예약된 보고서에 대한 보고서 생성 설정 지정 255

Firepower 추천 자동화 256
소프트웨어 업데이트 자동화 257
소프트웨어 다운로드 자동화 258
소프트웨어 푸시 자동화 259
소프트웨어 설치 자동화 259
취약성 데이터베이스 업데이트 자동화 260
VDB 업데이트 다운로드 자동화 261
VDB 업데이트 설치 자동화 262
예약된 작업을 통해 URL 필터링 업데이트 자동화 263
예약된 작업 검토 264
작업 목록 세부 정보 265
일정표에서 예약된 작업 보기 265
예약된 작업 수정 266
예약된 작업 삭제 266
예약된 작업 기록 267

장 11 데이터 스토리지 269
FMC에 저장된 데이터 269
FMC 데이터베이스에서 데이터 제거 270
외부 데이터 스토리지 271
Cisco Security Analytics and Logging 원격 이벤트 스토리지 옵션 비교 272
Stealthwatch 클라우드의 원격 데이터 스토리지 272
Stealthwatch 어플라이언스의 원격 데이터 스토리지 273
데이터 스토리지 기록 273

장 12 **Firepower Management Center** 고가용성 275
Firepower Management Center 고가용성 정보 275
Firepower Management Center 고가용성의 역할 및 상태 비교 276
Firepower Management Center 고가용성 쌍의 이벤트 처리 276
AMP 클라우드 연결 및 악성코드 정보 277
URL 필터링 및 보안 인텔리전스 277

Firepower Management Center 페일오버 중에 사용자 데이터 처리 277
Firepower Management Center 고가용성 쌍의 구성 관리 277
Cisco Threat Intelligence Director(TID) 및 고가용성 구성 277
SSO 및 고가용성 쌍 277
Firepower Management Center 백업 중에 고가용성 동작 278
Firepower Management Center 고가용성 스플릿 브레인 278
고가용성 쌍의 Firepower Management Center 업그레이드 279
Firepower Management Center 고가용성 문제 해결 280
Firepower Management Center 고가용성을 위한 요구 사항 281
하드웨어 요구 사항 281
가상 플랫폼 요건 281
소프트웨어 요구 사항 282
FMC 고가용성 설정에 대한 라이선스 요구 사항 282
Firepower Management Center 고가용성을 설정하기 위한 사전 요건 283
Firepower Management Center 고가용성 설정 284
Firepower Management Center 고가용성 상태 보기 285
고가용성 중에 Firepower Management Center 간 동기화된 구성 데이터 286
Firepower Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인 287
Firepower Management Center 고가용성 쌍에서 피어 전환 287
페어링된 Firepower Management Center 간 커뮤니케이션 일시 중지 288
페어링된 Firepower Management Center 간 통신 재시작 288
고가용성 쌍의 Firepower Management Center IP 주소 변경 289
Firepower Management Center 고가용성 비활성화 289
고가용성 쌍의 FMC 교체 290
오류가 발생한 기본 FMC 교체(백업 성공) 290
오류가 발생한 기본 FMC 교체(백업 실패) 292
오류가 발생한 보조 FMC 교체(백업 성공) 293
오류가 발생한 보조 FMC 교체(백업 실패) 294
FMC 고가용성 히스토리 294

장 13 디바이스 관리 기본 사항 297

디바이스 관리 관련 정보 297
Firepower Management Center 및 디바이스 관리 관련 정보 297
Firepower Management Center로 관리할 수 있는 내용 298
정책 및 이벤트 이상 298
디바이스 관리 인터페이스 299
매니지드 디바이스의 관리 인터페이스 299
FTD 데이터 인터페이스를 사용하여 관리하는 방법에 대한 정보 300
디바이스 모델별 관리 인터페이스 지원 300
디바이스 관리 인터페이스의 네트워크 라우트 301
NAT 환경 302
관리 및 이벤트 트래픽 채널 예시 304
디바이스 관리 요구 사항 및 사전 요건 305
FTD 초기 설정 완료 305
FMC에 디바이스 추가 311
FMC에서 디바이스 삭제 315
디바이스 그룹 추가 315
디바이스 설정 구성 316
시스템 종료 관리 316
관리 설정 편집 317
FMC에서 호스트 이름 또는 IP 주소 업데이트 317
관리에서 데이터로 FMC 액세스 인터페이스 변경 318
데이터에서 관리로 FMC 액세스 인터페이스 변경 321
데이터 인터페이스 관리를 위한 FMC 액세스 세부정보 보기 323
CLI에서 디바이스 관리 인터페이스 수정 327
CLI에서 관리에 사용되는 FTD 데이터 인터페이스 수정 334
FMC가 연결을 상실할 경우 컨피그레이션을 롤백 336
데이터 인터페이스에서 관리 연결성 문제 해결 337
일반 설정 편집 342
다른 디바이스에 구성 복사 343
라이선스 설정 편집 345
고급 설정 편집 345

AAB(Automatic Application Bypass) 구성 345
로컬 라우터 트래픽 검사 346
빠른 경로 규칙(8000 Series) 설정 347
개체 그룹 검색 구성 349
인터페이스 개체 최적화 구성 350
디바이스의 관리자 변경 351
디바이스에서 FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다. 351
새 FMC 식별 352
Firepower Device Manager에서 FMC로 전환 353
FMC에서 Firepower Device Manager로 전환 354
디바이스 정보 보기 356
디바이스 관리 페이지 정보 357
일반 정보 357
라이선스 정보 358
시스템 정보 358
상태 정보 358
관리 정보 359
Advanced Settings(고급 설정) 359

부 III: 시스템 모니터링 및 문제 해결 361

장 14 대시보드 363
대시보드 정보 363
Firepower System 대시보드 위젯 364
위젯 가용성 365
사용자 역할별 대시보드 위젯 가용성 365
사전 정의된 대시보드 위젯 366
어플라이언스 정보 위젯 367
어플라이언스 상태 위젯 367
상관관계 이벤트 위젯 367

현재 인터페이스 상태 위젯 368
현재 세션 위젯 368
맞춤형 분석 위젯 369
디스크 사용량 위젯 373
인터페이스 트래픽 위젯 374
침입 이벤트 위젯 374
네트워크 컴플라이언스 위젯 375
제품 라이선싱 위젯 376
제품 업데이트 위젯 376
RSS 피드 위젯 377
시스템 로드 위젯 377
시스템 시간 위젯 377
화이트 목록 이벤트 위젯 378
대시보드 관리 378
대시보드 추가 379
대시보드에 위젯 추가 379
위젯 환경설정 구성 380
맞춤형 대시보드 생성 381
맞춤형 대시보드 옵션 381
위젯 디스플레이 맞춤 설정 382
대시보드 옵션 수정 383
대시보드 시간 설정 수정 383
대시보드 이름 변경 384
Viewing Dashboards 385

장 15
상태 모니터링 387
상태 모니터링 요구 사항 및 사전 요건 387
상태 모니터링 정보 387
상태 모듈 389
상태 모니터링 구성 397
상태 정책 398

기본 상태 정책 398
상태 정책 생성 398
상태 정책 적용 399
상태 정책 수정 400
상태 정책 삭제 401
상태 모니터 블랙리스트 402
어플라이언스를 블랙리스트에 추가 402
상태 정책 모듈을 블랙리스트에 추가 403
상태 모니터 알림 404
상태 모니터 알림 정보 404
상태 모니터 알림 생성 405
상태 모니터 알림 수정 406
상태 모니터 알림 삭제 406
상태 모니터 사용 407
디바이스 상태 모니터 408
시스템 세부 사항 및 문제 해결 보기 409
디바이스 상태 모니터 보기 410
FMC 상태 모니터 보기 418
어플라이언스에 대해 모든 모듈 실행 418
특정 상태 모듈 실행 419
상태 모듈 알림 그래프 생성 420
상태 모니터 상태 카테고리 420
상태 이벤트 보기 421
상태 이벤트 보기 421
모듈 및 어플라이언스별로 상태 이벤트 보기 422
상태 이벤트 테이블 보기 422
7000 및 8000 Series 디바이스에 대한 하드웨어 알림 세부 정보 423
상태 이벤트 테이블 426
상태 모니터링 기록 428

장 16 시스템 모니터링 431

시스템 통계 관련 정보 431
호스트 통계 섹션 431
Disk Usage(디스크 사용량) 섹션 432
Processes(프로세스) 섹션 432
프로세스 상태 필드 432
시스템 데몬 434
실행 파일및 시스템 유틸리티 436
The SFDataCorrelator 프로세스 통계 섹션 439
침입 이벤트 정보 섹션 440
시스템 통계 보기 440
시스템 메시지 441
메시지 유형 442
메시지 관리 443
시스템 메시지 관리 444
구축 메시지 보기 444
상태 메시지 보기 445
작업 메시지 보기 445
작업 메시지 관리 446
알림 동작 설정 446

장 17 시스템 감사 449
시스템 로그 449
시스템 로그 보기 449
시스템 로그 필터 구문 450
시스템 감사 정보 451
감사 기록 451
감사 레코드 보기 451
감사 레코드 억제 455

장 18 시스템 문제 해결 461
문제 해결의 첫 번째 단계 461

시스템 메시지 462
메시지 유형 462
메시지 관리 464
기본 시스템 정보 보기 464
어플라이언스 정보 보기 465
시스템 메시지 관리 465
구축 메시지 보기 465
상태 메시지 보기 466
작업 메시지 보기 466
작업 메시지 관리 467
알림 동작 설정 467
상태 모니터 알림의 메모리 사용량 임계값 468
이벤트 상태 모니터 알림의 디스크 사용량 및 소모 469
문제 해결을 위한 상태 모니터 보고서 473
특정 시스템 기능에 대한 문제 해결 파일 생성 473
고급 문제 해결 파일 다운로드 474
일반 문제 해결 475
연결 기반 문제 해결 475
연결 문제 해결 476
Firepower Threat Defense 디바이스의 고급 문제 해결 476
웹 인터페이스에서 FTD CLI 사용 476
기능별 문제 해결 477

부 IV: 구축 관리 479

장 19 도메인 관리 481
도메인을 사용하는 다중 테넌시 소개 481
도메인 용어 482
도메인 속성 483
도메인 요구 사항 및 사전 요건 485
도메인 관리 485

새 도메인 생성 486
도메인 간 데이터 이동 487
도메인 간 디바이스 이동 487
도메인 관리 기록 489

장 20 정책 관리 491
정책 관리를 위한 요구 사항 및 사전 요건 491
정책 구축 491
구성 변경 사항 구축을 위한 모범 사례 492
구축 상태 493
구축 견적 494
구축 미리보기 494
선택적 정책 구축 495
컨피그레이션 변경 사항 구축 498
디바이스에 기존 구성을 재구축하십시오 500
구축 히스토리 보기 501
구축 롤백 502
디바이스에서 구축 롤백 504
구축 롤백 기록 보기 505
Snort® 재시작 시나리오 505
정책 적용 중에 트래픽 검사 506
Snort® 재시작 트래픽 동작 507
구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션 510
즉시 Snort 프로세스를 재시작시키는 변경 사항 513
정책 비교 513
정책 비교 514
정책 보고서 515
현재 정책 보고서 생성 515
만료된 정책 516
제한된 구축에 대한 성능 고려 사항 516
침입 방지 없이 검색 517

검색 없이 침입 방지 518
정책 관리 히스토리 519

장 21

규칙 관리: 일반 특성 523
규칙 관리 요구 사항 및 사전 요건 523
규칙 소개 524
규칙 조건 유형 525
규칙 조건 메커니즘 527
보안 영역 조건 528
네트워크 조건 530
네트워크 조건 구성 530
VLAN 조건 531
포트 및 ICMP 코드 조건 532
포트 조건 구성 534
애플리케이션 조건(애플리케이션 컨트롤) 535
애플리케이션 조건 및 필터 구성 536
애플리케이션 특성 538
애플리케이션 제어 모범 사례 539
애플리케이션 제어 구성 모범 사례 541
애플리케이션 관련 참고 사항 및 제한 사항 543
애플리케이션 제어 규칙 문제 해결 544
URL 조건(URL 필터링) 545
사용자, 영역 및 ISE 속성 조건(사용자 제어) 545
사용자 제어 사전 요구 사항 546
사용자 및 영역 조건 구성 547
ISE 속성 조건 구성 548
사용자 제어 문제 해결 549
날짜 및 시간 기준 규칙 적용 551
규칙 검색 551
디바이스별 규칙 필터링 552
문제가 있는 규칙 식별 553

규칙 및 기타 정책 경고 554
규칙 관리 기록: 일반 특성 555

장 22 재사용 가능 개체 557
재사용 가능한 개체 소개 558
개체 관리자 560
개체 가져오기 560
개체 수정 563
개체 및 사용 현황 보기 564
개체 또는 개체 그룹 필터링 565
개체 정렬 566
개체 그룹 566
재사용 가능 개체 그룹화 566
개체 재정의 568
개체 재정의 관리 569
개체 재정의 허용 570
개체 재정의 추가 570
개체 오버라이드 편집 571
네트워크 개체 571
네트워크 개체 생성 571
네트워크 개체 가져오기 572
포트 개체 572
포트 개체 생성 573
포트 개체 가져오기 574
애플리케이션 필터 574
VLAN 태그 개체 574
VLAN 태그 개체 생성 574
URL 개체 575
URL 개체 생성 575
지리위치 개체 576
지리위치 개체 생성 576

보안 영역 577
보안 영역 개체 생성 578
시간 범위 개체 578
시간 범위 개체 생성 578
표준 시간대 개체 580
변수 집합 580
침입 정책 내 변수 집합 581
변수 582
사전 정의된 기본 변수 582
네트워크 변수 585
포트 변수 586
고급 변수 588
변수 재설정 588
집합에 변수 추가 589
중첩 변수 590
변수 집합 관리 592
변수 집합 생성 593
변수 관리 593
변수 추가 594
변수 편집 595
보안 인텔리전스 목록 및 피드 597
보안 인텔리전스 개체 수정 방법 598
글로벌 및 도메인 보안 인텔리전스 목록 598
보안 인텔리전스 목록 및 멀티테넌시 599
전역 보안 인텔리전스 목록에 항목 추가 600
전역 보안 인텔리전스 목록에서 항목 삭제 602
보안 인텔리전스 목록 및 피드 업데이트 602
보안 인텔리전스 피드에 대한 업데이트 빈도 변경 603
사용자 지정 보안 인텔리전스 목록 및 피드 603
사용자 지정 목록 및 피드: 요구 사항 603
URL 목록 및 피드: URL 구문 및 일치 기준 604

맞춤형 보안 인텔리전스 피드 605
맞춤형 보안 인텔리전스 목록 607
싱크홀 개체 609
싱크홀 개체 생성 609
파일 목록 610
파일 목록에 대한 소스 파일 610
파일 목록에 개별 SHA-256 값 추가 611
파일 목록에 개별 파일 업로드 612
파일 목록에 소스 파일 업로드 613
파일 목록에서 SHA-256 값 수정 614
파일 목록에서 소스 파일 다운로드 615
암호 그룹 목록 615
암호 그룹 목록 생성 615
고유 이름 개체 616
고유 이름(DN) 개체 생성 617
PKI 개체 618
내부 인증 기관 개체 619
CA 인증서 및 개인 키 가져오기 620
CA 인증서 및 개인 키 가져오기 620
새 CA 인증서 및 개인 키 생성 621
새로 서명된 인증서 621
서명되지 않은 CA 인증서 및 CSR 생성 622
CSR에 응답하여 발행된 서명된 인증서 업로드 622
CA 인증서 및 개인 키 다운로드 623
CA 인증서 및 개인 키 다운로드 623
신뢰할 수 있는 인증 기관 개체 624
신뢰할 수 있는 CA 개체 624
신뢰할 수 있는 CA 개체 추가 625
신뢰할 수 있는 CA 개체의 인증서 해지 목록 625
신뢰할 수 있는 CA 개체에 인증서 해지 목록 추가 626
외부 인증서 개체 626

외부 인증서 개체 추가 627
내부 인증서 개체 627
내부 인증서 개체 추가 628
인증서 등록 개체 628
인증서 등록 개체 추가 630
인증서 등록 개체 SCEP 옵션 632
인증서 등록 개체 인증서 매개변수 633
인증서 등록 개체 키 옵션 634
인증서 등록 개체 폐기 옵션 634
키 체인 개체 635
키 체인 개체 생성 636
DNS 서버 그룹 개체 637
DNS 서버 그룹 개체 생성 637
SLA 모니터 개체 638
접두사 목록 639
IPv6 접두사 목록 구성 640
IPv4 접두사 목록 구성 640
경로 맵 641
액세스 목록 644
확장 ACL 개체 설정 645
표준 ACL 개체 설정 646
AS 경로 개체 647
커뮤니티 목록 648
정책 목록 649
VPN 개체 650
FTD IKE 정책 651
IKEv1 정책 개체 구성 651
IKEv2 정책 개체 구성 652
FTD IPSec 제안 654
IKEv1 IPsec 제안 개체 설정 654
IKEv2 IPsec 제안 개체 설정 655

FTD 그룹 정책 개체 656
그룹 정책 개체 설정 656
그룹 정책 일반 옵션 657
그룹 정책 AnyConnect 옵션 659
그룹 정책 고급 옵션 662
FTD 파일 개체 663
FTD 인증서 맵 개체 665
주소 풀 666
FlexConfig 개체 667
RADIUS 서버 그룹 667
RADIUS 서버 그룹 옵션 668
RADIUS 서버 옵션 669
SSO(Single Sign-On) 서버 추가 670
재사용 가능 개체 히스토리 672

장 23 **Firepower Threat Defense** 인증서 기반 인증 675
FTD 인증서 기반 인증 요구 사항 및 사전 요건 675
Firepower Threat Defense VPN 인증서 가이드라인 및 제한 사항 676
FTDVPN 인증서 매핑 677
자체 서명 등록을 사용한 인증서 설치 678
SCEP 등록을 사용한 인증서 설치 679
수동 등록을 사용한 인증서 설치 680
PKCS12 파일을 가져오는 방법으로 인증서 설치 681
FTD VPN 인증서 문제 해결 681
Firepower Threat Defense 인증서 기반 인증 히스토리 682

부 V: 클래식 디바이스 구성 기본 사항 683

장 24 클래식 디바이스 관리 기본 사항 685
클래식 디바이스 관리 요구 사항 및 사전 요건 685
원격 관리 구성(클래식 디바이스) 685

매니지드 디바이스에서 원격 관리 구성 686
매니지드 디바이스에서 원격 관리 수정 687
관리 포트 변경 687
인터페이스 설정 688
물리적 하드웨어 보기 688
인터페이스 페이지 689
인터페이스 아이콘 690
물리적 하드웨어 보기 사용 690
센싱 인터페이스 설정 691
HA 링크 인터페이스 설정 692
인터페이스 비활성화 693
Cisco ASA FirePOWER 인터페이스 관리 694
7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위 695
보안 영역 개체의 수정 버전 동기화 695

장 25

IPS 디바이스 구축 및 구성 697
IPS 디바이스 구축 및 구성 소개 697
IPS 디바이스 구축 라이선스 요구 사항 697
IPS 디바이스 구축 요구 사항 및 사전 요건 697
수동 IPS 구축 698
Firepower System의 패시브 인터페이스 698
패시브 인터페이스 구성 699
인라인 IPS 구축 700
Firepower System의 인라인 인터페이스 702
인라인 인터페이스 구성 702
Firepower System의 인라인 집합 703
인라인 집합 보기 704
인라인 집합 추가 705
고급 인라인 설정 옵션 706
고급 인라인 집합 옵션 구성 707
인라인 집합 삭제 708

부 VI: **Firepower Threat Defense** 시작하기 709

장 26 **Firepower Threat Defense**에 대한 투명 또는 라우팅 방화벽 모드 711

방화벽 모드 정보 711

라우팅 방화벽 모드 정보 711

투명 방화벽 모드 정보 712

네트워크에서 투명 방화벽 사용 712

진단 인터페이스 713

라우팅 모드 기능의 트래픽 전달 713

브리지 그룹 정보 713

BVI(Bridge Virtual Interface) 714

투명 방화벽 모드의 브리지 그룹 714

라우팅 방화벽 모드의 브리지 그룹 715

Layer 3 트래픽 허용 716

허용되는 MAC 주소 716

BPDU 처리 717

MAC 주소 대 경로 조회 비교 717

투명 모드의 브리지 그룹에 대해 지원되지 않는 기능 718

라우팅 모드의 브리지 그룹에 대해 지원되지 않는 기능 719

기본 설정 720

방화벽 모드에 대한 지침 721

방화벽 모드 설정 722

장 27 다음 위치의 **Firepower Threat Defense**에 대한 논리적 디바이스 **Firepower 4100/9300** 725

Firepower 인터페이스 정보 725

섀시 관리 인터페이스 725

인터페이스 유형 726

FXOS 인터페이스와 애플리케이션 인터페이스 비교 727

공유 인터페이스 확장성 730

공유 인터페이스 모범 사례 730

공유 인터페이스 사용 예시 732
공유 인터페이스 리소스 보기 739
Firepower Threat Defense에 대한 인라인 집합 링크 상태 전파 739
논리적 디바이스 정보 740
독립형 논리적 디바이스와 클러스터형 논리적 디바이스 740
논리적 디바이스 애플리케이션 인스턴스: 컨테이너 및 기본 740
컨테이너 인스턴스 인터페이스 741
섀시가 패킷을 분류하는 방법 741
분류의 예 742
연속 컨테이너 인스턴스 745
일반적인 다중 인스턴스 구축 746
컨테이너 인스턴스 인터페이스용 자동 MAC 주소 747
컨테이너 인스턴스 리소스 관리 748
다중 인스턴스 기능의 성능 확장 요인 748
컨테이너 인스턴스 및 고가용성 748
컨테이너 인스턴스 및 클러스터링 748
컨테이너 인스턴스용 라이선스 748
논리적 디바이스의 요구 사항 및 사전 요구 사항 749
하드웨어 및 소프트웨어 조합에 대한 요건 및 사전 요구 사항 749
컨테이너 인스턴스의 요구 사항 및 사전 요구 사항 751
고가용성 요구 사항 및 전제 조건 752
논리적 디바이스 관련 지침 및 제한 사항 753
Firepower 인터페이스에 대한 지침 및 제한 사항 753
일반 지침 및 제한 사항 755
인터페이스 구성 756
인터페이스 활성화 또는 비활성화 756
실제 인터페이스 구성 757
EtherChannel(포트 채널) 추가 758
컨테이너 인스턴스에 VLAN 하위 인터페이스 추가 760
논리적 디바이스 구성 761
컨테이너 인스턴스에 대한 리소스 프로파일 추가 761

용 독립형 Firepower Threat Defense 추가 763
고가용성 쌍 추가 769
Firepower Threat Defense 논리적 디바이스의 인터페이스 변경 769
애플리케이션 콘솔에 연결 771
History for Firepower Threat Defense Logical Devices 773

부 VII: **Firepower Threat Defense** 인터페이스 및 디바이스 설정 781

장 28 **Firepower Threat Defense** 인터페이스 개요 783
관리/진단 인터페이스 783
관리 인터페이스 783
진단 인터페이스 783
인터페이스 모드 및 유형 784
보안 영역 및 인터페이스 그룹 785
Auto-MDI/MDIX 기능 786
인터페이스의 기본 설정 786
물리적 인터페이스 활성화 및 이더넷 설정 787
Firepower Management Center를 사용한 동기화 인터페이스 변경 788

장 29 **Firepower Threat Defense** 일반 방화벽 인터페이스 793
정규 방화벽 인터페이스 요구 사항 및 사전 요건 793
Firepower 1010 스위치 포트 구성 794
Firepower 1010 스위치 포트 관련 정보 794
Firepower 1010 포트 및 인터페이스 이해 794
Auto-MDI/MDIX 기능 795
Firepower 1010 스위치 포트에 대한 지침 및 제한 사항 795
스위치 포트 및 PoE(Power over Ethernet) 구성 796
스위치 포트 모드 활성화 또는 비활성화 797
VLAN 인터페이스 구성 797
스위치 포트를 액세스 포트로 구성 799
스위치 포트를 트렁크 포트로 구성 801

PoE(Power over Ethernet) 구성 803
EtherChannel 및 이중 인터페이스 구성 804
EtherChannel 및 이중 인터페이스 정보 804
이중 인터페이스 관련 정보(ASA 플랫폼 전용) 804
EtherChannel 정보 805
EtherChannel 및 이중 인터페이스에 대한 지침 807
이중화 인터페이스 구성(ASA 플랫폼만 해당) 809
EtherChannel 구성 810
VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성 812
VLAN 하위 인터페이스에 대한 가이드라인 및 제한 사항 812
디바이스 모델별 VLAN 하위 인터페이스의 최대 수 813
하위 인터페이스 추가 813
라우팅 및 투명 모드 인터페이스 구성 814
라우팅 및 투명 모드 인터페이스 정보 814
이중 IP 스택(IPv4 및 IPv6) 815
라우팅 모드 및 투명 모드 인터페이스에 대한 지침 및 제한 사항 815
라우팅 모드 인터페이스 구성 817
브리지 그룹 인터페이스 구성 821
일반 브리지 그룹 멤버 인터페이스 파라미터 구성 821
BVI(Bridge Virtual Interface) 구성 823
투명 모드의 진잔(관리) 인터페이스 구성 824
IPv6 주소 지정 구성 826
IPv6 정보 826
전역 IPv6 주소 구성 827
IPv6 네이버 검색 구성 829
고급 인터페이스 설정 구성 832
고급 인터페이스 구성 정보 832
MAC 주소 정보 832
MTU 정보 833
TCP MSS 정보 834
브리지 그룹 트래픽에 대한 ARP 검사 835

MAC 주소 테이블 836
기본 설정 836
ARP 검사 및 MAC 주소 테이블에 대한 지침 837
MTU 구성 837
MAC 주소 구성 838
고정 ARP 항목 추가 839
고정 MAC 주소를 추가하고 브리지 그룹에 대한 MAC 학습을 비활성화합니다. 840
보안 구성 파라미터 설정 841
Firepower Threat Defense 일반 방화벽 인터페이스 기록 843

장 30

Firepower Threat Defense 인라인 집합 및 패시브 인터페이스 847
IPS 인터페이스 847
IPS 인터페이스 유형 847
인라인 집합용 하드웨어 바이패스 정보 848
하드웨어 바이패스 트리거 848
하드웨어 우회 전환 849
Snort Fail Open vs.하드웨어 바이패스 849
하드웨어 바이패스 Status(상태) 849
인라인 집합의 요구 사항 및 사전 요건 850
인라인 집합 및 패시브 인터페이스 가이드라인 851
패시브 인터페이스 구성 852
인라인 집합 구성 853
Firepower Threat Defense 인라인 집합 및 패시브 인터페이스 기록 857

장 31

Threat Defense용 **DHCP** 및 **DDNS** 서비스 859
DHCP 및 DDNS 서비스 정보 859
DHCPv4 서버 정보 859
DHCP 옵션 859
DHCP 릴레이 에이전트 소개 860
DHCP 및 DDNS 요구 사항 및 사전 요건 860
DHCP 및 DDNS 서비스에 대한 지침 861

DHCP 서버 구성 862
DHCP 릴레이 에이전트 구성 864
동적 DNS 구성 865

장 32 **Firepower 1000/2100 용 SNMP** 873
Firepower 1000/2100 시리즈용 SNMP 정보 873
Firepower 1000/2100용 SNMP 활성화 및 SNMP 속성 구성 873
Firepower 1000 /2100용 SNMP 트랩 생성 875
Firepower 1000/2100에 대한 SNMP 사용자 생성 876

장 33 **QoS(Quality of Service) Firepower Threat Defense** 879
QoS 소개 879
QoS 정책 정보 879
QoS 요구 사항 및 사전 요건 880
QoS 정책을 사용한 속도 제한 881
QoS 정책 생성 882
QoS 정책에 대한 대상 디바이스 설정 882
QoS 규칙 구성 883
QoS 규칙 구성 요소 884

부 VIII: **Firepower Threat Defense** 고가용성 및 확장성 887

장 34 **Firepower Threat Defense**의 고가용성 889
Firepower Threat Defense 고가용성 정보 889
고가용성 시스템 요구 사항 889
하드웨어 요구 사항 890
소프트웨어 요구 사항 890
고가용성 쌍의 FTD 디바이스에 대한 라이선스 요구 사항 891
페일오버 및 스테이트풀 페일오버 링크 891
페일오버 링크 891
스테이트풀 페일오버 링크 893

페일오버 및 데이터 링크 중단 방지 893
MAC 주소와 IP 주소 - 고가용성 895
스테이트풀 페일오버 896
지원 기능 896
지원되지 않는 기능 898
고가용성에 대한 브리지 그룹 요구 사항 898
장애 조치 상태 모니터링 899
유닛 상태 모니터링 899
인터페이스 모니터링 899
장애 조치 시간 901
액티브/스탠바이 페일오버 정보 902
기본/보조 역할 및 액티브/스탠바이 상태 903
시작 시 액티브 유닛 결정 903
페일오버 이벤트 903
고가용성 요구 사항 및 전제 조건 904
고가용성 지침 905
Firepower Threat Defense 고가용성 쌍 추가 906
선택적 고가용성 파라미터 구성 908
스탠바이 IP 주소 및 인터페이스 모니터링 구성 908
고가용성 페일오버 기준 수정 909
가상 MAC 주소 구성 910
Manage(관리) 고가용성 910
Firepower Threat Defense 고가용성 쌍의 활성 피어 전환 910
고가용성 일시 중단 또는 재개 911
FTD 고가용성 쌍의 유닛 교체 912
기본 FTD HA 유닛을 백업 없이 교체 912
보조 FTD HA 유닛을 백업 없이 교체 913
고가용성 쌍의 유닛 분리 914
고가용성 쌍 등록 해제 914
모니터링 고가용성 915
페일오버 기록 보기 915

스테이트풀 페일오버 통계 보기 915

장 35

Firepower Threat Defense 클러스터링 917

Firepower 4100/9300 섀시 클러스터링 정보 917

부트스트랩 컨피그레이션 918

클러스터 멤버 918

Cluster Control Link 919

섀시 간 클러스터링을 위한 클러스터 제어 링크 크기 조정 919

섀시 간 클러스터링을 위한 클러스터 제어 링크 이중화 919

섀시 간 클러스터링을 위한 클러스터 제어 링크 안정성 920

클러스터 제어 링크 네트워크 920

관리 네트워크 920

관리 인터페이스 920

클러스터 인터페이스 921

Spanned EtherChannels 921

VSS 또는 vPC에 연결 922

구성 복제 922

클러스터링용 라이선스 922

클러스터링의 요구 사항 및 사전 요구 사항 923

클러스터링 지침 및 제한 사항 926

클러스터링 설정 930

FXOS: Firepower Threat Defense 클러스터 추가 930

Firepower Threat Defense 클러스터 생성 930

클러스터 유닛 추가 941

FMC: 클러스터 추가 943

FMC: 클러스터, 데이터, 진단 인터페이스 구성 948

FXOS: 클러스터 유닛 제거 950

FMC: 클러스터 멤버 관리 952

새 클러스터 멤버 추가 952

클러스터 멤버 교체 953

멤버 비활성화 954

클러스터 재참가 955
데이터 유닛 삭제 955
제어 유닛 변경 957
클러스터 멤버 조정 957
FMC: 클러스터 모니터링 958
클러스터링에 대한 참조 959
Firepower Threat Defense 기능 및 클러스터링 959
클러스터링으로 지원되지 않는 기능 959
클러스터링을 위한 중앙 집중식 기능 960
동적 라우팅 및 클러스터링 960
연결 설정 961
FTP 및 클러스터링 961
NAT 및 클러스터링 962
SIP 검사 및 클러스터링 963
SNMP 및 클러스터링 963
Syslog 및 클러스터링 963
TLS/SSL 연결 및 클러스터링 964
Cisco TrustSec 및 클러스터링 964
성능 확장 요소 964
제어 유닛 선택 964
클러스터 내의 고가용성 965
섀시 애플리케이션 모니터링 965
유닛 상태 모니터링 965
인터페이스 모니터링 965
데코레이터 애플리케이션 모니터링 966
실패 이후 상태 966
클러스터 다시 참가 966
데이터 경로 연결 상태 복제 967
클러스터에서 연결을 관리하는 방법 968
연결 역할 968
새 연결 소유권 969

샘플 데이터 흐름 969
클러스터링 기록 970

부 IX: **Firepower Threat Defense** 라우팅 975

장 36 **Firepower Threat Defense** 라우팅 개요 977
경로 결정 977
지원되는 경로 유형 978
고정 대 동적 978
단일 경로 대 다중 경로 978
평면 대 계층형 978
연결 상태 대 거리 벡터 979
라우팅을 위한 지원되는 인터넷 프로토콜 979
라우팅 테이블 980
라우팅 테이블을 채우는 방법 980
경로의 관리 거리 981
동적 및 부동 정적 경로 백업 982
포워딩 결정 방법 982
클러스터링의 동적 라우팅 983
관리 트래픽용 라우팅 테이블 984
ECMP(Equal-Cost Multi-Path) 라우팅 984
경로 맵 정보 984
허용 및 거부 절 985
절의 일치 및 설정 값 985

장 37 **Firepower Threat Defense**에 대한 가상 라우팅 987
가상 라우터 및 VRF(가상 라우팅 및 포워딩) 정보 987
가상 라우터의 애플리케이션 988
전역 및 사용자 정의 가상 라우터 988
가상 라우터 인식 정책 구성 989
인터커넥트 가상 라우터 990

중복된 IP 주소 991
디바이스 모델별 최대 가상 라우터 수 992
가상 라우터를 위한 요구 사항 및 사전 요건 993
가상 라우터 대한 지침 및 제한 사항 993
FMC 웹 인터페이스 라우팅 페이지에 대한 수정 사항 995
가상 라우터 관리 페이지 996
가상 라우터 생성 996
가상 라우터 구성 996
가상 라우터 수정 998
가상 라우터 제거 999
가상 라우터의 구성 예시 1000
가상 라우터를 통해 원거리 서버로 라우팅하는 방법 1000
중복된 주소 공간에 인터넷 액세스를 제공하는 방법 1005
RA VPN 액세스를 가상 라우터의 내부 네트워크에 허용하는 방법 1012
사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법 1015
가상 라우팅에서 두 개의 중복되는 네트워크 호스트 간에 트래픽을 라우팅하는 방법 1019
BVI 인터페이스를 사용하여 라우팅 방화벽 모드에서 중복 세그먼트를 관리하는 방법 1022
중복되는 네트워크로 사용자 인증을 구성하는 방법 1026
Firepower Threat Defense의 가상 라우터 기록 1033

장 38

Firepower Threat Defense 정적 및 기본 경로 1035
고정 경로 및 기본 경로 소개 1035
기본 라우터 1035
고정 경로 1035
원치 않는 트래픽을 지우기 위한 null0 인터페이스로의 경로 1036
경로 우선 순위 1036
투명 방화벽 모드 및 브리지 그룹 경로 1036
고정 경로 추적 1037
정적 경로 요구 사항 및 사전 요건 1037
고정 경로 및 기본 경로를 위한 지침 1038
고정 경로 추가 1038

장 39 **Firepower Threat Defense OSPF** 1041

Firepower Threat Defense OSPF 1041

OSPF 정보 1041

Fast Hello 패킷에 대한 OSPF 지원 1043

OSPF의 Fast Hello 패킷 지원 사전 요구 사항 1043

OSPF Hello 간격 및 Dead 간격 1043

OSPF Fast Hello 패킷 1043

OSPF Fast Hello 패킷 기능의 이점 1044

OSPFv2와 OSPFv3의 구현 차이점 1044

OSPF 요구 사항 및 사전 요건 1044

OSPF에 대한 지침 1045

OSPFv2 구성 1047

OSPF 영역, 범위 및 가상 링크 구성 1047

OSPF 재배포 구성 1050

OSPF 영역 간 필터링 구성 1051

OSPF 필터 규칙 구성 1053

OSPF 요약 주소 구성 1054

OSPF 인터페이스 및 네이버 구성 1055

OSPF 고급 속성 구성 1057

OSPFv3 구성 1060

OSPFv3 영역, 경로 요약 및 가상 링크 구성 1060

OSPFv3 재배포 구성 1062

OSPFv3 요약 접두사 설정 1064

OSPFv3 인터페이스, 인증 및 네이버 설정 1065

OSPFv3 고급 속성 설정 1068

장 40 **Firepower Threat Defense BGP** 1073

BGP 소개 1073

라우팅 테이블 변경 사항 1073

BGP를 사용해야 하는 시기 1074

BGP 경로 선택 1075
BGP 다중 경로 1075
BGP 요구 사항 및 사전 요건 1076
BGP를 위한 지침 1077
BGP 구성 1077
BGP 기본 설정 구성 1078
SNMP 일반 설정 구성 1080
BGP 네이버 설정 구성 1082
BGP 집계 주소 설정 1086
BGPv4 필터링 설정 1087
BGP 네트워크 설정 1087
BGP 재배포 설정 1088
BGP 라우트 삽입 설정 1089

장 41 **Firepower Threat Defense RIP** 1091
RIP 정보 1091
라우팅 업데이트 프로세스 1092
RIP 라우팅 메트릭 1092
RIP 안정성 기능 1092
RIP 타이머 1092
RIP에 대한 요구 사항 및 사전 요건 1093
RIP 가이드라인 1093
RIP 설정 1094

장 42 **Firepower Threat Defense** 멀티캐스트 라우팅 1099
멀티캐스트 라우팅 정보 1099
IGMP 프로토콜 1100
stub 멀티캐스트 라우팅 1100
PIM 멀티캐스트 라우팅 1101
PIM 소스별 멀티캐스트 지원 1101
멀티캐스트 양방향 PIM 1101

PIM BSR(부트스트랩 라우터) 1102
PIM BSR(부트스트랩 라우터) 용어 1102
멀티캐스트 그룹 개념 1103
멀티캐스트 주소 1103
클러스터링 1103
멀티캐스트 라우팅 요구 사항 및 사전 요건 1103
멀티캐스트 라우팅 지침 1104
IGMP 기능 구성 1104
멀티캐스트 라우팅 활성화 1105
IGMP 프로토콜 구성 1106
IGMP 액세스 그룹 구성 1107
IGMP 고정 그룹 구성 1108
IGMP 조인 그룹 구성 1109
PIM 기능 구성 1110
PIM 프로토콜 구성 1110
PIM 네이버 필터 구성 1111
PIM 양방향 네이버 필터 구성 1112
PIM 랑데부 포인트 설정 1113
PIM 라우트 트리 설정 1114
PIM 요청 필터 설정 1115
Firepower Threat Defense 디바이스를 후보 BSR(Bootstrap Router)로 구성 1115
멀티캐스트 라우트 설정 1116
멀티캐스트 경계 필터 설정 1117

부 X: **Firepower Threat Defense VPN** 1119

장 43 **Firepower Threat Defense VPN 개요** 1121
VPN 유형 1121
VPN 기본 사항 1122
IKE(Internet Key Exchange) 1123
IPSec 1123

VPN 패킷 플로우 1124
VPN 라이선싱 1125
VPN 연결의 보안 수준 결정 1125
보안 인증 요구 사항 준수 1125
사용할 암호화 알고리즘 결정 1125
사용할 해시 알고리즘 결정 1126
사용할 Diffie-Hellman 모듈러스 그룹 결정 1127
제거되었거나 사용되지 않는 해시 알고리즘, 암호화 알고리즘 및 Diffie-Hellman 모듈러스 그룹 1128
VPN 토폴로지 옵션 1128
Point-to-Point VPN 토폴로지 1129
허브 앤 스포크 VPN 토폴로지 1129
풀 메시 VPN 토폴로지 1130
암시적 토폴로지 1131

장 44 **Site-to-Site VPN Firepower Threat Defense** 1133
Firepower Threat Defense Site-to-Site VPN 정보 1133
Firepower Threat Defense Site-to-Site VPN 지침 및 제한 사항 1135
사이트 간 VPN 요구 사항 및 사전 요건 1135
Firepower Threat Defense Site-to-Site VPN 관리 1136
Firepower Threat Defense Site-to-Site VPN 구성 1137
FTD VPN 엔드포인트 옵션 1138
FTD VPN IKE 옵션 1140
FTD VPN IPsec 옵션 1141
FTD 고급 Site-to-site VPN 구축 옵션 1143
FTD VPN 고급 IKE 옵션 1143
FTD VPN 고급 IPsec 옵션 1144
FTD 고급 Site-to-site VPN 터널 옵션 1145
Sysopt Connection Permit-vpn 옵션 활성화 1146
Virtual Tunnel Interface 정보 1146
Virtual Tunnel Interface에 대한 지침 및 제한 사항 1147

VTI 인터페이스 추가 1148
라우트 기반 사이트 대 사이트 VPN 생성 1149
VTI에 대한 추가 구성 1150
사이트 간 VPN 기록 1152

장 45 **Remote Access VPN Firepower Threat Defense** 1155
원격 액세스 VPN 개요 1155
Remote Access VPN 기능 1156
AnyConnect 구성 요소 1157
Remote Access VPN 인증 1158
권한 및 속성 정책 시행 이해 1159
AAA 서버 연결 이해 1160
원격 액세스 VPN 라이선스 요구 사항 1162
원격 액세스 VPN 요구 사항 및 사전 요건 1162
Remote Access VPN 가이드라인 및 제한 사항 1162
새 Remote Access VPN 연결 구성 1165
Remote Access VPN 구성 사전 요구 사항 1165
새 Remote Access VPN 정책 생성 1166
Firepower Threat Defense 디바이스의 액세스 제어 정책 업데이트 1168
(선택 사항) NAT 제외 설정 1169
DNS 구성 1170
AnyConnect 클라이언트 프로파일 XML 파일 추가 1171
(선택 사항) 스플릿 터널링 구성 1172
구성 확인 1172
원격 액세스 VPN 정책 대상 디바이스 설정 1173
선택적 Remote Access VPN 구성 1173
연결 프로파일 설정 1173
여러 연결 프로파일 설정 1174
VPN 클라이언트에 대한 IP 주소 설정 1175
Remote Access VPN에 대한 AAA 설정 1177
연결 프로파일에 대한 별칭 생성 또는 업데이트 1183

Remote Access VPN을 위한 액세스 인터페이스 구성 1184
Remote Access VPN 고급 옵션 설정 1186
Cisco AnyConnect Remote Access VPN 클라이언트 이미지 1186
Remote Access VPN 주소 할당 정책 1188
연결 프로파일 매핑에 대한 인증서 설정 1189
그룹 정책 구성 1189
LDAP 특성 매핑 구성 1190
IPsec 설정 1192
RADIUS 동적 권한 부여 1198
RADIUS 동적 권한 부여 구성 1198
이중 인증 1199
RSA 이중 인증 구성 1200
듀오 이중 인증 구성 1202
보조 인증 1203
Remote Access VPN 보조 인증 구성 1204
SAML 2.0을 사용한 SSO(Single Sign-On) 인증 1206
SAML SSO(Single Sign-On) 인증 구성 1207
Remote Access VPN AAA 사용자 지정 1208
클라이언트 인증서를 통한 VPN 사용자 인증 1208
클라이언트 인증서 및 AAA 서버를 통한 Remote Access VPN 로그인 설정 1209
VPN 세션에 대한 암호 변경 관리 1211
인증을 위한 LDAP 또는 Active Directory 설정 1212
RADIUS 서버로 계정 기록 전송 1213
권한 부여 서버에 그룹 정책 선택 위임 1214
그룹 정책 또는 기타 속성 선택을 권한 부여 서버로 재정의 1215
사용자 그룹에 대한 VPN 액세스 거부 1216
사용자 그룹에 대한 연결 프로파일 선택 제한 1217
Remote Access VPN 클라이언트에 대한 AnyConnect 클라이언트 프로파일 업데이트 1218
Remote Access VPN 예시 1219
사용자별 AnyConnect 대역폭을 제한하는 방법 1219
Active Directory 영역 생성 및 설정 1219

QoS 정책 및 규칙 생성 1220
Remote Access VPN 정책 생성 또는 업데이트 1221
사용자 ID 기반 액세스 제어 규칙에 VPN ID를 사용하는 방법 1222
Active Directory 영역 생성 및 설정 1222
ID 정책 및 ID 규칙 생성 1223
ID 정책을 액세스 제어 정책과 연결 1223
Remote Access VPN 정책 생성 또는 업데이트 1224
AnyConnect 관리 VPN 터널 구성 1225
AnyConnect 관리 VPN 터널 요구 사항 및 사전 요건 1225
AnyConnect 관리 VPN 터널의 제한 사항 1226
FTD에서 AnyConnect 관리 VPN 터널 구성 1226
원격 액세스 VPN 히스토리 1228

장 46
Firepower Threat Defense VPN 모니터링 1231
VPN 요약 대시보드 1231
VPN 요약 대시보드 보기 1231
VPN 세션 및 사용자 정보 1232
Remote Access VPN 활성 세션 보기 1232
Remote Access VPN 사용자 활동 보기 1232
VPN 상태 이벤트 1233
VPN 상태 이벤트 보기 1233

장 47
Firepower Threat Defense VPN 문제 해결 1235
시스템 메시지 1235
VPN 시스템 로그 1235
VPN 시스템 이벤트 로그 보기 1236
디버그 명령 1236
debug aaa 1238
debug crypto 1239
debug crypto ca 1240
debug crypto ikev1 1241
debug crypto ikev2 1241

debug crypto ipsec 1242
debug ldap 1242
debug ssl 1243
debug webvpn 1243

부 XI: **Firepower Threat Defense** 고급 설정 1247

장 48 **Threat Defense Service** 정책 1249
Firepower Threat Defense Service 정책 정보 1249
서비스 정책과 FlexConfig 및 기타 기능의 관계 1250
연결 설정이란? 1250
서비스 정책을 위한 요구 사항 및 사전 요건 1251
서비스 정책 가이드라인 및 제한 사항 1252
Firepower Threat Defense Service 정책 설정 1252
서비스 정책 규칙 구성 1253
비동기 라우팅의 TCP 상태 검사 우회(TCP 상태 우회) 1256
비동기 라우팅 문제 1256
TCP 상태 우회 가이드라인 및 제한 사항 1257
TCP 상태 우회 구성 1258
TCP 시퀀스 임의 설정 비활성화 1260
서비스 정책 규칙 예시 1261
SYN 플러딩 DoS 공격(TCP 가로채기)로부터 서버 보호 1262
Firepower Threat Defense 디바이스가 트레이스라우트(traceroute)에 표시되도록 설정 1265
서비스 정책 모니터링 1267
Firepower Threat Defense Service 정책 기록 1268

장 49 **Firepower Threat Defense**에 대한 **FlexConfig** 정책 1269
FlexConfig 정책 개요 1269
FlexConfig 정책에 대한 추천 사용 1270
FlexConfig 개체의 CLI 명령 1270
ASA 소프트웨어 버전 및 현재 CLI 컨피그레이션 확인 1271
금지된 CLI 명령 1272

템플릿 스크립트 1274
FlexConfig 변수 1274
변수 처리 방법 1275
값이 디바이스에 대해 반환하는 사항을 확인하는 방법 1278
FlexConfig 정책 개체 변수 1279
FlexConfig 시스템 변수 1280
사전 정의된 FlexConfig 개체 1281
사전 정의된 텍스트 개체 1286
FlexConfig 정책에 대한 요구 사항 및 사전 요건 1291
FlexConfig 가이드라인 및 제한 사항 1291
FlexConfig 정책을 사용한 디바이스 설정 맞춤 설정 1291
FlexConfig 개체 구성 1293
FlexConfig 개체에 정책 개체 변수 추가 1296
비밀 키 구성 1297
FlexConfig 텍스트 개체 설정 1298
FlexConfig 정책 설정 1299
FlexConfig 정책에 대한 대상 디바이스 설정 1300
FlexConfig 정책 미리보기 1301
구축된 설정 확인 1302
FlexConfig를 사용하여 설정된 기능 제거 1304
FlexConfig의 예시 1306
Precision Time Protocol을 구성하는 방법(ISA 3000) 1306
정전(ISA 3000)에 대한 자동 하드웨어 우회를 구성하는 방법 1310
정책 기반 라우팅 구성 방법 1312
FlexConfig를 위한 기록 1320

장 50

Cisco ISA 3000에 대한 알람 1323
알람 정보 1323
알람 입력 인터페이스 1324
알람 출력 인터페이스 1324
Syslog 알람 1325

SNMP 알람 1325
알람 기본값 1325
알람 요구 사항 및 사전 요건 1326
ISA 3000에 대한 알람 구성 1326
알람 입력 접촉부 구성 1326
전원 공급 장치 알람 구성 1329
온도 알람 구성 1332
알람 모니터링 1335
알람 상태 모니터링 1335
Syslog 메시지에서 알람 모니터링 1335
외부 알람 끄기 1336
알람에 대한 기록 1336

부 XII: 어플라이언스 플랫폼 설정 1337

장 51 시스템 구성 1339
시스템 컨피그레이션 요구 사항 및 전제 조건 1340
시스템 구성 관련 정보 1340
Firepower Management Center 시스템 구성 탐색 1340
시스템 구성 설정 1341
어플라이언스 정보 1343
어플라이언스 정보 보기 1344
기본 시스템 정보 보기 1344
HTTPS 인증서 1344
기본 HTTPS 서버 인증서 1345
맞춤형 HTTPS 서버 인증서 1345
HTTPS 클라이언트 인증서 1345
현재 서버 인증서 보기 1346
인증서 서명 요청 생성 및 제출 1346
서버 인증서 업로드 1347
서버 인증서 업로드 1347

유효한 사용자 인증서 필요 1348
기본 HTTPS 서버 인증서 갱신 1349
외부 데이터베이스 액세스 설정 1349
데이터베이스에 대한 외부 액세스 활성화 1350
데이터베이스 이벤트 제한 수 1350
데이터베이스 이벤트 제한 구성 1351
데이터베이스 이벤트 제한 수 1351
Management Interfaces(관리 인터페이스)관리 인터페이스 1353
FMC 관리 인터페이스 정보 1353
FMC의 관리 인터페이스 1353
FMC 모델별 관리 인터페이스 지원 1354
FMC 관리 인터페이스의 네트워크 라우트 1354
NAT 환경 1355
관리 및 이벤트 트래픽 채널 예시 1357
FMC 관리 인터페이스 수정 1358
종료 또는 재시작 1362
FMC를 종료하거나 재시작합니다. 1362
원격 스토리지 관리 1363
로컬 스토리지 설정 1363
원격 스토리지에 대한 NFS 설정 1364
원격 스토리지에 대한 SMB 설정 1365
원격 스토리지에 대한 SSH 설정 1366
원격 스토리지 관리 고급 옵션 1366
검증 번경 1367
검증 변경 구성 1368
검증 변경 옵션 1368
정책 변경 코멘트 1369
정책 변경 추적 코멘트 구성 1369
액세스 목록 1370
액세스 목록 구성 1370
감사 로그 1371

감사 로그 스트리밍 구성 1371
대시보드 설정 1373
대시보드에 대한 맞춤형 분석 위젯 활성화 1373
DNS 캐시 1373
DNS 캐시 속성 설정 1373
이메일 공지 1374
메일 릴레이 호스트 및 알림 주소 구성 1374
언어 선택 1375
웹 인터페이스의 언어 설정 1375
로그인 배너 1376
로그인 배너 사용자 지정 1376
SNMP 폴링 1376
SNMP 폴링 구성 1377
STIG 컴플라이언스 1378
STIG 컴플라이언스 활성화 1378
시간 및 시간 동기화 1379
FMC의 시간을 NTP 서버와 동기화 1380
네트워크 NTP 서버에 액세스하지 않고 시간 동기화 1382
시간 동기화 설정 변경 정보 1383
현재 시스템 시간, 소스 및 NTP 서버 연결 상태 보기 1383
NTP 서버 상태 1384
전역 사용자 구성 1385
비밀번호 재사용 한도 설정 1386
성공적인 로그인 추적 1386
임시 잠금 활성화 1387
최대 동시 세션 수 설정 1388
세션 시간 초과 1388
세션 시간 제한 구성 1388
취약성 매핑 1389
서버의 취약성 매핑 1389
원격 콘솔 액세스 관리 1390

시스템에서 원격 콘솔 설정 1390
LOM(Lights-Out Management) 사용자 액세스 구성 1391
LOM(Lights-Out Management) 사용자 액세스 활성화 1392
SoL(Serial over LAN) 연결 구성 1392
IPMItool을 사용한 SoL(Serial over LAN) 설정 1394
IPMIutil을 사용한 SoL(Serial over LAN) 설정 1394
LOM(Lights-Out Management) 개요 1394
IPMItool을 사용한 LOM(Lights-Out Management) 구성 1396
IPMIutil을 사용한 LOM(Lights-Out Management) 구성 1396
VMware Tools 및 가상 시스템 1396
VMware용 Firepower Management Center의 VMWare Tools 활성화 1397
시스템 구성 기록 1397

장 52 플랫폼 설정 정책 1401
플랫폼 설정 소개 1401
플랫폼 설정 정책을 위한 요구 사항 및 사전 요건 1402
플랫폼 설정 정책 관리 1402
플랫폼 설정 정책 생성 1403
플랫폼 설정 정책에 대한 대상 디바이스 설정 1403

장 53 클래식 디바이스에 대한 플랫폼 설정 1405
클래식 디바이스에 대한 플랫폼 설정 관련 정보 1405
클래식 디바이스에 대한 플랫폼 설정 요구 사항 1406
클래식 디바이스에 대한 플랫폼 설정 구성 1407
클래식 디바이스에 대한 액세스 목록 구성 1407
클래식 디바이스에서의 감사 로그 스트리밍 1408
감사 로그에서 시스템 로그 필터링 1409
7000/8000 시리즈 디바이스에 대한 외부 인증 활성화 1410
7000/8000 시리즈 디바이스에 대한 외부 인증 관련 정보 1411
7000/8000 시리즈 웹 인터페이스 언어 설정 1412
클래식 디바이스에 대한 로그인 배너 맞춤 설정 1412

NTP 서버와 클래식 디바이스의 시간 동기화 1413
클래식 디바이스에 대한 세션 시간 초과 구성 1414
클래식 디바이스에서의 SNMP 폴링 구성 1415
7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성 1416
FMC로의 패킷 전송 금지 1417
7000/8000 시리즈 디바이스의 관리 인터페이스 구성 1417
7000/8000 시리즈 디바이스 종료 또는 재시작 1421
7000/8000 시리즈 디바이스의 시스템 시간 보기 1422

장 54

Firepower Threat Defense 플랫폼 설정 1423
ARP 검사 설정 1423
배너 설정 1425
DNS 구성 1425
프래그먼트 처리 설정 1427
HTTP 설정 1428
ICMP 액세스 규칙 구성 1429
SSL 설정 1431
SSL 설정 정보 1432
에서 SSH(Secure Shell) 설정 1435
SMTP 설정 1437
Threat Defense에 대한 SNMP 설정 1437
SNMPv3 사용자 추가 1439
SNMP 호스트 추가 1441
SNMP 트랩 구성 1442
시스템 로그 구성 관련 정보 1445
Syslog 정보 1445
심각도 레벨 1446
Syslog 메시지 필터링 1446
Syslog 메시지 클래스 1447
로깅 지침 1450
FTD 디바이스에 대한 Syslog 로깅 구성 1451

보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정 1452
로깅 활성화 및 기본 설정 1452
로깅 대상 활성화 1454
이메일 주소로 Syslog 메시지 전송 1455
사용자 지정 이벤트 목록 생성 1456
Syslog 메시지 생성 속도 제한 1457
Syslog 설정 1458
Syslog 서버 설정 1459
전역 시간 제한 구성 1461
Threat Defense를 위한 NTP 시간 동기화 구성 1463
정책 애플리케이션에 대한 디바이스 표준 시간대 구성 1464
Firepower Threat Defense 플랫폼 설정 기록 1465

장 55 보안 인증 컴플라이언스 1469
보안 인증 컴플라이언스 모드 1469
보안 인증서 컴플라이언스 특성 1470
보안 인증서 컴플라이언스 추천 1472
어플라이언스 강화 1474
네트워크 보호 1475
보안 인증서 컴플라이언스 활성화 1475

부 XIII: **NAT(**네트워크 주소 변환**)** 1479

장 56 **NAT** 정책 관리 1481
NAT 정책 요구 사항 및 사전 요건 1481
NAT 정책 관리 1482
NAT 정책 생성 1482
NAT 정책 설정 1483
NAT 정책 대상 설정 1485
NAT 정책 복사 1486

장 57

Firepower Threat Defense용 NAT(네트워크 주소 변환) 1487

NAT를 사용해야 하는 이유 1487

NAT 기본 사항 1488

NAT 용어 1488

NAT 유형 1489

라우팅된 모드 및 투명 모드의 NAT 1489

라우팅 모드의 NAT 1489

투명 모드 또는 브리지 그룹 내 NAT 1490

자동 NAT 및 수동 NAT 1491

자동 NAT 1492

수동 NAT 1492

자동 NAT와 수동 NAT 비교 1492

NAT 규칙 순서 1493

NAT 인터페이스 1495

NAT 라우팅 구성 1495

매핑된 인터페이스와 동일한 네트워크의 주소 1496

고유한 네트워크의 주소 1496

실제 주소와 동일한 주소(ID NAT) 1496

NAT용 지침 1497

NAT용 방화벽 모드 지침 1497

IPv6 NAT 지침 1497

IPv6 NAT 모범 사례 1498

검사된 프로토콜에 대한 NAT 지원 1498

NAT 추가 지침 1500

Threat Defense NAT 구성 1502

여러 디바이스에 대한 NAT 규칙 맞춤 설정 1504

NAT 규칙 테이블 검색 및 필터링 1506

동적 NAT 1507

동적 NAT 정보 1507

동적 NAT의 단점 및 장점 1508

동적 자동 NAT 구성 1509
동적 수동 NAT 구성 1510
동적 PAT 1513
동적 PAT 정보 1513
동적 PAT의 단점 및 장점 1514
PAT 풀 개체 지침 1514
동적 자동 PAT 구성 1515
동적 수동 PAT 구성 1517
포트 블록 할당으로 PAT 설정 1521
고정 NAT 1524
고정 NAT 정보 1524
고정 자동 NAT 구성 1528
고정 수동 NAT 구성 1530
ID NAT 1533
ID 자동 NAT 구성 1533
ID 수동 NAT 구성 1535
Firepower Threat Defense의 NAT 규칙 속성 1537
인터페이스 개체 NAT 속성 1538
자동 NAT에 대한 Translation 속성 1539
수동 NAT에 대한 Translation 속성 1540
PAT 풀 NAT 속성 1541
고급 NAT 속성 1542
IPv6 네트워크 변환 1544
NAT64/46: IPv6 주소를 IPv4로 변환 1544
NAT64/46 예: 내부 IPv6 네트워크 및 외부 IPv4 인터넷 1545
NAT64/46 예: 내부 IPv6 네트워크와 외부 IPv4 인터넷 및 DNS 변환 1547
NAT66: IPv6 주소를 다른 IPv6 주소로 변환 1551
NAT66 예, 네트워크 간의 고정 변환 1551
NAT66 예, 간단한 IPv6 인터페이스 PAT 1554
NAT 모니터링 1556
NAT의 예 1557

내부 웹 서버에 대한 액세스 제공(고정 자동 NAT) 1557
외부 웹 서버의 내부 호스트 및 고정 NAT에 대한 동적 자동 NAT 1560
여러 매핑된 주소가 있는 내부 로드 밸런서(고정 자동 NAT, 일대다) 1565
FTP, HTTP 및 SMTP용 단일 주소(포트 변환 고정 자동 NAT) 1568
대상에 따라 다른 변환(동적 수동 PAT) 1574
대상 주소 및 포트에 따라 다른 변환(동적 수동 PAT) 1579
NAT 및 사이트 대 사이트 VPN 1584
NAT를 사용하여 DNS 쿼리 및 응답 재작성 1590
DNS64 회신 수정 1591
DNS 회신 수정, 외부의 DNS 서버 1597
DNS 회신 수정, 호스트 네트워크의 DNS 서버 1601
FTD NAT 기록 1604

부 XIV: 액세스 제어 1607

장 58 액세스 제어의 이해 1609
액세스 제어 소개 1609
Access Control Policy Default Action(액세스 제어 정책 기본 작업) 1610
파일 및 침입 정책을 사용한 심층 검사 1612
침입 정책 및 파일 정책을 사용한 액세스 제어 트래픽 처리 1612
파일 및 침입 검사 순서 1614
액세스 제어 정책 상속 1615

장 59 액세스 제어의 모범 사례 1617
액세스 제어의 모범 사례 1617
액세스 제어 규칙 순서에 대한 모범 사례 1618
규칙 순서 지정 모범 사례 1618
규칙 선점 1619
규칙 작업 및 규칙 순서 1620
콘텐츠 제한 규칙 순서 1621
애플리케이션 규칙 순서 1621

SSL 규칙 순서 1621
URL 규칙 순서 1622
규칙 간소화 및 집중모범 사례 1622
최대 액세스 제어 규칙 및 침입 정책 개수 1623

장 60 액세스 제어 정책 1625
액세스 제어 정책 구성 요소 1626
액세스 제어 정책 요구 사항 및 사전 요건 1628
액세스 제어 정책 관리 1628
시스템 생성 액세스 제어 정책 1629
기본 액세스 제어 정책 만들기 1629
액세스 제어 정책 수정 1630
액세스 제어 정책 상속 관리 1632
기본 액세스 제어 정책 선택 1633
기본 정책에서 액세스 제어 정책 설정 상속 1633
하위 액세스 제어 정책의 설정 잠금 1634
도메인에 액세스 제어 정책 필요 1635
액세스 제어 정책에 대한 대상 디바이스 설정 1635
액세스 제어 정책용 로깅 설정 1636
액세스 제어 정책 고급 설정 1637
액세스 제어에 다른 정책 연결 1641
정책 적중 횟수 보기 1642
액세스 제어 정책 히스토리 1643

장 61 액세스 제어 규칙 1645
액세스 제어 규칙 소개 1645
액세스 제어 규칙 관리 1647
액세스 제어 규칙 구성 요소 1648
액세스 제어 규칙 순서 1649
액세스 제어 규칙 요구 사항 및 사전 요건 1650
액세스 제어 규칙 범주 추가 1651

액세스 제어 규칙 생성 및 수정 1651
액세스 제어 규칙 활성화 및 비활성화 1653
하나의 액세스 제어 정책에서 다른 정책으로 액세스 제어 규칙 복사 1654
사전 필터 정책으로 액세스 제어 규칙 이동 1654
액세스 제어 규칙 포지셔닝 1657
액세스 제어 규칙 작업 1658
액세스 제어 규칙 모니터 작업 1658
액세스 제어 규칙 신뢰 작업 1659
액세스 제어 규칙 차단 작업 1659
액세스 제어 규칙 인터랙티브 차단 작업 1659
액세스 제어 규칙 허용 작업 1660
액세스 제어 규칙 코멘트 1661
액세스 제어 규칙에 설명 추가 1662
액세스 컨트롤 규칙 기록 1662

장 62

URL 필터링 1665
URL 필터링 개요 1665
카테고리 및 평판을 사용한 URL 필터링 정보 1665
URL 카테고리 및 평판 설명 1666
Cisco Cloud의 URL 필터링 데이터 1667
URL 필터링 모범 사례 1667
HTTPS 트래픽 필터링 1670
URL 필터링의 라이선스 요건 1671
URL 필터링을 위한 요구 사항 및 사전 요건 1671
범주 및 평판을 사용한 URL 필터링 설정 방법 1672
범주 및 평판을 사용한 URL 필터링 활성화 1674
URL 필터링 옵션 1674
URL 조건 설정 1675
URL 조건이 포함된 규칙 1677
URL 규칙 순서 1677
DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타) 1678

도메인 조회 중 URL을 식별하도록 DNS 필터링 활성화(베타) 1678
DNS 필터링 제한 1679
DNS 필터링 및 이벤트 1679
수동 URL 필터링 1679
수동 URL 필터링 옵션 1680
범주 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의 1681
URL 필터링 상태 모니터 설정 1682
URL 범주 및 평판 1682
URL 범주 집합이 변경되면 작업 수행 1683
URL 카테고리 및 평판 변경: 이벤트에 미치는 영향 1685
URL 필터링 기록 1685

장 63

HTTP 응답 페이지 및 인터랙티브 차단 1689
HTTP 응답 페이지 정보 1689
HTTP 대응 페이지의 제한 1689
HTTP 응답 페이지 요구 사항 및 사전 요건 1690
HTTP 응답 페이지 선택 1691
HTTP 응답 페이지를 사용한 인터랙티브 차단 1691
인터랙티브 차단 설정 1692
차단된 웹사이트의 사용자 우회 시간 제한 설정 1693

장 64

보안 인텔리전스 차단 목록 1695
보안 인텔리전스 정보 1695
보안 인텔리전스 모범 사례 1696
보안 인텔리전스를 위한 라이선스 요건 1697
보안 인텔리전스 요구 사항 및 사전 요건 1697
보안 인텔리전스 소스 1697
보안 인텔리전스 설정 1698
보안 인텔리전스 옵션 1700
보안 인텔리전스 카테고리 1702
차단 목록 아이콘 1704

설정 예 : 보안 인텔리전스 차단 1704
보안 인텔리전스 모니터링 1706
보안 인텔리전스 차단 재정의 1706
보안 인텔리전스 문제 해결 1707
사용 가능한 옵션 목록에 보안 인텔리전스 범주가 없음 1707
메모리 사용 문제 해결 1707
보안 인텔리전스 차단 목록 히스토리 1708

장 65

DNS 정책 1709
DNS 정책 개요 1709
DLP 정책 구성 요소 1710
DNS 정책을 위한 라이선스 요구 사항 1711
DNS 프로파일 요구 사항 및 사전 요건 1711
DNS 정책 관리 1711
기본 DNS 정책 생성 1712
DNS 정책 편집 1713
DNS 규칙 1713
DNS 규칙 생성 및 편집 1714
DNS 규칙 관리 1715
DNS 규칙 활성화 및 비활성화 1715
DNS 규칙 순서 평가 1715
DNS 규칙 작업 1716
DNS 규칙 조건 1718
DNS 및 보안 영역을 기준으로 트래픽 제어 1718
DNS 및 네트워크를 기준으로 트래픽 제어 1719
DNS 및 VLAN을 기준으로 트래픽 제어 1719
DNS 목록, 피드 또는 카테고리를 기준으로 트래픽 제어 1720
DNS 정책 구축 1721

장 66

사전 필터링 및 사전 필터 정책 1723
사전 필터링 정보 1723

사전 필터링 및 액세스 제어 비교 1723
통과 터널 및 액세스 제어 1726
사전 필터링 모범 사례 1727
사전 필터 정책 요구 사항 및 사전 요건 1727
사전 필터링 설정 1728
사전 필터 정책 정보 1729
터널 규칙과 사전 필터 규칙 비교 1730
터널 및 사전 필터 규칙 구성 요소 1731
터널 영역 및 사전 필터링 1733
터널 영역 사용 1734
Creating Tunnel Zones 1736
사전 필터 규칙을 액세스 제어 정책으로 이동 1737
사전 필터 정책 적중 횟수 1739
대규모 플로우 오프로드 1739
플로우 오프로드 제한 1741
사전 필터링 기록 1742

장 67 **IAB(Intelligent Application Bypass)** 1745
IAB 소개 1745
IAB 옵션 1746
인텔리전트 애플리케이션 우회에 대한 요구 사항 및 사전 조건 1748
Intelligent Application Bypass 구성 1748
IAB 로깅 및 분석 1750

장 68 콘텐츠 제한을 사용하는 액세스 제어 1755
콘텐츠 제한 정보 1755
콘텐츠 제한 요구 사항 및 사전 요건 1757
액세스 제어 규칙을 사용하여 콘텐츠 제한 시행 1757
액세스 제어 규칙에 대한 안전 검색 옵션 1759
액세스 제어 규칙에 대한 YouTube EDU 옵션 1759
DNS 싱크홀을 사용하여 콘텐츠 제한 적용 1759

부 XV: 암호화된 트래픽 처리 1763

장 69 트래픽 해독 이해 1765

트래픽 암호 해독 설명 1765

TLS 암호화 가속 1767

TLS 암호화 가속 지침 및 제한 사항 1768

TLS 암호화 가속 상태 보기 1769

TLS/SSL 모범 사례 1770

암호 해독 사례 1770

트래픽을 암호 해독해야 하는 경우와 하면 안 되는 경우 1771

암호 해독 및 파기(발신 트래픽) 1772

알려진 키 암호 해독(수신 트래픽) 1773

기타 TLS/SSL 규칙 작업 1773

TLS 1.3 서버 ID 검색 1773

TLS/SSL 규칙 예시 1774

비보안 프로토콜 차단 1774

TLS/SSL 규칙 구성 요소 1776

TLS/SSL 규칙 순서 평가 1777

다중 규칙 예시 1778

TLS/SSL 정책 및 규칙을 구성하는 방법 1780

TLS/SSL 검사 어플라이언스 구축 시나리오 1782

인라인 구축의 트래픽 암호 해독 1782

인라인 구축의 암호화된 트래픽 모니터링 1784

인라인 구축의 암호화된 트래픽 암호 해독 1784

인라인 구축의 암호화된 트래픽 차단 1785

인라인 구축에서 개인 키로 암호화된 트래픽 검사 1786

인라인 구축에서 다시 서명된 인증서로 암호화된 트래픽 검사 1788

TLS/SSL 기록 1790

장 70 SSL 정책 생성 시작 1793

SSL 정책 개요 1793
SSL 정책 기본 작업 1794
암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션 1795
SSL 정책 요구 사항 및 사전 요건 1797
SSL 정책 관리 1797
기본 SSL 정책 생성 1798
해독 불가 트래픽에 대한 기본 처리 설정 1799
SSL 정책 수정 1800

장 71

TLS/SSL 규칙 시작하기 1803
TLS/SSL 규칙 개요 1803
TLS/SSL 규칙 지침 및 제한 사항 1804
TLS/SSL 암호 해독 사용 지침 1804
TLS/SSL 규칙을 지원하지 않는 기능 1804
TLS/SSL 암호 해독 금지 지침 1805
TLS/SSL 암호 해독 - 파기 지침 1806
TLS/SSL 암호 해독 - 알려진 키 지침 1807
TLS/SSL 차단 지침 1808
TLS/SSL 인증서 고정 지침 1808
TLS/SSL 하트비트 지침 1809
TLS/SSL 익명 암호 그룹 제한 1809
TLS/SSL 노멀라이저 지침 1809
기타 TLS/SSL 규칙 지침 1809
TLS/SSL 규칙 요구 사항 및 사정 요건 1810
TLS/SSL 규칙 생성 및 수정 1810
규칙 카테고리에 TLS/SSL 규칙 추가 1812
번호로 TLS/SSL 규칙 포지셔닝 1812
TLS/SSL 규칙 트래픽 처리 1813
암호화된 트래픽 검사 설정 1814
TLS/SSL 규칙 순서 평가 1815
TLS/SSL 규칙 조건 1816

TLS/SSL 규칙 조건 유형 1817
TLS/SSL 규칙 작업 1819
TLS/SSL 규칙 모니터링 작업 1819
TLS/SSL 규칙 Do Not Decrypt(암호 해독 안 함) 작업 1819
TLS/SSL 규칙 차단 작업 1819
TLS/SSL 규칙 암호 해독 작업 1820
TLS/SSL 규칙 동작 구성 1820
암호 해독 설정 - 재서명 작업 1821
암호 해독 설정 - 알려진 키 작업 1822
TLS/SSL 관리 규칙 1822
TLS/SSL 규칙 검색 1822
TLS/SSL 규칙 검색 1823
TLS/SSL 규칙 활성화 및 비활성화 1823
TLS/SSL 규칙 이동 1824
새새 TLS/SSL 규칙 카테고리 추가 1824

장 72

TLS/SSL 규칙을 사용한 암호 해독 조정 1827
TLS/SSL 규칙 조건 개요 1827
암호 해독 조정 요구 사항 및 사전 요건 1828
서버 인증서 기반 TLS/SSL 규칙 조건 1828
인증서 고유 이름 TLS/SSL 규칙 조건 1829
암호화된 트래픽을 인증서 고유 이름(DN)으로 제어 1830
인증서 TLS/SSL 규칙 조건 1832
암호화된 트래픽을 인증서로 제어 1832
인증서 상태 TLS/SSL 규칙 조건 1833
외부 인증 증명 신뢰 1837
인증서 상태를 기준으로 트래픽 매칭 1839
암호 그룹 TLS/SSL 규칙 조건 1841
암호화된 트래픽을 암호 그룹으로 제어 1844
암호화 프로토콜 버전 TLS/SSL 규칙 조건 1844
트래픽을 암호화 프로토콜 버전으로 제어 1845

장 73 SSL 하드웨어 엑셀러레이션(Hardware Acceleration) 모니터링 1847
정보 카운터 1847
알림 카운터 1848
오류 카운터 1848
치명적 카운터 1849

장 74 TLS/SSL 규칙 문제 해결 1851
TLS/SSL 피닝 정보 1851
TLS/SSL 피닝 문제 해결 1851
알 수 없는 또는 잘못된 인증서 또는 인증 기관 문제 해결 1854
TLS/SSL 암호 그룹 확인 1856

부 XVI: AMP(Advanced Malware Protection) 및 파일 제어 1859

장 75 파일 정책 및 악성코드 보호 1861
파일 정책 및 Advanced Malware Protection 정보 1861
파일 정책 1862
파일 정책 요구 사항 및 사전 요건 1862
파일 및 악성코드 정책을 위한 라이선스 요구 사항 1863
파일 정책 및 악성코드 탐지 모범 사례 1863
파일 규칙 모범 사례 1863
파일 탐지 모범 사례 1864
파일 차단 모범 사례 1864
파일 정책 모범 사례 1865
악성코드 차단 설정 방법 1866
악성 코드 차단 계획 및 준비 1867
파일 정책 구성 1868
액세스 제어 구성에 파일 정책 추가 1869
악성코드 보호를 수행하는 액세스 제어 규칙 구성 1869
악성코드 차단 유지 보수 및 모니터링 설정 1870

악성코드 차단을 위한 클라우드 연결 1871
AMP 클라우드 연결 구성 1872
AMP 클라우드 연결 요구 사항 및 모범 사례 1873
AMP 클라우드 선택 1873
Cisco AMP Private Cloud 1874
(퍼블릭 또는 프라이빗) AMP 클라우드와의 연결 관리 1875
AMP 옵션 변경 1876
동적 분석 연결 1877
동적 분석 요구 사항 1877
기본 동적 분석 연결 보기 1877
동적 분석 온프레미스 어플라이언스(Cisco Threat Grid) 1877
시스템 유지 관리: 동적 분석 대상인 파일 유형 업데이트 1879
파일 정책 및 파일 규칙 1880
파일 정책을 생성하거나 수정합니다. 1880
고급 및 아카이브 파일 검사 옵션 1880
파일 정책 관리 1884
파일 규칙 1885
파일 규칙 구성 요소 1885
파일 규칙 작업 1886
파일 규칙 생성 1894
악성 코드 차단을 위한 액세스 제어 규칙 로깅 1896
회귀적 속성 변경 1896
(선택 사항) AMP for Endpoints를 사용한 악성코드 방지 1896
악성코드 방지 비교: Firepower 대 AMP for Endpoints 1897
Firepower와 AMP for Endpoints 통합 정보 1898
Firepower와 AMP for Endpoints 통합의 이점 1898
AMP for Endpoints 및 AMP Private Cloud 1898
Firepower와 AMP for Endpoints 통합 1898
파일 정책 및 악성코드 보호 히스토리 1901

장 76 파일 및 악성코드 탐지 성능 및 저장 조정 1903

파일 및 악성코드 탐지 성능 및 저장 옵션 1903
파일 및 악성코드 탐지 성능 및 저장 조정 1905

부 XVII: TID 인텔리전스 및 위협 분석 1907

장 77 Cisco Threat Intelligence Director(TID) 1909
Cisco Threat Intelligence Director(TID) 개요 1909
TID 및 보안 인텔리전스 1911
Threat Intelligence Director의 성능 영향 1911
Cisco Threat Intelligence Director(TID) 및 고가용성 구성 1912
TID(Threat Intelligence Director) 요구 사항 및 사전 요건 1912
플랫폼, 요소 및 라이선스 요구 사항 1912
소스 요구 사항 1913
설정 방법 Cisco Threat Intelligence Director(TID) 1914
지원할 정책 구성 TID 1915
데이터 소스 수집 옵션 1916
소스로 사용할 TAXII 피드 가져오기 1917
URL에서 소스 가져오기 1918
소스로 사용할 로컬 파일 업로드 1920
중복 표시기 처리 1921
TID 소스의 TLS/SSL 설정 구성 1921
TID 액세스 권한이 있는 사용자 역할 1923
TID 데이터 백업 및 복구 정보 1923
TID 인시던트 및 관찰 데이터 분석 1924
관찰 및 사고 생성 1924
사고 보기 및 관리 1925
사고 요약 정보 1926
사고 세부 사항 1927
TID 관찰에 대한 이벤트 보기 1931
Firepower Management Center 이벤트의 TID 관찰 1931
수행하는 작업에 영향을 미치는 요소 1932

TID-Firepower Management Center 작업 우선 순위 1933
Cisco Threat Intelligence Director(TID) 구성 보기 및 변경 1936
요소(매니지드 디바이스)의 TID 상태 보기 1937
소스 보기 및 관리 1937
소스 요약 정보 1938
소스 상태 세부 사항 1939
지표 보기 및 관리 1940
지표 요약 정보 1941
지표 세부사항 1942
관찰 가능 개체 보기 및 관리 1943
관찰 가능 개체 요약 정보 1944
테이블 보기에서 TID 데이터 필터링 1945
TID 구성의 상속 1945
여러 상위에서 TID 설정 상속 1946
상속된 TID 설정 재정의 정보 1946
소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정 1947
게시 일시 중지 정보 1948
TID 일시 중지 및 요소에서 TID 데이터 제거 1949
소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시 1949
관찰 가능 개체 게시 빈도 수정 1950
차단 금지 목록에 TID 관찰 가능 항목 추가 1951
차단 금지 목록에 TID 관찰 가능 항목 추가 1951
STIX 소스 파일 보기 1952
문제 해결 Cisco Threat Intelligence Director(TID) 1952
기록Cisco Threat Intelligence Director(TID) 1955

부 XVIII: 침입 탐지 및 방지 1959

장 78 침입 탐지 및 방지 개요 1961
네트워크 분석 및 침입 정책 기본 사항 1961
정책이 트래픽에서 침입을 검토하는 방법 1962

복호화, 정규화 및 전처리: 네트워크 분석 정책 1963
액세스 제어 규칙: 침입 정책 선택 1964
침입 검사: 침입 정책, 규칙 및 변수 집합 1965
침입 이벤트 생성 1966
시스템 제공 및 맞춤형 네트워크 분석 및 침입 정책 1967
시스템 제공 네트워크 분석 및 침입 정책 1968
맞춤형 네트워크 분석 및 침입 정책의 이점 1969
맞춤형 네트워크 분석 정책의 이점 1970
사용자 지정 침입 정책의 이점 1970
사용자 지정 정책의 한계 1971
네트워크 분석 및 침입 정책에 대한 라이선스 요건 1974
네트워크 분석 및 침입 정책 요구 사항 및 사전 요건 1974
탐색 패널: 네트워크 분석 및 침입 정책 1974
충돌 및 변경: 네트워크 분석 및 침입 정책 1976
네트워크 분석 또는 침입 정책 종료 1977

장 79

침입 및 네트워크 분석 정책의 레이어 1979
레이어 기본 사항 1979
네트워크 분석 및 침입 정책 레이어를 위한 라이선스 요건 1979
네트워크 분석 및 침입 정책 레이어에 대한 요구 사항 및 사전 요건 1980
레이어 스택 1980
기본 레이어 1981
시스템 제공 기반 정책 1981
맞춤형 기본 정책 1982
규칙 업데이트가 기본 정책에 미치는 영향 1982
기반 정책 변경 1983
Firepower Recommendations 레이어 1984
레이어 관리 1985
공유 레이어 1986
레이어 관리 1987
레이어 탐색 1988

레이어 내 침입 규칙 1988
레이어에서 침입 규칙 구성 1990
다중 레이어에서 규칙 설정 제거 1991
사용자 지정 기본 정책에서 규칙 변경 허용하기 1992
레이어의 사전 처리기 및 고급 설정 1993
레이어 내 전처리기 및 고급 설정 구성 1994

장 80 침입 정책 시작하기 1995
침입 정책 기본 사항 1995
침입 정책을 위한 라이선스 요건 1997
침입 정책 요구 사항 및 사전 요건 1997
침입 정책 관리 1997
맞춤형 침입 정책 생성 1998
맞춤형 침입 정책 생성 1999
Snort 2 침입 정책 편집 1999
침입 정책 변경 2000
침입 방지를 수행하는 액세스 제어 규칙 설정 2001
액세스 제어 규칙 설정 및 침입 정책 2001
침입 방지 수행을 위한 액세스 제어 규칙 구성 2002
인라인 구축의 삭제 작업 2002
인라인 배포에서 삭제 작업 설정하기 2003
이중 시스템 구축의 삭제 작업 2003
침입 정책 고급 설정 2004
침입 탐지 및 방지에 대한 성능 최적화 2005

장 81 규칙을 사용하여 침입 정책 조정 2007
침입 규칙 조정 기본 사항 2007
침입 규칙 유형 2008
침입 규칙 라이선스 요구 사항 2009
침입 규칙 요구 사항 및 사전 요건 2009
침입 정책의 침입 규칙 보기 2009

침입 규칙 페이지 열 2010
침입 규칙 세부 사항 2011
침입 규칙 세부 사항 보기 2011
침입 규칙에 대한 임계값 설정 2012
침입 규칙에 대한 삭제 설정 2013
규칙 세부 사항 페이지에서 동적 규칙 상태 설정 2013
침입 규칙에 대한 SNMP 알림 설정 2014
침입 규칙에 설명 추가 2015
침입 정책의 침입 규칙 필터 2015
침입 규칙 필터 참고 사항 2015
침입 정책 규칙 필터 구성 가이드라인 2016
침입 규칙 설정 필터 2019
침입 규칙 콘텐츠 필터 2019
침입 규칙 카테고리 2021
침입 규칙 필터 구성 요소 2021
침입 규칙 필터 사용 2022
침입 정책에서 규칙 필터 설정 2022
침입 규칙 상태 2023
침입 규칙 상태 옵션 2024
침입 규칙 상태 설정 2024
침입 정책의 침입 이벤트 알림 필터 2025
침입 이벤트 임계값 2025
침입 이벤트 임계값 설정 2025
침입 이벤트 임계값 추가 및 수정 2027
침입 이벤트 임계값 보기 및 삭제 2029
침입 정책 삭제 설정 2029
침입 정책 삭제 유형 2030
침입 규칙에 대한 침입 이벤트 삭제 2030
삭제 조건 보기 및 삭제 2031
동적 침입 규칙 상태 2032
동적 침입 규칙 상태 설정 2033

규칙 페이지에서 동적 규칙 상태 설정 2034
침입 규칙 설명 추가 2035

장 82 네트워크 자산에 대한 침입 방지 맞춤화 2037
Firepower 권장 규칙 정보 2037
Firepower 추천 기본 설정 2038
Firepower 추천 고급 설정 2039
Firepower 추천 생성 및 적용 2040

장 83 민감한 데이터 탐지 2043
민감한 데이터 탐지 기본 사항 2043
전역 민감한 데이터 탐지 옵션 2044
개별 민감한 데이터 유형 옵션 2045
시스템 제공 민감한 데이터 유형 2046
민감한 데이터 탐지 라이선스 요건 2047
민감한 데이터 탐지 요구 사항 및 사전 요건 2048
민감한 데이터 탐지 구성 2048
모니터링된 애플리케이션 프로토콜 및 민감한 데이터 2050
모니터링할 애플리케이션 프로토콜 선택 2050
특별 케이스: FTP 트래픽에서 민감한 데이터 탐지 2051
맞춤형 민감한 데이터 유형 2052
맞춤형 민감한 데이터 유형의 데이터 패턴 2052
맞춤형 민감한 데이터 유형 설정 2054
맞춤형 민감한 데이터 유형 수정 2056

장 84 침입 이벤트 로깅 글로벌 제한 2057
전역 규칙 임계값 기본 사항 2057
전역 규칙 임계값 옵션 2058
전역 임계값에 대한 라이선스 요건 2060
전역 임계값 요구 사항 및 사전 요건 2060
전역 임계값 구성 2061

전역 임계값 비활성화 2062

장 85

침입 규칙 편집기 2063
침입 규칙 수정 소개 2063
침입 규칙 편집기 라이선스 요구 사항 2064
침입 규칙 편집기 요구 사항 및 사전 요건 2064
규칙 구조 2065
침입 규칙 헤더 2065
침입 규칙 헤더 작업 2066
침입 규칙 헤더 프로토콜 2067
침입 규칙 헤더 방향 2068
침입 규칙 헤더 소스 및 대상 IP 주소 2068
침입 규칙 헤더 소스 및 대상 포트 2071
침입 이벤트 세부 정보 2072
맞춤형 분류 추가 2076
이벤트 우선 순위 정의 2076
이벤트 참조 정의 2077
맞춤형 규칙 생성 2077
새 규칙 작성 2078
기존 규칙 수정 2079
규칙 문서 보기 2080
침입 규칙에 코멘트 추가 2081
사용자 지정 규칙 삭제 2082
규칙 검색 2083
침입 규칙에 대한 검색 기준 2084
침입 규칙 편집기 페이지에서 규칙 필터링 2085
필터링 가이드라인 2085
키워드 필터링 2085
문자열 필터링 2087
키워드 및 문자열 조합 필터링 2087
규칙 필터링 2087

침입 규칙의 키워드 및 인수 2088
content 및 protected_content 키워드 2088
기본 content 또는 protected_content 키워드 인수 2090
content 또는 protected_content 키워드 검색 위치 2091
개요: HTTP content 및 protected_content 키워드 인수 2094
개요: content 키워드 빠른 패턴 매처 2098
replace 키워드 2101
byte_jump 키워드 2102
byte_test 키워드 2104
byte_extract 키워드 2106
개요: pcre 키워드 2109
pcre 구문 2110
pcre 수식자 옵션 2112
pcre 예시 키워드 값 2115
metadata 키워드 2117
서비스 메타데이터 2119
메타데이터 검색 가이드라인 2124
IP 헤더 값 2125
ICMP 헤더 값 2128
TCP 헤더 값 및 스트림 크기 2129
stream_reassembly 키워드 2133
SSL 키워드 2133
appid 키워드 2135
애플리케이션 레이어 프로토콜 값 2136
RPC 키워드 2136
ASN.1 키워드 2137
urilen 키워드 2138
DCE/RPC 키워드 2139
SIP 키워드 2142
GTP 키워드 2144
SCADA 키워드 2157

Modbus 키워드 2157
DNP3 키워드 2158
CIP 및 ENIP 키워드 2161
S7Commplus 키워드 2161
패킷 특성 2163
활성 응답 키워드 2165
resp 키워드 2166
react 키워드 2167
detection_filter 키워드 2167
tag 키워드 2169
flowbits 키워드 2170
flowbits 키워드 옵션 2170
flowbits 키워드 사용 가이드라인 2172
flowbits 키워드 예시 2172
http_encode 키워드 2177
http_encode 키워드 구문 2178
http_encode 키워드 예시: 2개의 http_endcode 키워드를 사용하여 2개의 인코딩 검색 2178
개요: file_type 및 file_group 키워드 2178
file_type 및 file_group 키워드 2179
file_data 키워드 2180
pkt_data 키워드 2181
base64_decode 및 base64_data 키워드 2181

장 86

침입 방지 성능 조정 2185
침입 방지 성능 조정 정보 2185
침입 방지 성능 조정 라이선스 요건 2186
침입 방지 성능 조정 요구 사항 및 사전 요건 2186
침입에 대한 패턴 일치 제한 2186
침입 규칙용 정규식 제한 재정의 2187
침입 규칙용 정규식 제한 재정의 2188
패킷 침입당 이벤트 생성 제한 2189

패킷당 생성되는 침입 이벤트 제한 2189
패킷 및 침입 규칙 레이턴시 임계값 구성 2190
패킷 레이턴시 임계값 2190
패킷 레이턴시 임계값 참고 사항 2192
패킷 레이턴시 임계값 활성화 2192
패킷 레이턴시 임계값 구성 2192
Rule Latency Thresholding 2193
규칙 레이턴시 임계값 참고 2195
규칙 레이턴시 임계값 구성 2195
침입 성능 통계 로깅 구성 2196
침입 성능 통계 로깅 구성 2197

부 XIX: 고급 네트워크 분석 및 전처리 2199

장 87 네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정 2201
네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정 정보 2201
네트워크 분석 및 침입 정책에 대한 고급 액세스 제어 설정 요구 사항 및 사전 요건 2201
트래픽이 식별되기 전에 통과하는 패킷 검사 2202
트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례 2202
트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정 2203
네트워크 분석 정책 고급 설정 2203
기본 네트워크 분석 정책 설정 2204
네트워크 분석 규칙 2205
네트워크 분석 규칙 설정 2206
네트워크 분석 규칙 관리 2206

장 88 네트워크 분석 정책 시작하기 2209
네트워크 분석 정책 기본 사항 2209
네트워크 분석 정책에 대한 라이선스 요건 2210
네트워크 분석 정책 요구 사항 및 사전 요건 2210
네트워크 분석 정책 관리 2210

Snort 3에 대한 맞춤형 네트워크 분석 정책 생성 2211
네트워크 분석 정책 매핑 2215
네트워크 분석 정책 매핑 보기 2215
네트워크 분석 정책 생성 2215
네트워크 분석 정책 수정 2216
네트워크 분석 정책 사용자 정의 2216
Snort 2에 대한 맞춤형 네트워크 분석 정책 생성 2220
사용자 지정 네트워크 분석 정책 만들기 2220
네트워크 분석 정책 관리 2221
네트워크 분석 정책 설정 및 캐시된 변경 사항 2221
네트워크 분석 정책 수정 2222
네트워크 분석 정책의 전처리기 설정 2223
인라인 구축의 전처리기 트래픽 수정 2224
네트워크 분석 정책 참고 사항의 전처리기 설정 2225

장 89

애플리케이션 레이어 프리프로세서 2227
애플리케이션 계층 전처리기 소개 2227
애플리케이션 계층 전처리기 라이선스 요구 사항 2228
애플리케이션 계층 전처리기 요구 사항 및 사전 요건 2228
DCE/RPC 전처리기 2228
연결 없는 DCE/RPC 트래픽 및 연결 지향 DCE/RPC 트래픽 2229
DCE/RPC 대상 기반 정책 2230
RPC over HTTP 전송 2231
DCE/RPC 전역 옵션 2231
DCE/RPC 대상 기반 정책 옵션 2233
트래픽 관련 DCE/RPC 규칙 2238
DCE/RPC 전처리기 구성 2238
DNS 전처리기 2240
DNS 전처리기 옵션 2241
DNS 전처리기 구성 2243
FTP/텔넷 디코더 2244

전역 FTP 및 텔넷 옵션 2244
텔넷 옵션 2244
서버 레벨 FTP 옵션 2245
FTP 명령 검증 성명 2248
클라이언트 레벨 FTP 옵션 2249
FTP/텔넷 디코더 설정 2250
HTTP 검사 전처리기 2252
전역 HTTP 정상화 옵션 2253
서버 레벨 HTTP 정상화 옵션 2254
서버 레벨 HTTP 정상화 인코딩 옵션 2263
HTTP 검사 전처리기 설정 2266
추가 HTTP 검사 전처리기 규칙 2268
Sun RPC 전처리기 2269
Sun RPC 전처리기 옵션 2269
Sun RPC 전처리기 구성 2270
SIP 전처리기 2270
SIP 전처리기 옵션 2271
SIP 전처리기 구성 2274
추가 SIP 전처리기 규칙 2274
GTP 전처리기 2276
GTP 전처리기 규칙 2276
GTP 전처리기 설정 2276
IMAP 전처리기 2277
IMAP 전처리기 옵션 2278
IMAP 전처리기 구성 2279
추가 IMAP 전처리기 규칙 2280
POP 전처리기 2280
POP 전처리기 옵션 2281
POP 전처리기 구성 2282
추가 POP 전처리기 규칙 2283
SMTP 전처리기 2283

SMTP 전처리기 옵션 2284
SMTP 복호화 구성 2288
SSH 전처리기 2289
SSH 전처리기 옵션 2290
SSH 전처리기 구성 2293
SSL 전처리기 2294
SSL 전처리 작동 방식 2294
SSL 전처리기 옵션 2295
SSL 전처리기 구성 2297
SSL 전처리기 규칙 2298

장 90

SCADA 프리프로세서 2299
SCADA 전처리기 소개 2299
SCADA 전처리기 라이선스 요구 사항 2299
SCADA 전처리기 요구 사항 및 사전 요건 2300
Modbus 전처리기 2300
Modbus 전처리기 포트 옵션 2300
Modbus 전처리기 구성 2300
Modbus 전처리기 규칙 2302
DNP3 전처리기 2302
DNP3 전처리기 옵션 2302
DNP3 전처리기 구성 2303
DNP3 전처리기 규칙 2304
CIP 전처리기 2305
CIP 전처리기 옵션 2305
CIP 이벤트 2306
CIP 전처리기 규칙 2306
CIP 전처리기 설정 지침 2307
CIP 전처리기 설정 2308
S7Commplus 전처리기 2309
S7Commplus 전처리기 구성 2309

장 91

전송 및 네트워크 계층 전처리기 2311

전송 및 네트워크 계층 전처리기 소개 2311

전송 및 네트워크 레이어 전처리기에 대한 라이선스 요구 사항 2312

전송 및 네트워크 계층 전처리기 요구 사항 및 사전 요건 2312

고급 전송/네트워크 전처리기 설정 2312

무시된 VLAN 헤더 2312

침입 삭제 규칙에서의 활성 응답 2313

고급 전송/네트워크 전처리기 옵션 2314

고급 전송/네트워크 전처리기 설정 2315

체크섬 확인 2315

체크섬 확인 옵션 2316

체크섬 확인 2316

인라인 정상화 전처리기 2317

인라인 표준화 옵션 2318

인라인 표준화 설정 2323

IP 조각 모음 전처리기 2324

IP 단편화 익스플로잇 2324

대상 기반 조각 모음 정책 2325

IP 조각 모음 옵션 2325

IP 조각 모음 구성 2328

패킷 디코더 2330

패킷 디코더 옵션 2330

패킷 복호화 구성 2333

TCP 스트림 전처리 2334

상태 관련 TCP 익스플로잇 2334

대상 기반 TCP 정책 2335

TCP 스트림 리어셈블리 2335

TCP 스트림 전처리 옵션 2337

TCP 스트림 전처리 구성 2344

UDP 스트림 전처리 2346

UDP 스트림 전처리 옵션 2346
UDP 스트림 전처리 구성 2347

장 92 특정 위협 탐지 2349
특정 위협 탐지 소개 2349
특정 위협 탐지 라이선스 요건 2349
특정 위협 탐지 요구 사항 및 사전 요건 2350
Back Orifice 탐지 2350
Back Orifice 탐지 전처리기 2350
Back Orifice 탐지 2351
포트스캔 탐지 2351
포트스캔 유형, 프로토콜 및 필터링된 민감도 레벨 2352
포트스캔 이벤트 생성 2354
포트스캔 이벤트 패킷 보기 2356
포트스캔 탐지 구성 2357
속도 기반 공격 방지 2359
속도 기반 공격 방지 예시 2361
detection_filter 키워드 예시 2361
동적 규칙 상태 임계값 설정 및 삭제 예시 2362
전정책적 속도 기반 탐지 및 임계값 설정 또는 삭제 예시 2363
여러 필터링 방법으로 속도 기반 탐지 예시 2364
속도 기반 공격 방지 옵션 및 설정 2365
속도 기반 공격 방지, 탐지 필터링 및 임계값 설정 또는 삭제 2367
속도 기반 공격 방지 구성 2367

장 93 적응형 프로파일 2371
적응형 프로파일 정보 2371
적응형 프로파일 라이선스요구 사항 2372
적응형 프로파일 요구 사항 및 사전 요건 2372
적응형 프로파일 및 Firepower 권장 규칙 2372
적응형 프로파일 옵션 2373

적응형 프로파일 구성 2374

부 XX: 검색 및 ID 2375

장 94 네트워크 검색 및 ID 소개 2377

호스트, 애플리케이션 및 사용자 검색 및 ID 데이터에 사용 2377

호스트 및 애플리케이션 탐지 기초 2378

운영 체제 및 호스트 데이터의 수동 탐지 2378

운영 체제 및 호스트 데이터의 활성 탐지 2378

애플리케이션 및 운영 체제에 대한 현재 ID 2379

현재 사용자 ID 2380

애플리케이션 및 운영 체제 ID 충돌 2380

Firepower System의 Netflow 데이터 2381

NetFlow 데이터를 사용하기 위한 요건 2382

NetFlow와 매니지드 디바이스 데이터의 차이점 2382

사용자 ID 정보 2385

ID 용어 2385

사용자 ID 모범 사례 2386

ID 구축 2388

사용자 활동 데이터베이스 2389

사용자 데이터베이스 2390

Firepower System 호스트 및 사용자 제한 2391

Firepower System 호스트 제한 2391

Firepower System 사용자 한도 2392

장 95 호스트 ID 소스 2395

개요: 호스트 데이터 수집 2395

호스트 ID 소스 요구 사항 및 사전 요건 2396

시스템에서 탐지할 수 있는 호스트 운영체제 결정 2396

호스트 운영체제 식별 2397

맞춤형 핑거프린팅 2397

핑거프린트 관리 2398
핑거프린트 활성화 및 비활성화 2399
활성 핑거프린트 편집 2399
비활성 핑거프린트 편집 2400
클라이언트에 대한 맞춤형 핑거프린트 생성 2401
서버에 대한 맞춤형 핑거프린트 생성 2403
호스트 입력 데이터 2406
서드파티 데이터 사용 요구 사항 2406
서드파티 제품 매핑 2407
서드파티 제품 매핑 2407
서드파티 제품 수정 매핑 2409
서드파티 취약성 매핑 2410
맞춤형 제품 매핑 2411
맞춤형 제품 매핑 생성 2411
맞춤형 제품 매핑 목록 편집 2412
맞춤형 제품 매핑 활성화 및 비활성화 2413
호스트 입력 클라이언트 설정 2413
Nmap 스캐닝 2414
Nmap 교정 옵션 2415
Nmap 스캔 지침 2422
예: Nmap을 사용하여 알 수 없는 운영 체제 확인 2424
예: Nmap을 사용하여 새 호스트에 응답 2425
Nmap 스캔 관리 2426
Nmap 스캔 인스턴스 추가 2427
Nmap 스캔 인스턴스 편집 2428
Nmap 스캔 대상 추가 2429
Nmap 스캔 대상 편집 2430
Nmap 교정 생성 2430
Nmap 교정 편집 2433
온디맨드 Nmap 스캔 실행 2433
Nmap 스캔 결과 2434

Nmap 스캔 결과 보기 2435
Nmap 스캔 결과 필드 2436
Nmap 스캔 결과 가져오기 2437
호스트 ID 소스 기록 2437

장 96 애플리케이션 탐지 2439
개요: 애플리케이션 탐지 2439
애플리케이션 탐지기 기초 2440
웹 인터페이스에서 애플리케이션 프로토콜 식별 2441
클라이언트 탐지의 암시적 애플리케이션 프로토콜 탐지 2443
호스트 제한 및 검색 이벤트 로깅 2443
애플리케이션 탐지 특별 고려 사항 2443
애플리케이션 탐지 요구 사항 및 사전 요건 2445
맞춤형 애플리케이션 탐지기 2445
맞춤형 애플리케이션 탐지기 및 사용자 정의 애플리케이션 필드 2445
맞춤형 애플리케이션 탐지기 설정 2449
사용자 정의 애플리케이션 생성 2450
기본 탐지기에서 탐지 패턴 지정 2451
고급 탐지기에서 탐지 기준 지정 2452
맞춤형 애플리케이션 프로토콜 탐지기 테스트 2453
탐지기 상세정보 보기 또는 다운로드 2454
탐지기 목록 정렬 2454
탐지기 목록 필터링 2455
탐지기 목록에 대한 필터 그룹 2455
다른 탐지기 페이지로 이동 2456
탐지기 활성화 및 비활성화 2456
맞춤형 애플리케이션 탐지기 편집 2457
탐지기 삭제 2458

장 97 영역 생성 및 관리 2461
영역 및 영역 시퀀스 정보 2461

영역 및 신뢰할 수 있는 도메인 2463
영역에 지원되는 서버 2463
지원되는 서버 개체 클래스 및 속성 이름 2464
영역 라이선스 요건 2465
영역 요구 사항 및 사전 요건 2466
영역 생성 2466
영역 필드 2467
영역 디렉토리 및 다운로드 동기화 2470
Active Directory에 안전하게 연결 2472
Active Directory 서버 이름 찾기 2472
Active Directory 서버의 루트 인증서 내보내기 2473
영역 디렉터리 설정 2475
사용자 및 그룹 다운로드 2476
영역 시퀀스 생성 2477
영역 관리 2479
영역 비교 2479
영역 및 사용자 다운로드 문제 해결 2480
영역 또는 사용자 불일치 탐지 2483
영역 히스토리 2484

장 98

ISE/ISE-PIC를 사용하여 사용자 제어 2485
ISE/ISE-PIC ID 소스 2485
대상 SGT(Security Group Tag) 매칭 2486
ISE/ISE-PIC의 라이선스 요구 사항 2487
ISE/ISE-PIC 요구 사항 및 사전 요건 2487
ISE/ISE-PIC 지침 및 제한 사항 2488
사용자 제어에 대한 ISE/ISE-PIC 설정 방법 2490
영역을 사용하지 않고 ISE를 구성하는 방법 2490
영역을 사용해 사용자 제어에 대한 ISE/ISE-PIC를 설정하는 방법 2491
ISE/ISE-PIC 구성 2492
ISE에서 보안 그룹 및 SXP 게시 구성 2493

FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기 2495
시스템 인증서 내보내기 2496
ISE/ISE-PIC 인증서 가져오기 2497
사용자 제어를 위한 ISE/ISE-PIC 설정 2497
ISE/ISE-PIC 설정 필드 2499
ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결 2500
ISE/ISE-PIC 기록 2502

장 99
캡티브 포털을 사용하여 사용자 제어 2505
캡티브 포털 ID 소스 2505
캡티브 포털 라이선스 요구 사항 2506
캡티브 포털 요구 사항 및 사전 요건 2506
캡티브 포털 가이드라인 및 제한 사항 2506
사용자 제어에 대한 캡티브 포털 설정 방법 2508
캡티브 포털 설정 1부: ID 정책 생성 2510
캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성 2512
캡티브 포털 설정 3부: 사용자 액세스 컨트롤 규칙 생성 2513
캡티브 포털 설정 4부: SSL 암호 해독 생성-정책 재서명 2514
캡티브 포털 설정 5부: ID 및 SSL 정책과 액세스 컨트롤 정책 연결 2515
캡티브 포털(captive portal) 필드 2516
캡티브 포털에서 애플리케이션 제외 2517
캡티브 포털(captive portal) ID 소스 문제 해결 2518
캡티브 포털 기록 2519

장 100
Remote Access VPN을 사용하여 사용자 제어 2521
Remote Access VPN ID 소스 2521
사용자 제어에 대한 RA VPN 설정 2522
원격 액세스 VPN ID 소스 문제 해결 2523
RA VPN 기록 2523

장 101
TS 에이전트를 사용하여 사용자 제어 2525

TS(Terminal Services) 에이전트 ID 소스 2525
TS 에이전트 가이드라인 2525
사용자 제어에 대한 TS 에이전트 설정 2526
TS 에이전트 ID 소스 문제 해결 2526
TS 에이전트 기록 2527

장 102

ID 정책 생성 및 관리 2529
ID 정책 정보 2529
ID 정책 라이선스 요구 사항 2530
ID 정책 요구 사항 및 사전 요건 2530
ID 규칙 생성 2531
Identity Rule Fields(ID 규칙 필드) 2532
ID 정책 생성 2534
ID 규칙 관리 2535
ID 정책 관리 2536

장 103

네트워크 검색 정책 2537
개요: 네트워크 검색 정책 2537
네트워크 검색 정책 요구 사항 및 사전 요건 2538
네트워크 검색 맞춤 설정 2538
네트워크 검색 정책 설정 2539
네트워크 검색 규칙 2539
네트워크 검색 규칙 구성 2540
작업 및 검색된 자산 2541
모니터링되는 네트워크 2542
포트 제외 2544
네트워크 검색 규칙의 영역 2546
트래픽 기반 탐지 ID 소스 2547
고급 네트워크 검색 옵션 설정 2550
네트워크 검색 일반 설정 2551
네트워크 검색 일반 설정 구성 2551

네트워크 검색 ID 충돌 설정 2552
네트워크 검색 ID 충돌 확인 설정 2553
네트워크 검색 취약성 영향 평가 옵션 2553
네트워크 검색 취약성 영향 평가 활성화 2554
보안 침해 지표 2554
보안 침해 지표 규칙 활성화 2555
네트워크 검색 정책에 NetFlow 엑스포터 추가 2556
네트워크 검색 데이터 스토리지 설정 2556
네트워크 검색 데이터 스토리지 설정 2558
네트워크 검색 이벤트 기록 설정 2558
네트워크 검색 OS 및 서버 ID 소스 추가 2559
네트워크 검색 전략 문제 해결 2560

부 XXI: 상관관계 및 컴플라이언스 2563

장 104 컴플라이언스 화이트 목록 2565
컴플라이언스 화이트 목록 소개 2565
규정준수 화이트리스트 대상 네트워크 2567
규정준수 화이트 리스트 호스트 프로필 2568
운영 체제별 호스트 프로파일 2568
공유 호스트 프로파일 2569
화이트 위반 트리거 2569
컴플라이언스 요구 사항 및 사전 요건 2571
규정준수 화이트 목록 생성 2571
규정준수 화이트 목록에 대한 대상 네트워크 설정 2573
화이트 리스트 호스트 프로필 빌드 2574
규정준수 화이트리스트에 애플리케이션 프로토콜 추가 2575
규정 준수 화이트 목록에 클라이언트 추가 2576
규정준수 화이트리스트에 웹 애플리케이션 추가 2576
규정준수 화이트리스트에 프로토콜 추가 2577
규정준수 화이트리스트 관리 2577

규정준수 화이트 목록 편집 2578
공유 호스트 프로파일 관리 2580

장 105 상관관계 정책 2583
상관관계 정책 및 규칙 소개 2583
컴플라이언스 요구 사항 및 사전 요건 2585
상관관계 정책 설정 2585
규칙 및 화이트 리스트에 응답 추가 2586
상관관계 정책 관리 2586
상관관계 규칙 설정 2587
침입 이벤트 트리거 기준 구문 2589
악성코드 이벤트 트리거 기준 구문 2592
검색 이벤트 트리거 기준 구문 2594
사용자 활동 이벤트 트리거 기준 구문 2597
호스트 입력 이벤트 트리거 기준 구문 2598
연결 이벤트 트리거 기준 구문 2599
트래픽 프로파일 변경 구문 2603
상관관계 호스트 프로파일 자격 구문 2605
사용자 자격 구문 2607
연결 추적기 2608
연결 추적기 추가 2609
연결 추적기 구문 2610
연결 추적기 이벤트 구문 2613
외부 호스트의 과도한 연결에 대한 샘플 설정 2613
과도한 BitTorrent 데이터 전송에 대한 샘플 설정 2615
스누즈 및 비활성 기간 2617
상관관계 규칙 작성 원리 2617
상관관계 규칙에 조건 추가 및 연결 2619
상관관계 규칙 조건에 여러 값 사용 2620
상관관계 규칙 관리 2620
상관관계 응답 그룹 설정 2621

상관관계 응답 그룹 관리 2622

장 106 트래픽 프로파일 2623

트래픽 프로파일 소개 2623

트래픽 프로파일 조건 2625

트래픽 프로필 요구 사항 및 사전 요건 2627

트래픽 프로파일 관리 2627

트래픽 프로파일 설정 2628

트래픽 프로파일 조건 추가 2629

트래픽 프로파일에 호스트 프로파일 자격 추가 2630

트래픽 프로파일 조건 구문 2631

트래픽 프로파일의 호스트 프로파일 자격 구문 2632

트래픽 프로파일 조건에서 여러 값 사용 2635

장 107 치료 2637

교정 요구 사항 및 사전 요건 2637

교정 소개 2637

Cisco IOS Null Route 교정 2638

Cisco IOS 라우터에 대한 교정 설정 2639

Nmap 스캔 교정 2644

속성 값 교정 설정 2644

세트 속성값 교정 구성 2644

교정 모듈 관리 2646

교정 인스턴스 관리 2646

단일 교정 모듈 인스턴스 관리 2647

부 XXII: 보고 및 알림 2649

장 108 보고서 작업 2651

보고서 요구 사항 및 사전 요건 2651

보고서 소개 2651

위험 보고서 2652
위험 보고서 생성, 보기 및 인쇄 2652
Introduction to Reports(보고서 소개) 2653
설계 보고서 정보 2653
보고서 템플릿 2653
보고서 템플릿 필드 2654
보고서 템플릿 생성 2655
보고서 템플릿 설정 2659
보고서 템플릿 관리 2671
보고서 생성 정보 2673
보고서 생성 2673
보고서 생성 옵션 2674
생성 시 이메일로 보고서 배포 2675
향후 보고서 예약 2675
생성된 보고서 작업 정보 2675
보고서 보기 2675
보고서 다운로드 2676
보고서 원격 저장 2677
원격 스토리지로 보고서 이동 2677
보고서 삭제 2678
보고 기록 2679

장 109 알림 응답을 사용한 외부 알림 2681
Firepower Management Center 알림 응답 2681
알림 응답 지원 설정 2682
알림 응답 요구 사항 및 사전 요건 2682
SNMP 알림 응답 생성 2683
Syslog 알림 응답 생성 2684
시스템 로그 알림 시설 2685
Syslog 심각도 레벨 2686
이메일 알림 응답 생성 2687

영향 플래그 알림 설정 2688
검색 이벤트 알림 설정 2688
AMP for Networks 알림 설정 2689

장 110 침입 이벤트에 대한 외부 알림 2691
침입 이벤트에 대한 외부 알림 정보 2691
침입 이벤트 외부 알림 라이선스 요구 사항 2692
침입 이벤트 외부 알림 요구 사항 및 사전 요건 2692
침입 이벤트에 대한 SNMP 알림 설정 2692
침입 SNMP 알림 옵션 2693
침입 이벤트를 위한 시스템 로그 알림 설정 2694
침입 시스템 로그 알림에 대한 시설 및 Severities(심각도) 2695
침입 이벤트에 대한 이메일 알림 설정 2696
침입 이메일 알림 옵션 2697

부 XXIII: 이벤트 및 자산 분석 툴 2699

장 111 **Context Explorer** 사용 2701
Context Explorer(상황 탐색기) 정보 2701
대시보드 및 Context Explorer 간 차이 2702
트래픽 및 침입 이벤트 횟수 시간 그래프 2703
보안 침해 지표 섹션 2703
지표별 호스트 그래프 2703
호스트별 지표 그래프 2704
네트워크 정보 섹션 2704
운영 체제 그래프 2704
소스 IP별 트래픽 그래프 2704
소스 사용자별 트래픽 그래프 2705
액세스 제어 작업별 연결 그래프 2705
대상 IP별 트래픽 그래프 2705
인그레스/이그레스 보안 영역별 트래픽 그래프 2705

애플리케이션 정보 섹션 2706
애플리케이션 정보 섹션 초점 2706
위험/비즈니스 관련성 및 애플리케이션별 트래픽 그래프 2707
위험/비즈니스 관련성 및 애플리케이션별 침입 이벤트 그래프 2707
위험/비즈니스 관련성 및 애플리케이션별 호스트 그래프 2708
애플리케이션 상세정보 목록 2708
보안 인텔리전스 섹션 2709
카테고리별 보안 인텔리전스 트래픽 그래프 2709
소스 IP별 보안 인텔리전스 트래픽 그래프 2709
대상 IP별 보안 인텔리전스 트래픽 그래프 2709
침입 정보 섹션 2710
영향별 침입 이벤트 그래프 2710
상위 공격자 그래프 2710
상위 사용자 그래프 2710
우선 순위별 침입 이벤트 그래프 2711
상위 대상 그래프 2711
상위 인그레스/이그레스 보안 영역 그래프 2711
침입 이벤트 상세정보 목록 2711
파일 정보 섹션 2712
상위 파일 유형 그래프 2712
상위 파일 이름 그래프 2712
성향별 파일 그래프 2712
상위 호스트 전송 파일 그래프 2713
상위 호스트 수신 파일 그래프 2713
상위 악성코드 탐지 그래프 2713
지리위치 정보 섹션 2714
이니시에이터/응답자 국가별 연결 그래프 2714
소스/목적지 국가별 침입 이벤트 그래프 2714
전송/수신 국가별 파일 이벤트 그래프 2715
URL 정보 섹션 2715
URL별 트래픽 그래프 2715

URL 카테고리별 트래픽 그래프 2716
URL 평판별 트래픽 그래프 2716
Context Explorer 요구 사항 및 사전 요건 2716
Context Explorer(상황 탐색기) 새로 고침 2717
Context Explorer(상황 탐색기) 시간 범위 설정 2717
Context Explorer(상황 탐색기) 섹션 최소화 및 최대화 2718
Context Explorer(상황 탐색기) 데이터에 대해 드릴다운 2718
Context Explorer의 필터 2719
데이터 유형 필드 옵션 2720
추가 필터 창에서 필터 생성 2723
콘텍스트 메뉴에서 빠른 필터 생성 2724
필터링된 Context Explorer(상황 탐색기) 보기 저장 2724
필터 데이터 보기 2725
필터 삭제 2725

장 112 네트워크 맵 사용 2727
네트워크 맵 요구 사항 및 사전 요건 2727
네트워크 맵 2727
호스트 네트워크 맵 2728
네트워크 디바이스 네트워크 맵 2729
모바일 디바이스 네트워크 맵 2730
보안 침해 지표 네트워크 맵 2730
애플리케이션 프로토콜 네트워크 맵 2731
취약성 네트워크 맵 2732
호스트 속성 네트워크 맵 2733
네트워크 맵 보기 2733
맞춤형 네트워크 토폴로지 2734
맞춤형 토폴로지 생성 2734
네트워크 검색 정책에서 네트워크 가져오기 2735
맞춤형 토폴로지에 수동으로 네트워크 추가 2736
맞춤형 토폴로지 활성화 및 비활성화 2736

맞춤형 토폴로지 편집 2737

장 113 인시던트 2739

인시던트 처리 정보 2739

인시던트의 정의 2739

일반 인시던트 처리 프로세스 2740

Firepower System의 인시던트 유형 2742

인시던트 라이선스 요구 사항 2743

인시더트 요구 사항 및 사전 요건 2743

맞춤형 인시던트 유형 생성 2743

인시던트 생성 2744

인시던트 편집 2744

인시던트 보고서 생성 2745

장 114 조회 사용 2747

조회 소개 2747

Whois 조회 수행 2747

IP 주소에 대한 지리위치 정보 찾기 2748

장 115 외부 툴을 사용하여 이벤트 분석 2749

Cisco SecureX와의 통합 2749

다음을 이용한 이벤트 분석 Cisco SecureX Threat Response 2749

Cisco SecureX Threat Response에서 이벤트 데이터 보기 2750

웹 기반 리소스를 사용한 이벤트 조사 2750

상황별 크로스 실행 리소스 관리 정보 2751

맞춤형 상황별 크로스 실행 리소스 요구 사항 2751

상황별 크로스 실행 리소스 추가 2752

상황별 크로스 실행을 이용한 이벤트 조사 2753

다음에 대한 교차 실행 링크 설정 Stealthwatch 2754

Security Events(보안 이벤트)에 대한 시스템 로그 메시지 전송 정보 2755

보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보 2755

보안 이벤트 시스템 로그 메시지 구성 모범 사례 2755
FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기 2756
클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기 2759
보안 이벤트 시스템 로그에 대한 설정 위치 2760
Security(보안) 이벤트 시스템 로그 메시지 구조 2764
보안 이벤트 시스템 로그 메시지의 시설 2767
Firepower System 로그 메시지 유형 2768
보안 이벤트에 대한 시스템 로그 제한 사항 2769
eStreamer 서버 스트리밍 2769
시스템 로그 및 eStreamer의 보안 이벤트 비교 2770
(시스템 로그가 아닌) eStreamer로만 전송된 데이터 2770
eStreamer 이벤트 유형 선택 2772
eStreamer 클라이언트 커뮤니케이션 설정 2772
Splunk의 이벤트 분석 2773
IBM QRadar의 이벤트 분석 2773
외부 툴을 사용한 이벤트 데이터 분석 기록 2774

부 XXIV: 워크플로 2779

장 116 워크플로 2781
개요: 워크플로 2781
사전 정의 워크플로 2782
사전 정의 침입 이벤트 워크플로 2782
사전 정의 악성코드 워크플로 2783
사전 정의 파일 워크플로 2784
사전 정의 캡처 파일 워크플로 2784
사전 정의 연결 데이터 워크플로 2785
사전 정의 보안 인텔리전스 워크플로 2787
사전 정의 호스트 워크플로 2787
사전 정의 보안 침해 지표 워크플로 2787
사전 정의 애플리케이션 워크플로 2788

사전 정의 애플리케이션 상세정보 워크플로 2789
사전 정의 서버 워크플로 2789
사전 정의 호스트 속성 워크플로 2789
사전 정의 검색 이벤트 워크플로 2790
사전 정의 사용자 워크플로 2790
사전 정의 취약성 워크플로 2790
사전 정의 서드파티 취약성 워크플로 2791
사전 정의 상관관계 및 화이트 목록 워크플로 2791
사전 정의 시스템 워크플로 2792
맞춤형 테이블 워크플로 2792
워크플로 사용 2793
사용자 역할별 워크플로 액세스 2795
워크플로 선택 2795
워크플로 페이지 2797
워크플로 페이지 탐색 툴 2798
워크플로 페이지 이동 툴 2798
파일 경로 아이콘 2799
호스트 프로파일 아이콘 2799
위협 점수 아이콘 2800
워크플로 툴바 2800
드릴다운 페이지 사용 2801
테이블 보기 페이지 사용 2802
지리위치 2802
지리위치 상세정보 2803
연결 이벤트 그래프 2804
연결 이벤트 그래프 사용 2805
이벤트 시간 제약 조건 2811
이벤트에 대한 세션별 타임 윈도우 맞춤 설정 2812
이벤트에 대한 기본 타임 윈도우 2816
이벤트 보기 제약 조건 2818
이벤트 제약 2819

복합 이벤트 보기 제약 2820
복합 이벤트 보기 제약 사용 2821
워크플로 간 탐색 2821
북마크 2822
즐겨찾기 생성 2822
즐겨찾기 보기 2823
워크플로우 히스토리 2823

장 117 이벤트 검색 2825
이벤트 검색 2825
검색 제약 조건 2826
일반 검색 제약 조건 2826
검색 내 와일드카드 및 특수문자 2827
검색 내 개체 및 애플리케이션 필터 2827
검색 내 시간 제약 조건 2827
검색 내 IP 주소 2828
검색의 URL 2829
검색 내 매니지드 디바이스 2829
검색 내 포트 2829
검색 내 이벤트 필드 2830
검색 수행 2831
검색 저장 2832
저장된 검색 로드 2833
셸을 통해 쿼리 재정의 2833
셸 기반 쿼리 관리 구문 2834
오래 실행되는 쿼리 중지 2834
이벤트 검색 히스토리 2835

장 118 사용자 지정 워크플로 2837
맞춤형 워크플로 소개 2837
저장된 맞춤형 워크플로 2837

맞춤형 워크플로 생성 2839
비 연결 데이터 기반 맞춤형 워크플로 생성 2840
맞춤형 연결 데이터 워크플로 생성 2841
맞춤형 워크플로 사용 및 관리 2842
사전 정의 테이블 기반 맞춤형 워크플로 보기 2842
맞춤형 테이블 기반 맞춤형 워크플로 보기 2843
맞춤형 워크플로 2843

장 119 사용자 지정 표 2845
맞춤형 테이블 소개 2845
사전 정의 맞춤형 테이블 2845
가능한 테이블 조합 2846
사용자 정의 맞춤형 테이블 2850
맞춤형 테이블 생성 2851
맞춤형 테이블 수정 2851
맞춤형 테이블 삭제 2852
맞춤형 테이블 기반 워크플로 보기 2852
맞춤형 테이블 검색 2853
맞춤형 테이블 기록 2855

부 XXV: 이벤트 및 자산 2857

장 120 연결 로깅 2859
연결 로깅 정보 2859
항상 로깅되는 연결 2860
로깅할 수 있는 기타 연결 2861
규칙 및 정책 작업이 로깅에 미치는 영향 2861
모니터링된 연결에 대한 로깅 2862
신뢰할 수 있는 연결에 대한 로깅 2862
차단된 연결에 대한 로깅 2863
허용된 연결에 대한 로깅 2864

연결 시작 또는 종료 로깅 2865
Firepower Management Center 대 외부 로깅 2866
연결 로깅 제한사항 2867
이벤트가 이벤트 뷰어에 표시되는 경우 2867
연결 로깅 모범 사례 2868
연결 로깅 요구 사항 및 사전 요건 2870
연결 로깅 설정 2870
SSL 규칙으로 암호 해독 가능 연결 로깅 2870
보안 인텔리전스로 연결 로깅 2871
액세스 제어 규칙으로 연결 로깅 2872
정책 기본 작업으로 연결 로깅 2873
긴 URL의 로깅 제한 2874

장 121 연결 및 보안 인텔리전스 이벤트 2875
연결 이벤트 정보 2875
연결 또는 보안 인텔리전스 이벤트 2876
NetFlow 연결 2876
연결 요약(그래프에 대한 집계된 데이터) 2876
오래 실행되는 연결 2877
외부 응답자의 연결 요약 통합 2877
연결 및 보안 인텔리전스 이벤트 필드 2877
연결 및 보안 인텔리전스 이벤트 필드 정보 2892
이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침 2893
연결 이벤트 이유 2893
연결 이벤트 필드 채우기 요구 사항 2895
연결 이벤트 필드에서 제공되는 정보 2896
연결 및 보안 인텔리전스 이벤트 테이블 사용 2900
연결 내에서 탐지된 파일 및 악성코드 보기 2903
연결에 연결된 침입 이벤트 보기 2904
암호화된 연결 인증서 세부 정보 2904
연결 요약 페이지 보기 2905

연결 및 보안 인텔리전스 이벤트 기록 2906

장 122

침입 이벤트 작업 2909
침입 이벤트 정보 2909
침입 이벤트 검토 및 평가용 도구 2910
침입 이벤트 라이선스 요구 사항 2910
침입 이벤트 요구 사항 및 사전 요건 2910
침입 이벤트 보기 2911
침입 이벤트 필드 정보 2912
침입 이벤트 필드 2912
침입 이벤트 영향 레벨 2924
침입 이벤트 관련 연결 데이터 보기 2925
검토된 침입 이벤트 표시 2926
이전에 검토된 침입 이벤트 보기 2927
검토된 침입 이벤트를 검토되지 않은 것으로 표시 2927
전처리기 이벤트 2927
전처리기 생성기 ID 2928
침입 이벤트 워크플로 페이지 2931
침입 이벤트 워크플로 사용 2932
침입 이벤트 드릴다운 페이지 제약 조건 2934
침입 이벤트 테이블 보기 제약 조건 2934
침입 이벤트 패킷 보기 사용 2935
이벤트 정보 필드 2937
프레임 정보 필드 2943
데이터 링크 레이어 정보 필드 2944
네트워크 레이어 정보 보기 2945
Viewing Transport Layer Information 2947
패킷 바이트 정보 보기 2950
내부 소스 침입 이벤트 2950
침입 이벤트 클립보드 2951
클립보드 보고서 생성 2951

클립보드에서 이벤트 삭제 2952
침입 이벤트 통계 보기 2952
호스트 통계 자료 2953
이벤트 개요 2953
이벤트 통계 2954
침입 이벤트 성능 그래프 보기 2955
침입 이벤트 성능 통계 그래프 유형 2955
침입 이벤트 그래프 보기 2960
침입 이벤트 기록 2961

장 123

파일/악성코드 이벤트 및 네트워크 파일 경로 분석 2963
파일/악성코드 이벤트 및 네트워크 파일 경로 분석 정보 2963
파일 및 악성코드 이벤트 2964
파일 및 악성코드 이벤트 유형 2965
파일 이벤트 2965
악성코드 이벤트 2965
회귀적 악성코드 이벤트 2965
AMP for Endpoints에 의해 생성된 악성코드 이벤트 2966
파일 및 악성코드 이벤트 워크플로 사용 2967
파일 및 악성코드 이벤트 필드 2968
악성코드 이벤트 하위 유형 2979
파일 및 악성코드 이벤트 필드에서 사용할 수 있는 정보 2981
분석된 파일에 대한 세부 정보 보기 2984
파일 구성 보고서 2984
AMP 프라이빗 클라우드에서 파일 세부 정보 보기 2984
위협 점수 및 동적 분석 요약 보고서 2984
캡처된 파일 워크플로 사용 2985
캡처된 파일 필드 2986
저장된 파일 다운로드 2991
분석을 위해 수동으로 파일 제출 2991
네트워크 파일 전파 흔적 분석 2992

최근 탐지된 악성코드 및 분석된 경로 분석 2992
네트워크 파일 경로 분석 상세정보 보기 2993
네트워크 파일 경로 분석 요약 정보 2993
네트워크 파일 경로 분석 맵 및 관련 이벤트 목록 2995
네트워크 파일 경로 분석 사용 2996
AMP for Endpoints 콘솔의 이벤트 데이터 작업 2998
파일, 악성코드 이벤트 및 네트워크 파일 경로 분석 기록 2999

장 124

호스트 프로파일 사용 3001
호스트 프로파일에 대한 요구 사항 및 사전 요건 3001
호스트 프로파일 3002
호스트 프로파일 제한 3003
호스트 프로파일 보기 3003
호스트 프로파일의 기본 호스트 정보 3004
호스트 프로파일의 운영 체제 3006
운영 체제 ID 보기 3008
현재 운영 체제 ID 설정 3008
운영 체제 ID 충돌 3009
충돌하는 운영 체제 ID를 현재 ID로 만들기 3009
운영 체제 ID 충돌 해결 3010
호스트 프로파일의 서버 3010
호스트 프로파일의 서버 상세정보 3012
서버 상세정보 보기 3014
서버 ID 수정 3014
서버 ID 충돌 해결 3015
호스트 프로파일의 웹 애플리케이션 3015
호스트 프로파일에서 웹 애플리케이션 삭제 3017
호스트 프로파일의 호스트 프로토콜 3017
호스트 프로파일에서 프로토콜 삭제 3018
호스트 프로파일의 보안 침해 지표 3018
호스트 프로파일의 VLAN 태그 3018

호스트 프로파일의 사용자 기록 3019
호스트 프로파일의 호스트 속성 3019
사전 정의된 호스트 속성 3019
화이트 목록 호스트 속성 3020
사용자 정의 호스트 속성 3020
텍스트 또는 URL 기반 호스트 속성 생성 3021
정수 기반 호스트 속성 생성 3022
목록 기반 호스트 속성 생성 3022
호스트 속성값 설정 3023
호스트 프로파일의 화이트 목록 위반 3023
공유 화이트 목록 호스트 프로파일 생성 3024
호스트 프로파일의 악성코드 탐지 3024
호스트 프로파일의 취약성 3025
취약성 패치 다운로드 3026
개별 호스트 취약성 비활성화 3027
개별 취약성 비활성화 3027
호스트 프로파일의 스캔 결과 3028
호스트 프로파일에서 호스트 스캔 3028
호스트 프로파일 기록 3029

장 125 검색 이벤트 작업 3031
검색 이벤트 요구 사항 및 사전 요건 3031
검색 이벤트의 검색 및 ID 데이터 3031
검색 이벤트 통계 보기 3032
통계 요약 섹션 3033
이벤트 분류 섹션 3034
프로토콜 분류 섹션 3035
애플리케이션 프로토콜 분류 섹션 3035
OS 분류 섹션 3035
검색 성능 그래프 보기 3035
검색 성능 그래프 유형 3036

검색 및 ID 워크플로 사용 3037
검색 및 호스트 입력 이벤트 3039
검색 이벤트 유형 3039
호스트 입력 이벤트 유형 3043
검색 및 호스트 입력 이벤트 보기 3045
검색 이벤트 필드 3046
호스트 데이터 3047
호스트 데이터 보기 3047
호스트 데이터 필드 3048
선택한 호스트에 대한 트래픽 프로파일 생성 3053
선택한 호스트를 기반으로 규정준수 화이트리스트 생성 3053
호스트 속성 데이터 3054
호스트 속성 보기 3054
호스트 속성 데이터 필드 3055
선택한 호스트에 대해 호스트 속성 설정 3056
보안 침해 지표 데이터 3056
보안 침해 지표 데이터 보기 및 작업 3056
보안 침해 지표 데이터 필드 3058
단일 호스트에 대한 보안 침해 지표 규칙 상태 수정 3059
보안 침해 지표 태그의 소스 이벤트 보기 3059
보안 침해 지표 태그 해결 3059
서버 데이터 3060
서버 데이터 보기 3060
서버 데이터 필드 3061
애플리케이션 및 애플리케이션 상세정보 데이터 3064
애플리케이션 데이터 보기 3064
애플리케이션 데이터 필드 3065
애플리케이션 세부사항 데이터 보기 3067
애플리케이션 세부사항 데이터 필드 3067
취약성 데이터 3069
취약성 데이터 필드 3069

취약성 비활성화 3071
취약성 데이터 보기 3071
취약성 세부사항 보기 3072
다중 취약성 비활성화 3073
서드파티 취약성 데이터 3073
서드파티 취약성 데이터 보기 3074
서드파티 취약성 데이터 필드 3074
활성 세션, 사용자 및 사용자 활동 데이터 3076
사용자 관련 필드 3076
활성 세션 데이터 3083
사용자 데이터 3084
사용자 활동 데이터 3087
사용자 프로파일 및 호스트 기록 3089
검색 이벤트 작업 히스토리 3091

장 126 상관관계 및 규정 준수 이벤트 3093
상관관계 이벤트 보기 3093
상관관계 이벤트 필드 3095
컴플라이언스 화이트 목록 워크플로우 사용 3097
화이트리스트 이벤트 보기 3099
화이트 목록 이벤트 필드 3099
화이트리스트 위반 보기 3101
화이트 목록 위반 필드 3101
교정 상태 이벤트 3103
교정 상태 이벤트 보기 3103
교정 상태 테이블 필드 3104
교정 상태 이벤트 테이블 사용 3105

부록 A: 보안, 인터넷 액세스 및 통신 포트 3107
보안 요건 3107
Cisco Cloud 3107

인터넷 액세스 요구 사항 3108
통신 포트 요구 사항 3110

부록 B: 명령줄 참조 3113
클래식 디바이스 CLI 정보 3113
클래식 디바이스 CLI 모드 3114
클래식 디바이스 CLI 액세스 레벨 3114
클래식 디바이스 CLI 관리 명령 3114
configure password 3114
exit 3115
expert 3115
history 3116
logout 3116
? (물음표) 3116
클래식 디바이스 CLI 명령 표시 3117
access-control-config 3117
경보 3118
arp-tables 3118
audit-log 3119
우회 3119
high-availability 명령 3120
config 3120
high-availability ha-statistics 3120
cpu 3120
database 명령 3121
processes 3122
slow-query-log 3122
device-settings 3122
disk 3123
disk-manager 3123
dns 3123
fan-status 3124
fastpath-rules 3124

gui 3125
hostname 3125
호스트 3125
hyperthreading 3126
inline-sets 3126
인터페이스 3127
ifconfig 3127
lcd 3127
link-aggregation 명령 3128
  구성 3128
  statistics 3128
link-state 3129
log-ips-connection 3129
관리자 3129
memory 3130
모델 3130
mpls-depth 3131
NAT 명령 3131
  active-dynamic 3131
  active-static 3132
  allocators 3132
  config 3132
  dynamic-rules 3132
  플로우 3133
  static-rules 3133
netstat 3133
network 3134
network-modules 3134
network-static-routes 3134
ntp 3135
perfstats 3135
portstats 3136
power-supply-status 3136

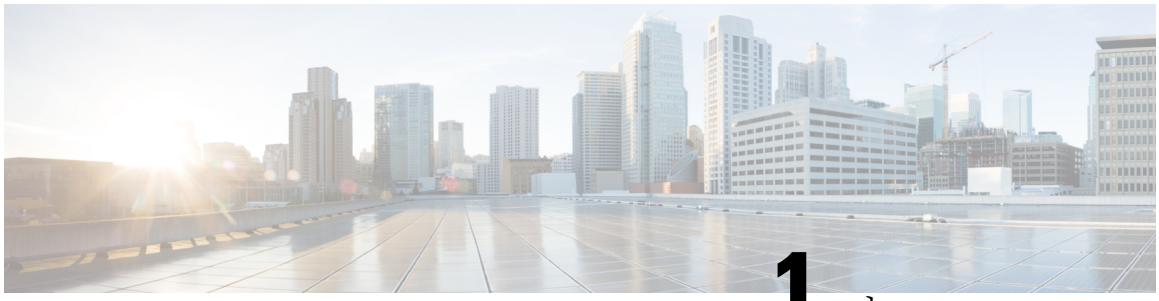
process-tree 3136
processes 3137
route 3137
routing-table 3138
serial-number 3138
ssl-policy-config 3138
스태킹 3139
summary 3139
시간 3140
traffic-statistics 3140
user 3141
사용자 3141
버전 3142
virtual-routers 3143
virtual-switches 3143
vmware-tools 3143
VPN 명령 3144
config 3144
config by virtual router 3145
status 3145
status by virtual router 3145
카운터 3145
counters by virtual router 3146
클래식 디바이스 CLI 구성 명령 3146
우회 3146
high-availability 3147
gui 3147
lcd 3147
log-ips-connections 3148
manager 명령 3148
add 3148
delete 3149
mpls-depth 3149

network 명령 3150
dns searchdomains 3150
dns servers 3150
hostname 3150
http-proxy 3151
http-proxy-disable 3151
ipv4 delete 3152
ipv4 dhcp 3152
ipv4 manual 3152
ipv6 delete 3153
ipv6 dhcp 3153
ipv6 manual 3153
ipv6 router 3153
management-interface disable 3154
management-interface disable-event-channel 3154
management-interface disable-management-channel 3155
management-interface enable 3155
management-interface enable-event-channel 3156
management-interface enable-management-channel 3156
management-interface tcpport 3157
management-port 3157
static-routes ipv4 add 3157
static-routes ipv4 delete 3158
static-routes ipv6 add 3158
static-routes ipv6 delete 3158
password 3159
stacking disable 3159
user 명령 3160
access 3160
add 3160
aging 3161
delete 3161
비활성화 3161
enable 3162

forcereset 3162
maxfailedlogins 3162
minpasswdlen 3163
password 3163
strengthcheck 3163
잠금 해제 3164
vmware-tools 3164
클래식 디바이스 CLI 시스템 명령 3165
access-control 명령 3165
archive 3165
clear-rule-counts 3165
롤백 3166
disable-http-user-cert 3166
file 명령 3166
copy 3167
delete 3167
list 3167
secure-copy 3168
generate-troubleshoot 3168
ldapsearch 3169
lockdown 3169
nat rollback 3170
reboot 3170
restart 3171
shutdown 3171
클래식 디바이스 CLI 기록 3172

부록 C: **Firepower Management Center** 명령줄 참조 3175
Firepower Management Center CLI 정보 3175
Firepower Management Center CLI 모드 3176
Firepower Management Center CLI 관리 명령 3176
exit 3176
expert 3177

? (물음표) 3177
Firepower Management Center CLI show 명령 3177
버전 3178
Firepower Management Center CLI 구성 명령 3178
password 3178
Firepower Management Center CLI 시스템 명령 3179
generate-troubleshoot 3179
lockdown 3179
reboot 3180
restart 3180
shutdown 3180
Firepower Management Center CLI의 기록 3181



1 장

Firepower 시작하기

Cisco Firepower는 네트워크 보안 및 트래픽 관리 제품들로 구성된 통합 제품군으로, 특별히 구축된 플랫폼에 또는 소프트웨어 솔루션으로서 구축됩니다. 이 시스템에서는 조직의 보안 정책(네트워크 보호 지침)을 준수하는 방식으로 네트워크 트래픽을 처리할 수 있습니다.

일반적인 구축에서는 네트워크 세그먼트에 설치된 여러 트래픽 센싱 매니지드 디바이스가 분석을 위해 트래픽을 모니터링하고 관리자에게 보고합니다.

- Firepower Management Center
- Firepower Device Manager
- ASDM(Adaptive Security Device Manager)

관리자는 관리, 분석 및 보고 작업을 수행하는 데 사용할 수 있는 그래픽 유저 인터페이스가 포함된 중앙 집중식 관리 콘솔을 제공합니다.

이 가이드는 *Firepower Management Center* 관리 어플라이언스를 중점적으로 다룹니다. Firepower Device Manager 또는 ASDM을 통해 관리되는 ASA with FirePOWER Services에 관한 내용은 이러한 관리방법에 대한 가이드를 참조하십시오.

- *Firepower Device Manager*용 *Cisco Firepower Threat Defense* 구성 가이드
- *ASA with FirePOWER Services* 로컬 관리 구성 가이드

- 빠른 시작: 기본 설정, 2 페이지
- Firepower 디바이스, 7 페이지
- Firepower 기능, 8 페이지
- FMC 검색, 13 페이지
- 도메인 전환 Firepower Management Center, 14 페이지
- 상황 메뉴, 14 페이지
- Firepower 온라인 도움말, 방법 및 문서, 16 페이지
- Firepower System IP 주소 규칙, 19 페이지
- 추가 리소스, 20 페이지
- Firepower 시작 기록, 20 페이지

빠른 시작: 기본 설정

Firepower 기능 설정은 강력하고 유연하게 기본 및 고급 구성을 지원할 수 있습니다. 다음 섹션을 사용하여 신속하게 Firepower Management Center 및 해당 매니지드 디바이스를 설정하고 제어 및 분석 트래픽을 시작합니다.

물리적 어플라이언스에서 초기 설정 설치 및 수행

프로시저

해당 어플라이언스에 대한 문서를 사용하여 모든 물리적 어플라이언스에서 초기 설정을 설치 및 수행합니다.

- **Firepower Management Center**
  - 해당 하드웨어 모델의 *Cisco Firepower Management Center* 시작 가이드

    http://www.cisco.com/go/firepower-mc-install

- **Firepower Threat Defense** 매니지드 디바이스

  중요 이 페이지에서 Firepower Device Manager 문서를 무시합니다.

  - Cisco Firepower 1010 시작 가이드
  - Cisco Firepower 1100 Series 시작 가이드
  - Cisco Firepower 2100 Series 시작 가이드
  - Cisco Firepower 4100 시작 가이드
  - Cisco Firepower 9300 시작 가이드
  - Firepower Management Center를 사용하는 ASA 5508-X 및 ASA 5516-X용 Cisco Firepower Threat Defense 빠른 시작 가이드

- 클래식 매니지드 디바이스
  - Cisco ASA FirePOWER 모듈 빠른 시작 가이드
  - Cisco Firepower 8000 Series 시작 가이드
  - Cisco Firepower 7000 Series 시작 가이드

가상 어플라이언스 구축

구축에 가상 어플라이언스가 포함된 경우 이러한 단계를 수행합니다. 문서 로드맵을 사용하여 아래에 나열된 문서를 찾습니다. http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

프로시저

단계 **1** Management Center 및 디바이스에 사용할 지원되는 가상 플랫폼을 결정합니다(모두 동일하지는 않음). *Cisco Firepower* 호환성 가이드를 참조하십시오.

단계 **2** 다음과 같은 사용자 환경에 대한 문서를 사용하여 가상 Firepower Management Center를 구축합니다.

- VMware에서 실행되는 Firepower Management Center Virtual: *VMware* 구축용 *Cisco Firepower Management Center* 빠른 시작 가이드
- AWS에서 실행되는 Firepower Management Center Virtual: *AWS* 구축용 *Cisco Firepower Management Center* 빠른 시작 가이드
- KVM에서 실행되는 Firepower Management Center Virtual: *KVM* 구축용 *Cisco Firepower Management Center* 빠른 시작 가이드

단계 **3** 다음과 같은 어플라이언스에 대한 문서를 사용하여 가상 디바이스를 구축합니다.

- VMware에서 실행되는 NGIPSv : *VMware*용 *Cisco Firepower NGIPSv* 빠른 시작 가이드
- VMware에서 실행되는 Firepower Threat Defense Virtual: *Firepower Management Center* 빠른 시작 가이드를 사용하는 *Firepower ASA 5508-X* 및 *ASA 5516-X*용 *Cisco Firepower Threat Defense*
- AWS에서 실행되는 Firepower Threat Defense Virtual: *AWS* 구축용 *Cisco Firepower Threat Defense Virtual* 빠른 시작 가이드
- KVM에서 실행되는 Firepower Threat Defense Virtual: *KVM* 구축용 *Cisco Firepower Threat Defense Virtual* 빠른 시작 가이드
- Azure에서 실행되는 Firepower Threat Defense Virtual: *Azure* 구축용 *Cisco Firepower Threat Defense Virtual* 빠른 시작 가이드

최초 로그인

새 FMC에 처음 로그인하기 전에, 물리적 어플라이언스에서 초기 설정 설치 및 수행, 2 페이지 또는 가상 어플라이언스 구축, 3 페이지의 설명에 따라 어플라이언스를 준비합니다.

새 FMC(또는 출고 시 설정으로 새로 복원된 FMC)에 처음 로그인할 때는, CLI 또는 웹 인터페이스용 관리자 계정을 사용하고 사용자의 FMC 모델에 맞는 *Cisco Firepower Management Center* 시작 가이드의 지침을 따르십시오. 초기 구성 프로세스가 끝나면 시스템의 다음 요소를 구성하게 됩니다.

- 두 관리자 계정(웹 인터페이스 액세스용 하나와 CLI 액세스용 하나)의 비밀번호는 사용자 어카운트 가이드라인 및 제한 사항에서 설명하는 강력한 비밀번호 요구 사항을 준수해, 같은 값으로 설정됩니다. 시스템은 초기 구성 프로세스에서만 두 관리자 계정의 비밀번호를 동기화합니다. 나중에 아무 관리자 계정의 비밀번호를 변경하면 두 계정의 비밀번호가 달라지며, 강력한 비밀번호 요건이 웹 인터페이스 관리자 계정에 적용되지 않게 됩니다. (웹 인터페이스에서 내부 사용자 추가 참조)
- FMC이(가) 자체 관리 인터페이스(eth0)를 통한 네트워크 통신에 사용하는 다음 네트워크 설정은 기본값이나 사용자가 입력한 값으로 설정됩니다.
  - FQDN(Fully Qualified Domain Name)(`<hostname>.<domain>`)
  - IPv4 구성에 대한 부팅 프로토콜(DHCP 또는 고정/수동)
  - IPv4 주소
  - 네트워크 마스크
  - 게이트웨이
  - DNS 서버
  - NTP 서버

  이러한 설정의 값은 FMC 웹 인터페이스에서 확인하고 변경할 수 있습니다. 자세한 내용은 FMC 관리 인터페이스 수정, 1358 페이지 및 시간 및 시간 동기화, 1379 페이지의 내용을 참조하십시오.
- 초기 구성 중에 FMC는 주 단위로 자동 GeoDB 업데이트를 구성합니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, GeoDB 업데이트 예약, 185 페이지.
- 초기 구성 중 FMC는 주간 작업을 예약하여 FMC 및 매지니드 디바이스의 최신 소프트웨어를 다운로드합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약이 실패하고 FMC가 인터넷에 액세스할 수 있다면 소프트웨어 다운로드 자동화, 258 페이지.

  중요 이 작업은 FMC에 소프트웨어 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.
- 초기 구성 중에 FMC는 주간 작업을 예약하여 로컬에 저장된 구성 전용 백업을 수행합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약에 실패하면 설명에 따라 백업을 수행하는 반복 작업을 예약하는 것이 좋습니다. FMC 백업 예약, 248 페이지.
- 초기 구성 중 FMC는 Cisco 지원 사이트에서 최신 취약점 데이터베이스(VDB)를 다운로드하고 설치합니다. 이 작업은 한 번만 수행하면 됩니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 시스템을 최신 상태로 유지하고자 하고 FMC가 인터넷에 액세스할 수 있다면 취약성 데이터베이스 업데이트 자동화, 260 페이지.

- 초기 구성 중에 버전 FMC는 Cisco 지원 사이트에서 매일 자동 침입 규칙 업데이트를 구성합니다. (FMC는 다음에 영향을 받는 정책을 구축하는 경우 영향을 받는 관리되는 디바이스에 자동으로 침입 규칙 업데이트를 구축합니다.) 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, 반복 되는 침입 규칙 업데이트 구성, 189 페이지.

FMC 초기 구성이 완료되면, 디바이스 관리 기본 사항, 297 페이지에서 설명하는 디바이스 관리 페이지가 웹 인터페이스에 표시됩니다. (이것은 첫 번째 관리자 사용자 로그인에서만 표시되는 기본 로그인 페이지입니다. 관리자나 다른 사용자가 하는 이후 로그인에서는 홈 페이지 지정, 41 페이지에서 설명하는 방법에 따라 기본 로그인 페이지가 결정됩니다.)

초기 구성이 끝나면, 기본 정책 및 구성 설정, 5 페이지에 설명된 대로 기본 정책을 구성하여 트래픽 제어 및 분석을 시작합니다.

기본 정책 및 구성 설정

대시보드, Context Explorer 및 이벤트 테이블에서 데이터를 확인하려면 기본 정책을 구축해야 합니다.

참고 이것이 정책 또는 특징 및 기능에 대한 전체 설명은 아닙니다. 다른 기능 및 고급 구성에 대한 지침은 이 가이드의 나머지 부분을 참조하십시오.

시작하기 전에

- 웹 인터페이스 또는 CLI용 관리자 계정으로 웹 인터페이스에 로그인하고, https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.html에서 제공하는 하드웨어 모델별 *Cisco Firepower Management Center* 시작 가이드의 설명에 따라 초기 구성을 수행합니다.

프로시저

단계 **1** 기본 표준 시간대 설정, 46 페이지에 설명된 대로 이 어카운트의 시간대를 설정합니다.

단계 **2** 필요하다면 Firepower System 라이선싱, 157 페이지의 설명에 따라 라이선스를 추가합니다.

단계 **3** FMC에 디바이스 추가, 311 페이지의 설명에 따라 매니지드 디바이스를 구축에 추가합니다.

단계 **4** 다음에 설명된 대로 매니지드 디바이스를 구성합니다.

- IPS 디바이스 구축 및 구성 소개, 697 페이지기본 디바이스에서 수동 또는 인라인 인터페이스 구성
- Firepower Threat Defense 인터페이스 개요, 783 페이지Firepower Threat Defense 디바이스에 투명 또는 라우팅 모드 구성
- Firepower Threat Defense 인터페이스 개요, 783 페이지Firepower Threat Defense 디바이스에 인터페이스 구성

단계 **5** 기본 액세스 제어 정책 만들기, 1629 페이지에 설명된 대로 액세스 제어 정책을 구성합니다.

- 대부분의 경우 Cisco는 Balanced Security and Connectivity(보안과 연결의 균형 유지) 침입 정책을 기본 작업으로 설정할 것을 제안합니다. 자세한 내용은 Access Control Policy Default Action(액세스 제어 정책 기본 작업), 1610 페이지 및 시스템 제공 네트워크 분석 및 침입 정책, 1968 페이지를 참조하십시오.
- 대부분의 경우 Cisco는 조직의 보안 규제 준수 요구사항을 충족시키기 위해 연결 로깅 활성화를 제안합니다. 디스플레이를 복잡하게 만들거나 시스템을 마비시키지 않도록 로깅할 연결을 결정하는 경우 네트워크에서의 트래픽을 고려합니다. 자세한 내용은 연결 로깅 정보, 2859 페이지를 참고하십시오.

단계 **6** 상태 정책 적용, 399 페이지에 설명된 대로 시스템 제공 기본 상태 정책을 적용합니다.

단계 **7** 시스템 구성 설정 중 일부를 맞춤화합니다.

- 서비스에 대한 인바운드 연결을 허용하려면(예: SNMP 또는 시스템 로그) 액세스 목록 구성, 1370 페이지에 설명된 대로 액세스 목록에서 포트를 수정합니다.
- 데이터베이스 이벤트 제한 구성, 1351 페이지에 설명된 대로 데이터베이스 이벤트 제한에 대해 알아보고 편집하는 것이 좋습니다.
- 디스플레이 언어를 변경하려는 경우, 웹 인터페이스의 언어 설정, 1375 페이지에 설명된 대로 언어 설정을 편집합니다.
- 해당 조직에서 프록시 서버를 사용하여 네트워크 액세스를 제한하고, FMC 관리 인터페이스 수정, 1358 페이지에 설명된 대로 프록시 설정을 편집합니다.

단계 **8** 네트워크 검색 정책 설정, 2539 페이지에 설명된 대로 네트워크 검색 정책을 맞춤화합니다. 기본적으로 네트워크 검색 정책은 네트워크의 모든 트래픽을 분석합니다. 대부분의 경우 Cisco는 RFC 1918에서 주소 검색을 제한합니다.

단계 **9** 다음과 같이 다른 일반 설정을 맞춤화하는 것이 좋습니다.

- 메시지 센터 팝업 표시를 원하지 않는 경우, 알림 동작 설정, 446 페이지에 설명된 대로 알림을 비활성화합니다.
- 시스템 변수에 대한 기본값을 맞춤화하려는 경우, 변수 집합, 580 페이지에 설명된 대로 변수 사용에 대해 알아봅니다.
- 추가 로컬 인증 사용자 계정를 생성하고 FMC에 액세스하려는 경우, 사용자 어카운트 만들기내부 사용자 추가, 55 페이지의 내용을 참조하십시오.
- LDAP 또는 RADIUS 외부 인증을 사용하여 FMC에 대한 액세스를 허용하려는 경우, 외부 인증외부 인증 구성, 57 페이지의 내용을 참조하십시오.

단계 **10** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

다음에 수행할 작업

- Firepower 기능, 8 페이지 및 이 가이드의 나머지 부분에 설명된 다른 기능을 검토하고 구성하는 것이 좋습니다.

Firepower 디바이스

일반적인 구축에서는 여러 트래픽 처리 디바이스가 같은 Firepower Management Center에 보고하는데, 이곳에서는 운영, 관리, 분석, 보고 작업을 수행할 수 있습니다.

클래식 디바이스

클래식 디바이스는 차세대 IPS (NGIPS) 소프트웨어를 실행 합니다. 그 기능은 다음과 같습니다.

- Firepower 7000 시리즈와 Firepower 8000 시리즈는 물리적 디바이스입니다.
- VMware에서 호스팅되는 NGIPSv입니다.
- FirePOWER 서비스를 이용하는 ASA로, 일부 ASA 5500-X 시리즈 디바이스에서 사용할 수 있습니다(ISA 3000 포함). ASA는 우선 시스템 정책을 제공하고, 그런 다음 검색 및 액세스 제어를 위해 트래픽을 ASA FirePOWER 모듈로 전달합니다.

  ASA CLI나 ASDM을 사용하여 ASA FirePOWER 디바이스에서 ASA 기반 기능을 구성해야 합니다. 디바이스 고가용성, 스위칭, 라우팅, VPN, NAT 등이 이러한 기능에 속합니다. FMC를 사용하여 ASA FirePOWER 인터페이스를 구성할 수는 없으며, ASA FirePOWER를 SPAN 포트 모드로 구축한다면 FMC GUI에 ASA 인터페이스가 표시되지 않습니다. 또한 FMC를 사용하여 ASA FirePOWER 프로세스를 종료하거나, 다시 시작하거나, 관리할 수도 없습니다.

Firepower Threat Defense 디바이스

FTD(Firepower Threat Defense) 디바이스는 NGIPS 기능을 제공하는 NGFW(차세대 방화벽)입니다. NGFW 및 플랫폼 기능에는 사이트 대 사이트 및 원격 액세스 VPN, 강력한 라우팅, NAT, 클러스터링 및 기타 애플리케이션 검사 및 액세스 제어 최적화가 있습니다.

FTD는 다양한 물리적 및 가상 플랫폼에서 사용할 수 있습니다.

호환성

특정 디바이스 모델, 가상 호스팅 환경, 운영 체제 등과 호환되는 소프트웨어를 포함한 관리자-디바이스 호환성에 대한 자세한 내용은 Cisco Firepower 릴리스 노트 및 Cisco FirePOWER 호환성 가이드를 참조하십시오.

Firepower 7000/8000 시리즈 디바이스 판매 종료

7000/8000 시리즈 디바이스에서는 Firepower 버전 6.5 이상으로 업그레이드하거나 버전 6.5 이상을 새로 설치할 수 없습니다. 본 가이드 및 관련 온라인 도움말은 이러한 디바이스를 구성하거나 관리하는 방법은 설명하지 않습니다.

지원되는 이전 Firepower 버전을 실행하는 7000/8000 시리즈 디바이스를 관리한다면, 다음 리소스를 사용하십시오.

- FMC-디바이스 호환성에 관한 자세한 내용은 Cisco Firepower 호환성 가이드의 *Firepower Management Centers* 관련 정보 섹션을 참조하십시오.
- 디바이스 구성 및 관리에 대해서는 디바이스 버전에 맞는 Firepower Management Center 구성 가이드를 참조하십시오.

Firepower 기능

이러한 테이블에는 몇 가지 흔히 사용되는 Firepower 기능 목록이 표시됩니다.

어플라이언스 및 시스템 관리 기능

생소한 문서를 찾으려면 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html의 내용을 참조하십시오.

기능	구성...	설명...
Firepower 어플라이언스 로그인 사용자 어카운트 관리	Firepower 인증	Firepower System 사용자 인증 FMC의 사용자 계정, 49 페이지 및 디바이스 사용자 계정, 135 페이지
시스템 하드웨어 및 소프트웨어의 상태 모니터링	상태 모니터링 정책	상태 모니터링 정보, 387 페이지
어플라이언스 데이터 백업	백업 및 복원	백업 및 복원, 203 페이지
새 Firepower 버전으로 업그레이드	시스템 업데이트	Cisco Firepower Management Center 업그레이드 설명서 Firepower 릴리스 노트
물리적 어플라이언스 기준	공장 기본값으로 복원(리이미징)	Cisco Firepower Management Center 업그레이드 설명서, 신규 설치 수행에 관한 지침 링크 목록.
어플라이언스에서 VDB, 침입 규칙 업데이트 또는 GeoDB 업데이트	VDB(취약성 데이터베이스) 업데이트, 침입 규칙 업데이트, GeoDB(지리위치 데이터베이스) 업데이트	시스템 업데이트, 179 페이지
라이선스 제어 기능을 활용하기 위해 라이선스를 적용합니다.	기본 또는 스마트 라이선싱	Firepower 라이선스 정보, 157 페이지

기능	구성...	설명...
어플라이언스 운영의 연속성을 보장	매니지드 디바이스 고가용성 및/또는 Firepower Management Center 고가용성	7000 및 8000 Series 디바이스 고가용성 정보 Firepower Threat Defense 고가용성 정보, 889 페이지 Firepower Management Center 고가용성 정보, 275 페이지
여러 8000 Series디바이스의 처리 리소스를 결합	디바이스 스태킹	디바이스 스택 관련 정보
디바이스를 구성하고 두 개 이상의 인터페이스 사이에 트래픽을 라우팅합니다.	라우팅	가상 라우터 Firepower Threat Defense 라우팅 개요, 977 페이지
두 개 이상의 네트워크 사이에 패킷 스위칭을 구성합니다.	디바이스 전환	가상 스위치 브리지 그룹 인터페이스 구성, 821 페이지
인터넷 연결을 위해 비공개 주소를 공용 주소로 변환합니다.	NAT(네트워크 주소 변환)	NAT 정책 구성 Firepower Threat Defense용 NAT(네트워크 주소 변환), 1487 페이지
매니지드 Firepower Threat Defense 또는 7000/8000 시리즈 디바이스 간에 보안 터널을 설정합니다.	Site-to-Site(사이트 대 사이트) 가상사설망(VPN)	Firepower Threat Defense VPN 개요, 1121 페이지
원격 사용자와 매니지드 Firepower Threat Defense 디바이스 간에 보안 터널을 설정합니다.	원격 액세스 VPN	Firepower Threat Defense VPN 개요, 1121 페이지
매니지드 디바이스, 구성 및 이벤트에 대한 사용자 액세스 구분	도메인을 사용하는 다중 테넌시	도메인을 사용하는 다중 테넌시 소개, 481 페이지
REST API 클라이언트를 사용하여 어플라이언스 구성 보기 및 관리	REST API 및 REST API Explorer	REST API 환경 설정 *Firepower REST API* 빠른 시작 가이드
문제 해결	해당 없음	시스템 문제 해결, 461 페이지

플랫폼별 고가용성 및 확장성 기능

고가용성 구성(페일오버라고도 함)은 운영 연속성을 보장합니다. 클러스터링 구성은 단일 논리 디바이스로 여러 디바이스를 함께 그룹화하여, 처리량 증가 및 이중화를 달성합니다.

플랫폼	고가용성	클러스터링
Firepower Management Center	예	—
Firepower Management Center Virtual	예(자세한 내용은 가상 플랫폼 요건, 281 페이지을 참조하십시오.)	—
Firepower Threat Defense: • Firepower 1000 Series • Firepower 2100 Series • ASA 5500-X Series • ISA 3000	예	—
Firepower Threat Defense: • Firepower 4100/9300 섀시	예	예
Firepower Threat Defense Virtual: • VMWare • KVM	예	—
Firepower Threat Defense Virtual(퍼블릭 클라우드): • AWS • Azure	—	—
NGIPSv	—	—
ASA FirePOWER	이러한 구축에서 ASA 디바이스는 우선 시스템 정책을 제공하고 그런 다음 검색 및 액세스 제어를 위해 트래픽을 ASA FirePOWER 모듈로 전달합니다. 고가용성 및 확장성 구성에 대한 자세한 내용은 ASA 설명서를 참조하십시오.	

고가용성 구성은 운영 연속성을 보장합니다. 스태킹 구성은 단일 논리 디바이스로 여러 디바이스를 함께 그룹화하고, 처리량 증가 및 이중화를 달성합니다.

플랫폼	고가용성	스태킹
Firepower Management Center	예 MC750 제외	—
Firepower Management Center Virtual	—	—
Firepower NGIPS: • Firepower 7010, 7020, 7030, 7050 • Firepower 7110, 7115, 7120, 7125 • Firepower 8120, 8130 • AMP 7150, 8050, 8150	예	—
Firepower NGIPS: • Firepower 8140 • Firepower 8250, 8260, 8270, 8290 • Firepower 8350, 8360, 8370, 8390 • AMP 8350	예	—
Firepower NGIPS: • ASA FirePOWER • NGIPSv	—	—

관련 항목

7000 및 8000 Series 디바이스 고가용성 정보
Firepower Threat Defense 고가용성 정보, 889 페이지
Firepower Management Center 고가용성 정보, 275 페이지

잠재적 위협 탐지, 방지 및 처리 기능

생소한 문서를 찾으려면 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html의 내용을 참조하십시오.

기능	구성...	설명...
네트워크 트래픽 검사, 로그 및 작업 수행	일부 다른 정책보다 상위에 있는 액세스 제어 정책	액세스 제어 소개, 1609 페이지
IP 주소, URL 및/또는 도메인 이름 연결 차단 또는 모니터링	액세스 제어 정책 내 보안 인텔리전스	보안 인텔리전스 정보, 1695 페이지

기능	구성...	설명...
네트워크의 사용자가 액세스할 수 있는 웹 사이트를 제어	정책 규칙 내 URL 필터링	URL 필터링, 1665 페이지
네트워크의 악성 트래픽 및 침입을 모니터링	침입 정책	침입 정책 기본 사항, 1995 페이지
검사 없이 암호화된 트래픽 차단 암호화 또는 해독된 트래픽 검사	SSL 정책	SSL 정책 개요, 1793 페이지
캡슐화된 트래픽 심층 검사 맞춤화 및 빠른 경로 지정으로 성능 향상	사전 필터 정책	사전 필터링 정보, 1723 페이지
액세스 제어에서 허용되거나 신뢰하는 네트워크 트래픽 속도 제한	QoS(Quality of Service) 정책	QoS 정책 정보, 879 페이지
네트워크에서 파일(악성코드 포함) 허용 또는 차단	파일/악성코드 정책	파일 정책 및 악성코드 보호, 1861 페이지
패시브 또는 액티브 사용자 인증을 구성하여 사용자 인식 및 사용자 제어 수행	사용자 인식, 사용자 ID, ID 정책	영역 및 ID 정책 정보 ID 정책 정보, 2529 페이지
네트워크의 트래픽에서 호스트, 애플리케이션 및 사용자 데이터를 수집하고 사용자 제어 수행	네트워크 검색 정책	개요: 네트워크 검색 정책, 2537 페이지
Firepower 시스템 외부의 툴을 사용하여 네트워크 트래픽 및 잠재적인 위협에 대한 데이터를 수집하고 분석합니다.	외부 툴과 통합	외부 툴을 사용하여 이벤트 분석, 2749 페이지
애플리케이션 탐지 및 제어 수행	애플리케이션 탐지기	개요: 애플리케이션 탐지, 2439 페이지
문제 해결	해당 없음	시스템 문제 해결, 461 페이지

외부 툴과 통합

생소한 문서를 찾으려면 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html의 내용을 참조하십시오.

기능	구성...	설명...
네트워크의 조건이 관련 정책을 위반할 때 자동으로 치료를 시작	치료	교정 소개, 2637 페이지 *Firepower System Remediation API* 설명서

기능	구성...	설명...
맞춤 개발 된 클라이언트 애플리케이션으로 Firepower Management Center 스트림 이벤트 데이터	eStreamer 통합	eStreamer 서버 스트리밍, 2769 페이지 *Firepower System eStreamer* 통합 가이드
서드파티 클라이언트를 사용하여 Firepower Management Center에서 데이터베이스 테이블 쿼리	외부 데이터베이스 액세스	외부 데이터베이스 액세스 설정, 1349 페이지 *Firepower System* 데이터베이스 액세스 설명서
서드파티 소스에서 데이터를 가져오는 방법으로 검색 데이터를 보완	호스트 입력	호스트 입력 데이터, 2406 페이지 *Firepower System Host Input API* 설명서
외부 이벤트 데이터 스토리지 도구 및 기타 데이터 리소스를 사용하여 이벤트 조사	외부 이벤트 분석 툴과 통합	외부 툴을 사용하여 이벤트 분석, 2749 페이지
문제 해결	해당 없음	시스템 문제 해결, 461 페이지

FMC 검색

웹 인터페이스 메뉴 옵션 검색

웹 인터페이스의 최상위 메뉴에서 페이지의 위치를 찾으려면 검색합니다. 예를 들어 서비스 품질 설정을 보거나 구성하려면 **QoS**를 검색합니다.

시작하기 전에

이 기능은 클래식 테마에서 사용할 수 없습니다. 테마를 변경하려면 웹 인터페이스 모양 변경, 40 페이지의 내용을 참조하십시오.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스 상단의 메뉴 모음에서 검색( )을 클릭합니다.

단계 **2** 원하는 메뉴 옵션 이름의 문자를 하나 이상 입력합니다.

단계 **3** 페이지로 이동하려면 제안 목록에서 항목을 클릭합니다.

도메인 전환 Firepower Management Center

다중 도메인 구축에서 사용자 역할 권한은 사용자가 액세스할 수 있는 도메인과 그러한 각 도메인 내에서 사용자가 갖는 권한을 결정합니다. 단일 사용자 어카운트를 여러 도메인에 연결하고 각 도메인에서 해당 사용자에 대해 서로 다른 권한을 할당할 수 있습니다. 예를 들어 전역 도메인에서 사용자에게 읽기 전용 권한을 할당할 수 있지만 하위 도메인에서는 관리자 권한을 할당할 수 있습니다.

여러 도메인과 연결된 사용자는 동일한 웹 인터페이스 세션 내에서 도메인 간에 전환할 수 있습니다.

툴바에서 사용자 이름 하단에 시스템이 사용 가능한 도메인 트리를 표시합니다. 트리:

- 상위 도메인이 표시되지만, 사용자 어카운트에 할당된 권한에 따라 이러한 도메인에 대한 액세스를 비활성화할 수 있습니다.
- 동위 및 하위 도메인을 포함하여 사용자 어카운트가 액세스할 수 없는 다른 모든 도메인을 숨깁니다.

특정 도메인으로 전환하는 경우, 시스템에 다음과 같이 표시됩니다.

- 해당 도메인에만 관련된 데이터.
- 해당 도메인에 대해 사용자에게 할당된 사용자 역할에 따라 결정되는 메뉴 옵션.

프로시저

사용자 이름 하단에 있는 드롭다운 목록에서 액세스하려는 도메인을 선택합니다.

상황 메뉴

Firepower System 웹 인터페이스의 특정 페이지는 Firepower System의 다른 기능에 액세스하기 위한 바로가기로 사용할 수 있는 오른쪽 클릭(가장 일반적) 또는 왼쪽 클릭 상황 메뉴를 지원합니다. 상황 메뉴의 내용은 액세스하는 위치(페이지 및 특정 데이터)에 따라 달라집니다.

예를 들면 다음과 같습니다.

- IP 주소 핫스팟은 사용 가능한 whois 및 호스트 프로파일 정보를 포함하여, 해당 주소와 관련된 호스트에 대한 정보를 제공합니다.
- SHA-256 해시 값 핫스팟을 사용하면 파일의 SHA-256 해시 값을 정상 목록 또는 맞춤형 탐지 목록에 추가하거나, 복사할 전체 해시 값을 볼 수 있습니다.

Firepower System 상황 메뉴를 지원하지 않는 페이지 또는 위치에는 브라우저의 일반적인 상황 메뉴가 표시됩니다.

정책 편집기

수많은 정책 편집기에는 각 규칙에 대한 핫스팟이 포함되어 있습니다. 규칙 잘라내기, 복사 및 붙여넣기, 규칙 상태 설정, 규칙 수정 등 새 규칙 및 카테고리를 삽입할 수 있습니다.

침입 규칙 편집기

침입 규칙 편집기에는 각 침입 규칙에 대한 핫스팟이 포함되어 있습니다. 규칙을 수정하고, 규칙 상태를 설정하고, 임계값 및 억제 옵션을 구성하고, 규칙 문서를 볼 수 있습니다. 경우에 따라 콘텍스트 메뉴의 **Rule documentation(**규칙 문서**)**을 클릭한 후 문서 팝업창에 있는 **Rule Documentation(**규칙 문서**)**을 클릭하고 더 구체적인 규칙 세부 정보를 확인할 수 있습니다.

이벤트 뷰어

Event(이벤트) 페이지(Analysis(분석) 메뉴 하단에서 사용 가능한 드릴다운 페이지 및 테이블 보기)에는 각 이벤트, IP 주소, URL, DNS 쿼리, 특정 파일의 SHA-256 해시 값에 대한 핫스팟이 포함되어 있습니다. 대부분의 이벤트 유형을 보는 동안 다음을 수행할 수 있습니다.

- Context Explorer에서 관련 정보 보기
- 새 창에서 이벤트 정보로 드릴다운
- 이벤트 필드에 포함된 텍스트가 너무 길어 이벤트 보기에 모두 표시할 수 없는 경우(예: 파일의 SHA-256 해시 값, 취약성 설명, URL) 전체 텍스트 보기
- 상황별 크로스 실행 기능을 사용하여, 외부 소스에서 Firepower로 제공되는 요소에 대한 세부 정보를 표시하는 웹 브라우저 창을 엽니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지를 참고하십시오.

연결 이벤트를 보는 동안 항목을 기본 보안 인텔리전스 차단 목록 및 차단 안 함 리스트에 추가할 수 있습니다.

- IP 주소 핫스팟의 IP 주소
- URL 핫스팟의 URL 또는 도메인 이름
- DNS 쿼리 핫스팟의 DNS 쿼리

캡처된 파일, 파일 이벤트, 악성코드 이벤트를 보는 동안 다음을 수행할 수 있습니다.

- 정상 목록 또는 맞춤형 탐지 목록에 파일을 추가하거나 이 목록에서 파일 제거
- 파일의 복사본 다운로드
- 아카이브 파일 내의 중첩된 파일 보기
- 중첩된 파일의 상위 아카이브 파일 다운로드
- 파일 구성 보기
- 로컬 악성코드 및 동적 분석을 위해 파일 제출

침입 이벤트를 보는 동안 침입 규칙 편집기 또는 침입 정책에서와 유사한 작업을 수행할 수 있습니다.

- 트리거 규칙 수정
- 규칙 상태 설정(규칙 비활성화 포함)
- 임계값 및 억제 옵션 구성
- 규칙 문서 보기 경우에 따라 콘텍스트 메뉴의 **Rule documentation(**규칙 문서**)**을 클릭한 후 문서 팝업창에 있는 **Rule Documentation(**규칙 문서**)**을 클릭하고 더 구체적인 규칙 세부 정보를 확인할 수 있습니다.

침입 이벤트 패킷 보기

침입 이벤트 패킷 보기에는 IP 주소 핫스팟이 포함되어 있습니다. 패킷 보기는 왼쪽 클릭 상황 메뉴를 사용합니다.

대시보드

많은 대시보드 위젯에 Context Explorer에서 관련 정보를 볼 수 있는 핫스팟이 포함되어 있습니다. 대시보드 위젯에는 또한 IP 주소 및 SHA-256 해시 값 핫스팟도 포함할 수 있습니다.

Context Explorer

Context Explorer에는 차트, 테이블 및 그래프에 핫스팟이 포함되어 있습니다. Context Explorer에서 허용하는 것보다 더 자세히 그래프 또는 목록의 데이터를 검사하려면 관련 데이터의 테이블 보기로 드릴다운할 수 있습니다. 관련 호스트, 사용자, 애플리케이션, 파일 및 침입 규칙 정보도 볼 수 있습니다.

Context Explorer는 왼쪽 클릭 상황 메뉴를 사용하며, 여기에는 Context Explorer의 고유한 필터링 및 기타 옵션도 포함됩니다.

관련 항목

보안 인텔리전스 목록 및 피드, 597 페이지

Firepower 온라인 도움말, 방법 및 문서

웹 인터페이스 온라인 도움말 연결 방법:

- 각 페이지에서 상황별 도움말 링크 클릭
- 온라인 > 도움말 선택

How To는 Firepower Management Center에서의 작업을 통해 이동하는 워크스루를 제공하는 위젯입니다. 이 워크스루를 통해 사용자가 탐색해야 할 수도 있는 다양한 UI 화면과 상관없이 각 단계를 차례로 수행하여 작업을 완료하는 데 필요한 단계를 수행할 수 있습니다. How To 위젯은 기본적으로 활성화됩니다. 이 위젯을 비활성화하려면 **User Preferences(**사용자 환경 설정**)**를 사용자 이름 하단에 있는 드롭다운 목록에서 선택하고 **How-To Settings(How-To** 설정**)**에서 **Enable How-Tos(How-To** 활성화**)** 확인란의 선택을 취소합니다.

참고 이 워크스루는 일반적으로 모든 UI 페이지에 사용할 수 있으며 사용자 역할에 따라 제한되지 않습니다. 그러나 사용자의 권한에 따라 일부 메뉴 항목이 Firepower Management Center 인터페이스에 나타나지 않습니다. 따라서 워크스루는 그러한 페이지에서는 실행되지 않습니다.

다음 워크스루는 Firepower Management Center에서 사용할 수 있습니다.

- Register FMC with Cisco Smart Account(Cisco Smart Account으로 FMC 등록): 이 워크스루를 통해 Cisco Smart Account으로 Firepower Management Center를 등록할 수 있습니다.
- Set up a Device and add it to FMC(디바이스 설정 및 FMC에 추가): 이 워크스루를 통해 디바이스를 설정하고 Firepower Management Center에 디바이스를 추가할 수 있습니다.
- Configure Date and Time(날짜 및 시간 구성): 이 워크스루를 통해 플랫폼 설정 정책을 사용하여 Firepower Threat Defense 디바이스의 날짜 및 시간을 구성할 수 있습니다.
- Configure Interface Settings(인터페이스 설정 구성): 이 워크스루를 통해 Firepower Threat Defense 디바이스에서 인터페이스를 구성할 수 있습니다.
- Create an Access Control Policy(액세스 제어 정책 생성): 액세스 제어 정책은 하향식으로 평가되는 순서가 정해진 규칙 집합으로 구성됩니다. 이 워크스루를 통해 액세스 제어 정책을 생성할 수 있습니다.
- Add an Access Control Rule(액세스 제어 규칙 추가) - A Feature Walkthrough(기능 워크스루): 이 워크스루는 액세스 제어 규칙의 구성 요소와 Firepower Management Center에서 해당 규칙을 사용하는 방법을 설명합니다.
- Configure Routing Settings(라우팅 설정 구성): 다양한 라우팅 프로토콜이 Firepower Threat Defense에서 지원됩니다. 고정 경로는 특정 목적지 네트워크로 향하는 트래픽을 어디로 보낼지 정의합니다. 이 워크스루를 통해 디바이스에 대한 정적 라우팅을 구성할 수 있습니다.
- (Create a NAT Policy) - (A Feature Walkthrough): 이 워크스루를 통해 NAT 정책을 생성하고 NAT 규칙의 다양한 기능을 연습할 수 있습니다.

문서 로드맵을 사용하여 Firepower 시스템에서 관련 추가 문서를 찾을 수 있습니다: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

FMC 구축에 대한 최상위 문서 목록 페이지

Firepower Management Center 구축, 버전 6.0 +을 구성하는 경우 다음 문서가 도움이 될 수 있습니다.

참고 일부 연결된 문서는 Firepower Management Center 구축에 적용할 수 없습니다. 예를 들어, 일부 링크는 Firepower와 무관합니다. 혼동을 피하기 위해 문서 제목에 주의하십시오. 또한 일부 문서는 여러 제품을 다루며 여러 제품 페이지에 표시될 수 있습니다.

Firepower Management Center

- Firepower Management Center 하드웨어 어플라이언스:

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Firepower Management Center 가상 어플라이언스:
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

NGIPS(Next Generation Intrusion Prevention System) 디바이스라고도 함.

- ASA with FirePOWER Services:
  - ASA 5500-X with FirePOWER Services:
    - https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html
    - https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html
  - ISA 3000 with FirePOWER Services:

    https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

- Firepower 8000 시리즈:

  https://www.cisco.com/c/en/us/support/security/firepower-8000-series-appliances/tsd-products-support-series-home.html

- Firepower 7000 시리즈:

  https://www.cisco.com/c/en/us/support/security/firepower-7000-series-appliances/tsd-products-support-series-home.html

- AMP for Networks:

  https://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-series-home.html

- NGIPSv(가상 디바이스):

  https://www.cisco.com/c/en/us/support/security/ngips-virtual-appliance/tsd-products-support-series-home.html

문서 내 라이선스 설명

섹션 앞부분에 있는 License(라이선스) 설명문에는 섹션에 설명된 기능을 활성화하기 위해 Firepower System에서 매니지드 디바이스에 할당해야 하는 Classic(클래식) 또는 Smart(스마트) 라이선스에 대해 나와 있습니다.

라이선스 기능은 추가된 경우가 많기 때문에 라이선스 설명문에는 각 기능에 대해 가장 필요한 라이선스만 제시됩니다.

License(라이선스) 설명문에 있는 "or(또는)" 문장은 섹션에 설명된 기능을 활성화하기 위해 매니지드 디바이스에 특정 라이스를 할당해야 하지만 라이선스를 추가하면 기능을 추가할 수 있다는 의미를 나타냅니다. 예를 들어, 파일 정책 내에서 일부 파일 규칙 작업에는 디바이스에 Protection(보호) 라이선스가 필요하지만 다른 작업에는 Malware(악성코드) 라이선스가 필요합니다.

라이선스에 대한 자세한 내용은 Firepower 라이선스 정보, 157 페이지를 참조하십시오.

관련 항목

Firepower 라이선스 정보, 157 페이지

문서 내 지원 디바이스 설명

특정 장이나 주제 앞부분에 있는 Supported Devices(지원 디바이스) 설명문은 지정된 디바이스 시리즈, 제품군 또는 모델에서만 지원되는 기능을 설명합니다. 예를 들어 많은 기능은 Firepower Threat Defense 디바이스에서만 지원됩니다.

이 릴리스에서 지원되는 플랫폼에 대한 자세한 내용은 릴리스 노트를 참조하십시오.

문서 내 액세스 설명

이 문서 각 절차의 앞부분에 있는 Access(액세스) 설명문은 절차 수행에 필요한 사전 정의된 사용자 역할을 설명합니다. 목록에 표시된 역할이 해당 절차를 수행할 수 있습니다.

맞춤형 역할이 있는 사용자는 사전 정의 역할이 있는 사용자와 다른 권한 집합을 가질 수 있습니다. 특정 절차에 대한 액세스 요구 사항을 나타내는 데 사전 정의 역할이 사용된 경우, 권한이 유사한 맞춤형 역할도 액세스 권한을 갖게 됩니다. 맞춤형 역할이 있는 일부 사용자는 약간 다른 메뉴 경로를 사용하여 구성 페이지에 도달할 수 있습니다. 예를 들어 침입 정책 권한만 있는 맞춤형 역할을 가진 사용자는 액세스 제어 정책을 통한 표준 경로가 아니라 침입 정책을 통해 네트워크 분석 정책에 액세스할 수 있습니다.

사용자 역할에 대한 자세한 내용은 사전 정의된 사용자 역할사용자 역할, 50 페이지과 맞춤형 사용자 역할웹 인터페이스의 사용자 역할 맞춤화, 127 페이지를 참조하십시오.

Firepower System IP 주소 규칙

IPv4 CIDR(Classless Inter-Domain Routing) 표기법 및 유사한 IPv6 접두사 길이 표기법을 사용하여 Firepower System의 여러 위치에서 주소 블록을 정의할 수 있습니다.

CIDR 또는 접두사 길이 표기법을 사용하여 IP 주소 블록을 지정하려는 경우, Firepower System은 마스크 또는 접두사 길이에 의해 지정된 네트워크 IP 주소의 일부만 사용합니다. 예를 들어, 10.1.2.3/8을 입력한 경우 Firepower System은 10.0.0.0/8을 사용합니다.

즉 Cisco에서는 CIDR 또는 접두사 길이 표기법을 사용하는 경우 비트 경계에 있는 네트워크 IP 주소를 사용하는 표준 방식을 권장하지만 Firepower System은 이를 요구하지 않습니다.

추가 리소스

Firewalls Community(방화벽 커뮤니티)는 Cisco의 광범위한 문서를 보완하는 참조 자료의 완전한 저장소입니다. 여기에는 하드웨어 3D 모델, 하드웨어 구성 선택기, 제품 참고자료, 구성 예시, 문제 해결 기술 노트, 교육용 동영상, 실습 및 Cisco Live 세션, 소셜 미디어 채널, Cisco Blogs 및 Technical Publications 팀에서 게시한 모든 문서에 대한 링크가 포함됩니다.

조정자를 비롯하여 커뮤니티 사이트 또는 동영상 공유 사이트에 게시하는 개인 중 일부는 Cisco Systems의 직원입니다. 그러한 사이트에 게시한 의견 및 해당 코멘트에 대한 의견은 원래 저자의 개인적 의견이며 Cisco의 의견이 아닙니다. 내용은 정보 제공 목적으로만 제공되며 Cisco 또는 타사의 추천 또는 의사표현으로 간주되어서는 안 됩니다.

참고 Firewalls Community(방화벽 커뮤니티)에 있는 동영상, 기술 노트 및 참조 자료는 Firepower Management Center의 이전 버전을 가리킵니다. 동영상이나 기술 노트에 참조된 Firepower Management Center 버전이 유저 인터페이스에서와 차이가 있어 절차가 동일하지 않을 수 있습니다.

Firepower 시작 기록

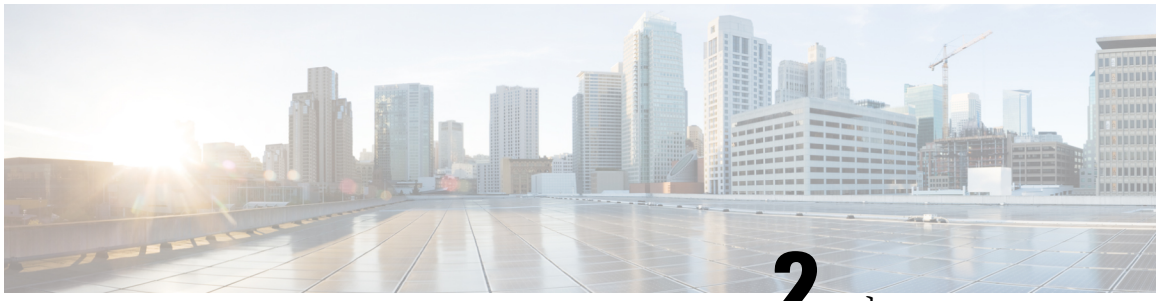
기능	버전	세부 사항
웹 인터페이스 페이지 검색	6.7	보거나 변경할 페이지를 검색할 수 있습니다. 예를 들어 **QoS**를 검색하여 QoS(Quality of Service) 설정을 구성할 페이지를 찾을 수 있습니다. 신규/수정된 화면: FMC 웹 인터페이스 창 상단에 새 돋보기 버튼이 있습니다. 플랫폼: FMC(클래식 테마를 사용할 때는 사용할 수 없음)

기능	버전	세부 사항
초기 구성 마법사	6.5	신규 또는 출고 시 설정으로 복원된 FMC에 처음으로 로그인하면, 이제 버전 6.5를 지원하는 FMC 모델에 대한 *Cisco Firepower Management Center* 시작 가이드에 문서화된 초기 구성 마법사가 관리자 사용자에게 표시됩니다. 마법사는 다음 항목을 구성합니다. • 두 관리자 계정(웹 인터페이스 액세스용 하나와 CLI 액세스용 하나)의 비밀번호는 강력한 비밀번호 요구 사항을 준수하는 같은 값으로 설정됩니다. • FMC이(가) 자체 관리 인터페이스(eth0)를 통한 네트워크 통신에 사용하는 네트워크 설정을 구성합니다. • GeoDB와 FMC 및 관련 매지니드 디바이스용 시스템 소프트웨어 주간 자동 업데이트를 예약합니다. • FMC에 대한 주간 로컬 저장 구성 전용 자동 백업을 예약합니다. 신규/수정된 화면: 관리자 사용자의 최초 로그인 지원되는 플랫폼: FMC

부

사용자 어카운트

- Firepower System에 로그인, 25 페이지
- 사용자 환경설정 지정, 39 페이지
- FMC의 사용자 계정, 49 페이지
- 디바이스 사용자 계정, 135 페이지



2 장

Firepower System에 로그인

다음 주제에서는 Firepower System에 로그인 하는 방법을 설명합니다.

- Firepower System 사용자 어카운트, 25 페이지
- Firepower System 유저 인터페이스, 27 페이지
- Firepower Management Center 웹 인터페이스 로그인, 30 페이지
- SSO를 사용한 FMC 웹 인터페이스 로그인, 31 페이지
- 7000 또는 8000 Series 디바이스의 웹 인터페이스에 로그인, 33 페이지
- CAC 크리덴셜로 Firepower Management Center에 로그인, 33 페이지
- CAC 크리덴셜을 사용하여 7000 또는 8000 Series 디바이스에 로그인, 34 페이지
- FMC Command Line Interface에 로그인, 35 페이지
- 7000/8000 시리즈, ASA FirePOWER, NGIPSv 디바이스에서 CLI에 로그인, 36 페이지
- 마지막 로그인 보기, 37 페이지
- Firepower System 웹 인터페이스에서 로그아웃, 37 페이지
- Firepower 시스템 로그인 기록, 38 페이지

Firepower System 사용자 어카운트

사용자 이름과 비밀번호를 제공해야 웹 인터페이스 또는 FMC 및 매니지드 디바이스의 CLI에 액세스할 수 있습니다. 매니지드 디바이스에서, 구성 레벨 액세스 권한이 있는 CLI 사용자는 `expert` 명령을 이용해 Linux 셸에 액세스할 수 있습니다. FMC에서는 모든 CLI 사용자가 `expert` 명령을 사용할 수 있습니다. FTD 및 FMC를 외부 인증을 사용하도록 구성하면 사용자 자격 증명을 외부 LDAP 또는 RADIUS 서버에 저장합니다. CLI 액세스 권한을 취소하거나 외부 사용자에게 제공할 수 있습니다.FMC는 인증 및 권한 부여를 위해 SAML(Security Assertion Markup Language) 2.0 개방형 표준을 준수하는 SSO 제공자를 사용하여 SSO(Single Sign-On)를 지원하도록 구성할 수 있습니다.

FMC CLI는 모든 명령에 액세스할 수 있는 단일 관리자 사용자를 제공합니다. FMC 웹 인터페이스 사용자가 액세스할 수 있는 기능은 관리자가 사용자 계정에 부여하는 권한에 의해 제어됩니다. 매니지드 디바이스의 경우 사용자가 CLI 및 웹 인터페이스에서 액세스할 수 있는 기능은 사용자 계정에 부여된 권한과 관리자에 의해 제어됩니다.

참고 시스템은 사용자 어카운트를 기반으로 사용자 활동을 감사합니다. 따라서 사용자들이 올바른 어카운트로 시스템에 로그인하도록 해야 합니다.

주의 모든 FMC CLI 사용자 및 (매니지드 디바이스의 경우) 구성 레벨 CLI 액세스 권한이 있는 사용자는 Linux 셸에서 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- 외부 인증을 설정하는 경우 CLI 액세스 권한이 있는 사용자 목록을 적절하게 제한해야 합니다.
- 매니지드 디바이스에 CLI 액세스 권한을 부여할 때는, 구성 레벨 CLI 액세스로 내부 사용자 목록을 제한합니다.
- Linux 셸 사용자는 설정해선 안 됩니다. 사전 정의된 관리자 사용자 및 CLI에서 관리자 사용자가 생성한 사용자만 사용해야 합니다.

주의 Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다.

다양한 어플라이언스가 각기 다른 기능으로 서로 다른 유형의 사용자 어카운트를 지원합니다.

Firepower Management Centers

Firepower Management Center다음 같은 사용자 어카운트를 지원합니다.

- 웹 인터페이스 액세스를 위한 사전 정의된 관리자 어카운트. 관리자 역할이 주어지며 웹 인터페이스를 통해 관리할 수 있습니다.
- 맞춤형 사용자 계정으로, 웹 인터페이스 액세스를 제공하며 관리자 사용자와 관리자 권한이 있는 사용자가 생성하고 관리할 수 있습니다.
- CLI 액세스를 위한 사전 정의된 관리자 계정입니다. 이 계정으로 로그인하는 사용자는 `expert` 명령을 사용해 Linux 셸 액세스 권한을 얻을 수 있습니다.

  초기 구성에서 CLI 관리자 계정과 웹 인터페이스 관리자 계정의 비밀번호가 동기화되지만, 원한다면 이후 두 관리자 계정에 별도의 비밀번호를 설정할 수 있습니다.

주의 시스템 보안을 위해 Cisco에서는 Linux 셸 사용자를 어플라이언스에서 추가로 설정하지 않도록 권장합니다.

7000 및 8000 Series 디바이스

7000 및 8000 Series 디바이스는 다음과 같은 사용자 어카운트 유형을 지원합니다.

- 사전 정의된 관리자 어카운트. 모든 형태의 디바이스 액세스에 사용될 수 있습니다.
- 맞춤형 사용자 어카운트. 관리자 사용자 및 관리자 역할이 주어진 사용자가 생성하고 관리할 수 있습니다.

7000 및 8000 Series는 사용자에 대한 외부 인증을 지원합니다.

NGIPSv 디바이스

NGIPSv 디바이스는 다음과 같은 사용자 어카운트 유형을 지원합니다.

- 사전 정의된 관리자 어카운트. 모든 형태의 디바이스 액세스에 사용될 수 있습니다.
- 맞춤형 사용자 어카운트. 관리자 사용자 및 Config(구성) 액세스 권한이 있는 사용자가 생성하고 관리할 수 있습니다.

NGIPSv는 사용자에 대한 외부 인증을 지원하지 않습니다.

ASA FirePOWER 디바이스

ASA FirePOWER 모듈은 다음 사용자 어카운트 유형을 지원합니다.

- 사전 정의된 관리자 어카운트.
- 맞춤형 사용자 어카운트. 관리자 사용자 및 Config(구성) 액세스 권한이 있는 사용자가 생성하고 관리할 수 있습니다.

ASA FirePOWER 모듈은 사용자에 대한 외부 인증을 지원하지 않습니다. ASA CLI 및 ASDM을 통한 ASA 디바이스 액세스가 *Cisco ASA* 시리즈 일반 작업 *CLI* 구성 가이드 및 *Cisco ASA* 시리즈 일반 작업 *ASDM* 구성 가이드에 설명되어 있습니다.

Firepower System 유저 인터페이스

어플라이언스 유형에 따라 웹 기반 GUI, 보조 CLI 또는 Linux 셸을 사용하여 Firepower 어플라이언스와 상호작용할 수 있습니다. Firepower Management Center 구축에서는 FMC GUI로 대부분의 구성 작업을 수행합니다. 소수의 작업에서만 CLI나 Linux 셸을 이용해 어플라이언스에 바로 액세스해야 합니다. Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸 사용은 권장하지 않습니다.

브라우저 요구 사항에 대한 내용은 Firepower 릴리스 노트를 참조하십시오.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면, 시스템이 SSH 연결을 종료합니다.

어플라이언스	웹 기반 **GUI**	보조 **CLI**	**Linux** 셸
Firepower Management Center	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • 운영, 관리 및 분석 작업에 사용할 수 있습니다.	• 사전 정의된 관리자 사용자 및 맞춤형 외부 사용자 계정에서 지원됩니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.	• 사전 정의된 관리자 사용자에 대해 지원됩니다. • Firepower Management Center CLI에서 `expert` 명령을 통해 액세스해야 합니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시하거나 FMC 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.
7000 및 8000 Series 디바이스	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • 초기 설정, 기본 분석 및 구성 작업에만 사용할 수 있습니다.	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시한 설정 및 문제해결 목적으로만 사용해야 합니다.	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • 구성 액세스 권한이 있는 CLI 사용자가 `expert` 명령으로 액세스할 수 있습니다. • Cisco TAC가 지시하거나 FMC 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.

어플라이언스	웹 기반 **GUI**	보조 **CLI**	**Linux** 셸
NGIPSv	—	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 어카운트에 대한 지원 • SSH 연결 또는 VM 콘솔을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시한 설정 및 문제해결 목적으로만 사용해야 합니다.	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 어카운트에 대한 지원 • `expert` 명령을 사용하여 Config(구성) 액세스 권한이 있는 CLI 사용자가 액세스할 수 있습니다. • Cisco TAC가 지시하거나 FMC 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.
ASA FirePOWER 모듈	—	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • SSH 연결을 사용하여 액세스할 수 있습니다. 콘솔 포트를 사용하여 액세스할 수도 있습니다. • 구성 및 관리 작업에 사용할 수 있습니다.	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 어카운트에 대한 지원 • `expert` 명령을 사용하여 Config(구성) 액세스 권한이 있는 CLI 사용자가 액세스할 수 있습니다. • Cisco TAC가 지시하거나 FMC 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.

관련 항목

사용자 어카운트 관리

내부 사용자 추가, 55 페이지

웹 인터페이스 고려 사항

- 조직에서 인증에 CAC(Common Access Cards)를 사용한다면, LDAP로 인증한 외부 사용자는 CAC 자격 증명을 사용하여 어플라이언스의 웹 인터페이스에 대한 액세스를 얻을 수 있습니다.
- 기본 홈페이지 상단에 나열되는 메뉴 및 메뉴 옵션은 사용자 어카운트에 대한 권한을 기반으로 합니다. 그러나 기본 홈 페이지에 대한 링크에는 사용자 어카운트 권한 전반을 포괄하는 옵션이 포함되어 있습니다. 사용자 어카운트에 부여된 권한과 다른 권한을 필요로 하는 링크를 클릭하는 경우, 시스템 경고 메시지가 나타나고 활동을 기록합니다.

- 상당한 시간이 걸리는 프로세스의 경우 웹 브라우저에 스크립트가 응답하지 않는다는 메시지가 표시될 수 있습니다. 이러한 경우 완료될 때까지 스크립트가 계속 진행되도록 해야 합니다.

관련 항목

홈 페이지 지정, 41 페이지

세션 시간 초과

세션 시간 초과에서 제외되도록 달리 구성하지 않는 한, 기본적으로 1시간 동안 활동이 없으면 Firepower System에서 자동으로 로그아웃됩니다.

참고 SSO 사용자의 경우 FMC 세션이 시간 초과되면 디스플레이가 IdP 인터페이스로 잠시 리디렉션된 다음 FMC로그인 페이지로 리디렉션됩니다. SSO 세션이 다른 곳에서 종료되지 않는 한 누구나 로그인 페이지에서 **Single Sign-On(**단일 로그인**)** 링크를 클릭하여 로그인 자격 증명을 제공하지 않고 FMC에 액세스 할 수 있습니다. FMC보안을 유지하고 다른 사용자가 SSO 계정을 사용하여 FMC에 액세스하는 것을 방지하려면 FMC 로그인 세션을 무인 상태로 두지 말고 FMC에서 로그 아웃할 때 IdP의 SSO 페더레이션에서 로그 아웃하는 것이 좋습니다.

Administor(관리자) 역할이 부여된 사용자는 다음 설정을 통해 어플라이언스에 대한 세션 시간 초과 간격을 변경할 수 있습니다.

System(시스템**)** > **Configuration(**구성**)** > **Shell Timeout(**셸 시간 초과**)**

어플라이언스	설정
Firepower Management Center	**System(**시스템**)** > **Configuration(**구성**)** > **Shell Timeout(**셸 시간 초과**)**
7000 및 8000 Series 디바이스	**Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Shell Timeout(**셸 시간 초과**)**

관련 항목

세션 시간 제한 구성, 1388 페이지
SAML SSO(Single Sign-On) 구성, 74 페이지

Firepower Management Center 웹 인터페이스 로그인

참고 이 작업은 LDAP 또는 RADIUS 서버로 인증된 내부 사용자 및 외부 사용자에게 적용됩니다. SSO 로그인에 대해서는 SSO를 사용한 FMC 웹 인터페이스 로그인, 31 페이지의 내용을 참조하십시오.

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 FMC이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 FMC은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 FMC에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 사용자 어카운트 만들기에 설명된 대로 사용자 어카운트를 생성합니다.

프로시저

단계 **1** 브라우저에서 **https://***ipaddress_or_hostname/*으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 FMC와(과) 일치합니다.

단계 **2** **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 사용자 이름과 비밀번호를 입력합니다. 다음 지침에 유의하십시오.

- 사용자 이름은 대/소문자를 구분하지 않습니다.
- 다중 도메인 구축에서 사용자 이름 앞에 사용자 어카운트가 생성된 도메인을 추가합니다. 모든 상위 도메인을 앞에 추가할 필요는 없습니다. 예를 들어 사용자 어카운트가 SubdomainB에서 생성되고 상위 도메인이 DomainA인 경우, 사용자 이름을 다음 형식에 입력합니다.

  ```
  SubdomainB\username
  ```

- 조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. SecurID PIN을 먼저 생성해야 Firepower System에 로그인할 수 있습니다.

단계 **3** **Login(**로그인**)**을 클릭합니다.

관련 항목

세션 시간 초과, 30 페이지

SSO를 사용한 FMC 웹 인터페이스 로그인

FMC는 SAML(Security Assertion Markup Language) 2.0 개방형 표준을 준수하는 SSO 제공자로 구현된 SSO(Single-Sign On) 페더레이션에 참여하도록 구성할 수 있습니다. SSO 사용자 계정은 IdP(Identityy Provider)에서 설정해야 하며 계정 이름으로 이메일 주소를 사용해야 합니다. 사용자 이름이 이메일 주소가 아니거나 SSO 로그인이 실패하면 시스템 관리자에게 문의하십시오.

참고 FMC는 SSO 계정에 대한 CAC 자격 증명을 사용한 로그인을 지원하지 않습니다.

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 FMC이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 FMC은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 FMC에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

시작하기 전에

- SSO 액세스를 위해 FMC를 구성합니다. SAML SSO(Single Sign-On) 구성, 74 페이지의 내용을 참조하십시오.
- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 문의하여 SSO IdP에서 계정을 구성하십시오.

프로시저

단계 **1** 브라우저에서 **https://***ipaddress_or_hostname/*으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 FMC와(과) 일치합니다.

참고 SSO 사용자는 SSO 액세스를 위해 특별히 구성된 로그인 URL을 사용하여 FMC에 지속적으로 액세스해야 합니다. 관리자에게 문의하십시오.

단계 **2** **Single Sign-On(**단일 인증**)** 링크를 클릭합니다.

단계 **3** 시스템은 다음 두 가지 방법 중 하나로 응답합니다.

- SSO 페더레이션에 이미 로그인한 경우 FMC 기본 홈 페이지가 나타납니다.
- SSO 페더레이션에 아직 로그인하지 않은 경우에는 FMC가 브라우저를 IdP의 로그인 페이지로 리디렉션합니다. IdP에서 로그인 프로세스를 완료하면 FMC 기본 홈 페이지가 나타납니다.

관련 항목

세션 시간 초과, 30 페이지
SAML SSO(Single Sign-On) 구성, 74 페이지

7000 또는 8000 Series 디바이스의 웹 인터페이스에 로그인

사용자는 7000 및 8000 Series 디바이스에서 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 디바이스에 해당하는 Firepower 시작 가이드와 사용자 어카운트 만들기에 설명된 대로 초기 설정 프로세스를 완료하고 사용자 어카운트를 생성합니다.

프로시저

단계 **1** 브라우저에서 `https://호스트 이름/`으로 직접 이동합니다. 여기서 `호스트 이름`은 액세스하려는 매니지드 디바이스의 호스트 이름에 해당합니다.

단계 **2** **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 사용자 이름과 비밀번호를 입력합니다. 다음 지침에 유의하십시오.

- 사용자 이름은 대/소문자를 구분하지 않습니다.
- 조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. SecurID PIN을 먼저 생성해야 Firepower System에 로그인할 수 있습니다.

단계 **3** **Login(**로그인**)**을 클릭합니다.

관련 항목

세션 시간 초과, 30 페이지

CAC 크리덴셜로 Firepower Management Center에 로그인

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 FMC이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 FMC은(는) 한 번에 하나의 로그인 세션만 지원합니다.

- 다른 FMC에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

주의 활성 브라우징 세션 중에는 CAC를 제거하지 마십시오. 세션 중에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 사용자 어카운트 만들기에 설명된 대로 사용자 어카운트를 생성합니다.
- CAC 인증 구성에 설명된 대로 CAC 인증 및 권한 부여를 구성합니다.

프로시저

단계 **1** 조직에서 안내하는 대로 CAC를 삽입합니다.

단계 **2** 브라우저에서 **https://***ipaddress_or_hostname*/으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 FMC와(과) 일치합니다.

단계 **3** 메시지가 표시되면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

단계 **4** 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **5** **Continue(**계속**)**를 클릭합니다.

관련 항목

CAC 인증
LADP로 CAC(Common Access Card) 인증 구성, 72 페이지
세션 시간 초과, 30 페이지
FMC에 대한 SSO 지침, 74 페이지

CAC 크리덴셜을 사용하여 7000 또는 8000 Series 디바이스에 로그인

사용자는 7000 및 8000 Series 디바이스에서 단일 활성 세션으로 제한됩니다.

주의 활성 브라우징 세션 중에는 CAC를 제거하지 마십시오. 세션 중에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 사용자 어카운트 만들기에 설명된 대로 사용자 어카운트를 생성합니다.
- CAC 인증 구성에 설명된 대로 CAC 인증 및 권한 부여를 구성합니다.

프로시저

단계 **1** 조직에서 안내하는 대로 CAC를 삽입합니다.

단계 **2** 브라우저에서 `https://hostname/`으로 이동합니다. 여기서 *hostname*은 액세스하려는 어플라이언스의 호스트 이름에 해당합니다.

단계 **3** 메시지가 표시되면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

단계 **4** 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **5** **Continue(**계속**)**를 클릭합니다.

관련 항목

CAC 인증
LADP로 CAC(Common Access Card) 인증 구성, 72 페이지
세션 시간 초과, 30 페이지

FMC Command Line Interface에 로그인

관리자 CLI 사용자와 특정 사용자 지정 외부 사용자는 FMC CLI에 로그인할 수 있습니다.

주의 Cisco TAC가 지시하거나 FMC 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면, 시스템이 SSH 연결을 종료합니다.

시작하기 전에

관리자 사용자로 초기 구성 프로세스를 완료합니다. 최초 로그인, 3 페이지의 내용을 참조하십시오.

프로시저

단계 1 관리자 사용자 이름과 비밀번호를 사용하여, SSH 또는 콘솔 포트를 통해 FMC에 연결합니다.

조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. 로그인하기 전에 SecurID PIN을 생성해야 합니다.

단계 2 사용 가능한 CLI 명령 중 하나를 사용합니다.

7000/8000 시리즈, ASA FirePOWER, NGIPSv 디바이스에서 CLI에 로그인

기본 CLI 구성 액세스만 있어도 기본 매니지드 디바이스에는 바로 로그인할 수 있습니다.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면, 시스템이 SSH 연결을 종료합니다.

시작하기 전에

- 기본 관리자 사용자를 사용하여 초기 로그인에 대한 초기 설정 프로세스를 완료합니다.
- **configure user add** 명령을 사용하여 CLI에 로그인할 수 있는 사용자 어카운트를 추가로 생성할 수 있습니다.
- 7000 및 8000 Series 디바이스의 경우, 사용자 어카운트 만들기에 설명된 대로 웹 인터페이스에서 사용자 어카운트를 생성합니다.

프로시저

단계 1 디바이스의 관리 인터페이스(호스트 이름 또는 IP 주소)에 대한 SSH나 콘솔을 사용합니다.

콘솔 기본값을 이용해 운영 체제 CLI에 액세스한 ASA FirePOWER 디바이스입니다. 이 경우 Firepower CLI에 액세스하려면 추가 단계인 **`session sfr`**을 거쳐야 합니다.

조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. 로그인하기 전에 SecurID PIN을 생성해야 합니다.

단계 2 CLI 프롬프트에서 명령줄 액세스 수준에서 허용되는 명령 중 하나를 사용합니다.

마지막 로그인 보기

권한이 없는 사용자가 여러분의 자격 증명을 이용해 Firepower Management Center에 로그인할 것 같다면, 마지막으로 자격 증명을 이용해 로그인한 날짜, 시간, IP 주소를 확인하십시오.

시작하기 전에

이 기능은 클래식 테마를 사용할 때만 지원됩니다. 사용자 환경 설정에서 이 UI 테마를 선택할 수 있습니다.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** 브라우저 창의 오른쪽 상단에서 로그인하는 데 사용한 사용자 ID를 찾습니다.

단계 **3** 자신의 사용자 이름을 클릭합니다.

단계 **4** 이전 로그인 관련 정보가 메뉴 하단에 표시됩니다.

Firepower System 웹 인터페이스에서 로그아웃

Firepower System 웹 인터페이스를 더 이상 활발하게 사용하지 않는 경우, Cisco에서는 로그아웃할 것을 권장합니다. 잠시 웹 브라우저에서 떨어져 있는 경우에도 마찬가지입니다. 로그아웃하면 웹 세션이 종료되며, 내 크리덴셜로 타인이 어플라이언스를 사용할 수 없도록 합니다.

참고 FMC에서 SSO 세션에서 로그 아웃하는 경우 시스템에서 로그 아웃하면 브라우저가 조직의 SSO IdP로 리디렉션됩니다. FMC 보안을 유지하고 다른 사용자가 SSO 계정을 사용하여 FMC에 액세스하는 것을 방지하려면 IdP의 SSO 페더레이션에서 로그 아웃하는 것이 좋습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Logout(**로그아웃**)**를 선택합니다.

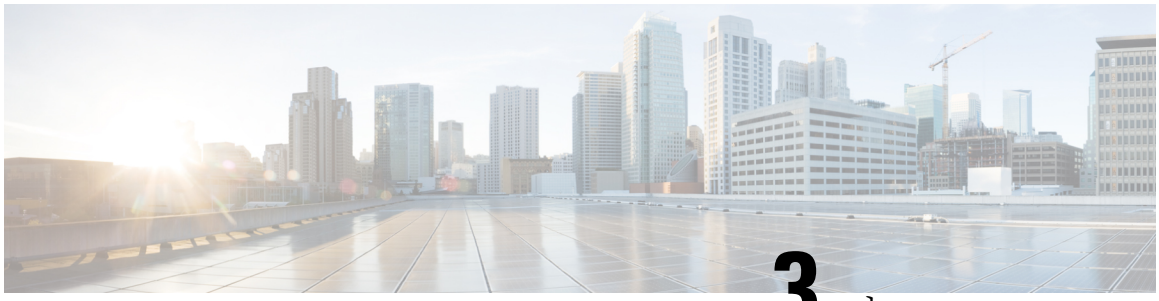
단계 **2** FMC의 SSO 세션에서 로그 아웃하는 경우 시스템이 조직의 SSO IdP로 리디렉션합니다. FMC 보안을 위해 IdP에서 로그 아웃합니다.

관련 항목

세션 시간 초과, 30 페이지

Firepower 시스템 로그인 기록

기능	버전	세부 사항
SAML 2.0 준수 SSO 제공자를 사용하는 SSO(Single Sign-On) 지원을 추가했습니다.	6.7	타사 SAML 2.0 준수 ID 제공자(IdP)에서 설정된 사용자가 로그인 페이지에서 새로운 **SSO(Single Sign-On)** 링크를 사용하여 FMC에 로그인하는 기능을 추가했습니다. 신규/수정된 화면: 로그인 화면
다음에 대한 마지막 로그인 정보 확인 Firepower Management Center	6.5	마지막으로 로그인한 날짜, 시간 및 IP 주소를 확인합니다. 신규/수정된 메뉴: 창의 오른쪽 상단에 있는 메뉴로, 로그인하는 데 사용한 사용자 이름을 표시합니다. 지원되는 플랫폼: FMC
다음에 대한 자동 CLI 액세스 FMC	6.5	SSH를 이용해 FMC에 로그인하면, CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI `expert` 명령을 사용하면 Linux 셸에 액세스할 수 있습니다. 참고 이 기능을 이용하면 버전 6.3 기능인 FMC에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 FMC에서는 **System(**시스템**)** > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)** 페이지가 표시되지 않습니다. 물리적 FMC에서는 계속 표시됩니다.
SSH 로그인 실패 횟수를 제한합니다.	6.3	사용자가 SSH를 통해 디바이스에 액세스하고 3회 연속 로그인 시도가 실패한 경우, 해당 디바이스가 SSH 세션을 종료합니다.
CLI 액세스를 활성화 및 비활성화 하는 기능 FMC	6.3	신규/수정된 화면: FMC 웹 인터페이스 관리자가 사용할 수 있는 새 체크박스: **Enable CLI Access(CLI** 액세스 활성화**)(System(**시스템**)** > **Configuration(**구성**)**에 위치) > (**Console Configuration(**콘솔 구성**))** 페이지 • 선택: SSH를 사용하여 FMC에 로그인하면 CLI에 액세스할 수 있습니다. • 선택 취소: SSH를 사용하여 FMC에 로그인하면 Linux 셸에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다. 지원되는 플랫폼: FMC



3 장

사용자 환경설정 지정

다음 주제에서는 사용자 환경설정을 지정하는 방법을 설명합니다.

- 사용자 환경설정 소개, 39 페이지
- 비밀번호 변경, 39 페이지
- 만료된 비밀번호 변경, 40 페이지
- 웹 인터페이스 모양 변경, 40 페이지
- 홈 페이지 지정, 41 페이지
- 이벤트 보기 구성, 41 페이지
- 기본 표준 시간대 설정, 46 페이지
- 기본 대시보드 지정, 47 페이지
- 사용자 환경 설정 지정 기록, 48 페이지

사용자 환경설정 소개

사용자 역할에 따라 사용자 계정에 대한 특정 기본 설정을 지정할 수 있습니다.

다중 도메인 구축에서 사용자 환경설정은 계정이 액세스하는 모든 도메인에 적용됩니다. 홈페이지 및 대시보드 환경설정을 지정하는 경우, 특정 페이지와 대시보드 위젯은 도메인에 의해 제한됩니다.

비밀번호 변경

모든 사용자 어카운트는 비밀번호로 보호됩니다. 언제라도 비밀번호를 변경할 수 있으며, 사용자 어카운트에 대한 설정에 따라 정기적으로 비밀번호를 변경해야 하는 경우도 있습니다.

비밀번호 강도 확인을 활성화하면, 비밀번호는 사용자 어카운트 가이드라인 및 제한 사항에서 설명하는 강력한 비밀번호 요구 사항을 준수해야 합니다.

LDAP 또는 RADIUS 사용자일 경우 웹 인터페이스를 통해 비밀번호를 변경할 수 없습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Change Password(**비밀번호 변경**)**를 클릭합니다.

단계 **3** 선택 사항으로, **Show password(**비밀번호 표시**)** 확인란을 선택하면 이 대화상자를 이용하는 동안 비밀번호를 확인할 수 있습니다.

단계 **4** **Current Password(**현재 비밀번호**)**를 입력합니다.

단계 **5** 다음 2가지 옵션을 사용할 수 있습니다.

- **New Password(**새 비밀번호**)**와 **Confirm Password(**비밀번호 확인**)**에 새 비밀번호를 입력합니다.
- **Generate Password(**비밀번호 생성**)**을 클릭하면 나열된 기준을 준수하는 비밀번호를 시스템이 대신 생성합니다. (이렇게 생성되는 비밀번호는 기억하기가 쉽지 않습니다. 이 옵션을 선택한다면 비밀번호를 기록해 두십시오.)

단계 **6** **Apply(**적용**)**를 클릭합니다.

만료된 비밀번호 변경

사용자 어카운트의 설정에 따라 비밀번호가 만료될 수 있습니다. 비밀번호 만료 기한은 계정 생성 시 설정됩니다. 비밀번호가 만료된 경우 Password Expiration Warning(비밀번호 만료 경고) 페이지가 나타납니다.

프로시저

Password Expiration Warning(비밀번호 만료 경고) 페이지에는 다음과 같이 두 가지 옵션이 있습니다.

- 지금 비밀번호를 변경하려면 **Change Password(**비밀번호 변경**)**를 클릭합니다. 남은 경고 일수가 0일 경우, 반드시 비밀번호를 변경해야 합니다.

  팁 비밀번호 강도 확인을 활성화하면, 비밀번호는 사용자 어카운트 가이드라인 및 제한 사항에서 설명하는 강력한 비밀번호 요구 사항을 준수해야 합니다.

- 비밀번호를 나중에 변경하려면 **Skip(**넘어가기**)**을 클릭합니다.

웹 인터페이스 모양 변경

웹 인터페이스가 표시되는 방식을 변경할 수 있습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다. **General(**일반**)** 탭은 기본적으로 표시됩니다.

단계 **2** 테마를 선택합니다.

- 밝게
- **Dusk(**일몰**)** (베타)
- 클래식(6.6 이전 릴리스의 모양과 느낌)

홈 페이지 지정

웹 인터페이스에서 어플라이언스의 홈페이지로 사용할 페이지를 지정할 수 있습니다. 기본 홈 페이지는 기본 대시보드**(Overview(**개요**)** > **Dashboards(**대시보드**))**이며, 외부 데이터베이스 사용자처럼 대시보드 액세스 권한이 없는 사용자 계정은 제외됩니다. (기본 대시보드를 설정하는 방법은 기본 대시보드 지정, 47 페이지을 참조하십시오.)

다중 도메인 구축에서 선택한 홈페이지가 사용자 어카운트가 액세스하는 모든 도메인에 적용됩니다. 참고로 여러 도메인에 자주 액세스하는 계정에 대한 홈페이지를 선택하는 경우, 특정 페이지가 전역 도메인으로 제한됩니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Home Page(**홈페이지**)**를 클릭합니다.

단계 **3** 홈페이지로 사용할 페이지를 드롭다운 목록에서 선택합니다.

드롭다운 목록의 옵션은 사용자 어카운트의 액세스 권한에 따라 달라집니다. 자세한 내용은 사용자 어카운트 권한사용자 역할, 50 페이지를 참고하십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

이벤트 보기 구성

Firepower Management Center의 이벤트 보기 특성을 구성하려면 Event View Settings(이벤트 보기 설정) 페이지를 사용합니다. 일부 이벤트 보기 구성은 특정 사용자 역할만 사용할 수 있습니다. External Database User(외부 데이터베이스 사용자) 역할이 주어진 사용자는 이벤트 보기 설정 유저 인터페이스의 일부를 볼 수 있으나, 그러한 설정을 변경하더라도 크게 달라지지 않습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Event View Settings(**이벤트 보기 설정**)**를 클릭합니다.

단계 **3** **Event Preferences(**이벤트 환경 설정**)** 섹션에서 이벤트 보기의 기본 특징을 구성합니다. 이벤트 보기 환경 설정, 42 페이지를 참조하십시오.

단계 **4** **File Preferences(**파일 환경설정**)** 섹션에서 구성 파일 다운로드 환경 설정을 구성합니다. 파일 다운로드 환경설정, 43 페이지를 참조하십시오.

단계 **5** **Default Time Windows(**기본 시간대**)** 섹션에서 기본 시간 창(복수 가능)을 구성합니다. 기본 시간대, 44 페이지를 참조하십시오.

단계 **6** **Default Workflow(**기본 워크플로**)** 섹션에서 기본 워크플로를 구성합니다. 기본 워크플로, 46 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

이벤트 보기 환경 설정

Event View Settings(이벤트 보기 설정) 페이지의 Event Preferenes(이벤트 환경설정) 섹션을 사용하여 Firepower System의 이벤트 보기 기본 특징을 구성합니다. 이 섹션은 모든 사용자 역할에서 사용할 수 있으나 이벤트 보기 권한이 없는 사용자에게는 별 의미가 없습니다.

다음 필드가 Event Preferences(이벤트 환경설정) 섹션에 나타납니다.

- **Confirm "All" Actions("**모든" 작업 확인**)** 필드는 어플라이언스에서 이벤트 보기의 모든 이벤트에 적용될 작업에 대해 반드시 사용자에게 확인하는지 여부를 제어합니다.

  예를 들어 이 설정이 활성화된 상태에서 이벤트 보기의 **Delete All(**모두 삭제**)**을 클릭할 경우, 현재 제약 조건을 충족하는 모든 이벤트(현재 페이지에 표시되지 않은 이벤트 포함)를 삭제할 것임을 사용자가 확인해야 어플라이언스가 데이터베이스에서 이를 삭제합니다.

- **Resolve IP Addresses(IP** 주소 분해**)** 필드는 어플라이언스가 이벤트 보기에서 가급적 IP 주소 대신 호스트 이름을 표시하도록 합니다.

  많은 IP 주소를 포함하고 이 옵션을 활성화한 경우 이벤트 보기에 표시되는 속도가 느려질 수 있습니다. 참고로 이 설정을 적용하려면 관리 인터페이스 구성을 사용해 시스템 설정에서 DNS 서버를 설정해야 합니다.

- **Expand Packet View(**패킷 보기 확대**)** 필드에서는 침입 이벤트에 대한 패킷 보기가 나타나는 방식을 구성할 수 있습니다. 기본적으로 어플라이언스는 패킷 보기의 축소 버전을 표시합니다.
  - **None(**해당 없음**)** - 패킷 보기 중 Packet Information(패킷 정보) 섹션의 모든 하위 섹션을 축소합니다.
  - **Packet Text(**패킷 텍스트**)** - Packet Text(패킷 텍스트) 하위 섹션만 확장합니다.
  - **Packet Bytes(**패킷 바이트**)** - Packet Bytes(패킷 바이트) 하위 섹션만 확장합니다.

- **All(**모두**)** - 모든 섹션을 확장합니다.

기본 설정과 무관하게 언제라도 패킷 보기에서 섹션을 수동 확장하여 캡처된 패킷에 대한 세부 정보를 볼 수 있습니다.

- **Rows Per Page(**페이지당 행 수**)** 필드에서는 페이지당 몇 개의 이벤트 행을 드릴다운 페이지 및 테이블 보기에 표시할 것인지를 제어합니다.
- **Refresh Interval(**새로 고침 간격**)** 필드에서는 이벤트 보기의 새로 고침 간격을 분 단위로 설정합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다. 이 간격은 대시보드에 적용되지 않습니다.
- **Statistics Refresh Interval(**통계 새로 고침 간격**)**은 Intrusion Event Statistics(침입 이벤트 통계) 페이지, Discovery Statistics(탐색 통계) 페이지와 같은 이벤트 요약 페이지의 새로 고침 간격을 제어합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다. 이 간격은 대시보드에 적용되지 않습니다.
- **Deactivate Rules(**규칙 비활성화**)** 필드는 다음과 같이 표준 텍스트 규칙에 의해 생성된 침입 이벤트의 패킷 보기에 표시되는 링크를 제어합니다.
  - **All Policies(**모든 정책**)** - 로컬에 정의된 모든 사용자 지정 침입 정책에서 표준 텍스트 규칙을 비활성화하는 단일 링크
  - **Current Policy(**현재 정책**)** - 현재 배포된 침입 정책에서만 표준 텍스트 규칙을 비활성화하는 단일 링크 기본 정책의 규칙은 비활성화할 수 없습니다.
  - **Ask(**질문**)** - 이 옵션 각각의 링크

패킷 보기에서 이 링크를 표시하려면 사용자 어카운트가 관리자 또는 침입 관리자 액세스 권한을 가져야 합니다.

관련 항목

Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지

파일 다운로드 환경설정

로컬 파일 다운로드의 기본 특성을 구성하려면 Event View Settings(이벤트 보기 설정) 페이지의 File Preferences(파일 환경설정)섹션을 사용합니다. 이 섹션은 Administrator(관리자), Security Analyst(보안 분석가) 또는 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 사용자 역할만 사용할 수 있습니다.

어플라이언스에서 캡처된 파일의 다운로드를 지원하지 않을 경우 이 옵션은 비활성화됩니다.

다음 필드가 File Preferences(파일 환경설정) 섹션에 나타납니다.

- **Confirm 'Download File' Actions('**다운로드 파일' 확인 작업**)** 확인란은 파일을 다운로드할 때마다 File Download(파일 다운로드) 팝업 창이 나타나 경고를 표시하고 계속 또는 취소를 선택하게 할지를 제어합니다.

주의 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

파일을 다운로드할 때마다이 옵션을 비활성화할 수 있습니다.

- 캡처된 파일을 다운로드할 때 비밀번호로 보호되는 .zip 아카이브가 생성되며 여기에 파일이 들어 있습니다. **Zip File Passward(Zip** 파일 비밀번호**)** 필드에서는 .zip 파일에 대한 액세스 권한을 제한하기 위해 사용할 비밀번호를 정의합니다. 이 필드를 비워 둘 경우 비밀번호 없이 아카이브 파일이 생성됩니다.
- The **Show Zip File Password(Zip** 파일 비밀번호 표시**)** 확인란에서는 **Zip File Password(Zip** 파일 비밀번호**)** 필드에 일반 텍스트 아니면 난독 문자를 표시할지 선택합니다. 이 필드의 값을 지우면 **Zip File Password(Zip** 파일 비밀번호**)**는 난독 문자를 표시합니다.

기본 시간대

시간 범위라고도 하는 시간대는 임의의 이벤트 보기에서 이벤트에 대한 시간 제약 조건을 부여합니다. 시간대의 기본 동작을 제어하려면 Event View Settings(이벤트 보기 설정) 페이지의 Default Time Windows(기본 시간대) 섹션을 사용합니다.

이 섹션에 대한 사용자 역할 액세스 권한은 다음과 같습니다.

- Administor(관리자) 및 Maintenance Users(유지 보수 사용자)는 전체 섹션에 액세스할 수 있습니다.
- Security Analysts(보안 분석가)와 Security Analysts(Read Only)(보안 분석가(읽기 전용))는 **Audit Log Time Window(**감사 로그 시간대**)**을 제외한 모든 옵션에 액세스할 수 있습니다.
- Access Admins(액세스 관리자), Discovery Admins(검색 관리자), External Database Users(외부 데이터베이스 사용자), Intrusion Admins(침입 관리자), Network Admins(네트워크 관리자), Security Approvers(보안 승인자)는 **Events Time Window(**이벤트 시간대**)** 옵션만 액세스할 수 있습니다.

기본 시간대 설정과 무관하게 이벤트 분석 중 언제라도 개별 이벤트 보기의 시간대를 수동 변경할 수 있습니다. 또한 시간대 설정은 현재 세션에 대해서만 유효합니다. 로그아웃했다가 다시 로그인하면 시간대는 이 페이지에서 구현한 기본값으로 재설정됩니다.

3가지 이벤트 유형에 대해 기본 시간대를 설정할 수 있습니다.

- **Events Time Window(**이벤트 시간대**)**에서는 시간에 의한 제약이 가능한 대부분의 이벤트에 대해 단일 기본 시간 창을 설정합니다.
- **Audit Log Time Window(**감사 로그 시간대**)**에서는 감사 로그에 대한 기본 시간 창을 설정합니다.
- **Health Monitoring Time Window(**상태 모니터링 시간대**)**에서는 상태 이벤트에 대한 기본 시간 창을 설정합니다.

사용자 어카운트에서 액세스 가능한 이벤트 유형에 대해서만 시간대를 설정할 수 있습니다. 모든 사용자 유형이 이벤트 시간대를 설정할 수 있습니다. Administrators(관리자), Maintenance Users(유지 보수 사용자), Security Analysts(보안 분석가)는 상태 모니터링 시간 창을 설정할 수 있습니다. Administrators(관리자)와 Maintenance Users(유지 보수 사용자)는 감사 로그 시간대를 설정할 수 있습니다.

모든 이벤트 보기를 시간으로 제약할 수 없으므로, 시간 창 설정은 호스트, 호스트 속성, 애플리케이션, 클라이언트, 취약점, 사용자 ID 또는 규정준수 화이트리스트 위반을 표시하는 이벤트 보기에는 적용되지 않습니다.

이벤트 유형별로 하나씩 **Multiple(**다중**)** 시간대를 사용하거나 모든 이벤트에 적용되는 **Single(**단일**)** 시간대를 사용할 수 있습니다. 단일 시간 창을 사용할 경우 3가지 시간 창 유형에 대한 설정이 사라지고 새로운 **Global Time Window(**전역 시간대**)** 설정이 나타납니다.

시간대에는 3가지 유형이 있습니다.

- 고정*(static)* 유형은 특정 시작 시간부터 종료 시간까지 생성된 모든 이벤트를 표시합니다.
- 확장*(expanding)* 유형은 특정 시작 시간부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 시간대가 확장되고 새 이벤트가 이벤트 보기에 추가됩니다.
- 슬라이딩*(sliding)* 유형은 특정 시작 시간(예: 1일 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 시간 창이 "슬라이딩"하므로 구성된 범위(이 예에서는 지난 1일)의 이벤트만 볼 수 있습니다.

모든 시간대의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다.

다음 옵션이 **Time Window Settings(**시간대 설정**)** 드롭다운 목록에 나타납니다.

- **Show the Last - Sliding(**마지막 표시 - 슬라이딩**)** 옵션에서는 사용자가 지정한 길이의 슬라이딩 기본 시간대를 구성할 수 있습니다.

  어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하면 시간대가 "슬라이딩"하므로 항상 지난 1시간의 이벤트가 표시됩니다.

- **Show the Last - Static/Expanding(**마지막 표시 - 고정/확장**)** 옵션에서는 사용자가 지정한 길이의 고정 또는 확장 기본 시간대를 구성할 수 있습니다.

  static(고정**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 활성화합니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다.

  expanding(확장**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 비활성화합니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대 현재 시간으로 확장됩니다.

- **Current Day - Static/Expanding(**현재 날짜 - 고정/확장**)** 옵션에서는 현재 날짜에 대해 고정 또는 확장 기본 시간대를 구성할 수 있습니다. 현재 날짜는 현재 세션의 표준 시간대 설정에 따라 자정에 시작합니다.

static(고정**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 활성화합니다. 어플라이언스는 자정부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다.

expanding(확장**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 비활성화합니다. 어플라이언스는 자정부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대가 현재 시간으로 확장됩니다. 로그아웃하기 전 24시간 이상 분석이 계속될 경우 이 시간대가 24시간을 초과할 수 있습니다.

- **Current Week - Static/Expanding(**현재 주 - 고정/확장**)** 옵션에서는 현재 주에 대해 고정 또는 확장 기본 시간대를 구성할 수 있습니다. 현재 주는 현재 세션의 표준 시간대 설정에 따라 이전 일요일 자정에 시작합니다.

  static(고정**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 활성화합니다. 어플라이언스는 자정부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다.

  expanding(확장**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 비활성화합니다. 어플라이언스는 일요일 자정부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대는 현재 시간으로 확장됩니다. 로그아웃하기 전 1주일 이상 분석이 계속될 경우, 시간대는 1주를 초과할 수 있습니다.

기본 워크플로

워크플로는 분석가가 이벤트 평가에 사용하는 데이터를 표시하는 일련의 페이지입니다. 어플라이언스는 이벤트 유형별로 하나 이상의 사전 정의된 워크플로를 기본적으로 제공합니다. 예를 들어 Security Analyst(보안 분석가)라면 수행하는 분석 유형에 따라 10가지 침입 이벤트 워크플로 중에서 선택할 수 있으며, 각 워크플로는 각기 다른 방식으로 침입 이벤트 데이터를 전달합니다.

어플라이언스는 이벤트 유형별로 하나의 기본 워크플로가 구성되어 있습니다. 예를 들어 Events by Priority and Classification(우선순위 및 분류별 이벤트) 워크플로는 침입 이벤트의 기본 워크플로입니다. 즉 침입 이벤트(검토된 침입 이벤트 포함)를 볼 때마다 Events by Priority and Classification(우선순위 및 분류별 이벤트) 워크플로가 표시됩니다.

그러나 각 이벤트 유형에 대한 기본 워크플로를 변경할 수 있습니다. 구성 가능한 기본 워크플로는 사용자 역할에 따라 달라집니다. 예를 들어 침입 이벤트 분석가는 기본 검색 이벤트 워크플로를 설정할 수 없습니다.

기본 표준 시간대 설정

이 설정은 작업 예약 및 대시보드 보기와 같은 사용자 계정에 대해서만 웹 인터페이스에 표시되는 시간을 결정합니다. 이 설정은 시스템 시간을 변경하거나 다른 사용자에게 영향을 주지 않으며, 일반적으로 UTC를 사용하는 시스템에 저장된 데이터에는 영향을 미치지 않습니다.

경고! User Preferences(사용자 환경 설정)의 Time Zone(표준 시간대) 기능에서는 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 변경할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.

참고 이 기능은 시간 기반 정책 적용에 사용되는 표준 시간대에 영향을 주지 않습니다. **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**에서 디바이스의 표준 시간대를 설정합니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Time Zone(**표준 시간대**)**을 클릭합니다.

단계 **3** 사용하려는 표준 시간대가 속한 대륙이나 지역을 선택합니다.

단계 **4** 사용하려는 표준 시간대에 해당하는 국가 및 주 이름을 선택합니다.

기본 대시보드 지정

Overview(개요**)** > **Dashboards(**대시보드**)**를 선택하는 경우 기본 대시보드가 나타납니다. 변경되지 않는 경우, 모든 사용자에 대한 기본 대시보드는 요약(Summary) 대시보드입니다. 사용자 역할이 Administrator(관리자), Maintenance(유지 관리) 또는 Security Analyst(보안 분석가)인 경우 기본 대시보드를 변경할 수 있습니다.

다중 도메인 구축에서 선택한 기본 대시보드가 사용자 어카운트가 액세스하는 모든 도메인에 적용됩니다. 여러 도메인에 자주 액세스하는 계정에 대한 대시보드를 선택하는 경우, 특정 대시보드 위젯이 도메인에 의해 제한됩니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Dashboard Settings(**대시보드 설정**)**을 클릭합니다.

단계 **3** 기본으로 사용할 대시보드를 드롭다운 목록에서 선택합니다. **None(**해당 없음**)**을 선택하는 경우 **Overview(**개요**)** > **Dashboards(**대시보드**)**를 선택하면 확인할 대시보드를 선택할 수 있습니다.

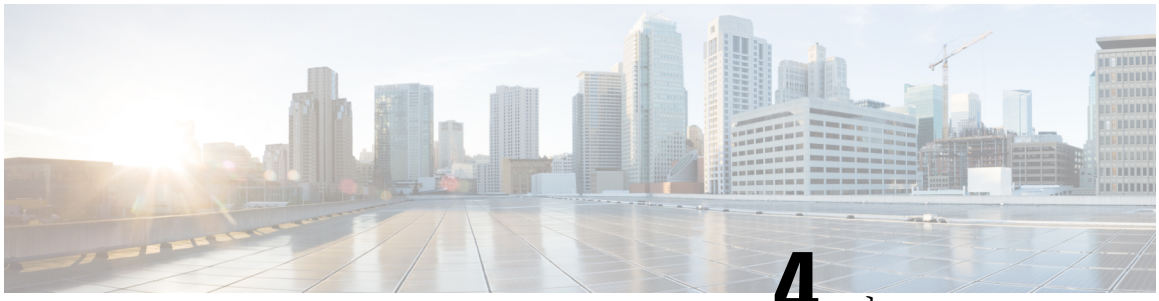
단계 **4** **Save(**저장**)**를 클릭합니다.

관련 항목

Viewing Dashboards, 385 페이지

사용자 환경 설정 지정 기록

기능	버전	세부 사항
UI 테마	6.7 6.6	FMC 웹 인터페이스의 모양과 느낌을 선택할 수 있습니다. Light 테마를 선택하거나 이전 FMC 릴리스에서 사용된 Classic 테마를 사용합니다. 6.7에서는 Dusk 테마가 실험(베타) 기능으로 추가되었습니다. 신규/수정된 화면: User Name(사용자 이름) > **User Preferences(**사용자 환경 설정**)** > **General(**일반**)** > **UI Themes(UI** 테마**)** 지원되는 플랫폼: FMC
향상된 비밀번호 보안	6.5	이제 새로운 강력한 비밀번호 요구 사항이 문서의 단일 위치에 표시되며, 이 장에서 상호참조됩니다. 비밀번호 변경 인터페이스에 새 필드인 **Show Password(**비밀번호 표시**)** 및 **Generate Password(**비밀번호 생성**)**가 추가되었습니다. 신규/수정된 화면: User Name(사용자 이름) > **User Preferences(**사용자 환경 설정**)** > **General(**일반**)** > **Change Password(**비밀번호 변경**)** 지원되는 플랫폼: FMC



4 장

FMC의 사용자 계정

FMC에는 웹 및 CLI 액세스에 필요한 기본 관리자 계정이 포함되어 있습니다. 이 장에서는 맞춤형 사용자 계정을 생성하는 방법을 설명합니다. Firepower System에 로그인, 25 페이지의 내용을 참조하여 FMC에 사용자 계정으로 로그인하는 방법을 자세히 알아보십시오.

- FMC 사용자 계정 정보, 49 페이지
- FMC용 사용자 계정 지침 및 제한 사항, 54 페이지
- FMC 사용자 계정 요구 사항 및 사전 요건, 55 페이지
- 내부 사용자 추가, 55 페이지
- 외부 인증 구성, 57 페이지
- SAML SSO(Single Sign-On) 구성, on page 74
- 웹 인터페이스의 사용자 역할 맞춤화, 127 페이지
- LDAP 인증 연결 문제 해결, 132 페이지
- FMC 사용자 계정 히스토리, 134 페이지

FMC 사용자 계정 정보

FMC에 세 종의 맞춤형 사용자 계정, 즉 LDAP 또는 RADIUS 서버에서 내부 사용자, 외부 사용자로 또는 SAML 2.0 규정 준수 SSO ID 제공자에서 SSO 사용자로 추가할 수 있습니다. FMC은 매니지드 디바이스에서 별도 사용자 계정을 유지 관리합니다. 예를 들어 사용자를 FMC에 추가하는 경우, 해당 사용자만 FMC에 액세스할 수 있습니다. 해당 사용자 이름을 사용해 매니지드 디바이스에 직접 로그인할 수 없습니다. 매니지드 디바이스에서 사용자를 별도로 추가해야 합니다.

내부 및 외부, 그리고 SSO 사용자

FMC에서는 다음 3 가지 유형의 사용자를 지원합니다.

- 내부 사용자—FMC는 사용자 인증을 위해 로컬 데이터베이스를 검사합니다. 내부 사용자에 대한 자세한 내용은 내부 사용자 추가, 55 페이지을 참조하십시오.
- 외부 사용자—사용자가 로컬 데이터베이스에 없는 경우, 시스템이 외부 LDAP 또는 RADIUS 인증 서버에 쿼리합니다. 외부 사용자에 대한 자세한 내용은 외부 인증 구성, 57 페이지을 참조하십시오.

- SSO user(SSO 사용자)-계정이 SSO ID 제공자 측에서 구성된 경우 사용자가 FMC 로그인 페이지의 **SSO(Single Sign-On)** 링크를 사용하여 로그인하고 FMC에서는 인증 및 권한 부여를 위해 사용자를 IdP로 리디렉션합니다. SSO 사용자에 대한 자세한 내용은 SAML SSO(Single Sign-On) 구성, 74 페이지을 참조하십시오.

웹 인터페이스 및 **CLI** 액세스

FMC에는 웹 인터페이스, CLI(콘솔 (시리얼 포트 또는 키보드 및 모니터)에서 액세스하거나 SSH를 사용하여 관리 인터페이스에 액세스할 수 있음) 및 Linux 셸이 있습니다. 관리 UI에 대한 자세한 내용은 Firepower System 유저 인터페이스, 27 페이지을 참조하십시오.

FMC 사용자 유형 및 액세스 가능한 UI에 대한 다음 정보를 참조하십시오.

- 관리 사용자 - FMC은 두 개의 서로 다른 내부 관리자 사용자를 지원합니다. 하나는 웹 인터페이스용이며 다른 하나는 CLI 액세스용입니다. 시스템 초기화 프로세스에서 두 관리자 계정의 비밀번호를 동기화하기 때문에 처음에는 두 계정이 동일하지만, 서로 다른 내부 메커니즘을 이용해 추적하며 초기 구성 후에 달라질 수 있습니다. 시스템 초기화에 관한 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오. (웹 인터페이스 관리자의 암호를 변경하려면 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)**를 사용합니다. CLI 관리자의 암호를 변경하려면, FMC CLI 명령 **configure password**을 사용합니다.)
- 내부 사용자 - 웹 인터페이스에 추가된 내부 사용자는 웹 인터페이스 액세스만 할 수 있습니다.
- 외부 사용자 - 외부 사용자가 웹 인터페이스에 액세스할 수 있으며, 선택적으로 CLI 액세스를 구성할 수 있습니다.
- SSO 사용자 - SSO 사용자는 웹 인터페이스 액세스만 가능합니다.

⚠

주의 CLI 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Cisco TAC가 지시하거나 FMC 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다. CLI 사용자는 Linux 셸에서 `sudoers` 권한을 얻을 수 있으며 이로 인해 보안 위험이 발생됩니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- CLI 액세스 권한이 있는 외부 사용자 목록을 적절하게 제한해야 합니다.
- Linux 셸에서 바로 사용자를 추가하지 마십시오. 이 장에서 설명하는 절차만 사용해야 합니다.

사용자 역할

CLI 사용자 역할

FMC의 CLI 외부 사용자는 사용자 역할이 없습니다. CLI 사용자는 사용 가능한 명령을 모두 사용할 수 있습니다.

웹 인터페이스 사용자 역할

사용자 권한은 할당된 사용자 역할을 기반으로 합니다. 예를 들어, 분석가에게 Security Analyst(보안 분석가) 및 Discovery Admin(검색 관리자) 같은 사전 정의된 역할을 부여하고 디바이스를 관리하는 보안 관리자를 위해 Admin(관리자) 역할을 남겨둘 수 있습니다. 조직의 요구 사항에 부합하는 액세스 권한을 가진 맞춤형 사용자 역할을 생성할 수도 있습니다.

FMC는 다음의 사전 정의된 사용자 역할을 포함합니다.

참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할은 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)** 및 **System(**시스템**)** > **Users(**사용자**)** > **User Roles(**사용자 역할**)**의 역할 이름에 **(**읽기 전용**)**이라고 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 동시 세션 제한에 대한 자세한 내용은 전역 사용자 구성, 1385 페이지을 참조하십시오.

액세스 관리자

Policies(정책**)** 메뉴에서 액세스 제어 정책 및 관련된 기능에 대한 액세스를 제공합니다. 액세스 관리자는 정책을 구축할 수 없습니다.

관리자

관리자는 제품의 모든 항목에 액세스할 수 있습니다. 해당 세션은 보안 침해 시 더 심각한 위험을 초래하므로 로그인 세션 시간 초과에서 면제할 수 없습니다.

관리자 역할의 사용은 보안을 위해 필요한 경우로 제한해야 합니다.

검색 관리자

Policies(정책**)** 메뉴에서 네트워크 검색, 애플리케이션 탐지 및 상관 관계 기능에 대한 액세스를 제공합니다. 검색 관리자는 정책을 구축할 수 없습니다.

외부 데이터베이스 사용자**(**읽기 전용**)**

JDBC SSL 연결을 지원하는 애플리케이션을 사용하여 Firepower System 데이터베이스에 대한 읽기 전용 액세스를 제공합니다. 타사 애플리케이션이 Firepower System 어플라이언스를 인증하려면 시스템 설정에서 데이터베이스 액세스를 활성화해야 합니다. 외부 데이터베이스 사용자는 웹 인터페이스에서 **Help(**도움말**)** 메뉴의 온라인 도움말 관련 옵션에만 액세스할 수 있습니다. 이 역할의 기능이 웹 인터페이스와 무관하므로 용이한 지원 및 비밀번호 변경에 대한 액세스만 제공됩니다.

침입 관리자

Policies(정책**)** 및 **Objects(**개체**)** 메뉴에서 모든 침입 정책, 침입 규칙 및 네트워크 분석 정책 기능에 대한 액세스를 제공합니다. 침입 관리자는 정책을 구축할 수 없습니다.

유지 보수 사용자

모니터링 및 유지 보수 기능에 대한 액세스를 제공합니다. 유지 보수 사용자는 **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 유지 보수 관련 옵션에 액세스할 수 있습니다.

네트워크 관리자

Policies(정책**)** 메뉴에서 액세스 제어, SSL 검사, DNS 정책 및 ID 정책 기능에 대한 액세스를 비롯해 **Devices(**디바이스**)** 메뉴에서 디바이스 구성 기능에 대한 액세스도 제공합니다. 네트워크 관리자는 디바이스에 구성 변경 사항을 구축할 수 있습니다.

보안 분석가

Overview(개요**)**, **Analysis(**분석**)**, **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 보안 이벤트 분석 기능에 대한 액세스와 상태 이벤트에 대한 읽기 전용 액세스를 제공합니다.

보안 분석가**(**읽기 전용**)**

Overview(개요**)**, **Analysis(**분석**)**, **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 보안 이벤트 분석 기능과 상태 이벤트 기능에 대한 읽기 전용 액세스를 제공합니다.

이 역할의 사용자는 다음 작업도 수행할 수 있습니다.

- 특정 디바이스에 대한 상태 모니터 페이지에서 문제 해결 파일을 생성하고 다운로드합니다.
- 사용자 기본 설정에서 파일 다운로드 기본 설정을 지정합니다.
- 사용자 기본 설정에서 이벤트 로그 보기의 기본 기간을 설정합니다(**Audit Log Time Window(**감사 로그 시간 기간**)** 제외).

보안 승인자

Policies(정책**)** 메뉴에서 액세스 제어 및 관련된 정책과 네트워크 검색 정책에 대한 제한된 액세스를 제공합니다. 보안 승인자는 이러한 정책을 확인하고 구축할 수 있지만 정책을 변경할 수는 없습니다.

사용자 암호

다음 규칙은 LOM(Lights-Out Management)을 사용하거나 사용하지 않도록 설정한 FMC의 내부 사용자 계정에 대한 비밀번호에 적용됩니다. 외부에서 인증한 계정이나 보안 인증 규정 준수를 활성화한 시스템에서는 다른 비밀번호 요구 사항이 적용됩니다. 자세한 내용은 외부 인증 구성 및 보안 인증 컴플라이언스, 1469 페이지를 참고하십시오.

FMC 초기 설정에서, 시스템은 관리자 사용자에게 아래 테이블에서 설명하는 LOM 활성화 사용자에 대한 강력한 비밀번호 요구 사항을 준수하는 계정 비밀번호를 설정하도록 요구합니다. 이때 시스템은 웹 인터페이스 관리자와 CLI 액세스 관리자의 비밀번호를 동기화합니다. 초기 구성이 끝나면 웹 인터페이스 관리자는 강력한 비밀번호 요구 사항을 제거할 수 있지만, CLI 액세스 관리자는 강력한 비밀번호 요구사항을 준수해야 합니다.

	LOM 활성화되지 않음	**LOM** 활성화됨, 관리자 사용자
비밀번호 강도 확인 설정	비밀번호는 다음을 포함해야 합니다. • 최소 8자 또는 관리자가 사용자에 대해 설정한 문자 수 중 더 긴 값 • 반복되는 문자 2개 미만 • 소문자 1개 이상 • 대문자 1개 이상 • 하나 이상의 숫자가 필요합니다. • 특수문자 1개 이상(! @ # * - _ + 등) 시스템은 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열을 포함하는 특수한 사전을 이용해 비밀번호를 검사합니다.	비밀번호는 다음을 포함해야 합니다. • 8~20개 사이의 문자(MC 1000, MC 2500, MC 4500의 경우 상한은 20자가 아닌 14자입니다.) • 반복되는 문자 2개 미만 • 소문자 1개 이상 • 대문자 1개 이상 • 하나 이상의 숫자가 필요합니다. • 특수문자 1개 이상(! @ # * - _ + 등) 특수 문자 규칙은 물리적 FMC 시리즈에 따라 다릅니다. 아래 마지막 글머리 기호에 나열된 특수 문자만 선택하는 방법을 권장합니다. 비밀번호에는 사용자 이름을 포함하지 마십시오. 시스템은 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열을 포함하는 특수한 사전을 이용해 비밀번호를 검사합니다.

	LOM 활성화되지 않음	LOM 활성화됨, 관리자 사용자
비밀번호 강도 확인 해제	비밀번호는 관리자가 사용자에 대해 설정한 최소 문자 수 이상을 포함해야 합니다. (자세한 내용은 내부 사용자 추가, 55 페이지를 참조해 주십시오.)	비밀번호는 다음을 포함해야 합니다. • 8~20개 사이의 문자(MC 1000, MC 2500, MC 4500의 경우 상한은 20자가 아닌 14자입니다.) • 다음 4개 범주 중 3개 이상의 문자: • 대문자 • 소문자 • 숫자 • 특수 문자(! @ # * - _ + 등) 특수 문자 규칙은 물리적 FMC 시리즈에 따라 다릅니다. 아래 마지막 글머리 기호에 나열된 특수 문자만 선택하는 방법을 권장합니다. 비밀번호에는 사용자 이름을 포함하지 마십시오.

FMC용 사용자 계정 지침 및 제한 사항

기본값

- FMC는 모든 형태의 액세스에 대해 로컬 사용자 계정으로 관리자 사용자를 포함합니다. 관리자 사용자를 삭제할 수 없습니다. 기본 초기 비밀번호는 **Admin123**입니다. 시스템은 초기화 프로세스 중에 비밀번호를 변경하게 합니다. 시스템 초기화에 관한 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오.
- 기본적으로 다음 설정이 FMC의 모든 사용자 어카운트에 적용됩니다.
  - 비밀번호 재사용에는 제한이 없습니다.
  - 시스템은 성공한 로그인을 추적하지 않습니다.
  - 시스템에서 잘못된 로그인 크리덴셜을 입력한 사용자에 대해 시간이 정해진 임시 잠금을 강제 적용하지 않습니다.
  - 동시에 열 수 있는 읽기 전용 및 읽기/쓰기 세션 수에 대한 사용자 정의 제한은 없습니다.

  모든 사용자에 대한 이러한 설정을 시스템 구성으로 변경할 수 있습니다. (**System(**시스템**)** > **Configuration(**설정**)** > **User Configuration(**사용자 설정**))** 전역 사용자 구성, 1385 페이지를 참조하십시오.

FMC 사용자 계정 요구 사항 및 사전 요건

모델 지원

FMC

지원되는 도메인

- SSO 구성 - 전역 전용.
- 기타 모든 기능 - 모두.

사용자 역할

- SSO 구성 - 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다.
- 기타 모든 기능 - 관리자 역할의 모든 사용자
- LADP로 CAC(Common Access Card) 인증 구성, 72 페이지에서는 Network Admin(네트워크 관리자) 역할도 지원합니다.

내부 사용자 추가

이 절차에서는 FMC에 대한 사용자 지정 내부 사용자 계정을 추가하는 방법을 설명합니다.

System(시스템**)** > **Users(**사용자**)** > **Users(**사용자**)**에는 사용자가 LDAP 또는 RADIUS 인증을 통해 로그인할 때 수동으로 추가한 내부 사용자와 자동으로 추가된 외부 사용자가 모두 표시됩니다. 외부 사용자의 경우 더 높은 권한이 있는 역할을 할당하면 이 화면에서 사용자 역할을 수정할 수 있지만 비밀번호 설정은 수정할 수 없습니다.

FMC의 다중 도메인 구축에서 사용자는 생성된 도메인에서만 표시될 수 있습니다. 글로벌 도메인에서 사용자를 추가한 다음, 리프 도메인에 사용자 역할을 할당하는 경우 사용자가 리프 도메인에 "속하는" 경우에도 해당 사용자는 추가된 전역 **Users(**사용자**)** 페이지에 계속해서 표시됩니다.

디바이스에서 보안 인증 컴플라이언스 또는 LOM(Lights-Out Management)을 활성화하면 다른 비밀번호 제한이 적용됩니다. 보안 인증 컴플라이언스에 대한 자세한 내용은 보안 인증 컴플라이언스, 1469 페이지의 내용을 참조하십시오.

리프 도메인에서 사용자를 추가하면 해당 사용자는 글로벌 도메인에서 표시되지 않습니다.

참고 여러 관리자 사용자가 동시에 FMC에서 새 사용자를 생성하지 않도록 하십시오. 사용자 데이터베이스 액세스 충돌로 인해 오류가 발생할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**을 선택합니다.

단계 **2** **Create User**(사용자 생성)를 클릭합니다.

단계 **3** **User Name(**사용자 이름**)**을 입력합니다.

사용자 이름은 다음 제한 사항을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-), 밑줄(_) 및 마침표(.).
- 문자는 대문자 또는 소문자일 수 있습니다.
- 하이픈(-), 밑줄(_) 및 마침표(.) 이외의 특수 문자 또는 문장 부호를 포함할 수 없습니다.

단계 **4** **Real Name(**실명**)**: 계정이 속한 사용자 또는 부서를 식별하기 위한 설명 정보를 입력합니다.

단계 **5** **Use External Authentication Method(**외부 인증 방법 사용**)** 확인란은 LDAP 또는 RADIUS를 통해 로그인할 때 자동으로 추가된 사용자를 대상으로 확인됩니다. 외부 사용자를 사전 구성할 필요가 없으므로 이 필드를 무시할 수 있습니다. 외부 사용자의 경우 확인란을 선택 취소하여 이 사용자를 내부 사용자로 되돌릴 수 있습니다.

단계 **6** **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 값을 입력합니다.

값은 이 사용자에게 설정한 비밀번호 옵션을 준수해야 합니다.

단계 **7** **Maximum Number of Failed Logins(**최대 실패 로그인 시도 횟수**)**를 설정합니다.

공백 없이 정수를 입력하여 각 사용자가 로그인에 실패한 후 어카운트가 잠길 때까지 로그인을 시도할 수 있는 최대 횟수를 지정합니다. 기본 설정은 5회입니다. **0**을 사용하면 로그인 실패 횟수의 제한이 사라집니다. 관리자 어카운트는 보안 인증 컴플라이언스를 활성화한 경우를 제외하고 실패한 로그인의 최대 수 이후에 잠금에서 제외됩니다.

단계 **8** **Minimum Password Length(**최소 비밀번호 길이**)**를 설정합니다.

공백 없이 정수를 입력하여 사용자 비밀번호의 최소 길이를 글자 수로 지정합니다. 기본 설정은 **8**입니다. 값이 **0**이면 최소 길이 제한이 없습니다.

단계 **9** **Days Until Password Expiration(**비밀번호 만료 시까지의 일수**)**을 설정합니다.

여기에 입력한 일수가 지나면 사용자의 비밀번호가 만료됩니다. 기본 설정은 **0**이며, 이렇게 하면 비밀번호가 만료되지 않습니다. 기본값에서 변경하는 경우, 사용자 목록의 **Password Lifetime(**비밀번호 수명**)** 열에는 각 사용자의 비밀번호에서 남아 있는 일수가 나타납니다.

단계 **10** **Days Before Password Expiration Warning(**비밀번호 만료 경고까지 남은 일수**)**을 설정합니다.

비밀번호가 만료되기 전에 사용자에게 비밀번호를 변경하게 하는 경고 일수를 입력합니다. 기본 설정은 **0**일입니다.

단계 **11** 사용자 **Options(**옵션**)**를 설정합니다.

- **Force Password Reset on Login(**로그인 시 비밀번호 재설정 강제 실행**)** - 사용자가 다음에 로그인할 때 비밀번호를 변경하도록 강제 실행합니다.

- **Check Password Strength(**비밀번호 보안 수준 확인**)** - 강력한 비밀번호가 필요합니다. 비밀번호 강도 확인을 활성화하면, 비밀번호는 사용자 암호, 52 페이지에서 설명하는 강력한 비밀번호 요구 사항을 준수해야 합니다.
- **Exempt from Browser Session Timeout(**브라우저 세션 시간 초과에서 제외**)** - 사용자의 로그인 세션이 비활성화로 인한 종료에서 제외됩니다. 관리자 역할의 사용자는 면제받을 수 없습니다.

단계 **12** **User Role Configuration(**사용자 역할 구성**)** 영역에서 사용자 역할을 할당합니다. 사용자 역할에 대한 자세한 내용은 웹 인터페이스의 사용자 역할 맞춤화, 127 페이지의 내용을 참조하십시오.

외부 사용자의 경우, 사용자 역할이 그룹 구성원 자격(LDAP)을 통해 할당되거나 사용자 속성(RADIUS)을 기반으로 할당되면 최소 액세스 권한을 제거할 수 없습니다. 단, 추가 권한은 할당할 수 있습니다. 사용자 역할이 디바이스에서 설정하는 기본 사용자 역할인 경우, 제한 없이 사용자 어카운트에서 역할을 수정할 수 있습니다. 사용자 역할을 수정하는 경우 **Users(**사용자**)** 탭의 **Authentication Method(**인증 방법**)** 열에 **External - Locally Modified(**외부 - 로컬로 수정됨**)** 상태가 나타납니다.

표시되는 옵션은 디바이스가 단일 도메인 또는 다중 도메인 구축에 있는지 여부에 따라 달라집니다.

- 단일 도메인 - 사용자를 할당할 사용자 역할을 선택합니다.
- 다중 도메인 — 다중 도메인 구축에서 관리자 액세스 권한이 할당된 모든 도메인에서 사용자 계정을 생성할 수 있습니다. 사용자는 각 도메인에서 다른 권한을 가질 수 있습니다. 상위 도메인 및 하위 도메인 모두에서 사용자 역할을 할당할 수 있습니다. 예를 들어 글로벌 도메인에서 사용자에게 읽기 전용 권한을 할당할 수 있지만 하위 도메인에서는 관리자 권한을 할당할 수 있습니다. 다음 단계를 참조하십시오.
  1. **Add Domain(**도메인 추가**)**을 클릭합니다.
  2. **Domain(**도메인**)** 드롭다운 목록에서 도메인을 선택합니다.
  3. 사용자를 할당할 사용자 역할을 선택합니다.
  4. **Save(**저장**)**를 클릭합니다.

단계 **13** (선택 사항, 물리적 FMC의 경우에만 해당됨) 사용자에게 관리자 역할을 할당한 경우, 관리자 옵션이 나타납니다. **Allow Lights-Out Management Access(Lights-Out Management** 액세스 허용**)**를 선택하여 사용자에게 Lights-Out Management 액세스 권한을 부여할 수 있습니다. Lights-Out Management에 대한 자세한 내용은 LOM(Lights-Out Management) 개요, 1394 페이지의 내용을 참조하십시오.

단계 **14** **Save(**저장**)**를 클릭합니다.

외부 인증 구성

외부 인증을 활성화하려면 하나 이상의 외부 인증 개체를 추가해야 합니다.

외부 인증 정보

외부 인증을 활성화하는 경우, 외부 인증 개체에 지정된 대로 FMC에서 LDAP 또는 RADIUS 서버로 사용자 자격 증명을 확인합니다.

웹 인터페이스 액세스를 위한 여러 외부 인증 개체를 구성할 수 있습니다. 예를 들어 외부 인증 개체가 5개인 경우, 그러한 개체에서 사용자는 웹 인터페이스 액세스를 인증받을 수 있습니다. CLI 액세스는 외부 인증 개체를 하나만 사용할 수 있습니다. 외부 인증 개체를 하나 이상 활성화하는 경우, 사용자는 목록에서 첫 번째 개체로만 인증할 수 있습니다.

외부 인증 개체는 FMC 및 FTD 디바이스가 사용할 수 있습니다. 다양한 어플라이언스/디바이스 유형 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다.

참고 시간 제한 범위는 FTD와 FMC가 다르므로 개체를 공유할 때는 FTD의 더 적은 시간 제한 범위(LDAP의 경우 1~30초, RADIUS의 경우 1~300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD 외부 인증 설정이 작동하지 않습니다.

FMC의 경우, 외부 인증 객체를 **System(**시스템**)** > **User(**사용자**)** > **External Authentication(**외부 인증**)** 탭에서 직접 활성화합니다. 이 설정은 FMC 사용에만 영향을 주며 매니지드 디바이스 사용에 대해 이 탭에서 활성화할 필요는 없습니다. FTD 디바이스의 경우, 디바이스에 구축하는 플랫폼 설정에서 외부 인증 객체를 활성화해야 합니다.

웹 인터페이스 사용자는 내부 인증 개체에 있는 CLI 사용자와 별개로 정의됩니다. RADIUS의 CLI 사용자의 경우, 외부 인증 개체의 RADIUS 사용자 이름목록을 사전 구성해야 합니다. LDAP의 경우, 필터를 지정하여 LDAP 서버의 CLI 사용자와 매칭할 수 있습니다.

CAC 인증을 위해 구성된 CLI 액세스를 위한 LDAP 개체를 사용할 수 없습니다.

참고 Linux 셸 액세스 권한이 있는 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 다음을 확인하십시오.

- Linux 셸 액세스 권한이 있는 사용자 목록 제한
- Linux 셸 사용자를 생성 금지

LDAP 정보

LDAP(Lightweight Directory Access Protocol)를 사용하면 중앙의 한 위치에 개체(예: 사용자 크리덴셜)를 조직하는 네트워크에서 디렉토리를 설정할 수 있습니다. 그러면 여러 애플리케이션에서 이 크리덴셜 및 크리덴셜 설명에 사용된 정보에 액세스할 수 있습니다. 사용자 크리덴셜을 변경해야 하는 경우, 한 곳에서 변경할 수 있습니다.

Microsoft는 Active Directory 서버가 2020년에 LDAP 바인딩 및 LDAP 서명을 시행할 것이라고 발표했습니다. Microsoft는 이러한 설정을 기본 설정으로 사용할 때 Microsoft Windows에 권한 상승 취약점이 존재하여 MITM(man-in-the-middle) 공격자가 Windows LDAP 서버에 인증 요청을 성공적으로 전

달할 수 있기 때문에 이러한 요구 사항을 적용하고 있습니다. 자세한 내용은 Microwoft 지원 사이트에서 2020 LDAP 채널 바인딩 및 Windows용 LDAP 서명 요구 사항을 참조하십시오.

아직 수행하지 않은 경우 TLS/SSL 암호화를 사용하여 Active Directory 서버에서 인증을 시작하는 것이 좋습니다.

RADIUS 정보

RADIUS(Remote Authentication Dial In User Service)는 네트워크 리소스에 대한 사용자 액세스의 인증, 권한 부여, 어카운팅에 사용되는 인증 프로토콜입니다. RFC 2865를 준수하는 모든 RADIUS 서버에 대해 인증 개체를 생성할 수 있습니다.

Firepower 디바이스는 SecurID 토큰 사용을 지원합니다. SecurID를 사용하여 서버에서 인증을 구성하는 경우, 해당 서버에서 인증된 사용자는 SecurID PIN 끝에 SecurID 토큰을 추가하고 이를 로그인 비밀번호로 사용합니다. SecurID를 지원하기 위해 Firepower 디바이스에서 추가로 구성할 사항은 없습니다.

FMC에 대한 LDAP 외부 인증 개체 추가

LDAP 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

시작하기 전에

- 해당 장치에서 도메인 이름 조회를 위해 DNS 서버를 지정해야 합니다. 이 절차에서 IP 주소는 지정하고 LDAP 서버에 대한 호스트 이름은 지정하지 않더라도, LDAP 서버는 인증을 위한 URI를 반환할 수 있으며 여기에는 호스트 이름이 포함됩니다. 호스트 이름을 지정하려면 DNS 조회가 필요합니다. FMC 관리 인터페이스 수정, 1358 페이지를 참조하고 DNS 서버를 추가합니다.
- CAC 인증과 함께 사용할 LDAP 인증 개체를 구성하는 경우 컴퓨터에 삽입된 AC를 제거해서는 안 됩니다. 사용자 인증서를 활성화한 다음에는 항상 CAC가 삽입된 상태여야 합니다.

프로시저

단계 1 **System**(시스템) > **Users**(사용자)을 선택합니다.

단계 2 **External Authentication**(외부 인증) 탭을 클릭합니다.

단계 3 **Add External Authentication Object**(외부 인증 개체 추가)를 클릭합니다.

단계 4 **Authentication Method**(인증 방법)을 **LDAP**로 설정합니다.

단계 5 (선택 사항) CAC 인증 및 권한 부여에 이 인증 개체를 사용하려는 경우 **CAC** 확인란을 선택할 수도 있습니다.

CAC 인증 및 권한 부여를 전부 구성하려면 LADP로 CAC(Common Access Card) 인증 구성, 72 페이지에 있는 절차를 따라야 합니다. 이 개체는 CLI 사용자에게는 사용할 수 없습니다.

단계 6 **Name**(이름)과 **Description**(설명)(선택 사항)을 입력합니다.

단계 **7** 드롭다운 목록에서 **Server Type(**서버 유형**)**을 선택합니다.

팁 **Set Defaults(**기본 설정**)**을 클릭하면 디바이스가 **User Name Template(**사용자 이름 템플릿**)**, **UI Access Attribute(UI** 액세스 속성**)**, **CLI Access Attribute(CLI** 액세스 속성**)**, **Group Member Attribute(**그룹 구성원 속성**)** 및 **Group Member URL Attribute(**그룹 구성원 **URL** 속성**)** 필드를 서버 유형의 기본값으로 채웁니다.

단계 **8** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

단계 **9** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **10** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **11** **LDAP-Specific Parameters(LDAP** 전용 파라미터**)**를 입력합니다.

a) 액세스를 원하는 LDAP 디렉터리에 대해 **Base DNs(**기본 **DN)**를 입력합니다. 예를 들어, 예시 회사의 보안 조직에서 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다. 아니면 **Fetch DN(DN** 가져오기**)**을 클릭하고, 드롭다운 목록에서 적절한 기본 고유 이름을 선택합니다.

b) (선택 사항) **Base Filter(**기본 필터**)**를 입력합니다. 예를 들어 디렉토리 트리의 사용자 개체에 `physicalDeliveryOfficeName` 속성이 있고 a뉴욕 사무실의 사용자는 그 속성 값이 `NewYork`인 경우 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.

CAC 인증을 사용하는 경우 활성 사용자 계정만 필터링하려면(비활성화된 사용자 계정 제외) `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`를 입력합니다. 이 기준은 `ldpgrp` 그룹에 속하는 AD 내에서 사용자 계정을 검색하며 `userAccountControl` 속성 값이 `2`(비활성화됨)가 아닙니다.

c) LDAP 서버를 검색하기에 크리덴셜이 충분한 사용자의 경우, **User Name(**사용자 이름**)**을 입력합니다. 예를 들어 OpenLDAP 서버에 연결하려는 경우, 해당 사용자 개체에 `uid` 속성이 있으며 예시 회사 보안 부서 관리자 개체의 `uid`값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.

d) **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 사용자 비밀번호를 입력합니다.

e) (선택 사항) **Show Advanced Options(**고급 옵션 표시**)**를 클릭하고 다음 고급 옵션을 구성합니다.

- **Encryption(**암호화**)- None (**해당 없음**)**, **TLS**또는 **SSL**을 클릭 합니다.

  포트를 지정한 다음 암호화 방식을 변경할 경우, 그 방법에 대해서는 포트가 기본값으로 재설정됩니다. **None(**해당 없음**)** 또는 **TLS**인 경우, 포트는 기본값인 389로 재설정됩니다. SSL 암호화를 선택할 경우 포트는 636로 재설정됩니다.

- **SSL Certificate Upload Path(SSL** 인증서 업로드 경로**)**—SSL 또는 TLS 암호화인 경우, **Choose File(**파일 선택**)**을 클릭하여 인증서를 선택해야 합니다.

  이전에 업로드한 인증서를 대체하려는 경우, 새 인증서를 업로드하고 구성을 디바이스에 다시 적용하여 새 인증서로 복사합니다.

  참고 TLS 암호화는 모든 플랫폼에서 인증서가 필요합니다. 항상 끼어들기 공격을 방지하기 위해 SSL에 대한 인증서를 업로드하는 것이 좋습니다.

- **User Name Template(**사용자 이름 템플릿**)**— **UI Access Attribute(UI** 액세스 속성**)**에 해당하는 템플릿을 제공합니다. 예를 들어 예시 회사의 보안 조직에서 근무하는 모든 사용자를 인증하기 위해 UI 액세스 속성이 `uid`인 OpenLDP 서버에 연결하는 경우, `uid=%s,ou=security,dc=example,dc=com`를 **User Name Template(**사용자 이름 템플릿**)** 필드에 입력합니다. Microsoft Active Directory 서버에서는 `%s@security.example.com`이라고 입력할 수 있습니다.

  이 필드는 CAC 인증을 위해 필요합니다.

- **Timeout(**시간 초과**)**—백업 연결로 전환하기 전 시간(초)을 1과 1024 사이로 입력합니다. 기본값은 30입니다.

  참고 시간 초과 범위는 FTD와 FMC에 따라 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 초과 범위 (1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD LDAP 컨피그레이션이 작동하지 않습니다.

단계 **12** (선택 사항) **Attribute Mapping(**속성 매핑**)**을 구성하고 속성에 따라 사용자를 검색합니다.

- **UI Access Attribute(UI** 액세스 속성**)**을 입력하거나 **Fetch Attrs(**속성 가져오기**)**를 클릭하여 사용 가능한 속성 목록을 검색합니다. 예를 들어 Microsoft Active Directory Server의 경우 Active Directory Server 사용자 개체에 `uid` 속성이 없기 때문에 UI Access Attribute(UI 액세스 속성)를 사용하여 사용자를 검색할 수도 있습니다. 그 대신 `userPrincipalName` 속성을 검색할 수 있는데, `userPrincipalName`을 **UI Access Attribute(UI** 액세스 속성**)** 필드에 입력하면 됩니다.

  이 필드는 CAC 인증을 위해 필요합니다.

- 사용자 고유 유형 이외의 쉘(shell) 액세스 속성을 사용하려는 경우 **CLI Access Attribute(CLI** 액세스 속성**)**를 입력합니다. 예를 들어 Microsoft Active Directory Server에서 `sAMAccountName` CLI 액세스 속성을 사용하여 셸 액세스 사용자를 가져오려면 `sAMAccountName`을 입력합니다.

단계 **13** (선택 사항) **Group Controlled Access Roles(**그룹 제어 액세스 역할**)**를 구성합니다.

액세스 제어 그룹에 역할을 사용하여 사용자의 권한을 구성하지 않는 경우, 사용자는 외부 인증 정책에서 기본적으로 부여된 권한만 갖습니다.

a) (선택 사항) 사용자 역할에 해당하는 필드에 해당 역할이 부여되는 사용자를 포함하는 LDAP 그룹의 DN을 입력합니다.

   참조하는 모든 그룹이 LDAP 서버에 있어야 합니다. 고정 LDAP 그룹 또는 동적 LDAP 그룹을 참조할 수 있습니다. 고정 LDAP 그룹은 특정 사용자를 가리키는 그룹 개체 특성에 의해 멤버십이 결정되며, 동적 LDAP 그룹에서는 사용자 개체 특성에 따라 그룹 사용자를 가져오는 LDAP 검색을 생성하여 멤버십을 결정합니다. 어떤 역할에 대한 그룹 액세스 권한은 그룹의 멤버인 사용자에게만 영향을 미칩니다.

   동적 그룹을 사용하는 경우 LDAP 서버에 구성된 대로 LDAP 쿼리가 사용됩니다. 이런 이유로 Firepower 디바이스는 검색 반복 횟수를 4회로 제한하여 검색 구문 오류로 인한 무한 루프를 방지합니다.

   예제:

Administrator(관리자**)** 필드에 다음과 같이 입력하여 예시 회사의 정보 기술 조직에서 이름을 인증할 수 있습니다.

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

c) 정적 그룹을 사용하는 경우, **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다.

예제**:**

기본 Security Analyst 액세스에 대한 고정 그룹의 멤버십을 표시하기 위해 `member(멤버)` 속성을 사용하는 경우 `member(멤버)`라고 입력합니다.

d) 동적 그룹을 사용하는 경우, **Group Member URL Attribute(**그룹 멤버 **URL** 속성**)**을 입력합니다.

예제**:**

`memberURL` 속성이 기본 관리자 액세스에 대해 지정한 동적 그룹의 멤버를 가져오는 LDAP 검색을 포함할 경우 `memberURL`이라고 입력합니다.

사용자의 역할을 변경하는 경우, 변경된 외부 인증 개체는 저장/배포하고 **Users(**사용자**)** 화면에서 해당 사용자를 제거해야 합니다. 이 사용자는 다음 로그인 시 자동으로 재추가됩니다.

단계 **14** (선택 사항) CLI 사용자를 허용하도록 **CLI Access Filter(CLI** 액세스 필터**)**를 설정합니다.

CLI 액세스에 대해 LDAP 인증을 하지 않으려면 이 필드를 비워 둡니다. CLI 사용자를 지정하려면 다음 방법 중 하나를 선택합니다.

- 인증 설정을 구성할 때 지정한 것과 동일한 필터를 사용하려면 **Same as Base Filter(**기본 필터와 동일**)**를 선택합니다.
- 속성 값에 따라 관리자 사용자 엔트리를 검색하려면 속성 이름, 비교 연산자, 필터로 사용할 속성 값을 괄호로 묶어 입력합니다. 예를 들어 모든 네트워크 관리자에게 `manager` 속성이 있고 그 값이 `shell`이라면 `(manager=shell)`이라는 기본 필터를 설정할 수 있습니다.

사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

참고 **CLI Access Filter(CLI** 액세스 필터**)**에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 만들지 마십시오. 내부 FMC 사용자만 관리자여야 합니다. **CLI Access Filter(CLI** 액세스 필터**)**에 관리자를 포함하지 마십시오.

단계 **15** (선택 사항) **Test(**테스트**)**를 클릭하고 LDAP 서버와의 연결을 테스트합니다.

테스트 출력에서는 유효한 사용자 이름과 유효하지 않은 사용자 이름을 나열합니다. 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-), 영숫자를 포함할 수 있습니다. 1,000명이 넘는 사용자로 서버와의 연결을 테스트할 경우 UI 페이지 크기 제한 때문에 1,000명의 사용자만 반환됩니다. 테스트에 실패하는 경우 LDAP 인증 연결 문제 해결, 132 페이지을 참조하십시오.

단계 **16** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수도 있습니다. **User Name(**사용자 이름**)** `uid` 및 **Password(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

Microsoft Active Directory Server에 연결하는 경우 `uid` 대신 UI 액세스 속성을 제공했다면 해당 속성의 값을 사용자 이름으로 사용합니다. 해당 사용자의 정규화된 DN을 지정할 수도 있습니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제**:**

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

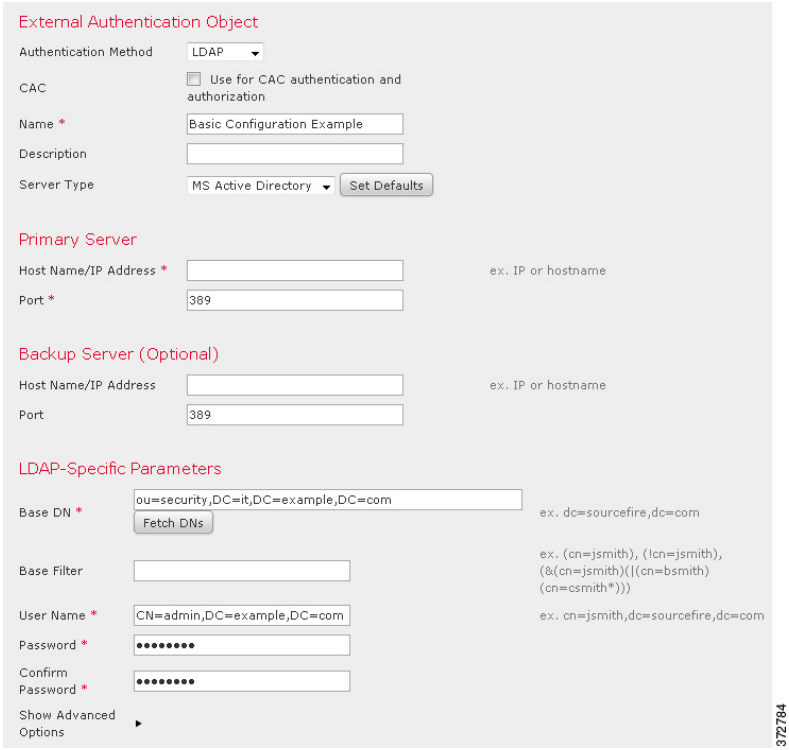
단계 **17** **Save(**저장**)**를 클릭합니다.

단계 **18** 이 서버의 사용을 활성화합니다. FMC 사용자에 대한 외부 인증 활성화, 71 페이지를 참조하십시오.

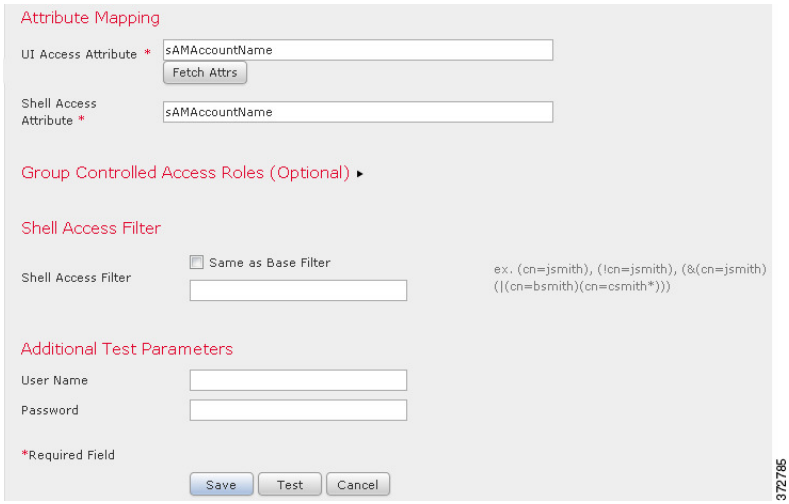
예

기본 예시

다음 그림은 Microsoft Active Directory Server를 위한 LDAP 로그인 인증 개체의 기본 구성입니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 389을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다.



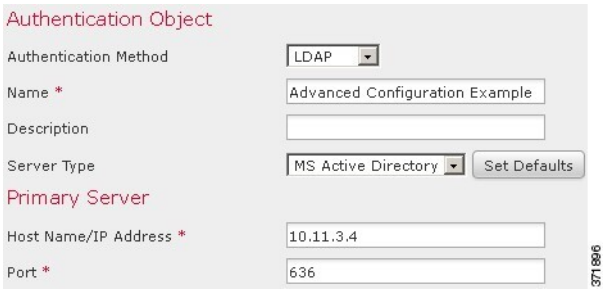
그러나 이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. MS Active Directory Server 유형을 선택하고 **Set Defaults(**기본값 설정**)**을 클릭하면 UI Access Attribute(UI 액세스 속성)이 `sAMAccountName`으로 설정됩니다. 이에 따라 Firepower System에서는 사용자가 Firepower System에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

또한 Shell Access Attribute(셸 액세스 속성)가 `sAMAccountName`이면 사용자가 어플라이언스의 CLI 계정에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

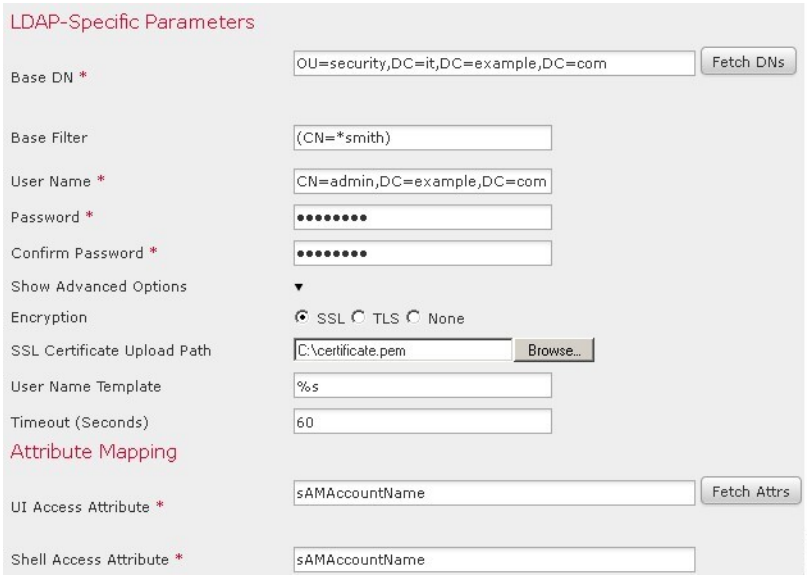
이 서버에는 기본 필터가 적용되지 않으므로 Firepower System에서는 기본 DN이 나타내는 디렉토리의 모든 개체에 대해 특성을 검사합니다. 기본 기간(또는 LDAP 서버에 설정된 시간 초과 기간)이 경과하면 서버와의 연결이 시간 초과됩니다.

고급 예시

이 예에서는 Microsoft Active Directory Server에 대한 LDAP 로그인 인증 개체의 고급 구성을 보여줍니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 636을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다. 그러나 이 서버는 기본 필터 `(cn=*smith)`가 있습니다. 이 필터는 CN이 `smith`로 끝나는 사용자만 서버에서 가져오도록 제한합니다.

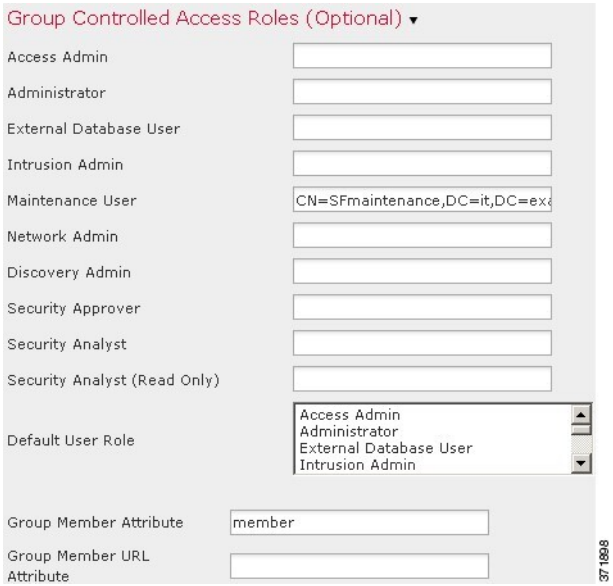


서버와의 연결은 SSL로 암호화되고 `certificate.pem`이라는 인증서가 연결에 사용됩니다. 또한 **Timeout(**시간 초과**)** 설정 때문에 60초가 지나면 서버와의 연결이 시간 초과됩니다.

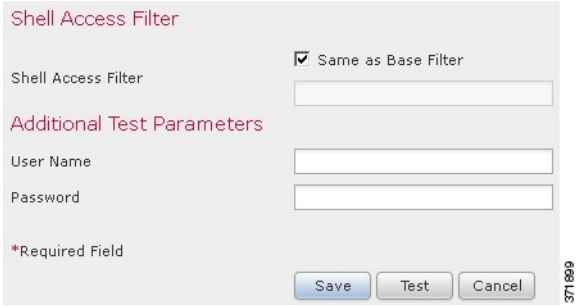
이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. 구성에 `sAMAccountName`이라는 UI Access Attribute(UI 액세스 속성)가 포함되어 있습니다. 이에 따라 Firepower System에서는 사용자가 Firepower System에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

또한 Shell Access Attribute(셸 액세스 속성)가 `sAMAccountName`이면 사용자가 어플라이언스의 CLI 계정에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

여기에는 그룹 설정도 포함되어 있습니다. `member` 그룹 속성과 `CN=SFmaintenance,DC=it,DC=example,DC=com`이라는 기본 도메인 이름을 갖는 그룹의 모든 멤버에게 Maintenance User(유지 보수 사용자) 역할이 자동으로 지정됩니다.



셸 액세스 필터는 기본 필터와 동일하게 설정되므로, 동일한 사용자가 웹 인터페이스뿐 아니라 CLI를 통해서도 어플라이언스에 액세스할 수 있습니다.



FMC에 대한 RADIUS 외부 인증 개체 추가

RADIUS 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 **2** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **3** **Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **4** **Authentication Method(**인증 방법**)**을 **RADIUS**로 설정합니다.

단계 **5** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **6** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

단계 **7** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **8** **RADIUS Secret Key(RADIUS** 비밀 키**)**를 입력합니다.

단계 **9** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **10** (선택 사항) **RADIUS-Specific Parameters(RADUIS** 특정 파라미터**)**를 입력합니다.

a) **Timeout(**시간 초과**)**을 초 단위(1~1024)로 입력하고 기본 서버를 다시 시도합니다. 기본값은 30입니다.

참고 시간 제한 범위는 FTD와 FMC에서 서로 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위(1 ~ 300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD RADIUS 컨피그레이션이 작동하지 않습니다.

b) **Retries(**재시도**)**를 입력하고 백업 서버로 이동합니다. 기본값은 3입니다.

c) 사용자 역할에 해당하는 필드에 각 사용자의 이름을 입력하거나 해당 역할에 지정될 식별 특성-값 쌍을 입력합니다.

사용자 이름과 속성-값 쌍은 쉼표로 구분합니다.

예제**:**

보안 분석가인 모든 사용자가 `Analyst(분석가)`를 `User-Category(사용자-카테고리)` 속성 값으로 갖는 경우, `User-Category=Analyst`를 **Security Analyst(**보안 분석가 목록**)** 필드에 입력하고 해당 사용자에게 해당 역할을 부여할 수 있습니다.

예제**:**

Administrator(관리자) 역할을 사용자인`jsmith`와 `jdoe`에게 부여하려면 `jsmith, jdoe`를 **Administrator(**관리자**)** 필드에 입력합니다.

예제**:**

Maintenance User(유지 보수 사용자) 역할을 `User-Category(사용자-카테고리)` 값이 `Maintenance(유지 보수)`인 모든 사용자에게 부여하려면 `User-Category=Maintenance`를 **Maintenance User(**유지 보수 사용자**)** 필드에 입력합니다.

d) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

사용자의 역할을 변경하는 경우, 변경된 외부 인증 개체는 저장/배포하고 **Users(**사용자**)** 화면에서 해당 사용자를 제거해야 합니다. 이 사용자는 다음 로그인 시 자동으로 재추가됩니다.

단계 **11** (선택 사항) **Define Custom RADIUS Attributes(**맞춤형 **RADIUS** 속성 정의**)**.

RADIUS 서버가 `/etc/radiusclient`의 `dictionary` 파일에 없는 속성의 값을 반환할 경우, 이러한 속성을 사용하여 해당 속성을 갖는 사용자에 대한 역할을 설정하려면 그러한 속성을 정의해야 합니다. RADIUS 서버에서 사용자 프로파일을 확인하여 사용자에 대해 반환되는 속성을 찾을 수 있습니다.

a) **Attribute Name(**속성 이름**)**을 입력합니다.

속성을 정의할 때 영숫자로 구성된 속성의 이름을 제공합니다. 속성 이름의 단어는 공백이 아닌 대시로 구분해야 합니다.

b) 정수로 **Attribute ID(**속성 **ID)**를 입력합니다.

속성 ID는 정수이며 `etc/radiusclient/dictionary` 파일에 있는 기존 속성 ID와 충돌해서는 안 됩니다.

c) **Attribute Type(**속성 유형**)** 드롭다운 목록에서 선택합니다.

속성의 유형을 문자열, IP 주소, 정수 또는 날짜로 지정합니다.

d) **Add(**추가**)**를 클릭하고 맞춤형 속성을 추가합니다.

RADIUS 인증 개체를 생성하는 경우 해당 개체에 대한 새로운 사전 파일이 `/var/sf/userauth` 디렉토리에 있는 디바이스에 생성됩니다. 추가하는 모든 맞춤형 속성은 사전 파일에 추가됩니다.

예제**:**

RADIUS 서버가 Cisco 라우터가 있는 네트워크에서 사용되는 경우 `Ascend-Assign-IP-Pool` 속성을 사용하여 특정 IP 주소 풀에서 로그인한 모든 사용자에게 특정 역할을 부여할 수 있습니다. `Ascend-Assign-IP-Pool`은 정수 속성으로서 사용자가 로그인할 수 있는 주소 풀을 정의합니다. 여기서 정수는 지정된 IP 주소 풀의 번호를 나타냅니다.

맞춤형 속성을 표시하려면 속성 이름 `Ascend-IP-Pool-Definition`, 속성 ID `218`, 속성 유형 `integer`로 맞춤형 속성을 생성합니다.

그런 다음 `Ascend-Assign-IP-Pool=2`를 **Security Analyst (Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력하여 `Ascend-IP-Pool-Definition` 속성의 값이 `2`인 모든 사용자에게 읽기 전용 보안 분석가 권한을 부여할 수 있습니다.

단계 **12** (선택 사항) **CLI Access Filter(CLI** 액세스 필터**)** 영역 **Administrator CLI Access User List(**관리자 **CLI** 액세스 사용자 목록**)** 필드에 CLI 액세스 권한이 있어야 하는 사용자 이름을 쉼표로 구분하여 입력합니다.

이러한 사용자 이름은 RADIUS 서버의 사용자 이름과 일치해야 합니다. 이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

CLI 액세스에 대해 RADIUS 인증을 하지 않으려면 이 필드를 비워 둡니다.

참고 셸 액세스 필터에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 모두 제거합니다. FMC에서는 내부 CLI 사용자만 관리자이니, 관리자 외부 사용자를 생성하지 마십시오.

단계 **13** (선택 사항) **Test(**테스트**)**를 클릭해 RADIUS 서버와 FMC 연결을 테스트합니다.

단계 **14** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수 있습니다. **User Name(**사용자 이름**)** 및 **Passowrd(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제:

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

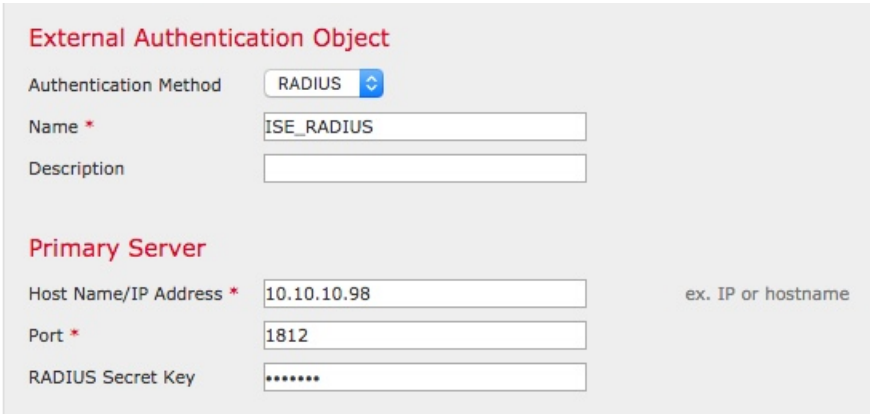
단계 **15** **Save(**저장**)**를 클릭합니다.

단계 **16** 이 서버의 사용을 활성화합니다. FMC 사용자에 대한 외부 인증 활성화, 71 페이지를 참조하십시오.

예

단순한 사용자 역할 할당

다음 그림은 포트 1812에서 IP 주소 10.10.10.98을 사용하여 Cisco ISE(Identity Services Engine)를 실행하는 서버를 위한 RADIUS 로그인 인증 개체의 예를 보여줍니다. 정의된 백업 서버가 없습니다.



다음 예는 RADIUS 관련 매개변수를 보여줍니다. 여기에는 시간 초과(30초) 및 Firepower System이 백업 서버에 연결을 시도하기 전 실패한 재시도 횟수(있는 경우)가 포함됩니다.

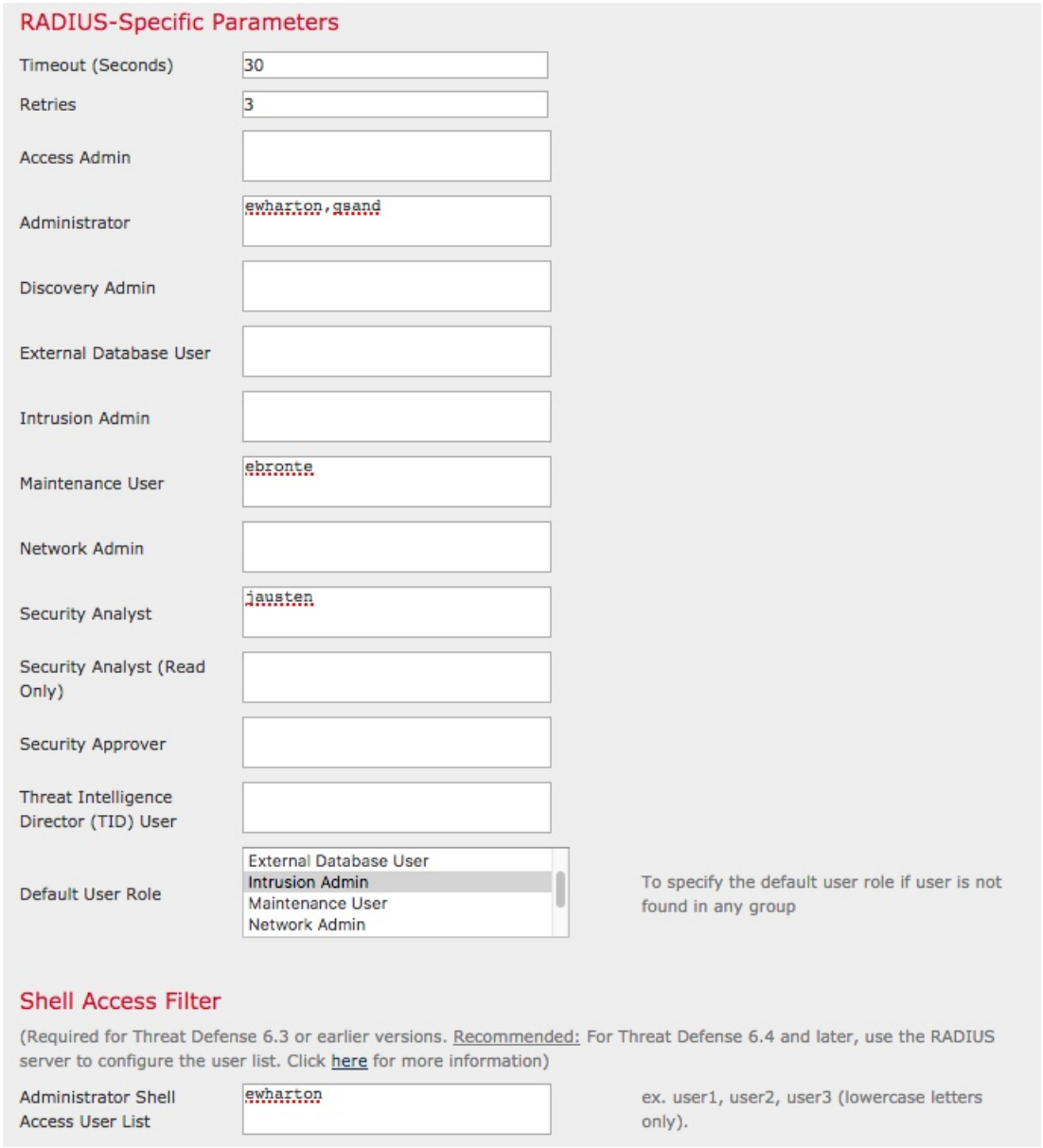
이 예에서는 RADIUS 사용자 역할 구성의 주요 측면을 보여줍니다.

사용자 `ewharton` 및 `gsand`에게 웹 인터페이스 Administrator(관리자) 액세스 권한이 주어집니다.

사용자 `cbronte`에게 웹 인터페이스 Maintenance User(유지 보수 사용자) 액세스 권한이 주어집니다.

사용자 `jausten`에게 웹 인터페이스 Security Analyst(보안 분석가) 액세스 권한이 주어집니다.

사용자 `ewharton`은 CLI 계정을 사용하여 디바이스에 로그인할 수 있습니다.



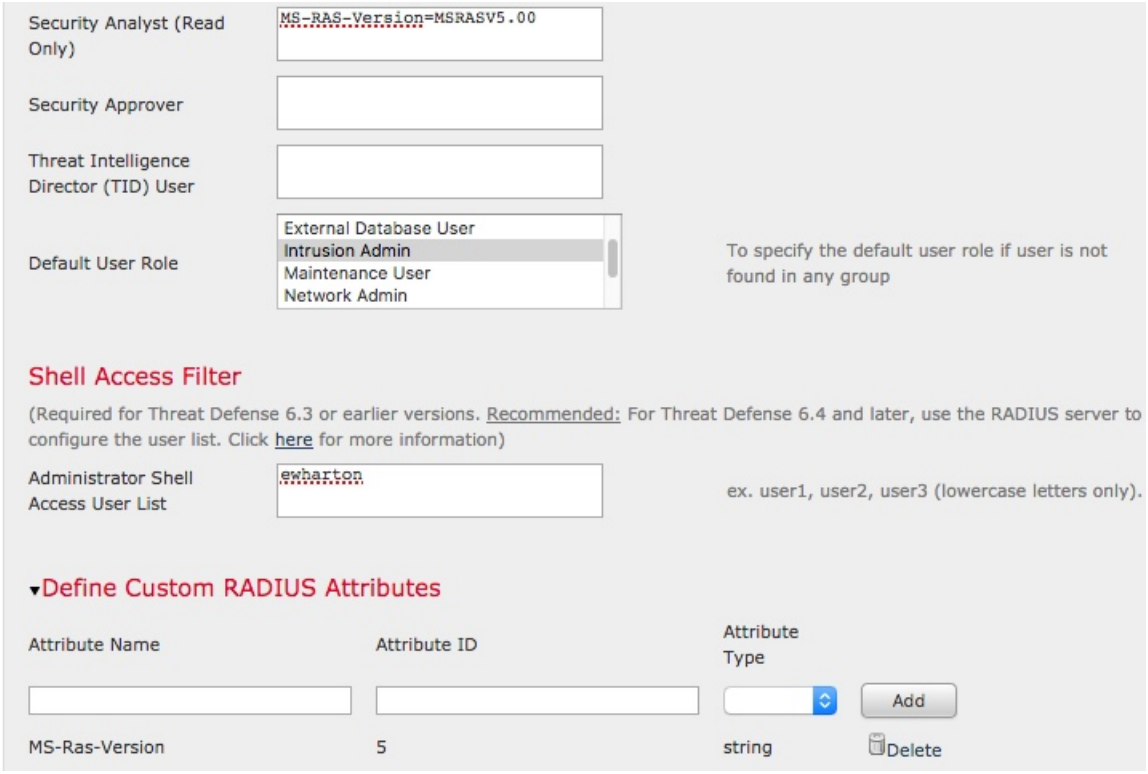
다음 그림은 이 예시에서의 역할 구성을 나타냅니다.

속성-값 쌍을 매칭하는 사용자의 역할

속성-값 쌍을 사용하여 특정 사용자 역할을 갖는 사용자를 식별할 수 있습니다. 사용하는 속성이 맞춤형 속성일 경우 해당 맞춤형 속성을 정의해야 합니다.

다음 그림은 이전의 예와 동일한 ISE 서버를 위한 샘플 RADIUS 로그인 인증 개체에 포함된 역할 설정 및 맞춤형 속성 정의를 보여줍니다.

그러나 여기서는 Microsoft 원격 액세스 서버가 사용 중이므로 `MS-RAS-Version` 맞춤형 속성 한 명 이상의 사용자에게 반환됩니다. 참고로 `MS-RAS-Version` 맞춤형 속성은 문자열입니다. 이 예에서는 Microsoft v. 5.00 원격 액세스 서버를 통해 RADIUS로 로그인하는 모든 사용자가 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 역할을 받아야 하므로 속성-값 쌍 `MS-RAS-Version= MSRASV5.00`을 **Security Analyst(Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력합니다.



FMC 사용자에 대한 외부 인증 활성화

관리 사용자에 대한 외부 인증을 활성화하는 경우, External Authentication(외부 인증) 개체에 지정된 대로 FMC이 LDAP 또는 RADIUS 서버로 사용자 크리덴셜을 확인합니다.

시작하기 전에

FMC에 대한 LDAP 외부 인증 개체 추가, 59 페이지 및 FMC에 대한 RADIUS 외부 인증 개체 추가, 66 페이지에 따라 외부 인증 개체를 1개 이상 추가합니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **3** 외부 웹 인터페이스 사용자에 대한 기본 사용자 역할을 설정합니다.

역할이 없는 사용자가 어떤 작업도 수행할 수 없습니다. 외부 인증 개체에 정의된 사용자 역할이 이 기본 사용자 역할보다 우선합니다.

a) **Default User Roles(**기본 사용자 역할**)** 값을 클릭합니다(기본적으로 none(해당 없음) 선택됨).

a) **Default User Role Configuration(**기본 사용자 역할 구성**)** 대화 상자에서 사용하려는 역할(복수 가능)을 선택합니다.

b) **Save(**저장**)**를 클릭합니다.

단계 **4** 사용하려는 각 외부 인증 개체 옆 슬라이더 활성화됨( )를 클릭합니다. 개체를 1개 이상 활성화하는 경우, 사용자가 지정된 순서대로 서버와 비교됩니다. 다음 단계를 참조하고 서버를 재정렬합니다.

셸 인증을 활성화 하는 경우에 셸 액세스 필터를 포함 하는 외부 인증 개체를 활성화 해야 합니다. 또한 CLI 액세스 사용자는 인증 개체가 목록에서 순위가 가장 높은 서버에 대해서만 인증할 수 있습니다.

단계 **5** (선택 사항) 인증 요청이 발생한 경우 서버를 드래그 앤 드롭하고 인증 순서를 변경합니다.

단계 **6** 외부 사용자에 대해 CLI 액세스를 허용하려면, **Shell Authentication(**셸 인증**)** > **Enabled(**활성화**)**를 선택합니다.

첫 번째 외부 인증 개체 이름이 **Enabled(**활성화**)** 옵션 옆에 표시되고 첫 번째 개체만 CLI 액세스에 사용된다고 알립니다.

단계 **7** **Save and Apply(**저장 및 적용**)**를 클릭합니다.

LADP로 CAC(Common Access Card) 인증 구성

조직에서 CAC(Common Access Card)를 사용할 경우, LDAP 인증을 설정하여 웹 인터페이스에 로그인하는 FMC 사용자를 인증할 수 있습니다. CAC 인증으로 사용자는 어플라이언스에 별도의 사용자 이름과 비밀번호를 제공하지 않고 곧바로 로그인할 수 있습니다.

CAC 인증 사용자는 EDIPI(electronic data interchange personal identifier) 번호로 식별됩니다.

24시간 동안 활동이 없는 경우, 디바이스가 CAC 인증 사용자를 **Users(**사용자**)** 탭에서 삭제합니다. 다음에 로그인할 때마다 사용자가 다시 추가되지만, 사용자 역할에 대한 수동 변경사항은 다시 구성해야 합니다.

시작하기 전에

CAC 컨피그레이션 프로세스의 일환으로 사용자 인증서를 활성화하려면 브라우저에 유효한 사용자 인증서(여기서는 CAC를 통해 브라우저에 전달된 인증서)가 반드시 있어야 합니다. CAC 인증 및 권한 부여를 구성하면 네트워크의 사용자는 브라우징 세션 내내 CAC 연결을 유지해야 합니다. 세션 중

에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

프로시저

단계 **1** 조직의 지침대로 CAC를 삽입합니다.

단계 **2** 브라우저에서 **https://***ipaddress_or_hostname*/로 이동합니다. 여기서*ipaddress* 또는 *hostname*은 사용자 디바이스와 일치합니다.

단계 **3** 메시지가 표시되면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

단계 **4** 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **5** Login(로그인) 페이지의 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에서 Administrator(관리자) 권한이 있는 사용자로 로그인합니다. 아직 CAC 크리덴셜을 사용하여 로그인 할 수 없습니다 .

단계 **6** **System** > **Users** > **External Authentication**(시스템 사용자 외부 인증)을 선택합니다.

단계 **7** FMC에 대한 LDAP 외부 인증 개체 추가, 59 페이지의 절차에 따라 CAC 전용 LDAP 인증 개체를 생성합니다. 다음 항목을 구성해야 합니다.

- **CAC** 확인란
- **LDAP-Specific Parameters(LDAP** 관련 매개변수**)** > **Show Advanced Options(**고급 옵션 표시**)** > **User Name Template(**사용자 이름 템플릿**)**
- **Attribute Mapping(**속성 매핑**)** > **UI Access Attribute(UI** 액세스 속성**)**

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** FMC 사용자에 대한 외부 인증 활성화, 71 페이지에 설명된 대로 외부 인증 및 CAC 인증을 활성화합니다.

단계 **10** **System(**시스템**)** > **Configuration(**구성**)**를 선택하고 **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **11** 필요하다면 HTTPS 서버 인증서 가져오기에 설명된 절차에 따라 HTTPS 서버 인증서를 가져옵니다.

사용하려는 CAC에서 동일한 CA(인증 기관)이 HTTPS 서버 인증서와 사용자 인증서를 발급해야 합니다.

단계 **12** **HTTPS User Certificate Settings(HTTPS** 사용자 인증서 설정**)**에서 **Enable User Certificates(**사용자 인증서 활성화**)**를 선택합니다. 자세한 내용은 유효한 HTTPS 클라이언트 인증서 필요를 참고하십시오.

단계 **13** CAC 크리덴셜로 Firepower Management Center에 로그인, 33 페이지에 따라 디바이스에 로그인합니다.

SAML SSO(Single Sign-On) 구성

조직의 다른 애플리케이션뿐만 아니라 FMC에 로그인하는 사용자에게 인증 및 권한 부여를 제공하는 시스템 인 SSO(Single Sign-On)를 사용하도록 FMC를 구성할 수 있습니다. 이러한 SSO 설정에 참여하도록 구성된 애플리케이션은 페더레이션 서비스 제공자 애플리케이션이라고 합니다. SSO 사용자는 한 번 로그인하면 동일한 페더레이션의 멤버인 모든 서비스 제공자 애플리케이션에 액세스할 수 있습니다.

SAML SSO(Single Sign-On)

SSO용으로 구성된 FMC는 로그인 페이지에 단일 로그인 링크를 제공합니다. SSO 액세스를 위해 구성된 사용자가 이 링크를 클릭하면 FMC 로그인 페이지에서 사용자 이름과 암호를 제공하지 않고 인증 및 권한 부여를 위해 IdP로 리디렉션됩니다. IdP에서 성공적으로 인증되면 SSO 사용자는 FMC 웹 인터페이스로 다시 리디렉션되고 로그인됩니다.이를 수행하기 위해 FMC와 IdP 간의 모든 통신은 브라우저를 중개자로 사용하여 수행됩니다. 따라서 FMC에서는 ID 제공자에 직접 액세스하기 위해 네트워크 연결이 필요하지 않습니다.

FMC에서는 인증 및 권한 부여를 위해 SAML(Security Assertion Markup Language) 2.0 공개 표준을 준수하는 SSO 제공자를 사용하는 SSO를 지원합니다. FMC 웹 인터페이스는 다음 SSO 제공자에 대한 구성 옵션을 제공합니다.

- Okta
- OneLogin
- Azure
- PingID의 PingOne for Customers 클라우드 솔루션

Note Cisco Secure Sign On SSO 제품은 FMC를 사전 통합된 서비스 제공자로 인식하지 않습니다.

FMC에 대한 SSO 지침

FMC를 SSO 연합 멤버로 설정할 때는 다음 사항에 유의하십시오.

- FMC는 한 번에 하나의 SSO 제공자만 있는 SSO를 지원할 수 있습니다. 예를 들어, SSO용 OneLogin 및 Okta를 모두 사용하도록 FMC를 설정할 수 없습니다.
- FMC고가용성 설정의 FMC는 SSO를 지원할 수 있지만, 다음 사항을 고려해야 합니다.
  - SSO 설정은 고가용성 쌍의 멤버 간에 동기화되지 않습니다. 쌍의 각 멤버에서 SSO를 별도로 설정해야 합니다.
  - 고가용성 쌍의 두 FMC는 모두 SSO에 동일한 IdP를 사용해야 합니다. SSO에 대해 설정된 각 FMC의 IdP에서 서비스 제공자 애플리케이션을 설정해야 합니다.

- 둘 다 SSO를 지원하도록 설정된 FMC 고가용성 쌍에서는 사용자가 SSO를 사용하여 보조 FMC에 처음으로 액세스하기 전에 먼저 사용자가 SSO를 통해 기본 FMC에 한 번 이상 로그인해야합니다.
- 고가용성 쌍에서 FMC에 대해 SSO를 설정하는 경우:
  - 기본 FMC에서 SSO를 설정하는 경우, 보조 FMC에서 SSO를 설정할 필요가 없습니다.
  - 보조 FMC에서 SSO를 설정하는 경우, 기본 FMC에서도 SSO를 설정해야 합니다. (SSO 사용자는 보조 FMC에 로그인하기 전에 기본 FMC에 한 번 이상 로그인해야 하기 때문입니다.)

- 멀티테넌시를 사용하는 FMC에서 SSO 구성은 전역 도메인 레벨에서만 적용할 수 있으며, 전역 도메인 및 모든 하위 도메인에 적용됩니다.
- 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다.
- FMC는 IdP에서 시작된 SSO를 지원하지 않습니다.
- FMC는 SSO 계정에 대한 CAC 자격 증명을 사용한 로그인을 지원하지 않습니다.
- CC 모드를 사용하는 구축에서는 SSO를 설정하지 마십시오.
- SSO 활동은 Subsystem(하위 시스템) 필드에 Login(로그인) 또는 Logout(로그아웃)이 지정된 FMC 감사 로그에 기록됩니다.

Related Topics

Firepower Management Center 고가용성, 275 페이지
도메인 관리, 481 페이지
CAC 크리덴셜로 Firepower Management Center에 로그인, 33 페이지
보안 인증 컴플라이언스, 1469 페이지
감사 기록, 451 페이지

SSO 사용자 계정

ID 공급자는 사용자 및 그룹 구성을 직접 지원할 수도 있고, Active Directory, RADIUS 또는 LDAP와 같은 다른 사용자 관리 애플리케이션에서 사용자 및 그룹을 가져올 수도 있습니다. 이 문서에서는 IdP 사용자 및 그룹이 이미 설정되어 있다고 가정하고 SSO를 지원하도록 IdP와 작동하도록 FMC를 구성하는 방법을 중점적으로 다룹니다. 다른 사용자 관리 애플리케이션의 사용자 및 그룹을 지원하도록 IdP를 구성하려면 IdP 벤더 설명서를 참조하십시오.

사용자 이름 및 암호를 포함하여 SSO 사용자에 대한 대부분의 계정 특성은 IdP에서 설정됩니다. SSO 계정은 처음 로그인할 때까지 FMC 웹 인터페이스 사용자 페이지에 나타나지 않습니다.

Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

SSO 사용자에 대한 다음 계정 특성은 **System(**시스템**)** > **User(**사용자**)** > **Edit User(**사용자 편집**)** 아래의 FMC 웹 인터페이스에서 구성할 수 있습니다.

- 실제 이름
- 브라우저 세션 시간 초과에서 제외

SSO 사용자에 대한 사용자 역할 매핑

기본적으로 FMC에 대한 SSO 액세스 권한이 부여된 모든 사용자에게는 보안 분석가(읽기 전용) 역할이 할당됩니다. 이 기본값을 변경하고 사용자 역할 매핑이 있는 특정 SSO 사용자 또는 그룹에 대해 이 기본값을 재정의할 수 있습니다. FMC SSO 구성을 설정하고 성공적으로 테스트한 후 FMC SSO 사용자가 로그인할 때 할당되는 사용자 역할을 설정하도록 사용자 역할 매핑을 구성할 수 있습니다.

사용자 역할을 매핑하려면 FMC에서 구성 설정을 SSO IdP 애플리케이션의 설정과 조정해야 합니다. 사용자 역할은 사용자 또는 IdP 애플리케이션에 정의된 그룹에 할당할 수 있습니다. 사용자는 그룹의 구성원일 수도 있고 아닐 수도 있으며, 사용자 또는 그룹 정의는 조직 내의 다른 사용자 관리 시스템(예: Active Directory)에서 IdP로 가져오거나 가져올 수 없습니다. 따라서 FMC SSO 사용자 역할 매핑을 효과적으로 구성하려면 SSO 페더레이션이 구성되는 방식과 SSO IdP 애플리케이션에서 사용자, 그룹 및 해당 역할이 할당되는 방식을 숙지해야 합니다. 이 문서에서는 사용자 역할 매핑을 지원하기 위해 IdP와 함께 작동하도록 FMC를 구성하는 방법을 중점적으로 다룹니다. IdP 내에서 사용자 또는 그룹을 생성하거나 사용자 관리 애플리케이션에서 IdP로 사용자 또는 그룹을 가져오려면 IdP 벤더 설명서를 참조하십시오.

사용자 역할 매핑에서 IdP는 FMC 서비스 공급자 애플리케이션에 대한 역할 특성을 유지하며, 해당 FMC에 대한 액세스 권한이 있는 각 사용자 또는 그룹은 역할 특성에 대한 문자열 또는 식으로 구성됩니다(속성 값에 대한 요구 사항은 각 IdP마다 다름). FMC에서 해당 역할 속성의 이름은 SSO 구성의 일부입니다. FMC SSO 구성에는 FMC 사용자 역할 목록에 할당된 식 목록도 포함됩니다. 사용자가 SSO를 사용하여 FMC에 로그인하면 FMC에서는 해당 사용자(또는 구성에 따라 해당 사용자 그룹)의 역할 속성 값을 각 FMC 사용자 역할의 식과 비교합니다. FMC에서는 식이 사용자가 제공한 속성 값과 일치하는 모든 역할을 사용자에게 할당합니다.

Note 개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 설정할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다.

FMC에서 SSO(Single Sign-On) 활성화

Before you begin

- SAML SSO 관리 애플리케이션에서 FMC에 대한 서비스 제공자 애플리케이션을 구성하고 서비스 제공자 애플리케이션에 사용자 또는 그룹을 할당합니다.
  - Okta용 FMC 서비스 제공자 애플리케이션을 구성하려면 Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 79의 내용을 참조하십시오.
  - OneLogin용 FMC 서비스 제공자 애플리케이션을 구성하려면 OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91의 내용을 참조하십시오.
  - Azure 용 FMC 서비스 제공자 애플리케이션을 구성하려면 *Azure*용 *FMC* 서비스 제공자 애플리케이션 구성, 21 페이지를 참조하십시오.
  - PingID의 PingOne for Customers 클라우드 솔루션에 대해 FMC 서비스 제공자 애플리케이션을 구성하려면 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 117의 내용을 참조하십시오.
  - SAML 2.0 호환 SSO 제공자에 대해 FMC 서비스 제공자 애플리케이션을 구성하려면 SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 122의 내용을 참조하십시오.

Procedure

단계 **1** 시스템 > 사용자 > **SSO(Single Sign-On)**를 선택합니다.

단계 **2** **SSO(Single Sign-On)** 구성 슬라이더를 클릭하여 SSO를 활성화합니다.

단계 **3** **Configure SSO(SSO 구성)** 버튼을 클릭합니다.

단계 **4** **Select FMC SAML Provider(FMC SAML 제공자 선택)** 대화 상자에서 선택한 SSO IdP 라디오 버튼을 클릭하고 **Next(다음)**를 클릭합니다.

What to do next

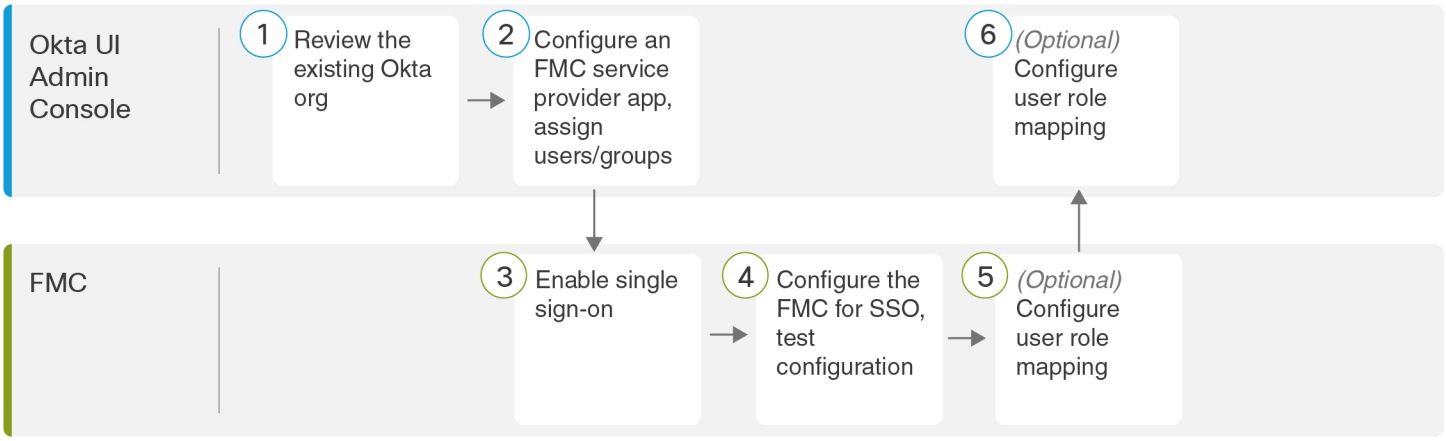
선택한 SSO 제공자에 적합한 지침을 진행합니다.

- Okta SSO용 FMC를 구성합니다. Okta SSO용 FMC 구성, on page 81의 내용을 참조하십시오.
- PingID의 PingOne for Customers 클라우드 솔루션을 사용하여 SSO용 FMC를 구성합니다. PingID PingOne for Customers을 사용하여 SSO용 FMC을 구성합니다., on page 119의 내용을 참조하십시오.
- Azure SSO용 FMC를 구성합니다. Azure SSO용 FMC 구성, on page 106의 내용을 참조하십시오.
- OneLogin SSO용 FMC를 구성합니다. OneLogin SSO용 FMC 구성, on page 93의 내용을 참조하십시오.

- SAML 2.0 호환 제공자를 사용하여 SSO용 FMC를 구성합니다. SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 123의 내용을 참조하십시오.

Okta로 SSO(Single Sign-On) 구성

Okta를 사용하여 SSO를 구성하려면 다음 작업을 참조하십시오.



1	Okta UI 관리 콘솔	Okta 조직 검토, on page 78
2	Okta UI 관리 콘솔	Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 79
3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 77
4	FMC	Okta SSO용 FMC 구성, on page 81
5	FMC	Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82
6	Okta UI 관리 콘솔	Okta IdP에서 사용자 역할 매핑 구성, on page 83

Okta 조직 검토

Okta에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션 디바이스 및 애플리케이션을 포함하는 엔티티를 *org*라고 합니다. Okta 조직에 FMC를 추가하기 전에 해당 구성을 숙지하십시오. 다음 질문을 검토하십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 Okta org 내 그룹 구성원입니까?
- 사용자 및 그룹 정의가 Okta의 기본 설정이거나 Active Directory, RADIUS 또는 LDAP와 같은 사용자 관리 애플리케이션에서 가져온 것입니까?

- FMC에서 SSO를 지원하려면 Okta org에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 FMC가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 Okta org 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 구성할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다.

이 문서에서는 Okta Classic UI 관리 콘솔에 대해 잘 알고 있으며 슈퍼 관리자 권한이 필요한 구성 기능을 수행할 수 있는 계정이 있다고 가정합니다. 자세한 내용은 온라인에서 확인 가능한 Okta 문서를 참조하십시오.

Okta를 위한 FMC 서비스 제공자 애플리케이션 구성

Okta Classic UI 관리 콘솔에서 이 지침을 사용하여 Okta 내에 FMC 서비스 공급자 애플리케이션을 생성하고 해당 애플리케이션에 사용자 또는 그룹을 할당합니다. SAML SSO 개념 및 Okta 관리 콘솔에 대해 숙지해야 합니다. 이 문서에서는 모든 기능을 갖춘 SSO 조직을 설정하는 데 필요한 모든 Okta 기능에 대해 설명하지는 않습니다. 예를 들어 사용자 및 그룹을 생성하거나 다른 사용자 관리 애플리케이션에서 사용자 및 그룹 정의를 가져오려면 Okta 문서를 참조하십시오.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- SSO 페더레이션 그리고 해당 사용자 및 그룹을 숙지하십시오. Okta 조직 검토, on page 78을 참조하십시오.
- 필요한 경우 Okta 조직에서 사용자 계정 및/또는 그룹을 생성합니다.

Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 FMC 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** Okta Classic UI 관리 콘솔에서 FMC용 서비스 공급자 애플리케이션을 생성합니다. 다음 항목을 선택하여 FMC 애플리케이션을 구성합니다.

- 플랫폼에 대해 **Web(웹)**을 선택합니다.
- **Sign on(로그온)** 방법으로 `SAML 2.0`을 선택합니다.
- **SSO(Single Sign On) URL**을 제공합니다.

  이는 브라우저가 IdP를 대신하여 정보를 전송하는 FMC URL입니다.

  FMC 로그인 URL에 `saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Use this for Recipient URL and Destination URL(수신자 URL 및 대상 URL에 사용)**를 활성화합니다.
- 대상 **URI(SP 엔티티 ID)**를 입력합니다.

  이 이름은 종종 URL로 형식이 지정되는 서비스 제공자(FMC)의 전역 고유 이름입니다.

  FMC 로그인 URL에 `/saml/metadata` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- **Name ID Format(이름 ID 형식)**에서 `Unspecified(지정되지 않음)`를 선택합니다.

단계 **2** (애플리케이션에 그룹을 할당하는 경우엔 선택 사항입니다.) 개별 Okta 사용자를 FMC 애플리케이션에 할당합니다. (FMC 애플리케이션에 그룹을 할당하려는 경우 해당 그룹의 멤버인 사용자를 개인으로 할당하지 마십시오.)

단계 **3** (애플리케이션에 개별 사용자를 할당하는 경우엔 선택 사항입니다.) Okta 그룹을 FMC 애플리케이션에 할당합니다.

단계 **4** (선택 사항) FMC에서 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 공급자 애플리케이션용 SAML XML 메타 데이터 파일을 Okta에서 로컬 컴퓨터로 다운로드할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77을 참조하십시오.

Okta SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 사용하십시오.

시작하기 전에

- Okta Classic UI 관리 콘솔에서 FMC 서비스 제공자 애플리케이션을 생성합니다. Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 79의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

Procedure

단계 **1** (이 절차는 FMC에서 SSO(Single Sign-On) 활성화, on page 77에서 곧바로 이어집니다.) **Configure Okta Metadata(Okta** 메타데이터 구성**)**에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 구성 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. Okta SSO 서비스 제공자 애플리케이션에서 다음 값을 입력합니다. (Okta Classic UI 관리 콘솔에서 이러한 값을 검색합니다.)
     - **ID** 제공자 **SSO(Single Sign-On) URL**
     - **ID** 제공자 발급자
     - **X.509** 인증서
- Okta에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 79의 4단계) 파일을 FMC에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 설정 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 Okta 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82의 내용을 참조하십시오. 역할 매핑을 설정하지 않기로 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82의 4단계에서 설정한 사용자 역할이 할당됩니다.

Okta에 대한 사용자 역할 매핑 구성 FMC

FMC 웹 인터페이스에서 사용자 역할을 설정하는 데 구성할 필드는 선택한 SSO 제공자에 관계없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다.

Before you begin

- Okta 사용자 그룹 매핑 정보를 검토합니다. Okta 조직 검토, on page 78의 내용을 참조하십시오.
- FMC에 대한 SSO 서비스 제공자 애플리케이션을 설정합니다. Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 79의 내용을 참조하십시오.
- FMC에서 SSO(Single Sign-On)를 활성화하고 설정합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77 및 Okta SSO용 FMC 구성, on page 81의 내용을 참조하십시오.

Procedure

단계 **1** **System**(시스템) > **Users**(사용자)를 선택합니다.

단계 **2** **Single Sign-On**(단일 인증) 탭을 클릭합니다.

단계 **3** **Advanced Configuration(Role Mapping)**(고급 구성(역할 매핑))을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 사용자 또는 그룹에 대한 사용자 역할을 매핑하는 데 Okta FMC 제공자 애플리케이션에 설정된 속성 이름과 일치해야 합니다. (Okta IdP에서 역할 매핑을 위한 사용자 속성 구성, on page 83의 1단계 또는 Okta IdP에서 역할 매핑을 위한 그룹 속성 구성, on page 84의 1단계 참조)

단계 **6** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. (FMC는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성값과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

- 서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. Okta IdP에서 사용자 역할 매핑 구성, on page 83의 내용을 참조하십시오.

Okta IdP에서 사용자 역할 매핑 구성

개별 사용자 권한 또는 그룹 권한에 따라 Okta Classic UI 관리 콘솔에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한에 따라 매핑하려면 Okta IdP에서 역할 매핑을 위한 사용자 속성 구성, on page 83의 내용을 참조하십시오.
- 그룹 권한에 따라 매핑하려면 Okta IdP에서 역할 매핑을 위한 그룹 속성 구성, on page 84의 내용을 참조하십시오.

SSO 사용자가 FMC에 로그인하면 Okta는 Okta IdP에서 설정된 사용자 또는 그룹 역할 속성값을 FMC에 제공합니다. FMC에서는 해당 속성값을 SSO 설정의 각 FMC 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여합니다. (일치 항목이 없으면 FMC는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. FMC는 FMC 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 Okta에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. 또한 FMC는 Okta에 설정된 FMC 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 롤 매핑은 FMC에 더 효율적입니다. Okta 조직 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

Okta IdP에서 역할 매핑을 위한 사용자 속성 구성

Okta 클래식 UI 관리 콘솔에서 다음 지침을 통해 Okta 기본 사용자 프로파일에 맞춤형 역할 매핑 속성을 추가합니다.

Okta 서비스 제공자 애플리케이션은 다음 두 가지 유형의 사용자 프로파일 중 하나를 사용할 수 있습니다.

- Okta 사용자 프로파일: 모든 맞춤형 속성으로 확장할 수 있습니다.
- 앱 사용자 프로파일: 지원되는 속성에 대해 타사 애플리케이션 또는 디렉토리(예: Active Directory, LDAP 또는 Radius)를 쿼리하여 Okta가 생성하는 사전 정의된 목록의 속성으로만 확장할 수 있습니다.

Okta 조직에서 사용자 프로파일 유형을 사용할 수 있습니다. 설정 방법에 대한 자세한 내용은 Okta 설명서를 참조하십시오. 어떤 사용자 프로파일 유형을 사용하든, FMC와 함께 사용자 역할 매핑을 지원하려면 FMC에 각 사용자의 역할 매핑 식을 전달하도록 프로파일에 맞춤형 속성을 구성해야 합니다.

이 문서에서는 Okta 사용자 프로파일을 통한 역할 매핑에 대해 설명합니다. 앱 프로파일을 사용하여 매핑하려면 맞춤형 속성을 설정하기 위해 조직에서 사용 중인 타사 사용자 관리 애플리케이션에 익숙해야 합니다. 자세한 내용은 Okta 설명서를 참조하십시오.

Before you begin

- Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 79에 설명된 대로 Okta IdP에서 FMC 서비스 제공자 애플리케이션을 설정합니다.
- Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82에 설명된 대로 FMC에서 SSO 사용자 역할 매핑을 설정합니다.

Procedure

단계 **1** 기본 Okta 사용자 프로파일에 새 속성을 추가합니다.

- **Data type(**데이터 유형**)**은 `string`으로 선택합니다.
- Okta IdP가 FMC로 보낼 변수 이름을 제공합니다. 여기에는 사용자 역할 매핑에 일치하는 식이 포함되어 있습니다. 이 변수 이름은 **Group Member Attribute(**그룹 멤버 속성**)**에 대해 FMC SSO 설정에서 입력한 문자열과 일치해야 합니다. (Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82의 5단계 참조)

단계 **2** 이 프로파일을 사용하여 FMC 서비스 제공자 애플리케이션에 할당된 각 사용자에 대해 방금 생성한 사용자 역할 속성에 값을 할당합니다.

식을 사용하여 FMC에서 사용자에게 할당할 역할을 나타냅니다. FMC에서는 이 문자열을 Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82의 6단계에서 각 FMC 사용자 역할에 할당한 식과 비교합니다. (FMC 사용자 역할 식과 비교하기 위해 FMC에서는 Okta에서 수신한 속성값을 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 식으로 처리합니다.)

Okta IdP에서 역할 매핑을 위한 그룹 속성 구성

Okta Classic UI 관리 콘솔에서 다음 지침을 통해 사용자 지정 역할 매핑 그룹 속성을 FMC 서비스 공급자 애플리케이션에 추가하십시오. FMC는 Okta FMC 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다.

Okta 서비스 제공자 애플리케이션은 다음 두 가지 유형의 그룹 중 하나를 사용할 수 있습니다.

- Okta 그룹: 모든 맞춤형 속성으로 확장할 수 있습니다.
- 애플리케이션 그룹: 지원되는 속성에 대해 타사 애플리케이션 또는 디렉토리(예: Active Directory, LDAP 또는 Radius)를 쿼리하여 Okta가 생성하는 사전 정의된 목록의 속성으로만 확장할 수 있습니다.

Okta 조직에서 두 가지 유형의 그룹을 사용할 수 있습니다. 설정 방법에 대한 자세한 내용은 Okta 설명서를 참조하십시오. 어떤 그룹 유형을 사용하든 간에 FMC와 함께 사용자 역할 매핑을 지원하려면 FMC에 그룹에 대한 역할 매핑 식을 전달하기 위한 맞춤형 속성을 설정해야 합니다.

이 문서에서는 Okta 그룹을 사용한 역할 매핑에 대해 설명합니다. 애플리케이션 그룹과 매핑하려면 맞춤형 속성을 설정하기 위해 조직에서 사용 중인 타사 사용자 관리 애플리케이션에 익숙해야 합니다. 자세한 내용은 Okta 설명서를 참조하십시오.

Before you begin

- Okta IdP에서 FMC 서비스 제공자 애플리케이션을 설정합니다. Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 79의 내용을 참조하십시오.
- FMC에서 사용자 역할 매핑을 설정합니다. Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82의 내용을 참조하십시오.

Procedure

FMC 서비스 제공자 애플리케이션에 대한 새 SAML 그룹 속성을 생성합니다.

- **Name(**이름**)**에는 FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 대해 입력한 것과 같은 문자열을 사용합니다. (Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82의 5단계 참조)
- **Filter(**필터**)**에서 FMC가 그룹의 멤버에 할당할 역할을 나타내는 식을 지정합니다. Okta는 이 값을 사용자가 멤버인 그룹의 이름과 비교하여 FMC에 일치하는 그룹 이름을 전송합니다. 그다음 FMC는 Okta에 대한 사용자 역할 매핑 구성 FMC, on page 82의 6단계에서 각 FMC 사용자 역할에 할당한 정규식과 해당 그룹 이름을 비교합니다.

Okta 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 FMC의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 Okta의 FMC 서비스 제공자 애플리케이션 설정에 있습니다.

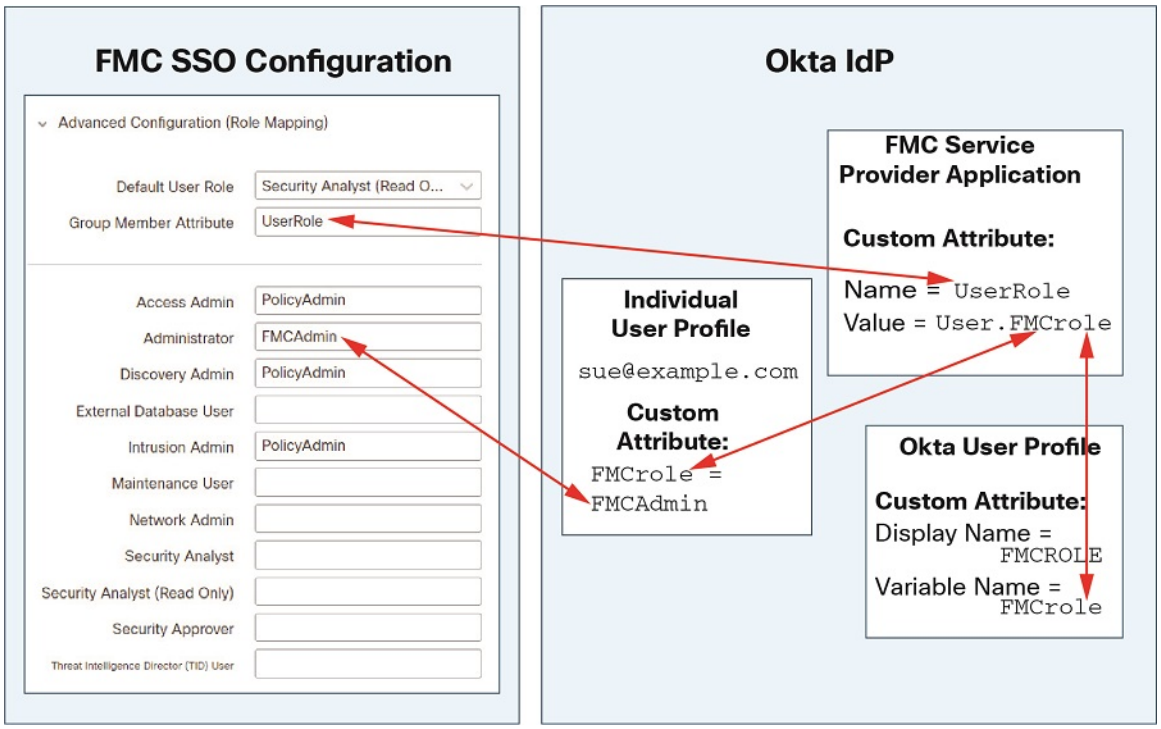
Note 개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 설정할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. 또한 FMC는 FMC에 설정된 FMC 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다.

개별 사용자 계정의 Okta 역할 매핑 예제

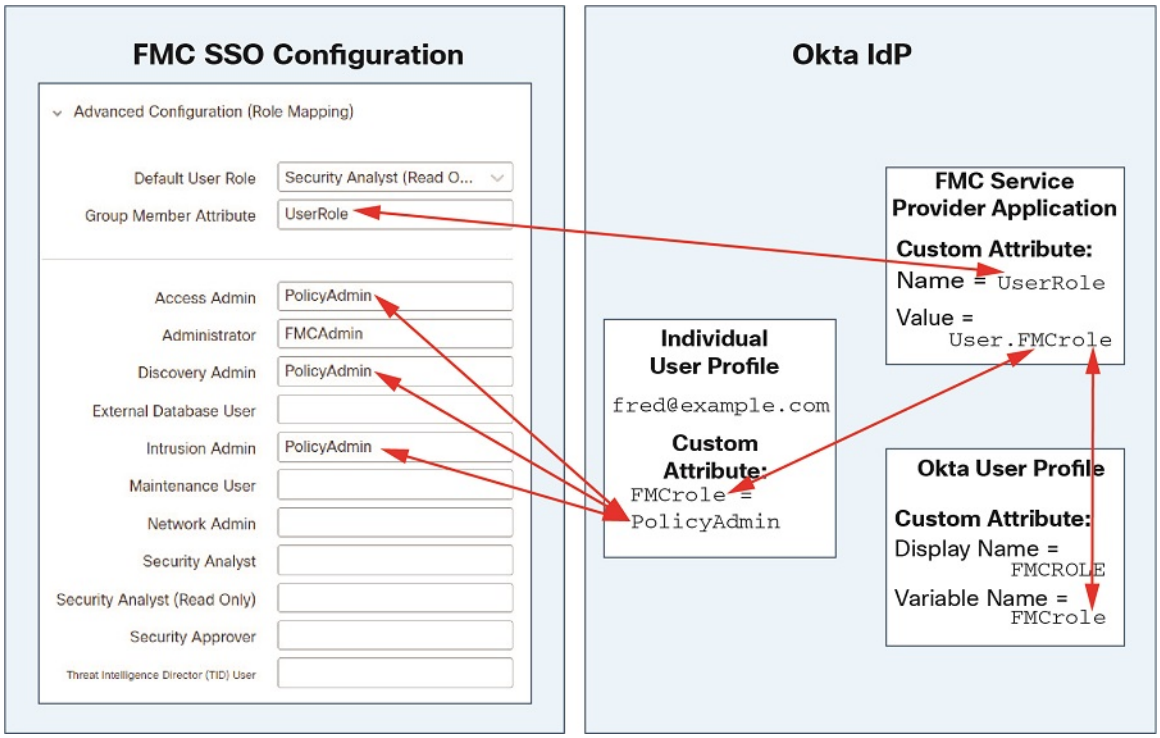
개별 사용자에 대한 역할 매핑에서 Okta FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성 이름과 일치하는 이름을 갖는 사용자 지정 속성이 있습니다 (이 예에서는 `UserRole`). Okta의 사용자 프로파일에도 사용자 지정 속성이 있습니다(이 예에서는 `FMCrole`이라는 변수). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 Okta가 사용자 역할 매핑 정보를 FMC에 전달할 때 해당 사용자에게 할당된 사용자 지정 속성값을 사용하도록 설정합니다.

다음 다이어그램은 FMC 및 Okta 설정의 관련 필드와 값이 개별 어카운트에 대한 사용자 역할 매핑에서 서로 어떻게 대응되는지를 보여줍니다. 각 다이어그램은 FMC 및 Okta UI 관리 콘솔에서 동일한 SSO 설정을 사용하지만, Okta UI 관리 콘솔의 각 사용자에 대한 설정은 FMC에서 서로 다른 방법으로 각 사용자에게 상이한 역할을 할당합니다.

- 이 다이어그램에서 sue@example.com은 `FMCrole` 값 `FMCAdmin`을 사용하며, FMC는 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 `FMCrole` 값 `PolicyAdmin`을 사용하며, FMC는 액세스 관리자, 검색 관리자 및 침입 관리자 역할을 할당합니다.



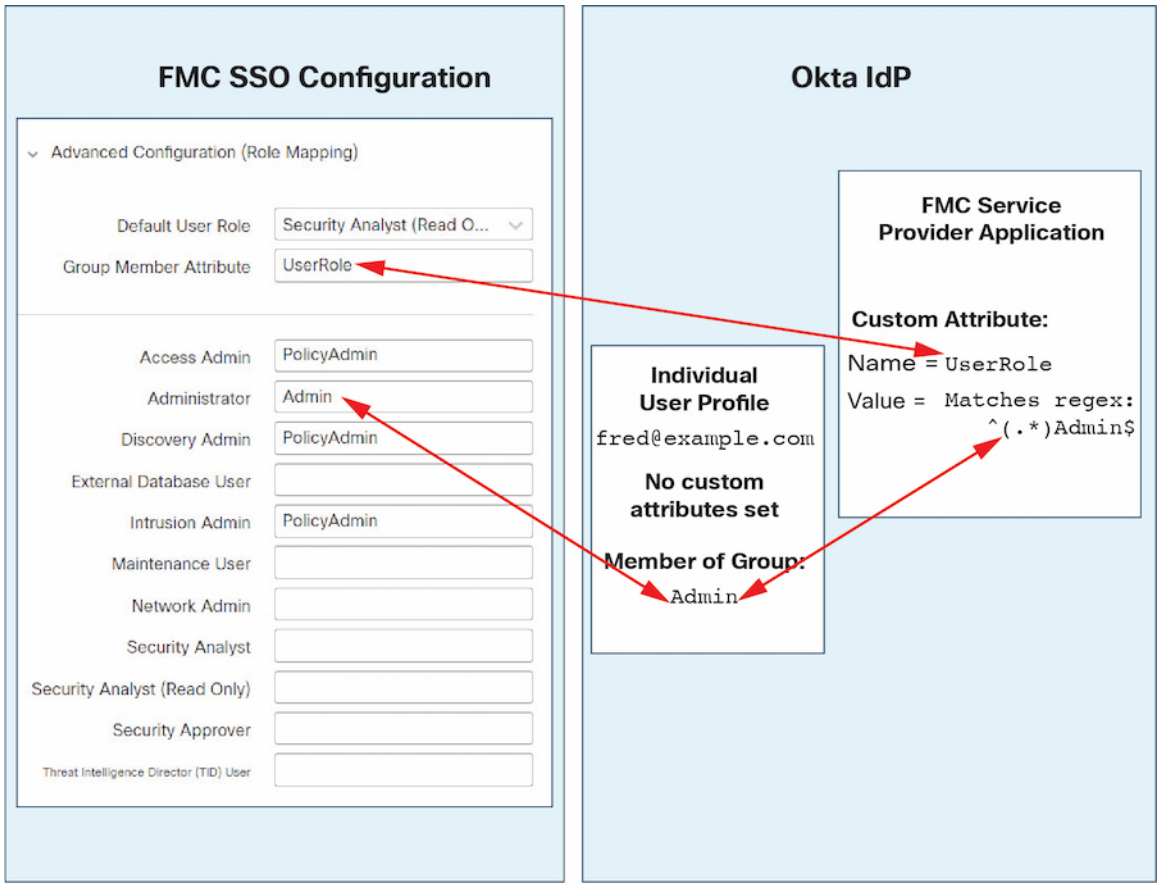
- FMC를 위해 Okta 서비스 애플리케이션에 할당된 다른 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석가(읽기 전용)가 할당됩니다.
  - Okta 사용자 프로파일에서 `FMCrole` 변수에 할당된 값이 없습니다.
  - Okta 사용자 프로필에서 `FMCrole` 변수에 할당된 값이 FMC의 SSO 설정에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **Okta** 역할 매핑 예

그룹에 대한 역할 매핑에서 Okta FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성의 이름(이 예에서는 `UserRole`)과 일치하는 이름을 갖는 사용자 지정 그룹 속성이 있습니다. Okta는 FMC SSO 로그인 요청을 처리할 때 사용자의 그룹 멤버십을 서비스 FMC 애플리케이션 그룹 속성(이 경우에는 `^(.*)Admin$`)에 할당된 식과 비교합니다. Okta는 그룹 속성과 일치하는 사용자의 그룹 멤버십을 FMC에게 전송합니다. FMC에서는 수신하는 그룹 이름을 각 사용자 역할에 대해 구성한 정규식과 비교하고 그에 따라 사용자 역할을 할당합니다.

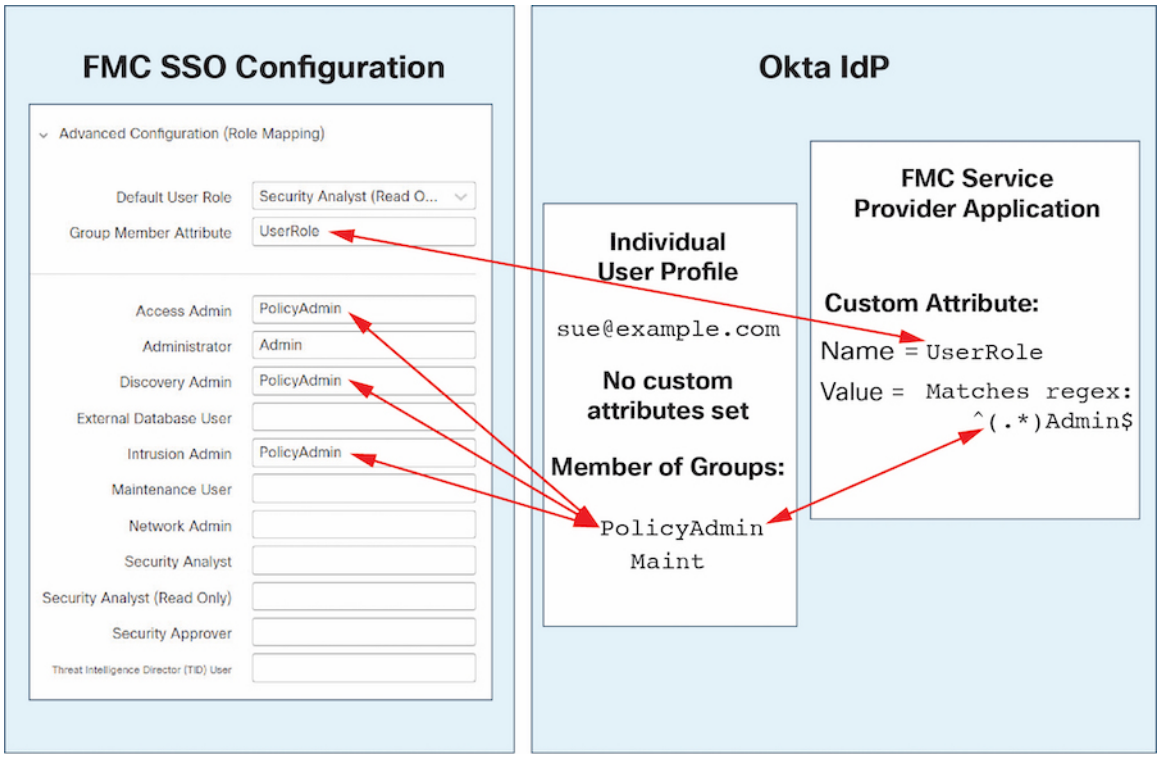
다음 다이어그램은 FMC 및 Okta 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치하는지를 보여줍니다. 각 다이어그램은 FMC 및 Okta UI 관리 콘솔에서 동일한 SSO 설정을 사용하지만, Okta UI 관리 콘솔의 각 사용자에 대한 설정은 FMC에서 서로 다른 방법으로 각 사용자에게 상이한 역할을 할당합니다.

- 이 다이어그램에서 fred@example.com은 Okta IdP 그룹 `Admin`의 멤버이며 `^ (.*)Admin$` 식과 일치합니다. Okta는 FMC Fred의 `관리자` 그룹 멤버십을 전송하고 FMC는 관리자에게 관리자 역할을 할당합니다.

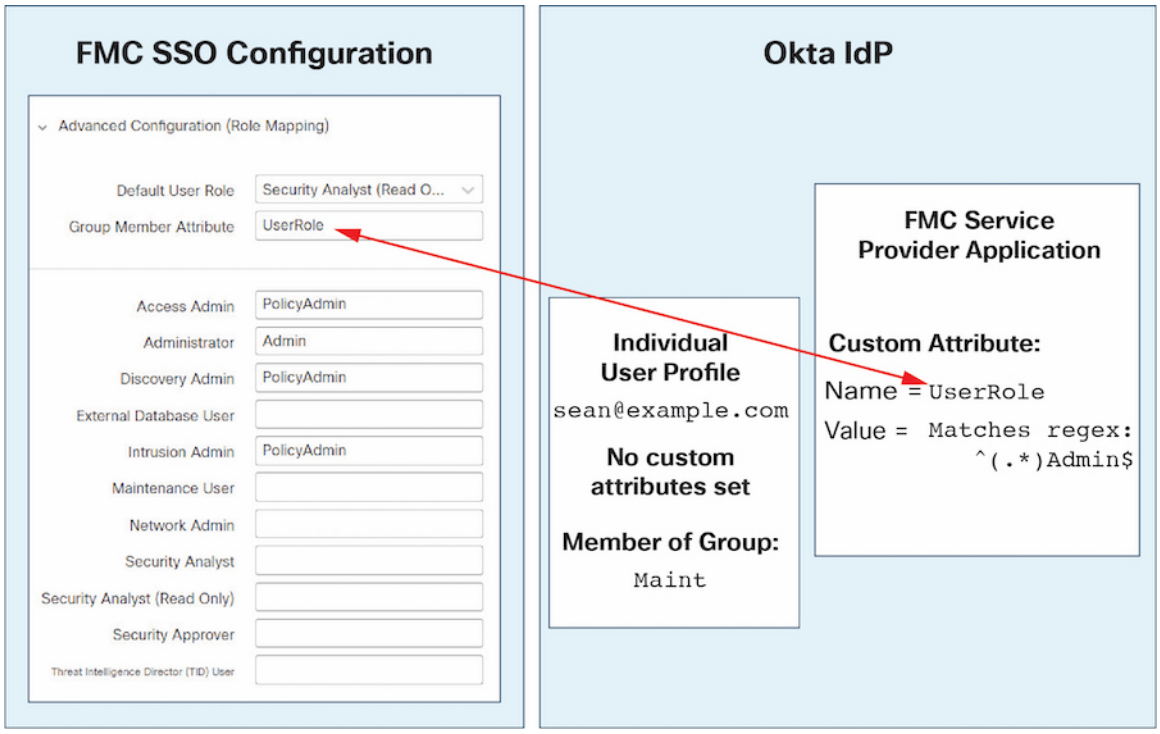


- 이 다이어그램에서 sue@example.com은 `^(.*)Admin$` 식과 일치하는 Okta IdP 그룹 `PolicyAdmin`의 멤버입니다. Okta는 FMC Sue의 `PolicyAdmin` 그룹 멤버십을 전송하고 FMC에서 Access Admin, Discovery Admin 및 Intrusion Admin 역할을 할당합니다.

  Sue는 Okta 그룹 `Maint`의 멤버이지만이 그룹 이름이 Okta FMC 서비스 애플리케이션의 그룹 멤버십 속성에 할당된 식과 일치하지 않으므로 Okta는 Sue의 `Maint` 그룹 멤버십에 대한 정보를 FMC에 전송하지 않습니다. `Maint` 그룹은 FMC가 그녀에게 할당하는 역할에 참여하지 않습니다.



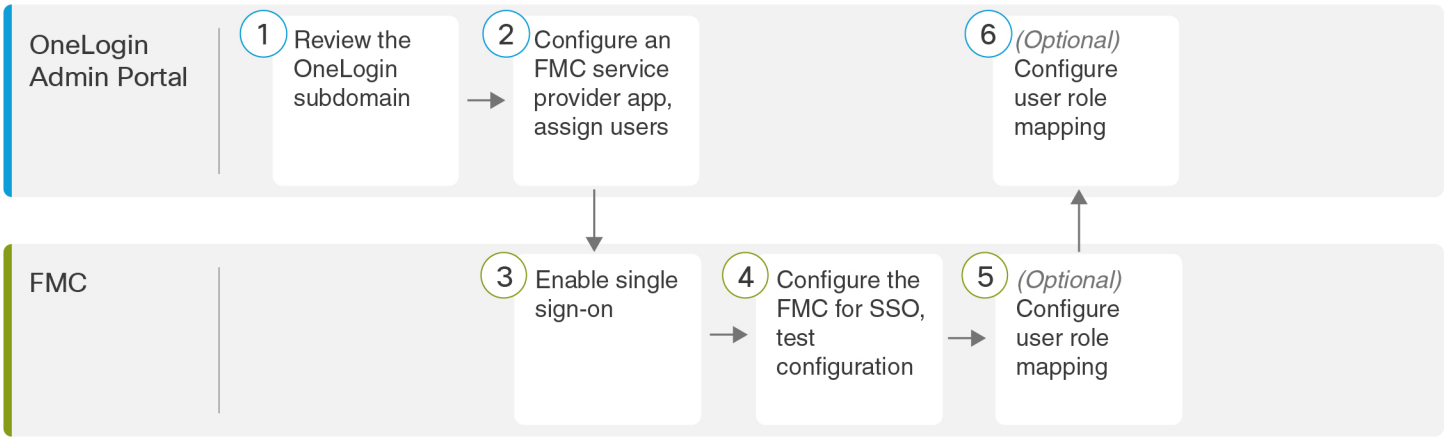
- 이 다이어그램에서 sean@example.com은 Okta IdP 그룹 `Maint`의 멤버입니다. 이 그룹 이름은 `^(.*)Admin$` 식과 일치하지 않습니다. 따라서 sean@example.com이 FMC에 로그인하면 Okta는 `Maint` 그룹 멤버십에 대한 정보를 FMC로 전송하지 않으며, Sean은 유지 보수 사용자 역할이 아닌(보안 분석가(읽기 전용)) 기본 사용자 역할(보안)을 할당 받습니다.



이 다이어그램은 역할 매핑 전략을 설정할 때 사전 계획의 중요성을 보여줍니다. 이 예에서는 `Maint` 그룹의 멤버인 이 FMC에 대한 액세스 권한이 있는 모든 Okta 사용자에게 기본 사용자 역할만 할당할 수 있습니다. FMC는 Okta 서비스 애플리케이션 구성에서 하나의 맞춤형 그룹 특성만 사용하도록 지원합니다. 해당 속성에 할당하는 식과 일치하도록 설정한 그룹 이름은 신중하게 작성해야 합니다. FMC SSO 구성의 사용자 역할 할당 문자열에서 정규식을 사용하여 역할 매핑에 유연성을 추가할 수 있습니다. 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다.

OneLogin으로 SSO(Single Sign-On) 구성

OneLogin을 사용하여 SSO를 구성하려면 다음 작업을 참조하십시오.



1	FMC	OneLogin 하위 도메인 검토, on page 91
2	FMC	OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91
3	OneLogin 관리 포털	FMC에서 SSO(Single Sign-On) 활성화, on page 77
4	OneLogin 관리 포털	OneLogin SSO용 FMC 구성, on page 93
5	OneLogin 관리 포털	FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94
6	FMC	OneLogin IdP에서 사용자 역할 매핑 구성, on page 95

OneLogin 하위 도메인 검토

OneLogin에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션 디바이스 및 애플리케이션을 포함하는 엔티티를 하위 도메인이라고 합니다. OneLogin 하위 도메인에 FMC를 추가하기 전에 해당 구성을 숙지하십시오. 다음 질문을 검토하십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 그룹의 OneLogin 하위 도메인 구성원 내에 있습니까?
- Active Directory, Google Apps 또는 LDAP와 같은 서드 파티 디렉터리의 사용자 및 그룹이 OneLogin 하위 도메인과 동기화됩니까?
- FMC에서 SSO를 지원하려면 OneLogin 하위 도메인에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 FMC 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 FMC가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 OneLogin 하위 도메인 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

개별 사용자 또는 그룹을 기준으로 매핑할 FMC 역할을 구성할 수 있지만 단일 FMC 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

이 문서에서는 사용자가 OneLogin 관리 포털에 대해 잘 알고 있으며 슈퍼 사용자 권한이 있는 계정을 가지고 있다고 가정합니다. 사용자 역할 매핑을 구성하려면 맞춤형 사용자 필드를 지원하는 OneLogin Unlimited 요금제를 구독해야 합니다. 자세한 내용은 온라인에서 사용 가능한 OneLogin 설명서를 참조하십시오.

OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성

OneLogin 관리 포털에서 이 지침을 사용하여 OneLogin 내에 FMC 서비스 공급자 애플리케이션을 생성하고 해당 애플리케이션에 사용자 또는 그룹을 할당합니다. SAML SSO 개념 및 OneLogin 관리 포

털에 대해 숙지해야 합니다. 이 문서에서는 모든 기능을 갖춘 SSO 조직을 설정하는 데 필요한 모든 OneLogin 기능에 대해 설명하지는 않습니다. 예를 들어 사용자 및 그룹을 생성하거나 다른 사용자 관리 애플리케이션에서 사용자 및 그룹 정의를 가져오려면 OneLogin 문서를 참조하십시오.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 숙지하십시오. OneLogin 하위 도메인 검토, on page 91의 내용을 참조하십시오.
- 필요한 경우 OneLogin 하위 도메인에 사용자 계정을 생성합니다.

  Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

  Note 여러 URL로 FMC 웹 인터페이스에 연결할 수 있는 경우 (예: 정규화된 도메인 이름 및 IP 주소) SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** **SAML Test Connector (Advanced)**를 기본으로 사용하여 FMC서비스 제공자 애플리케이션을 생성합니다.

단계 **2** 다음 설정으로 애플리케이션을 구성합니다.

- **Audience (Entity ID)(**대상**(**엔티티 **ID))**의 경우, `/saml/metadata` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`

- **Recipient(**수신자**)**에 대해 FMC 로그인 URL에 `/aml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **ACS(**소비자**) URL** 검사기의 경우 OneLogin에서 올바른 FMC URL을 사용하고 있는지 확인하는 데 사용하는 식을 입력합니다. ACS URL을 사용하고 다음과 같이 변경하여 간단한 유효성 검사기를 만들 수 있습니다.
  - ACS URL의 시작 부분에 `^`를 추가합니다.
  - ACS URL의 끝에 `$`를 추가합니다.
  - ACS URL 내에서 모든 `/` 및 `?` 앞에 `\`를 삽입합니다.

예를 들어, ACS URL `https://ExampleFMC/saml/acs`의 경우 적절한 URL 유효성 검사기는 `^https:\/\/ExampleFMC\/saml\/acs$`가 됩니다.

- **ACS(**소비자**) URL**의 경우 FMC 로그인 URL에 `/saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Login URL(**로그인 **URL)**의 경우 FMC 로그인 URL에 `/saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **SAML Initiator(SAML** 개시자**)**에 대해 `Service Provider(통신 사업자)`를 선택합니다.

단계 **3** OneLogin 사용자를 FMC 사업자 애플리케이션에 할당합니다.

단계 **4** (선택 사항) FMC에서 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 공급자 애플리케이션용 SAML XML 메타 데이터를 OneLogin에서 로컬 컴퓨터로 다운로드할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

OneLogin SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 참조하십시오.

Before you begin

- OneLogin 관리 포털에서 FMC 서비스 제공자 애플리케이션을 생성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91의 내용을 참조하십시오.
- SSO(Single Sign-On)를 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

Procedure

단계 1 이 단계는 FMC에서 SSO(Single Sign-On) 활성화, on page 77에서 곧바로 이어집니다. **Configure OneLogin Metadata(OneLogin** 메타데이터 설정**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. OneLogin 서비스 제공 애플리케이션에서 다음 SSO 설정 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**: OneLogin에서 **SAML 2.0** 엔드포인트**(HTTP)**를 입력합니다.
     - **ID** 제공자 발급자: OneLogin의 발급자 **URL**을 입력합니다.
     - **X.509** 인증서: OneLogin에서 **X.509** 인증서를 입력합니다.

- OneLogin에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91의 4단계), 파일을 FMC에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 2 **Next(**다음**)**를 클릭합니다.

단계 3 **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 설정 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 4 **Test Configuration(**설정 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 설정과 OneLogin 서비스 제공자 애플리케이션 설정을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 5 시스템에서 설정 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94의 내용을 참조하십시오. 역할 매핑을 설정하지 않기로 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94의 4단계에서 설정한 사용자 역할이 할당됩니다.

FMC에서 OneLogin 사용자 역할 매핑 구성

FMC 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다.

Before you begin

- OneLogin 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 91의 내용을 참조하십시오.
- FMC에 대한 SSO 서비스 제공자 애플리케이션을 구성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91를 참조하십시오.
- FMC에서 단일 인증(SSO)을 활성화 및 구성합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77 그리고 OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91을 참조하십시오.

Procedure

단계 **1** 시스템 > 사용자 > **SSO(Single Sign-On)System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 **2** **Advanced Configuration (Role Mapping)(**고급 설정**(**역할 매핑**))**을 펼칩니다.

단계 **3** **Default User Role(**기본 사용자 역할**)** 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **4** **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다. 이 문자열은 OneLogin의 FMC 서비스 공급자 애플리케이션에서 역할 매핑에 대해 정의하는 사용자 지정 매개 변수의 필드 이름과 일치해야 합니다. (OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성, on page 96의 1단계 또는 OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성, on page 97의 1단계 참조)

단계 **5** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. OneLogin IdP에서 사용자 역할 매핑 구성, on page 95의 내용을 참조하십시오.

OneLogin IdP에서 사용자 역할 매핑 구성

개별 권한 또는 그룹 권한을 기반으로 Onelogin 관리 포털에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한에 따라 매핑하려면 OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성, on page 96의 내용을 참조하십시오.
- 그룹 권한에 따라 매핑하려면 OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성, on page 97의 내용을 참조하십시오.

SSO 사용자가 FMC에 로그인하면 OneLogin은 OneLogin IdP에서 설정된 사용자 정의 사용자 필드에서 사용자 또는 그룹 역할 속성값을 FMC에 제공합니다. FMC에서는 해당 속성값을 SSO 설정의 각 FMC 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여

합니다. (일치 항목이 없으면 FMC는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. FMC는 FMC 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 OneLogin에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. FMC는 OneLogin에 설정된 하나의 맞춤형 사용자 필드만 이용한 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 역할 매핑은 FMC에 더 효율적입니다. OneLogin 하위 도메인 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성

OneLogin 관리 포털을 사용하여 FMC 서비스 제공자 애플리케이션 및 맞춤형 사용자 필드에 대한 맞춤형 파라미터를 생성합니다. 이는 SSO 로그인 프로세스 중에 OneLogin이 사용자 역할 정보를 FMC에 전달할 수 있는 수단을 제공합니다.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 91을 참조하십시오.
- OneLogin에서 FMC 서비스 제공자 애플리케이션을 생성하고 구성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91의 내용을 참조하십시오.
- FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** FMC 서비스 제공자 애플리케이션에 대한 맞춤형 매개 변수를 생성합니다.

- **Field Name(**필드 이름**)**의 경우 FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 이름을 사용합니다. FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94의 4단계를 참조합니다.
- **Value(**값**)**에 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 2단계에서 구성할 고객 사용자 필드의 이름과 일치해야 합니다.

단계 **2** FMC 액세스 권한이 있는 각 OneLogin 사용자에 대한 사용자 역할 정보를 포함할 맞춤형 사용자 필드를 만듭니다.

- **Name(**이름**)** 필드의 경우 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 1단계에 설명된 애플리케이션 맞춤형 매개 변수에 대해 제공된 값과 일치해야 합니다.

- **Short name(**축약 이름**)**의 경우 필드의 축약된 대체 이름을 제공합니다. (이는 OneLogin 프로그래밍 인터페이스에 사용됩니다.)

단계 **3** FMC 서비스 제공자 애플리케이션에 대한 액세스 권한이 있는 각 사용자에 대해 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 값을 할당합니다.

사용자가 SSO를 사용하여 FMC에 로그인할 때 해당 사용자에 대해 이 필드에 할당하는 값은 FMC이(가) SSO 구성에서 FMC 사용자 역할에 할당한 식과 비교하는 값입니다. (FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94의 5단계 참조)

What to do next

- 다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성

OneLogin 관리 포털을 사용하여 FMC 서비스 제공자 애플리케이션 및 맞춤형 사용자 필드에 대한 맞춤형 파라미터를 생성합니다. OneLogin 사용자를 그룹에 할당합니다. 그런 다음 맞춤형 사용자 필드와 사용자 그룹 간에 하나 이상의 매핑을 생성하여 OneLogin이 사용자의 그룹 멤버십을 기반으로 맞춤형 사용자 필드에 값을 할당하도록 합니다. 이는 SSO 로그인 프로세스 중에 OneLogin이 그룹 기반 사용자 역할 정보를 FMC에 전달할 수 있는 수단을 제공합니다.

OneLogin 서비스 제공자 애플리케이션은 다음 두 가지 유형의 그룹 중 하나를 사용할 수 있습니다.

- OneLogin 기본 그룹.
- Active Directory, Google Apps 또는 LDAP와 같은 서드 파티 애플리케이션에 동기화된 그룹입니다.

FMC 그룹 역할 매핑을 위해 그룹 유형 중 하나를 사용할 수 있습니다. 이 문서에서는 OneLogin 그룹을 사용한 역할 매핑에 대해 설명합니다. 서드파티 애플리케이션 그룹을 사용하려면 사용자의 조직에서 사용하고 있는 서드파티 사용자 관리 애플리케이션을 숙지해야 합니다. 자세한 내용은 OneLogin 문서를 참고하십시오.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 91을 참조하십시오.
- OneLogin에서 FMC 서비스 제공자 애플리케이션을 생성하고 구성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 91의 내용을 참조하십시오.
- FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** FMC 서비스 제공자 애플리케이션에 대한 맞춤형 매개 변수를 생성합니다.

- **Field Name(**필드 이름**)**의 경우 FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 이름을 사용합니다. FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94의 4단계를 참조합니다.
- **Value(**값**)**에 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는이 절차의 2단계에서 구성할 고객 사용자 필드의 이름과 일치해야 합니다.

단계 **2** FMC 액세스 권한이 있는 각 OneLogin 사용자에 대한 사용자 역할 정보를 포함할 맞춤형 사용자 필드를 만듭니다.

- **Name(**이름**)** 필드의 경우 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 1단계에 설명된 애플리케이션 맞춤형 매개 변수에 대해 제공된 값과 일치해야 합니다.
- **Short name(**축약 이름**)**의 경우 필드의 축약된 대체 이름을 제공합니다. (이는 OneLogin 프로그래밍 인터페이스에 사용됩니다.)

단계 **3** 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 그룹 기반 값을 할당하려면 하나 이상의 사용자 필드 매핑을 만듭니다. 각 OneLogin 사용자 그룹에 올바른 FMC 사용자 역할을 할당하는 데 필요한 수의 매핑을 생성합니다.

- 사용자 그룹 필드와 그룹 이름을 비교하여 매핑에 대해 하나 이상의 조건을 생성합니다.
- 여러 조건을 생성하는 경우 사용자 그룹이 매핑을 수행할 조건 중 하나 또는 모두와 일치해야 하는지 여부를 선택합니다.
- 매핑에 대한 **Action(**동작**)**을 생성해서 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 값을 할당합니다. **Name(**이름**)** 필드 그리고 사용자가 지정한 조건을 충족하는 모든 사용자에 대해 OneLogin이 맞춤형 사용자 필드에 할당하는 문자열을 제공합니다.

  FMC에서는 이 문자열을 FMC에서 OneLogin 사용자 역할 매핑 구성, on page 94의 5단계에서 각 FMC 사용자 역할에 할당한 식과 비교합니다.
- 변경을 완료하면 모든 매핑을 다시 적용합니다.

What to do next

- 다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

OneLogin 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 FMC의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 OneLogin의 FMC 서비스 제공자 애플리케이션 설정에 있습니다.

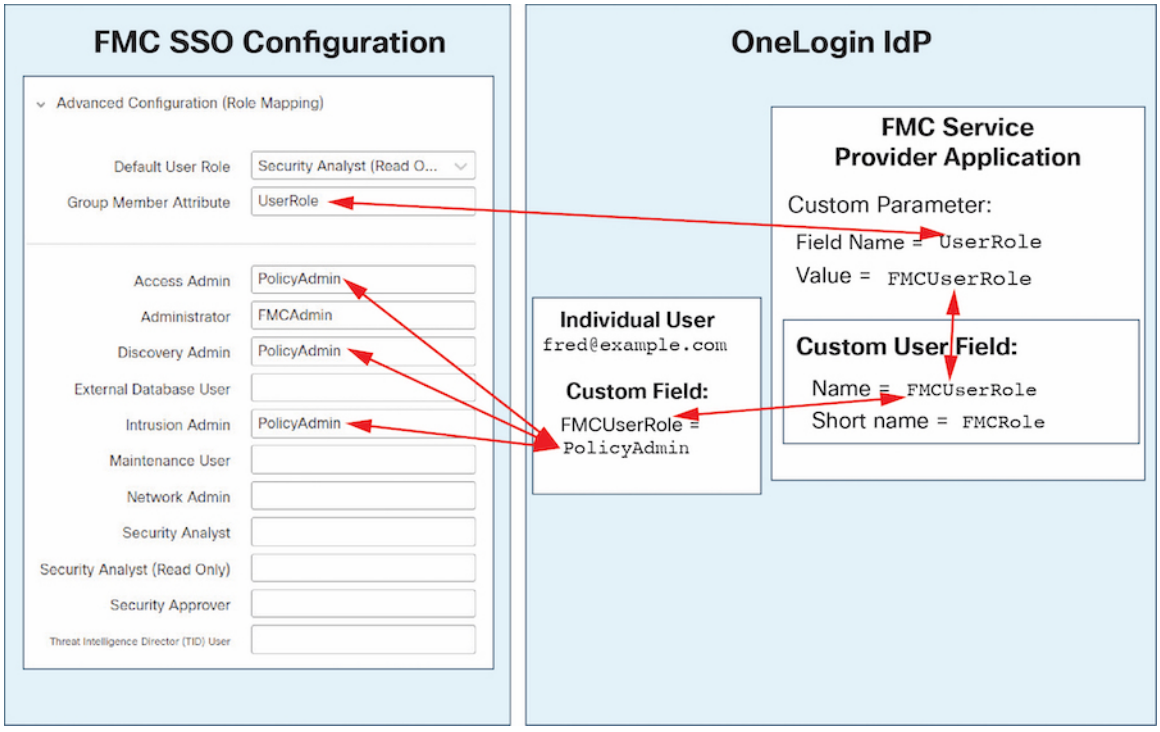
Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. FMC는 OneLogin에 설정된 하나의 맞춤형 사용자 필드만 이용한 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 역할 매핑은 FMC에 더 효율적입니다. OneLogin 하위 도메인 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

개별 사용자 계정에 대한 **OneLogin** 역할 매핑 예

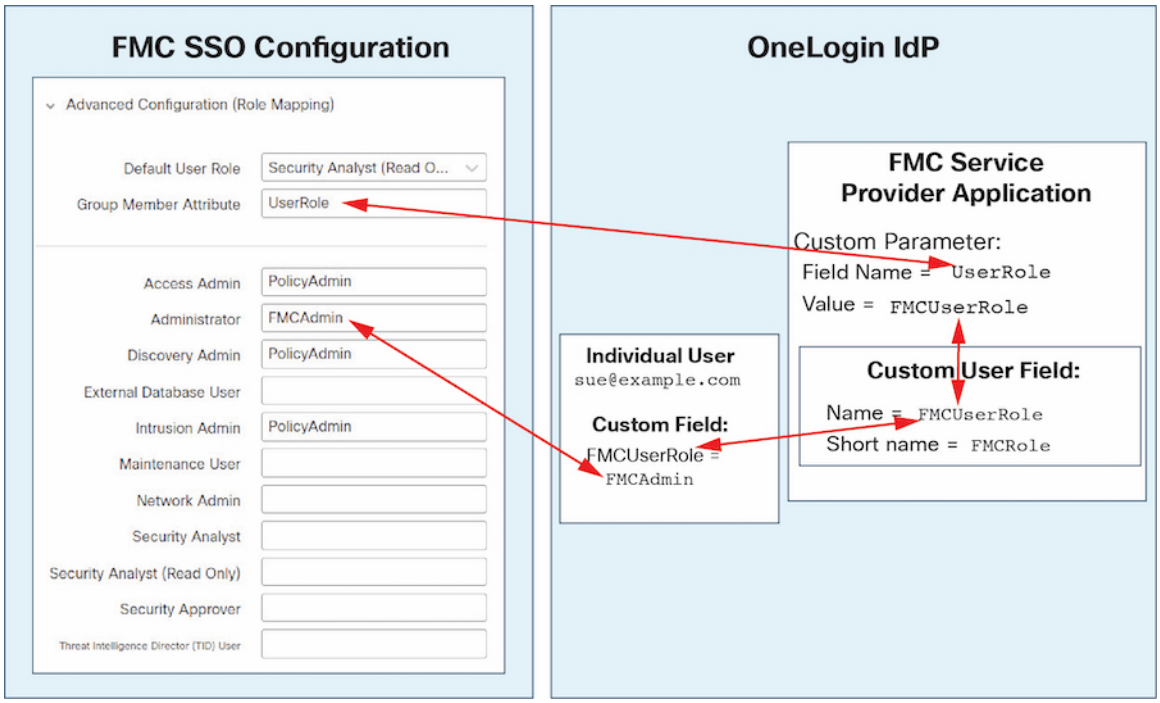
개별 사용자에 대한 역할 매핑에서 OneLogin FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성 이름과 일치하는 이름을(이 예에서는 `UserRole`) 갖는 사용자 지정 속성이 있습니다. OneLogin에는 맞춤형 사용자 필드도 정의되어 있습니다(이 예에서는 `FMCUserRole`). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 OneLogin이 사용자 역할 매핑 정보를 FMC에 전달할 때 해당 사용자의 사용자 지정 필드 `FMCUserRole`의 값을 사용하도록 설정합니다.

다음 다이어그램은 FMC 및 OneLogin 구성의 관련 필드와 값이 개별 계정에 대한 사용자 역할 매핑에서 서로 어떻게 대응하는지를 보여줍니다. 각 다이어그램은 FMC 및 OneLogin 관리 포털에서 동일한 SSO 컨피그레이션을 사용하지만, OneLogin 관리 포털의 각 사용자에 대한 컨피그레이션은 각 사용자에게 FMC에서 서로 다른 역할을 할당하기 위해서 달라집니다.

- 이 다이어그램에서 fred@example.com은 `FMCUserrole` 값 `PolicyAdmin`을 사용하며, FMC는 액세스 관리자, 검색 관리 및 침입 관리자 역할을 할당합니다.



- 이 다이어그램에서 sue@example.com은 `FMCUserRole` 값 `FMCAdmin`을 사용하며, FMC는 관리자 역할을 할당합니다.



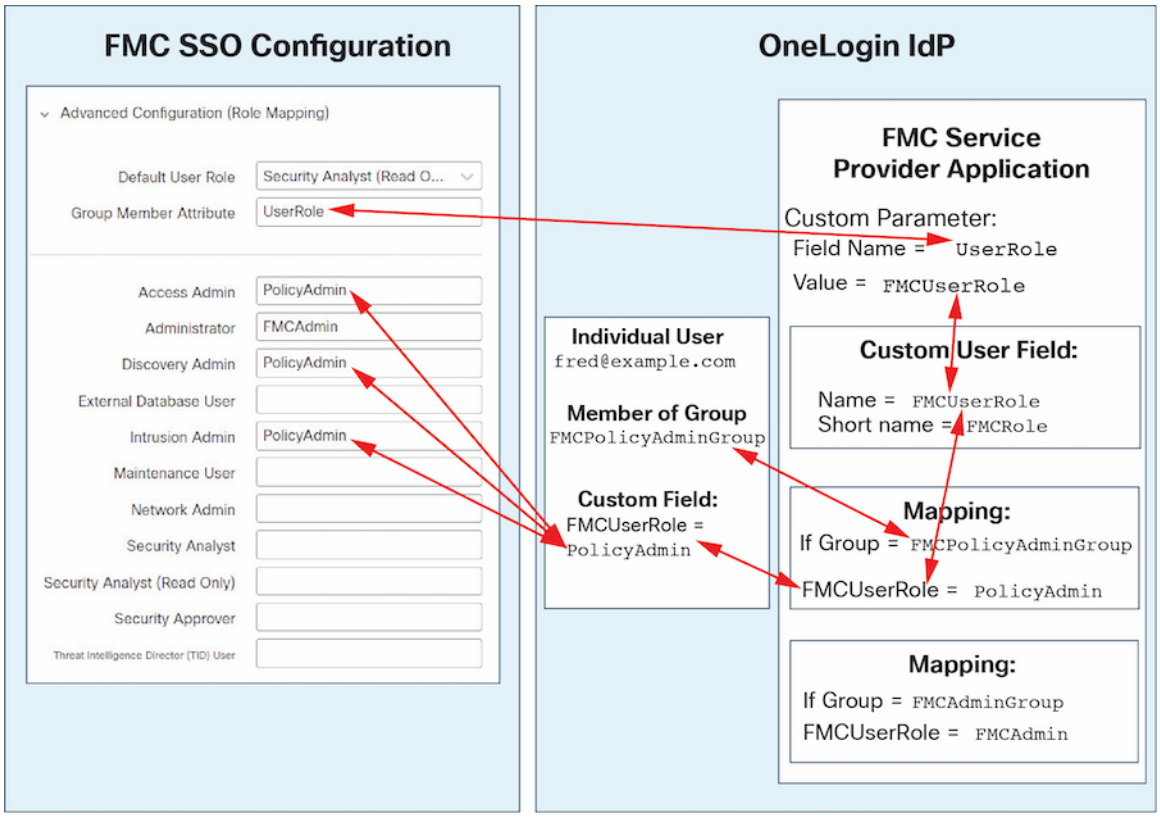
- 이 FMC를 위해 OneLogin 서비스 애플리케이션에 할당된 다른 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석(읽기 전용)이 할당됩니다.
  - `FMCUserRole` 맞춤형 사용자 필드에 할당된 값이 없습니다.
  - `FMCUserRole` 맞춤형 사용자 필드에 할당된 값이 FMC의 SSO 구성에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **OneLogin** 역할 매핑 예

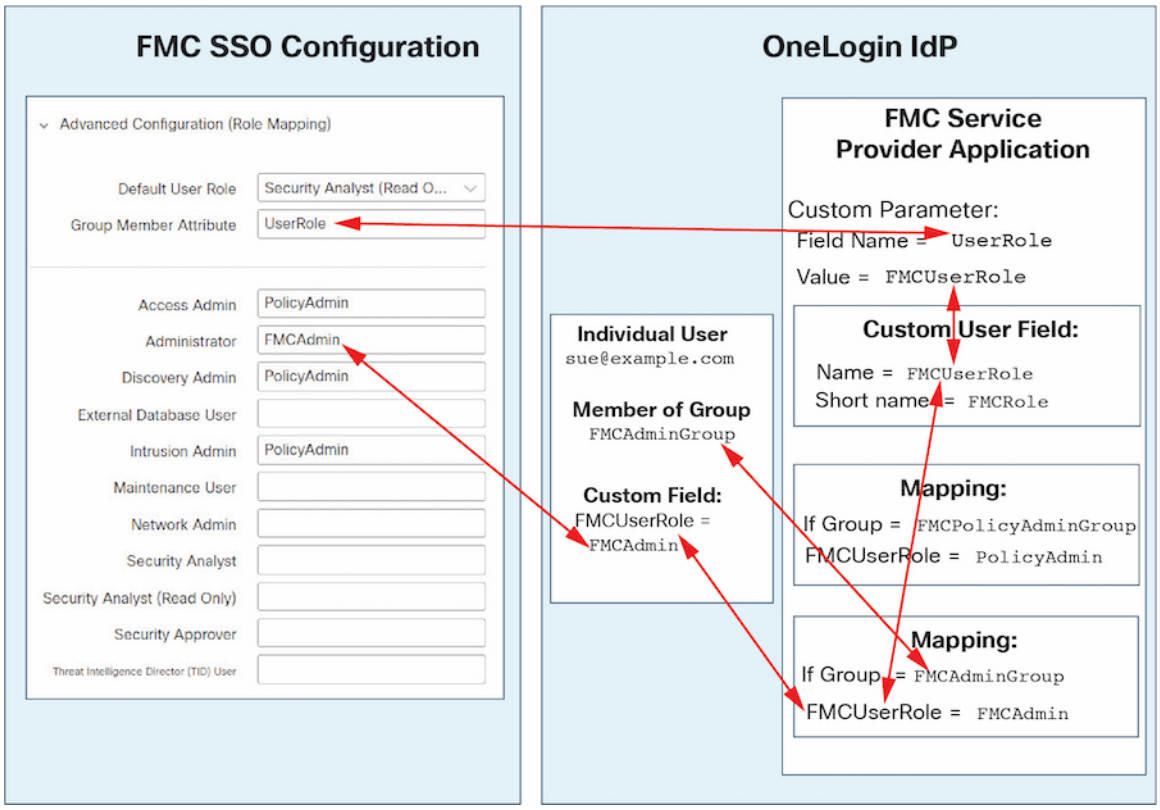
그룹에 대한 역할 매핑에서 OneLogin FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성의 이름(이 예에서는 `UserRole`)과 일치하는 이름을 갖는 사용자 지정 매개 변수가 있습니다. OneLogin에는 맞춤형 사용자 필드도 정의되어 있습니다(이 예에서는 `FMCUserRole`). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 OneLogin이 사용자 역할 매핑 정보를 FMC에 전달할 때 해당 사용자의 사용자 지정 필드 `FMCUserRole`의 값을 사용하도록 설정합니다. 사용자 그룹 매핑을 지원하려면 OneLogin 내에서 매핑을 설정하여 해당 사용자의 OneLogin 그룹 멤버십을 기반으로 각 사용자의 `FMCUserRole` 필드에 값을 할당해야 합니다.

다음 다이어그램은 FMC 및 OneLogin 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치 하는지를 보여줍니다. 각 다이어그램은 FMC 및 OneLogin 관리 포털에서 동일한 SSO 구성을 사용하지만, OneLogin 관리 포털의 각 사용자에 대한 구성은 각 사용자에게 FMC에서 서로 다른 역할을 할당하기 위해서 달라집니다.

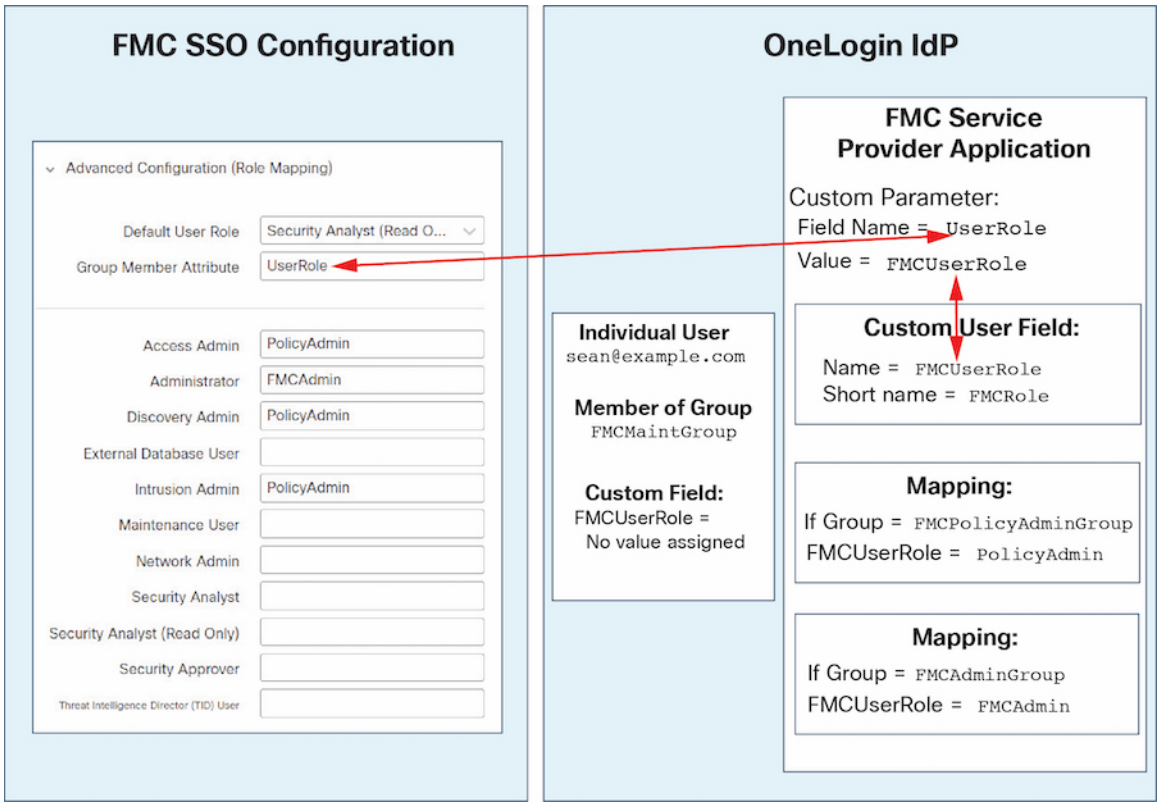
- 이 다이어그램에서 fred@example.com은 OneLogin IdP 그룹 `FMCPolicyAdminGroup`의 멤버입니다. OneLogin 매핑은 `PolicyAdmin` 값을 `FMCPolicyAdminGroup` 멤버에 대한 맞춤형 사용자 필드 `FMCUserRole`에 할당합니다. FMC에서는 프레드 및 `FMCPolicyAdminGroup`의 다른 멤버에게 Access Admin, Discovery Admin 및 Intrusion Admin 역할을 할당합니다.



- 이 다이어그램에서 sue@example.com은 OneLogin IdP 그룹 `FMCAdminGroup`의 멤버입니다. OneLogin 매핑은 FMCAdmin 값을 `FMCPolicyAdminGroup` 멤버에 대한 맞춤형 사용자 필드 `FMCUserRole`에 할당합니다. FMC는 Sue 및 `FMCAdminGroup`의 다른 멤버에게 관리자 역할을 할당합니다.

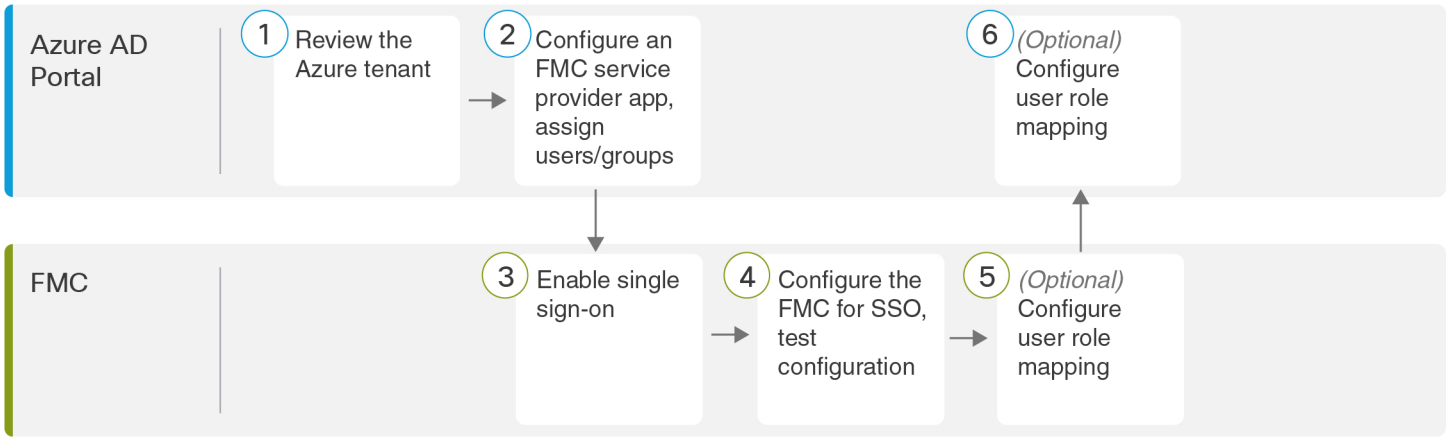


- 이 다이어그램에서 sean@example.com은 Idp 그룹 `FMCMaintGroup`의 멤버입니다. 이 그룹과 연결된 OneLogin 매핑이 없으므로 OneLogin은 사용자 지정 사용자 필드 `FMCUserRole`에 대해 값을 할당하지 않습니다. FMC에서는 유지 보수 사용자 역할이 아닌 기본 사용자 역할(보안 분석가 (읽기 전용))을 할당합니다.



Azure AD로 SSO(Single Sign-On, 단일 인증) 구성

Azure를 사용하여 SSO를 설정하려면 다음 작업을 참조하십시오.



1	Azure AD 포털	Azure 테넌트 검토, on page 104
2	Azure AD 포털	Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104

3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 77
4	FMC	Azure SSO용 FMC 구성, on page 106
5	FMC	FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108
6	Azure AD 포털	Azure IdP에서 사용자 역할 매핑 구성, on page 108

Azure 테넌트 검토

Azure AD는 Microsoft의 멀티 테넌트 클라우드 기반 ID 및 액세스 관리 서비스입니다. Azure에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션된 디바이스를 포함하는 엔터티를 테넌트라고 합니다. Azure 테넌트에 FMC를 추가하기 전에 해당 조직에 대해 잘 알고 있어야 합니다. 다음 질문을 고려해보십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 그룹의 Azure 테넌트 구성원 내에 있습니까?
- 사용자 및 그룹이 다른 디렉토리 제품입니까?
- FMC에서 SSO를 지원하려면 Azure 테넌트에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 FMC 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 FMC가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 Azure 테넌트 내의 사용자 및 그룹을 어떻게 구성해야합니까?
- 개별 사용자 또는 그룹을 기준으로 매핑할 FMC 역할을 구성할 수 있지만 단일 FMC 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

이 문서에서는 사용자가 이미 Azure Active Directory 포털에 익숙하며 Azure AD 테넌트에 대한 애플리케이션 관리자 권한이 있는 계정을 가지고 있다고 가정합니다. FMC는 테넌트별 단일 로그인 및 단일 로그 아웃 엔드포인트에서만 Azure SSO를 지원합니다. Azure AD Premium P1 이상 라이선스 및 전역 관리자 권한이 있어야 합니다. 자세한 내용은 Azure 설명서를 참조하십시오.

Azure용 FMC 서비스 제공자 애플리케이션 구성

Azure Active Directory 포털을 사용하여 Azure Active Directory 테넌트 내에 FMC 서비스 제공자 애플리케이션을 만들고 기본 구성 설정을 구성합니다.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- Azure 테넌트와 해당 사용자 및 그룹을 숙지하십시오. Azure 테넌트 검토, on page 104 참조하십시오.
- 필요한 경우 Azure 테넌트에서 사용자 계정 및/또는 그룹을 생성합니다.

  Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

  Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 FMC 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** Azure AD SAML 툴킷을 기본으로 사용하여 FMC 서비스 제공자 애플리케이션을 생성합니다.

단계 **2** 기본 **SAML** 구성에 대한 다음 설정을 사용하여 애플리케이션을 구성합니다.

- **Identifier(**엔티티 **ID)**의 경우, `/saml/metadata` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- 회신 **URL(**어설션 소비자 서비스 **URL)**의 경우 `/saml/acs` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **URL** 로그인의 경우 `/sam/acs` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`

단계 **3** FMC에서 로그인을 위한 사용자 이름을 사용자 계정과 연결된 이메일 주소로 지정하도록 애플리케이션의 고유 사용자 식별자 이름**(**이름 **ID)** 클레임을 편집합니다.

- **Source(**소스**)**에 대해 `Attribute(속성)`를 선택합니다.

- 소스 속성의 경우: `user.mail`을 선택합니다.

단계 **4** FMC에서 SSO를 보호하기 위한 인증서를 생성합니다. 인증서에 다음 옵션을 사용합니다.

- Signing option(서명 옵션)을 Sign SAML response and assertion(SAML 응답 및 어설션 서명)으로 변경합니다.
- Signing Algorithm(서명 알고리즘)으로 SHA-256을 선택합니다.

단계 **5** 인증서의 Base-64 버전을 로컬 컴퓨터에 다운로드합니다. FMC 웹 인터페이스에서 Azure SSO를 구성할 때 필요합니다.

단계 **6** 애플리케이션의 SAML 기반 로그인 정보에서 다음 값을 확인합니다.

- 로그인 **URL**
- **Azure AD** 식별자

FMC 웹 인터페이스에서 Azure SSO를 구성할 때 이러한 값이 필요합니다.

단계 **7** (선택 사항) FMC에 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 제공자 애플리케이션(Azure 포털의 페더레이션 메타데이터 **XML**이라고 하는)의 SAML XML 메타데이터 파일을 로컬 컴퓨터에 다운로드할 수 있습니다.

단계 **8** 기존 Azure 사용자 및 그룹을 FMC 서비스 애플리케이션에 할당합니다.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note 사용자 역할 매핑을 구성하려는 경우 개별 사용자 권한 또는 그룹 권한에 따라 역할을 매핑하도록 구성할 수 있지만 단일 FMC 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

Azure SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 사용하십시오.

Before you begin

- Azure AD 포털에서 FMC 서비스 제공자 애플리케이션을 생성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

Procedure

단계 **1** 이 단계는 FMC에서 SSO(Single Sign-On) 활성화, on page 77에서 곧바로 이어집니다. **Configure Azure Metadata(Azure** 메타 데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. Azure SSO 서비스 제공자 애플리케이션에서 검색한 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**의 경우 Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 6단계에서 적어둔 로그인 **URL**을 입력합니다.
     - **Identity Provider Issuer(ID** 공급자 발급자**)**에 대해 Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 6단계에서 적어둔 **Azure AD** 식별자를 입력합니다.
     - **X.509** 인증서의 경우 Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 5단계에서 Azure에서 다운로드한 인증서를 사용합니다. (텍스트 편집기를 사용하여 인증서 파일을 열고 내용을 복사하여 **X.509 Certificate(X.509** 인증서**)** 필드에 붙여 넣습니다.)
- Azure에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 7단계) 파일을 FMC에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 Azure 서비스 제공자 애플리케이션을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 역할 매핑을 구성할 수 있습니다. FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108의 내용을 참조하십시오. 역할 매핑을 구성하지 않도록 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108의 4단계에서 구성한 기본 사용자 역할이 할당됩니다.

FMC에서 Azure에 대한 사용자 역할 매핑 구성

FMC 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관 없이 동일합니다. 하지만 구성한 값은 반드시 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방법을 고려해야 합니다.

Before you begin

- 기존 Azure 사용자 및 그룹을 검토합니다. Azure 테넌트 검토, on page 104을 참조하십시오.
- FMC에 대한 SSO 서비스 제공자 애플리케이션을 구성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 내용을 참조하십시오.
- FMC에서 단일 인증(SSO)을 활성화 및 구성합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77 그리고 Azure SSO용 FMC 구성, on page 106을 참조하십시오.

Procedure

단계 **1** **System**(시스템) > **Users**(사용자)를 선택합니다.

단계 **2** **Single Sign-On**(단일 인증) 탭을 클릭합니다.

단계 **3** 고급 구성(역할 매핑)을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭 다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 Azure의 FMC 서비스 제공자 애플리케이션에 대해 생성하는 사용자 클레임의 이름과 일치해야 합니다. Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성, on page 109의 1 단계 또는 Azure IdP에서 그룹용 사용자 역할 매핑 구성, on page 110의 1 단계를 참조하십시오.

단계 **6** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. (FMC는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성값과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. Azure IdP에서 사용자 역할 매핑 구성, on page 108을 참조하십시오.

Azure IdP에서 사용자 역할 매핑 구성

개별 사용자 권한 또는 그룹 권한을 기반으로 Azure AD 포털에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한을 기반으로 매핑하려면 Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성을 참조하십시오.

- 그룹 권한을 기준으로 매핑하려면 Azure IdP에서 그룹용 사용자 역할 매핑 구성을 참조하십시오.

SSO 사용자가 FMC에 로그인하면 Azure는 Azure AD 포털에 설정된 애플리케이션 역할에서 값을 얻는 사용자 또는 그룹 역할 속성값을 FMC에 제공합니다. FMC에서는 해당 속성값을 SSO 설정의 각 FMC 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여합니다. (일치 항목이 없으면 FMC는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. FMC는 FMC 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 Azure에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. FMC는 Azure에 설정된 하나의 클레임만 사용하여 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 역할 매핑은 FMC에 더 효율적입니다. Azure 테넌트 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성

Azure에서 FMC 서비스 애플리케이션의 개별 사용자에 대한 역할 매핑을 설정하려면 Azure AD Portal을 사용하여 애플리케이션에 클레임을 추가하고, 애플리케이션의 등록 매니페스트에 역할을 추가한 다음 사용자에게 역할을 할당합니다.

Before you begin

- Azure 테넌트를 검토합니다. Azure 테넌트 검토, on page 104의 내용을 참조하십시오.
- Azure에서 FMC 서비스 제공자 애플리케이션 생성하고 구성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 내용을 참조하십시오.
- FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108에 설명된 대로 SSO 사용자 역할 매핑을 설정합니다.

Procedure

단계 **1** 다음 특성을 사용하여 FMC 서비스 애플리케이션의 SSO 설정에 사용자 클레임을 추가합니다.

- **Name(**이름**)**: FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 문자열을 사용합니다. (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108의 5단계 참조)
- **Source(**소스**)**: `Attribute(속성)`를 선택합니다.
- **Source attribute(**소스 속성**)**: `user.assignedroles`를 선택합니다.

단계 **2** FMC 서비스 애플리케이션의 매니페스트(JSON 형식)를 편집하고 애플리케이션 역할을 추가하여 SSO 사용자에게 할당할 FMC 사용자 역할을 나타냅니다. 가장 간단한 방법은 기존 애플리케이션 역할 정의를 복사하고 다음 속성을 변경하는 것입니다.

- `displayName`: AD Azure Portal에 표시될 역할의 이름입니다.
- `description`: 역할에 대한 짧은 설명입니다.
- `Id`: 매니페스트 내의 ID 속성 중에서 고유해야 하는 영문숫자 문자열입니다.
- `value`: 하나 이상의 FMC 사용자 역할을 나타내는 문자열입니다. (참고: Azure에서는 이 문자열에 공백을 허용하지 않습니다.)

단계 **3** FMC 서비스 애플리케이션에 할당된 각 사용자에 대해 해당 애플리케이션의 매니페스트에 추가한 애플리케이션 역할 중 하나를 할당합니다. 사용자가 SSO를 사용하여 FMC에 로그인할 때 해당 사용자에게 할당하는 애플리케이션 역할은 서비스 애플리케이션에 대한 클레임에서 Azure가 FMC에 전송하는 값입니다. FMC에서는 클레임을 SSO 설정에서 FMC 사용자 역할에 할당한 식과 비교하고 (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108의 6단계 참조), 일치하는 모든 FMC 사용자 역할을 사용자에게 할당합니다.

What to do next

- 다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

Azure IdP에서 그룹용 사용자 역할 매핑 구성

Azure에서 FMC 서비스 애플리케이션의 사용자 그룹에 대한 역할 매핑을 설정하려면 Azure AD Portal을 사용하여 애플리케이션에 클레임을 추가하고, 애플리케이션의 등록 매니페스트에 역할을 추가한 다음 그룹에 역할을 할당합니다.

Before you begin

- Azure 테넌트를 검토합니다. Azure 테넌트 검토, on page 104의 내용을 참조하십시오.
- Azure에서 FMC 서비스 제공자 애플리케이션 생성하고 구성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 104의 내용을 참조하십시오.
- FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** 다음 특성을 사용하여 FMC 서비스 애플리케이션의 SSO 설정에 사용자 클레임을 추가합니다.

- **Name(**이름**)**: FMC SSO 구성에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 문자열을 사용합니다. (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108의 5단계 참조)
- **Source(**소스**)**: `Attribute(속성)`를 선택합니다.
- **Source attribute(**소스 속성**)**: `user.assignedroles`를 선택합니다.

단계 **2** FMC 서비스 애플리케이션의 매니페스트(JSON 형식)를 편집하고 애플리케이션 역할을 추가하여 SSO 사용자에게 할당할 FMC 사용자 역할을 나타냅니다. 가장 간단한 방법은 기존 애플리케이션 역할 정의를 복사하고 다음 속성을 변경하는 것입니다.

- `displayName`: AD Azure Portal에 표시될 역할의 이름입니다.
- `description`: 역할에 대한 짧은 설명입니다.
- `Id`: 매니페스트 내의 ID 속성 중에서 고유해야 하는 영문숫자 문자열입니다.
- `value`: 하나 이상의 FMC 사용자 역할을 나타내는 문자열입니다. (Azure에서는이 문자열에 공백을 허용하지 않습니다.)

단계 **3** FMC 서비스 애플리케이션에 할당된 각 그룹에 대해 해당 애플리케이션의 매니페스트에 추가한 애플리케이션 역할 중 하나를 할당합니다. 사용자가 SSO를 사용하여 FMC에 로그인할 때 해당 사용자 그룹에 할당하는 애플리케이션 역할은 서비스 애플리케이션에 대한 클레임에서 Azure가 FMC에 전송하는 값입니다. FMC에서는 클레임을 SSO 설정에서 FMC 사용자 역할에 할당한 식과 비교하고 (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 108의 6단계 참조), 일치하는 모든 FMC 사용자 역할을 사용자에게 할당합니다.

What to do next

다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

Azure 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 FMC의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 Azure의 FMC 서비스 제공자 애플리케이션 설정에 있습니다.

Note 개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 설정할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC는 Azure에 설정된 하나의 클레임만 사용하여 역할 매핑을 지원할 수 있습니다.

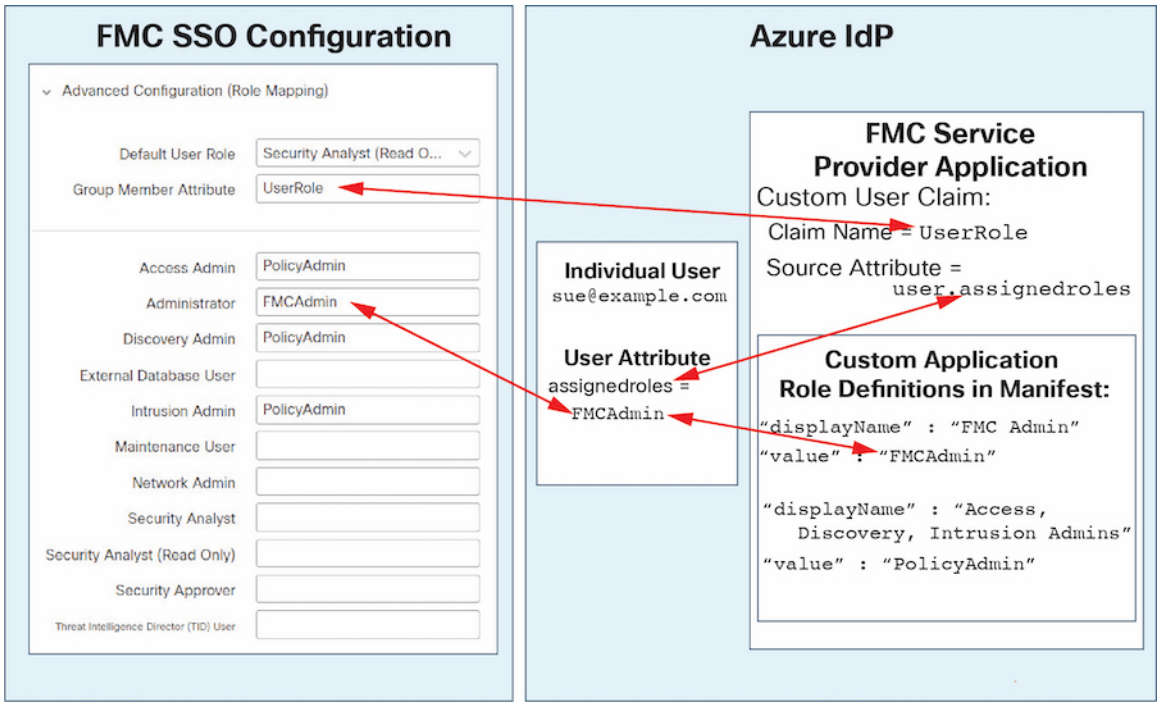
개별 사용자 계정에 대한 Azure 역할 매핑 예제

개별 사용자에 대한 역할 매핑에서 Azure FMC 서비스 애플리케이션에는 매니페스트 내에 정의된 사용자 지정 역할이 있습니다. (이 경우에는 FMCAdmin 및 PolicyAdmin입니다.) 이러한 역할은 사용자에게 할당할 수 있습니다. Azure는 해당 사용자의 할당된 역할 속성에 각 사용자에 대한 역할 할당을 저장합니다. 애플리케이션에 맞춤형 사용자 클레임도 정의되어 있으며, 이 클레임은 SSO를 통해 FMC에 로그인하는 사용자에 대해 할당된 사용자 역할에서 해당 값을 가져오도록 설정됩니다. Azure는 SSO 로그인 프로세스 중에 FMC에 클레임 값을 전달하고 FMC에서는 클레임 값을 FMCSSO 설정의 각 FMC 사용자 역할에 할당된 문자열과 비교합니다.

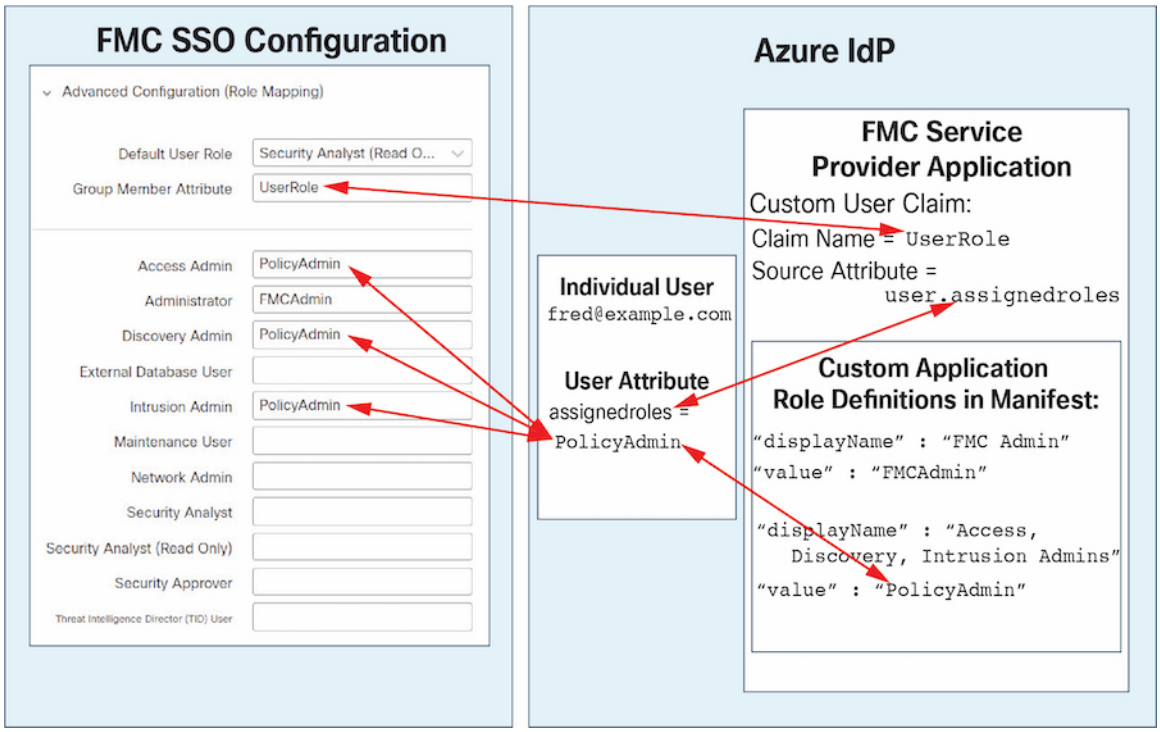
다음 다이어그램은 FMC 및 Azure 설정의 관련 필드와 값이 개별 계정에 대한 사용자 역할 매핑에서 서로 어떻게 대응하는지를 보여줍니다. 각 다이어그램은 FMC 및 Azure AD 포털에서 동일한 SSO 구

성을 사용하지만, Azure AD 포털의 각 사용자에 대한 설정은 FMC에서 각 사용자에게 서로 다른 역할을 할당하는 방식이 다릅니다.

- 이 다이어그램에서 sue@example.com은 assignedroles 속성값 `FMCAdmin`을 사용하며, FMC는 FMC 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 assignedroles 속성값 `PolicyAdmin`을 사용하며 FMC는 액세스 관리자, 검색 관리자 및 침입 관리자 역할을 할당합니다.



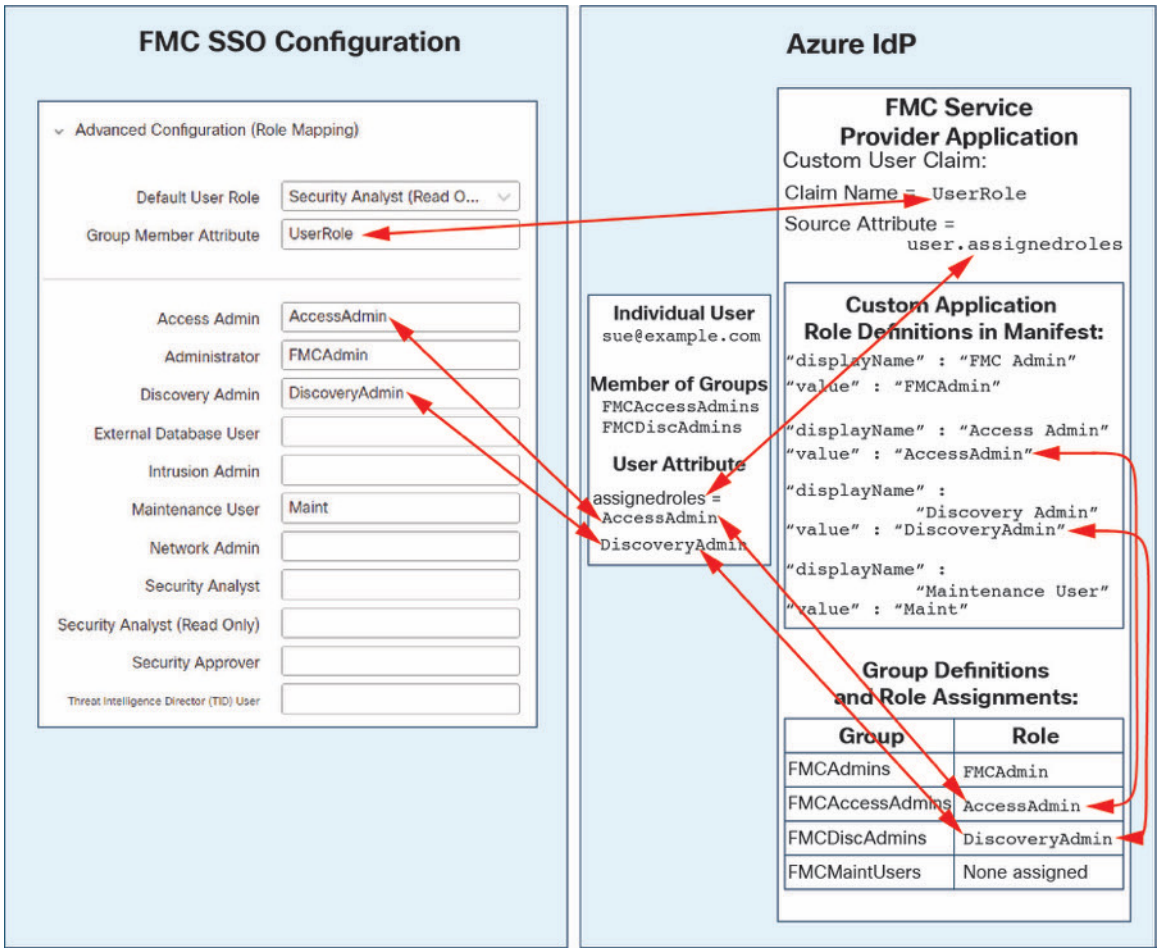
- FMC를 위해 Azure 서비스 애플리케이션에 할당된 기타 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석가(읽기 전용)가 할당됩니다.
  - assignedroles 속성에 할당된 값이 없습니다.
  - assignedroles 속성에 할당된 값이 FMC의 SSO 설정에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **Azure** 역할 매핑 예

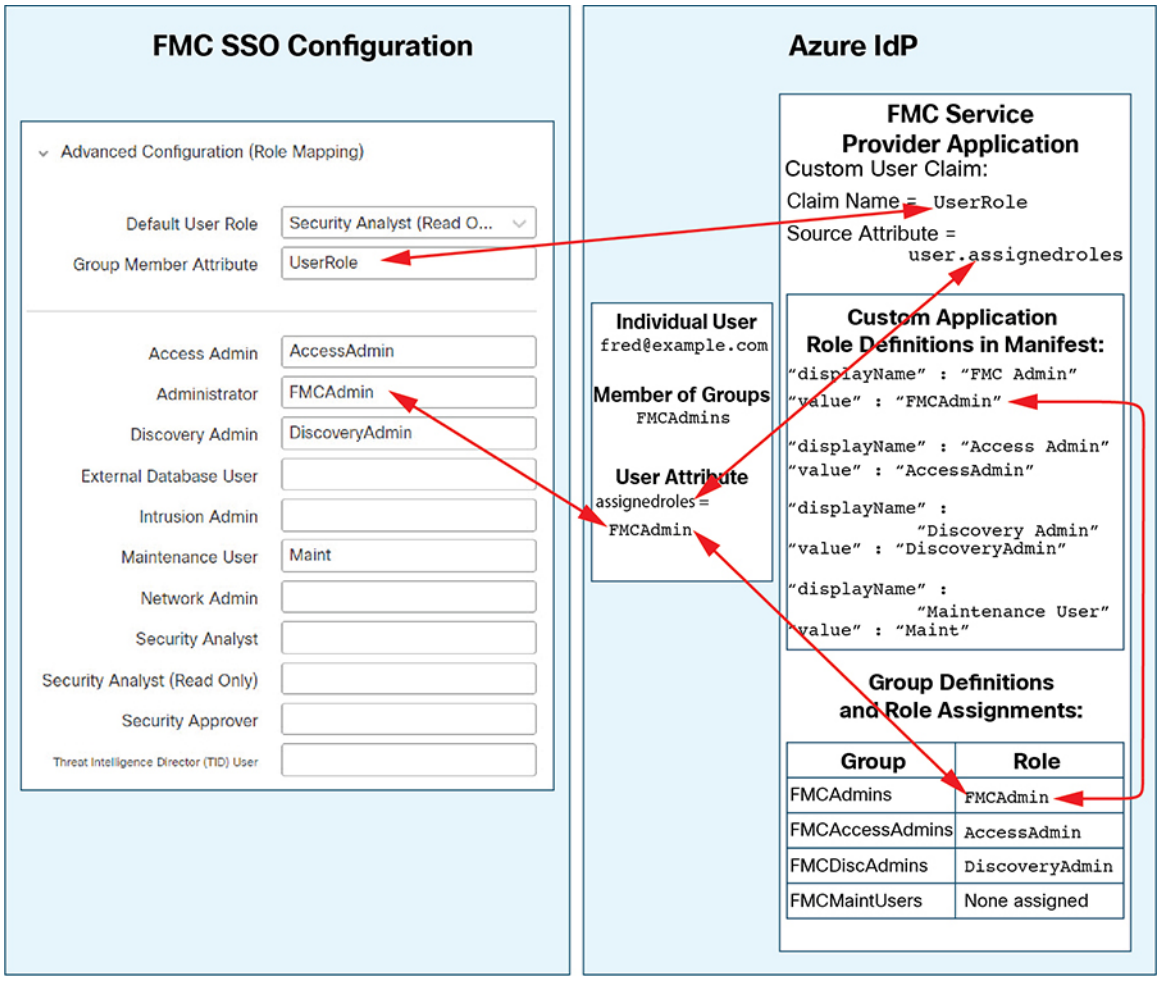
그룹에 대한 역할 매핑에서 Azure FMC 서비스 애플리케이션에는 매니페스트 내에 정의된 사용자 지정 역할이 있습니다. (이 경우 FMCAdmin, AccessAdmin, Discovery Admin 및 Maint입니다.) 이러한 역할은 그룹에 할당할 수 있습니다. Azure는 해당 그룹의 할당된 역할 속성에 각 그룹 멤버에 대한 역할 할당을 전달합니다. 애플리케이션에 맞춤형 사용자 클레임도 정의되어 있으며, 이 클레임은 SSO를 통해 FMC에 로그인하는 사용자에 대해 할당된 사용자 역할에서 해당 값을 가져오도록 설정됩니다. Azure는 SSO 로그인 프로세스 중에 FMC에 클레임 값을 전달하고 FMC에서는 클레임 값을 FMCSSO 설정의 각 FMC 사용자 역할에 할당된 문자열과 비교합니다.

다음 다이어그램은 FMC 및 Azure 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치하는지를 보여줍니다. 각 다이어그램은 FMC 및 Azure AD 포털에서 동일한 SSO 구성을 사용하지만, Azure AD 포털의 각 사용자에 대한 설정은 FMC에서 각 사용자에게 서로 다른 역할을 할당하는 방식이 다릅니다.

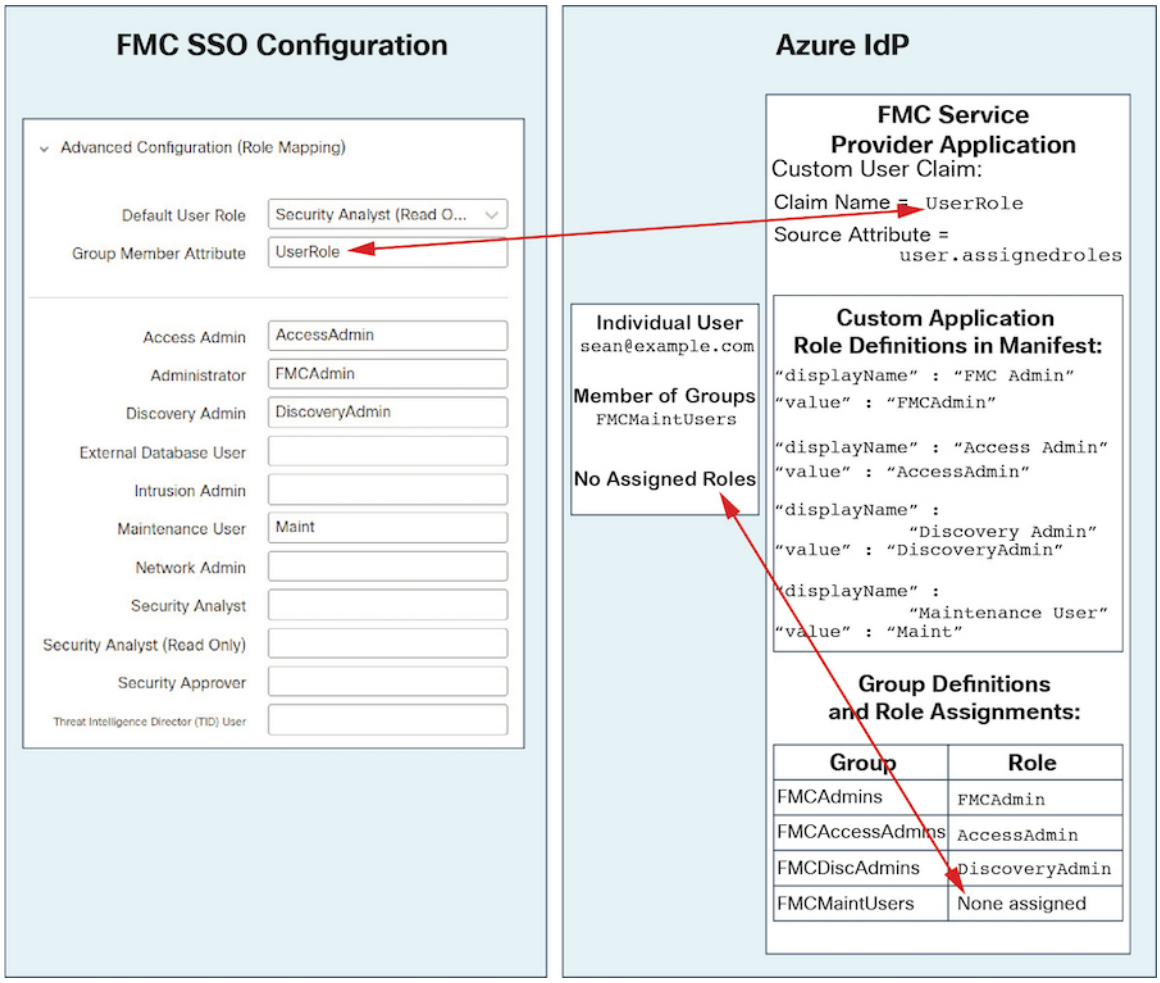
- 이 다이어그램에서 sue@example.com은 `FMCAccessAdmins` 및 `FMCDiscoveryAdmins` 그룹의 멤버입니다. 이러한 그룹에서 맞춤형 역할 `AccessAdmin` 및 `DiscoveryAdmin`을 상속합니다. Sue가 SSO를 사용하여 FMC에 로그인하면 FMC에서는 액세스 관리자 및 검색 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 `FMCAdmins` 그룹의 멤버이며, 이 그룹에서 맞춤형 역할 `FMCAdmin`을 상속합니다. 프레드가 SSO를 사용하여 FMC에 로그인하면 FMC는 관리자 역할을 할당합니다.

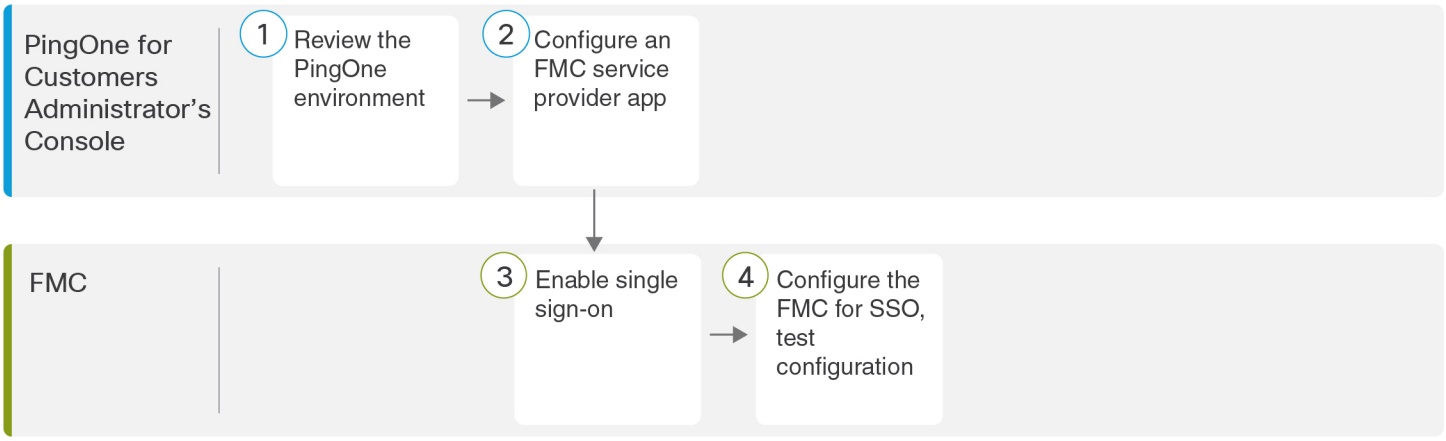


- 이 다이어그램에서 sean@example.com은 `FMCMaintUsers` 그룹의 멤버입니다. 그러나 Azure FMC 서비스 제공자 애플리케이션 내에서 `FMCMaintUsers`에 맞춤형 역할이 할당되지 않았기 때문에, 해당 사용자에게 할당된 역할이 없으며, SSO를 사용하여 FMC에 로그인할 때, FMC는 기본 역할인 Security Analyst(읽기 전용)를 지정합니다.



PingID로 SSO(Single Sign-On) 구성

PingID의 PingOne for Customers 제품을 사용하여 SSO를 설정하려면 다음 작업을 참조하십시오.



1	PingOne for Customers 관리자 콘솔	PingID PingOne for Customers 환경 검토, on page 117.
2	PingOne for Customers 관리자 콘솔	PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 117.
3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 77.
4	FMC	PingID PingOne for Customers을 사용하여 SSO용 FMC을 구성합니다., on page 119.

PingID PingOne for Customers 환경 검토

PingOne for Customers는 PingID의 클라우드 호스팅 IDaaS(Identity-as-a-Service) 제품입니다. PingOne for Customers에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션된 디바이스를 포함하는 엔터티를 환경이라고 합니다. PingOne 환경에 FMC를 추가하기 전에 해당 조직에 대해 잘 알고 있어야합니다. 다음 질문을 고려해 보십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- FMC에 대한 SSO 액세스를 지원하려면 사용자를 더 추가해야 합니까?

이 문서에서는 사용자가 PingOne for Customers 관리자 콘솔에 대해 잘 알고 있으며 조직 관리자 역할의 계정을 가지고 있다고 가정합니다.

PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정

PingOne for Customers 관리자 콘솔을 사용하여 PingOne for Customers 환경에서 FMC 서비스 제공자 애플리케이션을 생성하고 기본 구성 설정을 구성합니다. 이 문서에서는 모든 기능을 갖춘 SSO 환경을 설정하는 데 필요한 PingOne for Customers 기능을 전부 설명하지 않습니다. 가령 사용자를 생성하려면 PingOne for Customers 문서를 참조하면 됩니다.

Before you begin

- PingOne for Customers 환경 및 해당 사용자를 숙지하십시오.
- 필요한 경우, 사용자를 추가로 생성합니다.

Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 FMC 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** 다음 설정을 사용하여 사용자 환경에서 애플리케이션을 생성하려면 PingOne for Customers 관리자 콘솔을 확인하십시오.

- **Web App(**웹 앱**)** 애플리케이션 유형을 선택합니다.
- **SAML** 연결 유형을 선택합니다.

단계 **2** SAML 연결에 대해 다음 설정으로 애플리케이션을 구성합니다.

- **ACS URL**의 경우, `/sam/acs` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Signing Certificate(**서명 인증서**)**에 대해 Sign Assertion & Response(어설션 서명 및 응답)를 선택합니다.
- **Signing Algorithm(**서명 알고리즘**)**에 대해 RSA_SHA256을 선택합니다.
- **Entity ID(**엔티티 **ID)**의 경우, `/saml/metadata` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- **SLO Binding(SLO** 바인딩**)**의 경우, HTTP POST를 선택합니다.
- **Assertion Validity Duration(**어설션 유효 기간**)**에 300을 입력합니다.

단계 **3** 애플리케이션의 SAMLConnection 정보에서 다음 값을 확인합니다.

- **SSO(Single Sign-On)** 서비스
- 발급자 **ID**

FMC 웹 인터페이스에서 PingID의 PingOne for Customers 제품을 사용하여 SSO를 설정할 때 이러한 값이 필요합니다.

단계 **4** **SAML ATTRIBUTES(SAML** 속성**)**의 경우, 단일 필수 속성에 대해 다음을 선택합니다.

- **PINGONE USER ATTRIBUTE(PINGONE** 사용자 속성**):** `이메일 주소`
- **APPLICATION ATTRIBUTE(**애플리케이션 속성**):** `saml_subject`

단계 **5** X509 PEM(`.crt`) 형식으로 서명 인증서를 다운로드하여 로컬 컴퓨터에 저장합니다.

단계 **6** (선택 사항) FMC에 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 제공자 애플리케이션의 SAML XML 메타데이터 파일을 로컬 컴퓨터에 다운로드할 수 있습니다.

단계 **7** 애플리케이션을 활성화합니다.

What to do next

SSO(Single Sign-On)를 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

PingID PingOne for Customers을 사용하여 SSO용 FMC을 구성합니다.

FMC 웹 인터페이스에서 다음 지침을 참조하십시오.

Before you begin

- PingOne for Customers Administrator Console에서 FMC 서비스 제공자 애플리케이션을 생성합니다. PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 117의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

Procedure

단계 **1** 이 단계는 FMC에서 SSO(Single Sign-On) 활성화, on page 77에서 곧바로 이어집니다. **Configure PingID Metadata(PingID** 메타데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 컨피그레이션 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. PingOne for Customers Administrator Console에서 검색한 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**의 경우 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 117 3단계에서 적어둔 **SSO(Single Sign-On)** 서비스를 입력합니다.
     - **Identity Provider Issuer(ID** 제공자 발급자**)**의 경우 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 117 3단계에서 적어둔 발급자 **ID**를 입력합니다.
     - **X.509** 인증서의 경우 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 117 5단계 중 PingOne for Customers에서 다운로드한 인증서를 사용합니다. (텍스트 편집기를 사용하여 인증서 파일을 열고 내용을 복사하여 **X.509 Certificate(X.509** 인증서**)** 필드에 붙여 넣습니다.)

- PingOne for Customers에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우, (PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 117의 6단계) 파일을 FMC에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Advanced Configuration(Role Mapping)(**고급 구성**(**역할 매핑**))**을 펼칩니다.

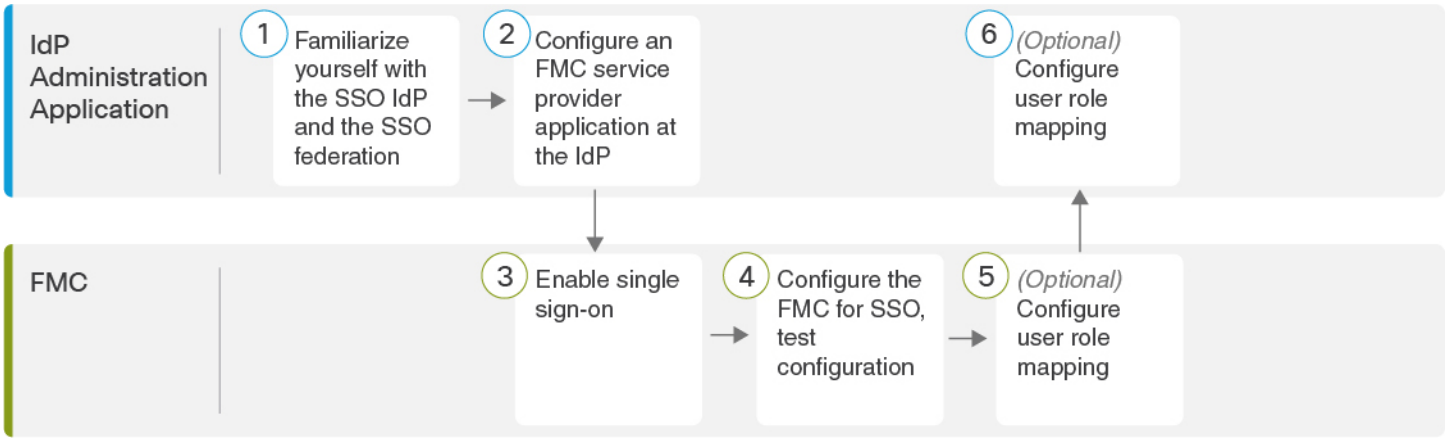
단계 **5** **Default User Role(**기본 사용자 역할**)** 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **6** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 PingOne for Customers 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **7** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

SAML 2.0 규정준수 SSO 제공자로 SSO(Single Sign-On) 구성

FMC에서는 SAML 2.0 SSO 프로토콜을 준수하는 모든 SSO ID 제공자(IdP)에서 SSO(Single Sign-On)를 지원합니다. 광범위한 SSO 제공자를 사용하기 위한 일반적인 지침은 높은 수준에서 수행할 작업을 처리해야 합니다. 이 문서에서 구체적으로 다루지 않은 제공자를 사용하여 SSO를 설정하려면 선택한 IdP를 능숙하게 다루어야 합니다. 이러한 작업을 통해 SAML 2.0을 준수하는 SSO 제공자를 사용하여 SSO(Single Sign-On)에 대해 FMC를 설정하는 단계를 결정할 수 있습니다.



1	IdP 관리 애플리케이션	SSO ID 제공자 및 SSO 페더레이션을 숙지합니다., on page 121.

2	IdP 관리 애플리케이션	SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 122.
3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 77.
4	FMC	SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 123.
5	FMC	SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정, on page 125.
6	IdP 관리 애플리케이션	SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정, on page 126에 전달하는 고성능 고속 어플라이언스입니다.

SSO ID 제공자 및 SSO 페더레이션을 숙지합니다.

다음 사항을 고려하여 IdP 벤더 설명서를 읽으십시오.

- SSO 제공자가 사용자에게 IdP를 사용하기 전에 서비스를 구독하거나 등록하도록 요구합니까?
- SSO 제공자가 일반적인 SSO 개념에 사용하는 용어는 무엇입니까? 예를 들어 페더레이션 서비스 공급자 애플리케이션 그룹을 참조하기 위해 Okta는 "org"를 사용하고 Azure는 "tenant"를 사용합니다.
- SSO 제공자가 SSO만 지원합니까 아니면 여러 요인(예: 다단계 인증 또는 도메인 관리)을 지원합니까? (이는 기능 간에 공유되는 일부 요소(특히 사용자 및 그룹)의 구성에 영향을 줄 수 있습니다.)
- IdP 사용자 계정에서 SSO를 구성하려면 어떤 권한이 필요합니까?
- SSO 제공자가 서비스 제공자 애플리케이션에 대해 설정해야 하는 구성은 무엇입니까? 예를 들어 Okta는 FMC와의 통신을 보호하기 위해 X509 인증서를 자동으로 생성하지만, Azure에서는 Azure 포털 인터페이스를 사용하여 해당 인증서를 생성해야 합니다.
- 사용자 및 그룹은 어떻게 생성되고 구성됩니까? 사용자는 그룹에 어떻게 할당됩니까? 사용자 및 그룹은 어떻게 서비스 제공자 애플리케이션에 대한 액세스 권한을 부여 받습니까?
- SSO 연결을 테스트하기 전에 SSO 제공자가 하나 이상의 사용자를 서비스 제공자 애플리케이션에 할당해야 합니까?
- SSO 제공자가 사용자 그룹을 지원합니까? 사용자 및 그룹 속성은 어떻게 구성됩니까? SSO 구성에서 어떻게 FMC 사용자 역할에 속성을 매핑할 수 있습니까

- FMC에서 SSO를 지원하려면 페더레이션에 사용자 또는 그룹을 더 추가해야 합니까?
- 사용자가 그룹의 페더레이션 구성원 내에 있습니까?
- 사용자 및 그룹 정의가 IdP에 기본적이거나 Active Directory, RADIUS 또는 LDAP와 같은 사용자 관리 애플리케이션에서 가져온 것입니까?
- 어떤 종류의 사용자 역할을 지정하시겠습니까? (사용자 역할을 할당하지 않도록 선택하는 경우 FMC는 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 사용자 역할 매핑을 위한 계획을 지원하려면 페더레이션 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성

일반적으로 SSO 제공자는 각 연동 애플리케이션에 대해 IdP에서 서비스 제공자 애플리케이션을 구성해야 합니다. SAML 2.0 SSO를 지원하는 모든 IdP는 서비스 제공자 애플리케이션에 대해 동일한 구성 정보가 필요하지만 일부 IdP는 자동으로 일부 구성 설정을 생성하는 반면, 일부는 모든 설정을 직접 구성해야 합니다.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 IdP에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- SSO 페더레이션 그리고 해당 사용자 및 그룹을 숙지하십시오. SSO ID 제공자 및 SSO 페더레이션을 숙지합니다., on page 121의 내용을 참조하십시오.
- IdP 계정에 이 작업을 수행하는 데 필요한 권한이 있는지 확인합니다.
- 필요한 경우 SSO 페더레이션에서 사용자 계정 및/또는 그룹을 생성합니다.

  Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL로 FMC 웹 인터페이스에 연결할 수 있는 경우 (예: 정규화된 도메인 이름 및 IP 주소) SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** IdP에서 새 서비스 제공자 애플리케이션을 생성합니다.

단계 **2** IdP에 필요한 값을 구성합니다. FMC에 SAML 2.0 SSO 기능을 지원하는 데 필요한 아래에 나열된 필드를 포함해야 합니다. 각기 다른 SSO 서비스 제공자가 SAML 개념에 대해 다른 용어를 사용하므로 이 목록은 IdP 애플리케이션에서 올바른 설정을 찾는 데 도움이 되도록 이러한 필드에 대한 대체 이름을 제공합니다.

- 서비스 제공자 엔티티 ID, 서비스 제공자 식별자, 대상 URI: URL 형식의 서비스 제공자(FMC)에 대한 전역 고유 이름. 이를 생성하려면 `/saml/metadata` 문자열(예: `https://ExampleFMC/saml/metadata`)을 FMC 로그인 URL에 추가합니다.
- SSO(Single Sign-On, 단일 인증) URL, 수신자 URL, 어설션 소비자 서비스 URL: 브라우저가 IdP를 대신하여 정보를 전송하는 서비스 제공자(FMC) 주소입니다. 이를 생성하려면 FMC 로그인 URL에 `saml/acs` 문자열(예: `https://ExampleFMC/saml/acs`)을 추가합니다.
- X.509 인증서: FMC와 IdP 간의 통신을 보호하기 위한 인증서입니다. 일부 IdP는 인증서를 자동으로 생성할 수 있으며, 일부는 IdP 인터페이스를 사용하여 명시적으로 생성해야 할 수 있습니다.

단계 **3** (선택적으로 애플리케이션에 그룹을 할당하는 경우) 개별 사용자를 FMC 애플리케이션에 할당합니다. (FMC 애플리케이션에 그룹을 할당하려는 경우 해당 그룹의 멤버를 개인으로 할당하지 마십시오.)

단계 **4** (애플리케이션에 개별 사용자를 할당하는 경우엔 선택 사항입니다.) FMC 애플리케이션에 사용자 그룹을 할당합니다.

단계 **5** (선택 사항) 일부 IdP는 이 작업에서 구성한 정보가 포함된 SAML XML 메타데이터 파일을 생성하는 기능을 제공합니다. IdP가 이 기능을 제공하는 경우, 파일을 로컬 컴퓨터에 다운로드하여 FMC에서 SSO 구성 프로세스를 쉽게 수행할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 사용하십시오. SAML 2.0 호환 SSO 제공자를 사용하여 SSO에 대해 FMC를 구성하려면 IdP의 정보가 필요합니다.

Before you begin

- SSO 페더레이션의 조직과 해당 사용자 및 그룹을 검토합니다.
- IdP에서 FMC 서비스 제공자 애플리케이션을 구성합니다. SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 123의 내용을 참조하십시오.
- IdP에서 서비스 제공자 애플리케이션에 대한 다음 SSO 구성 정보를 수집합니다. 각기 다른 SSO 서비스 제공자가 SAML 개념에 대해 다른 용어를 사용하므로 이 목록은 IdP 애플리케이션에서 올바른 값을 찾는 데 도움이 되도록 이러한 필드에 대한 대체 이름을 제공합니다.
  - ID 공급자 SSO(Single Sign-On) URL, 로그인 URL: 브라우저가 FMC 대신 정보를 전송하는 IdP URL입니다.
  - ID 제공자 발급자, ID 제공자 발급자 URL, 발급자 URL: IdP의 전역 고유 이름으로, 대개 URL 형식으로 지정됩니다.
  - FMC와 IdP 간의 통신을 보호하기 위한 X.509 디지털 인증서.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77의 내용을 참조하십시오.

Procedure

단계 **1** (이 절차는 FMC에서 SSO(Single Sign-On) 활성화, on page 77에서 곧바로 이어집니다.) **Configure SAML Metadata(SAML** 메타데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 컨피그레이션 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. SSO 서비스 제공자 애플리케이션에서 이전에 얻은 다음 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**
     - **ID** 제공자 발급자
     - **X.509** 인증서
- IdP에서 생성된 XML 메타데이터 파일을 저장한 경우(SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 122의 5 단계) FMC에 파일을 업로드 할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 4 **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 IdP의 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 5 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정, on page 125의 내용을 참조하십시오. 역할 매핑을 구성하지 않도록 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정, on page 125의 4단계에서 구성한 기본 사용자 역할이 할당됩니다.

SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정

SAML SSO 사용자 역할 매핑을 구현하려면 IdP 및 FMC에서 조정 구성을 설정해야 합니다.

- IdP에서 사용자 또는 그룹 속성을 설정하여 사용자 역할 정보를 전달하고 값을 할당합니다. IdP는 SSO 사용자를 인증하고 권한을 부여하고 나서 FMC에 이를 전송합니다.
- FMC에서 값을 사용자에게 할당할 각 FMC 사용자 역할과 연결합니다.

IdP가 권한 있는 사용자와 연결된 사용자 또는 그룹 속성을 FMC에 전송하는 경우, FMC에서는 속성 값을 각 FMC 사용자 역할에 연결된 값과 비교하고 일치를 생성하는 모든 역할을 사용자에게 할당합니다. FMC는 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 정규식으로 두 값을 모두 처리하며 비교를 수행합니다.

FMC 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다. IdP가 사용자 또는 그룹 속성에 대해 구문 제한을 적용할 수 있습니다. 그러한 경우에는 역할 이름 및 해당 요건과 호환되는 정규식으로 사용자 역할 매핑 체계를 구성해야 합니다.

Before you begin

- FMC에 대한 SSO 서비스 제공자 애플리케이션을 설정합니다. SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 122의 내용을 참조하십시오.
- FMC에서 SSO(Single Sign-On)를 활성화하고 설정합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 77 및 SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 123의 내용을 참조하십시오.

Procedure

단계 1 **System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 2 **Single Sign-On(**단일 인증**)** 탭을 클릭합니다.

단계 **3** **Advanced Configuration (Role Mapping)**(고급 설정(역할 매핑))을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 사용자 또는 그룹에 대한 사용자 역할을 매핑하기 위해 IdP FMC 서비스 제공자 애플리케이션에 설정된 속성 이름과 일치해야 합니다. (SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정, on page 126의 1단계 참조)

단계 **6** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. (FMC는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성값과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정, on page 126의 내용을 참조하십시오.

SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정

사용자 역할 매핑을 구성하는 자세한 단계는 IdP마다 다릅니다. 통신 사업자 애플리케이션에 대한 사용자 지정 사용자 또는 그룹 특성을 생성하는 방법을 결정하고 IdP에서 각 사용자 또는 그룹의 특성에 값을 할당하여 FMC에 사용자 또는 그룹 권한을 전달해야 합니다. 다음 사항에 주의하십시오.

- IdP가 서드 파티 사용자 관리 애플리케이션(예: Active Directory, LDAP 또는 Radius)에서 사용자 또는 그룹 프로파일을 가져오는 경우, 이는 역할 매핑에 속성을 사용하는 방법에 영향을 줄 수 있습니다.
- SSO 페더레이션 전체에서 사용자 및 그룹 역할 정의를 고려합니다.
- FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 IdP에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.
- 여러 사용자가 있는 경우, 그룹 역할 매핑은 일반적으로 FMC에 더 효율적입니다.
- FMC 애플리케이션에 사용자 그룹을 할당하는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.
- FMC 사용자 역할과의 일치를 확인하기 위해 FMC에서는 IdP에서 수신한 사용자 및 그룹 역할 속성 값을 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 정규식으로 처리합니다. IdP가 사용자 또는 그룹 속성에 대해 특정 구문 제한을 적용할 수 있습니다. 그러한 경우에는 역할 이름 및 해당 요건과 호환되는 정규식으로 사용자 역할 매핑 체계를 구성해야 합니다.

Before you begin

- IdP 계정에 이 작업을 수행하는 데 필요한 권한이 있는지 확인합니다.

- IdP에서 FMC 서비스 제공자 애플리케이션을 구성합니다(SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 122 참조).

Procedure

단계 **1** IdP에서 FMC로 전송될 속성을 생성하거나 지정하여 각 사용자 로그인에 대한 역할 매핑 정보를 포함합니다. 이는 사용자 속성, 그룹 속성 또는 IdP 또는 서드 파티 사용자 관리 애플리케이션에서 유지 관리하는 사용자 또는 그룹 정의와 같은 소스에서 값을 가져오는 다른 속성일 수 있습니다.

단계 **2** 속성의 값을 가져오는 방법을 구성합니다. 가능한 값을 FMC SSO 구성의 사용자 역할과 연결된 값으로 조정합니다.

웹 인터페이스의 사용자 역할 맞춤화

각 사용자 어카운트는 사용자 역할과 함께 정의해야 합니다. 이 섹션에서는 사용자 역할을 관리하는 방법 및 웹 인터페이스 액세스에 대한 맞춤형 사용자 역할을 구성하는 방법을 설명합니다. 기본 사용자 역할에 대해서는 사용자 역할, 50 페이지의 내용을 참조하십시오.

맞춤형 사용자 역할 생성

맞춤형 사용자 역할은 메뉴 기반 및 시스템 권한 집합을 보유할 수 있으며, 사전 정의된 사용자 역할 또는 또 다른 맞춤형 사용자 역할을 원래 그대로 유지하거나 복사하거나 또 다른 디바이스에서 가져올 수 있습니다.

참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 맞춤형 사용자 역할은 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)** 탭과 **System(**시스템**)** > **Users(**사용자**)** > **User Roles(**사용자 역할**)** 탭의 역할 이름에 **(**읽기 전용**)**이라고 자동으로 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다.

사용자 지정 역할을 생성하거나 기존 사용자 지정 역할을 수정하는 경우, 역할에 대해 선택된 모든 허가가 읽기 전용 기준을 충족한다면 시스템은 **(**읽기 전용**)**을 역할 이름에 자동으로 적용합니다. 텍스트 문자열을 역할 이름에 수동으로 추가하는 방법으로는 역할을 읽기 전용을 만들 수 없습니다. 동시 세션 제한에 대한 자세한 내용은 전역 사용자 구성, 1385 페이지의 내용을 참조하십시오.

주의 메뉴 기반 사용자 관리 권한이 있는 사용자는 자신의 권한을 높이거나 관리자 사용자 역할을 포함하여 광범위한 권한으로 새 사용자 계정을 생성할 수 있습니다. 시스템 보안을 위해 사용자 관리 권한이 있는 사용자 목록을 적절하게 제한하는 것이 좋습니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** 다음 방법 중 하나로 새 사용자 역할을 추가합니다.

- **Create User Role(**사용자 역할 생성**)**을 클릭합니다.
- 복사하려는 사용자 역할 옆에 있는 복사 ( )을 클릭합니다.
- 또 다른 디바이스에서 맞춤형 사용자 역할을 가져옵니다.

  1. 기존 디바이스에서 내보내기( )을 클릭하고 해당 역할을 PC에 저장합니다.
  2. 새 디바이스에서 **System(**시스템**)** > **Tools(**도구**)** > **Import(**가져오기/내보내기**)**를 선택합니다.
  3. **Upload Package(**패키지 업로드**)**를 클릭한 후 지침에 따라 새 디바이스에 저장된 사용자 역할을 가져 옵니다.

단계 **4** 새 사용자 역할의 **Name(**이름**)**을 입력합니다. 사용자 역할 이름은 대/소문자를 구별합니다.

단계 **5** (선택 사항) **Description(**설명**)**을 추가합니다.

단계 **6** 새 역할에 대해 **Menu-Based Permissions(**메뉴 기반 권한**)**를 선택합니다.

권한을 선택하면 모든 하위 항목이 선택되고 다중 값 권한이 첫 번째 값을 사용합니다. 상위 수준 권한의 선택을 취소할 경우 모든 하위 권한의 선택도 취소됩니다. 권한을 선택하지만 권한의 하위 항목은 선택하지 않는 경우, 권한이 기울임꼴 텍스트로 나타납니다.

사전 정의된 사용자 역할을 맞춤형 역할의 기반으로 사용하기 위해 복사하면 사전 정의 역할과 관련된 권한이 미리 선택됩니다.

맞춤형 사용자 역할에 제한적 검색을 적용할 수 있습니다. 이러한 검색은 사용자가 Analysis(분석) 메뉴에서 사용 가능한 페이지의 테이블에서 볼 수 있는 데이터를 제한합니다. 먼저 비공개 저장 검색을 생성하고 해당 메뉴 기반 권한의 **Restrictive Search(**제한된 검색**)** 드롭다운 메뉴에서 이를 선택하는 방법으로 제한적 검색을 구성할 수 있습니다.

단계 **7** (선택 사항) **External Database Access(**외부 데이터 액세스**)** 확인란을 선택하고 새 역할에 대한 데이터베이스 액세스 권한을 설정합니다.

이 옵션은 JDBC SSL 연결을 지원하는 애플리케이션을 사용하여 데이터베이스에 읽기 전용 액세스를 제공합니다. 타사 애플리케이션으로 디바이스를 인증하려면 시스템 설정에서 데이터베이스 액세스를 활성화해야 합니다.

단계 **8** (선택 사항) 새 사용자 역할에 대한 확대 권한을 설정하려면 사용자 역할 확대 활성화, 130 페이지을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

예

액세스 제어 관련 기능을 위한 맞춤형 사용자 역할을 생성해 사용자가 액세스 제어 및 연결된 정책을 보고 수정할 수 있는지 여부를 지정할 수 있습니다.

다음 테이블에는 생성할 수 있는 맞춤형 역할과 각 예에 대해 부여되는 사용자 권한이 나열되어 있습니다. 이 테이블에는 각 맞춤형 역할에 필요한 권한이 나열되어 있습니다. 이 예에서 정책 승인자는 액세스 제어 및 침입 정책을 볼 수 있지만 수정할 수는 없습니다. 정책 승인자는 디바이스에 구성 변경 사항을 구축할 수도 있습니다.

표 *1:* 샘플 액세스 제어 맞춤형 역할

맞춤형 역할 권한	예: 액세스 제어 편집기	예: 침입 및 네트워크 분석 편집기	예: 정책 승인자
액세스 제어	예	아니요	예
액세스 제어 정책	예	아니요	예
액세스 제어 정책 수정	예	아니요	아니요
침입 정책	아니요	예	예
침입 정책 수정	아니요	예	아니요
디바이스에 구성 구축	아니요	아니요	예

사용자 역할 비활성화

어떤 역할을 비활성화하면 해당 역할을 할당 받은 모든 사용자에게서 역할 및 관련 권한이 제거됩니다. 사전 정의 사용자 역할은 삭제할 수 없지만 이를 비활성화할 수는 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 사용자 역할을 표시하며 이러한 역할은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 사용자 역할도 표시되지만, 이러한 역할은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 사용자 역할을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** 활성화하거나 비활성화할 사용자 역할의 옆에 있는 슬라이더를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

어떤 역할의 사용자가 로그인한 상태에서 Lights-Out Management로 해당 역할을 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자 또는 사용자 역할을 복원할 경우, 사용자가 다시 웹 인터페이스에 로그인해야 IPMItool 명령에 다시 액세스할 수 있습니다.

사용자 역할 확대 활성화

이러한 기본 역할 외에 대상 지정된 다른 사용자 역할의 권한을 임시로 얻을 수 있는 권한과 비밀번호를 맞춤형 사용자 역할에 제공할 수 있습니다. 그러면 부재 시 어떤 사용자를 손쉽게 다른 사용자로 대체하거나 고급 사용자 권한의 사용을 면밀하게 추적하는 것이 가능합니다. 기본 사용자 역할은 에스컬레이션을 지원하지 않습니다.

예를 들어 기반 역할의 권한이 매우 제한적인 사용자가 관리자 역할로 에스컬레이션하여 관리 작업을 수행할 수 있습니다. 사용자가 자신의 비밀번호를 사용하거나 지정된 다른 사용자의 비밀번호를 사용하도록 이 기능을 구성할 수 있습니다. 두 번째 옵션에서는 해당되는 모든 사용자를 대상으로 하나의 확대 비밀번호를 손쉽게 관리할 수 있습니다.

사용자 역할 확대를 구성하려면 다음 워크플로를 참조하십시오.

프로시저

단계 **1** 확대 대상 역할 설정, 130 페이지. 한 번에 하나의 사용자 역할만 확대 대상 역할이 될 수 있습니다.

단계 **2** 확대를 위한 맞춤형 사용자 역할 구성, 131 페이지.

단계 **3** (로그인된 사용자의 경우) 사용자 역할 확대, 132 페이지.

확대 대상 역할 설정

어떤 사전 정의 또는 맞춤형 사용자 역할도 시스템 차원 확대 대상 역할이 되도록 지정할 수 있습니다. 이는 맞춤형 역할이 능력이 된다면 에스컬레이션할 수 있는 역할입니다. 한 번에 하나의 사용자 역할만 확대 대상 역할이 될 수 있습니다. 각 확대는 로그인 세션 동안 지속되며 감사 로그에 기록됩니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** **Configure Permission Escalation(**권한 확대 구성**)**을 클릭합니다.

단계 **4** **Excalation Target(**확대 대상**)** 드롭다운 목록에서 사용자 역할을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

확대 대상 역할의 변경은 즉시 적용됩니다. 확대된 세션의 사용자는 이제 새 확대 대상의 권한을 갖습니다.

확대를 위한 맞춤형 사용자 역할 구성

확대 활성화의 대상이 되는 사용자는 확대가 활성화된 맞춤형 사용자 역할에 속해야 합니다. 이 절차에서는 맞춤형 사용자 역할에 대한 에스컬레이션을 활성화하는 방법을 설명합니다.

맞춤형 역할에 대해 에스컬레이션 비밀번호를 구성할 때 조직의 요구 사항을 고려하십시오. 여러 에스컬레이션 사용자를 손쉽게 관리하길 원할 경우 또 다른 사용자를 선택하여 해당 비밀번호를 확대 비밀번호로 사용하는 방법이 있습니다. 해당 사용자의 비밀번호를 변경하거나 사용자를 비활성화할 경우 해당 비밀번호를 필요로 하는 모든 에스컬레이션 사용자가 영향을 받습니다. 이 작업은 더 효율적으로 사용자 역할 확대를 관리할 수 있습니다. 특히 중앙에서 관리할 수 있는 외부 인증 사용자를 선택할 경우 더욱 그렇습니다.

시작하기 전에

확대 대상 역할 설정, 130 페이지에 따라 대상 사용자 역할을 설정합니다.

프로시저

단계 **1** 맞춤형 사용자 역할 생성, 127 페이지에 설명된 대로 맞춤형 사용자 역할의 구성을 시작합니다.

단계 **2** **System Permissions(**시스템 권한**)**에서 **Set this role to escalate to: Maintenance User(**이 역할을 다음으로 에스컬레이션하도록 설정**:** 유지 보수 사용자**)** 확인란을 선택합니다.

현재 에스컬레이션 대상 목표가 확인란 옆에 나열됩니다.

단계 **3** 이 역할에서 에스컬레이션에 사용할 비밀번호를 선택합니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 이 역할을 갖는 사용자가 확대 시 각자의 비밀번호를 사용하게 하려면 **Authenticate with the assigned user's password(**할당된 사용자의 비밀번호로 인증**)**를 선택합니다.
- 이 역할의 사용자가 다른 사용자의 비밀번호를 사용하게 하려면 **Authenticate with the specified user's password(**지정한 사용자의 비밀번호로 인증**)**를 선택하고 해당 사용자 이름을 입력합니다.

  참고 다른 사용자의 비밀번호로 인증할 경우 어떠한 사용자 이름이라도, 심지어 비활성화되었거나 존재하지 않는 사용자의 이름도 입력할 수 있습니다. 비밀번호가 에스컬레이션에 사용되는 사용자를 비활성화할 경우 해당 비밀번호를 필요로 하는 역할의 사용자는 에스컬레이션이 불가능해집니다. 에스컬레이션을 신속하게 제거해야 하는 경우 이 기능을 사용할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

사용자 역할 확대

사용자가 확대 권한이 있는 맞춤형 사용자 역할이 있는 경우, 해당 사용자는 언제라도 대상 역할의 권한으로 확대할 수 있습니다. 확대는 사용자 환경 설정에 영향을 주지 않습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Escalate Permissions(**권한 확대**)**를 선택합니다.

이 옵션이 표시되지 않는다면 관리자가 사용자 역할에 대해 확대를 활성화 하지 않은 것입니다

단계 **2** 인증 비밀번호를 입력합니다.

단계 **3** **Escalate(**확대**)**를 클릭합니다. 이제 현재 역할 외에도 확대 대상 역할의 모든 권한을 갖게 되었습니다.

확대 로그인 세션의 남은 시간 동안 지속됩니다. 다시 기본 역할의 권한만 가지려면 로그아웃했다가 새 세션을 시작해야 합니다.

LDAP 인증 연결 문제 해결

LDAP 인증 개체를 생성하는 경우, 선택한 서버와의 연결에 실패하거나 원하는 사용자 목록을 가져오지 않는다면 개체의 설정을 조정할 수 있습니다.

연결 테스트 결과 연결에 실패할 경우, 다음 방법으로 구성 문제를 해결해보십시오.

- 웹 인터페이스 화면 상단 및 테스트 출력에 표시된 메시지를 참조하여 개체의 어느 영역에서 문제를 일으키는지 확인합니다.
- 개체에 사용한 사용자 이름과 비밀번호가 올바른지 확인합니다.
  - 사용자가 기본 DN에 나타난 디렉토리로 이동할 권한이 있는지 확인하기 위해 서드파티 LDAP 브라우저를 사용하여 LDAP 서버에 연결해봅니다.
  - 사용자 이름이 LDAP 서버의 디렉토리 정보 트리에서 고유한지 확인합니다.
  - 테스트 출력에 LDAP 바인드 오류 49가 있을 경우 해당 사용자에 대한 사용자 바인딩이 실패한 것입니다. 서드파티 애플리케이션을 통해 서버 인증을 시도하여 해당 연결에서도 바인딩이 실패하는지 확인합니다.
- 서버를 정확하게 식별했는지 확인합니다.
  - 서버 IP 주소 또는 호스트 이름이 정확한지 확인합니다.
  - 로컬 어플라이언스에서 연결할 인증 서버까지 TCP/IP 액세스 권한이 있는지 확인합니다.
  - 서버에 대한 액세스가 방화벽에 의해 차단되지 않고 개체에 구성한 포트가 열려 있는지 확인합니다.

  - TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 서버에 사용된 호스트 이름과 일치해야 합니다.
  - CLI 액세스를 인증하는 경우, 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
  - 서버 유형 기본값을 사용한 경우 정확한 서버 유형인지 확인하고 **Set Defaults(**기본값 설정**)**를 다시 클릭하여 기본값을 재설정합니다.

- 기본 DN을 입력한 경우 **Fetch DNs(DN** 가져오기**)**를 클릭하여 서버에서 사용 가능한 모든 기본 DN을 가져오고 그 목록에서 이름을 선택합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각각이 올바르고 제대로 입력되었는지 확인합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각 설정을 제거하고 그 설정 없이 개체를 테스트해봅니다.
- 기본 필터 또는 셸 액세스 필터를 사용하는 경우, 필터가 괄호로 묶여 있고 올바른 비교 연산자를 사용하고 있는지 확인합니다. 묶인 괄호를 포함하여 최대 450자까지 입력할 수 있습니다.
- 더 제한적인 기본 필터를 테스트하려면 사용자의 기본 DN으로 설정하여 그 사용자만 검색해봅니다.
- 암호화 연결을 사용하는 경우:
  - 인증서에 있는 LDAP 서버의 이름이 연결에 사용하는 호스트 이름과 매칭되는지 확인합니다.
  - 암호화 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 이름과 비밀번호가 제대로 입력되었는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 크리덴셜을 제거하고 개체를 테스트합니다.
- LDAP 서버에 연결하고 다음 구문을 사용하여 사용 중인 쿼리를 테스트합니다.

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

  에를 들어 `myrtle.example.com`의 보안 도메인에 연결하기 위해 `domainadmin@myrtle.example.com` 사용자와 (`cn=*`) 기본 필터를 사용하는 경우, 다음 구문으로 연결을 테스트할 수 있습니다.

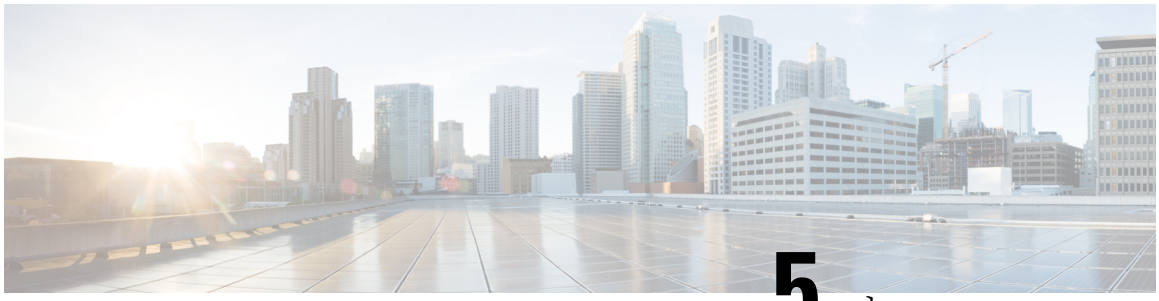
```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

연결 테스트에 성공했지만 플랫폼 설정 정책을 적용한 후 인증이 되지 않을 경우, 디바이스에 적용되는 플랫폼 설정 정책에서 인증 및 사용할 개체가 모두 활성화되었는지 확인합니다.

성공적으로 연결했지만 연결에서 검색되는 사용자 목록을 조정하려는 경우, 기본 필터 또는 셸 액세스 필터를 추가하거나 변경할 수 있습니다. 또는 더 제한적이거나 덜 제한적인 기본 DN을 사용할 수 있습니다.

FMC 사용자 계정 히스토리

기능	버전	세부 사항
SAML 2.0 호환 SSO 제공자를 사용하는 단일 로그인 지원을 추가했습니다.	6.7	타사 SAML 2.0 준수 ID 제공자 (IdP)에 구성된 외부 사용자에 대해 단일 로그인을 지원하는 기능을 추가했습니다. 여기에는 IdP에서 FMC 사용자 역할로 사용자 또는 그룹 역할을 매핑하는 기능이 포함됩니다. 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다. 신규/수정된 화면: 시스템 > 사용자 > **SSO(Single Sign-On)**
사용자 계정의 이름에 대한 새 필드를 추가했습니다.	6.6	내부 사용자 계정을 담당하는 사용자 또는 부서를 식별할 수 있는 필드를 추가했습니다. 신규/수정된 화면: **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)> Real Name(**실제 이름**)** 필드
Cisco Security Manager SSO(Single Sign-On)가 더 이상 지원되지 않음	6.5	FMC와 Cisco Security Manager 간의 SSO(Single Sign-On)는 Firepower 6.5부터 더 이상 지원되지 않습니다. 신규/수정된 화면: **System(**시스템**)** > **Users(**사용자**)CSM SSO(CSM Single Sign-on)**을 선택합니다.
향상된 비밀번호 보안	6.5	이제 새로운 강력한 비밀번호 요구 사항이 장의 단일 위치에 표시되며, 다른 장에서 상호참조됩니다. 수정된 화면 없음 지원되는 플랫폼: FMC



5 장

디바이스 사용자 계정

매니지드 디바이스는 CLI 액세스에 대한 기본 관리자 계정을 포함합니다. 이 장에서는 맞춤형 사용자 계정을 생성하는 방법을 설명합니다. 매니지드 디바이스에 사용자 계정으로 로그인하는 방법에 대한 자세한 내용은 Firepower System에 로그인, 25 페이지에서 확인할 수 있습니다.

- 디바이스 사용자 계정 정보, 135 페이지
- 디바이스의 사용자 계정에 대한 요구 사항 및 사전 요건, 136 페이지
- 디바이스 사용자 계정을 위한 지침 및 제한 사항, 137 페이지
- CLI에서 내부 사용자 추가, 137 페이지
- FTD에 대한 외부 인증 구성, 139 페이지
- LDAP 인증 연결 문제 해결, 152 페이지
- 디바이스용 사용자 계정 기록, 154 페이지

디바이스 사용자 계정 정보

매니지드 디바이스에서 맞춤형 사용자 계정을 내부 사용자로 추가할 수 있으며, FTD의 경우 LDAP 또는 RADIUS 서버에 외부 사용자로 추가할 수 있습니다. 매니지드 디바이스 각각은 별도 사용자 계정을 유지 관리합니다. 예를 들어 사용자를 FMC에 추가하는 경우, 해당 사용자만 FMC에 액세스할 수 있습니다. 해당 사용자 이름을 사용해 매니지드 디바이스에 직접 로그인할 수 없습니다. 매니지드 디바이스에서 사용자를 별도로 추가해야 합니다.

내부 및 외부 사용자

매니지드 디바이스는 두 가지 유형의 사용자를 지원합니다.

- 내부 사용자—디바이스는 사용자 인증을 위해 로컬 데이터베이스를 검사합니다. 내부 사용자에 대한 자세한 내용은 CLI에서 내부 사용자 추가, 137 페이지을 참조하십시오. FTD, NGIPSv 및 ASA FirePOWER는 내부 사용자를 지원합니다.
- 외부 사용자(FTD만 해당) - 사용자가 로컬 데이터베이스에 없는 경우, 시스템이 외부 LDAP 또는 RADIUS 인증 서버에 쿼리합니다. 외부 사용자에 대 한 자세한 내용은 FTD에 대한 외부 인증 구성, 139 페이지을 참조하십시오. FTD만 외부 사용자를 지원합니다.

CLI 액세스

Firepower 디바이스는 Linux에서 실행되는 Firepower CLI를 포함합니다. CLI를 사용하여 디바이스에서 내부 사용자를 생성할 수 있습니다. FMC를 통해 FTD 디바이스에서 외부 사용자를 설정할 수 있습니다. 관리 UI에 대한 자세한 내용은 Firepower System 유저 인터페이스, 27 페이지을 참조하십시오.

⚠

주의 CLI 설정 레벨 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스하고 Linux 셸에서 `sudoers` 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- TAC 감독하에 있거나 Firepower 사용자 설명서에서 명시적으로 지시한 경우에만 Linux 셸을 사용하십시오.
- CLI 액세스 권한이 있는 사용자 목록을 적절하게 제한해야 합니다.
- CLI 액세스 권한을 부여하는 경우, 구성 레벨 액세스로 사용자 목록을 제한합니다.
- Linux 셸에서 바로 사용자를 추가하지 마십시오. 이 장에서 설명하는 절차만 사용해야 합니다.
- Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, CLI 전문가 모드를 이용하여 Firepower 디바이스에 액세스해서는 안 됩니다.

CLI 사용자 역할

매지니드 디바이스의 경우, CLI에서의 명령에 대한 사용자 액세스는 할당하는 역할에 따라 달라집니다.

None

ㅈ사용자는 명령줄에서 디바이스에 로그인할 수 없습니다.

Config(컨피그레이션)

사용자는 구성 명령을 비롯하여 모든 명령에 액세스할 수 있습니다. 사용자에게 이 액세스 수준을 할당할 때는 각별히 주의하십시오.

기본

사용자는 비구성 명령에만 액세스할 수 있습니다. 내부 사용자 및 FTD 외부 RADIUS 사용자만 기본 역할을 지원합니다.

디바이스의 사용자 계정에 대한 요구 사항 및 사전 요건

모델 지원

- FTD내부 및 외부 사용자

- ASA FirePOWER내부 사용자
- NGIPSv내부 사용자

지원되는 도메인

모든

사용자 역할

외부 사용자 구성- 관리자 FMC 사용자

내부 사용자 구성-CLI 사용자 구성

디바이스 사용자 계정을 위한 지침 및 제한 사항

기본값

모든 디바이스는 로컬 사용자 어카운트로 관리자 사용자를 포함합니다. 관리자 사용자는 삭제할 수 없습니다. 기본 초기 비밀번호는 **Admin123**입니다. 시스템은 초기화 프로세스 중에 비밀번호를 변경하게 합니다. 시스템 초기화에 관한 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오.

CLI에서 내부 사용자 추가

CLI를 사용하여 FTD, ASA FirePOWER 및 NGIPSv 디바이스에서 내부 사용자를 생성합니다.

프로시저

단계 **1** Config(구성) 권한이 있는 계정을 사용하여 디바이스 CLI에 로그인합니다.

관리자 사용자 어카운트가 필수 권한을 갖고 있지만, Config(구성) 권한이 있는 모든 어카운트에도 작동합니다. SSH 세션 또는 콘솔 포트를 사용할 수 있습니다.

특정 FTD 모델의 경우, 콘솔 포트는 사용자를 FXOS CLI에 연결합니다. FTD CLI로 이동하려면 **connect ftd** 명령을 사용하십시오.

단계 **2** 사용자 계정을 생성합니다.

configure user add *username* {**basic** | **config**}

- *username(*사용자 이름*)* - 사용자 이름을 설정합니다. 사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.
  - 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
  - 모두 소문자

- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

- **basic**- 사용자에게 기본 액세스 권한을 제공합니다. 이 역할은 사용자가 구성 명령을 입력하는 것을 허용하지 않습니다.
- **config**- 사용자에게 컨피그레이션 액세스 권한을 제공합니다. 이 역할은 사용자에게 모든 명령에 대한 전체 관리자 권한을 제공합니다.

예제:

다음 예에서는 Config(구성) 액세스 권한이 있는 johncrichton이라는 이름의 사용자 어카운트를 추가합니다. 입력하고 있으므로 비밀번호가 표시되지 않습니다.

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

참고 **configure password** 명령을 사용하여 비밀번호를 변경할 수 있다고 사용자에게 알려줍니다.

단계 **3** (선택 사항) 보안 요건을 충족하도록 어카운트의 특성을 조정합니다.

다음 명령을 사용하여 기본 어카운트 동작을 변경할 수 있습니다.

- **configure user aging** *username max_days warn_days*

  사용자 비밀번호의 만료일을 설정합니다. 비밀번호가 유효한 최대 일수를 지정한 후 며칠 전부터 사용자에게 다가오는 만료일에 대해 경고할지 일수를 지정합니다. 두 값 모두 1~9999 범위이지만, 경고 일수는 최대 일수보다 작아야 합니다. 어카운트를 생성할 때 비밀번호 만료일이 없습니다.

- **configure user forcereset** *username*

  사용자가 다음 로그인 시 강제로 비밀번호를 변경하게 합니다.

- **configure user maxfailedlogins** *username number*

  어카운트를 잠그기 전에 허용되는 연속 실패 로그인의 최대 수를 1~9999 범위로 설정합니다. 계정의 잠금을 해제하려면 **configure user unlock** 명령을 사용하십시오. 새 어카운트에 대한 기본값은 로그인 5회 연속 실패입니다.

- **configure user minpasswdlen** *username number*

  최소 비밀번호 길이를 1~127 범위로 설정합니다.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  비밀번호 강도 검사를 활성화하거나 비활성화합니다. 이 경우 비밀번호를 변경할 때 사용자는 특정 비밀번호 기준을 충족해야 합니다. 사용자의 암호가 만료되거나 **configure user forcereset** 명령을 사용하는 경우, 이 요건은 사용자가 다음번 로그인할 때 자동으로 활성화됩니다.

단계 **4** 필요 시 사용자 어카운트를 관리합니다.

사용자가 자신의 어카운트를 잠글 수 있게 하거나, 어카운트를 제거하거나 다른 문제를 해결해야 합니다. 시스템에서 사용자 어카운트를 관리하려면 다음 명령을 사용합니다.

- **configure user access** *username* {**basic** | **config**}

  사용자 어카운트에 대한 권한을 변경합니다.

- **configure user delete** *username*

  지정된 어카운트를 삭제합니다.

- **configure user disable** *username*

  지정된 어카운트를 삭제하지 않고 비활성화합니다. 사용자는 어카운트를 활성화할 때까지 로그인할 수 없습니다.

- **configure user enable** *username*

  지정된 어카운트를 활성화합니다.

- **configure user password** *username*

  지정된 사용자에 대한 비밀번호를 변경합니다. 사용자는 일반적으로 **configure password** 명령을 사용하여 자신의 암호를 변경해야 합니다.

- **configure user unlock** *username*

  연속 실패 로그인 시도의 최대 횟수를 초과하므로 잠겨 있는 사용자 어카운트의 잠금을 해제합니다.

FTD에 대한 외부 인증 구성

FTD 디바이스에 대한 외부 인증을 활성화하려면 하나 이상의 외부 인증 개체를 추가해야 합니다.

FTD 외부 인증 정보

FTD 사용자에 대해 외부 인증을 사용하도록 설정하면 FTD는 외부 인증 개체에 지정된 LDAP 또는 RADIUS 서버를 사용하여 사용자 자격 증명을 확인합니다.

외부 인증 개체는 FMC 및 FTD 디바이스가 사용할 수 있습니다. 다양한 어플라이언스/디바이스 유형 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다. FTD의 경우, 디바이스에 구축하는 플랫폼 설정에서 하나의 외부 인증 개체만 활성화할 수 있습니다.

참고 시간 제한 범위는 FTD와 FMC가 다르므로 개체를 공유할 때는 FTD의 더 적은 시간 제한 범위(LDAP의 경우 1~30초, RADIUS의 경우 1~300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD 외부 인증 설정이 작동하지 않습니다.

참고 FTD 가상 디바이스에서 외부 인증은 지원되지 않습니다.

외부 인증 개체에서 필드 하위 집합만 FTD SSH 액세스에 사용됩니다. 다른 필드를 입력하는 경우, 해당 필드는 무시됩니다. 이 개체를 다른 디바이스 유형에 사용하는 경우, 해당 필드가 사용됩니다.

LDAP 사용자는 항상 Config(구성) 권한을 갖습니다. RADIUS 사용자는 Config(구성) 또는 Basic(기본) 사용자로 정의할 수 있습니다.

RADIUS 서버(Service-Type(서비스 유형) 속성)에서 사용자를 정의하거나 외부 인증 개체에서 사용자 목록을 미리 정의할 수 있습니다. LDAP의 경우, 필터를 지정하여 LDAP 서버의 CLI 사용자와 매칭할 수 있습니다.

참고 Linux 셸 액세스 권한이 있는 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 다음을 확인하십시오.

- Linux 셸 액세스 권한이 있는 사용자 목록 제한
- Linux 셸 사용자를 생성 금지

LDAP 정보

LDAP(Lightweight Directory Access Protocol)를 사용하면 중앙의 한 위치에 개체(예: 사용자 크리덴셜)를 조직하는 네트워크에서 디렉토리를 설정할 수 있습니다. 그러면 여러 애플리케이션에서 이 크리덴셜 및 크리덴셜 설명에 사용된 정보에 액세스할 수 있습니다. 사용자 크리덴셜을 변경해야 하는 경우, 한 곳에서 변경할 수 있습니다.

Microsoft는 Active Directory 서버가 2020년에 LDAP 바인딩 및 LDAP 서명을 시행할 것이라고 발표했습니다. Microsoft는 이러한 설정을 기본 설정으로 사용할 때 Microsoft Windows에 권한 상승 취약점이 존재하여 MITM(man-in-the-middle) 공격자가 Windows LDAP 서버에 인증 요청을 성공적으로 전달할 수 있기 때문에 이러한 요구 사항을 적용하고 있습니다. 자세한 내용은 Microwoft 지원 사이트에서 2020 LDAP 채널 바인딩 및 Windows용 LDAP 서명 요구 사항을 참조하십시오.

아직 수행하지 않은 경우 TLS/SSL 암호화를 사용하여 Active Directory 서버에서 인증을 시작하는 것이 좋습니다.

RADIUS 정보

RADIUS(Remote Authentication Dial In User Service)는 네트워크 리소스에 대한 사용자 액세스의 인증, 권한 부여, 어카운팅에 사용되는 인증 프로토콜입니다. RFC 2865를 준수하는 모든 RADIUS 서버에 대해 인증 개체를 생성할 수 있습니다.

Firepower 디바이스는 SecurID 토큰 사용을 지원합니다. SecurID를 사용하여 서버에서 인증을 구성하는 경우, 해당 서버에서 인증된 사용자는 SecurID PIN 끝에 SecurID 토큰을 추가하고 이를 로그인 비밀번호로 사용합니다. SecurID를 지원하기 위해 Firepower 디바이스에서 추가로 구성할 사항은 없습니다.

FTD에 대한 LDAP 외부 인증 개체 추가

FTD 관리를 위해서 외부 사용자를 지원할 수 있도록 LDAP 서버를 추가합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

외부 인증 객체 공유

외부 LDAP 개체는 FMC 및 FTD 디바이스가 사용할 수 있습니다. FMC 및 디바이스 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다.

참고 LDAP의 경우 FTD와 FMC의 시간 제한 범위가 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위(1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD에 대한 구축이 실패합니다.

FTD 지원되는 필드

LDAP 개체에서 필드 하위 집합만 FTD SSH 액세스에 사용됩니다. 다른 필드를 입력하는 경우, 해당 필드는 무시됩니다. 이 개체를 FMC에 사용하는 경우, 해당 필드가 사용됩니다. 이 절차는 FTD에 대한 지원되는 필드만 적용합니다. 다른 필드는 FMC에 대한 LDAP 외부 인증 개체 추가, 59 페이지 섹션을 참조하십시오.

사용자 이름

사용자 이름은 Linux에서 유효한 사용자 이름이어야 하며 소문자로 된 영숫자에 마침표(.) 또는 하이픈(-)을 사용해야 합니다. at 기호(@) 및 사선(/) 등 다른 특수 문자는 지원되지 않습니다. 외부 인증에 대한 관리자 사용자를 추가할 수 없습니다. 외부 사용자만 외부 인증 객체의 일부로 FMC에서 추가할 수 있습니다. CLI에서는 추가할 수 없습니다. 내부 사용자는 FMC가 아닌 CLI에서만 추가할 수 있습니다.

내부 사용자에 대해 **configure user add** 명령을 사용하여 동일한 사용자 이름을 구성한 경우, FTD가 우선 내부 사용자에 대해 비밀번호를 확인하고 실패한 경우 LDAP 서버를 확인합니다. 참고로 외부 사용자와 이름이 같은 내부 사용자를 나중에 추가할 수 없습니다. 기존 내부 사용자만 지원됩니다.

권한 레벨

LDAP 사용자는 항상 Config(구성) 권한을 갖습니다.

시작하기 전에

해당 장치에서 도메인 이름 조회를 위해 DNS 서버를 지정해야 합니다. 이 절차에서 IP 주소는 지정하고 LDAP 서버에 대한 호스트 이름은 지정하지 않더라도, LDAP 서버는 인증을 위한 URI를 반환할 수 있으며 여기에는 호스트 이름이 포함됩니다. 호스트 이름을 지정하려면 DNS 조회가 필요합니다. CLI에서 디바이스 관리 인터페이스 수정, 327 페이지를 참조하고 DNS 서버를 추가합니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**을 선택합니다.

단계 **2** **External Authentication(**외부 인증**)** 탭을 클릭합니다.

단계 **3** **Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **4** **Authentication Method(**인증 방법**)**을 **LDAP**로 설정합니다.

단계 **5** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **6** 드롭다운 목록에서 **Server Type(**서버 유형**)**을 선택합니다.

단계 **7** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

단계 **8** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **9** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **10** **LDAP-Specific Parameters(LDAP** 전용 파라미터**)**를 입력합니다.

a) 액세스를 원하는 LDAP 디렉터리에 대해 **Base DNs(**기본 **DN)**를 입력합니다. 예를 들어, 예시 회사의 보안 조직에서 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다. 아니면 **Fetch DN(DN** 가져오기**)**을 클릭하고, 드롭다운 목록에서 적절한 기본 고유 이름을 선택합니다.

b) (선택 사항) **Base Filter(**기본 필터**)**를 입력합니다. 예를 들어 디렉토리 트리의 사용자 개체에 `physicalDeliveryOfficeName` 속성이 있고 a뉴욕 사무실의 사용자는 그 속성 값이 `NewYork`인 경우 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.

c) LDAP 서버를 검색하기에 크리덴셜이 충분한 사용자의 경우, **User Name(**사용자 이름**)**을 입력합니다. 예를 들어 OpenLDAP 서버에 연결하려는 경우, 해당 사용자 개체에 `uid` 속성이 있으며 예시 회사 보안 부서 관리자 개체의 `uid`값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.

d) **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 사용자 비밀번호를 입력합니다.

e) (선택 사항) **Show Advanced Options(**고급 옵션 표시**)**를 클릭하고 다음 고급 옵션을 구성합니다.

- **Encryption(**암호화**)- None (**해당 없음**)**, **TLS**또는 **SSL**을 클릭 합니다.

  포트를 지정한 다음 암호화 방식을 변경할 경우, 그 방법에 대해서는 포트가 기본값으로 재설정됩니다. **None(**해당 없음**)** 또는 **TLS**인 경우, 포트는 기본값인 389로 재설정됩니다. SSL 암호화를 선택할 경우 포트는 636로 재설정됩니다.

- **SSL Certificate Upload Path(SSL** 인증서 업로드 경로**)**—SSL 또는 TLS 암호화인 경우, **Choose File(**파일 선택**)**을 클릭하여 인증서를 선택해야 합니다.

이전에 업로드한 인증서를 대체하려는 경우, 새 인증서를 업로드하고 구성을 디바이스에 다시 적용하여 새 인증서로 복사합니다.

참고 TLS 암호화는 모든 플랫폼에서 인증서가 필요합니다. SSL의 경우, FTD도 인증서가 필요합니다. 다른 플랫폼의 경우, SSL은 인증서가 필요하지 않습니다. 그러나 항상 끼어들기 공격을 방지하기 위해 SSL에 대한 인증서를 업로드하는 것이 좋습니다.

- (사용되지 않음) **User Name Template(**사용자 이름 템플릿**)** - FTD에서 사용되지 않습니다.
- **Timeout(**시간 초과**)**—백업 연결로 전환하기 전 시간(초)을 1과 30 사이로 입력합니다. 기본값은 30입니다.

  참고 시간 제한 범위는 FTD와 FMC에 따라 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위 (1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD LDAP 구성이 작동하지 않습니다.

단계 **11** (선택 사항) 사용자 고유 유형 이외의 쉘(shell) 액세스 속성을 사용하려는 경우 **CLI Access Attribute(CLI** 액세스 속성**)**를 입력합니다. 예를 들어 Microsoft Active Directory Server에서 `sAMAccountName` 쉘 액세스 속성을 사용하여 쉘 액세스 사용자를 가져오려면 `sAMAccountName`을 **CLI Access Attribute(CLI** 액세스 속성**)** 필드에 입력합니다.

단계 **12** **CLI Access Filter(CLI** 액세스 필터**)**를 설정합니다.

다음 방법 중 하나를 선택합니다.

- 인증 설정을 구성할 때 지정한 것과 동일한 필터를 사용하려면 **Same as Base Filter(**기본 필터와 동일**)**를 선택합니다.
- 속성 값에 따라 관리자 사용자 엔트리를 검색하려면 속성 이름, 비교 연산자, 필터로 사용할 속성 값을 괄호로 묶어 입력합니다. 예를 들어 모든 네트워크 관리자에게 `manager` 속성이 있고 그 값이 `shell`이라면 `(manager=shell)`이라는 기본 필터를 설정할 수 있습니다.

사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

참고 내부 사용자에 대해 동일한 사용자 이름을 구성한 경우, FTD가 우선 내부 사용자에 대해 비밀번호를 확인하고 실패한 경우 LDAP 서버를 확인합니다. 참고로 외부 사용자와 이름이 같은 내부 사용자를 나중에 추가할 수 없습니다. 기존 내부 사용자만 지원됩니다.

단계 **13** **Save(**저장**)**를 클릭합니다.

단계 **14** 이 서버의 사용을 활성화합니다. SSH에 대한 외부 인증 설정의 내용을 참조하십시오.

단계 **15** LDAP 서버에서 사용자를 나중에 추가 또는 삭제한다면, 사용자 목록을 새로 고침하고 매니지드 디바이스에 대한 Platform Settings(플랫폼 설정)를 재구축해야 합니다.

a) 각 LDAP 서버 옆에 새로 로침( )를 클릭합니다.

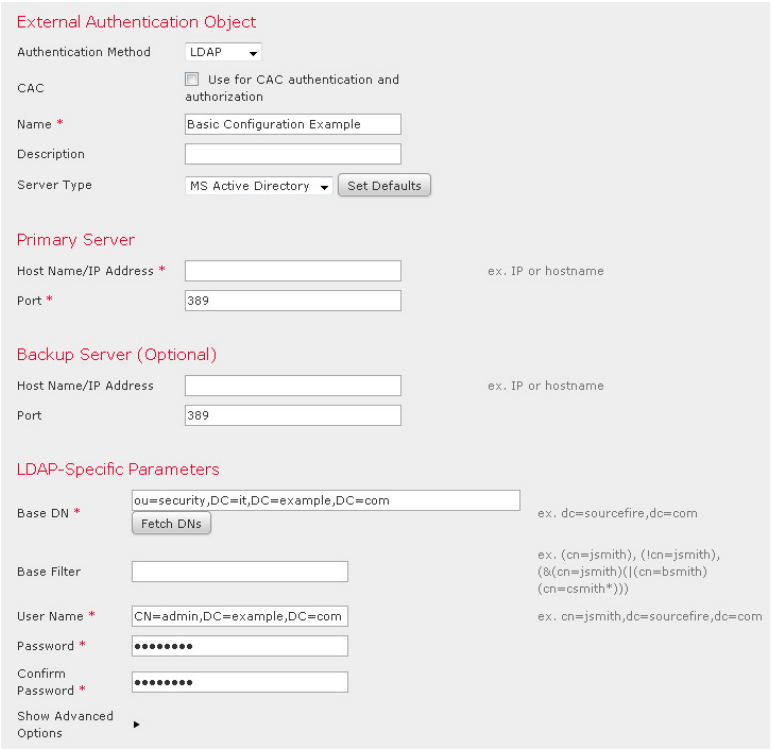
사용자 목록을 변경하는 경우, 디바이스에 대한 구성 변경을 구축하라는 메시지가 표시됩니다.

b) 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

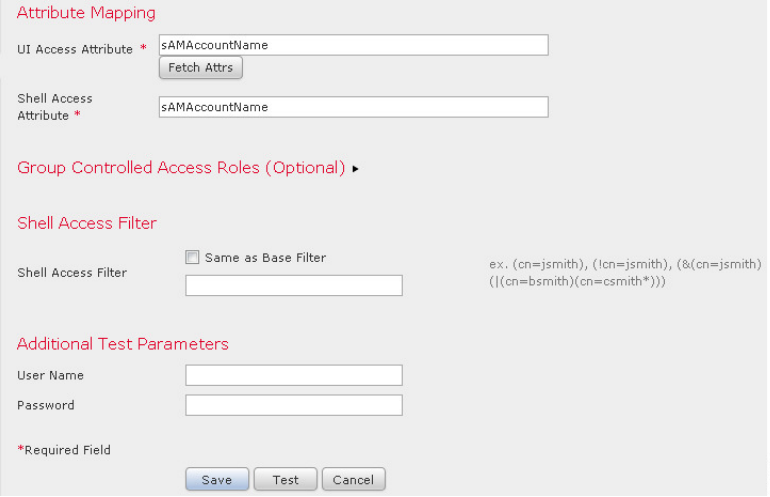
예

기본 예시

다음 그림은 Microsoft Active Directory Server를 위한 LDAP 로그인 인증 개체의 기본 구성입니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 389을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다.

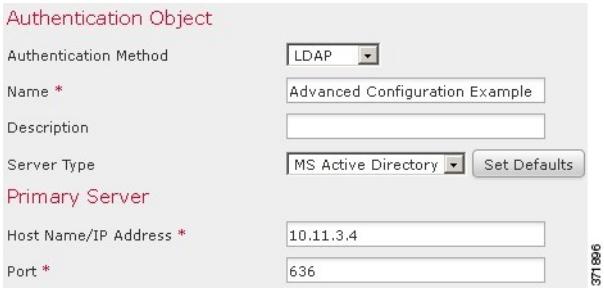


또한 Shell Access Attribute(셸 액세스 속성)가 `sAMAccountName`이면 사용자가 FTD에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

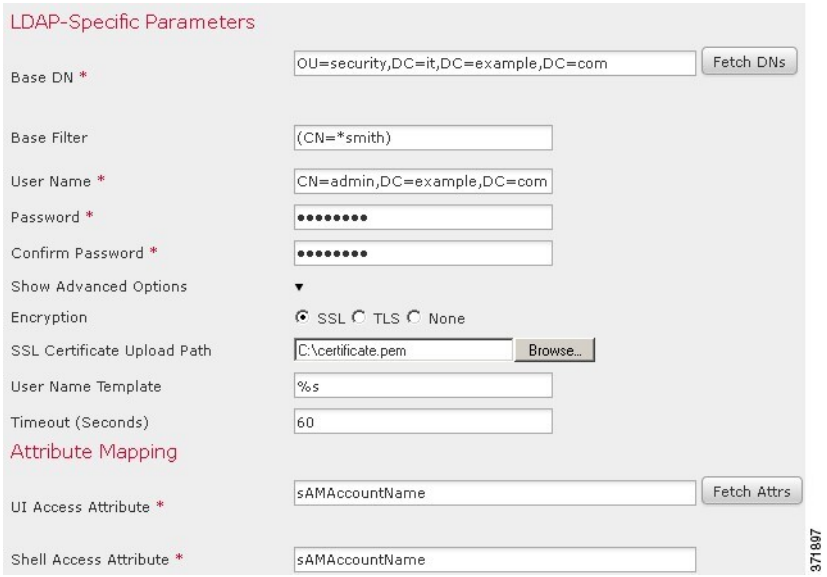
이 서버에는 기본 필터가 적용되지 않으므로 FTD에서는 기본 DN이 나타내는 디렉토리의 모든 개체에 대해 속성을 검사합니다. 기본 기간(또는 LDAP 서버에 설정된 시간 초과 기간)이 경과하면 서버와의 연결이 시간 초과됩니다.

고급 예시

이 예에서는 Microsoft Active Directory Server에 대한 LDAP 로그인 인증 개체의 고급 구성을 보여줍니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 636을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다. 그러나 이 서버는 기본 필터 `(cn=*smith)`가 있습니다. 이 필터는 CN이 `smith`로 끝나는 사용자만 서버에서 가져오도록 제한합니다.



서버와의 연결은 SSL로 암호화되고 `certificate.pem`이라는 인증서가 연결에 사용됩니다. 또한 **Timeout(**시간 초과**)** 설정 때문에 60초가 지나면 서버와의 연결이 시간 초과됩니다.

이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다.

또한 Shell Access Attribute(셸 액세스 속성)가 `sAMAccountName`이면 사용자가 FTD에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

다음 예에서 셸 액세스 필터는 기본 필터와 동일하게 설정됩니다.

FTD에 대한 RADIUS 외부 인증 개체 추가

FTD에 대한 RADIUS 서버를 추가하고 외부 사용자를 지원합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

외부 인증 객체 공유

FMC 및 디바이스 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다. FTD에서는 RADIUS 서버에서 사용자를 정의하는 것을 지원하지만, FMC에서는 외부 인증 객체에 사용자 목록

을 미리 정의해야 합니다. FTD에 대해 사전 정의된 목록 방법을 사용하도록 선택할 수 있지만, RADIUS 서버에서 사용자를 정의하려면 FTD 및 FMC에 대해 별도의 개체를 만들어야 합니다.

참고 시간 제한 범위는 FTD와 FMC에서 서로 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위(1 ~ 300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD RADIUS 구성이 작동하지 않습니다.

FTD 지원되는 필드

RADIUS 개체에서 필드 하위 집합만 FTD SSH 액세스에 사용됩니다. 다른 필드를 입력하는 경우, 해당 필드는 무시됩니다. 이 개체를 FMC에 사용하는 경우 해당 필드가 사용됩니다. 이 절차는 FTD에 대한 지원되는 필드만 적용합니다. 다른 필드는 FMC에 대한 RADIUS 외부 인증 개체 추가, 66 페이지 섹션을 참조하십시오.

사용자 이름

외부 인증에 대한 관리자 사용자를 추가할 수 없습니다. 외부 사용자만 외부 인증 객체의 일부로 FMC에서 추가할 수 있습니다. CLI에서는 추가할 수 없습니다. 내부 사용자는 FMC가 아닌 CLI에서만 추가할 수 있습니다.

내부 사용자에 대해 **configure user add** 명령을 사용하여 동일한 사용자 이름을 구성한 경우, FTD가 우선 내부 사용자에 대해 비밀번호를 확인하고 실패한 경우 RADIUS 서버를 확인합니다. 참고로 외부 사용자와 이름이 같은 내부 사용자를 나중에 추가할 수 없습니다. 기존 내부 사용자만 지원됩니다. RADIUS 서버에 정의된 사용자의 경우 권한 수준을 모든 내부 사용자와 동일하게 설정해야 합니다. 그렇지 않으면 외부 사용자 비밀번호를 사용하여 로그인할 수 없습니다.

프로시저

단계 **1** Service-Type 속성을 사용하여 RADIUS 서버에서 사용자를 정의합니다.

다음은 Service-Type 속성에 대해 지원되는 값입니다.

- Administrator(관리자) (6) - CLI에 대한 Config 액세스 권한을 제공합니다. 이러한 사용자는 CLI에서 모든 명령을 사용할 수 있습니다.
- NAS Prompt(NAS 프롬프트) (7) 또는 6 이외의 모든 레벨 - CLI에 대한 기본 액세스 권한을 제공합니다. 이러한 사용자는 모니터링 및 문제 해결을 위해 **show** 명령 같은 읽기 전용 명령을 사용할 수 있습니다.

이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

또는 외부 인증 객체에서 사용자를 미리 정의할 수 있습니다(단계 12, 148 페이지 단계 참조). FTD 및 에FMC 동일한 RADIUS 서버를 사용하는 한편 Service-Type(서비스-유형) 속성 방법을 FTD에 사용한다면, 동일한 RADIUS 서버를 식별하는 두 개의 외부 인증 개체를 생성합니다. 한 개체는 사전 정의된 **CLI Access Filter(CLI** 액세스 필터**)** 사용자(FMC에 사용)를 포함하며, 나머지 한 개체는 **CLI Access Filter(CLI** 액세스 필터**)**를 공란으로 둡니다(FTD에 사용).

단계 **2** FMC에서 **System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 **3** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **4** **Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **5** **Authentication Method(**인증 방법**)**을 **RADIUS**로 설정합니다.

단계 **6** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **7** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

참고 TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

단계 **8** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **9** **RADIUS Secret Key(RADIUS** 비밀 키**)**를 입력합니다.

단계 **10** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **11** (선택 사항) **RADIUS-Specific Parameters(RADUIS** 특정 파라미터**)**를 입력합니다.

a) **Timeout(**시간 초과**)**을 초 단위로(1부터 300까지) 입력하고 기본 서버를 다시 시도합니다. 기본값은 30입니다.

참고 시간 제한 범위는 FTD와 FMC에서 서로 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위(1 ~ 300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD RADIUS 컨피그레이션이 작동하지 않습니다.

b) **Retries(**재시도**)**를 입력하고 백업 서버로 이동합니다. 기본값은 3입니다.

단계 **12** (선택 사항) RADIUS 정의 사용자(단계 1, 147 페이지 단계 참조)를 사용하는 대신 **CLI Access Filter(CLI** 액세스 필터**)** 영역 **Administrator CLI Access User List(**관리자 **CLI** 액세스 사용자 목록**)** 필드에 CLI 액세스 권한이 있어야 하는 사용자 이름을 쉼표로 구분하여 입력합니다. 예를 들어, **`jchrichton, aerynsun, rygel`**을 입력합니다.

FTD에 **CLI Access Filter(CLI** 액세스 필터**)** 방법을 사용하여 FTD 및 다른 플랫폼 유형과 동일한 외부 인증 개체를 사용할 수 있습니다.

참고 RADIUS에서 정의한 사용자를 사용하려는 경우, **CLI Access Filter(CLI** 액세스 필터**)** 를 공란으로 두어야 합니다.

이러한 사용자 이름은 RADIUS 서버의 사용자 이름과 일치해야 합니다. 이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자

- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

단계 **13** (선택 사항) **Test(**테스트**)**를 클릭해 RADIUS 서버와 FMC 연결을 테스트합니다.

이 기능은 RADIUS 서버와 의 연결만 테스트합니다. 매니지드 디바이스와 RADIUS 서버의 연결을 테스트하는 기능은 없습니다.FMC

단계 **14** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수 있습니다. **User Name(**사용자 이름**)** 및 **Passowrd(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제**:**

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

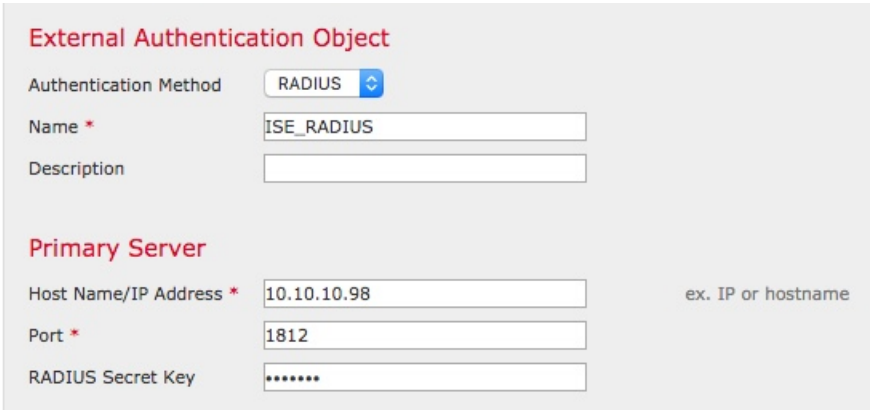
단계 **15** **Save(**저장**)**를 클릭합니다.

단계 **16** 이 서버의 사용을 활성화합니다. SSH에 대한 외부 인증 설정의 내용을 참조하십시오.

예

단순한 사용자 역할 할당

다음 그림은 포트 1812에서 IP 주소 10.10.10.98을 사용하여 Cisco ISE(Identity Services Engine)를 실행하는 서버를 위한 RADIUS 로그인 인증 개체의 예를 보여 줍니다. 정의된 백업 서버가 없습니다.



다음 예는 RADIUS 관련 매개변수를 보여 줍니다. 여기에는 시간 초과(30초) 및 Firepower System이 백업 서버에 연결을 시도하기 전 실패한 재시도 횟수(있는 경우)가 포함됩니다.

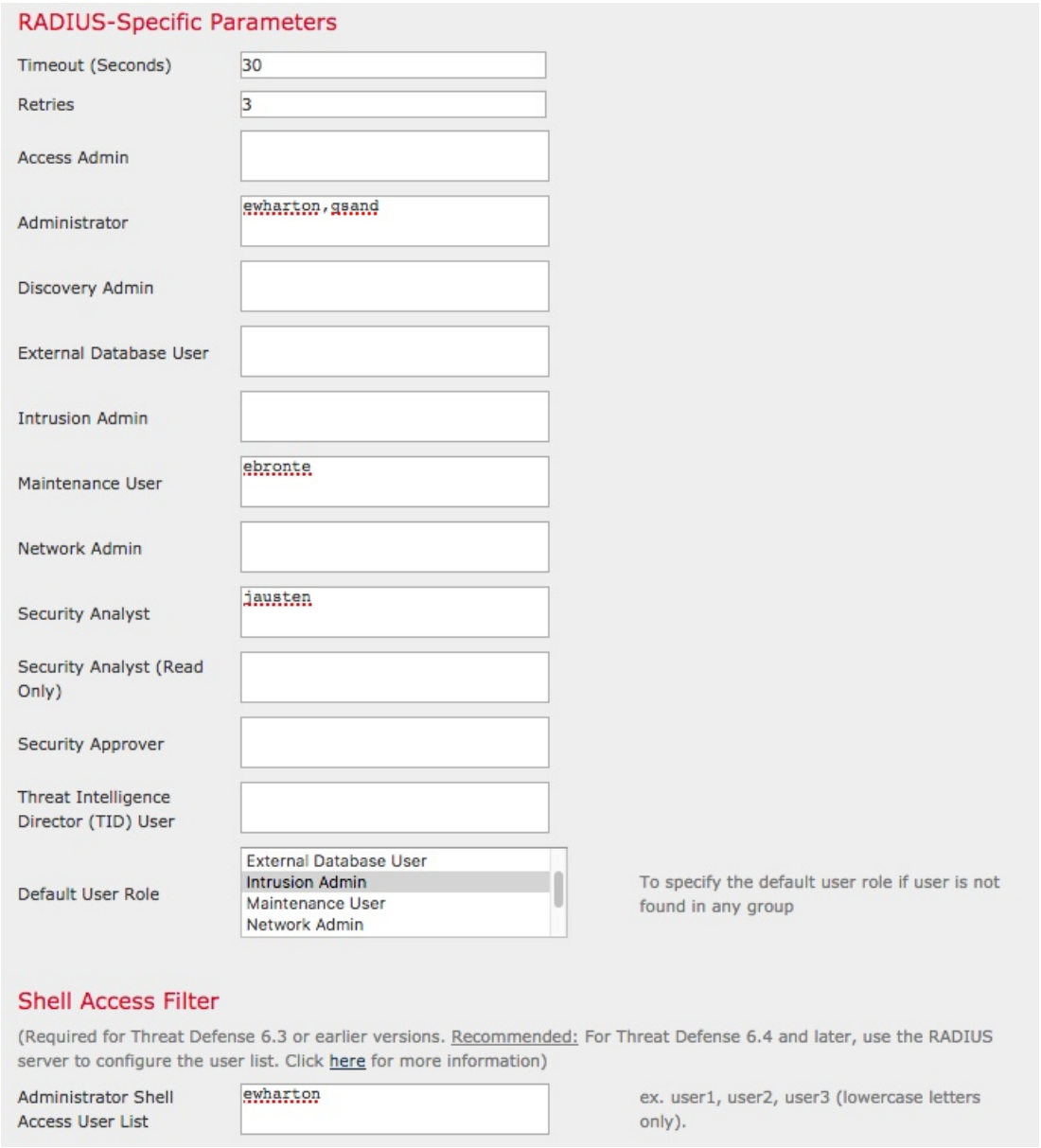
이 예에서는 RADIUS 사용자 역할 구성의 주요 측면을 보여줍니다.

사용자 `ewharton` 및 `gsand`에게 웹 인터페이스 Administrator(관리자) 액세스 권한이 주어집니다.

사용자 `cbronte`에게 웹 인터페이스 Maintenance User(유지 보수 사용자) 액세스 권한이 주어집니다.

사용자 `jausten`에게 웹 인터페이스 Security Analyst(보안 분석가) 액세스 권한이 주어집니다.

사용자 `ewharton`은 CLI 계정을 사용하여 디바이스에 로그인할 수 있습니다.



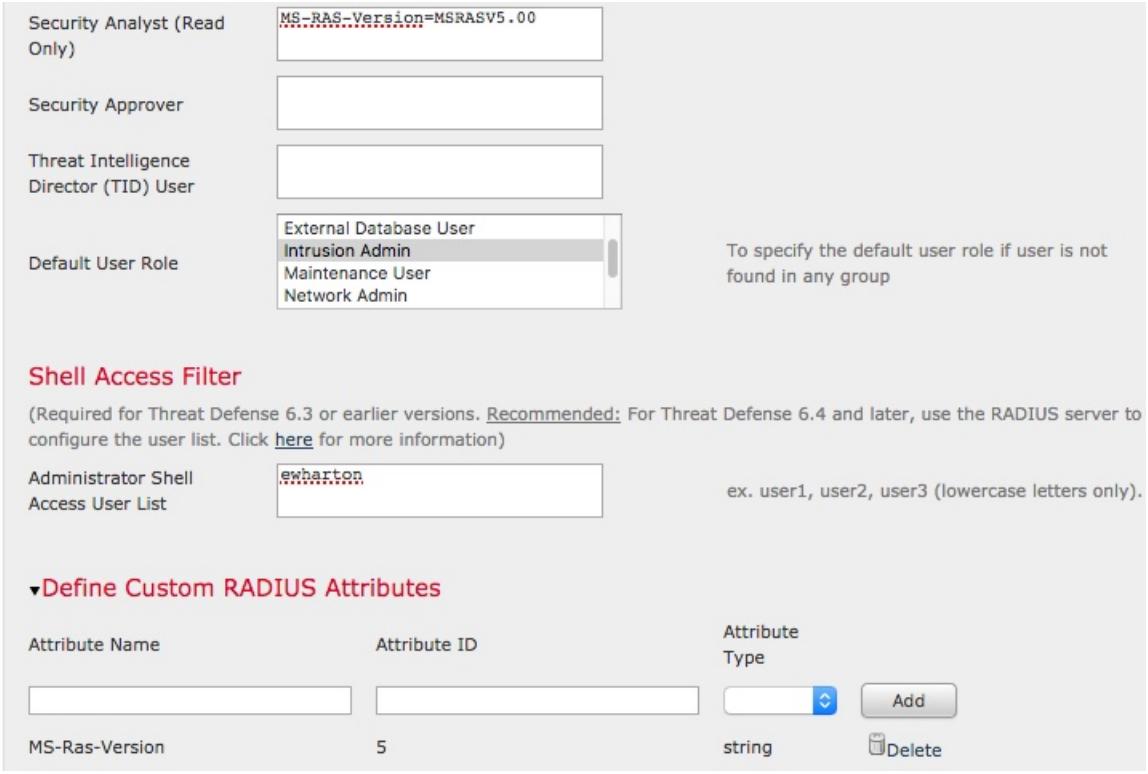
다음 그림은 이 예시에서의 역할 구성을 나타냅니다.

속성-값 쌍을 매칭하는 사용자의 역할

속성-값 쌍을 사용하여 특정 사용자 역할을 갖는 사용자를 식별할 수 있습니다. 사용하는 속성이 맞춤형 속성일 경우 해당 맞춤형 속성을 정의해야 합니다.

다음 그림은 이전의 예와 동일한 ISE 서버를 위한 샘플 RADIUS 로그인 인증 개체에 포함된 역할 설정 및 맞춤형 속성 정의를 보여 줍니다.

그러나 여기서는 Microsoft 원격 액세스 서버가 사용 중이므로 `MS-RAS-Version` 맞춤형 속성 한 명 이상의 사용자에게 반환됩니다. 참고로 `MS-RAS-Version` 맞춤형 속성은 문자열입니다. 이 예에서는 Microsoft v. 5.00 원격 액세스 서버를 통해 RADIUS로 로그인하는 모든 사용자가 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 역할을 받아야 하므로 속성-값 쌍 `MS-RAS-Version= MSRASV5.00`을 **Security Analyst(Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력합니다.



FTD 디바이스 사용자에 대한 외부 인증 활성화

Firepower Threat Defense Platform Settings(Firepower Threat Defense 플랫폼 설정)에서 External Authentication(외부 인증)을 활성화한 후 해당 설정을 매니지드 디바이스에 구축합니다. 자세한 내용은 SSH에 대한 외부 인증 설정를 참조하십시오.

LDAP 인증 연결 문제 해결

LDAP 인증 개체를 생성하는 경우, 선택한 서버와의 연결에 실패하거나 원하는 사용자 목록을 가져오지 않는다면 개체의 설정을 조정할 수 있습니다.

연결 테스트 결과 연결에 실패할 경우, 다음 방법으로 구성 문제를 해결해보십시오.

- 웹 인터페이스 화면 상단 및 테스트 출력에 표시된 메시지를 참조하여 개체의 어느 영역에서 문제를 일으키는지 확인합니다.
- 개체에 사용한 사용자 이름과 비밀번호가 올바른지 확인합니다.
  - 사용자가 기본 DN에 나타난 디렉토리로 이동할 권한이 있는지 확인하기 위해 서드파티 LDAP 브라우저를 사용하여 LDAP 서버에 연결해봅니다.
  - 사용자 이름이 LDAP 서버의 디렉토리 정보 트리에서 고유한지 확인합니다.
  - 테스트 출력에 LDAP 바인드 오류 49가 있을 경우 해당 사용자에 대한 사용자 바인딩이 실패한 것입니다. 서드파티 애플리케이션을 통해 서버 인증을 시도하여 해당 연결에서도 바인딩이 실패하는지 확인합니다.
- 서버를 정확하게 식별했는지 확인합니다.
  - 서버 IP 주소 또는 호스트 이름이 정확한지 확인합니다.
  - 로컬 어플라이언스에서 연결할 인증 서버까지 TCP/IP 액세스 권한이 있는지 확인합니다.
  - 서버에 대한 액세스가 방화벽에 의해 차단되지 않고 개체에 구성한 포트가 열려 있는지 확인합니다.
  - TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 서버에 사용된 호스트 이름과 일치해야 합니다.
  - CLI 액세스를 인증하는 경우, 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
  - 서버 유형 기본값을 사용한 경우 정확한 서버 유형인지 확인하고 **Set Defaults(**기본값 설정**)**를 다시 클릭하여 기본값을 재설정합니다.
- 기본 DN을 입력한 경우 **Fetch DNs(DN** 가져오기**)**를 클릭하여 서버에서 사용 가능한 모든 기본 DN을 가져오고 그 목록에서 이름을 선택합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각각이 올바르고 제대로 입력되었는지 확인합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각 설정을 제거하고 그 설정 없이 개체를 테스트해봅니다.
- 기본 필터 또는 셸 액세스 필터를 사용하는 경우, 필터가 괄호로 묶여 있고 올바른 비교 연산자를 사용하고 있는지 확인합니다. 묶인 괄호를 포함하여 최대 450자까지 입력할 수 있습니다.

- 더 제한적인 기본 필터를 테스트하려면 사용자의 기본 DN으로 설정하여 그 사용자만 검색해봅니다.
- 암호화 연결을 사용하는 경우:
  - 인증서에 있는 LDAP 서버의 이름이 연결에 사용하는 호스트 이름과 매칭되는지 확인합니다.
  - 암호화 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 이름과 비밀번호가 제대로 입력되었는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 크리덴셜을 제거하고 개체를 테스트합니다.
- LDAP 서버에 연결하고 다음 구문을 사용하여 사용 중인 쿼리를 테스트합니다.

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

에를 들어 `myrtle.example.com`의 보안 도메인에 연결하기 위해 `domainadmin@myrtle.example.com` 사용자와 (`cn=*`) 기본 필터를 사용하는 경우, 다음 구문으로 연결을 테스트할 수 있습니다.

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

연결 테스트에 성공했지만 플랫폼 설정 정책을 적용한 후 인증이 되지 않을 경우, 디바이스에 적용되는 플랫폼 설정 정책에서 인증 및 사용할 개체가 모두 활성화되었는지 확인합니다.

성공적으로 연결했지만 연결에서 검색되는 사용자 목록을 조정하려는 경우, 기본 필터 또는 셸 액세스 필터를 추가하거나 변경할 수 있습니다. 또는 더 제한적이거나 덜 제한적인 기본 DN을 사용할 수 있습니다.

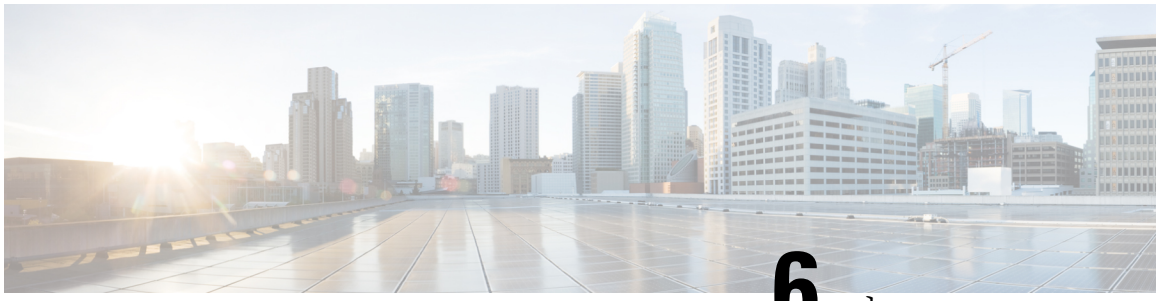
디바이스용 사용자 계정 기록

기능	버전	세부 사항
RADUIS 서버에 정의된 FTD 사용자에 대한 Service-Type(서비스 유형) 속성을 지원합니다.	6.4	FTD CLI 사용자의 RADIUS 인증의 경우, RADIUS 외부 인증 개체에서 사용자 이름을 사전 정의하고 해당 목록과 RADIUS 서버에 정의된 사용자 이름을 수동으로 매칭시켜야 했었습니다. 이제 Service-Type(서비스 유형) 속성을 사용하여 RADIUS 서버의 CLI 사용자를 정의하고 Basic(기본) 및 Config(구성) 사용자 역할을 정의할 수 있습니다. 이 방법을 사용하려면 외부 인증 개체에서 셸 액세스 필터를 공란으로 두어야 합니다. 신규/수정된 화면: **System(**시스템**)** > **Users(**사용자**)** > **External Authentication(**외부 인증**)** > **Add External Authentication Object(**외부 인증 개체 추가**)** > 셸 액세스 필터 **(Shell Access Filter)** 지원되는 플랫폼: FTD
FTD SSH 액세스를 위한 외부 인증	6.2.3	이제 FTD LDAP 또는 RADIUS를 사용하여 SSH 액세스를 위한 외부 인증을 구성할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **External Authentication(**외부 인증**)** 지원되는 플랫폼: FTD

II 부

Firepower System Management

- Firepower System 라이선싱, 157 페이지
- 시스템 업데이트, 179 페이지
- 백업 및 복원, 203 페이지
- 구성 가져오기 및 내보내기, 237 페이지
- 작업 예약, 245 페이지
- 데이터 스토리지, 269 페이지
- Firepower Management Center 고가용성, 275 페이지
- 디바이스 관리 기본 사항, 297 페이지



6 장

Firepower System 라이선싱

버전 6.6의 Licensing(라이선싱) 챕터에서 다양한 라이선스 유형, 서비스 구독, 라이선싱 요구 사항 등의 자세한 정보를 확인할 수 있습니다. 또한 이 장에서는 에어갭 솔루션에 대한 스마트 및 기본 라이선스와 라이선싱 구축 관련 절차 및 요구 사항도 확인할 수 있습니다.

다음 주제에서는 Firepower System 라이선싱 방법을 설명합니다.

- Firepower 라이선스 정보, 157 페이지
- 라이선싱 요구 사항 및 사전 요건, 158 페이지
- Firepower Management Center 라이선스 요구 사항, 158 페이지
- 평가판 라이선스 주의 사항, 159 페이지
- 모든 디바이스 라이선싱, 159 페이지
- FTD 디바이스에서 사용할 클래식 라이선스를 변환하는 방법, 168 페이지
- 디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당, 170 페이지
- 라이선스 만료, 171 페이지
- 이 가이드의 기타 라이선싱 정보, 174 페이지
- Firepower 라이선싱 관련 추가 정보, 176 페이지
- Cisco 지원 진단, 176 페이지
- 라이선싱 기록, 177 페이지

Firepower 라이선스 정보

Firepower 제품(Firepower Management Center 및 매니지드 디바이스)에는 기본 작업에 대한 라이선스가 포함되지만 일부 기능은 이 장에 설명된 대로 별도 라이선싱이나 서비스 스크립션이 필요합니다.

"right-to-use(사용 권한)" 라이선스는 만료되지 않지만 서비스 서브스크립션은 주기적으로 갱신해야 합니다.

제품에서 요구하는 라이선스의 유형은 사용하는 소프트웨어에 따라 달라지며 해당 소프트웨어를 실행하는 하드웨어는 관련이 없습니다.

참고 "NGFW"는 다양한 사람에 대한 다양한 사항을 의미하기 때문에 이 문서에서는 이 용어를 사용하지 않습니다.

라이선싱 요구 사항 및 사전 요건

모델 지원

모두 가능하지만 모델별로 필요한 특정 라이선스는 절차에 나와 있는 것과 다릅니다.

지원되는 도메인

글로벌, 표시된 경우를 제외하고.

사용자 역할

- 관리자

Firepower Management Center 라이선스 요구 사항

Firepower Management Center 매니지드 디바이스에 라이선스를 할당하고 시스템에 대한 라이선스를 관리할 수 있습니다.

하드웨어 **FMC**

하드웨어 Firepower Management Center는 디바이스 관리를 위한 추가 라이선스 구입이나 서비스 서브스크립션이 필요하지 않습니다.

가상 **FMC**

Firepower Management Center 가상은 추가 라이선스 요구 사항이 없습니다. Firepower Management Center Virtual 라이선스, 158 페이지의 내용을 참조하십시오.

Firepower Management Center Virtual 라이선스

일반적으로 Firepower Management Center 가상(FMCv)은 관리하는 각 FTD 디바이스에 대해 라이선스 엔타이틀먼트가 필요합니다. FMCv에는 클래식 디바이스를 관리하는 데 Firepower MCv 라이선스가 필요하지 않습니다.

단일 FMCv가 고가용성 쌍으로 구성되는 Firepower Threat Defense 디바이스를 관리하는 경우에도 각 디바이스에 대해 하나의 엔타이틀먼트가 필요합니다(FTD 쌍마다 엔타이틀먼트 하나가 아님).

고가용성 설정의 FMCv의 경우 FMC 고가용성 설정에 대한 라이선스 요구 사항, 282 페이지의 내용을 참조하십시오.

다중 인스턴스 구축에서 각 보안 모듈에 대해 하나의 엔타이틀먼트가 필요합니다.

스마트 라이선싱이 연결된 표준에서, 이러한 라이선스는 영구적입니다.

Specific License Reservation(특정 라이선스 예약)에서 이러한 라이선스에는 기한이 있습니다.

이 엔타이틀먼트는 Cisco Smart Software Manager에 **Firepower MCv** 디바이스 라이선스로 표시되며, 표시되는 엔타이틀먼트 수는 다양합니다.

평가판 라이선스 주의 사항

평가판 라이선스는 모드 기능을 사용할 수 없습니다. 평가판 라이선스의 기능을 부분적일 수 있으며 평가판 라이선싱에서 표준 라이선성으로의 전환이 원활하지 않을 수 있습니다.

예를 들어 Firepower Threat Defense 디바이스가 클러스터로 구성되어 있고 평가판 라이선스에서 스마트 라이선싱으로 전환하는 경우, 변경 사항을 배포할 때 서비스가 중단됩니다.

평가판 라이선스 주의사항에 대한 정보는 Licensing(라이선싱)에 관한 본 장 및 각 기능 배포에 관한 다른 장에 포함된 특정 기능 정보를 참조하십시오.

모든 디바이스 라이선싱

7000 및 8000 Series 및 NGIPSv 디바이스와 ASA FirePOWER 모듈은 기본 라이선스를 요구합니다. 이러한 디바이스를 이 문서에서는 종종 클래식 디바이스라고 합니다.

중요 Firepower 하드웨어는 실행하지만 Firepower 소프트웨어는 실행하지 않는 경우, 사용하고 있는 소프트웨어 제품에 대한 라이선싱 정보를 참조하십시오. 이 문서는 적용할 수 없습니다.

기본 라이선스는 PAK(제품 인증 키)를 활성화해야 하고 디바이스에 따라 달라집니다. 기본 라이선스는 때로 "traditional licensing(전통적 라이선싱)"이라고도 합니다.

제품 라이선스 등록 포털

Firepower 기능에 대해 하나 이상의 기본 라이선스를 구매하는 경우, 해당 라이선스는 Cisco Product License Registration Portal에서 관리할 수 있습니다.

https://cisco.com/go/license

이 포털을 사용에 관한 자세한 내용은 다음을 참조하십시오.

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

이러한 링크에 액세스하려면 계정 자격 증명이 필요합니다.

Firepower 기능에 대한 서비스 서브스크립션(클래식 라이선싱)

일부 기능은 서비스 서브스크립션이 필요합니다.

서비스 서브스크립션은 매니지드 디바이스에서 정해진 기간 동안 특정 Firepower 기능을 활성화합니다. 서비스 서브스크립션은 1년, 3년 또는 5년 기간으로 구입할 수 있습니다. 서브스크립션이 만료되는 경우, Cisco가 서브스크립션을 갱신해야 한다고 알려줍니다. 클래식 디바이스에 대한 서브스크립션이 만료되는 경우, 기능 유형에 따라 관련 기능을 사용할 수 없습니다.

표 *2:* 서비스 서브스크립션 및 해당 기본 라이선스

구매한 서브스크립션	**Firepower System**에서 할당하는 기본 라이선스
TA	제어 + 보호 (즉, 시스템 업데이트에 필요한 "위협 & 앱")
TAC	제어 + 보호 + URL 필터링
TAM	제어 + 보호 + 악성코드
TAMC	제어 + 보호 + URL 필터링 + 악성코드
URL	URL 필터링 (TA가 이미 존재하는 경우 애드온)
AMP	악성코드 (TA가 이미 존재하는 경우 애드온)

기본 라이선스를 사용하는 매니지드 디바이스를 구매하는 경우 제어 및 보호 라이선스가 포함됩니다. 이러한 라이선스는 영구적이지만, TA 서비스 서브스크립션도 구입해야 서비스 업데이트를 활성화할 수 있습니다. 추가 기능에 대한 서비스 서브스크립션은 선택 사항입니다.

기본 라이선스 유형 및 제한 사항

이 섹션에서는 Firepower System 구축에서 사용 가능한 기본 라이선스의 유형에 대해 설명합니다. 디바이스에서 활성화할 수 있는 라이선스는 해당 모델, 버전 및 활성화된 다른 라이선스에 따라 달라질 수 있습니다.

라이선스는 7000 및 8000 Series 및 NGIPSv 디바이스와 ASA FirePOWER 모듈의 모델에 따라 다릅니다. 라이선스가 디바이스 모델과 정확히 일치하지 않는 경우 매니지드 디바이스에서 라이선스를 활성화할 수 없습니다. 예를 들어, Firepower 8250 악성코드 라이선스(FP8250-TAM-LIC =)를 사용하여 8140 디바이스의 악성코드 기능을 활성화할 수 없습니다. Firepower 8140 악성코드 라이선스 (FP8140-TAM-LIC =)를 구매해야 합니다.

참고 NGIPSv 또는 ASA FirePOWER의 경우, 제어 라이선스를 사용하면 사용자 및 애플리케이션 제어를 수행할 수 있지만 이러한 디바이스는 스위칭, 라우팅, 스태킹 또는 7000 및 8000 Series 디바이스 고가용성을 지원하지 않습니다.

Firepower System의 라이선싱된 기능에 대한 액세스 권한이 차단될 수 있는 방법이 몇 가지 있습니다.

- Firepower Management Center에서 기본 라이선스를 제거할 수 있는데, 이는 해당 매니지드 디바이스 모두에 영향을 줍니다.
- 또한 특정 매니지드 디바이스에서 라이선싱된 기능을 비활성화할 수 있습니다.

일부 예외가 있지만, 만료 또는 삭제된 라이선스와 관련된 기능을 사용할 수 없습니다.

다음 표에는 Firepower System 기본 라이선스가 요약되어 있습니다.

표 ***3: Firepower System*** 기본 라이선스

Firepower System에서 할당하는 라이선스	구매한 서비스 서브스크립션	플랫폼	부여된 기능	추가 필요 항목	만료 가능**?**
Any(모든)	TA, TAC, TAM 또는 TAMC	7000 및 8000 Series ASA FirePOWER NGIPSv	호스트, 애플리케이션 및 사용자 검색 SSL 및 TLS로 암호화된 트래픽 암호 해독 및 검사	없음	라이선스에 따라 달라집니다
보호	TA (디바이스에 포함)	7000 및 8000 Series ASA FirePOWER NGIPSv	침입 탐지 및 방지 파일 제어 보안 인텔리전스 필터링	없음	아니요
제어	none (없음) (디바이스에 포함)	7000 및 8000 Series	사용자 및 애플리케이션 제어 스위칭 및 라우팅 7000 및 8000 Series 디바이스 고가용성 7000 및 8000 Series NAT(Network Address Translation)	보호	아니요
제어	none (없음) (디바이스에 포함)	ASA FirePOWER NGIPSv	사용자 및 애플리케이션 제어	보호	아니요
악성코드	TAM, TAMC 또는 AMP	7000 및 8000 Series ASA FirePOWER NGIPSv	AMP for Networks (네트워크 기반 고급 악성코드 보호) 파일 스토리지	보호	예
URL 필터링	TAC, TAMC, 또는 URL	7000 및 8000 Series ASA FirePOWER NGIPSv	카테고리 및 평판 기반 URL 필터링	보호	예

Firepower System에서 할당하는 라이선스	구매한 서비스 서브스크립션	플랫폼	부여된 기능	추가 필요 항목	만료 가능?
VPN	none (없음) (자세한 내용은 영업팀에 문의)	7000 및 8000 Series	가상 사설망 구축	제어	예

보호 라이선스

보호 라이선스는 침입 탐지 및 방지, 파일 제어 및 보안 인텔리전스 필터링을 수행할 수 있습니다.

- 침입 탐지 및 방지를 사용하면 침입 및 공격의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다.
- *File control(*파일 제어*)*를 사용하면 사용자가 특정 애플리케이션 프로토콜에 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 악성코드 라이선스가 필요한 *AMP for Networks* 는 제한적인 해당 파일 유형 집합을 속성에 따라 검사 및 차단할 수 있습니다.
- *Security Intelligence filtering(*보안 인텔리전스 필터링*)*을 사용하면 트래픽이 액세스 제어 규칙에 따라 분석의 대상이 되기 전에 특정 IP 주소, URL 및 DNS 도메인 이름을 차단 목록에 추가하고 이를 오고가는 트래픽을 거부할 수 있습니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 차단할 수 있습니다. 경우에 따라 Seurity Intelligence 필터링에 "모니터링 전용" 설정을 사용할 수 있습니다.

보호 라이선스(및 제어 라이선스)는 클래식 매니지드 디바이스를 구매하는 경우 자동으로 포함됩니다. 이러한 라이선스는 영구적이지만, TA 서비스 서브스크립션도 구입해야 서비스 업데이트를 활성화할 수 있습니다.

액세스 제어 정책을 구성하여 라이선스 없이 Protection(보호) 관련 검사를 수행할 수 있지만, 먼저 보호 라이선스를 Firepower Management Center에 추가한 후 정책의 대상이 되는 디바이스에서 활성화할 때까지 해당 정책을 적용할 수 없습니다.

보호 라이선스를 Firepower Management Center에서 삭제하거나 매니지드 디바이스에서 보호를 비활성화하면 Firepower Management Center는 영향을 받는 디바이스에서 침입 및 파일 이벤트의 인지를 중지합니다. 결과적으로, 해당 이벤트를 트리거 기준으로 사용하는 상관성 규칙이 실행을 중지합니다. 또한 Firepower Management Center은 Cisco 제공 정보나 서드파티 Security Intelligence 정보를 검색하기 위해 인터넷에 접속하지 않습니다. 보호 라이선스를 다시 활성화할 때까지 기존 정책을 다시 배포할 수 없습니다.

보호 라이선스가 URL 필터링, 악성코드 및 제어 라이선스에 필요하므로, 보호 라이선스를 삭제 또는 비활성화하는 것은 URL 필터링, 악성코드 및 제어 라이선스를 삭제 또는 비활성화하는 것과 영향이 같습니다.

제어 라이선스

제어 라이선스를 사용하면 액세스 제어 규칙에 사용자 및 애플리케이션 상태를 추가하여 사용자 및 애플리케이션 제어를 수행할 수 있습니다. 7000 및 8000 Series 디바이스 한정으로, 이 라이선스를 사용하면 스위칭 및 라우팅(DHCP 릴레이 및 NAT 포함), 디바이스 고가용성 쌍을 구성할 수 있습니다. 매니지드 디바이스에서 제어 라이선스를 활성화하려면 보호 라이선스도 활성화해야 합니다. 제어 라이선스(및 보호 라이선스)는 클래식 매니지드 디바이스를 구매하는 경우 자동으로 포함됩니다. 이러한 라이선스는 영구적이지만, TA 서비스 서브스크립션도 구입해야 서비스 업데이트를 활성화할 수 있습니다.

클래식 매니지드 디바이스에 대해 제어 라이선스를 활성화하지 않은 경우, 사용자 및 애플리케이션 조건을 액세스 제어 정책의 규칙에 추가할 수 있지만 해당 정책을 디바이스에 배포할 수는 없습니다. 7000 또는 8000 Series디바이스에 대해 제어 라이선스를 활성화하지 않으면, 다음도 수행할 수 없습니다.

- 스위칭, 라우팅 또는 하이브리드 인터페이스 생성
- NAT 항목 생성
- 가상 라우터에 대한 DHCP 릴레이 구성
- 디바이스 스위치 또는 라우팅을 포함하는 디바이스 구성 배포
- 디바이스 간 고가용성 설정

참고 제어 라이선스 없이 가상 스위치와 라우터를 생성할 수 있지만 이들을 채우기 위한 스위칭 및 라우팅 인터페이스가 없으면 유용하지 않습니다.

Firepower Management Center에서 제어 라이선스를 삭제하거나 개발 장치에서 제어를 비활성화하는 경우는 다음과 같습니다.

- 영향을 받는 디바이스는 스위칭 또는 라우팅 수행을 중단하지 않으며 디바이스 고가용성 쌍도 중단하지 않습니다.
- 기존 구성을 계속 편집하고 삭제할 수는 있지만, 영향을 받는 디바이스에 그러한 변경 사항을 배포할 수 없습니다.
- 새로운 스위칭, 라우팅 또는 하이브리드 인터페이스를 추가할 수 없으며, 새 NAT 항목을 추가하거나 DHCP 릴레이를 구성하거나 7000 또는 8000 Series 디바이스 고가용성을 설정할 수도 없습니다.
- 사용자 또는 애플리케이션 조건이 있는 규칙이 포함된 경우 기존 액세스 제어 정책을 다시 배포할 수 없습니다.

클래식 디바이스에 대한 **URL** 필터링 라이선스

URL 필터링을 사용하면 액세스 제어 규칙을 작성할 수 있습니다. 이 규칙은 모니터링된 호스트에서 요청하고 URL 정보와 상호 연결된 해당 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정

합니다. URL 필터링 라이선스를 활성화하려면 보호 라이선스도 활성화해야 합니다. 클래식 디바이스에 대한 URL 필터링 라이선스를 위협 & 앱(TAC) 또는 위협 & 앱 및 악성코드(TAMC) 서브스크립션과 결합된 서비스 서브스크립션으로 구입할 수 있습니다. 위협 & 앱(TA) 서브스크립션이 이미 활성화된 시스템의 경우 애드온 서브스크립션(URL)으로도 구입할 수 있습니다.

팁 URL 필터링 라이선스가 없는 경우, 허용하거나 차단하려는 개별 URL 또는 URL 그룹을 지정할 수 있습니다. 이를 통해 웹 트래픽에 대한 세분화된 사용자 지정 제어를 가질 수 있지만 URL 카테고리와 평판 데이터를 사용하여 네트워크 트래픽을 필터링할 수는 없습니다.

URL 필터링 라이선스 없이도 액세스 제어 규칙에 카테고리 및 평판 기반 URL 조건을 추가할 수 있지만, Firepower Management Center은 URL 정보를 다운로드하지 않습니다. URL 필터링 라이선스를 Firepower Management Center에 추가한 후 정책의 대상이 되는 디바이스에서 활성화할 때까지는 액세스 제어 정책을 배포할 수 없습니다.

Firepower Management Center에서 라이선스를 삭제하거나 매니지드 디바이스에서 URL 필터링을 비활성화하는 경우, URL 필터링에 대한 액세스가 차단될 수 있습니다. 또한 URL 필터링 라이선스가 만료될 수 있습니다. 라이선스가 만료되거나 라이선스를 비활성화하는 경우, URL 조건이 포함된 액세스 제어 규칙이 URL 필터링을 즉시 중지하고 Firepower Management Center은 더 이상 업데이트를 URL 데이터에 다운로드할 수 없습니다. 카테고리 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.

클래식 디바이스에 대한 악성코드 라이선스

악성코드 라이선스를 사용하면 AMP for Networks 와 Cisco Threat Grid이 포함된 Cisco AMP(고급 악성코드 보호)를 수행할 수 있습니다. 매니지드 디바이스를 사용하여 네트워크를 통해 전송된 파일에서 악성코드를 탐지 및 차단할 수 있습니다. 악성코드 라이선스를 활성화하려면 보호 라이선스도 활성화해야 합니다. 악성코드 라이선스를 위협 & 앱(TAM) 또는 위협 & 앱 및 URL 필터링(TAMC) 서브스크립션과 결합된 서브스크립션으로 구입할 수 있습니다. 위협 & 앱(TA) 서브스크립션이 이미 활성화된 시스템의 경우 애드온 서브스크립션(AMP)으로도 구입할 수 있습니다.

참고 7000 및 8000 Series 악성코드 라이선스가 활성화된 매니지드 디바이스는 사용자가 동적 분석을 구성하지 않은 경우에도 AMP 클라우드 연결을 주기적으로 시도합니다. 따라서, 디바이스의 Interface Traffic(인터페이스 트래픽) 대시보드 위젯은 전송된 트래픽을 보여주며, 이는 예상된 작업입니다.

사용자는 파일 정책의 일부로서 AMP for Networks 를 구성한 후 하나 이상의 액세스 제어 규칙과 연결합니다. 파일 정책은 사용자가 특정 애플리케이션 프로토콜을 통해 특정 유형의 파일을 업로드 또는 다운로드하는지를 탐지할 수 있습니다. AMP for Networks 을 통해 로컬 악성 코드 분석 및 파일 사전 분류를 사용하여 그러한 제한된 파일 유형의 집합에 악성코드가 있는지 검사할 수 있습니다. 또한 Cisco Threat Grid 클라우드에서 특정 파일 유형을 다운로드 및 전송하여 동적 분석과 Spero 분석으로 해당 파일에 악성코드가 포함되었는지 여부를 결정합니다. 이러한 파일에서 네트워크 파일 경로를 상세히 볼 수 있습니다. 악성코드 라이선스는 또한 특정 파일을 파일 목록에 추가하고 파일 정책 내에서 파일 목록을 활성화하며, 해당 파일이 탐지되면 자동으로 허용하거나 차단하도록 허용합니다.

AMP for Networks 구성을 포함하는 액세스 제어 정책을 배포하기 전에 반드시 악성코드 라이선스를 추가한 후, 정책의 대상이 되는 디바이스에서 이 라이선스를 활성화해야 합니다. 나중에 디바이스에서 이 라이선스를 비활성화하는 경우, 해당 디바이스에 기존 액세스 제어 정책을 다시 배포할 수 없습니다.

악성코드 라이선스가 모두 삭제되거나 만료된 경우, 시스템에서 AMP 클라우드에 대한 쿼리를 중단하며 AMP 클라우드에서 전송한 회귀적 이벤트 확인도 중지합니다. AMP for Networks 구성이 포함된 경우, 기존 액세스 제어 정책은 재적용할 수 없습니다. 악성코드 라이선스가 만료되거나 삭제된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 시간 창이 만료된 후 시스템은 해당 파일에 `Unavailable(사용 불가)` 속성을 할당합니다.

AMP for Networks 및 Cisco Threat Grid를 구축하는 경우에만 악성코드 라이선스가 필요합니다. 악성코드 라이선스가 없는 경우, Firepower Management Center은 엔드포인트 악성코드 이벤트용 AMP 및 IOC(보안 침해 지표)를 AMP 클라우드에서 받을 수 있습니다.

파일 및 악성코드 정책을 위한 라이선스 요구 사항, 1863 페이지에 있는 중요 정보도 참조하십시오.

7000 및 8000 시리즈 디바이스에 대한 VPN 라이선스

VPN을 사용하면 인터넷이나 기타 네트워크 등 공개 소스를 통해 엔드포인트 간 안전한 터널을 설정할 수 있습니다. 7000 및 8000 Series 디바이스의 가상 라우터 간에 안전한 VPN 터널을 구축하도록 Firepower System을 구성할 수 있습니다. VPN을 활성화하려면 보호 및 제어 라이선스도 활성화해야 합니다. VPN 라이선스를 구입하려면 영업팀에 문의하십시오.

VPN 라이선스가 없는 경우, 7000 및 8000 Series디바이스에서 VPN 구축을 구성할 수 없습니다. 구축은 생성할 수 있지만 거기에 추가할 VPN이 활성화된 라우팅 인터페이스가 없으면 효용이 없습니다.

Firepower Management Center에서 VPN 라이선스를 삭제하거나 개별 디바이스에서 VPN을 비활성화하는 경우, 영향을 받는 디바이스가 현재 VPN 구축을 중단하지 않습니다. 기존 구축을 수정 및 삭제할 수는 있지만 영향을 받는 디바이스에 변경 사항을 구축할 수는 없습니다.

디바이스 스택 및 고가용성 쌍의 기본 라이선스

개별 디바이스는 해당 라이선스를 보유한 후 7000 또는 8000 Series 디바이스 고가용성 쌍으로 스태킹 또는 구성될 수 있습니다. 디바이스를 스태킹한 후에는 전체 스택에 대해서만 라이선스를 변경할 수 있습니다. 그러나 7000 또는 8000 Series 디바이스 고가용성 쌍에서 활성화된 라이선스를 변경할 수 없습니다.

디바이스 스택 관련 정보 및 디바이스 고가용성 요구 사항도 참조하십시오.

기본 라이선스 보기

프로시저

필요에 따라 다음 중 하나를 수행합니다.

보려는 내용	수행해야 할 작업
Firepower Management Center에 추가한 기본 라이선스 및 해당 유형, 상태, 사용, 만료 날짜를 포함하는 세부정보, 그러한 라이선스가 적용되는 매니지드 디바이스.	**System**(시스템) > **Licenses**(라이선스) > **Classic Licenses**(기본 라이선스)를 선택합니다. 요약에는 구입한 라이선스의 수와 사용 중인 라이선스의 수(괄호로 표시)가 나와 있습니다.
각 매니지드 디바이스에 적용된 라이선스	**Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.
상태 모니터에서 라이선스 상태	기본 라이선스 모니터 상태 모듈을 상태 정책에 사용합니다. 자세한 내용은 상태 모니터링, 387 페이지, 상태 모듈, 389 페이지 및 상태 정책 생성, 398 페이지을 참조하십시오.
대시보드의 라이선스 개요	Product Licensing(제품 라이선싱) 위젯을 원하는 대시보드에 추가합니다. 자세한 내용은 제품 라이선싱 위젯, 376 페이지, 대시보드에 위젯 추가, 379 페이지 및 사용자 역할별 대시보드 위젯 가용성, 365 페이지을 참조하십시오.

라이선스 키를 식별합니다.

라이선스 키는 Cisco 라이선스 등록 포털에서 Firepower Management Center를 고유하게 식별합니다. 관리 포트 (eth0)의 MAC 주소와 제품 코드 (예를 들어, 66)의 구성 된는 Firepower Management Center; 예를 들어, 66:00:00:77:FF:CC:88 합니다.

Cisco License Registration Portal에서 라이선스 키를 사용하여 필요한 라이선스 텍스트를 가져오고 라이선스를 Firepower Management Center에 추가합니다.

프로시저

단계 **1** **System**(시스템) > **Licenses**(라이선스) > **Classic Licenses**(기본 라이선스)를 선택합니다.

단계 **2** **Add New License**(새 라이선스 추가)를 클릭합니다.

단계 **3** **Add Feature License**(기능 라이선스 추가) 대화상자 상단에 있는 **License Key**(라이선스 키) 필드 값을 참조하십시오.

다음에 수행할 작업

- 라이선스를 Firepower Management Center에 추가합니다. 기본 라이선스 생성 및 추가 Firepower Management Center, 167 페이지를 참조하십시오.

이 절차에는 라이선스 키를 사용하여 실제 라이선스 텍스트를 생성하는 과정이 포함됩니다.

기본 라이선스 생성 및 추가 Firepower Management Center

참고 백업이 완료된 후 라이선스를 추가할 경우, 이 라이선스는 백업이 복구된다고 해도 제거되거나 덮어써지지 않습니다. 복원 시 충돌을 방지하려면 백업을 복원하기 전에 라이선스가 어디에 사용되었는지에 유의하여 해당 라이선스를 제거합니다. 그리고 백업을 복원한 후 라이선스를 추가하고 재구성합니다. 충돌이 발생하면 Support(지원부)에 문의하십시오.

팁 또한 지원 사이트에 로그인한 후 **Licenses(**라이선스**)** 탭에서 라이선스를 요청할 수 있습니다.

시작하기 전에

- 라이선스를 구매할 때 Cisco가 제공한 소프트웨어 클레임 인증서에 PAK(제품 활성화 키)가 있는지 확인합니다. 레거시, Cisco 이전 라이선스가 있는 경우 지원팀에 문의합니다.
- Firepower Management Center에 대한 라이선스 키를 식별합니다. 라이선스 키를 식별합니다., 166 페이지를 참조하십시오.
- 이 절차를 완료하려면 사용자 계정의 자격 증명이 필요합니다.

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.

단계 **2** **Add New License(**새 라이선스 추가**)**를 클릭합니다.

단계 **3** 해당하는 작업을 계속 진행합니다.

- 이미 라이선스 텍스트를 가져온 경우 8단계로 건너뜁니다.
- 여전히 라이선스 텍스트를 가져와야 한다면 다음 단계로 이동합니다

단계 **4** **Get License(**라이선스 가져오기**)**를 클릭하여 Cisco 라이선스 등록 포털을 엽니다.

참고 현재 컴퓨터를 사용하여 인터넷에 액세스할 수 없는 경우, 액세스가 가능한 컴퓨터로 전환하고 http://cisco.com/go/license로 이동합니다.

단계 **5** 라이선스 등록 포털에서 PAK로 라이선스를 생성합니다.

이 단계에는 구매 과정에서 받은 PAK 뿐만 아니라 Firepower Management Center에 대한 라이선스 키도 필요합니다.

자세한 내용은 제품 라이선스 등록 포털, 159 페이지를 참조하십시오.

단계 **6** 라이선스 등록 포털이나 라이선스 등록 포털에서 발송한 이메일에서 라이선스 텍스트를 복사합니다.

중요 포털 또는 이메일 메시지에 있는 라이선스 텍스트 블록에는 하나 이상의 라이선스가 포함될 수 있습니다. 각 라이선스는 BEGIN LICENSE 행과 END LICENSE 행으로 구분됩니다. 한 번에 라이선스 하나만 복사하고 붙이도록 합니다.

단계 **7** Firepower Management Center 웹 인터페이스에서 **Add Feature License(**기능 라이선스 추가**)** 페이지로 돌아갑니다.

단계 **8** 라이선스 텍스트를 **License(**라이선스**)** 필드에 붙입니다.

단계 **9** **Verify License(**라이선스 확인**)**을 클릭합니다.

라이선스가 유효하지 않은 경우, 라이선스 텍스트를 제대로 복사했는지 확인합니다.

단계 **10** **Submit License(**라이선스 제출**)**을 클릭합니다.

다음에 수행할 작업

- 라이선스를 매니지드 디바이스로 할당합니다. 디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당, 170 페이지을 참조하십시오. 매니지드 디바이스에서 라이선스가 부여된 기능을 사용하려면 그러한 디바이스에 라이선스를 반드시 할당해야 합니다.

FTD 디바이스에서 사용할 클래식 라이선스를 변환하는 방법

LRP(라이선스 등록 포털) 또는 CSSM(Cisco Smart Software Manager)를 사용하여 라이선스를 전환할 수 있으며, 디바이스에 이미 할당된 미사용 PAK(제품 인증 키) 또는 기본 라이선스를 전환할 수 있습니다.

중요 이 프로세스를 취소할 수 없습니다. 라이선스가 원래 기본 라이선스였더라도 스마트 라이선스를 기본 라이선스로 전환할 수 없습니다.

Cisco.com에 있는 문서에서 기본 라이선스는 "traditional(전통적)" 라이선스라도고 합니다.

시작하기 전에

- 기본 라이선스가 아직 제품 인스턴스에 할당되지 않은 미사용 PAK인 경우, 기본 라이선스를 스마트 라이선스로 전환하는 것은 어렵지 않습니다.
- 하드웨어가 Firepower Threat Defense를 실행할 수 있어야 합니다. *Cisco Firepower* 호환성 가이드(https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html)를 참조하십시오.

- 스마트 어카운트가 있어야 합니다. 어카운트가 없는 경우 하나를 생성합니다. 스마트 어카운트를 생성하고 라이선스 보유의 내용을 참조하십시오.
- 변환하려는 PAK 또는 라이선스가 스마트 어카운트에 나타나야 합니다.
- Cisco Smart Software Manager 대신 라이선스 등록 포털을 사용하여 전환하는 경우, 스마트 어카운트 크리덴셜이 있어야 전환 프로세스를 개시할 수 있습니다.

프로시저

단계 **1** 수행할 전환 프로세스는 라이선스 사용 여부에 따라 달라집니다.

- 전환하려는 PAK가 미사용인 경우, PAK 전환에 대한 지침을 따르십시오.
- 전환하려는 PAK가 이미 디바이스에 할당된 경우, 기본 라이선스 전환에 대한 지침을 따르십시오.

  기존 기본 라이선스가 아직 디바이스에 등록되어 있는지 확인합니다.

단계 **2** 다음 문서에서 전환 유형(PAK 또는 설치된 기본 라이선스)에 대한 지침을 참조하십시오.

- LRP를 사용하여 PAK 또는 라이선스를 변환하는 경우:
  - 라이선스 등록 포털을 통한 전환 프로세스 단계에 대한 비디오를 보시려면 https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780를 클릭합니다.
  - 다음 https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu 문서에서 "Convert(전환)"을 검색합니다.

    전환 절차는 세 가지가 있습니다. 상황에 맞는 전환 절차를 선택합니다.
  - LRP(라이선스 등록 포털)(https://tools.cisco.com/SWIFT/LicensingUI/Home)에 로그인하고 위 문서의 지침을 따르십시오.
- CSSM을 활용하여 PAK 또는 라이선스를 변환하는 경우:
  - 하이브리드 라이선스를 스마트 소프트웨어 라이선스 *QRG*로 전환:

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - CSSM(https://software.cisco.com/#SmartLicensing-LicenseConversion)에 로그인하고 위 다음 문서에 있는 전환 유형(PAK 또는 설치된 기본 라이선스)에 대한 지침을 따르십시오.

단계 **3** 하드웨어에 Firepower Threat Defense를 새로 설치합니다.

하드웨어에 대한 지침을 참조하십시오(https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html).

단계 **4** Firepower Device Manager을 사용하여 이 디바이스를 독립형 디바이스로 관리하려는 경우:

*Firepower Device Manager*용 *Cisco Firepower Threat Defense* 구성 가이드(https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html)에서 디바이스 라이선싱에 관한 정보를 참조하십시오.

이 절차의 나머지 부분을 건너뜁니다.

단계 **5** 이미 Firepower Management Center에 스마트 라이선싱을 구축한 경우:

a) 새 Firepower Threat Defense 디바이스에서 스마트 라이선싱을 설정합니다.

여러 매니지드 디바이스에 라이선스 할당의 내용을 참조하십시오.

b) 새 스마트 라이선스가 디바이스에 성공적으로 적용되었는지 확인합니다.

FTD 라이선스 및 라이선스 상태 보기의 내용을 참조하십시오.

단계 **6** 아직 Firepower Management Center에 스마트 라이선싱을 구축하지 않은 경우:

스마트 라이선스 등록의 내용을 참조하십시오.

디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당

몇 가지 예외는 있지만 매니지드 디바이스에서 비활성화한 라이선스와 관련된 기능은 사용할 수 없습니다.

참고 동일한 보안 모듈/엔진에 있는 컨테이너 인스턴스의 경우, 각 인스턴스에 라이선스를 적용합니다. 참고로 보안 모듈/엔진는 보안 모듈/엔진의 모든 인스턴스에 대해 기능당 하나의 라이선스만 사용합니다.

시작하기 전에

- 디바이스를 Firepower Management Center에 추가합니다. FMC에 디바이스 추가, 311 페이지의 내용을 참조하십시오.
- 이 작업을 수행하려면 관리자 또는 네트워크 관리자 권한으로 로그인해야 합니다. 여러 도메인을 사용하여 작업하는 경우 리프 도메인에서 이 작업을 수행해야 합니다.
- 스마트 라이선스를 할당하는 경우:
  - 한 번에 여러 디바이스에 스마트 라이선스를 적용 해야 하는 경우 다음 절차를 수행하는 대신 스마트 라이선스 페이지를 사용합니다. 여러 매니지드 디바이스에 라이선스 할당의 내용을 참조하십시오.
  - 스마트 라이선스를 매니지드 디바이스에 배포 준비: 스마트 라이선스 등록 참조

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 라이선스를 활성화 또는 비활성화하려는 디바이스 옆에 있는 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 디바이스를 클릭합니다.

단계 **4** License(라이선스) 섹션 옆에 있는 수정( )을 클릭합니다.

단계 **5** 해당 확인란을 선택하거나 지우고 디바이스에 대한 라이선스를 할당하거나 비활성화합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 스마트 라이선스를 할당하는 경우, 라이선스 상태를 확인합니다.

  System(시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**로 이동하여 Smart License(스마트 라이선스) 테이블 상단에 있는 필터에 디바이스의 호스트 이름 또는 IP 주소를 입력한 후, 라이선스 유형별 각 디바이스에 녹색 원(확인 표시( ))만 표시되는지 확인합니다. 다른 아이콘이 표시되는 경우, 아이콘 위에 마우스를 놓으면 자세한 정보가 표시됩니다.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

라이선스 만료

- 라이선스 만료 vs. 서비스 서브스크립션 만료
- Smart Licensing
- 특정 라이선스 예약
- Classic Licensing
- 서브스크립션 갱신

라이선스 만료 **vs.** 서비스 서브스크립션 만료

Q. Firepower 기능 라이선스가 만료되나요?

A. 엄밀히 말해 Firepower 기능 라이선스는 만료되지 않습니다. 대신 그러한 라이선스를 지원하는 서비스 서브스크립션이 만료됩니다. 서비스 서브스크립션에 대한 세부정보는 https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html에서 사용 가능한 *Firepower Management*

Center 구성 가이드의 "Service Subscriptions for Firepower Features(Firepower 기능용 서비스 서브스크립션)"을 참조하십시오.

Smart Licensing

Q. 제품 인스턴스 등록 토큰이 만료될 수 있나요?

A. 토큰은 지정된 유효 기간 내에 제품 등록에 사용되지 않으면 만료될 수 있습니다. Cisco Smart Software Manager에서 토큰을 생성하는 경우, 토큰 유효일수를 설정합니다. 토큰을 사용하여 Firepower Management Center을 등록하기 전에 토근이 만료되는 경우, 새 토큰을 생성해야 합니다.

토큰을 사용하여 Firepower Management Center을 등록한 경우, 토큰 만료일은 더 이상 의미가 없습니다. 토큰 만료일이 경과하는 경우, 해당 토큰을 사용하여 등록한 Firepower Management Center에 아무런 영향도 주지 않습니다.

토큰 만료일은 서브스크립션 만료일에 영향을 주지 않습니다.

자세한 내용은 *Cisco Smart Software Manager* 사용자 가이드를 참조하십시오.

Q. 스마트 라이선스/서비스 서브스크립션이 만료되었거나 만료될 예정이라면 어떻게 알 수 있나요?

A. 서비스 서브스크립션이 언제 만료되는지 (또는 언제 만료되었는지) 확인하려면 Cisco Smart Software Manager에서 사용자 엔타이틀먼트를 검토합니다.

Firepower Management Center에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택하여 기능 라이선스에 대한 서비스 서브스크립션이 현재 준수 상태인지 확인할 수 있습니다. 이 페이지의 테이블에서 제품 등록 토큰을 통해 Firepower Management Center와 연결된 스마트 라이선스 엔타이틀먼트를 간략히 보여줍니다. **License Status(**라이선스 상태**)**를 기준으로 기능 라이선스에 대한 서비스 서브스크립션이 현재 준수 상태인지 확인할 수 있습니다.

Firepower Device Manager에서 Smart License(스마트 라이선스) 페이지를 사용하여 시스템에 대한 현재 라이선스 상태를 확인합니다. **Device(**디바이스**)**를 클릭한 다음 Smart License(스마트 라이선스) 요약에서 **View Configuration(**구성 보기**)**를 클릭합니다.

또한 Cisco Smart Software Manager가 라이선스 만료 3개월 전에 사용자에게 알림을 보냅니다.

Q. 스마트 라이선스/서브스크립션이 만료되면 어떻게 되나요?

A. 구매한 서비스 서브스크립션이 만료되는 경우, Firepower Management Center와 스마트 어카운트에 해당 어카운트가 미준수 상태인 것으로 표시됩니다. Cisco가 서브스크립션을 갱신해야 한다고 알려줍니다. Subscription Renewals(서브스크립션 갱신)을 참조하십시오. 다른 영향은 없습니다.

특정 라이선스 예약

Q. 특정 라이선스 예약이 만료되면 어떻게 되나요?

A. SLR 라이선스는 기간이 정해져 있습니다.

필요한 라이선스가 사용 불가능하거나 만료된 경우, 다음 작업이 제한됩니다.

- 디바이스 등록
- 정책 구축

Classic Licensing

Q. 기본 라이선스/서비스 서브스크립션이 만료되었거나 만료될 예정이라면 어떻게 알 수 있나요?

A. Firepower Management Center에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.

이 페이지에서 테이블에는 Firepower Management Center에 추가된 기본 라이선스가 요약되어 있습니다.

Status(상태**)** 필드를 기준으로 기능 라이선스에 대한 서비스 서브스크립션이 현재 준수 상태인지 확인할 수 있습니다.

Expires(만료**)** 필드의 날짜를 기준으로 서비스 서브스크립션이 언제 만료되는지 (또는 언제 만료되었는지) 확인할 수 있습니다.

또한 Cisco 제품 라이선스 등록 포털에서 라이선스 정보를 검토하여 이 정보를 얻을 수 있습니다.

Q. 'IPS 기간 서브스크립션이 여전히 IPS에 필요한가'의 의미는 무엇일까요?

A. 이 메시지는 보호 및 제어 기능은 사용 권한 라이선스(영구적) 뿐만 아니라 주기적으로 갱신해야 하는 하나 이상의 관련 서비스 서브스크립션이 필요하다는 것을 알려줍니다. 사용하려는 서비스 서브스크립션이 현재 사용 중이고 만료가 임박하지 않은 경우, 아무런 작업도 필요하지 않습니다.

Q. 기본 라이선스/서브스크립션이 만료되면 어떻게 되나요?

A. 기본 라이선스를 지원하는 서비스 서브스크립션이 만료된 경우, Cisco가 해당 서브스크립션을 갱신해야 하다고 알려줍니다. Subscription Renewals(서브스크립션 갱신)을 참조하십시오.

기능 유형에 따라 관련 기능을 사용할 수 없습니다.

표 *4:* 기본 라이선스/서브스크립션 만료의 영향

기본 라이선스	가능한 지원 서브스크립션	만료 영향
제어	TA, TAC, TAM, TAMC	기존 Firepower 기능을 계속 사용할 수 있지만, 애플리케이션 서명 업데이트를 포함해 VDB 업데이트를 다운로드할 수 없습니다.
보호	TA, TAC, TAM, TAMC	침입 검사는 계속 수행할 수 있지만, 침입 규칙 업데이트를 다운로드할 수 없습니다.

기본 라이선스	가능한 지원 서브스크립션	만료 영향
URL 필터링	URL, TAC, TAMC	• URL 조건이 포함된 액세스 제어 규칙은 즉시 URL 필터링을 중지합니다. • 카테고리 및 평판에 따라 트래픽을 필터링하는 다른 정책(예: SSL 정책)도 즉시 해당 작업을 중지합니다. • Firepower Management Center는 더 이상 업데이트를 URL 데이터로 다운로드할 수 없습니다. • URL 카테고리 및 평판 필터링을 수행하는 기존 정책을 다시 구축할 수 없습니다.
악성코드	AMP, TAM TAMC	• 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 시간 창이 만료된 후 시스템은 해당 파일에 `Unavailable`(사용 불가) 속성을 할당합니다. • 시스템이 AMP 클라우드 쿼리를 중지하며 AMP 클라우드에서 전송하는 회귀적 이벤트 확인을 중지합니다. • Firepower용 AMP 구성이 포함된 경우, 기존 액세스 제어 정책은 재적용할 수 없습니다.

서브스크립션 갱신

Q. 만료되는 기본 라이선스를 어떻게 갱신하나요?

A. 만료되는 기본 라이선스를 갱신하려면, 새 PAK 키를 구매하고 동일한 프로세스를 수행하여 새로운 스크립션을 구현하면 됩니다.

Q. Firepower Management Center에서 Firepower 서비스 서브스크립션을 갱신할 수 있나요?

A. 아닙니다. Firepower 서비스 서브스크립션(클래식 또는 스마트)을 갱신하려면 Cisco Commerce Workspace 또는 Cisco Service Contract Center 중 하나를 통해 새 서브스크립션을 구입해야 합니다.

이 가이드의 기타 라이선싱 정보

대상	확인
Smart Licensing authority와의 FMC 통신용 인터페이스에 대한 정보	디바이스 관리 인터페이스, 299 페이지 및 하위 항목

대상	확인
라이선싱 방화벽 요구사항	인터넷 액세스 요구 사항, 3108 페이지
이 문서 각 절차의 시작 부분에 있는 테이블에 설명된 라이선스 정보	문서 내 라이선스 설명, 19 페이지
백업 복원 시 중요한 라이선스 고려 사항	백업 및 복원, 203 페이지
규칙 및 정책 적용 및 트리거 방식에 대한 라이선스의 효과	다음을 포함하는 정책 및 규칙 정보 • 액세스 제어 규칙 관리, 1647 페이지 • 액세스 제어 규칙 구성 요소, 1648 페이지조건에 대한 정보 • TLS/SSL 규칙 지침 및 제한 사항, 1804 페이지 • TLS/SSL 규칙 구성 요소, 1776 페이지 • QoS 정책을 사용한 속도 제한, 881 페이지
라이선싱 관련 구축 및 정책 또는 규칙 관리 오류	다음을 포함해 이 가이드에 설명된 정책 및 규칙 정보 • 규칙 및 기타 정책 경고, 554 페이지 • QoS 정책을 사용한 속도 제한, 881 페이지
SSL 라이선싱 요구 사항	Firepower Threat Defense에 대한 SSL 설정 , 1431 페이지의 사전 요구 사항
SSL 프리프로세서 기능에 대한 라이선싱 요구 사항	SSL 전처리기, 2294 페이지
엔드포인트 통합 AMP에 대한 라이선싱	악성코드 방지 비교: Firepower 대 AMP for Endpoints, 1897 페이지
클라이언트 및 서비스 서버의 라이선싱 및 라이선스 및 스트림 리어셈블리	TCP 스트림 전처리 옵션, 2337 페이지
라이선싱 및 Cisco Threat Intelligence Director(TID)	플랫폼, 요소 및 라이선스 요구 사항, 1912 페이지
연결 이벤트에 대한 라이선싱 영향	연결 이벤트 필드 채우기 요구 사항, 2895 페이지
라이선싱 및 기타 대시보드 위젯에 대한 정보	사용자 역할별 대시보드 위젯 가용성, 365 페이지 맞춤형 분석 위젯, 369 페이지
라이선싱 상태 모니터에 대한 정보	스마트 라이선스 모니터 및 기본 라이선스 모니터에 대한 정보 상태 모듈, 389 페이지

Firepower 라이선싱 관련 추가 정보

일반 라이선싱 관련 질문 해결을 위한 자세한 내용은 다음 문서를 참조하시기 바랍니다.

- *Firepower* 라이선스 *FAQ(*자주 묻는 질문*)* 문서:

  https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html

- *Cisco Firepower System* 기능 라이선스 문서:

  https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

Cisco 지원 진단

Cisco Support Diagnostics는 사용자가 활성화하는 클라우드 기반 TAC 지원 서비스입니다. 이 서비스를 활성화하면 FMC(Firepower Management Center)와 FTD(Firepower Threat Defense), FMC(Firepower Management Center)와 Cisco Cloud 간의 보안 연결이 설정되어 시스템 상태 관련 정보를 스트리밍합니다.

Cisco Support Diagnostics는 TAC 사례 중에 Cisco TAC가 디바이스에서 필수 데이터를 안전하게 수집하게 하여, 문제 해결 중에 향상된 사용자 경험을 제공합니다. 또한 Cisco의 자동 문제 탐지 시스템을 이용해 운영 상태 데이터를 주기적으로 수집하고 처리하여, 문제가 발생하기 전에 미리 통보합니다. TAC 사례 중의 데이터 수집 서비스는 지원 계약을 한 모든 사용자가 이용할 수 있지만, 사전 알림 서비스는 특정 서비스 계약이 있는 사용자만 사용할 수 있습니다.

Cisco Support Diagnostics나 Cisco Success Network를 활성화하면, Firepower Management Center는 Firepower Management Center와 Cisco Cloud 간의 보안 연결을 항상 설정하고 유지 관리합니다. 언제든 Cisco Success Network와 Cisco Support Diagnostics를 모두 비활성화하면 이 연결을 끌 수 있으며, 이 경우 이상의 기능과 Cisco Cloud의 연결이 끊어집니다. 그러나 Cisco Support Diagnostics를 활성화하면, Firepower Threat Defense(FTD) 및 Cisco Cloud와 함께 FMC와 Cisco Cloud 간의 보안 연결이 설정 및 유지됩니다. 따라서 Cisco Support Diagnostics가 비활성화되면 두 보안 연결이 모두 해제됩니다.

관리자는 특정 시스템 기능에 대한 문제 해결 파일 생성, 473 페이지의 단계에 따라 FMC에서 수집하는 샘플 데이터 세트를 확인하여 문제 해결 파일을 열고, 파일을 열어 내용을 살펴볼 수 있습니다.

FMC는 수집된 데이터를 **System(**시스템**)** > **Integration(**통합**)** > **Cloud Services(**클라우드 서비스**)** 페이지에 지정된 지역 클라우드로 전송합니다. 이 설정은 Cisco Success Network에서 설명하는 Cisco Support Network와 다음을 이용한 이벤트 분석 Cisco SecureX Threat Response, 2749 페이지에서 설명하는 Cisco Threat Response 통합에도 사용합니다.

Cisco Support Diagnostics 활성화

Cisco Support Diagnostics는 Cisco Smart Software Manager를 이용해 Firepower Management Center를 등록할 때 활성화합니다. 참고, 스마트 라이선스 등록.

Licenses(라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 페이지에서 현재 Cisco Support Diagnostics 등록 정보를 확인하고, 등록 상태를 변경할 수 있습니다. 참고, Cisco 지원 진단 등록 변경, 177 페이지.

Cisco 지원 진단 등록 변경

Cisco Support Diagnostics는 Cisco Smart Software Manager를 이용해 Firepower Management Center를 등록할 때 활성화합니다. 그 후 다음 절차를 사용하여 등록 상태를 확인 또는 변경합니다.

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 클릭합니다.

단계 **2** Cisco Support Diagnostics 옆에 있는 Smart License Status(스마트 라이선스 상태)에서 **Enabled/Disabled(**활성화/비활성화**)** 제어를 클릭하고 설정을 적절하게 변경합니다.

참고 계속하기 전에 **Enabled/Disabled(**활성화/비활성화**)** 제어 옆에 있는 정보를 읽으십시오.

단계 **3** **Apply Changes(**변경 사항 적용**)**를 클릭합니다.

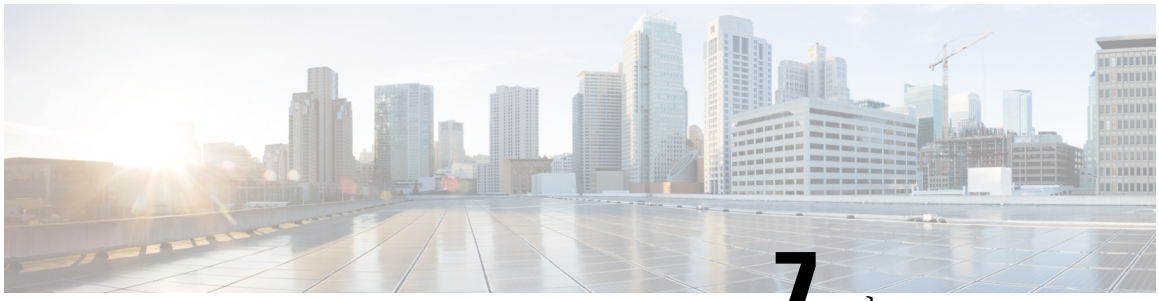
다음에 수행할 작업

Cisco Support Diagnostics를 활성화했다면, **System(**시스템**)** > **Integration(**통합**)** > **Cloud Services(**클라우드 서비스**)** > **Cisco Cloud Region(Cisco Cloud** 지역**)**에서 지역 클라우드 설정을 확인해 시스템 데이터 전송 위치를 설정합니다.

라이선싱 기록

기능	버전	세부 사항
고가용성 쌍의 FMCv(Virtual FMC)	6.7	FMC 고가용성 설정에 대한 라이선스 요구 사항, 282 페이지의 내용을 참조하십시오.
Firepower 4100/9300의 FTD에 대한 다중 인스턴스 기능 라이선스	6.3	이제 Firepower 4100/9300에서 다중 FTD 컨테이너 인스턴스를 구축할 수 있습니다. 보안 모듈/엔진별 기능당 하나의 라이선스만 필요합니다. 기본 라이선스가 각 인스턴스에 자동으로 할당됩니다. 신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 지원되는 플랫폼: Firepower 4100/9300에서의 FTD

기능	버전	세부 사항
에어 갭(Air-Gapped) 구축을 위한 특정 라이선스 예약	6.3	Cisco License Authority와 통신하기 위해 인터넷에 연결할 수 없는 고객은 특정 라이선스 예약을 사용할 수 있습니다. 자세한 내용은 SLR(Specific License Reservation)을 참조하십시오. 신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)** (이 옵션은 기본적으로 사용할 수 없습니다.) 지원되는 플랫폼: FMC, FTD
제한된 고객에 대한 내보내기 제어 기능	6.3	제한된 기능을 사용할 수 없는 스마트 어카운트를 보유한 특정 고객은 승인을 얻고 기간이 정해진 라이선스를 구매할 수 있습니다. 자세한 내용은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화을 참조하십시오. 지원되는 플랫폼: FMC, FTD
Firepower Threat Defense 디바이스 스마트 라이선싱 구축을 위한 고급 지침	6.3	새 항목이 엔드 투 엔드 지침: Firepower Threat Defense 디바이스 라이선스를 부여하는 방법를 제공합니다. 이 항목에서 링크된 항목에서 새롭게 개선된 정보를 확인할 수도 있습니다.
시스템 상태 정보를 Cisco Cloud로 스트리밍하도록 허용하는 Cisco Support Diagnostics	6.5	Cisco Support Diagnostics는 Firepower Management Center와 Firepower Threat Defense가 보안 연결을 통해 시스템 상태 관련 정보를 Cisco Cloud로 스트리밍할 수 있게 하는, 사용자가 활성화하는 기능입니다. 자세한 내용은 Cisco 지원 진단, 176 페이지을 참조해 주십시오. 신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 지원되는 플랫폼: FMC, FTD



7 장

시스템 업데이트

다음 항목에서는 Firepower 구축을 업데이트 하는 방법을 설명합니다.

- Firepower 업데이트 정보, 179 페이지
- 시스템 업데이트 요구 사항 및 사전 요건, 180 페이지
- Firepower 업데이트에 대한 가이드라인 및 제한 사항, 180 페이지
- Firepower System 소프트웨어 업그레이드, 181 페이지
- VDB 수동 업데이트, 182 페이지
- GeoDB(지리위치 데이터베이스) 업데이트, 183 페이지
- 침입 규칙 업데이트, 186 페이지
- 에어-갭(Air-Gapped) 구축 유지 관리, 196 페이지
- 시스템 업데이트 히스토리, 197 페이지

Firepower 업데이트 정보

Cisco에서는 Firepower 구축을 위해 몇 가지 유형의 업그레이드 및 업데이트를 배포합니다. 릴리스 노트 또는 권고 문구에 달리 설명되어 있지 않으면 업데이트를 수행해도 구성은 수정되지 않습니다. 주요 업그레이드를 설치 삭제할 수 없으며 VDB, GeoDB 또는 SRU의 이전 버전을 반환할 수도 없습니다.

표 ***5: Firepower*** 업그레이드 및 업데이트

업데이트 유형	설명	도메인
주요 업그레이드	새로운 기능이 포함되며 대규모의 제품 변경이 수반될 수 있습니다. 새로 설치 또는 복원은 할 수 있지만, 설치 삭제는 할 수 없습니다. 운영 체제를 별도로 업그레이드하는 디바이스의 경우, 컴패니언 운영 체제도 함께 업그레이드해야 할 가능성이 높습니다. EULA(최종 사용자 라이선스 계약)를 다시 수락해야 합니다.	전역만 해당

업데이트 유형	설명	도메인
마이너 업그레이드(패치)	제한된 범위의 수정 사항을 포함합니다. 설치 삭제는 할 수 있지만, 새로 설치 또는 복원은 할 수 없습니다. 주 버전으로 복원한 다음 부 버전으로 업그레이드해야 합니다.	전역만 해당
취약성 데이터베이스(VDM)	취약성, 운영 체제, 애플리케이션, 클라이언트 및 동적 분석에 사용할 수 있는 파일 유형을 탐지를 업데이트합니다.	전역만 해당
침입 규칙(SRU)	새로운 침입 규칙과 업데이트된 침입 규칙 및 프리프로세서 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 또한 규칙을 삭제하고, 새로운 규칙 카테고리와 기본 변수를 제공하며, 기본 변수 값을 변경할 수 있습니다.	Cisco 제공: 전역만 해당 로컬 가져오기: 모두
GeoDB(Geolocation database)	탐지된 IP 주소에 연결할 수 있는 물리적 위치, 연결 유형 등의 정보를 업데이트합니다. 지리위치 세부정보를 보거나 위치 기반 액세스 제어를 수행하려면 GeoDB를 설치해야 합니다.	전역만 해당

시스템 업데이트 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

글로벌 달리 명시되지 않은 경우

사용자 역할

관리자

Firepower 업데이트에 대한 가이드라인 및 제한 사항

업데이트 하기 전에

Firepower 구축 구성 요소(VDB, GeoDB, SRU 등)를 업데이트하기 전에, 업데이트에 포함된 릴리스 노트 또는 권고 문구를 반드시 읽어야 합니다. 호환성, 사전 요구 사항, 새로운 기능, 동작 변경, 경고 등 중요 및 릴리스 별 정보를 제공합니다.

Firepower Management Center 구축의 성공적인 시스템 소프트웨어 업그레이드를 준비 및 완료하는 방법에 대한 세부 사항은 Cisco Firepower Management Center 업그레이드 설명서를 참조합니다.

이 기능을 사용하여 구성된 업데이트는 UTC 기준으로 예약되며, 따라서 사용자의 위치와 날짜에 따라 작업이 지역적으로 실행됩니다. 또한 업데이트는 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받는다면, 예약된 업데이트는 현지 시간에 따라 여름에는 겨울보다 1시간 '후'에 실행됩니다

중요 예약된 업데이트가 의도한 시점에 수행되는지 확인하기를 적극 권장합니다.

대역폭 지침

업데이트를 하려면 대량의 데이터를 Firepower Management Center에서 매니지드 디바이스로 전송해야 합니다. 시작하기 전에 관리 네트워크에 전송을 수행 할 수 있는 충분한 대역폭이 있는지 확인하십시오. Troubleshooting Tech Note(문제 해결 기술 노트)를 참조하십시오(https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html).

Firepower System 소프트웨어 업그레이드

Firepower Management Center 구축 업그레이드는 복잡한 프로세스일 수 있습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다. 업그레이드 프로세스에서 업그레이드 스크립트를 호출하는 기계적 단계를 실제로 수행하는 것만큼 계획과 준비도 철저하게 고려해야 합니다.

초기 구성 중 FMC는 주간 작업을 예약하여 FMC 및 매지니드 디바이스의 최신 소프트웨어를 다운로드합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약이 실패하고 FMC가 인터넷에 액세스할 수 있다면 소프트웨어 다운로드 자동화, 258 페이지. 이 작업은 FMC에 소프트웨어 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.

이 프로세스의 첫 번째 단계는 구축을 평가하고 업그레이드 경로를 생성하는 것입니다. 이는 어떤 어플라이언스 및 구성 요소를 업그레이드할 것이며, 어떤 순서로 업그레이드할 것인 지에 대한 상세한 계획입니다. 업그레이드 경로의 기능은 다음과 같습니다.

- 관리자-디바이스 호환성 유지.
- 필요에 따라 운영 체제 및 호스팅 환경 업그레이드 포함.
- 다른 작업 포함. 백업, 패키지 다운로드, 대역폭 및 디스크 공간 검사, 업그레이드 전/후 구성 변경 등이 있습니다.
- 트래픽 흐름 및 검사에서 잠재적인 중단 식별.

Firepower Management Center 구축의 성공적인 업그레이드를 준비 및 완료하는 방법에 대한 세부 사항은 Cisco Firepower Management Center 업그레이드 설명서를 참조하십시오.

VDB 수동 업데이트

Cisco VDB(취약성 데이터베이스)는 호스트가 영향을 받기 쉬운 알려진 취약성의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. 시스템이 VDB를 사용하여 특정 호스트가 침해 위험을 높이는지 여부를 결정합니다.

Cisco는 VDB에 주기적인 업데이트를 제공합니다. Firepower Management Center에서 VDB 및 관련 매핑 업데이트에 걸리는 시간은 네트워크 맵에 있는 호스트 수에 따라 달라집니다. 호스트 수를 1000으로 나누면 업데이트 수행에 걸리는 대략적인 시간(분)이 나옵니다.

Firepower Management Center이 인터넷에 액세스할 수 없거나 VDB 업데이트를 Firepower Management Center에 수동으로 업로드하려는 경우, 이 절차를 사용합니다. VDB 업데이트를 자동화하려면 작업 일정 관리를 사용합니다(**System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**). 자세한 내용은 취약성 데이터베이스 업데이트 자동화, 260 페이지 섹션을 참조해 주십시오.

중요 자동 VDB 업데이트를 예약하지 않는 경우, 이러한 업데이트를 정기적으로 확인해야 합니다. 업데이트는 매일 단 1회 발생하며 https://www.cisco.com/go/firepower-software의 해당 하위 페이지에 게시됩니다.

주의 Firepower Management Center를 선택하여 VDB(취약성 데이터베이스) 업데이트 설치를 시작할 때 경고 메시지가 나타나는 경우, VDB를 설치한 후 구성을 구축해야 하며 구축 후 Snort 프로세스가 다시 시작됩니다. Firepower Threat Defense 디바이스에 대한 구축 보류에 대한 추가 경고가 구축 대화 상자에 나타납니다. 트래픽이 중단되는 동안 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오. Firepower Management Center에만 적용되는 VDB 업데이트 시 재시작되지 않으므로 구축할 수 없습니다.

시작하기 전에

- https://www.cisco.com/go/firepower-software에서 업데이트 다운로드.
- Snort 재시작으로 인해 업데이트가 트래픽 흐름 및 검사에 미치는 영향을 고려. 유지 보수 창에서 업데이트를 수행하는 것이 좋습니다.

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택한 후, **Product Updates(**제품 업데이트**)**를 클릭합니다.

단계 **2** VDB 업데이트를 Firepower Management Center로 업로드 하는 방법을 선택합니다.

- Cisco.com에서 직접 다운로드—**Download Updates(**업데이트 다운로드**)**를 클릭합니다. Cisco Support & Download 사이트에 액세스 하는 경우, Firepower Management Center가 최신 VDB를 다

운로드합니다. Firepower Management Center은 어플라이언스의 현재 버전에 연결된 각 패치 및 핫픽스(주 릴리스는 제외)에 대한 패키지도 다운로드합니다.

- 수동 업로드—**Upload Update(**업데이트 업로드**)**를 클릭한 후, **Choose File(**파일 선택**)**을 클릭합니다. 이전에 다운로드한 업데이트를 찾은 다음 **Upload(**업로드**)**를 클릭합니다.

VDB 업데이트가 Firepower 소프트웨어 업그레이드 및 설치 삭제 프로그램 패키지와 동일한 페이지에 나타납니다.

단계 **3** 업데이트를 설치합니다.

a) Vulnerability and Fingerprint Database update(취약성 및 지문 데이터베이스 업데이트) 옆에 있는 Install(설치)를 클릭합니다

b) Firepower Management Center을(를) 선택합니다.

c) **Install(**설치**)**을 클릭합니다.

단계 **4** (선택 사항) Message Center에서 업데이트 진행 상황을 모니터링합니다.

업데이트가 완료될 때까지 매핑된 취약성 관련 작업을 수행하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

업데이트가 완료되고 된 후, 시스템이 새 취약성 정보를 사용합니다. 그러나 구성을 구축해야 업데이트된 애플리케이션 탐지기 및 운영 체제 지문을 적용할 수 있습니다.

단계 **5** 업데이트 성공을 확인합니다.

Help(도움말**)** > **About(**정보**)**를 선택하고 VDB 현재 버전을 확인합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

구성 구축

GeoDB(지리위치 데이터베이스) 업데이트

Cisco GeoDB(Geolocation Database, 지리위치 데이터베이스)는 라우팅 가능한 IP 주소와 관련된 지리 데이터(국가, 도시, 좌표 등) 및 연결 관련 데이터(인터넷 서비스 공급자, 도메인 이름, 연결 유형 등)의 데이터베이스입니다. 시스템이 탐지된 IP 주소와 일치하는 GeoDB 정보를 탐지하면, 해당 IP 주소와 관련된 위치 정보 정보를 볼 수 있습니다. 국가 또는 대륙 이외의 모든 위치 정보 세부 정보를 보려면 시스템에 GeoDB를 설치해야 합니다. Cisco는 GeoDB에 주기적인 업데이트를 제공합니다.

초기 구성 중에 FMC는 주 단위로 자동 GeoDB 업데이트를 구성합니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, GeoDB 업데이트 예약, 185 페이지.

GeoDB를 업데이트하려면 Firepower Management Center의 Geolocation Updates(지리위치 업데이트) 페이지(**System(**시스템**)** > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**)를 사용하

십시오. Support(지원) 페이지 또는 어플라이언스에서 다운로드한, GeoDB 업데이트를 업로드하면 이 페이지에 나타납니다.

참고 수동으로 또는 Geolocation Updates(지리위치 업데이트) 페이지에서 **Download and install geolocation update from the Support Site(**지원 사이트에서 지리위치 업데이트 다운로드**)**를 클릭하여 지원 사이트에서 업데이트를 직접 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우, 손상될 수 있습니다.

GeoDB를 업데이트하는 데 필요한 시간은 어플라이언스에 따라 다릅니다. 일반적으로 설치하는 데 30~40분이 수요됩니다. GeoDB 업데이트를 수행해도 지리위치 정보의 지속적인 수집을 비롯한 기타 시스템 기능이 중단되지는 않지만, 업데이트를 완료하는 동안 시스템 리소스가 사용됩니다. 업데이트를 예약하는 경우 이를 고려하십시오.

GeoDB 업데이트는 GeoDB의 이전 버전을 무시하고 즉시 적용됩니다. GeoDB를 업데이트할 때, Firepower Management Center는 매니지드 디바이스 관련 데이터를 자동으로 업데이트합니다. GeoDB 업데이트가 구축 전반에 적용되려면 몇 분 정도 걸릴 수 있습니다. 업데이트 후 다시 구축할 필요가 없습니다.

GeoDB 수동 업데이트(인터넷 연결)

어플라이언스가 인터넷에 액세스 할 수 있는 경우에만 Support Site에 자동으로 연결하여 새 GeoDB 업데이트를 가져올 수 있습니다

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**을(를) 선택합니다.

단계 **2** **Geolocation Updates(**지리위치 업데이트**)**를 클릭합니다.

단계 **3** **Download and install geolocation update from the Support Site(**지원 사이트에서 지리위치 업데이트 다운로드 및 설치**)**를 선택합니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.
시스템에 Cisco 지원 사이트(http://www.cisco.com/cisco/web/support/index.html)에서 최신 업데이트를 확인하는 Geolocation Update(지리위치 업데이트) 작업에 대한 대기 행렬이 생성됩니다.

단계 **5** 필요한 경우 작업 상태를 모니터링합니다. 작업 메시지 보기, 445 페이지를 참조하십시오.

단계 **6** 업데이트 완료 후, Geolocation Updates(위치 정보 업데이트) 페이지로 돌아가거나 **Help(**도움말**)** > **About(**정보**)**를 선택하여 설치한 업데이트에 GeoDB 구축 번호가 일치하는지 확인합니다.

GeoDB 수동 업데이트(인터넷 연결 없음)

Firepower Management Center가 인터넷 액세스 권한이 없는 경우, Cisco 지원 사이트에 네트워크에 있는 로컬 컴퓨터에 GeoDB 업데이트를 다운로드한 후 수동으로 Firepower Management Center에 업로드합니다.

프로시저

단계 **1** Cisco 지원 사이트(http://www.cisco.com/cisco/web/support/index.html)에서 업데이트를 수동으로 다운로드합니다.

단계 **2** **System(**시스템**)** > **Updates(**업데이트**)**을(를) 선택합니다.

단계 **3** **Geolocation Updates(**지리위치 업데이트**)**를 클릭합니다.

단계 **4** **Upload and install geolocation update(**지리위치 업데이트 업로드 및 설치**)**를 선택합니다.

단계 **5** 다운로드한 업데이트를 찾은 다음 **Upload(**업로드**)**를 클릭합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

단계 **7** 필요한 경우 작업 상태를 모니터링합니다. 작업 메시지 보기, 445 페이지를 참조하십시오.

단계 **8** 업데이트 완료 후, Geolocation Updates(위치 정보 업데이트) 페이지로 돌아가거나 **Help(**도움말**)** > **About(**정보**)**를 선택하여 설치한 업데이트에 GeoDB 구축 번호가 일치하는지 확인합니다.

GeoDB 업데이트 예약

초기 구성 중에 FMC는 주 단위로 자동 GeoDB 업데이트를 구성합니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, 이 주제.

시작하기 전에

FMC이 인터넷에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택한 후, **Geolocation Updates(**지리위치 업데이트**)**를 클릭합니다.

단계 **2** **Recurring Geolocation Updates(**반복되는 지리위치 업데이트**)**에서 **Enable Recurring Weekly Updates(**반복되는 주간 업데이트 활성화**)**를 체크합니다.

단계 **3** **Update Start Time(**업데이트 시작 시간**)**을 지정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

침입 규칙 업데이트

새로운 취약성이 알려지면 Cisco Talos Intelligence Group(Talos)은 가져올 수 있는 침입 규칙 업데이트를 Firepower Management Center로 릴리스하고, 그런 다음 변경된 구성을 매니지드 디바이스에 구축하여 구현합니다. 이러한 업데이트는 침입 규칙, 전처리기 규칙 및 규칙을 사용하는 정책에 영향을 줍니다.

규칙 업데이트는 누적되며, Cisco에서는 항상 최신 업데이트를 가져올 것을 권장합니다. 현재 설치된 규칙의 버전과 일치하거나 이전의 침입 규칙 업데이트는 가져올 수 없습니다.

침입 규칙 업데이트는 다음을 제공할 수 있습니다.

- 신규 및 수정된 규칙 및 규칙 상태 — 규칙 업데이트는 신규 및 업데이트된 침입 규칙과 전처리기 규칙을 제공합니다. 새 규칙의 경우, 규칙 상태는 각 시스템이 제공하는 침입 정책에서 다를 수 있습니다. 예를 들어, 새 규칙은 Security Over Connectivity(연결성에 우선하는 보안) 침입 정책에서 활성화되며 Connectivity Over Security(보안에 우선하는 연결성) 침입 정책에서는 비활성화됩니다. 규칙 업데이트는 기존 규칙의 기본 상태를 변경하거나, 기존 규칙을 완전히 삭제할 수 있습니다.
- 새 규칙 카테고리 — 규칙 업데이트에는 새 규칙 카테고리가 포함될 수 있는데, 이는 항상 추가됩니다.
- 수정된 프리프로세서 및 고급 설정 — 규칙 업데이트는 시스템이 제공한 침입 정책에 있는 고급 설정 및 시스템이 제공한 네트워크 분석 정책에 있는 전처리기 설정을 변경할 수 있습니다. 이들은 또한 액세스 제어 정책의 고급 전처리 및 성능 옵션에 대한 기본값을 업데이트할 수 있습니다.
- 신규 및 수정된 변수 — 규칙 업데이트는 기존의 기본 변수에 대한 기본값을 변경할 수 있지만, 변경 사항을 재정의하지 않습니다. 새로운 변수는 항상 추가됩니다.

다중 도메인 구축에서는 로컬 침입 규칙을 모든 도메인에 가져올 수 있지만 Talos의 침입 규칙 업데이트는 전역 도메인에만 가져올 수 있습니다.

침입 규칙 업데이트가 정책을 수정하는 시점에 대한 이해

침입 규칙 업데이트는 모든 액세스 제어 정책뿐만 아니라 시스템이 제공한 네트워크 분석 정책 및 사용자 지정 네트워크 분석 정책 모두에도 영향을 미칠 수 있습니다.

- 시스템제공—시스템이 제공한 네트워크 분석 및 침입 정책에 대한 변경 사항뿐만 아니라 고급 액세스 제어 설정에 대한 모든 변경 사항은 업데이트한 후 정책을 다시 구축할 때 자동으로 적용됩니다.
- 사용자 지정 — 각 사용자 지정 네트워크 분석 및 침입 정책은 시스템이 제공한 정책을 자체 기반으로, 또는 정책 체인의 궁극적인 기반으로 사용하므로 규칙 업데이트는 사용자 지정 네트워크 분석 및 침입 정책에 영향을 미칠 수 있습니다. 하지만, 규칙 업데이트가 자동으로 해당 변경 사항을 적용하는 것을 방지할 수 있습니다. 이를 통해 규칙 업데이트를 가져오는 것과 별개로 시스템 제공 기본 정책을 수동으로 업데이트할 수 있습니다. (사용자 지정 정책별 기반으로 실행되는) 선택 사항과 관계없이, 시스템이 제공한 정책에 대한 업데이트는 사용자 지정한 어떤 설정도 재지정하지 않습니다.

규칙 업데이트를 가져오면 네트워크 분석 및 침입 정책에 캐시된 변경 사항이 모두 제거된다는 점에 유의하십시오. 사용자의 편의를 위해, Rule Updates(규칙 업데이트) 페이지는 캐시된 변경 사항이 있는 정책및 변경한 사용자을 나열합니다.

침입 규칙 업데이트 구축

침입 규칙 업데이트를 통해 수행된 변경 사항을 적용하려면 구성을 재구축해야 합니다. 규칙 업데이트를 가져올 때 영향을 받는 디바이스에 자동으로 재구축하도록 시스템을 구성할 수 있습니다. 이 접근법은 침입 규칙 업데이트가 시스템이 제공하는 기본 침입 정책을 수정할 수 있는 경우에 특히 유용합니다.

반복 침입 규칙 업데이트

Rule Updates(규칙 업데이트) 페이지를 사용하여 일 단위, 주 단위 또는 월 단위로 규칙 업데이트를 가져올 수 있습니다.

침입 규칙 업데이트 가져오기에서 적용 가능한 하위 태스크는 다운로드, 설치, 기본 정책 업데이트 및 구성 구축 순서로 수행됩니다. 1개의 하위 태스크가 완료되면, 다음 하위 태스크가 시작됩니다.

시스템은 이전 단계에서 지정한 대로 예약된 시간에 규칙 업데이트를 설치하고 변경된 구성을 구축합니다. 가져오기 작업 중 또는 작업 이전에 로그 오프하거나 웹 인터페이스를 사용하여 다른 작업을 수행할 수 있습니다. 가져오기 작업 중에 액세스된 경우, Rule Update Log(규칙 업데이트 로그)는 빨간색 상태( )를 표시하며, Rule Update Log(규칙 업데이트 로그) 상세 보기에서 메시지가 나타나면 이를 확인할 수 있습니다. 규칙 업데이트 크기 및 콘텐츠에 따라, 몇 분이 지난 후에 상태 메시지가 표시될 수 있습니다.

초기 구성 중에 버전 FMC는 Cisco 지원 사이트에서 매일 자동 침입 규칙 업데이트를 구성합니다. (FMC는 다음에 영향을 받는 정책을 구축하는 경우 영향을 받는 관리되는 디바이스에 자동으로 침입 규칙 업데이트를 구축합니다.) 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, 반복 되는 침입 규칙 업데이트 구성, 189 페이지.

로컬 침입 규칙 가져오기

로컬 침입 규칙은 로컬 컴퓨터에 ASCII 또는 UTF-8로 인코딩한 일반 텍스트 파일로 가져오는 맞춤형 표준 텍스트 규칙입니다. Snort 사용자 설명서의 지침을 사용하여 로컬 규칙을 생성할 수 있습니다. 지침은 http://www.snort.org에서 다운로드할 수 있습니다.

다중 도메인 구축에서 로컬 침입 규칙을 모든 도메인으로 가져올 수 있습니다. 현재 도메인 및 상위 도메인에서 가져온 로컬 침입 규칙을 볼 수 있습니다.

침입 규칙 일회성 수동 업데이트

Firepower Management Center이 인터넷 액세스할 수 없는 경우, 새로운 침입 규칙 업데이트를 수동으로 가져옵니다.

프로시저

단계 **1** Cisco 지원 사이트(http://www.cisco.com/cisco/web/support/index.html)에서 업데이트를 수동으로 다운로드합니다.

단계 **2** **System(**시스템**)** > **Updates(**업데이트**)**를 선택한 후, **Rule Updates(**규칙 업데이트**)** 탭을 클릭합니다.

단계 **3** 사용자가 생성했거나 가져온 사용자 정의 규칙을 삭제된 폴더로 옮기려는 경우, 툴바에 있는 **Delete All Local Rules(**모든 로컬 규칙 삭제**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** **Rule Update or text rule file to upload and install(**규칙 업데이트 또는 업로드 및 설치할 텍스트 규칙 파일**)**을 선택하고 **Browse(**검색**)**를 클릭하여 규칙 업데이트 파일을 탐색하고 선택합니다.

단계 **5** 업데이트가 완료된 후 매니지드 디바이스에 정책을 자동으로 다시 구축하려는 경우, **Reapply all policies after the rule update import completes(**규칙 업데이트 가져오기가 완료된 후 모든 정책 재적용**)**을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다. 시스템에 규칙 업데이트가 설치되고 Rule Update Log(규칙 업데이트 로그) 상세 보기가 표시됩니다.

참고 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 Support(지원팀)에 문의하십시오.

침입 규칙 일회성 자동 업데이트

새 침입 규칙 업데이트를 자동으로 가져오려면 어플라이언스가 인터넷에 액세스해야 지원 사이트에 연결할 수 있습니다.

시작하기 전에

- Firepower Management Center에서 인터넷에 액세스할 수 있는지 확인합니다. 보안, 인터넷 액세스 및 통신 포트, 3107 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

팁 **Policies(**정책**)** > **Intrusion(**침입**)** > **Intrusion Rules(**침입 규칙**)**를 선택하여 액세스하는 Rule Editor(규칙 편집기) 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다.

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** 사용자가 생성했거나 가져온 사용자 정의 규칙을 삭제된 폴더로 옮기려는 경우, 툴바에 있는 **Delete All Local Rules(**모든 로컬 규칙 삭제**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** **Download new Rule Update from the Support Site(**지원 사이트에서 새로운 규칙 업데이트 다운로드**)**를 선택합니다.

단계 **5** 업데이트가 완료된 후 매니지드 디바이스에 변경된 구성을 자동으로 다시 구축하려는 경우, **Reapply all policies after the rule update import completes(**규칙 업데이트 가져오기가 완료된 후 모든 정책 재적용**)** 확인란을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.
시스템에 규칙 업데이트가 설치되고 Rule Update Log(규칙 업데이트 로그) 상세 보기가 표시됩니다.

주의 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 Support(지원팀)에 문의하십시오.

반복 되는 침입 규칙 업데이트 구성

초기 구성 중에 버전 FMC는 Cisco 지원 사이트에서 매일 자동 침입 규칙 업데이트를 구성합니다. (FMC는 다음에 영향을 받는 정책을 구축하는 경우 영향을 받는 관리되는 디바이스에 자동으로 침입 규칙 업데이트를 구축합니다.) 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, 이 섹션.

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

팁 **Policies(**정책**)** > **Intrusion(**침입**)** > **Intrusion Rules(**침입 규칙**)**를 선택하여 액세스하는 Rule Editor(규칙 편집기) 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다.

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** 사용자가 생성했거나 가져온 사용자 정의 규칙을 삭제된 폴더로 옮기려는 경우, 툴바에 있는 **Delete All Local Rules(**모든 로컬 규칙 삭제**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** **Enable Recurring Rule Update Imports from the Support Site(**지원 사이트에서 반복 규칙 업데이트 가져오기 활성화**)** 확인란을 선택합니다.

Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기**)** 섹션 제목 아래에 가져오기 상태 메시지가 나타납니다.

단계 **5** **Import Frequency(**가져오기 빈도**)** 필드에서 다음을 지정합니다.

- 업데이트 빈도(**Daily(**매일**)**, **Weekly(**매주**)**, or **Monthly(**매월**)**)
- 업데이트를 수행할 주나 월의 날짜
- 업데이트를 시작하려는 시간

단계 **6** 업데이트가 완료된 후 매니지드 디바이스에 변경된 구성을 자동으로 다시 구축하려는 경우, **Deploy updated policies to targeted devices after rule update completes(**규칙 업데이트 완료 후 업데이트된 정책을 대상 디바이스에 구축**)** 확인란을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

주의 침입 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 지원팀에 문의하십시오.

Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기) 섹션 제목 아래의 상태 메시지가 변경되어 규칙 업데이트가 아직 실행되지 않았음을 나타냅니다.

로컬 침입 규칙 가져오기 모범 사례

로컬 규칙 파일을 가져올 때 다음 지침을 따르십시오.

- 규칙 가져오기 도구를 사용하려면 모든 맞춤형 규칙을 ASCII 또는 UTF-8로 인코딩된 일반 텍스트로 가져와야 합니다.
- 텍스트 파일 이름은 영숫자 및 공백을 포함할 수 있지만 밑줄(_), 마침표(.) 및 대시(-)를 제외한 특수 문자는 포함할 수 없습니다.
- 시스템이 단일 파운드 문자(#)로 시작되는 로컬 규칙을 가져오지만, 삭제된 것으로 플래그 표시됩니다.
- 시스템이 단일 파운드 문자(#)로 시작하는 로컬 규칙을 가져오지만, 파운드 문자 2개(##)로 시작하는 로컬 규칙은 가져오지 않습니다.
- 규칙은 확장 문자를 사용할 수 없습니다.
- 다중 도메인 구축에서 시스템은 전역 도메인으로 가져오거나 생성된 규칙에 GID 1을 할당하고 다른 모든 도메인에서는 도메인 별 GID를 1000과 2000 사이로 할당합니다.
- 로컬 규칙을 가져올 때 GID(Generator ID)를 지정할 필요가 없습니다. 이렇게 하면 표준 텍스트 규칙에 GID 1만 지정됩니다.
- 처음으로 규칙을 가져오는 경우, Snort ID (SID) 또는 개정 번호를 지정하지 마십시오. 이렇게 하면 삭제된 규칙을 포함해 다른 규칙의 SID와 충돌을 피할 수 있습니다. 시스템은 해당 규칙에 다음으로 사용 가능한 1000000 이상의 사용자 지정 규칙 SID와 수정 번호 1을 자동으로 할당합니다.

  SID가 있는 규칙을 가져와야 하는 경우, SID는 1,000,000 이상의 고유 숫자가 될 수 있습니다.

  다중 도메인 구축에서 여러 관리자가 동시에 로컬 규칙을 가져오는 경우, 시스템이 시퀀스의 중간 숫자를 다른 도메인에 할당했기 때문에 개별 도메인 내의 SID가 비순차적으로 보일 수 있습니다.
- 이전에 가져온 로컬 규칙의 업데이트된 버전을 가져올 경우 또는 삭제한 로컬 규칙을 되돌리는 경우, 반드시 시스템이 할당한 SID와 현재 개정 번호보다 큰 개정 번호를 포함해야 합니다. 규칙을 편집하여 현재 또는 삭제된 규칙의 개정 번호를 결정할 수 있습니다.

  참고 로컬 규칙을 삭제하면 자동으로 개정 번호가 증가합니다. 이 디바이스를 통해 로컬 규칙을 복원할 수 있습니다. 삭제된 모든 로컬 규칙은 로컬 규칙 카테고리에서 삭제된 규칙 카테고리로 이동합니다.
- 규칙에 다음 중 하나가 포함되는 경우 가져오기가 실패합니다.

- 2147483647 보다 큰 SID.
- 64자를 초과하는 소스 또는 대상 포트의 목록.
- 다중 도메인 구축에서 전역 도메인으로 가져오는 경우, GID:SID 조합은 GID 1과 이미 다른 도메인에 있는 SID를 사용합니다. 이는 해당 조합이 버전 6.2.1 이전에 존재했음을 나타냅니다. GID 1과 고유한 SID를 사용하여 규칙을 다시 가져올 수 있습니다.

- 더 이상 사용되지 않는 `threshold` 키워드를 침입 정책의 침입 이벤트 임계값 설정 기능과 조합하여 사용하는, 가져온 로컬 규칙을 활성화하는 경우 정책 인증이 실패합니다.
- 가져온 모든 로컬 규칙은 로컬 규칙 카테고리에 자동으로 저장됩니다.
- 시스템은 사용자가 가져오는 로컬 규칙을 항상 비활성화된 규칙 상태로 설정합니다. 로컬 규칙을 침입 정책에서 사용하기 전에 상태를 수동으로 설정해야 합니다.

로컬 침입 규칙 가져오기

- 로컬 규칙 파일이 로컬 침입 규칙 가져오기 모범 사례, 190 페이지에 설명된 지침을 따르는지 확인합니다.
- 로컬 침입 규칙을 가져오는 프로세스가 보안 정책을 준수하는지 확인합니다.
- 대역폭 제한 및 Snort 재시작으로 인해 가져오기가 트래픽 흐름 및 검사에 미치는 영향을 고려합니다. 유지 보수 기간 중 규칙 업데이트를 예약하는 것이 좋습니다.
- 모든 도메인에서 이 작업을 수행할 수 있습니다.

이 절차를 사용하여 로컬 침입 규칙을 가져옵니다. 가져온 침입 규칙이 로컬 규칙 카테고리에 비활성화된 상태로 나타납니다.

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택한 후, **Rule Updates(**규칙 업데이트**)** 탭을 클릭합니다.

단계 **2** (선택 사항) 기존 로컬 규칙을 삭제합니다.

Delete All Local Rules(모든 로컬 규칙 삭제**)**를 클릭한 후, 생성했거나 가져온 모든 침입 규칙을 삭제된 폴더로 옮기는지 확인합니다.

단계 **3** **One-Time Rule Update/Rules Import(**일회성 규칙 업데이트/규칙 가져오기**)** 아래에서 **Rule update or text rule file to upload and install(**업로드 및 설치할 규칙 업데이트 또는 텍스트 규칙 파일**)**을 선택한 다음 **Choose File(**파일 선택**)**을 클릭하여 로컬 규칙 파일을 찾습니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

단계 **5** Message Center의 가져오기 진행 상황을 모니터링합니다.

Message Center를 표시하려면, 메뉴 바에서 System Status(시스템 상태)를 클릭합니다. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 가져오기가 실패했다고 나타나더라도 가져오기를 재시작하지 마십시오. 대신 Cisco TAC에 문의하십시오.

다음에 수행할 작업

- 침입 정책을 수정하고 가져온 규칙을 활성화합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

규칙 업데이트 로그

Firepower Management Center은 사용자가 가져오는 각 규칙 업데이트 및 로컬 규칙 파일에 대한 레코드를 생성합니다.

각 레코드에는 파일을 가져온 사용자의 타임 스탬프, 이름 및 가져오기가 성공 또는 실패되었음을 나타내는 상태 아이콘이 포함됩니다. 가져온 모든 규칙 업데이트 및 로컬 파일 규칙의 목록을 유지할 수 있고, 목록에서 가져온 모든 레코드를 삭제할 수 있으며, 가져온 모든 규칙 및 규칙 업데이트 구성 요소에 대한 세부 레코드에 액세스할 수 있습니다.

Rule Update Import Log(규칙 업데이트 가져오기 로그) 상세 보기에서는 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 개체에 대한 세부 레코드가 나열됩니다. 특정 요건에 일치하는 정보만 포함하는 나열된 레코드로부터 사용자 지정 워크플로 또는 보고서를 생성할 수도 있습니다.

침입 규칙 업데이트 로그 테이블

표 ***6:*** 침입 규칙 업데이트 로그 필드

필드	설명
요약	가져오기 파일의 이름입니다. 가져오기가 실패한 경우, 실패 이유에 대한 간략한 설명이 파일 이름 아래에 나타납니다.
Time(시간)	가져오기가 시작된 날짜 및 시간입니다.
User ID(사용자 ID)	가져오기를 시작한 사용자의 사용자 이름입니다.
상태	가져오기 여부: • 성공함( ) • 실패 또는 현재 진행 중 빨간색 상태( ) 가져오기 작업 진행 중에는 실패했거나 완료되지 않은 가져오기를 나타내는 빨간색 상태 아이콘이 Rule Update Log(규칙 업데이트 로그) 페이지에 나타나고 가져오기가 성공적으로 완료된 경우에만 이 아이콘이 녹색으로 바뀝니다.

팁 침입 규칙 업데이트 가져오기가 진행되는 동안 나타나는 가져오기 세부사항을 볼 수 있습니다.

침입 규칙 업데이트 로그 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

팁 침입 규칙 편집기 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다 (**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**).

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** **Rule Update Log(**규칙 업데이트 로그**)**를 클릭합니다.

단계 **4** 다음 2가지 옵션을 사용할 수 있습니다.

- View(보기) - 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 개체에 대한 세부 사항을 보려면 확인하려는 파일 옆에 있는 보기 ( )를 클릭합니다. 침입 규칙 업데이트 가져오기 로그 세부 정보 보기, 195 페이지의 내용을 참조하십시오.
- Delete(삭제) - 파일에 포함된 모든 개체에 대한 세부 레코드를 포함하여 가져오기 파일 레코드를 가져오기 로그에서 삭제하려면 가져오기 파일 이름 옆에 있는 삭제( )를 클릭합니다.

  참고 로그에서 파일을 삭제해도 가져오기 파일에서 가져온 모든 개체를 삭제하는 것은 아니며, 가져오기 로그 레코드만 삭제합니다.

침입 규칙의 필드에 로그를 업데이트합니다.

팁 단일 가져오기 파일에 대한 레코드만 표시된 Rule Update Import Log(규칙 업데이트 가져오기 로그) 상세 보기의 툴바에서 **Search(**검색**)**를 클릭하여 검색을 시작하는 경우에도 Rule Update Import Log(규칙 업데이트 가져오기 로그) 데이터베이스 전체를 검색합니다. 검색에 포함할 모든 개체를 포함하도록 시간 제약 조건을 설정해야 합니다.

침입 규칙의 필드에 로그를 업데이트합니다.

표 *7:* 규칙 업데이트 가져오기 로그 상세 보기 필드

필드	설명
Action(조치)	다음 중 하나가 개체 유형에 발생했음을 나타냅니다. • new(신규) (해당 규칙이 어플라이언스에 처음 저장된 경우) • changed(변경됨)(규칙 업데이트 구성 요소 또는 규칙의 경우, 규칙 업데이트 구성 요소가 변경되었거나 규칙이 더 높은 수정 번호 및 동일한 GID 및 SID를 지닙니다.) • collision(충돌) (규칙 업데이트 구성 요소 또는 규칙의 경우, 해당 수정 버전이 기존 구성 요소 또는 규칙과 충돌하여 가져오기를 건너뛰었습니다.) • deleted(탐지됨)(규칙의 경우, 규칙이 규칙 업데이트에서 삭제되었습니다.) • enabled(활성화됨)(규칙 업데이트 수정에서 전처리기, 규칙 또는 다른 기능이 시스템 제공 기본 정책에서 활성화되었습니다.) • disabled(비활성화됨) (규칙의 경우, 시스템 제공 기본 정책에서 규칙이 비활성화되었습니다.) • drop(삭제)(규칙의 경우, 시스템 제공 기본 정책에서 규칙이 Drop and Generate Events(삭제 후 이벤트 생성)로 설정되었습니다.) • error(오류)(규칙 업데이트 또는 로컬 규칙 파일의 경우, 가져오기가 실패했습니다.) • apply(적용)(해당 가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes(**규칙 업데이트 가져오기가 완료된 후 침입 정책 다시 적용**)** 옵션이 활성화되었습니다.)
기본 작업	규칙 업데이트에 의해 정의된 기본 작업. 가져온 개체 유형이 rule(규칙)인 경우, 기본 작업은 Pass(통과), Alert(경고) 또는 Drop(삭제)입니다. 다른 모든 가져온 개체 유형의 경우, 기본 작업이 없습니다.
세부 사항	구성 요소 또는 규칙에 고유한 문자열. 규칙의 경우, 변경된 규칙의 GID, SID 및 이전 수정 번호이며, previously (GID:SID:Rev)(이전(GID:SID:Rev))로 표시됩니다. 변경되지 않은 규칙의 경우 이 필드는 비어 있습니다.
도메인	침입 정책이 업데이트된 규칙을 사용할 수 있는 도메인. 하위 도메인의 침입 정책도 규칙을 사용할 수 있습니다. 이 필드는 다중 도메인 구축에서만 나타납니다.
GID	규칙에 대한 생성기 ID. 예를 들어, 1 (표준 텍스트 규칙, 전역 도메인 또는 레거시 GID) 또는 3 (공유 개체 규칙).
이름	규칙 Message(메시지) 필드에 해당하는 규칙 및 규칙 업데이트 구성 요소에 대해 가져온 개체의 이름이 구성 요소 이름입니다.
정책	가져온 규칙의 경우, 이 필드는 All(모두)로 표시됩니다. 이는 해당 규칙 가져오기가 성공하였고 모든 적절한 기본 침입 정책에서 활성화될 수 있다는 의미입니다. 가져온 개체의 다른 유형의 경우, 이 필드는 비어 있습니다.
Rev	규칙의 수정 번호.
규칙 업데이트	규칙 업데이트 파일 이름.

필드	설명
SID	규칙의 SID.
시간	가져오기가 시작된 날짜 및 시간입니다.
유형	가져온 개체 유형. 다음 중 하나일 수 있습니다. • `rule update component(규칙 업데이트 구성 요소)`(규칙 팩 또는 정책 팩과 같은 가져온 구성 요소) • `rule(규칙)`(규칙의 경우, 신규 또는 업데이트된 규칙입니다. 버전 5.0.1에서 이 값이 더 이상 사용되지 않는 `update(업데이트)` 값을 대체했다는 점에 유의하십시오.) • `policy apply(정책 적용)`(해당 가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes(**규칙 업데이트 가져오기가 완료된 후 침입 정책 다시 적용**)** 옵션이 활성화되었습니다.)
개수	각 레코드의 개수(1). 표를 제한할 때 표 보기에 Count(개수) 필드가 나타나며, Rule Update Log(규칙 업데이트 로그) 상세 보기는 기본적으로 규칙 업데이트 레코드에 제한됩니다. 이 필드는 검색할 수 없습니다.

침입 규칙 업데이트 가져오기 로그 세부 정보 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

팁 **Policies(**정책**)** > **Intrusion(**침입**)** > **Intrusion Rules(**침입 규칙**)**를 선택하여 액세스하는 Rule Editor(규칙 편집기) 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다.

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** **Rule Update Log(**규칙 업데이트 로그**)**를 클릭합니다.

단계 **4** 보려는 상세 레코드의 파일 옆에 있는 보기 ( )를 클릭합니다.

단계 **5** 다음 작업을 수행할 수 있습니다.

- Bookmark(즐겨찾기) — 현재 페이지를 즐겨찾기 하려면 **Bookmark This Page(**이 페이지 즐겨찾기에 등록**)**를 클릭합니다.
- Edit Search(검색 편집) — 현재 단일 제약조건이 미리 입력된 검색 페이지를 열려면 Search Constraints(검색 제약조건) 옆에 있는 **Edit Search(**검색 편집**)** 또는 **Save Search(**검색 저장**)**를 선택합니다.
- Manage bookmarks(즐겨찾기 관리) — 즐겨찾기 관리 페이지로 이동하려면 **Report Designer(**리포트 디자이너**)**를 클릭합니다.

- Report(보고서) — 현재 보기의 데이터를 기반으로 보고서를 생성하려면 **Report Designer(**리포트 디자이너**)**를 클릭합니다.
- Search(검색) — 규칙 업데이트 가져오기 로그 데이터베이스 전체에서 규칙 업데이트 가져오기 레코드를 검색하려면 **Search(**검색**)**를 클릭합니다.
- Sort(정렬) — 현재 워크플로 페이지에서 레코드를 정렬하고 유지하려면 자세한 내용은 드릴다운 페이지 사용, 2801 페이지을 참조하십시오.
- Switch workflows(워크플로 전환) — 일시적으로 다른 워크플로를 사용하려면 **(**워크플로 전환**)**을 클릭합니다.

에어-갭(Air-Gapped) 구축 유지 관리

Firepower system이 인터넷에 연결되어 있지 않으면, 필수 업데이트가 자동으로 발생하지 않습니다. 이러한 업데이트를 수동으로 가져오고 설치해야 합니다. 다음 정보를 참조하십시오.

- VDB 수동 업데이트, 182 페이지
- 침입 규칙 일회성 수동 업데이트, 187 페이지
- GeoDB 수동 업데이트(인터넷 연결 없음), 185 페이지
- *Firepower Management Center* 소프트웨어 업데이트 가이드

  https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html

시스템 업데이트 히스토리

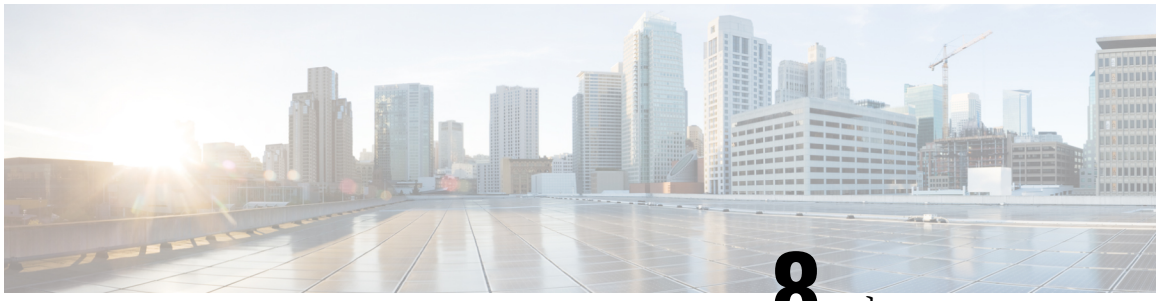
기능	버전	세부정보
FTD 업그레이드 상태 보고 및 취소/재시도 옵션 개선	6.7.0	

기능	버전	세부정보
		이제 디바이스 관리 페이지에서 진행 중인 FTD 디바이스 업그레이드 및 준비 확인 상태와 7일 간의 업그레이드 성공/실패 기록을 볼 수 있습니다. 메시지 센터는 향상된 상태 및 오류 메시지도 제공합니다. 클릭 한 번으로 디바이스 관리 및 메시지 센터에서 액세스할 수 있는 새로운 Upgrade Status(업그레이드 상태) 팝업에 남은 비율/시간, 특정 업그레이드 단계, 성공/실패 데이터, 업그레이드 로그 등의 자세한 업그레이드 정보가 표시됩니다. 또한 이 팝업에서 실패 또는 진행 중인 업그레이드를 수동으로 취소하거나(**Cancel Upgrade(**업그레이드 취소**)**) 실패한 업그레이드를 재시도 할 수 있습니다(**Retry Upgrade(**업그레이드 재시도**)**). 업그레이드를 취소하면 디바이스가 업그레이드 전 상태로 돌아갑니다. 참고 수동으로 취소하거나 실패한 업그레이드를 재시도하려면 FMC를 사용하여 FTD 디바이스를 업그레이드 할 때 나타나는 새로운 자동 취소 옵션을 비활성화해야합니다. **Automatically cancel on upgrade failure and roll back to the previous version(**업그레이드 실패시 자동으로 취소하고 이전 버전으로 롤백합니다**)**. 이 옵션을 활성화하면 업그레이드 실패시 디바이스가 자동으로 업그레이드 전 상태로 돌아갑니다. 패치에 대해서는 자동 취소가 지원되지 않습니다. HA 또는 클러스터형 구축에서는 자동 취소가 각 디바이스에 개별적으로 적용됩니다. 즉, 한 디바이스에서 업그레이드에 실패하면 해당 디바이스만 복귀됩니다. 신규/수정된 화면: • FTD 업그레이드 패키지의 **System(**시스템**)** > **Update(**업데이트**)** > **Product Updates(**제품 업데이트**)** > **Available Updates(**사용 가능한 업데이트**)** > **Install(**설치**)** 아이콘 • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Upgrade(**업그레이드**)** • **Message Center(**메시지 센터**)** > **Tasks(**작업**)** 새로운 FTD CLI 명령: • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry**

기능	버전	세부정보
업그레이드는 디스크 공간을 절약하기 위해 PCAP 파일 제거	6.7.0	Firepower 어플라이언스를 업그레이드하려면 사용 가능한 디스크 공간이 충분해야 합니다. 그렇지 않으면 업그레이드에 실패합니다. 업그레이드 시 이제 로컬에 저장된 PCAP 파일이 제거됩니다.
사용자 정의 침입 규칙 가져오기에서 규칙 충돌 경고	6.7.0	FMC에서는 이제 사용자 정의(로컬) 침입 규칙을 가져올 때 규칙 충돌을 경고합니다. 이전에는 충돌이 발생한 규칙 가져오기가 완전히 실패하는 버전 6.6.0.1을 제외하고 시스템은 충돌을 일으키는 규칙을 자동으로 건너 뛰었습니다. Rule Updates(규칙 업데이트) 페이지에서 규칙 가져오기에 충돌이 발생한 경우 Status(상태) 열에 경고 아이콘이 표시됩니다. 자세한 내용을 보려면 경고 아이콘 위에 포인터를 올려 놓고 툴팁을 확인하십시오. 기존 규칙과 동일한 SID/수정 번호를 가진 침입 규칙을 가져오려고 할 때 충돌이 발생합니다. 항상 업데이트된 버전의 사용자 정의 규칙에 새 수정 번호가 포함되어 있는지 확인해야 합니다. 자세한 모범 사례는 로컬 침입 규칙 가져오기 모범 사례, 190 페이지의 내용을 참조하십시오. 신규/수정 화면: 시스템 > 업데이트 > 규칙 업데이트에 경고 아이콘이 추가되었습니다
내부 웹 서버에서 FTD 업그레이드 패키지 가져오기	6.6.0	이제 FTD 디바이스가 FMC가 아닌 자체 내부 웹 서버에서 업그레이드 패키지를 가져올 수 있습니다. 이 옵션은 FMC와 디바이스 간의 대역폭이 제한되어 있는 경우 특히 유용합니다. 또한 FMC의 공간을 절약합니다. 참고 이 기능은 버전 6.6.0 이상을 실행하는 FTD 디바이스에서만 지원됩니다. 버전 6.6.0으로의 업그레이드에는 지원되지 않으며, FMC 또는 클래식 디바이스에서는 지원되지 않습니다. 신규/수정 화면: **System(**시스템**) > Updates(**업데이트**) > Upload Update(**업데이트 업로드**)** 버튼**> Specify software update source(**소프트웨어 업데이트 소스 지정**)** 옵션
FMC는 초기 설정 중에 최신 VDB를 다운로드하여 설치	6.6.0	새 이미지 또는 재이미징된 FMC를 설정하면 시스템이 자동으로 VDB(취약점 데이터베이스) 업데이트를 시도합니다. 이 작업은 한 번만 수행하면 됩니다. FMC에서 인터넷에 액세스할 수 있는 경우 자동 반복 VDB 업데이트 다운로드 및 설치를 수행하도록 작업을 예약하는 것이 좋습니다.

기능	버전	세부정보
FMC는 초기 설정 중에 소프트웨어 다운로드 및 GeoDB 업데이트를 예약합니다.	6.5.0	새 이미지 또는 재이미징된 FMC를 설정하면 시스템에서 다음 일정을 자동으로 예약합니다. • FMC 및 매니지드 디바이스의 소프트웨어 업데이트를 다운로드하는 주간 작업 • GeoDB 주간 업데이트 이런 작업은 UTC 기준으로 예약되므로, 사용자가 있는 위치와 날짜에 따라 지역적으로 실행됩니다. 또한 작업은 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받을 경우 예약된 작업은 현지 시간에 따라 여름에는 겨울보다 1시간 '늦게' 실행됩니다. 자동 예약 구성을 검토하고 필요한 경우 조정할 것을 강력하게 권장합니다.
FMC 업그레이드가 예약된 작업을 연기	6.7.0 6.4.0.10	FMC 업그레이드가 예약된 작업을 연기합니다. 업그레이드 중에 시작하도록 예약된 모든 작업은 업그레이드 후 재부팅하고 5분 후에 시작됩니다. 참고 업그레이드를 시작하기 전에 실행 중인 작업이 완료되었는지 확인해야 합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 이 기능은 지원되는 버전에서 모든 업그레이드를 지원합니다. 2021년 1월 현재 버전 6.4.0.10 이상 패치 및 버전 6.7.0 이상이 포함되어 있습니다. 이 기능은 지원되지 않는 버전에서 지원되는 버전으로 업그레이드 할 때는 지원되지 않습니다.
서명된 SRU, VDB 및 GeoDB 업데이트	6.4.0	따라서 Firepower에서는 올바른 업데이트 파일을 사용하고 있는지 확인할 수 있습니다. 이제 시스템은 SRU(침입 규칙), VDB(취약점 데이터베이스) 및 GeoDB(지리위치 데이터베이스)에 서명된 업데이트를 사용합니다. 이전 버전은 서명되지 않은 패키지를 계속 사용합니다. Cisco 지원 및 다운로드 사이트에서 업데이트를 수동으로 다운로드하지 않는 한(예: 무선 연결 구축) 기능에 차이가 있어서는 안 됩니다. 그러나 SRU, VDB 및 GeoDB 업데이트를 수동으로 다운로드하여 설치하는 경우 현재 버전에 맞는 패키지를 다운로드해야 합니다. 서명된 업데이트 파일은 'Sourcefire'대신 'Cisco'로 시작하고 .sh 대신 .sh.REL.tar로 끝납니다. • SRU: Cisco_Firepower_SRU-날짜-빌드-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-버전.sh.REL.tar • GeoDB: Cisco_GEODB_Update-날짜-빌드.sh.REL.tar 서명된(.tar) 패키지의 압축을 풀지 마십시오.

기능	버전	세부정보
더 빠른 업그레이드	6.4.0	이벤트 데이터베이스가 개선되어 이제 Firepower 어플라이언스를 더 빠르게 업그레이드할 수 있습니다.



8 장

백업 및 복원

- 백업 및 복원 정보, 203 페이지
- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지
- Firepower 어플라이언스 백업, 211 페이지
- Firepower 어플라이언스 복구, 218 페이지
- 백업 및 원격 스토리지 관리, 231 페이지
- 백업 및 복원 기록, 234 페이지

백업 및 복원 정보

재해부터 복구할 수 있는 능력은 모든 시스템 유지 보수 계획에서 필수적인 부분입니다. 재해 복구 계획의 일환으로, 정기적인 백업을 수행하여 원격 위치를 보호하는 것이 좋습니다.

온디맨드 백업

FMC, 7000/8000 시리즈 디바이스 및 여러 FTD 디바이스에 대해 FMC에서 온 디맨드 백업을 수행할 수 있습니다.

7000/8000 시리즈 디바이스의 로컬 웹 인터페이스를 사용하여 온 디맨드 백업을 수행할 수도 있습니다. 7000/8000 시리즈 디바이스의 로컬 백업 관리는 FMC의 백업 관리와는 약간 다르며 옵션도 적지만, 일반적으로 동일한 방식으로 작동합니다. FMC를 사용하여 이러한 디바이스를 원격으로 백업할 수 있습니다.

자세한 내용은 Firepower 어플라이언스 백업, 211 페이지를 참고하십시오.

예약 백업

FMC 또는 7000/8000 시리즈 디바이스에서 스케줄러를 사용하여 백업을 자동화할 수 있습니다. FMC에서의 원격 디바이스 백업은 예약할 수 없습니다.

FMC 설정 프로세스는 매주 설정 전용 백업을 예약하여 로컬에 저장합니다. 이는 전체 오프 사이트 백업을 대체하지 않습니다. 초기 설정이 완료되면 예약된 작업을 검토하고 조직의 요구에 맞게 조정해야 합니다.

자세한 내용은 예약 백업, 248 페이지를 참고하십시오.

백업 파일 저장

로컬로 백업을 저장할 수 있습니다. 그러나 NFS, SMB 또는 SSHFS 네트워크 볼륨을 원격 스토리지로 마운트하여 Firepower 어플라이언스를 안전한 원격 위치에 백업하는 것이 좋습니다. 이렇게 하면 모든 후속 백업이 해당 볼륨에 복사되지만, 계속해서 FMC를 사용하여 백업을 관리할 수 있습니다.

자세한 내용은 원격 스토리지 관리, 1363 페이지 및 백업 및 원격 스토리지 관리, 231 페이지를 참조하십시오.

Firepower 어플라이언스 복원

로컬 Backup Management(백업 관리) 페이지에서 FMC 및 7000/8000 시리즈 디바이스를 복구합니다. FTD 디바이스를 복구하려면 FTD CLI를 사용해야 합니다.

자세한 내용은 Firepower 어플라이언스 복구, 218 페이지를 참고하십시오.

백업이란?

FMC 백업에는 다음이 포함될 수 있습니다.

- 설정

  FMC 웹 인터페이스에서 설정할 수 있는 모든 설정은 원격 스토리지 및 감사 로그 서버 인증서 설정을 제외하고 설정 백업에 포함됩니다. 다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는만 백업할 수는 없습니다.

- 이벤트.

  이벤트 백업에는 FMC 데이터베이스의 모든 이벤트가 포함됩니다. 그러나 FMC 이벤트 백업에는 침입 이벤트 검토 상태가 포함되지 않습니다. 복구된 침입 이벤트는 Reviewed Events(검토된 이벤트) 페이지에 나타나지 않습니다.

디바이스 백업은 항상 설정 전용입니다.

복구되는 항목

설정을 복구하면 극히 드문 예외를 제외하고 모든 백업된 설정을 덮어씁니다. FMC에서 이벤트를 복구하면 침입 이벤트를 제외한 모든 기존 이벤트를 덮어씁니다.

다음 사항을 이해하고 계획해야 합니다.

- 백업되지 않은 항목은 복구할 수 없습니다.

  FMC 설정 백업에는 원격 스토리지 및 감사 로그 서버 인증서 설정이 포함되지 않으므로 복구 후에 이러한 설정을 다시 구성해야 합니다. 또한 FMC 이벤트 백업에는 침입 이벤트 검토 상태가 포함되지 않으므로 복구된 침입 이벤트는 Reviewed Events(검토된 이벤트) 페이지에 나타나지 않습니다.

- VPN 인증서 복구에 실패했습니다.

FTD 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 FTD 디바이스에서 VPN 인증서를 제거합니다. FTD 디바이스를 복구한 후에는 모든 VPN 인증서를 다시 추가/다시 등록해야 합니다.

- 공장 설정으로 새로 고침 또는 이미지 재설치 대신 구성된 FMC로 복구하면 침입 이벤트와 파일 목록이 병합됩니다.

  FMC 이벤트 복구 프로세스는 침입 이벤트를 덮어쓰지 않습니다. 대신 백업의 침입 이벤트가 데이터베이스에 추가됩니다. 중복을 방지하려면 복구 전에 기존 침입 이벤트를 삭제하십시오.

  FMC 설정 복구 프로세스는 AMP for Networks에서 사용되는 정상 및 사용자 지정 탐지 파일 목록을 덮어쓰지 않습니다. 대신 기존 파일 목록을 백업의 파일 목록과 병합합니다. 파일 목록을 교체하려면 복구하기 전에 기존 파일 목록을 삭제하십시오.

백업 및 복구 요구 사항

백업 및 복구에는 다음 요구 사항이 있습니다.

모델 요구 사항: 백업

다음을 백업할 수 있습니다.

- FMC
- FTD: 독립형, 네이티브 인스턴스, 컨테이너 인스턴스 또는 HA
- FTDv: VMware, 독립형 또는 HA
- 7000/8000 시리즈 디바이스

백업은 다음에 대해 지원되지 않습니다.

- FTD: 클러스터링된 디바이스
- FTDv: KVM, AWS, Azure
- NGIPSv
- ASA FirePOWER

백업 및 복구가 지원되지 않는 디바이스를 교체해야 한다면 디바이스별 설정을 수동으로 다시 생성해야 합니다. 하지만 FMC 백업은 매지니드 디바이스에 구축하는 정책과 다른 구성은 백업하지 않으며, FMC에서 이미 디바이스로 전송하는 이벤트도 백업하지 않습니다.

모델 요구 사항: 복구

교체 매니지드 디바이스는 교체하려는 디바이스와 동일한 모델이어야 하며 동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스를 사용해야 합니다.

FMC의 경우 RMA 시나리오에서 백업 및 복구를 사용할 수 있을 뿐 아니라 FMC 간에 설정 및 이벤트를 마이그레이션할 수도 있습니다. 지원되는 대상 및 대상 모델을 포함한 자세한 내용은 Firepower Management Center 모델 마이그레이션 가이드의 내용을 참조하십시오.

버전 요구 사항

모든 백업의 첫 번째 단계로 패치 레벨을 참고합니다. 백업을 복구하려면 이전 어플라이언스와 새 어플라이언스에서 패치를 포함하여 동일한 Firepower 버전을 실행해야 합니다.

또한 Firepower 4100/9300 섀시에서 Firepower 소프트웨어를 복구하려면 섀시에서 호환되는 FXOS 버전을 실행해야 합니다.

FMC 백업의 경우 동일한 VDB 또는 SRU가 없어도 됩니다. 그러나 백업을 복구하면 기존 VDB가 백업 파일의 VDB로 대체됩니다.

라이선스 요건

모범 사례 및 절차에 설명된 대로 라이선싱 또는 고아 엔타이틀먼트 문제를 해결합니다. 라이선싱 충돌이 발견되면 Cisco TAC에 문의하십시오.

도메인 요구 사항

수신:

- FMC 백업 또는 복구: 전역 전용.
- FMC에서 디바이스 백업: 전역 전용.
- 디바이스 복구 : 없음. 로컬로 디바이스를 복구합니다.

다중 도메인 구축에서는 이벤트백업할 수는 없습니다. 구성도 함께 백업해야 합니다.

백업 및 복원 지침 및 제한 사항

백업 및 복원에는 다음과 같은 지침 및 제한 사항이 있습니다.

백업 및 복원은 재해 복구**/RMA**에 사용됩니다.

백업 및 복원은 주로 RMA 시나리오를 위한 것입니다. 결함이 있거나 고장난 물리적 어플라이언스의 복원 프로세스를 시작하기 전에, Cisco TAC에 연락해 교체 하드웨어를 요청하십시오.

백업 및 복원을 사용하여 FMC 간에 구성 및 이벤트를 마이그레이션할 수도 있습니다. 따라서 조직의 성장, 물리적 구현에서 가상 구현으로의 마이그레이션, 하드웨어 새로 고침 등의 기술적 또는 비즈니스적 이유로 인해 FMC를 쉽게 교체할 수 있습니다.

백업 및 복원은 구성 가져오기/내보내기가 아닙니다.

백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 또는 디바이스 간에 구성을 복사하거나, 새 구성을 테스트하는 동안 다른 구성을 저장하지는 마십시오. 대신 가져오기/내보내기 기능을 사용해야 합니다.

예를 들어 FTD 디바이스 백업에는 디바이스의 관리 IP 주소 및 디바이스가 관리 FMC에 연결하는 데 필요한 모든 정보가 포함됩니다. 다른 FMC에서 매니지드 디바이스에 FTD 백업을 복구하지 마십시오. 복구된 디바이스는 백업에 지정된 FMC에 연결을 시도합니다.

복구는 개별적으로 그리고 로컬에서 진행됩니다.

개별적으로 그리고 로컬로 Firepower 어플라이언스에 복구합니다. 이것은 다음을 의미합니다:

- HA(고가용성) FMC 또는 디바이스는 일괄 복구할 수 없습니다. 이 가이드의 복구 절차에서는 HA 환경에서 복구하는 방법을 설명합니다.
- FMC를 사용하여 디바이스를 복구할 수는 없습니다. FMC 및 7000/8000 시리즈 디바이스의 경우 로컬 웹 인터페이스를 사용하여 복구할 수 있습니다. FTD 디바이스의 경우 FTD CLI를 사용해야 합니다.
- FMC 사용자 계정을 사용하여 매니지드 디바이스 중 하나에 로그인하고 복구할 수는 없습니다. Firepower 어플라이언스는 자체 사용자 계정을 유지 관리합니다.

Firepower 4100/9300에 대한 구성 가져오기/내보내기 지침

구성 내보내기 기능을 사용하여 Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정을 포함하는 XML 파일을 원격 서버 또는 로컬 컴퓨터로 내보낼 수 있습니다. 나중에 해당 구성 파일을 가져와서 구성 설정을 Firepower 4100/9300 섀시에 빠르게 적용하여, 알려진 정상적인 구성으로 돌아가거나 시스템 장애로부터 복구할 수 있습니다.

지침 및 제한 사항

- 구성 파일의 내용을 수정하지 마십시오. 구성 파일을 수정하면 해당 파일을 사용한 구성 가져오기가 실패할 수 있습니다.
- 애플리케이션 관련 구성 설정은 구성 파일에 포함되지 않습니다. 애플리케이션 관련 설정 및 구성을 관리하려면 애플리케이션에서 제공하는 구성 백업 도구를 사용해야 합니다.
- Firepower 4100/9300 섀시에서 설정을 가져오면 Firepower 4100/9300 섀시에 있는 모든 기존의 설정(논리적 디바이스 포함)이 삭제되고 가져오기 파일에 포함된 설정으로 완전히 교체됩니다.
- RMA 시나리오를 제외하고 설정을 내보낸 곳과 동일한 Firepower 4100/9300 섀시로 설정 파일만 가져오는 것이 좋습니다.
- 구성을 가져오는 Firepower 4100/9300 섀시의 플랫폼 소프트웨어 버전은 내보낼 때와 동일한 버전이어야 합니다. 버전이 다르면 가져오기 작업의 성공이 보장되지 않습니다. Firepower 4100/9300 섀시를 업그레이드 또는 다운그레이드할 때마다 백업 설정을 내보내는 것이 좋습니다.
- 구성을 가져오는 Firepower 4100/9300 섀시에는 내보냈을 때와 동일한 슬롯에 동일한 네트워크 모듈이 설치되어 있어야 합니다.
- 구성을 가져오는 Firepower 4100/9300 섀시에는, 가져오는 내보내기 파일에 정의된 논리적 디바이스에 대해 올바른 소프트웨어 애플리케이션 이미지가 설치되어 있어야 합니다.

- 기존 백업 파일을 덮어쓰지 않으려면, 백업 작업 시 파일 이름을 변경하거나 기존 파일을 다른 위치에 복사합니다.

백업 및 복원을 위한 모범 사례

백업 및 복구에는 다음과 같은 모범 사례가 있습니다.

백업 시기

유지 보수 기간 또는 사용률이 낮은 다른 시간에 백업하는 것이 좋습니다.

시스템이 백업 데이터를 수집하는 동안 데이터 상관관계(FMC만 해당) 도출이 일시적으로 일시 중지될 수 있으며, 백업 관련된 구성은 할 수 없게 됩니다.

다음 상황에서 백업해야 합니다.

- 정기 예약 백업.

  재해 복구 계획의 일환으로, 정기적인 백업 수행을 권장합니다.

  버전 6.5.0 이상 FMC 설정 프로세스는 매주 설정 전용 백업을 예약하여 로컬에 저장합니다. 이는 전체 오프 사이트 백업을 대체하지 않습니다. 초기 설정이 완료되면 예약된 작업을 검토하고 조직의 요구에 맞게 조정해야 합니다. 자세한 내용은 예약 백업, 248 페이지를 참고하십시오.

- SLR 변경 후.

  SLR(Specific Licensing Reservations)을 변경한 후 FMC를 백업합니다. 변경을 수행한 다음 이전 백업을 복원할 경우, 특정 라이선싱 반환 코드에 문제가 발생하여 고아 엔타이틀먼트가 발생할 수 있습니다.

- 업그레이드 또는 이미지 재설치 전.

  업그레이드가 심각하게 실패할 경우, 이미지를 재설치하고 복구해야 할 수 있습니다. 이미지 재설치는 시스템 비밀번호를 포함하여 대부분의 설정을 공장 기본값으로 되돌립니다. 최근 백업이 있는 경우, 보다 신속하게 정상 작업으로 돌아갈 수 있습니다.

- 업그레이드 후.

  새로 업그레이드한 구축의 스냅샷을 생성할 수 있도록 업그레이드 후 백업합니다. 매니지드 디바이스를 업그레이드한 후 FMC를 백업하는 것이 좋습니다. 그러면 새 FMC 백업 파일이 해당 디바이스가 업그레이드되었음을 '인식'합니다.

백업 파일 보안 유지

백업은 암호화되지 않은 아카이브(.tar) 파일로 저장됩니다.

PKI 개체의 개인 키 - 구축 지원에 필요한 공개 키 인증서 및 페어링된 개인 키가 백업되기 전에 암호 해독됨을 나타냅니다. 키는 백업을 복원할 때 임의로 생성된 키로 다시 암호화됩니다.

주의 Firepower 어플라이언스를 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 어플라이언스에 남아 있는 백업은 수동으로 또는 업그레이드 프로세스에 의해 삭제되어 로컬에 저장된 백업을 제거합니다.

특히 백업 파일은 암호화되지 않으므로 무단 액세스를 허용하지 않습니다. 백업 파일이 수정되면 복원 프로세스가 실패하게 됩니다. Admin/Maint(관리/유지 관리) 역할의 사용자는 원격 스토리지에서 파일을 이동하고 삭제할 수 있는 백업 관리 페이지에 액세스할 수 있습니다.

FMC의 시스템 설정에서 NFS, SMB 또는 SSHFS 네트워크 볼륨을 원격 스토리지로 마운트할 수 있습니다. 이렇게 하면 모든 후속 백업이 해당 볼륨에 복사되지만, 계속해서 FMC를 사용하여 백업을 관리할 수 있습니다. 자세한 내용은 원격 스토리지 관리, 1363 페이지 및 백업 및 원격 스토리지 관리, 231 페이지를 참조하십시오.

FMC만 네트워크 볼륨을 마운트합니다. 매니지드 디바이스 백업 파일은 FMC를 통해 라우팅됩니다. FMC와 해당 디바이스 간에 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)을 참조하십시오.

FTD 고가용성 구축의 백업 및 복구

FTD HA 구축에서는 다음을 수행해야 합니다.

- FMC에서 디바이스 쌍을 백업하되, FTD CLI에서 개별적으로 로컬에서 복구합니다.

  백업 프로세스에서는 FTD HA 디바이스용으로 고유한 백업 파일을 생성합니다. 특정 HA 피어를 다른 HA 피어의 백업 파일을 사용하여 복구하지 마십시오. 백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다.

  FTD HA 디바이스의 역할은 백업 파일 이름에 표시됩니다. 복구할 때는 적절한 백업 파일(기본 및 보조)을 선택해야 합니다.

- 복구하기 전에 HA를 일시 중단하거나 해제하지 마십시오.

  HA 설정을 유지 관리하면 복구 후 교체 디바이스를 쉽게 다시 연결할 수 있습니다. 이 작업을 수행하려면 HA 동기화를 다시 시작해야 합니다.

- 두 피어에서 동시에 restore CLI 명령을 실행하지 마십시오.

  백업이 성공했다고 가정하면 HA 쌍의 피어 중 하나 또는 둘 다를 교체할 수 있습니다. 동시에 수행할 수 있는 모든 물리적 교체 작업에는 랙킹 해제, 재랙킹 등이 있습니다. 그러나 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 두 번째 디바이스에서 restore 명령을 실행하지 마십시오.

백업에 성공하지 않고도 FTD HA 디바이스를 교체할 수 있습니다. FTD 고가용성 쌍의 유닛 교체, 912 페이지의 내용을 참조하십시오.

Firepower 4100/9300 섀시 백업 및 복구

Firepower 4100/9300 섀시에서 Firepower 소프트웨어를 복구하려면 섀시에서 호환되는 FXOS 버전을 실행해야 합니다.

Firepower 4100/9300 섀시를 백업할 때는 FXOS 설정도 백업하는 것이 좋습니다. 추가 모범 사례는 Firepower 4100/9300에 대한 구성 가져오기/내보내기 지침 , 207 페이지의 내용을 참조하십시오.

백업 전

백업하기 전에 다음을 수행해야 합니다.

- FMC에서 VDB 및 SRU를 업데이트합니다.

  항상 최신 취약성 데이터베이스(VDB) 및 침입 규칙 (SRU)을 사용하는 것이 좋습니다. FMC를 백업하기 전에 Cisco 지원 및 다운로드 사이트에서 최신 버전을 확인하십시오.

- 디스크 공간을 확인합니다.

  백업을 시작하기 전에 어플라이언스 또는 원격 스토리지 서버에 충분한 디스크 공간이 있는지 확인하십시오. 사용 가능한 공간이 Backup Management(백업 관리) 페이지에 표시됩니다.

  공간이 충분하지 않으면 백업이 실패할 수 있습니다. 특히 백업을 예약하는 경우, 정기적으로 백업 파일을 정리하거나 원격 스토리지 위치에 추가 디스크 공간을 할당해야 합니다.

복구 전

복구하기 전에 다음을 수행해야 합니다.

- 라이선스 변경 사항을 되돌립니다.

  백업 이후에 수행한 라이선싱 변경 사항을 되돌립니다.

  그렇지 않으면 복구 후 라이선스 충돌 또는 고아 엔타이틀먼트가 발생할 수 있습니다. 그러나 CSSM(Cisco Smart Software Manager)에서 등록을 취소하지 마십시오. CSSM에서 등록을 취소하는 경우, 복구 후 다시 등록을 취소한 다음 재등록해야 합니다.

  복구가 완료되면 라이선싱을 다시 설정합니다. 라이선싱 충돌 또는 고아 엔타이틀먼트가 확인되면 Cisco TAC에 문의하십시오.

- 결함이 있는 어플라이언스의 연결을 끊습니다.

  관리 인터페이스와 데이터 인터페이스(디바이스의 경우)의 연결을 끊습니다.

  FTD 디바이스를 복구하면 교체 디바이스의 관리 IP 주소가 이전 디바이스의 관리 IP 주소로 설정됩니다. IP 충돌 방지를 위해, 교체 디바이스에 백업을 복구하기 전에 관리 네트워크와 이전 디바이스의 연결을 끊으십시오.

  FMC 또는 7000/8000 시리즈 디바이스를 복구해도 관리 IP 주소는 변경되지 않습니다. 교체 시 수동으로 설정해야 하는데, 작업 전에 네트워크에서 이전 어플라이언스의 연결을 해제해야 합니다.

- 매니지드 디바이스를 등록 취소하지 마십시오.

FMC를 복구하든 매니지드 디바이스를 복구하든 관계없이 네트워크에서 어플라이언스의 물리적 연결을 끊더라도 FMC에서 디바이스를 등록 취소하지 마십시오.

등록을 취소한다면 보안 구역에서 인터페이스 매핑 같은 일부 디바이스 구성을 다시 설정해야 합니다. 복구 후에는 FMC와 디바이스가 정상적으로 통신을 시작해야 합니다.

- 이미지 재설치.

  RMA 시나리오에서는 교체 어플라이언스가 공장 기본값으로 설정된 상태로 제공됩니다. 그러나 교체 어플라이언스가 이미 설정된 경우, 이미지를 재설치하는 것이 좋습니다. 이미지를 재설치하면 시스템 암호를 포함하여 대부분의 설정이 공장 기본값으로 돌아갑니다. 주 버전으로만 이미지를 재설치할 수 있으므로 이미지를 재설치한 후에 패치를 적용해야 할 수 있습니다.

  이미지를 재설치하지 않을 경우, FMC 침입 이벤트 및 파일 목록이 덮어쓰이지 않고 병합됩니다.

복원 후

복구 후 다음을 수행해야 합니다.

- 복구되지 않은 항목을 재구성합니다.

  여기에는 라이선싱, 원격 스토리지 및 감사 로그 서버 인증서 설정 재구성이 포함될 수 있습니다. 또한 실패한 FTD VPN 인증서를 다시 추가/다시 등록해야 합니다.

- FMC에서 VDB 및 SRU를 업데이트합니다.

  항상 최신 취약성 데이터베이스(VDB) 및 침입 규칙(SRU)을 사용하는 것이 좋습니다. 이는 백업의 VDB가 교체 FMC의 VDB를 덮어쓰기 때문에 VDB에 특히 중요합니다.

- 구축.

  FMC를 복구한 후 모든 매니지드 디바이스에 구축합니다. 디바이스를 복구한 후 해당 디바이스에 구축합니다. 반드시 구축해야 합니다. 디바이스가 오래된 것으로 표시되지 않으면 Device Management(디바이스 관리) 페이지에서 강제 구축합니다. 디바이스에 기존 구성을 재구축하십시오, 500 페이지

Firepower 어플라이언스 백업

지원되는 어플라이언스에 대해 온 디맨드 또는 예약 백업을 수행할 수 있습니다.

FMC에서 디바이스를 백업하는 데 백업 프로필이 필요하지 않습니다. 그러나 7000/8000 시리즈 디바이스의 로컬 백업과 마찬가지로 FMC 백업에는 백업 프로파일이 필요합니다.. 온 디맨드 백업 프로세스를 통해 새 백업 프로파일을 생성할 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- FMC 백업, 212 페이지
- FMC에서 디바이스 백업, 213 페이지
- 7000/8000 시리즈 디바이스 로컬 백업, 216 페이지

- 백업 프로파일 생성, 217 페이지
- 예약 백업, 248 페이지

FMC 백업

온 디맨드 FMC 백업을 수행하려면 이 절차를 사용합니다.로컬 웹 인터페이스에서 7000/8000 시리즈 디바이스를 백업하려면 7000/8000 시리즈 디바이스 로컬 백업, 216 페이지의 내용을 참조하십시오.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 로컬 및 원격으로 저장된 모든 백업이 나열됩니다. 또한 백업을 저장하는 데 사용할 수 있는 디스크 공간의 양도 나열합니다. 공간이 충분하지 않으면 백업이 실패할 수 있습니다.

단계 **2** 기존 백업 프로파일을 사용할지 아니면 새로 시작할지를 선택합니다.

FMC 백업을 사용하려면 백업 프로파일을 사용하거나 생성해야 합니다.

- 기존 백업 프로파일을 사용하려면 **Backup Profiles(**백업 프로파일**)**를 클릭합니다.

  사용하려는 프로파일 옆에 있는 편집 아이콘을 클릭합니다. 그런 다음 **Start Backup(**백업 시작**)**을 클릭하여 지금 백업을 시작할 수 있습니다. 또는 프로파일을 편집하려면 다음 단계로 이동합니다.

- **Firepower Management Backup(Firepower** 관리 백업**)**을 클릭하여 새로 시작하고 새 백업 프로파일을 생성합니다.

  백업 프로파일의 이름을 입력합니다.

단계 **3** 백업할 항목을 선택합니다.

- 구성 백업
- 이벤트 백업

다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는만 백업할 수는 없습니다. 이러한 각 선택 항목에 대해 백업 및 백업되지 않는 항목에 대한 자세한 내용은 백업 및 복원 정보, 203 페이지의 내용을 참조하십시오.

단계 **4** FMC 백업 파일의 스토리지 위치를 적어둡니다.

이는 `/var/sf/backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. 자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참고하십시오.

단계 **5** (선택 사항) **Copy when complete(**완료 시 복사**)**를 활성화하여 완료된 FMC 백업을 원격 서버에 복사합니다.

호스트 이름 또는 IP 주소, 원격 디렉토리의 경로, 사용자 이름 및 암호를 제공합니다. 암호 대신 SSH 공유 키를 사용하려면 **SSH Public Key(SSH** 공유 키**)** 필드의 내용을 원격 서버에 있는 지정된 사용자의 `authorized_keys` 파일에 복사합니다.

참고 이 옵션은 백업을 로컬에 저장하거나 SCP를 원격 위치에 저장하려는 경우 유용합니다. SSH 원격 스토리지를 설정한 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉터리에 백업 파일을 복사하지 마십시오.

단계 **6** (선택 사항) **Email(**이메일**)**을 활성화하고 백업이 완료되면 알림을 받을 이메일 주소를 입력합니다.

이메일 알림을 받으려면 메일 서버에 연결하도록 FMC를 설정해야 합니다.메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

단계 **7** 온 디맨드 백업을 시작하려면 **Start Backup(**백업 시작**)**을 클릭합니다.

기존 백업 프로파일을 사용하지 않는 경우 시스템에서 자동으로 생성하여 사용합니다. 지금 백업을 실행하지 않으려는 경우 **Save(**저장**)** 또는 **Save As New(**새로 저장**)**를 클릭하여 프로파일을 저장할 수 있습니다. 두 경우 모두 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

단계 **8** 메시지 센터에서 진행 상황을 모니터링합니다.

시스템이 백업 데이터를 수집하는 동안 데이터 상관관계 도출이 일시적으로 일시 중지될 수 있으며, 백업 관련된 구성은 할 수 없게 됩니다. 원격 스토리지를 설정했거나 **Copy when complete(**완료시 복사**)**를 활성화한 경우 FMC가 원격 서버에 임시 파일을 쓸 수 있습니다. 이러한 파일은 백업 프로세스가 끝나면 정리됩니다.

다음에 수행할 작업

원격 스토리지를 설정했거나 **Copy when complete(**완료시 복사**)**를 활성화한 경우 백업 파일의 전송 성공을 확인합니다.

FMC에서 디바이스 백업

이 절차를 사용하여 다음 디바이스에 대한 온 디맨드 백업을 수행합니다.

- FTD: 물리적 디바이스, 독립형 또는 HA

- FTDv: VMware, 독립형 또는 HA
- 7000/8000 시리즈 디바이스

백업 및 복구는 클러스터된 디바이스를 포함하여 다른 플랫폼 또는 구성에 대해서는 지원되지 않습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

Firepower 4100/9300 섀시를 백업하는 경우에는 FXOS구성FXOS 구성 파일 내보내기, 215 페이지도 백업하는 것이 특히 중요합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을 선택한 다음 **Managed Device Backup(**매니지드 디바이스 백업**)**을 클릭합니다.

단계 **2** 하나 이상의 **Managed Devices(**매니지드 디바이스**)**를 선택합니다.

단계 **3** 아직 FMC에 전송되지 않은 이벤트 데이터를 백업하려면 **Include All Unified Files(**모든 통합 파일 포함**)**를 선택합니다.

단계 **4** 디바이스 백업 파일의 스토리지 위치를 적어 둡니다.

이는 `/var/sf/remote-backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. 자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참고하십시오.

단계 **5** 원격 스토리지를 설정하지 않은 경우, **Management Center**로 검색할지 여부를 선택합니다.

- 활성화됨(기본값): `/var/sf/remote-backup/`에 있는 FMC에 백업을 저장합니다.
- Disabled: `/var/sf/backup`의 디바이스에 백업을 저장합니다.

원격 백업 스토리지를 구성하면 백업 파일은 원격으로 저장되며 이 옵션은 적용되지 않습니다.

단계 **6** 온 디맨드 백업을 시작하려면 **Start Backup(**백업 시작**)**을 클릭합니다.

단계 **7** 메시지 센터에서 진행 상황을 모니터링합니다.

다음에 수행할 작업

원격 스토리지를 설정한 경우 백업 파일의 전송 성공을 확인합니다.

FXOS 구성 파일 내보내기

Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정을 포함하는 XML 파일을 원격 서버 또는 로컬 컴퓨터로 내보내려면 구성 내보내기 기능을 사용합니다.

참고 이 절차에서는 Firepower Threat Defense를 백업할 때 Firepower Chassis Manager을(를) 사용하여 FXOS 설정을 내보내는 방법을 설명합니다. CLI 절차는 Cisco Firepower 4100/9300 FXOS CLI 설정 가이드의 해당 버전을 참조하십시오.

시작하기 전에

Firepower 4100/9300에 대한 구성 가져오기/내보내기 지침 을 검토합니다.

프로시저

단계 **1** Firepower Chassis Manager에서 **System(**시스템**)** > **Configuration(**설정**)** > **Export(**내보내기**)**를 선택합니다.

단계 **2** 구성 파일을 로컬 컴퓨터로 내보내려면:

a) **Local(**로컬**)**을 클릭합니다.

b) **Export(**내보내기**)**를 클릭합니다.
구성 파일이 생성되고, 브라우저에 따라 기본 다운로드 위치로 파일이 자동으로 다운로드되거나 파일을 저장하라는 프롬프트가 표시될 수 있습니다.

단계 **3** 구성 파일을 원격 서버로 내보내려면:

a) **Remote(**원격**)**를 클릭합니다.

b) 원격 서버와의 통신에서 사용할 프로토콜을 선택합니다. FTP, TFTP, SCP, SFTP 중 하나일 수 있습니다.

c) 백업 파일을 저장할 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 섀시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브, 기타 읽기/쓰기 미디어일 수 있습니다.

IP 주소가 아니라 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.

d) 기본값 이외의 포트를 사용하려는 경우 **Port(**포트**)** 필드에 포트 번호를 입력합니다.

e) 시스템이 원격 서버에 로그인할 때 사용할 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

g) **Location(**위치**)** 필드에 구성 파일을 내보낼 전체 경로(파일 이름 포함)를 입력합니다.

h) 사용할 원격 구성에 대해 **Export(**내보내기**)**.
구성 파일이 생성되고 지정된 위치로 내보내기가 수행됩니다.

7000/8000 시리즈 디바이스 로컬 백업

7000/8000 시리즈 디바이스의 로컬 온 디맨드 백업을 수행하려면 이 절차를 사용합니다. 디바이스 백업은 항상 설정 전용입니다.

7000/8000 시리즈 디바이스의 로컬 백업 관리는 FMC의 백업 관리와는 약간 다르며 옵션도 적지만, 일반적으로 동일한 방식으로 작동합니다. 특정 요구 사항이 없는 한 FMC를 사용하여 이러한 디바이스를 원격으로 백업하는 것이 좋습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

프로시저

단계 **1** 디바이스의 로컬 웹 인터페이스에서 **System(**시스템**)** > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 로컬에 저장된 모든 백업이 나열됩니다. 또한 백업을 저장하는 데 사용할 수 있는 디스크 공간의 양도 나열합니다. 공간이 충분하지 않으면 백업이 실패할 수 있습니다.

단계 **2** 기존 백업 프로파일을 사용할지 아니면 새로 시작할지를 선택합니다.

7000/8000 시리즈 로컬 백업을 사용하려면 백업 프로파일을 사용하거나 생성해야 합니다. 온디맨드 백업을 수행할 때 기존 백업 프로파일을 선택하지 않으면 시스템에서 자동으로 생성하여 사용합니다. 그런 다음 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

- 기존 백업 프로파일을 사용하려면 **Backup Profiles(**백업 프로파일**)**를 클릭합니다.

  사용하려는 프로파일 옆에 있는 편집 아이콘을 클릭합니다. 그런 다음 **Start Backup(**백업 시작**)**을 클릭하여 지금 백업을 시작할 수 있습니다. 또는 프로파일을 편집하려면 다음 단계로 이동합니다.

- **Device Backup(**디바이스 백업**)**을 클릭하여 새로 시작하고 새 백업 프로파일을 생성합니다.

  백업 프로파일의 이름을 입력합니다.

단계 **3** (선택 사항) **Copy when complete(**완료되면 복사**)**를 활성화하여 완료된 백업을 원격 서버에 복사합니다.

이는 7000/8000 시리즈 로컬 백업용 원격 스토리지에 대한 유일한 옵션입니다.

호스트 이름 또는 IP 주소, 원격 디렉토리의 경로, 사용자 이름 및 암호를 제공합니다. 암호 대신 SSH 공유 키를 사용하려면 **SSH Public Key(SSH** 공유 키**)** 필드의 내용을 원격 서버에 있는 지정된 사용자의 `authorized_keys` 파일에 복사합니다.

단계 **4** (선택 사항) **Email(**이메일**)**을 활성화하고 백업이 완료되면 알림을 받을 이메일 주소를 입력합니다.

이메일 알림을 받으려면 메일 서버에 연결하도록 디바이스를 설정해야 합니다.메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

단계 **5** 온 디맨드 백업을 시작하려면 **Start Backup(**백업 시작**)**을 클릭합니다.

기존 백업 프로파일을 사용하지 않는 경우 시스템에서 자동으로 생성하여 사용합니다. 지금 백업을 실행하지 않으려는 경우 **Save(**저장**)** 또는 **Save As New(**새로 저장**)**를 클릭하여 프로파일을 저장할 수 있습니다. 두 경우 모두 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

단계 **6** 메시지 센터에서 진행 상황을 모니터링합니다.

시스템이 백업 데이터를 수집하는 동안 백업과 관련된 설정은 변경하지 못할 수 있습니다. **Copy when complete(**완료시 복사**)**를 활성화한 경우 디바이스가 원격 서버에 임시 파일을 쓸 수 있습니다. 이러한 파일은 백업 프로세스가 끝나면 정리됩니다.

다음에 수행할 작업

Copy when complete(완료시 복사**)**를 활성화한 경우 백업 파일의 전송 성공을 확인합니다.

백업 프로파일 생성

백업 프로파일은 백업된 환경 설정 집합, 즉 백업 대상, 백업 파일을 저장할 위치 등입니다.

FMC 백업 및 7000/8000 Series 로컬 백업에는 백업 프로파일이 필요합니다. 백업 프로파일은 FMC에서 디바이스를 백업하는 데 필요하지 않습니다.

온 디맨드 FMC 또는 7000/8000 시리즈 로컬 백업을 수행할 때 기존 백업 프로파일을 선택하지 않으면 시스템에서 자동으로 생성하여 사용합니다. 그런 다음 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

다음 절차에서는 온 디맨드 백업을 수행하지 않고 백업 프로필을 생성하는 방법을 설명합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**를 선택하고 **Backup Profiles(**백업 프로파일**)**를 클릭합니다.

단계 **2** **Create Profile(**프로필 생성**)**을 클릭하고 **Name(**이름**)**을 입력합니다.

단계 **3** (FMC 전용) 백업할 항목을 선택합니다.

7000/8000 시리즈 백업은 항상 설정 전용입니다.

- 구성 백업

- 이벤트 백업

다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는만 백업할 수는 없습니다. 이러한 각 선택 항목에 대해 백업 및 백업되지 않는 항목에 대한 자세한 내용은 백업 및 복원 정보, 203 페이지의 내용을 참조하십시오.

단계 **4** 백업 파일의 스토리지 위치를 적어둡니다.

FMC 백업 프로파일의 경우 이는 `/var/sf/backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. 7000/8000 로컬 백업 프로파일의 경우 항상 `/var/sf/backup/`입니다. 자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참고하십시오.

이는 `/var/sf/backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. 자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참고하십시오.

단계 **5** (선택 사항) **Copy when complete(**완료 시 복사**)**를 활성화하여 완료된 FMC 백업을 원격 서버에 복사합니다.

호스트 이름 또는 IP 주소, 원격 디렉토리의 경로, 사용자 이름 및 암호를 제공합니다. 암호 대신 SSH 공유 키를 사용하려면 **SSH Public Key(SSH** 공유 키**)** 필드의 내용을 원격 서버에 있는 지정된 사용자의 `authorized_keys` 파일에 복사합니다.

참고 이 옵션은 백업을 로컬에 저장하거나 SCP를 원격 위치에 저장하려는 경우 유용합니다. SSHFS 원격 스토리지를 설정한 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉터리에 백업 파일을 복사하지 마십시오.

단계 **6** (선택 사항) **Email(**이메일**)**을 활성화하고 백업이 완료되면 알림을 받을 이메일 주소를 입력합니다.

이메일 알림을 받으려면 메일 서버에 연결하도록 FMC를 설정해야 합니다.메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

단계 **7** **Save(**저장**)**를 클릭합니다.

Firepower 어플라이언스 복구

FMC 및 7000/8000 시리즈 디바이스의 경우 로컬 웹 인터페이스를 사용하여 백업에서 복구합니다. FTD 디바이스의 경우 FTD CLI를 사용해야 합니다. FMC를 사용하여 디바이스를 복구할 수는 없습니다.

다음 섹션에서는 Firepower 어플라이언스를 복구하는 방법을 설명합니다.

- 백업에서 FMC 복원, 219 페이지
- 백업에서 FTD 복구: Firepower 1000/2100 및 ASA-5500-X 시리즈, 220 페이지 (고가용성 예 포함)
- 백업에서 FTD 복원: Firepower 4100/9300 섀시, 223 페이지
- 백업에서 FTD 복원: FTDv, 228 페이지
- 백업에서 7000/8000 시리즈 디바이스 복구, 230 페이지

백업에서 FMC 복원

FMC 백업을 복구할 때 백업 파일에 포함된 구성 요소(이벤트, 설정) 중 일부 또는 전체를 복구하도록 선택할 수 있습니다.

참고 설정을 복구하면 극히 드문 예외를 제외하고 모든 설정을 덮어씁니다. 또한 FMC가 재부팅됩니다. 이벤트를 복구하면 침입 이벤트를 제외한 모든 기존 이벤트를 덮어씁니다. 준비가 되었는지 확인하십시오.

백업에서 FMC를 복구하려면 이 절차를 사용합니다.7000/8000 시리즈 디바이스를 복구하려면 백업에서 7000/8000 시리즈 디바이스 복구, 230 페이지의 내용을 참조하십시오.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

프로시저

단계 **1** 복구하려는 FMC에 로그인합니다.

단계 **2** **System(**시스템**)** > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 로컬 및 원격으로 저장된 모든 백업 파일이 나열됩니다. 백업 파일을 클릭하고 내용을 확인할 수 있습니다.

백업 파일이 목록에 없고 로컬 컴퓨터에 저장된 경우, **Upload Backup(**백업 업로드**)**을 클릭합니다. 백업 및 원격 스토리지 관리, 231 페이지의 내용을 참조하십시오.

단계 **3** 복구하려는 백업 파일을 선택하고 **Restore(**복구**)**를 클릭합니다.

단계 **4** 복구할 수 있는 구성 요소 중에서 선택한 다음 **Restore(**복구**)**를 다시 클릭하여 시작합니다.

단계 **5** 메시지 센터에서 진행 상황을 모니터링합니다.

설정을 복구하는 경우, FMC를 재부팅한 후 다시 로그인하면 됩니다.

다음에 수행할 작업

- 필요에 따라 복구 전에 되돌린 라이선싱 설정을 다시 구성합니다. 라이선싱 충돌 또는 분리 자격이 확인되면 Cisco TAC에 문의하십시오.

- 필요에 따라 원격 스토리지 및 감사 로그 서버 인증서 설정을 다시 구성합니다. 이러한 설정은 백업에 포함되지 않습니다.
- (선택 사항) SRU 및 VDB를 업데이트합니다. Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치하는 것이 좋습니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

백업에서 FTD 복구: Firepower 1000/2100 및 ASA-5500-X 시리즈

FTD 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

하드웨어 장애 시 이 절차에서는 Firepower 1000/2100 또는 ASA-5500-X 시리즈 FTD 디바이스를 독립형 또는 HA 쌍으로 교체하는 방법을 간략하게 설명합니다. 여기서는 교체하려는 디바이스 또는 디바이스의 백업에 액세스할 수 있다고 가정합니다. FMC에서 디바이스 백업, 213 페이지의 내용을 참조하십시오.

FTD HA 구축에서는 이 절차를 사용하여 피어 중 하나 또는 둘 다를 교체할 수 있습니다. 둘을 모두 교체하려면 restore CLI 명령을 제외한 두 디바이스에서 모든 단계를 동시에 수행합니다. 백업에 성공하지 않고도 FTD HA 디바이스를 교체할 수 있습니다. FTD 고가용성 쌍의 유닛 교체, 912 페이지의 내용을 참조하십시오.

참고 네트워크에서 디바이스의 연결을 끊을 때도 FMC에서 등록을 취소하지 마십시오. FTD HA 구축에서는 HA를 일시 중단하거나 해제하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

프로시저

단계 **1** 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco 반품 포털에서 RMA 프로세스를 시작할 수 있습니다.

단계 **2** 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- /var/sf/backup의 결함 있는 디바이스 자체
- /var/sf/remote-backup의 FMC
- 원격 스토리지 위치

FTD HA 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서 고유한 백업 파일을 생성합니다. 디바이스의 역할은 백업 파일 이름에 표시됩니다.

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **3** 결함이 있는 디바이스를 제거(분리)합니다.

모든 인터페이스의 연결을 끊습니다. FTD HA 구축에서는 페일오버 링크가 포함됩니다.

사용 중인 모델의 하드웨어 설치 및 시작 가이드를 참조하십시오.Cisco Firepower NGFW: 설치 및 업그레이드 가이드

참고 네트워크에서 디바이스의 연결을 끊을 때도 FMC에서 등록을 취소하지 마십시오. FTD HA 구축에서는 HA를 일시 중단하거나 해제하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 **4** 교체 디바이스를 설치하고 관리 네트워크에 연결합니다.

디바이스를 전원에 연결하고 관리 인터페이스를 관리 네트워크에 연결합니다. FTD HA 구축에서 페일오버 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Firepower NGFW: 설치 및 업그레이드 가이드

단계 **5** (선택 사항) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치하는 것이 좋습니다.

Cisco ASA 및 Firepower Threat Defense 이미지 재설치 가이드를 참조하십시오.

단계 **6** 교체 디바이스에서 초기 설정을 수행합니다.

관리자로 FTD CLI에 액세스합니다. 콘솔을 사용하거나 공장 기본 관리 인터페이스 IP 주소(192.168.45.45)에 SSH를 통해 연결할 수 있습니다. 설정 마법사에서 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 설정하라는 메시지를 표시합니다.

결함이 있는 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

사용 중인 모델에 대한 시작 가이드의 초기 설정 항목을 참조하십시오.Cisco Firepower NGFW: 설치 및 업그레이드 가이드

참고 교체 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 FMC 등록 프로세스를 시작합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **7** 교체 디바이스가 결함이 있는 디바이스와 동일한 Firepower 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 FMC에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 FTD 패치의 버전이 동일해야 합니다. FTD CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) FMC 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.FMC에 디바이스 추가, 311 페이지

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) FMC에서 새로 패치한 디바이스 등록을 취소합니다. FMC에서 디바이스 삭제, 315 페이지.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 FMC에 고스트 디바이스가 등록됩니다.

단계 **8** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다.

단계 **9** FTD CLI에서 백업을 복구합니다.

관리자로 FTD CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

FTD HA 구축에서 적절한 백업 파일(기본 및 보조)을 선택해야 합니다. 역할은 백업 파일 이름에 표시됩니다. HA 쌍의 두 디바이스를 모두 복구하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 두 번째 디바이스에서 restore 명령을 실행하지 마십시오.

단계 **10** FMC에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 FMC에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **11** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.
- HA 동기화를 다시 시작합니다. FTD CLI에서 `configure high-availability resume`을 입력합니다. 고가용성 일시 중단 또는 재개, 911 페이지의 내용을 참조하십시오.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 FTD 디바이스에서 VPN 인증서를 제거합니다. FTDVPN 인증서 매핑, 677 페이지의 내용을 참조하십시오.

단계 **12** 설정을 구축합니다.

반드시 구축해야 합니다. 복구된 디바이스가 오래된 것으로 표시되지 않으면 Device Management(디바이스 관리) 페이지에서 강제로 구축합니다.디바이스에 기존 구성을 재구축하십시오, 500 페이지

단계 **13** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Firepower NGFW: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업에서 FTD 복원: Firepower 4100/9300 섀시

FTD 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

이 절차에서는 하드웨어 장애 시 Firepower 4100/9300 섀시 교체 방법을 간략하게 설명합니다. 다음의 백업에 액세스할 수 있다고 가정합니다.

- 논리적 디바이스 또는 하나 이상의 디바이스를 교체합니다. FMC에서 디바이스 백업, 213 페이지의 내용을 참조하십시오.
- FXOS 설정. FXOS 구성 파일 내보내기, 215 페이지의 내용을 참조하십시오.

참고 네트워크에서 디바이스의 연결을 끊을 때도 FMC에서 등록을 취소하지 마십시오. 등록을 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

프로시저

단계 **1** 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco 반품 포털에서 RMA 프로세스를 시작할 수 있습니다.

단계 **2** 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 FMC
- 원격 스토리지 위치

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **3** FXOS 설정의 성공적인 백업을 찾습니다.

단계 **4** 결함이 있는 디바이스를 제거(분리)합니다.

모든 인터페이스의 연결을 끊습니다.

사용 중인 모델의 하드웨어 설치 및 시작 가이드를 참조하십시오.Cisco Firepower NGFW: 설치 및 업그레이드 가이드

참고 네트워크에서 디바이스의 연결을 끊을 때도 FMC에서 등록을 취소하지 마십시오. 등록을 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 **5** 교체 디바이스를 설치하고 관리 네트워크에 연결합니다.

디바이스를 전원에 연결하고 관리 인터페이스를 관리 네트워크에 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Firepower NGFW: 설치 및 업그레이드 가이드

단계 6 (선택 사항) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치하는 것이 좋습니다.

해당 Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager 설정 가이드에서 공장 기본 설정 복구에 대한 지침을 참조하십시오.

단계 7 FXOS가 호환되는 버전을 실행 중인지 확인합니다.

논리적 디바이스를 다시 추가하기 전에 호환되는 FXOS 버전을 실행 중이어야 합니다. Firepower Chassis Manager를 사용하여 백업된 FXOS 설정을 가져올 수 있습니다.구성 파일 가져오기, 226 페이지

단계 8 Firepower Chassis Manager를 사용하여 논리적 디바이스를 추가하고 초기 설정을 수행합니다.

결함이 있는 섀시의 논리적 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 논리적 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

사용 중인 모델의 시작 설명서에서 FMC 구축 장을 참조하십시오.Cisco Firepower NGFW: 설치 및 업그레이드 가이드

참고 논리적 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 FMC에 등록합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 9 교체 디바이스가 결함이 있는 디바이스와 동일한 Firepower 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 FMC에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 FTD 패치의 버전이 동일해야 합니다. FTD CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) FMC 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.FMC에 디바이스 추가, 311 페이지

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) FMC에서 새로 패치한 디바이스 등록을 취소합니다. FMC에서 디바이스 삭제, 315 페이지.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 FMC에 고스트 디바이스가 등록됩니다.

단계 10 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다.

단계 **11** FTD CLI에서 백업을 복구합니다.

관리자로 FTD CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

단계 **12** FMC에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 FMC에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **13** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 FTD 디바이스에서 VPN 인증서를 제거합니다. FTDVPN 인증서 매핑, 677 페이지의 내용을 참조하십시오.

단계 **14** 설정을 구축합니다.

반드시 구축해야 합니다. 복구된 디바이스가 오래된 것으로 표시되지 않으면 Device Management(디바이스 관리) 페이지에서 강제로 구축합니다.디바이스에 기존 구성을 재구축하십시오, 500 페이지

단계 **15** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Firepower NGFW: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

구성 파일 가져오기

Firepower 4100/9300 섀시에서 전에 내보낸 구성 설정을 적용하려면 구성 가져오기 기능을 사용할 수 있습니다. 이 기능을 사용하면 알려진 양호한 구성으로 돌아가거나 시스템 장애로부터 복구할 수 있습니다.

참고 이 절차에서는 Firepower 소프트웨어를 복구하기 전에 Firepower Chassis Manager을(를) 사용하여 FXOS 설정을 가져오는 방법을 설명합니다. CLI 절차는 Cisco Firepower 4100/9300 FXOS CLI 설정 가이드의 해당 버전을 참조하십시오.

시작하기 전에

Firepower 4100/9300에 대한 구성 가져오기/내보내기 지침 을 검토합니다.

프로시저

단계 **1** Firepower Chassis Manager에서 **System(**시스템**)** > **Tools(**도구**)** > **Import(**가져오기/내보내기**)**를 선택합니다.

단계 **2** 로컬 구성 파일로부터 가져오려면:

a) **Local(**로컬**)**을 클릭합니다.

b) **Choose File(**파일 선택**)**을 클릭하고 가져올 구성 파일을 찾아 선택합니다.

c) **Import(**가져오기**)**를 클릭합니다.
확인 대화 상자가 열리면서 계속 진행할 것인지를 물어보고 섀시를 재시작해야 한다고 경고합니다.

d) **Yes(**예**)**를 클릭하여 지정된 구성 파일을 가져올 것임을 확인합니다.
기존의 구성이 삭제되고, 가져오기 파일에 지정된 구성이 Firepower 4100/9300 섀시에 적용됩니다. 가져오는 동안 Breakout 포트 구성이 변경되는 경우 Firepower 4100/9300 섀시를 다시 시작해야 합니다.

단계 **3** 원격 서버에 있는 구성 파일로부터 가져오려면:

a) **Remote(**원격**)**를 클릭합니다.

b) 원격 서버와의 통신에서 사용할 프로토콜을 선택합니다. FTP, TFTP, SCP, SFTP 중 하나일 수 있습니다.

c) 기본값 이외의 포트를 사용하려는 경우 **Port(**포트**)** 필드에 포트 번호를 입력합니다.

d) 백업 파일을 저장할 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 섀시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브, 기타 읽기/쓰기 미디어일 수 있습니다.

IP 주소가 아니라 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.

e) 시스템이 원격 서버에 로그인할 때 사용할 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

g) **File Path(**파일 경로**)** 필드에 설정 파일의 전체 경로(파일 이름 포함)를 입력합니다.

h) 사용할 원격 구성에 대해 **Import(**가져오기**)**.
확인 대화 상자가 열리면서 계속 진행할 것인지를 물어보고 섀시를 재시작해야 한다고 경고합니다.

i) **Yes(예)**를 클릭하여 지정된 구성 파일을 가져올 것임을 확인합니다.
기존의 구성이 삭제되고, 가져오기 파일에 지정된 구성이 Firepower 4100/9300 섀시에 적용됩니다. 가져오는 동안 Breakout 포트 구성이 변경되는 경우 Firepower 4100/9300 섀시를 다시 시작해야 합니다.

백업에서 FTD 복원: FTDv

결함이 있거나 실패한 VMware용 Firepower Threat Defense Virtual 디바이스를 교체하려면 이 절차를 사용합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 FMC에서 등록을 취소하지 마십시오. 등록을 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

프로시저

단계 **1** 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 FMC
- 원격 스토리지 위치

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **2** 결함이 있는 디바이스를 제거합니다.

가상 시스템을 종료, 전원 끄기 및 삭제합니다. 절차는 가상 환경을 위한 설명서를 참조하십시오.

단계 **3** 교체 디바이스를 구축합니다.

Cisco Firepower Threat Defense Virtual for VMware 시작 가이드를 참고하십시오.

단계 **4** 교체 디바이스에서 초기 설정을 수행합니다.

VMware 콘솔을 사용하여 관리자로 FTD CLI에 액세스합니다. 설정 마법사에서 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 설정하라는 메시지를 표시합니다.

결함이 있는 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

시작 가이드에서 CLI 설정 항목을 참조하십시오. Cisco Firepower Threat Defense Virtual for VMware 시작 가이드.

참고 교체 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 FMC 등록 프로세스를 시작합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **5** 교체 디바이스가 결함이 있는 디바이스와 동일한 Firepower 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 FMC에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 FTD 패치의 버전이 동일해야 합니다. FTD CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) FMC 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.FMC에 디바이스 추가, 311 페이지

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) FMC에서 새로 패치한 디바이스 등록을 취소합니다. FMC에서 디바이스 삭제, 315 페이지.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 FMC에 고스트 디바이스가 등록됩니다.

단계 **6** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다.

단계 **7** FTD CLI에서 백업을 복구합니다.

관리자로 FTD CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

단계 **8** FMC에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 FMC에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **9** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 FTD 디바이스에서 VPN 인증서를 제거합니다. FTDVPN 인증서 매핑, 677 페이지의 내용을 참조하십시오.

단계 **10** 설정을 구축합니다.

반드시 구축해야 합니다. 복구된 디바이스가 오래된 것으로 표시되지 않으면 Device Management(디바이스 관리) 페이지에서 강제로 구축합니다.디바이스에 기존 구성을 재구축하십시오, 500 페이지

단계 **11** 데이터 인터페이스를 추가 및 설정합니다.

Cisco Firepower Threat Defense Virtual for VMware 시작 가이드 및 가상 환경 설명서를 참조하십시오.

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업에서 7000/8000 시리즈 디바이스 복구

이 절차에서는 7000/8000 시리즈 로컬 웹 인터페이스를 사용하여 백업에서 복구하는 방법을 설명합니다. 복구는 극히 드문 예외를 제외하고 모든 구성을 덮어 씁니다. 또한 디바이스를 재부팅합니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 205 페이지
- 백업 및 복원 지침 및 제한 사항, 206 페이지
- 백업 및 복원을 위한 모범 사례, 208 페이지

프로시저

단계 **1** 복구하려는 디바이스에 로그인합니다.

단계 **2** **System(**시스템**)** > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 로컬로 저장된 모든 백업 파일이 나열됩니다. 백업 파일을 클릭하고 내용을 확인할 수 있습니다.

백업 파일이 목록에 없고 로컬 컴퓨터에 저장한 경우 **Upload Backup(**백업 업로드**)**을 클릭합니다. 백업 및 원격 스토리지 관리, 231 페이지의 내용을 참조하십시오.

단계 **3** 복구하려는 백업 파일을 선택하고 **Restore(**복구**)**를 클릭합니다.

단계 **4** **Replace Configuration Data(**구성 데이터 교체**)**가 활성화되어 있는지 확인한 다음 **Restore(**복구**)**를 다시 클릭하여 시작합니다.

디바이스 백업은 항상 설정 전용입니다.

단계 **5** 디바이스가 재부팅될 때까지 메시지 센터에서 진행 상황을 모니터링합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

백업 및 원격 스토리지 관리

백업은 암호화되지 않은 아카이브(.tar) 파일로 저장됩니다. 파일 이름에는 다음을 포함할 수 있는 식별 정보가 포함됩니다.

- 백업 프로파일 또는 백업과 연결된 예약된 작업의 이름입니다.
- 백업된 어플라이언스의 표시 이름 또는 IP 주소입니다.
- 어플라이언스의 역할(예: HA 쌍의 멤버).

Firepower 어플라이언스를 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 어플라이언스에 남아 있는 백업은 수동으로 또는 업그레이드 프로세스에 의해 삭제될 수 있습니다. 업그레이드는 로컬에 저장된 백업을 제거합니다. 옵션에 대한 자세한 내용은 백업 스토리지 위치, 233 페이지의 내용을 참조하십시오.

⚠

주의 특히 백업 파일은 암호화되지 않으므로 무단 액세스를 허용하지 않습니다. 백업 파일이 수정되면 복원 프로세스가 실패하게 됩니다. Admin/Maint(관리/유지 관리) 역할의 사용자는 원격 스토리지에서 파일을 이동하고 삭제할 수 있는 백업 관리 페이지에 액세스할 수 있습니다.

다음 절차에서는 백업 파일을 관리하는 방법을 설명합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에 사용 가능한 백업이 나열됩니다. 또한 백업을 저장하는 데 사용할 수 있는 디스크 공간의 양도 나열합니다. 공간이 충분하지 않으면 백업이 실패할 수 있습니다.

단계 **2** 다음 중 하나를 수행합니다.

표 *8:* 원격 스토리지 및 백업 파일 관리

변경 후	수행해야 할 작업
FMC 시스템 설정을 편집할 필요 없이 백업을 위한 원격 스토리지를 활성화하거나 비활성화합니다.	**Enable Remote Storage for Backups(**백업에 원격 스토리지 활성화**)**를 클릭합니다. 이 옵션은 원격 스토리지를 설정한 후에만 나타납니다. 여기에서 토글하면 시스템 설정 (**System(**시스템**) > Configuration(**설정**) > Remote Storage Device(**원격 스토리지 디바이스**)**)에서도 토글됩니다. 팁 원격 스토리지 설정에 빠르게 액세스하려면 Backup Management(백업 관리) 페이지의 오른쪽 위에 있는 **Remote Storage(**원격 스토리지**)**를 클릭합니다.
FMC와 원격 스토리지 위치 간에 파일을 이동합니다.	**Move(**이동**)**를 클릭합니다. 원하는 만큼 파일을 앞뒤로 이동할 수 있습니다. 이렇게 하면 현재 위치에서 파일이 복사되지 않고 삭제됩니다. 백업 파일을 원격 스토리지에서 FMC로 이동할 때 FMC에 저장되는 위치는 백업의 종류에 따라 달라집니다. • FMC 백업: `/var/sf/backup` • 디바이스 백업: `/var/sf/remote-backup`
백업의 내용을 봅니다.	백업 파일을 클릭합니다.
백업 파일을 삭제합니다.	백업 파일을 선택하고 **Delete(**삭제**)**를 클릭합니다. 로컬 및 원격에 저장된 백업 파일을 모두 삭제할 수 있습니다.
컴퓨터에서 연락처 파일을 업로드합니다.	**Upload Backup(**백업 업로드**)**을 클릭하고 백업 파일을 선택한 다음 **Upload Backup(**백업 업로드**)**을 다시 클릭합니다.
백업을 컴퓨터에 다운로드합니다.	백업 파일을 선택하고 **Download(**다운로드**)**를 클릭합니다. 백업 파일을 이동하는 것과 달리 FMC에서 백업을 삭제하지 않습니다.

백업 스토리지 위치

다음 테이블에서는 Firepower 어플라이언스의 백업 스토리지 옵션에 대해 설명합니다.

표 *9:* 백업 스토리지 위치

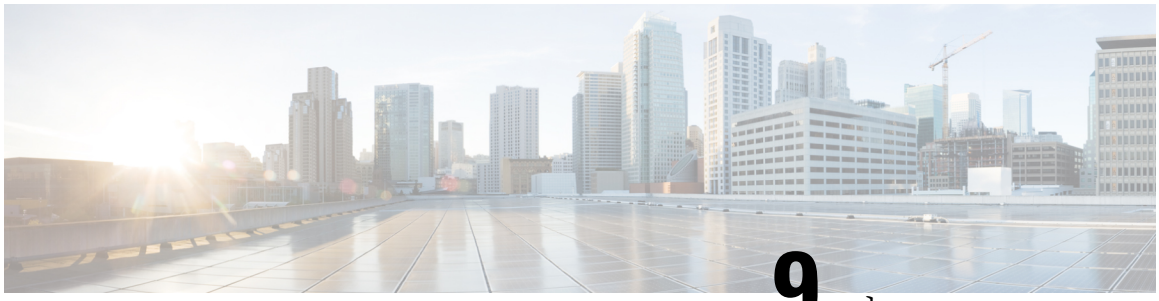
위치	세부 정보
원격(네트워크 볼륨(NFS, SMB, SSHFS) 마운트를 통해)	FMC의 시스템 설정에서 NFS, SMB 또는 SSHFS 네트워크 볼륨을 FMC 및 디바이스 백업용 원격 스토리지로 마운트할 수 있습니다. 원격 스토리지 관리, 1363 페이지의 내용을 참조하십시오.) 이렇게 하면 모든 후속 FMC 백업 및 *FMC* 시작 디바이스 백업이 해당 볼륨에 복사되지만, 계속해서 FMC를 사용하여 관리할 수 있습니다(복구, 다운로드, 업로드, 삭제, 이동). FMC만 네트워크 볼륨을 마운트합니다. 매니지드 디바이스 백업 파일은 FMC를 통해 라우팅됩니다. FMC와 해당 디바이스 간에 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)을 참조하십시오.
원격(복사를 통해)(SCP)	FMC 및 7000/8000 시리즈 로컬 백업의 경우, **Copy when complete(**완료 시 복사**)** 옵션을 사용하여 완료된 백업을 원격 서버에 안전하게 복사(SCP)할 수 있습니다. 네트워크 볼륨을 마운트하여 원격 스토리지와 비교할 때 **Copy when complete(**완료 시 복사**)**는 NFS 또는 SMB 볼륨에 복사할 수 없습니다. CLI 옵션을 제공하거나 디스크 공간 임계값을 설정할 수 없으며, 보고서의 원격 스토리지에는 영향을 주지 않습니다. 또한 백업 파일을 복사한 후에는 관리할 수 없습니다. 이 옵션은 백업을 로컬에 저장하고 SCP를 원격 위치에 저장하려는 경우 유용합니다. 또한 7000/8000 시리즈 로컬 백업용 원격 스토리지에 대한 유일한 옵션입니다. 참고 FMC 시스템 설정에서 SSHFS 원격 스토리지를 설정하는 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉토리에 백업 파일을 복사하지 마십시오.
로컬(FMC에서)	네트워크 볼륨을 마운트하여 원격 스토리지를 설정하지 않은 경우, FMC에 백업 파일을 저장할 수 있습니다. • FMC 백업은 `/var/sf/backup`에 저장됩니다. • 백업을 수행할 때 **Retrieve to Management Center(**관리 센터로 가져오기**)** 옵션을 활성화하면 디바이스 백업이 FMC의 `/var/sf/remote-backup`에 저장됩니다. 7000/8000 시리즈 로컬 백업은 FMC에 저장할 수 없습니다.

위치	세부 정보
로컬(디바이스에서)	디바이스 백업 파일은 다음의 경우 디바이스의 `/var/sf/backup`에 저장됩니다. • 네트워크 볼륨을 마운트하여 원격 스토리지를 설정하지 마십시오. • **Retrieve to Management Center(Management Center**로 검색**)**를 활성화하지 마십시오.

백업 및 복원 기록

기능	버전	세부 사항
컨테이너 인스턴스 지원	2.9.1	이제 FTD 컨테이너 인스턴스에서 FMC 백업/복원 도구를 사용할 수 있습니다. 신규/수정된 FMC 화면: **System(**시스템**) > Tools(**도구**) > Backup/Restore(**백업/복원**) > Managed Device Backup(**매니지드 디바이스 백업**)** 신규/수정된 FTD CLI 명령: **restore** 지원되는 플랫폼: Firepower 4100/9300 참고 Firepower 6.7 필요
복원을 위한 VDB 요구 사항	6.6	백업에서 FMC를 복원하면 기존 VDB가 백업 파일의 VDB로 대체됩니다. 복원하기 전에 VDB 버전을 더 이상 일치시킬 필요가 없습니다. 지원되는 플랫폼: FMC
자동으로 예약된 백업	6.5	신규 또는 재이미징된 FMC의 경우, 설정 프로세스는 FMC 구성을 백업하고 로컬에 저장하기 위해 매주 예약된 작업을 생성합니다. 지원되는 플랫폼: FMC

기능	버전	세부 사항
매니지드디바이스의 온디맨드 원격 백업	6.3	이제 FMC를 사용하여 특정 매니지드 디바이스의 온디맨드 원격 백업을 수행할 수 있습니다. 이전에는 7000 및 8000 시리즈 디바이스만 백업을 지원했고, 디바이스의 로컬 GUI를 사용해야 했습니다. 신규/수정된 화면: **System(**시스템**) > Tools(**도구**) > Backup/Restore(**백업/복원**) > Managed Device Backup(**매니지드 디바이스 백업**)** 신규/수정된 FTD CLI 명령: **restore** 지원되는 플랫폼: FTD 물리적 플랫폼, FTDv for VMware, 7000/8000 시리즈 예외: 6.7까지는 FTD 클러스터링 디바이스 또는 컨테이너 인스턴스는 지원하지 않습니다.



9 장

구성 가져오기 및 내보내기

다음 항목에서는 가져오기/내보내기 기능 사용 방법을 설명합니다.

- 컨피그레이션 가져오기/내보내기 정보, 237 페이지
- 구성 가져오기/내보내기 요구 사항 및 사전 요건, 239 페이지
- 컨피그레이션 내보내기, 240 페이지
- 컨피그레이션 가져오기, 240 페이지

컨피그레이션 가져오기/내보내기 정보

가져오기/내보내기 기능을 사용하여 어플라이언스 간에 구성을 복사할 수 있습니다. 구성 가져오기 및 내보내기는 백업 도구용이 아니지만 새로운 어플라이언스를 추가하는 프로세스를 간소화하는 데 사용될 수 있습니다.

단일 구성을 내보내거나 단일 동작으로 같은 유형 또는 다른 유형의 구성 집합을 내보낼 수 있습니다. 나중에 패키지를 다른 어플라이언스로 가져올 때 패키지의 어떤 구성을 가져올지 선택할 수 있습니다.

내보낸 패키지에는 해당 구성에 대한 개정 정보가 들어 있으며, 해당 구성을 다른 어플라이언스로 가져올 수 있는지 여부를 결정합니다. 어플라이언스 호환 되는 경우 패키지에 중복 구성, 시스템은 해결 옵션을 제공 합니다.

참고 가져오기 및 내보내기 어플라이언스는 동일한 버전의 Firepower System을 실행해야 합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다. 버전이 일치하지 않으면 가져오기가 실패합니다. 침입 규칙 업데이트 가져오기/내보내기 기능을 사용할 수 없습니다. 대신 최신 규칙 업데이트 버전을 다운로드하고 적용합니다.

가져오기/내보내기를 지원하는 구성

가져오기/내보내기는 다음 구성을 지원합니다.

- 액세스 제어 정책 및 이 정책에서 호출하는 정책: 네트워크 분석, 침입, SSL, 파일, Threat Defense Service Policy
- 액세스 제어와 무관한 침입 정책
- NAT 정책(Firepower Threat Defense만 해당)
- FlexConfig 정책. 그러나 정책을 내보내는 경우 모든 비밀 키 변수의 내용이 지워집니다. 비밀 키를 사용하는 FlexConfig 정책을 가져온 후 모든 비밀 키의 값을 수동으로 편집해야 합니다.
- 플랫폼 설정
- 상태 정책
- 알림 응답
- 애플리케이션 탐지기(사용자 정의 및 Cisco Professional Services 제공 모두)
- 대시보드
- 맞춤형 테이블
- 맞춤형 워크플로
- 저장된 검색
- 맞춤형 사용자 역할
- 보고서 템플릿
- 서드파티 제품 및 취약성 매핑

구성 가져오기/내보내기에 대한 특별 고려 사항

구성을 내보내는 경우 시스템도 다른 필수 구성을 내보냅니다. 예를 들어, 액세스 제어 정책 내보내기는 해당 정책이 호출하는 하위 정책, 해당 정책이 사용하는 개체 및 개체 그룹, 상위 정책 (다중 도메인 구축의 경우) 등을 내보냅니다. 또 다른 예로, 외부 인증이 활성화된 플랫폼 설정 정책을 내보내는 경우 인증 개체도 내보내게 됩니다. 그러나 몇 가지 예외가 있습니다.

- 시스템 제공 데이터베이스 및 피드— 시스템은 URL 필터링 카테고리 및 평판 데이터, Cisco Intelligence Feed 데이터 또는 GeoDB(지리위치 데이터베이스)를 내보내지 않습니다. 구축에 있는 모든 어플라이언스가 Cisco의 최신 정보를 받는지 확인하십시오.
- 전역 보안 인텔리전스 목록—시스템은 내보낸 구성과 관련된 전역 보안 인텔리전스 차단 리스트 및 차단 안 함 목록을 내보냅니다. (다중 도메인 구축에서 이는 현재 도메인과 상관없이 발생합니다.) 시스템은 하위 도메인 목록을 내보내지 않습니다.) 가져오기 프로세스는 이들 목록을 사용자가 생성한 목록으로 전환한 다음 가져온 구성으로 새 목록을 사용합니다. 이렇게 하면 가져온 목록이 기존의 전역 차단 목록 및 차단 안 함 목록과 충돌하지 않습니다. 가져오는 Firepower Management Center에서 가져온 구성으로 전역 목록을 사용하려면 목록을 수동으로 추가하십시오.

- 침입 정책 공유 계층 - 내보내기 프로세스가 침입 정책 공유 계층을 끊습니다. 이전에 공유된 계층은 패키지에 포함되며, 가져온 침입 정책에는 공유 계층이 포함되지 않습니다.
- 침입 정책 기본 변수 집합 - 내보내기 패키지에는 맞춤형 변수 및 시스템 제공 변수가 포함된 기본 변수 집합과 사용자 정의 값이 포함됩니다. 가져오기 프로세스는 기본 변수 집합을 가져오는 Firepower Management Center에서 가져온 값으로 업데이트합니다. 그러나 가져오기 프로세스는 내보내기 패키지에 없는 사용자 지정 변수를 삭제하지 않습니다. 가져오기 프로세스는 또한 내보내기 패키지에서 설정되지 않은 값에 대해 가져오는 Firepower Management Center에서 사용자 정의 값을 되돌리지 않습니다. 따라서 가져오는 Firepower Management Center이 기본 변수를 다르게 구성한 경우, 가져온 침입 정책이 예상과 다르게 작동할 수 있습니다.
- 맞춤형 사용자 개체—맞춤형 사용자 그룹 또는 개체를 Firepower Management Center에 생성한 경우 그리고 그러한 맞춤형 사용자 개체가 액세스 정책에 있는 어느 규칙의 일부인 경우, 내보내기 파일(.sfo)은 사용자 개체 정보를 전달하지 않습니다. 따라서 그러한 정책을 가져오는 경우, 그러한 맞춤형 사용자 개체에 대한 참조는 제거되며 대상 Firepower Management Center로 가져올 수 없습니다. 누락된 사용자 그룹으로 인한 탐지 문제를 방지하려면, 맞춤형 사용자 개체를 새 Firepower Management Center에 수동으로 추가하고 가져오기 후 액세스 제어 정책을 다시 구성합니다.

가져올 때 개체 및 개체 그룹:

- 일반적으로 가져오기 프로세스는 개체 및 그룹을 새 항목으로 가져 오며 기존 개체 및 그룹을 대체할 수 없습니다. 그러나 가져온 구성의 네트워크 및 포트 개체 또는 그룹이 기존 개체 또는 그룹과 일치하는 경우, 가져온 구성은 새 개체/그룹을 생성하는 대신 기존 개체/그룹을 다시 사용합니다. 시스템은 이름(자동 생성된 숫자 제외)과 각 네트워크 및 포트 개체/그룹의 내용을 비교하여 일치하는 항목을 결정합니다.
- 가져온 개체의 이름이 가져오는 Firepower Management Center에서 기존 개체와 일치하는 경우, 시스템이 가져온 개체 및 그룹 이름에 자동 생성된 번호를 추가하여 고유하게 만듭니다.
- 가져온 구성에서 사용되는 보안 영역 을 가져오는 Firepower Management Center에 의해 관리되는 매칭 유형 영역 에 매핑해야 합니다.
- 개인 키를 포함하는 PKI 개체를 사용하는 구성을 내보내는 경우, 시스템은 내보내기 전에 개인 키를 암호 해독합니다. 가져올 때 시스템은 무작위로 생성된 키로 해당 키를 암호화합니다.

구성 가져오기/내보내기 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자

컨피그레이션 내보내기

내보내는 구성 수 및 그러한 구성이 참조하는 개체의 수에 따라 내보내기 프로세스가 몇 분 정도 걸릴 수 있습니다.

팁 Firepower System의 많은 목록 페이지에는 목록 항목 옆에 **YouTube EDU**( )이 있습니다. 이 아이콘이 있으면 내보내기 절차의 빠른 대안으로서 사용할 수 있습니다.

시작하기 전에

- 가져오기 및 내보내기 어플라이언스에서 동일한 버전의 Firepower System 실행 중인지 확인합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Import/Export(**가져오기/내보내기**)**을(를) 선택합니다.

단계 **2** 축소( ) 및 확장( ) 아이콘을 클릭하여 사용 가능한 설정 목록을 축소하고 확대합니다.

단계 **3** 내보내려는 구성을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **4** 웹 브라우저의 프롬프트에 따라 내보낸 패키지를 컴퓨터에 저장합니다.

컨피그레이션 가져오기

가져오는 구성의 수 및 해당 구성이 참조하는 개체의 수에 따라 가져오기 절차에는 몇 분 정도 걸릴 수 있습니다.

참고 시스템에서 로그아웃하거나 다른 도메인으로 변경한 경우 또는 **Import(**가져오기**)**를 클릭한 후 사용자 세션이 시간 초과된 경우, 가져오기 프로세스가 완료될 때까지 백그라운드에서 계속 진행됩니다.

시작하기 전에

- 가져오기 및 내보내기 어플라이언스에서 동일한 버전의 Firepower System 실행 중인지 확인합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다.
- 가져오는 Firepower Management Center에 보안 영역을 생성합니다. 이 영역의 유형이 가져오는 액세스 제어 정책의 영역 유형과 일치해야 합니다. 자세한 내용은 보안 영역, 577 페이지를 참조하십시오.

프로시저

단계 **1** 가져오는 어플라이언스에서 **System(**시스템**)** > **Tools(**툴**)** > **Import/Export(**가져오기/내보내기**)**을 선택합니다.

단계 **2** **Upload Package(**패키지 업로드**)**를 클릭합니다.

단계 **3** 내보내기한 패키지의 경로를 입력하거나 해당 위치를 찾은 다음 **Upload(**업로드**)**를 클릭합니다.

단계 **4** 버전 불일치 또는 기타 문제가 없는 경우 가져오려는 구성을 선택한 다음 **Import(**가져오기**)**를 클릭합니다.
충돌 해결 또는 보안 영역 매핑을 수행할 필요가 없는 경우, 가가져오기가 완료되고 성공 메시지가 나타납니다. 이 절차의 나머지 부분을 건너뜁니다.

단계 **5** 메시지가 나타나면, Access Control Import Resolution(액세스 제어 가져오기 해결) 페이지에서 영역으로 가져온 구성에서 사용된 보안 영역를 가져오는 Firepower Management Center이 관리하는 매칭된 인터페이스 유형과 매핑합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

단계 **7** 메시지가 나타나면, Import Resolution(가져오기 해결) 페이지에서 가져오기 충돌 해결, 241 페이지에 설명된 대로 각 구성을 확장하고 적절한 옵션을 선택합니다.

단계 **8** **Import(**가져오기**)**를 클릭합니다.

단계 **9** 모든 피드를 업데이트합니다.

예를 들어, **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Security Intelligence(**보안 인텔리전스**)**로 이동하여 URL, Network(네트워크), DNS Lists(DNS 목록) 및 Feeds(피드) 페이지에서 **Update Feed(**피드 업데이트**)** 버튼을 클릭합니다.

가져온 정책은 피드 내용을 포함하지 않습니다.

단계 **10** 디바이스에 정책을 구축하기 전에 모든 피드 업데이트가 완료될 때까지 기다리십시오.

가져오기 충돌 해결

구성 가져오기를 시도하는 경우, 시스템에서 동일한 이름 및 유형의 구성이 이미 어플라이언스에 존재하는지 여부를 확인합니다. 다중 도메인 구축에서 시스템은 구성이 현재 도메인이나 상위 도메인 또는 하위 도메인에 정의 된 구성의 복제인지 여부도 결정합니다. (하위 도메인의 구성은 볼 수 없지

만, 하위 도메인에 중복된 이름이 있는 구성이 존재하는 경우 시스템이 충돌을 알립니다.) 가져오기에 중복 구성이 포함된 경우, 시스템은 다음 중 구축에 적합한 해결 옵션을 제공합니다.

- 기존 항목 유지

  시스템이 해당 구성을 가져오지 않습니다.

- 기존 항목 교체

  시스템이 가져오기에서 선택된 구성으로 현재 구성을 덮어씁니다.

- 최신 항목 유지

  타임 스탬프가 어플라이언스의 현재 구성에 대한 타임 스탬프보다 최근인 경우에만 시스템이 선택된 구성을 가져옵니다.

- 새 항목으로 가져오기

  시스템이 선택된 중복 구성을 가져오고 시스템 생성 번호를 이름에 추가하여 고유하게 만듭니다. (가져오기 프로세스를 완료하기 전에 이 이름을 변경할 수 있습니다.) 어플라이언스의 원래 구성이 변경되지 않습니다.

시스템에서 제공하는 해결 옵션은 구축에서 도메인을 사용하는지 여부, 가져온 구성이 현재 도메인에 정의된 구성과 중복되는지 여부 또는 현재 도메인의 상위 또는 하위 도메인에 정의된 구성인지 여부에 따라 달라집니다. 다음 표는 시스템에서 해결 옵션을 제공하거나 제공하지 않는 경우를 나열합니다.

해결 옵션	**Firepower Management Center**		매니지드 디바이스
	현재 도메인에서 중복	상위 또는 하위 도메인의 중복	
기존 항목 유지	예	예	예
기존 항목 교체	예	아니요	예
최신 항목 유지	예	아니요	예
새 항목으로 가져오기	예	예	예

사용자가 정상 또는 맞춤형 검색 파일 목록을 사용하는 파일 정책으로 액세스 제어 정책을 가져오고 파일 목록에는 중복 이름 충돌이 나타나는 경우, 시스템에서 위의 표에 설명된 대로 충돌 해결 옵션을 제공합니다. 그러나 시스템이 정책 및 파일 목록에 대해 수행하는 작업은 아래 표에 설명된 대로 다양합니다.

해결 옵션	시스템 작업	
	액세스 제어 정책 및 관련 파일 정책을 새 항목으로 가져오고 파일 목록을 병합합니다.	기존 액세스 제어 정책, 관련 파일 정책 및 파일 목록이 그대로 유지됩니다.
기존 항목 유지	아니요	예

해결 옵션	시스템 작업	
	액세스 제어 정책 및 관련 파일 정책을 새 항목으로 가져오고 파일 목록을 병합합니다.	기존 액세스 제어 정책, 관련 파일 정책 및 파일 목록이 그대로 유지됩니다.
기존 항목 교체	예	아니요
새 항목으로 가져오기	예	아니요
Keep newest(최신 상태로 유지**)**하고 가져오는 액세스 제어 정책이 최신 항목이 됩니다.	예	아니요
Keep newest(최신 상태로 유지**)**하고 기존 액세스 제어 정책이 최신 항목이 됩니다.	아니요	예

어플라이언스에서 가져온 구성을 수정하고 나중에 해당 어플라이언스로 해당 구성을 다시 가져 오는 경우, 유지할 구성 버전을 선택해야 합니다.

10 장

작업 예약

다음 항목에서는 작업을 예약하는 방법에 대해 설명합니다.

- 작업 예약 관련 정보, 245 페이지
- 작업 스케줄링 요구 사항 및 사전 요건, 246 페이지
- 반복 작업 구성, 246 페이지
- 예약된 작업 검토, 264 페이지
- 예약된 작업 기록, 267 페이지

작업 예약 관련 정보

여러 다양한 유형의 관리 작업이 한 번에 또는 주기적으로 지정된 시간에 실행되도록 일정을 관리할 수 있습니다.

중요 시스템의 작업 예약을 고려할 때는 다음 모범 사례를 염두에 두십시오.

- 초기 구성 중 FMC는 주간 작업을 예약하여 FMC 및 매지니드 디바이스의 최신 소프트웨어를 다운로드합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약이 실패하고 FMC가 인터넷에 액세스할 수 있다면 소프트웨어 다운로드 자동화, 258 페이지. 이 작업은 FMC에 소프트웨어 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.
- 초기 구성 중에 FMC는 주간 작업을 예약하여 로컬에 저장된 구성 전용 백업을 수행합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약에 실패하면 설명에 따라 백업을 수행하는 반복 작업을 예약하는 것이 좋습니다. FMC 백업 예약, 248 페이지.
- 초기 구성 중 FMC는 Cisco 지원 사이트에서 최신 취약점 데이터베이스(VDB)를 다운로드하고 설치합니다. 이 작업은 한 번만 수행하면 됩니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 시스템을 최신 상태로 유지하고자 하고 FMC가 인터넷에 액세스할 수 있다면 취약성 데이터베이스 업데이트 자동화, 260 페이지.

이 기능을 사용하여 설정된 작업은 UTC 기준으로 예약되며, 따라서 사용자의 위치와 날짜에 따라 작업이 지역적으로 실행됩니다. 또한 작업은 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받는다면, 예약된 작업은 현지 시간에 따라 여름에는 겨울보다 1시간 '후'에 실행됩니다

중요 예약된 작업이 의도한 시점에 수행되는지 확인하기를 적극 권장합니다.

참고 (자동화된 소프트웨어 업데이트를 포함하는 작업 또는 매니지드 디바이스에 업데이트를 푸시해야 하는 작업과 같은) 일부 작업은 낮은 대역폭을 가진 네트워크에 상당한 로드를 배치할 수 있습니다. 이와 같은 작업이 네트워크 사용 정도가 낮은 기간 동안 실행되도록 일정을 관리해야 합니다.

작업 스케줄링 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 유지 보수 사용자

반복 작업 구성

모든 유형의 작업에 동일한 프로세스를 사용하여 반복 작업의 빈도를 설정합니다.

웹 인터페이스에서 대부분의 페이지에 표시되는 시간은 로컬 시간입니다. 이 시간은 로컬 구성에서 지정하는 표준 시간대를 사용하여 결정됩니다. 또한 Firepower Management Center은 해당하는 경우 DST(일광 절약 시간)를 위해 해당 지역 시간 표시를 자동으로 조정합니다. 그러나, DST와 표준 시간을 오가는 전환 날짜를 포괄하는 반복 작업은 전환을 위해 조정되지 않습니다. 즉, 표준 시간 동안 오전 2시에 예약된 작업을 생성하는 경우, 이는 DST 동안 오전 3시에 실행됩니다. 유사하게, DST 동안 오전 2시에 예약된 작업을 생성하는 경우, 이는 표준 시간 동안 오전 1시에 실행됩니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 드롭다운 목록에서 일정을 예약할 작업 유형을 선택합니다.

단계 **4** **Schedule tast to run(**실행 작업 예약**)** 옵션 옆에 있는 **Recurring(**반복**)**을 클릭합니다.

단계 **5** **Start On(**착수 일자**)** 필드에서 반복 작업을 시작할 날짜를 지정합니다.

단계 **6** **Repeat Every(**반복 빈도**)** 필드에서 작업의 반복 빈도를 지정합니다.

숫자를 입력하거나 가동(▲) 및 아래쪽(▼)을 클릭하여 간격을 지정할 수 있습니다. 예를 들어 이틀마다 작업을 실행하려면 2를 입력하고 **Days(**일**)**를 클릭합니다.

단계 **7** **Run At(**착수 시간**)** 필드에서 반복 작업을 시작할 시간을 지정합니다.

단계 **8** 작업을 매주 또는 매월 실행하려면 **Repeat On(**반복 실행일**)** 필드에서 작업을 실행하려는 요일을 선택합니다.

단계 **9** 생성하려는 작업 유형에 대한 나머지 옵션을 선택합니다.

- 백업 - FMC 백업 예약, 248 페이지에 설명된 대로 백업 작업을 예약합니다.
- CRL 다운로드 - CRL(Certificate Revocation List) 다운로드 구성, 250 페이지에 설명된 대로 인증서 해지 목록 다운로드를 예약합니다.
- 정책 구축 - 정책 구축 자동화, 251 페이지에 설명된 대로 정책 구축을 예약합니다.
- Nmap 스캔 - Nmap 스캔 예약, 253 페이지에 설명된 대로 Nmap 스캔을 예약합니다.
- 보고 - 설명된 대로 보고서 생성을 예약합니다. 보고서 생성 자동화, 254 페이지
- Firepower 권장 규칙 - 설명된 대로 Firepower 권장 규칙 자동 업데이트를 예약합니다. Firepower 추천 자동화, 256 페이지
- 최신 업데이트 다운로드 - 소프트웨어 다운로드 자동화, 258 페이지 또는 VDB 업데이트 다운로드 자동화, 261 페이지에 설명된 대로 소프트웨어 또는 VDB 업데이트 다운로드를 예약합니다.
- 최신 업데이트 설치 - 소프트웨어 설치 자동화, 259 페이지 또는VDB 업데이트 설치 자동화, 262 페이지에 설명된 대로 Firepower Management Center 또는 매니지드 디바이스에 소프트웨어 또는 VDB 업데이트 설치를 예약합니다.
- 최신 업데이트 푸시 - 소프트웨어 푸시 자동화, 259 페이지에 설명된 매니지드 디바이스에 대한 소프트웨어 업데이트 푸시를 예약합니다.
- URL 필터링 데이터베이스 업데이트 - 설명된 대로 URL 필터링 데이터 자동 업데이트를 예약합니다. 예약된 작업을 통해 URL 필터링 업데이트 자동화, 263 페이지

단계 **10** **Save(**저장**)**를 클릭합니다.

예약 백업

Firepower Management Center 또는 7000/8000 시리즈 디바이스의 스케줄러를 사용하면 자체 백업을 자동화할 수 있습니다. FMC에서의 원격 디바이스 백업은 예약할 수 없습니다. 백업에 대한 자세한 내용은 백업 및 복원, 203 페이지의 내용을 참조하십시오.

원격 백업을 지원하지 않는 디바이스도 있습니다.

FMC 백업 예약

Firepower Management Center의 스케줄러를 사용하면 FMC와 디바이스 백업 모두를 자동화할 수 있습니다. 원격 백업을 지원하지 않는 디바이스도 있습니다. 자세한 내용은 백업 및 복원, 203 페이지를 참고하십시오.

참고 초기 구성 중에 FMC는 주간 작업을 예약하여 로컬에 저장된 구성 전용 백업을 수행합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약에 실패하면 설명에 따라 백업을 수행하는 반복 작업을 예약하는 것이 좋습니다. 이 주제.

시작하기 전에

백업 기본 설정을 지정하는 백업 프로 파일을 생성합니다. 백업 프로파일 생성, 217 페이지

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을(를) 선택합니다.

단계 **2** **Job Type** 목록에서 **Backup**을 선택합니다.

단계 **3** 백업을 한 번할지 반복 실행할지를 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업 관련 정보는 반복 작업 구성, 246 페이지의 내용을 참조하십시오.

단계 **4** 작업 이름을 입력합니다.

단계 **5** **Backup Type(**백업 유형**)**으로 **Management Center(**관리 센터**)**를 클릭합니다.

단계 **6** **Backup Profile(**백업 프로파일**)**을 선택합니다.

단계 **7** (선택 사항) **Comment(**코멘트**)**를 입력합니다.

코멘트를 간략하게 합니다. 코멘트는 schedule calendar(일정 달력) 페이지의 Task Details(작업 정보) 섹션에 나타납니다.

단계 **8** (선택 사항) **Email Status To:(**다음에 대한 이메일 상태**)** 필드에 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록을 입력합니다.

작업 상태 메시지를 전송하도록 이메일 릴레이 서버를 설정하는 방법은 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지의 내용을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

원격 디바이스 백업 예약

Firepower Management Center의 스케줄러를 사용하면 FMC와 디바이스 백업 모두를 자동화할 수 있습니다. 원격 백업을 지원하지 않는 디바이스도 있습니다. 자세한 내용은 백업 및 복원, 203 페이지를 참고하십시오.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을(를) 선택합니다.

단계 **2** **Job Type** 목록에서 **Backup**을 선택합니다.

단계 **3** 백업을 한 번할지 반복 실행할지를 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업 관련 정보는 반복 작업 구성, 246 페이지의 내용을 참조하십시오.

단계 **4** 작업 이름을 입력합니다.

단계 **5** **Backup Type(**백업 유형**)**으로 **Device(**디바이스**)**를 클릭합니다.

단계 **6** 하나 이상의 디바이스를 선택합니다.

목록에 없는 디바이스는 원격 백업을 지원하지 않습니다.

단계 **7** 백업용 원격 스토리지를 설정하지 않은 경우, **Management Center**로 검색할지 여부를 선택합니다.

- 활성화됨(기본값): `/var/sf/remote-backup/`에 있는 FMC에 백업을 저장합니다.
- Disabled(비활성화됨)(기본값): `/var/sf/backup`의 디바이스에 백업을 저장합니다.

원격 백업 스토리지를 구성하면 백업 파일은 원격으로 저장되며 이 옵션은 적용되지 않습니다.자세한 내용은 백업 및 원격 스토리지 관리, 231 페이지를 참조하십시오.

단계 **8** (선택 사항) **Comment(**코멘트**)**를 입력합니다.

코멘트를 간략하게 합니다. 코멘트는 schedule calendar(일정 달력) 페이지의 Task Details(작업 정보) 섹션에 나타납니다.

단계 **9** (선택 사항) **Email Status To:(**다음에 대한 이메일 상태**)** 필드에 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록을 입력합니다.

작업 상태 메시지를 전송하도록 이메일 릴레이 서버를 설정하는 방법은 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지의 내용을 참조하십시오.

단계 **10** **Save(**저장**)**를 클릭합니다.

로컬 7000 및 8000 Series 디바이스 백업 예약

7000 또는 8000 Series 디바이스의 스케줄러를 사용하면 자체 백업을 자동화할 수 있습니다. FMC를 사용하여 백업을 예약하려면 FMC 백업 예약, 248 페이지의 내용을 참조하십시오.

시작하기 전에

백업 기본 설정을 지정하는 백업 프로 파일을 생성합니다. 백업 프로파일 생성, 217 페이지

프로시저

단계 **1** 디바이스의 웹 인터페이스에서 **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을(를) 선택합니다.

단계 **2** **Job Type** 목록에서 **Backup**을 선택합니다.

단계 **3** 백업을 한 번할지 반복 실행할지를 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업 관련 정보는 반복 작업 구성, 246 페이지의 내용을 참조하십시오.

단계 **4** 작업 이름을 입력합니다.

단계 **5** **Backup Profile(**백업 프로파일**)**을 선택합니다.

단계 **6** (선택 사항) **Comment(**코멘트**)**를 입력합니다.

코멘트를 간략하게 합니다. 코멘트는 schedule calendar(일정 달력) 페이지의 Task Details(작업 정보) 섹션에 나타납니다.

단계 **7** (선택 사항) **Email Status To:(**다음에 대한 이메일 상태**)** 필드에 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록을 입력합니다.

작업 상태 메시지를 전송하도록 이메일 릴레이 서버를 설정하는 방법은 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지의 내용을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

CRL(Certificate Revocation List) 다운로드 구성

Firepower Management Center 또는 7000 또는 8000 Series 디바이스에 대한 로컬 웹 인터페이스를 사용하여 이 절차를 수행해야 합니다. 다중 도메인 구축에서 이 작업은 Firepower Management Center에 대해 전역 도메인에서만 지원됩니다.

사용자가 어플라이언스에 대한 사용자 인증서 또는 감사 로그 인증서를 사용하는 어플라이언스의 로컬 구성에서 CRL(인증서 해지 목록) 다운로드를 활성화하는 경우, 시스템에서 자동으로 CRL 다운

로드 작업을 생성합니다. 스케줄러를 사용하여 작업을 편집하고 업데이트 빈도를 설정할 수 있습니다.

시작하기 전에

- 사용자 인증서를 활성화 및 구성하고, CRL 다운로드 URL을 설정합니다. 자세한 내용은 유효한 사용자 인증서 필요, 1348 페이지를 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)**에서 **Download CRL(CRL** 다운로드**)**을 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 CRL 다운로드를 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **7** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 Firepower Management Center에 구성된 유효한 이메일 릴레이 서버가 있어야 합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

정책 구축 자동화

FMC에서 구성 설정을 수정한 후, 영향을 받는 디바이스에 해당 변경 사항을 구축해야 합니다.

다중 도메인 구축에서, 현재 도메인에 대해서만 정책 구축을 예약할 수 있습니다.

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. Snort® 재시작 트래픽 동작, 507 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)**에서 **Deploy Policies(**정책 구축**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Device(**디바이스**)** 필드에서 정책을 구축하려는 디바이스를 선택합니다.

단계 **7** 필요에 따라 **Skip deployment for up-to-date devices(**최신 디바이스에 대한 구축 건너뛰기**)** 확인란을 선택하거나 선택 취소합니다.

기본적으로 **Skip deployment for up-to-date devices(**최신 디바이스에 대한 구축 건너뛰기**)** 옵션이 활성화되어 정책 구축 프로세스에서 성능을 향상시킵니다.

참고 시스템은 Firepower Management Center 웹 인터페이스에서 시작된 정책 배포가 진행 중인 경우 예약된 정책 구축 작업을 수행하지 않습니다. 따라서 예약된 정책 배포 작업이 진행중인 경우, 시스템은 웹 인터페이스에서 정책 구축을 시작할 수 없습니다.

단계 **8** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **9** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지
만료된 정책, 516 페이지

Nmap 스캔 자동화

네트워크에 있는 대상에 대해 정기적인 Nmap 스캔을 예약할 수 있습니다. 스캔을 자동화하면 Nmap 스캔에서 전에 제공한 정보를 새로 고칠 수 있습니다. Firepower System이 Nmap 제공 데이터를 업데이트할 수 없으므로 데이터를 최신 상태로 유지하려면 정기적으로 다시 스캔해야 합니다. 네트워크의 호스트에서 식별되지 않은 애플리케이션이나 서버를 자동으로 테스트하도록 스캔을 예약할 수도 있습니다.

Discovery Administrator(검색 관리자)는 Nmap 스캔을 교정으로서 사용할 수도 있습니다. 예를 들어, 호스트에서 운영 체제 충돌이 발생하면 해당 충돌이 Nmap 스캔을 트리거할 수 있습니다. 스캔을 실행하면 호스트에 대한 업데이트된 운영 체제 정보를 얻게 되며, 이를 통해 충돌이 해결됩니다.

이전에 Nmap 검색 기능을 사용하지 않은 경우, 예약 검색을 정의하기 전에 Nmap 검색을 구성합니다.

관련 항목

Nmap 스캐닝, 2414 페이지

Nmap 스캔 예약

시스템에서 탐지된 호스트의 운영 체제, 애플리케이션 또는 서버가 Nmap 스캔 결과와 교체되면, 시스템은 호스트에 대해 Nmap에 의해 교체된 정보를 더 이상 업데이트하지 않습니다. Nmap 제공 서비스 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트를 스캔하려는 경우 Nmap 제공 운영 체제, 애플리케이션 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 호스트가 네트워크 맵에서 삭제된 후 다시 추가된 경우, Nmap 스캔 결과가 삭제되며 시스템은 호스트에 대한 모든 운영 체제 및 서비스 데이터의 모니터링을 다시 시작합니다.

다중 도메인 구축:

- 현재 도메인에 대해서만 스캔을 예약할 수 있습니다.
- 선택된 교정 및 Nmap 대상은 현재 도메인 또는 상위 도메인에 존재해야 합니다.
- 리프 도메인이 아닌 도메인에서 Nmap 스캔을 수행하도록 선택하면 해당 도메인의 각 하위 노드에서 동일한 대상을 검색합니다

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)**에서 **Nmap Scan(Nmap** 스캔**)**을 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **map Remediation(Nmap** 교정**)**필드에서 Nmap 교정을 선택합니다.

단계 **7** **Nmap Target(Nmap** 대상**)** 필드에서 스캔 대상을 선택합니다.

단계 **8** **Domain(**도메인**)** 필드에서 네트워크 맵을 보강하려는 도메인을 선택합니다.

단계 **9** 작업에 대 한 의견 하려는 경우 설명 필드에 설명을 입력합니다.

팁 코멘트 필드는 calendar schedule(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **10** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

보고서 생성 자동화

일정한 간격으로 실행되도록 보고를 자동화할 수 있습니다.

다중 도메인 구축에서, 현재 도메인에 대해서만 보고를 예약할 수 있습니다.

시작하기 전에

- 보고서 템플릿을 생성합니다. 자세한 내용은 보고서 템플릿, 2653 페이지를 참조하십시오.
- 스케줄러를 사용하여 이메일 보고를 배포하려는 경우, 메일 릴레이 호스트를 구성하고 보고 수신자와 메시지 정보를 지정하십시오. 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지 및 생성 시 이메일로 보고서 배포, 2675 페이지를 참조하십시오.
- (선택 사항) 예약된 보고의 파일 이름, 출력 형식, 기간 또는 이메일 배포 설정을 설정하거나 변경합니다. 예약된 보고서에 대한 보고서 생성 설정 지정, 255 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Report(**보고**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Report Template(**보고서 템플릿**)** 필드에서 report template(보고서 템플릿)을 선택합니다.

단계 **7** 작업에 대 한 의견 하려는 경우 설명 필드에 설명을 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

참고 이 옵션을 구성해도 보고가 배포되지는 않습니다.

단계 **9** 보고서에 데이터가 없는 경우(예: 보고서 기간에 특정 유형의 이벤트가 발생하지 않은 경우) 보고서 이메일 첨부 파일을 수신하지 않으려면 **If report is empty, still attach to email(**보고서가 비어 있는 경우에도 이메일에 첨부**)** 확인란을 선택합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

예약된 보고서에 대한 보고서 생성 설정 지정

이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

지정하거나 파일 이름, 출력 형식, 타임 윈도우를 변경하거나 예약된 보고서의 메일 설정을 이메일:

프로시저

단계 **1** 선택 **Overview(**개요**) > Reporting(**보고**) > Report Templates(**보고서 템플릿**)**을 선택합니다.

단계 **2** 변경하려는 보고서 템플릿에 대한 **Edit(**편집**)**을 클릭합니다.

단계 **3** **Generate(**생성**)**를 클릭합니다.

참고 이제 보고서를 생성하지 않고 보고서 생성 설정을 변경하려는 경우에 템플릿 구성 페이지에서 생성을 클릭해야 합니다. 보고서를 생성하지 않는 한 템플릿 목록 보기에서 생성을 클릭하는 경우 변경 사항은 저장되지 않습니다.

단계 **4** 설정을 수정합니다.

단계 **5** 보고서를 생성하지 않고 새 설정을 저장하려면 **Cancel (**취소**)**을 클릭합니다.

새 설정을 저장하고 보고서를 생성하려면 **Generate(**생성**)**를 클릭하고 이 절차의 나머지를 건너뛰고 합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 변경 하지 않은 경우에 저장 하 라는 프롬프트가 표시 되 면 **OK(**확인**)**를클릭 합니다.

Firepower 추천 자동화

사용자 지정 침입 정책에서 가장 최근에 저장된 구성 설정을 사용하여 네트워크에 대한 네트워크 검색 데이터를 기반으로 규칙 상태 권장 사항을 자동으로 생성할 수 있습니다.

참고 저장되지 않은 변경 사항이 있는 침입 정책에 대해 시스템이 예약 권장 사항을 자동으로 생성하는 경우, 자동으로 생성된 권장 사항을 규칙에 반영하려면 해당 정책에서 변경 사항을 취소하고 정책을 커밋해야 합니다.

작업이 실행되면 시스템에서 권장되는 규칙 상태를 자동으로 생성하고 정책 구성에 따라 침입 규칙의 상태를 수정합니다. 다음에 침입 정책을 구축할 때 수정된 규칙 상태가 반영됩니다.

다중 도메인 구축에서 현재 도메인 수준의 침입 정책 권장 사항을 자동화 할 수 있습니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 상위 도메인의 침입 정책에서 이 기능을 활성화하면 모든 하위 리프 도메인의 데이터를 사용하여 권장 사항이 생성됩니다. 이로 인해 일부 리프 도메인에는 없는 자산에 맞게 조정된 침입 규칙이 활성화되어 성능에 영향을 줄 수 있습니다.

시작하기 전에

- Firepower 권장 규칙에 설명 된 대로 IPS 정책 구성Firepower 추천 생성 및 적용, 2040 페이지
- 작업 상태 메시지가 이메일 하려는 경우 유효한 이메일 릴레이 서버를 구성 합니다.
- 권장 사항을 생성하려면 위협 스마트 라이선스 또는 보호 클래식 라이선스가 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)**에서 **Firepower Recommended Rules(Firepower** 권장 규칙**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Policies(**정책**)** 옆에서 권장 사항을 생성하려는 침입 정책을 하나 이상 선택합니다. 모든 침입 정책을 선택하려면 **All Policies(**모든 정책**)** 확인란을 선택합니다.

단계 **7** (선택 사항) **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트를 간략하게 합니다. 코멘트는 schedule calendar(일정 달력) 페이지의 Task Details(작업 정보) 섹션에 나타납니다.

단계 **8** (선택 사항) 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지
Firepower 권장 규칙 정보, 2037 페이지
메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

소프트웨어 업데이트 자동화

대부분의 패치 및 기능 릴리스를 Firepower System에 자동으로 다운로드 및 적용할 수 있습니다.

중요 초기 구성 중 FMC는 주간 작업을 예약하여 FMC 및 매지니드 디바이스의 최신 소프트웨어를 다운로드합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약이 실패하고 FMC가 인터넷에 액세스할 수 있다면 소프트웨어 다운로드 자동화, 258 페이지. 이 작업은 FMC에 소프트웨어 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.

소프트웨어 업데이트를 설치하기 위해 예약해야 하는 작업은 FMC를 업데이트하는지 또는 FMC를 사용하여 매니지드 디바이스를 업데이트하는지에 따라 다릅니다.

참고 Cisco에서는 FMC를 사용하여 매니지드 디바이스를 업데이트할 것을 적극 권장합니다.

- FMC를 업데이트하려면 Install Latest Update(최신 업데이트 설치) 작업을 사용하여 소프트웨어 설치를 예약하십시오.
- 매니지드 디바이스에서 소프트웨어 업데이트를 자동화하기 위해 FMC를 사용하려면 두 가지 작업을 예약해야 합니다.
  - Push Latest Update(최신 업데이트 푸시) 작업을 사용하여 매니지드 디바이스에 업데이트를 푸시(복사)합니다.
  - Install Latest Update(최신 업데이트 설치) 작업을 사용하여 매니지드 디바이스에 업데이트를 설치합니다.

  매니지드 디바이스에 대한 업데이트를 예약하는 경우, 푸시 및 설치 작업이 연속적으로 수행되도록 예약합니다. 설치하기 전에 먼저 업데이트를 디바이스에 적용해야 합니다. 프로세스가 완료될 때까지 작업 간에 충분한 시간을 둡니다. 적어도 30분 간격으로 작업을 예약합니다. 업데이트를 설치하기 위해 작업을 예약하지만 FMC에서 디바이스로 업데이트 복사가 완료되지 않은 경우 설치 작업이 성공하지 못합니다. 그러나 예약 설치 작업이 매일 반복되면 다음 날 작업이 실행될 때 푸시된 업데이트를 설치합니다.

참고 다음과 같은 두 상황에서는 업데이트를 수동으로 업로드하고 설치해야 합니다. 먼저, 중요한 업데이트를 Firepower System에 예약할 수 없는 상황입니다. 다음으로, 지원 사이트에 액세스할 수 없는 FMC의 업데이트 또는 푸시를 예약할 수 없는 경우입니다. FMC이 직접 인터넷에 연결되어 있지 않는 경우, 관리 인터페이스 구성을 사용하여 지원 사이트에서 업데이트를 다운로드 할 수 있도록 프록시를 설정해야 합니다.

디바이스 그룹에 업데이트를 설치하도록 예약된 작업은 푸시된 업데이트를 디바이스 그룹 내의 각 디바이스에 동시에 설치합니다. 디바이스 그룹 내의 각 디바이스에 대해 예약된 작업을 완료하는 데 충분한 시간을 둡니다.

이 프로세스를 세부적으로 제어하려면 업데이트가 해제되었음을 확인한 후 **Once(**한 번에**)** 옵션을 사용하여 오프 피크 시간 동안 업데이트를 다운로드하고 설치할 수 있습니다.

관련 항목

Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지
시스템 업데이트, 179 페이지

소프트웨어 다운로드 자동화

Cisco에서 최신 소프트웨어 업데이트를 자동으로 다운로드하는 예약된 작업을 생성할 수 있습니다. 이 작업을 사용하여 수동 설치하려는 업데이트의 다운로드를 예약할 수 있습니다.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Download Latest Update(**최신 업데이트 다운로드**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Update Items(**업데이트 항목**)**옆에 있는 **Software(**소프트웨어**)** 체크 박스를 선택합니다.

단계 **7** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

소프트웨어 푸시 자동화

매니지드 디바이스에서 소프트웨어 업데이트의 설치를 자동화하려면 설치 전에 디바이스에 업데이트를 푸시해야 합니다.

매니지드 디바이스에 소프트웨어 업데이트를 푸시하기 위한 작업을 생성하는 경우, 디바이스에 업데이트를 복사할 수 있도록 푸시 작업과 예약 설치 작업 사이에 충분한 시간을 두어야 합니다.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Push Latest Update(**최신 업데이트 푸시**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Device(**디바이스**)** 드롭다운 목록에서 업데이트할 디바이스를 선택합니다.

단계 **7** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

소프트웨어 설치 자동화

업데이트를 매니지드 디바이스에 푸시하는 작업과 업데이트를 설치하는 작업 사이에 충분한 시간을 두어야 합니다.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

주의 설치되고 있는 업데이트에 따라, 소프트웨어가 설치된 후 어플라이언스가 재부팅될 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type** 목록에서 **Install Latest Update**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Device(**장치**)** 드롭다운 목록에서 업데이트를 설치하려는 어플라이언스(Firepower Management Center 포함)를 선택합니다.

단계 **7** **Update Items(**업데이트 항목**)**옆에 있는 **Software(**소프트웨어**)** 확인란을 선택합니다.

단계 **8** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **9** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

취약성 데이터베이스 업데이트 자동화

Cisco는 Firepower System에서 인식하는 네트워크 자산, 트래픽 및 취약성 목록을 확장하기 위해 VDB(취약성 데이터베이스) 업데이트를 사용합니다. 예약 기능을 사용하여 VDB를 업데이트할 수 있으며 이를 통해 최신 정보를 사용하여 네트워크의 호스트를 평가할 수 있습니다.

VDB 업데이트를 자동화할 때 두 가지 별도의 단계를 자동화해야 합니다.

- VDB 업데이트를 다운로드합니다.
- VDB 업데이트를 설치합니다.

초기 구성 중 FMC는 Cisco 지원 사이트에서 최신 취약점 데이터베이스(VDB)를 다운로드하고 설치합니다. 이 작업은 한 번만 수행하면 됩니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 시스템을 최신 상태로 유지하고자 하고 FMC가 인터넷에 액세스할 수 있다면 이 섹션.

⚠

주의 VDB 업데이트에 매니지드 디바이스에 적용되는 변경 사항이 포함된 경우, VDB를 설치한 후 첫 번째 수동 또는 예약된 구축으로 Snort 프로세스가 다시 시작되고 트래픽 검사가 중단됩니다. Firepower Threat Defense 디바이스에 대해 보류 중인 구축이 재시작된다는 경고가 구축 대화 상자 메시지에 나타납니다. 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 사용자는 Firepower Management Center에만 적용되는 VDB 업데이트를 구축할 수 없으며 재시작이 유발되지 않습니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

프로세스가 완료될 때까지 작업 간에 충분한 시간을 둡니다. 예를 들어 업데이트를 설치하기 위해 작업을 예약하는데 업데이트가 충분히 다운로드되지 않은 경우 설치 작업이 성공하지 못합니다. 그러나 예약 설치 작업이 매일 반복되면 다음 날 작업이 실행될 때 다운로드된 VDB 업데이트를 설치합니다.

참고:

- 지원 사이트에 액세스할 수 없는 어플라이언스에 대해서는 업데이트를 예약할 수 없습니다. FMC이 직접 인터넷에 연결되어 있지 않는 경우, 관리 인터페이스 구성을 사용하여 지원 사이트에서 업데이트를 다운로드 할 수 있도록 프록시를 설정해야 합니다.
- 이 프로세스를 세부적으로 제어하려면 업데이트가 해제되었음을 확인한 후 **Once(**한 번에**)** 옵션을 사용하여 오프 피크 시간 동안 VDB 업데이트를 다운로드하고 설치할 수 있습니다.
- 다중 도메인 구축에서 전역 도메인에 대한 VDB 업데이트를 예약만 할 수 있습니다. 변경 사항은 정책을 재구축할 때 적용됩니다.

관련 항목

Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지

VDB 업데이트 다운로드 자동화

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type** 목록에서 **Download Latest Update**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.

- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Update Items(**업데이트 항목**)**옆에 있는 **Vulnerability Database(**취약성 데이터베이스**)** 확인란을 선택합니다.

단계 **7** 작업에 대 한 의견 하려는 경우 설명 필드에 설명을 입력합니다.

코멘트 필드는 calendar schedule(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

VDB 업데이트 설치 자동화

VDB 업데이트를 다운로드하는 작업과 업데이트를 설치하는 작업 사이에 충분한 시간을 두십시오.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

주의 VDB 업데이트에 매니지드 디바이스에 적용되는 변경 사항이 포함된 경우, VDB를 설치한 후 첫 번째 수동 또는 예약된 구축으로 Snort 프로세스가 다시 시작되고 트래픽 검사가 중단됩니다. Firepower Threat Defense 디바이스에 대해 보류 중인 구축이 재시작된다는 경고가 구축 대화 상자 메시지에 나타납니다. 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 사용자는 Firepower Management Center에만 적용되는 VDB 업데이트를 구축할 수 없으며 재시작이 유발되지 않습니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Install Latest Update(**최신 업데이트 설치**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Device(**디바이스**)** 드롭다운 목록에서 FMC를 선택합니다.

단계 **7** **Update Items(**업데이트 항목**)**옆에 있는 **Vulnerability Database(**취약성 데이터베이스**)** 확인란을 선택합니다.

단계 **8** 작업에 대 한 의견 하려는 경우 설명 필드에 설명을 입력합니다.

팁 코멘트 필드는 페이지의 View Tasks(작업 보기) 섹션에 표시되므로 이를 상대적으로 짧게 유지하십시오.

단계 **9** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

예약된 작업을 통해 URL 필터링 업데이트 자동화

URL 필터링을 위한 위협 데이터를 최신 상태로 유지하려면 시스템이 Cisco 종합적 보안 인텔리전스(CSI) 클라우드에서 데이터 업데이트를 얻어야 합니다.

기본적으로 URL 필터링을 사용하는 경우 자동 업데이트가 활성화됩니다. 그러나 이러한 업데이트가 발생할 시기를 제어해야 하는 경우, 기본 업데이트 메커니즘 대신 이 항목에서 설명하는 절차를 사용합니다.

일일 업데이트 양이 적다고 생각될 수도 있으나, 마지막 업데이트 이후 5일 이상 경과하면 새로운 URL 필터링 데이터를 다운로드하는 데 대역폭에 따라 20분 이상이 소요될 수 있습니다. 그런 다음 업데이트 자체를 수행하는 데 30분이 걸릴 수 있습니다.

시작하기 전에

- Firepower Management Center에서 인터넷에 액세스할 수 있는지 확인합니다. 보안, 인터넷 액세스 및 통신 포트, 3107 페이지의 내용을 참조하십시오.
- URL 필터링이 활성화되었는지 확인합니다. 자세한 내용은 범주 및 평판을 사용한 URL 필터링 활성화, 1674 페이지를 참조하십시오.
- **System(**시스템**)** > **Integration(**통합**)** 메뉴 아래의 **Cloud Services**에서 **Enable Automatic Updates(**자동 업데이트 활성화**)**가 선택되어 있지 않은지 확인합니다.
- 이 작업을 수행하려면 전역 도메인에 있어야 합니다. URL 필터링 라이선스도 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Update URL Filtering Database(URL** 필터링 데이터베이스 업데이트**)**를 선택합니다.

단계 **4** 업데이트 예약 방법으로 **Once(**한 번**)** 또는 **Recurring(**반복**)**을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 246 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **7** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

예약된 작업 검토

예약된 작업을 추가한 후, 이들을 확인하고 상태를 평가할 수 있습니다. 페이지의 View Options(보기 옵션) 섹션에서는 예약된 작업의 달력 및 목록을 사용하여 예약된 작업을 확인할 수 있습니다.

Calendar(달력) 보기 옵션을 사용하면 날짜별로 발생하는 예약된 작업을 확인할 수 있습니다.

Task List(작업 목록)에는 상태와 함께 작업 목록이 표시됩니다. 달력을 열면 일정 아래에 작업 목록이 나타납니다. 또한, 달력에서 날짜 또는 작업을 선택하여 작업 목록을 볼 수 있습니다.

이전에 생성한 예약된 작업을 수정할 수 있습니다. 이 기능은 매개 변수가 올바른지 확인하기 위해 예약된 작업을 한 번 테스트하려는 경우에 특히 유용합니다. 나중에, 작업이 성공적으로 완료된 후 이를 반복 작업으로 변경할 수 있습니다.

Schedule View(일정 보기) 페이지에서 수행할 수 있는 2가지 유형의 삭제가 있습니다. 아직 실행되지 않은 특정 일회성 작업을 삭제하거나 반복 작업의 각 인스턴스를 삭제할 수 있습니다. 반복 작업의 인스턴스를 삭제할 경우, 작업의 모든 인스턴스가 삭제됩니다. 한 번 실행하도록 예약된 작업을 삭제할 경우, 해당 작업만 삭제됩니다.

작업 목록 세부 정보

표 *10:* 작업 목록 열

열	설명
이름	예약된 작업의 이름 및 관련 코멘트를 표시합니다.
유형	예약된 작업의 유형을 표시합니다.
시작 시간	예약된 시작 날짜 및 시간을 표시합니다.
빈도	작업이 실행되는 빈도를 표시합니다.
마지막 실행 시간	실제 시작 날짜 및 시간을 표시합니다. 반복 작업의 경우, 가장 최근의 실행에 적용됩니다.
마지막 실행 상태	예약된 작업의 현재 상황을 설명합니다. • 확인 표시( )는 작업이 성공적으로 실행되었음을 나타냅니다. • 물음표 아이콘(물음표( ))은 작업이 알 수 없는 상태임을 나타냅니다. • 느낌표 아이콘( )은 작업이 실패했음을 나타냅니다. 반복 작업의 경우, 가장 최근의 실행에 적용됩니다.
다음 런타임	반복 작업의 경우, 다음 실행 시간이 표시됩니다. 일회성 작업에 N/A가 표시됩니다.
생성자	예약된 작업을 생성한 사용자의 이름을 표시합니다.
수정	예약된 작업을 수정합니다.
삭제	예약된 작업을 삭제합니다.

일정표에서 예약된 작업 보기

다중 도메인 구축에서, 현재 도메인에 대해서만 예약된 작업을 볼 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.
단계 **2** 캘린더 보기를 사용하여 다음 작업을 수행할 수 있습니다.

- 이전 연도로 이동하려면 이중 왼쪽 화살표( )를 클릭합니다.
- 이전 달로 이동하려면 단일 왼쪽 화살표( )를 클릭합니다.
- 다음 달로 이동하려면 단일 오른쪽 화살표( )를 클릭합니다.
- 다음 연도로 이동하려면 이중 오른쪽 화살표( )를 클릭합니다.
- 이번 달과 연도로 돌아가려면 **Today(**오늘**)**를 클릭합니다.
- 새로운 작업을 예약하려면 **Add Task(**작업 추가**)**를 클릭합니다.
- 달력 아래의 작업 목록 표에서 특정 날짜에 예약된 모든 작업을 보려면 날짜를 클릭합니다.
- 달력 아래의 작업 목록 표에서 작업을 확인하려면 날짜에서 특정 작업을 클릭합니다.

예약된 작업 수정

다중 도메인 구축에서, 현재 도메인에 대해서만 예약된 작업을 편집할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.
단계 **2** 달력에서 편집하려는 작업 또는 작업이 표시되는 날짜를 클릭하십시오.
단계 **3** **Task Details(**작업 세부 정부**)** 테이블에서, 편집할 작업 옆에 있는 수정( )을 클릭합니다.
단계 **4** 작업을 편집합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

예약된 작업 삭제

다중 도메인 구축에서, 현재 도메인에 대해서만 예약된 작업을 삭제할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** 달력에서 삭제하려는 작업을 클릭합니다. 반복 작업의 경우, 작업의 인스턴스를 클릭합니다.

단계 **3** **Task Details(**작업 세부 사항**)** 테이블에서 삭제( )를 클릭한 후 선택 내용을 확인합니다.

예약된 작업 기록

기능	버전	세부 사항
자동으로 예약된 업데이트	6.6	신규 또는 출고 시 설정으로 새로 복원된 FMC에 대해, 초기 설정 마법사는 Cisco 지원 사이트에서 일일 침입 규칙 업데이트를 자동으로 예약합니다. FMC는 다음에 영향을 받는 정책을 구축하는 경우, 자동 침입 규칙 업데이트를 구축합니다. 수정된 화면 없음 지원되는 플랫폼: FMC
자동으로 예약된 업데이트	6.5	신규 또는 출고 시 설정으로 새로 복원된 FMC에 대해, 초기 구성 마법사는 다음을 자동으로 예약합니다. • FMC 및 매니지드 디바이스의 소프트웨어 업데이트를 다운로드하는 주간 작업 • 로컬에 저장한 구성 전용 백업을 수행하는 주간 작업입니다. 수정된 화면 없음 지원되는 플랫폼: FMC
예약된 매니지드 디바이스 원격 백업	6.4	이제 FMC를 사용하여 특정 매니지드 디바이스의 원격 백업을 예약할 수 있습니다. 이전에는 7000 및 8000 시리즈 디바이스만 예약 백업을 지원했고, 디바이스의 로컬 GUI를 사용해야 했습니다. 신규/수정된 화면: **System(**시스템**) > Tools(**도구**) > Scheduling(**예약**) >** add/edit task(작업 추가/수정) **> Job Type: Backup(**작업 유형**:** 백업**)** 선택 **> Backup Type(**백업 유형**)** 선택 지원되는 플랫폼: FTD 물리적 플랫폼, FTDv for VMware, 7000/8000 시리즈 예외: FTD 클러스터링 디바이스 또는 컨테이너 인스턴스는 지원하지 않음

11 장

데이터 스토리지

- FMC에 저장된 데이터, 269 페이지
- 외부 데이터 스토리지, 271 페이지
- 데이터 스토리지 기록, 273 페이지

FMC에 저장된 데이터

대상	확인
FMC의 데이터 스토리지에 대한 일반 정보	디스크 사용량 위젯, 373 페이지
오래된 데이터 제거	FMC 데이터베이스에서 데이터 제거, 270 페이지
FMC의 데이터에 대한 외부 액세스 허용(고급 기능)	외부 데이터베이스 액세스 설정, 1349 페이지
백업	백업 및 원격 스토리지 관리, 231 페이지 및 하위 항목
보고서	로컬 스토리지 설정, 1363 페이지
이벤트	연결 로깅, 2859 페이지 데이터베이스 이벤트 제한 수, 1350 페이지 및 하위 항목
네트워크 검색 데이터	네트워크 검색 데이터 스토리지 설정, 2556 페이지 및 후속 주제
파일	모범 사례를 포함하여 파일 정책 및 악성코드 보호, 1861 페이지에 파일을 저장하는 방법을 설명합니다. 파일 및 악성코드 탐지 성능 및 저장 조정, 1903 페이지

대상	확인
패킷 데이터	일반 설정 편집, 342 페이지
사용자 및 사용자 활동	사용자 데이터베이스, 2390 페이지 사용자 활동 데이터베이스, 2389 페이지

FMC 데이터베이스에서 데이터 제거

데이터베이스 제거 페이지를 사용하여 검색, ID, 연결 및 보안 인텔리전스 데이터 파일을 FMC 데이터베이스에서 제거할 수 있습니다. 데이터베이스를 삭제하면 해당 프로세스가 다시 시작됩니다.

⚠

주의 데이터베이스를 삭제하면 Firepower Management Center에서 지정한 데이터가 제거됩니다. 데이터를 삭제한 후에는 복구할 수 없습니다 .

시작하기 전에

데이터를 제거하려면 관리자 또는 보안 분석가 권한이 있어야 합니다. 글로벌 도메인에만 속할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Data Purge(**데이터 제거**)**을(를) 선택합니다.

단계 **2** **Discovery and Identity(**검색 및 **ID)**에서 다음 중 하나 또는 모두를 실행합니다.

- 데이터베이스에서 모든 네트워크 검색 이벤트를 제거하려면 **Network Discovery Events(**네트워크 검색 이벤트**)** 확인란을 선택합니다.
- **Hosts(**호스트**)** 확인란을 선택하여 모든 호스트 및 Indications of Compromise flags(보안 침해 플래그 표시)를 데이터베이스에서 제거합니다.
- **User Activity(**사용자 활동**)** 확인란을 선택하고 모든 사용자 활동 이벤트를 데이터베이스에서 제거합니다.
- **User Identities(**사용자 **ID)** 확인란을 선택하고 모든 사용자 로그인 및 사용자 기록 데이터 를 데이터베이스에서 제거합니다.

단계 **3** **Connections(**연결**)** 아래에서 다음 중 하나 또는 모두를 실행합니다.

- **Connection Events(**연결 이벤트**)** 확인란을 선택하고 모든 연결 데이터를 데이터베이스에서 제거합니다.
- **Connection Summary Events(**연결 요약 이벤트**)** 확인란을 선택하고 모든 연결 요약 데이터를 데이터베이스에서 제거합니다.

- **Security Intelligence Events(**보안 인텔리전스 이벤트**)** 확인란을 선택하고 모든 보안 인텔리전스 데이터를 데이터베이스에서 제거합니다.

참고 **Connection Events(**연결 이벤트**)** 확인란을 선택해도 보안 인텔리전스 이벤트는 제거되지 않습니다. 보안 인텔리전스 데이터와의 연결은 계속 보안 인텔리전스(Security Intelligence) 이벤트 페이지에 나타납니다(Analysis(분석)> Connections(연결) 메뉴 하단) 따라서 **Security Intelligence Events(**보안 인텔리전스 이벤트**)** 확인란을 선택해도 보안 인텔리전스 데이터 관련 연결 이벤트는 제거되지 않습니다.

단계 **4** **Purge Selected Events(**선택된 이벤트 제거**)**를 클릭합니다.
항목이 삭제되고 해당 프로세스가 다시 시작됩니다.

외부 데이터 스토리지

선택적으로 원격 데이터 스토리지를 사용하여 특정 유형의 데이터를 저장할 수 있습니다.

대상	확인
백업	백업 및 원격 스토리지 관리, 231 페이지 및 하위 항목 원격 스토리지 관리, 1363 페이지 및 하위 항목
보고서	원격 스토리지 관리, 1363 페이지 및 하위 항목 원격 스토리지로 보고서 이동, 2677 페이지
Events(이벤트)	시스템 로그 및 기타 리소스에 대한 정보 외부 툴을 사용하여 이벤트 분석, 2749 페이지 Stealthwatch 클라우드의 원격 데이터 스토리지, 272 페이지 Stealthwatch 어플라이언스의 원격 데이터 스토리지, 273 페이지 연결 이벤트를 원격으로 저장하는 경우, FMC에서 연결 이벤트 스토리지를 비활성화하는 것이 좋습니다. 자세한 정보는 데이터베이스 이벤트 제한 수, 1350 페이지 및 하위 주제를 참조하십시오.

중요 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

Cisco Security Analytics and Logging 원격 이벤트 스토리지 옵션 비교

다음은 이벤트 데이터를 외부적으로 Firepower Management Center에 저장하는 비슷하지만, 다른 옵션입니다.

온프레미스	**SaaS**
방화벽 뒤에서 스토리지 시스템을 구매, 라이선싱, 설정합니다.	라이선스 및 데이터 스토리지 요금제를 구매하고 Cisco 클라우드로 데이터를 전송합니다.
지원되는 이벤트 유형: • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드	지원되는 이벤트 유형: • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드
시스템 로그를 통해 이벤트를 스토리지로 전송합니다.	시스템 로그를 통해 이벤트를 스토리지로 전송합니다.
Stealthwatch Management Console 어플라이언스를 사용하여 이벤트를 확인합니다. FMC 이벤트 뷰어에서 크로스 실행합니다.	라이선스에 따라 CDO 또는 Stealthwatch의 이벤트를 확인합니다. FMC 이벤트 뷰어에서 교차 실행합니다.
자세한 내용은 Stealthwatch 어플라이언스의 원격 데이터 스토리지, 273 페이지의 링크를 참조하십시오.	자세한 내용은 Stealthwatch 클라우드의 원격 데이터 스토리지, 272 페이지의 링크를 참조하십시오.

Stealthwatch 클라우드의 원격 데이터 스토리지

Cisco Security Analytics and Logging(SaaS) 을(를) 사용하여 선택한 Firepower 이벤트 데이터를 시스템 로그를 통해 Stealthwatch 클라우드로 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다.

자세한 내용은 https://cisco.com/go/firepower-sal-saas-integration-docs에 있는 *Firepower Management Center* 및 *Cisco SaaS(Security Analytics and Logging)* 통합 가이드를 참조하십시오

중요 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

Stealthwatch 어플라이언스의 원격 데이터 스토리지

Firepower 어플라이언스가 제공할 수 있는 것보다 더 많은 데이터 스토리지가 필요한 경우, Cisco Security Analytics 및 로깅(온프레미스) 을 사용하여 Firepower 데이터를 Stealthwatch 어플라이언스에 저장할 수 있습니다. 자세한 내용은 https://cisco.com/go/sal-on-prem-docs에서 확인 가능한 설명서를 참조하십시오.

또는 FMC의 이벤트에서 Stealthwatch의 관련 이벤트로 빠르게 피벗하려면 다음에 대한 교차 실행 링크 설정 Stealthwatch, 2754 페이지 및 상황별 크로스 실행을 이용한 이벤트 조사, 2753 페이지의 내용을 참조하십시오.

중요 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

데이터 스토리지 기록

기능	버전	세부 사항
Stealthwatch 어플라이언스의 원격 데이터 스토리지	6.7	이제 Cisco Security Analytics 및 로깅(온프레미스) 을 사용하여 대량의 Firepower 이벤트 데이터를 원격으로 저장할 수 있습니다. FMC에서 이벤트를 볼 때 신속하게 교차 실행을 수행하여 원격 데이터 스토리지 위치에서 이벤트를 확인할 수 있습니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다. 이벤트는 시스템 로그를 사용하여 전송됩니다. 이 솔루션은 SWE(Stealthwatch Enterprise) 버전 7.3을 실행하는 SMC(Stealthwatch Management Console) 가상 버전의 사용 가용성에 따라 달라집니다. Stealthwatch 어플라이언스의 원격 데이터 스토리지, 273 페이지의 내용을 참조하십시오.

기능	버전	세부 사항
Stealthwatch 클라우드의 원격 데이터 스토리지	6.4	시스템 로그를 사용하여 Cisco Security Analytics and Logging(SaaS) 을 통해 선택한 Firepower 데이터를 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다. 자세한 내용은 다음에 있는 *Firepower Management Center* 및 *Cisco SaaS(Security Analytics and Logging)* 통합 가이드를 참조하십시오. https://cisco.com/go/firepower-sal-saas-integration-docs

12 장

Firepower Management Center 고가용성

다음 주제에서는 Cisco Firepower Management Center의 액티브/스탠바이 고가용성 구성 방법을 설명합니다.

- Firepower Management Center 고가용성 정보, 275 페이지
- Firepower Management Center 고가용성을 위한 요구 사항, 281 페이지
- Firepower Management Center 고가용성을 설정하기 위한 사전 요건, 283 페이지
- Firepower Management Center 고가용성 설정, 284 페이지
- Firepower Management Center 고가용성 상태 보기, 285 페이지
- Firepower Management Center 고가용성 쌍에서 동기화된 설정, 286 페이지
- Firepower Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인, 287 페이지
- Firepower Management Center 고가용성 쌍에서 피어 전환, 287 페이지
- 페어링된 Firepower Management Center 간 커뮤니케이션 일시 중지, 288 페이지
- 페어링된 Firepower Management Center 간 통신 재시작, 288 페이지
- 고가용성 쌍의 Firepower Management Center IP 주소 변경, 289 페이지
- Firepower Management Center 고가용성 비활성화, 289 페이지
- 고가용성 쌍의 FMC 교체, 290 페이지
- FMC 고가용성 히스토리, 294 페이지

Firepower Management Center 고가용성 정보

운영 연속성을 보장하기 위해 고가용성 기능을 사용하면 이중 Firepower Management Center를 지정하고 디바이스를 관리할 수 있습니다. Firepower Management Center는 한 개의 어플라이언스가 액티브 유닛으로 디바이스를 관리하는 Active/Standby(액티브/스탠바이) 고가용성을 지원합니다. 스탠바이 유닛은 디바이스를 활동적으로 관리하지 않습니다. 액티브 유닛은 구성 데이터를 데이터 저장소로 기록하고 두 유닛 모두에 대해 데이터를 복제하며 필요한 경우 동기화를 사용하여 스탠바이 유닛과 정보를 공유합니다.

Active/Standby(액티브/스탠바이) 고가용성을 사용하면 보조 Firepower Management Center을 구성하고 장애가 발생한 경우 기본 Firepower Management Center의 기능을 대체합니다. 기본 Firepower Management Center에 장애가 발생하는 경우 보조 Firepower Management Center을 승격하여 액티브 유닛으로 만들 수 있습니다.

이벤트 데이터는 매니지드 디바이스에서 고가용성 쌍에 있는 Firepower Management Center 모두로 흐릅니다. 한 Firepower Management Center가 실패하면 다른 Firepower Management Center를 사용하여 중단 없이 네트워크를 모니터링할 수 있습니다.

참고로 고가용성 쌍으로 구성된 Firepower Management Center는 신뢰할 수 있는 동일한 관리 네트워크에 있어야 할 필요가 없으며 동일한 지리적 위치에 있어야 할 필요도 없습니다.

⚠

주의 시스템이 일부 기능을 기본 Firepower Management Center로 제한하므로 해당 어플라이언스가 실패하면 스탠바이 Firepower Management Center를 액티브로 승격해야 합니다.

원격 액세스 **VPN** 고가용성에 대한 정보

기본 디바이스에 Remote Access(원격 액세스) VPN 구성과 CertEnrollment 개체로 등록한 ID 인증서가 있는 경우, 보조 디바이스에 동일한 CertEnrollment 개체로 등록한 ID 인증서가 있어야 합니다. CertEnrollment 개체는 디바이스별 재정의로 인해 기본 및 보조 디바이스에 대해 서로 다른 값을 가질 수 있습니다. 고가용성 형성 하기 전에 두 개의 디바이스를 등록 하는 동일한 CertEnrollment 개체에만 개로 제한이 됩니다.

Firepower Management Center 고가용성의 역할 및 상태 비교

기본/보조 역할

Firepower Management Center의 고가용성 쌍을 설정할 때 한 Firepower Management Center를 기본, 다른 하나를 보조로 구성합니다. 컨피그레이션 중에는 기본 유닛의 정책이 보조 유닛에 동기화됩니다. 동기화가 끝나면 기본 Firepower Management Center은 액티브 피어가 되고 보조 Firepower Management Center는 보조 피어로 두 유닛이 매니지드 디바이스 및 정책 설정에 단일 어플라이언스로 작동합니다.

액티브/스탠바이 상태

고가용성 쌍에서 두 Firepower Management Center의 가장 큰 차이는 액티브 및 스탠바이 피어와 관련이 있습니다. 액티브 Firepower Management Center는 모든 기능을 사용할 수 있으며 디바이스와 정책을 관리할 수 있습니다. 스탠바이 Firepower Management Center는 기능이 숨겨져 있으며 설정 변경을 할 수 없습니다.

Firepower Management Center 고가용성 쌍의 이벤트 처리

고가용성 쌍의 두 Firepower Management Center가 관리된 디바이스에서 이벤트를 수신하므로 어플라이언스용 관리 IP 주소를 공유하지 않습니다. 즉 Firepower Management Center에 오류가 발생하는 경우 이벤트를 지속적으로 처리하기 위해 개입할 필요가 없습니다.

AMP 클라우드 연결 및 악성코드 정보

이들은 파일 정책 및 관련 컨피그레이션을 공유하지만 고가용성 쌍의 Firepower Management Center과 Cisco AMP Cloud 연결과 악성코드 성향을 공유하지 않습니다. 운영 연속성을 보장하고 탐지된 파일의 악성코드 속성이 두 Firepower Management Center및 기본과 보조 Firepower Management Center에 동일하려면 AMP 클라우드에 대한 액세스 권한이 있어야 합니다.

URL 필터링 및 보안 인텔리전스

URL 필터링과 보안 인텔리전스의 설정 및 정보는 고가용성 구축에서 Firepower Management Center 간에 동기화됩니다. 그러나 기본 Firepower Management Center만 URL 카테고리 및 평판 데이터 그리고 보안 인텔리전스 피드에 대한 업데이트를 다운로드합니다.

기본 Firepower Management Center에 장애가 발생하면 위협 인텔리전스 데이터 업데이트를 위해 보조 Firepower Management Center가 인터넷에 액세스할 수 있는지 확인하고 보조 Firepower Management Center의 웹 인터페이스를 사용해 액티브로 전환합니다.

Firepower Management Center 페일오버 중에 사용자 데이터 처리

기본 Firepower Management Center에 장애가 발생하면 보조 Firepower Management Center가 TS Agent 소스. ID 소스로 아직 확인되지 않은 사용자는 알 수 없음으로 식별됩니다.

다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.

Firepower Management Center 고가용성 쌍의 구성 관리

고가용성 구축에서 액티브 Firepower Management Center만 디바이스를 관리하고 정책을 적용할 수 있습니다. 두 Firepower Management Center 모두 지속적인 동기화 상태를 유지합니다.

액티브 Firepower Management Center에 오류가 발생하는 경우 고가용성 쌍은 사용자가 수동으로 스탠바이 어플라이언스를 액티브 상태로 승격할 때까지 저하 상태에 돌입합니다. 승격이 완료되면 어플라이언스는 유지 관리 모드 상태가 됩니다.

Cisco Threat Intelligence Director(TID) 및 고가용성 구성

고사용성 구성인 액티브 Firepower Management Center에서 TID을 호스팅하는 경우, 시스템은 TID 설정과 TID 데이터를 스탠바이 Firepower Management Center에 동기화하지 않습니다. 페일오버 후 데이터를 복구할 수 있도록 액티브 Firepower Management Center에서 정기적인 TID 데이터 백업을 수행하는 것을 권장합니다.

자세한 내용은 TID 데이터 백업 및 복구 정보, 1923 페이지를 참조하십시오.

SSO 및 고가용성 쌍

FMC고가용성 설정의 FMC는 SSO(Single Sign-On, 단일 인증)를 지원할 수 있지만, 다음 사항을 고려해야 합니다.

- SSO 설정은 고가용성 쌍의 멤버 간에 동기화되지 않습니다. 쌍의 각 멤버에서 SSO를 별도로 설정해야 합니다.
- 고가용성 쌍의 두 FMC는 모두 SSO에 동일한 ID 공급자(IdP)를 사용해야 합니다. SSO에 대해 설정된 각 FMC의 IdP에서 서비스 제공자 애플리케이션을 설정해야 합니다.
- 둘 다 SSO를 지원하도록 설정된 FMC 고가용성 쌍에서는 사용자가 SSO를 사용하여 보조 FMC에 처음으로 액세스하기 전에 먼저 사용자가 SSO를 통해 기본 FMC에 한 번 이상 로그인해야합니다.
- 고가용성 쌍에서 FMC에 대해 SSO를 설정하는 경우:
  - 기본 FMC에서 SSO를 설정하는 경우, 보조 FMC에서 SSO를 설정할 필요가 없습니다.
  - 보조 FMC에서 SSO를 설정하는 경우, 기본 FMC에서도 SSO를 설정해야 합니다. (SSO 사용자는 보조 FMC에 로그인하기 전에 기본 FMC에 한 번 이상 로그인해야 하기 때문입니다.)

관련 항목

SAML SSO(Single Sign-On) 구성, 74 페이지

Firepower Management Center 백업 중에 고가용성 동작

Firepower Management Center 고가용성 쌍에서 백업을 수행할 경우 백업 작업은 피어 간 동기화를 일시 중지합니다. 이 작업을 수행하는 동안 액티브 Firepower Management Center을 계속 사용할 수 있지만 스탠바이 피어는 사용할 수 없습니다.

백업이 완료되면 동기화가 재시작되어 액티브 피어의 프로세스를 일시적으로 비활성화합니다. 이 일시 중지 상태에 고가용성 페이지는 모든 프로세스가 다시 시작될 때까지 일시적으로 보류 페이지를 표시합니다.

Firepower Management Center 고가용성 스플릿 브레인

고가용성 쌍에서 액티브 Firepower Management Center이 중단(전원 문제, 네트워크/연결 문제)되는 경우 스탠바이 Firepower Management Center를 액티브 상태로 승격시킵니다. 원래 액티브 피어가 복구되면 두 피어 모두 액티브 상태로 간주할 수 있습니다. 이 상태를 '스플릿 브레인' 상태라고 합니다. 이러한 상황이 발생하면 시스템은 액티브 어플라이언스를 선택하고 다른 어플라이언스를 스탠바이로 전환하도록 합니다.

액티브 Firepower Management Center이 중단(또는 네트워크 오류로 연결 끊기)되는 경우 고가용성 또는 스위치 역할을 중단할 수 있습니다. 스탠바이 Firepower Management Center는 성능 저하 상태에 진입합니다.

참고 스플릿 브레인을 해결하면 보조로 사용하는 어플라이언스의 모든 디바이스 등록 및 정책 설정이 손실됩니다. 예를 들어 보조에 존재하던 정책 수정 내용을 전부 잃지만 기본에 있던 것은 보존됩니다. Firepower Management Center이 두 어플라이언스가 액티브 상태인 고가용성 스플릿 브레인 시나리오에 돌입하고 스플릿 브레인을 해소하기 전에 관리되는 디바이스를 등록하고 정책을 구축하는 경우 모든 정책을 내보내고 관리되는 디바이스를 새 고가용성이 재구성되기 전에 해당 스탠바이 Firepower Management Center에서 등록 해제해야 합니다. 그런 다음 액티브 Firepower Management Center에서 관리되는 디바이스를 등록하고 정책을 가져올 수 있습니다.

고가용성 쌍의 Firepower Management Center 업그레이드

Cisco는 온라인으로 다양한 유형의 업데이트를 주기적으로 배포합니다. 시스템 소프트웨어의 주요 및 사소한 업그레이트를 포함합니다. 고가용성 설정에서 Firepower Management Center에 이런 업데이트를 설치해야 할 수 있습니다.

경고! 업그레이드 중 하나 이상의 운영 Firepower Management Center이 있는지 확인하십시오.

시작하기 전에

업그레이드와 함께 배포된 릴리스 노트 또는 권고 사항을 읽습니다. 릴리스 정보에는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보가 제공됩니다.

프로시저

단계 **1** 액티브 Firepower Management Center의 웹 인터페이스에 액세스하고 데이터 동기화를 중단시키려면 페어링된 Firepower Management Center 간 커뮤니케이션 일시 중지, 288 페이지를 참조하십시오.

단계 **2** 스탠바이 Firepower Management Center을 업그레이드하려면 소프트웨어 업데이트 Firepower Management Center를 참조하십시오.
업그레이드가 완료되면 스탠바이 유닛이 액티브상태가 됩니다. 두 피어가 액티브인 경우 고가용성 쌍은 저하(스플릿 브레인) 상태가 됩니다.

단계 **3** 다른 Firepower Management Center을 업그레이드합니다.

단계 **4** 어떤 Firepower Management Center을 스탠바이로 사용할지 결정합니다. 동기화가 중지된 뒤 스탠바이에 추가된 모든 추가 장치 또는 정책은 액티브 Firepower Management Center에 동기화되지 않습니다. 이러한 추가 디바이스만 등록을 취소하고 유지하려는 설정을 내보냅니다.

새 액티브 Firepower Management Center을 선택한 경우 보조로 지정한 Firepower Management Center는 디바이스 등록 및 동기화되지 않은 정책 설정 구축을 잃게 됩니다.

단계 **5** 정책 및 디바이스의 최신 요구 설정이 있는 새 액티브 Firepower Management Center을 선택하여 스플릿 브레인을 해결합니다.

Firepower Management Center 고가용성 문제 해결

이 섹션에서는 Firepower Management Center 고가용성 운영 오류에 대한 일반적인 정보를 설명합니다.

오류	설명	해결책
대기 모드로 로그인하기 전에 액티브 Firepower Management Center에서 비밀번호를 재설정해야 합니다.	계정에 강제 비밀번호 재설정이 활성화된 상태에서 대기 FMC에 로그인하려 했습니다.	데이터베이스가 대기 FMC에 대해 읽기 전용이므로, 액티브 FMC의 로그인 페이지에서 비밀번호를 재설정해야 합니다.
500 내부	피어 역할 전환이나 동기화 중지 또는 재개 등 중요한 Firepower Management Center 고가용성 작업을 수행하는 동안 웹 인터페이스 접속을 시도할 때 표시될 수 있습니다.	작업이 완료되기를 기다린 뒤 웹 인터페이스를 사용합니다.
시스템 프로세스가 시작 중이니 기다려 주시기 바랍니다. 웹 인터페이스가 응답하지 않을 수 있습니다.	이는 고가용성 또는 데이터 동기화 중 Firepower Management Center이 재부팅될 때(수동 또는 전원 복구 중) 표시될 수 있습니다.	1. Firepower Management Center 셸에 액세스하여 `manage_hadc.pl` 명령을 사용해 Firepower Management Center 고가용성 구성 유틸리티에 액세스합니다. 참고 `sudo`를 사용하여 루트 사용자로 우틸리트를 실행합니다. 2. 옵션 5를 사용하여 미러링 작업을 일시 중지합니다. Firepower Management Center 웹 인터페이스를 재로딩합니다. 3. 웹 인터페이스를 사용하여 동기화를 다시 시작합니다. 시스템 > 통합을 선택하고 고가용성 탭을 클릭한 다음, 재시작 동기화를 선택합니다.

Firepower Management Center 고가용성을 위한 요구 사항

모델 지원

하드웨어 요구 사항, 281 페이지의 내용을 참조하십시오.

가상 모델 지원

가상 플랫폼 요건, 281 페이지의 내용을 참조하십시오.

지원되는 도메인

글로벌

사용자 역할

관리자

하드웨어 요구 사항

- 지원되는 하드웨어 모델:

  MC1500, MC2000, MC3500, MC4000

- 고가용성 설정의 두 Firepower Management Center은 동일한 모델이어야 합니다.
- 기본 Firepower Management Center 백업은 보조 Firepower Management Center에 복원하지 않아야 합니다.
- 대역폭 요구 사항: 두 Firepower Management Center 간 고가용성 설정을 구성하려면 최소 5Mbps 네트워크 대역폭이 확보되어야 합니다.
- 고가용성 설정의 두 Firepower Management Center가 서로 다른 데이터 센터에서 물리적 및 지리적으로 서로 분리되어 있을 수 있습니다.
- FMC 고가용성 설정에 대한 라이선스 요구 사항, 282 페이지도 참조하십시오.

가상 플랫폼 요건

두 개의 FMCv 가상 어플라이언스를 사용하여 고가용성(HA)을 설정하기 위한 요구 사항:

- FMCv는 VMware ESXi에서 실행 중이어야 합니다.
- FMCv-HA는 FMCv 10, 25 및 300에서 지원됩니다.
- 고가용성 설정의 두 FMCv 가상 어플라이언스는 동일한 디바이스 관리 용량을 가져야 합니다. 예를 들어, FMCv 25를 FMCv 300과 페어링할 수 없습니다.

- 고가용성 라이선싱 요건은 가상 FMC와 하드웨어 FMC에 따라 다릅니다. FMC 고가용성 설정에 대한 라이선스 요구 사항, 282 페이지의 내용을 참조하십시오.

소프트웨어 요구 사항

소프트웨어 버전, 침입 규칙 업데이트 버전, 취약성 데이터베이스 업데이트를 확인하려면 어플라이언스 정보 위젯에 액세스합니다. 이 위젯은 기본적으로 **Detailed Dashboard(**상세 대시보드**)** 및 **Summary Dashboard(**요약 대시보드**)**의 **Status(**상태**)** 탭에 나타납니다. 자세한 내용은 어플라이언스 정보 위젯, 367 페이지을 참조해 주십시오.

- 고가용성 구성의 두 Firepower Management Center는 주(첫 번째 번호), 부(두 번째 번호), 유지 보수(세 번째 번호) 소프트웨어 버전이 동일해야 합니다.
- 고가용성 구성의 두 Firepower Management Center에는 동일한 침입 규칙 업데이트가 설치되어 있어야 합니다.
- 고가용성 구성의 두 Firepower Management Center에는 동일한 취약성 데이터베이스 업데이트가 설치되어 있어야 합니다.
- 고가용성 구성의 두 Firepower Management Center에는 동일한 버전의 LSP(Lightweight Security Package)가 설치되어 있어야 합니다.

경고! 두 Firepower Management Center의 소프트웨어 버전, 침입 규칙 업데이트 버전, 취약성 데이터베이스 업데이트 버전이 동일하지 않은 경우 고가용성을 설정할 수 없습니다.

FMC 고가용성 설정에 대한 라이선스 요구 사항

하드웨어 **Firepower Management Center:** 모든 라이선스 유형

고가용성 쌍의 Firepower Management Center 하드웨어 어플라이언스에 필요한 특별한 라이선스는 없습니다.

고가용성 설정의 Firepower Management Center 하드웨어 어플라이언스로 관리되는 디바이스에는 동일한 수의 기능 라이선스 및 단일 Firepower Management Center 하드웨어 어플라이언스로 관리되는 디바이스인 서브스크립션이 요구됩니다.

특정 라이선스 예약 구축에서는 기본 FMC에서만 특정 라이선스 예약이 요구됩니다.

고가용성 페어가 구성되어 시스템이 자동으로 모든 기능 라이선스를 활성에서 스탠바이 Firepower Management Center로 복제하고 데이터 동기화 중 라이선스 변경을 업데이트하면, 페일오버에서 라이선스를 사용할 수 있습니다.

가상 **Firepower Management Center(FMCv):** 모든 라이선싱 유형

동일하게 라이선스가 부여된 FMCv 2개가 필요합니다(매니지드 디바이스 10개, 25개 또는 300개에 대한 엔타이틀먼트 포함).

예: 10개의 FTD 디바이스와 3개의 NGIPS 디바이스를 관리하는 FMCv 고가용성 쌍의 경우, 다음이 필요합니다.

- FMCv25 엔타이틀먼트 2개
- 아래 스마트 라이선싱에 설명된 대로 10개의 FTD 엔타이틀먼트
- 아래 클래식 라이선싱에 설명된 대로 3개의 NGIPS 엔타이틀먼트

고가용성 쌍을 분리하면 보조 FMCv와 연결된 FMCv 엔타이틀먼트가 해제됩니다. (이 예에서는 두 개의 독립형 FMCv25를 사용합니다.)

Classic Licensing

각 디바이스에는 단일 FMC 또는 고가용성 쌍(하드웨어 또는 가상)의 FMC로 관리되는 동일한 라이선스가 필요합니다.

예: Firepower Management Center 쌍으로 관리되는 두 8000 Series 디바이스에 대해 고급 악성코드 차단를 활성화하고 싶은 경우, 2개의 악성코드 라이선스와 TAM 서브스크립션을 구매하고 라이선스를 Firepower Management Center에 추가하고 두 8000 Series 기기의 라이선스를 액티브 Firepower Management Center에 할당합니다.

Firepower Management Center 고가용성을 설정하기 위한 사전 요건

설정 하기 전에 Firepower Management Center 고가용성 쌍:

- 해당 보조 Firepower Management Center에서 해당 기본 Firepower Management Center에서 필요한 정책 내보내기 자세한 내용은 컨피그레이션 내보내기, 240 페이지를 참고하십시오.
- 해당 보조 Firepower Management Center에 추가 장치가 부착되어 있지 않은지 확인하십시오. 해당 보조 Firepower Management Center에서 디바이스를 삭제하고 해당 기본 Firepower Management Center에 디바이스를 등록합니다. 자세한 정보는 FMC에서 디바이스 삭제, 315 페이지 및 FMC에 디바이스 추가, 311 페이지를 참조하십시오.
- 해당 기본 Firepower Management Center에 정책을 가져옵니다. 자세한 내용은 컨피그레이션 가져오기, 240 페이지를 참고하십시오.
- 해당 기본 Firepower Management Center에서 가져온 정책을 확인하고, 필요한 경우 편집하고, 적절한 장치에 구축합니다. 자세한 내용은 컨피그레이션 변경 사항 구축, 498 페이지를 참고하십시오.
- 해당 기본 Firepower Management Center에 새로 추가된 디바이스에 적절한 라이선스를 연결합니다. 자세한 내용은 디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당, 170 페이지를 참조하십시오.

이제 고가용성 설정을 위한 진행이 가능합니다. 자세한 내용은 Firepower Management Center 고가용성 설정, 284 페이지를 참고하십시오.

Firepower Management Center 고가용성 설정

고가용성 설정에는 피어 간 대역폭 및 정책 수에 따라 최대 몇 시간까지 상당한 시간이 걸릴 수 있습니다. 또한 스탠바이 Firepower Management Center에 동기화되어야 하는 액티브 Firepower Management Center에 등록된 디바이스 수에 따라 다릅니다. 고가용성 피어의 상태를 확인하기 위해 고가용성 페이지를 볼 수 있습니다.

시작하기 전에

- 모든 Firepower Management Center이 고가용성 시스템 요구 사항을 준수하는지 확인하십시오. 자세한 내용은 Firepower Management Center 고가용성을 위한 요구 사항, 281 페이지를 참조하십시오.
- 고가용성을 설정하기 위한 전제 조건을 완료하였는지 확인합니다. 자세한 내용은 Firepower Management Center 고가용성을 설정하기 위한 사전 요건, 283 페이지를 참고하십시오.

프로시저

단계 **1** 보조로 지정하려는 Firepower Management Center에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 이 Firepower Management Center의 역할에서 보조를 선택합니다.

단계 **5** 기본 **Firepower Managememt Center** 호스트 텍스트 상자에서 기본 Firepower Management Center의 호스트 이름 또는 IP 주소를 입력합니다.

기본 Firepower Management Center에 피어 FMC(공용 또는 프라이빗 IP 주소일 수 있음)에서 연결할 수 있는 IP 주소가 없는 경우에는 비워 둘 수 있습니다. 이 경우 등록 키와 고유 **NAT ID** 필드를 모두 사용하십시오. HA 연결을 활성화하려면 하나 이상의 FMC에 대한 IP 주소를 지정해야 합니다.

단계 **6** 등록 키 텍스트 상자에서 일회용 등록 키를 입력합니다.

등록 키는 최대 37자의 사용자가 정의한 영숫자 값입니다. 이 등록 키는 보조 및 기본 Firepower Management Center을 등록할 때 사용합니다.

단계 **7** 기본 IP 주소를 지정하지 않거나 기본 Firepower Management Center에서 보조 IP 주소를 지정하지 않을 경우 고유 **NAT ID** 필드에서 고유의 영숫자 ID를 입력합니다. 자세한 내용은 NAT 환경, 1355 페이지를 참조하십시오.

단계 **8** **Register(**등록**)**를 클릭합니다.

단계 **9** Admin 액세스 권한이 있는 계정을 사용하여 기본으로 지정할 Firepower Management Center에 로그인합니다.

단계 **10** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **11** 고가용성을 선택합니다.

단계 **12** 이 Firepower Management Center의 역할에서 기본을 선택합니다.

단계 **13** 보조 **Firepower Managememt Center** 호스트 텍스트 상자에서 보조 Firepower Management Center의 호스트 이름 또는 IP 주소를 입력합니다.

보조 Firepower Management Center에 피어 FMC(공용 또는 프라이빗 IP 주소일 수 있음)에서 연결 가능한 IP 주소가 없는 경우에는 비워 둘 수 있습니다. 이 경우 등록 키와 고유 **NAT ID** 필드를 모두 사용하십시오. HA 연결을 활성화하려면 하나 이상의 FMC에 대한 IP 주소를 지정해야 합니다.

단계 **14** 6단계에서 사용한 것과 동일한 1회용 등록 키를 등록 키 텍스트 상자에 입력합니다.

단계 **15** 필요한 경우 고유 **NAT ID** 텍스트 상자에 7단계에서 사용한 것과 동일한 NAT ID를 입력합니다.

단계 **16** **Register(**등록**)**를 클릭합니다.

다음에 수행할 작업

Firepower Management Center 고가용성 쌍을 설정한 후 액티브 Firepower Management Center에 등록된 디바이스는 자동으로 스탠바이 Firepower Management Center에 등록됩니다.

참고 등록된 디바이스에 NAT IP 주소가 있는 경우 자동 디바이스 등록이 실패하고 보조 Firepower Management Center의 고가용성 페이지가 디바이스를 로컬, 보류중으로 표시합니다. 스탠바이 Firepower Management Center 고가용성 페이즈에 표시된 디바이스에 다른 NAT IP 주소를 할당할 수 있습니다. 자동 등록이 스탠바이 Firepower Management Center에 실패하지만 디바이스가 액티브 Firepower Management Center에 등록된 것으로 표시되는 경우 Firepower Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인, 287 페이지를 참조합니다.

Firepower Management Center 고가용성 상태 보기

액티브 및 스탠바이 Firepower Management Center을 확인한 후 로컬 Firepower Management Center와 해당 피어에 대한 정보를 볼 수 있습니다.

참고 이때 로컬 피어는 시스템 상태를 확인하는 어플라이언스를 가리킵니다. 원격 피어는 액티브 또는 스탠바이 상태에 관계없이 다른 어플라이언스를 가리킵니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 Firepower Management Center 중 하나에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

다음을 볼 수 있습니다.

요약 정보

- 고가용성 쌍의 상태
- 고가용성 쌍의 현재 동기화 상태
- 액티브 피어의 IP 주소와 최근 동기화 시간
- 스탠바이 피어의 IP 주소와 최근 동기화 시간

시스템 상태

- 두 피어의 IP 주소
- 두 피어의 운영 체제
- 두 피어의 소프트웨어 버전
- 두 피어의 어플라이언스 모델

Firepower Management Center 고가용성 쌍에서 동기화된 설정

두 Firepower Management Center 사이에 고가용성을 설정하면 다음 설정 데이터가 동기화됩니다.

- 라이선스 등록
- 액세스 제어 정책
- 침입 규칙
- 악성코드 및 파일 정책
- DNS 정책
- ID 정책
- SSL 정책
- 사전 필터 정책
- 네트워크 검색 규칙
- 애플리케이션 탐지기
- 상관 관계 정책 규칙
- 알림
- 스캐너

- 응답 그룹
- 조사 이벤트에 대한 외부 리소스의 상황별 교차 실행
- 보안정책 교정 설정을 위해 두 Firepower Management Center에 사용자 정의 모듈을 설치해야 합니다. 보안정책 교정 설정에 대한 자세한 내용은 교정 모듈 관리, 2646 페이지를 참조하십시오.

Firepower Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인

스탠바이 Firepower Management Center에 자동 디바이스 등록이 실패하지만 액티브 Firepower Management Center로 등록된 경우 다음 단계를 완료합니다.

경고! 보조 Firepower Management Center RMA를 수행하거나 보조 Firepower Management Center를 추가하는 경우, 관리 대상 FTD가 등록 취소되므로 해당 설정이 삭제될 수 있습니다.

프로시저

단계 **1** 액티브 Firepower Management Center에서 디바이스를 등록 취소합니다.

단계 **2** 영향을 받는 디바이스의 CLI에 로그인합니다.

단계 **3** CLI 명령을 실행합니다. **configure manager delete**.

이 명령은 현재 Firepower Management Center을 비활성화하고 제거합니다.

단계 **4** CLI 명령을 실행합니다. **configure manager add**.

이 멸영은 Firepower Management Center에 연결하기 위한 디바이스를 구성합니다.

팁 액티브 Firepower Management Center에 한해 디바이스의 원격 관리를 구성합니다. 고가용성이 구성되면 디바이스는 자동으로 스탠바이 Firepower Management Center에 의해 관리되도록 추가됩니다.

단계 **5** 액티브 Firepower Management Center에 로그인하고 디바이스를 등록합니다.

Firepower Management Center 고가용성 쌍에서 피어 전환

시스템이 일부 기능을 액티브 Firepower Management Center로 제한하므로 해당 어플라이언스가 실패하면 스탠바이 Firepower Management Center를 액티브로 승격해야 합니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 Firepower Management Center 중 하나에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 액티브를 스탠바이로, 스탠바이를 액티브로 로컬 역할을 변경하려면 피어 역할 전환을 선택합니다. 그러면 기본 또는 보조 지정은 변경되지 않은 채 두 피어 간 역할이 전환됩니다.

페어링된 **Firepower Management Center** 간 커뮤니케이션 일시 중지

일시적으로 고가용성을 비활성화하려는 경우 Firepower Management Center 간의 통신 채널을 비활성화할 수 있습니다. 액티브 피어에서 동기화를 중단하면 액티브 또는 스탠바이 피어 중 하나에서 동기화를 재개할 수 있습니다. 그러나 스탠바이 피어의 동기화를 중단하면 스탠바이 피어에서만 동기화를 재개할 수 있습니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 Firepower Management Center 중 하나에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 동기화 일시 정지를 선택합니다.

페어링된 **Firepower Management Center** 간 통신 재시작

일시적으로 고가용성을 비활성화하려는 경우 Firepower Management Center 간 통신 채널을 활성화하여 고가용성을 재시작할 수 있습니다. 액티브 유닛에서 동기화를 중단한 경우 스탠바이 또는 액티브 유닛 모두에서 동기화를 재개할 수 있습니다. 그러나 스탠바이 유닛의 동기화를 중단하면 스탠바이 유닛에서만 동기화를 재개할 수 있습니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 Firepower Management Center 중 하나에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 동기화 재개를 선택합니다.

고가용성 쌍의 Firepower Management Center IP 주소 변경

참고 7000 및 8000 Series 관리되는 디바이스에서 원격 관리를 편집하는 동안 이 문제가 발생한 경우 매니지드 디바이스에서 원격 관리 수정, 687 페이지를 참조합니다.

고가용성 피어 중 하나에 대한 IP 주소가 변경되면 고가용성이 저하 상태에 진입합니다. 고가용성을 복구하려면 수동으로 IP 주소를 변경해야 합니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 Firepower Management Center 중 하나에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 피어 관리자를 선택합니다.

단계 **5** 수정( )를 선택합니다.

단계 **6** Firepower System의 컨텍스트 내에서만 사용되는 어플라이언스의 표시 이름을 입력합니다.

다른 표시 이름을 입력해도 어플라이언스에 대한 호스트 이름은 변경되지 않습니다.

단계 **7** FQDN(Fully Qualified Domain Name) 또는 로컬 DNS를 통해 확인한 유효한 IP 주소(호스트 이름) 또는 호스트 IP 주소를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

Firepower Management Center 고가용성 비활성화

프로시저

단계 **1** 고가용성 쌍의 Firepower Management Center 중 하나에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 고가용성 분리를 선택합니다.

단계 **5** 관리되는 디바이스를 처리하기 위해 다음 옵션 중 하나를 선택합니다.

- 이 Firepower Management Center의 모든 관리되는 디바이스를 제어하기 위해 이 콘솔에서 등록된 디바이스 관리를 선택합니다. 피어에서 모든 디바이스가 등록 해제됩니다.
- 다른 Firepower Management Center의 모든 관리되는 디바이스를 제어하기 위해 피어 콘솔에서 등록된 디바이스 관리를 선택합니다. 이 Firepower Management Center에서 모든 디바이스가 등록 해제됩니다.
- 모든 디바이스 관리를 중지하려면 두 콘솔에서 등록된 디바이스 관리 중지를 선택합니다. 두 Firepower Management Center에서 모든 디바이스가 등록 해제됩니다.

참고 보조 Firepower Management Center에서 등록된 디바이스를 관리하도록 선택할 경우 디바이스는 기본 Firepower Management Center에서 등록 해제됩니다. 디바이스가 이제 보조 Firepower Management Center에서 관리되도록 등록됩니다. 그러나 이런 디바이스에 적용된 라이선스는 고가용성 해제 작업에 의해 등록 해제됩니다. 이제 보조 Firepower Management Center에서 디바이스 라이선스 재등록(활성화)를 진행해야 합니다. 자세한 내용은 FTD 디바이스에서 라이선스 이동 또는 제거를 참조하십시오.

단계 **6** **OK(확인)**를 클릭합니다.

고가용성 쌍의 FMC 교체

Firepower Management Center 고가용성 쌍에서 장애가 발생한 장치를 교체하는 경우 다음 절차 중 하나를 따라야 합니다. 다음 표는 4개의 오류 상황과 해당 교체 절차를 설명합니다.

오류 상태	데이터 백업 상태	교체 절차
기본 FMC 오류	데이터 백업 성공	오류가 발생한 기본 FMC 교체(백업 성공), 290 페이지
	데이터 백업 실패	오류가 발생한 기본 FMC 교체(백업 실패), 292 페이지
보조 FMC 오류	데이터 백업 성공	오류가 발생한 보조 FMC 교체(백업 성공), 293 페이지
	데이터 백업 실패	오류가 발생한 보조 FMC 교체(백업 실패), 294 페이지

오류가 발생한 기본 FMC 교체(백업 성공)

두 Firepower Management Center, FMC1 및 FMC2는 고가용성 쌍의 일부입니다. FMC1은 기본이며 FMC2는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 기본 Firepower Management Center인 FMC1을 교체하는 단계를 설명합니다.

시작하기 전에

오류가 발생한 기본 Firepower Management Center의 데이터 백업이 성공했는지 확인합니다.

프로시저

단계 1 오류가 발생한 Firepower Management Center - FMC1에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 2 기본 Firepower Management Center - FMC1에 오류가 발생하면 보조 Firepower Management Center인 FMC2의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 자세한 내용은 Firepower Management Center 고가용성 쌍에서 피어 전환, 287 페이지를 참고하십시오.

이때 보조 Firepower Management Center - FMC2를 액티브로 전환합니다.

기본 Firepower Management Center - FMC1이 교체될 때까지 FMC2를 액티브 Firepower Management Center로 사용할 수 있습니다.

주의 Firepower Management Center 고가용성을 FMC2에서 분리하지 마십시오. (오류 발생 전에) FMC1에서 FMC2에 동기화된 라이선스가 FMC2에서 제거되어 FMC2에서 구축 작업을 수행할 수 없게 됩니다.

단계 3 FMC1과 동일한 소프트웨어 버전으로 Firepower Management Center을 리이미징하고 교체합니다.

단계 4 FMC1에서 생성한 데이터 백업을 새 Firepower Management Center에 복원합니다.

단계 5 FMC2와 일치시키기 위해 필수 Firepower Management Center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

새 Firepower Management Center 및 FMC2 모두 액티브 피어이므로 고가용성에 스플릿 브레인이 발생합니다.

단계 6 Firepower Management Center 웹 인터페이스가 액티브 어플라이언스를 선택하도록 할 경우 FMC2를 액티브로 선택합니다.

이때 FMC2의 최신 설정이 새 Firepower Management Center - FMC1에 동기화됩니다.

단계 7 설정 동기화가 성공하면 보조 Firepower Management Center - FMC2의 웹 인터페이스에 액세스하여 기본Firepower Management Center - FMC1의 역할을 액티브로 전환합니다. 자세한 내용은 Firepower Management Center 고가용성 쌍에서 피어 전환, 287 페이지를 참고하십시오.

단계 8 새 Firepower Management Center - FMC1에서 수신된 기본 라이선스를 적용하고 기존 라이선스를 삭제합니다. 자세한 내용은 기본 라이선스 생성 및 추가 Firepower Management Center, 167 페이지를 참고하십시오.

스마트 라이선스가 원활하게 작동합니다.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 Firepower Management Center이 정상적으로 작동합니다.

오류가 발생한 기본 FMC 교체(백업 실패)

두 Firepower Management Center, FMC1 및 FMC2는 고가용성 쌍의 일부입니다. FMC1은 기본이며 FMC2는 보조입니다. 이 작업은 데이터 백업이 실패한 경우 오류가 발생한 기본 Firepower Management Center인 FMC1을 교체하는 단계를 설명합니다.

프로시저

단계 **1** 오류가 발생한 Firepower Management Center - FMC1에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 **2** 기본 Firepower Management Center - FMC1에 오류가 발생하면 보조 Firepower Management Center인 FMC2의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 자세한 내용은 Firepower Management Center 고가용성 쌍에서 피어 전환, 287 페이지를 참고하십시오.

이때 보조 Firepower Management Center - FMC2를 액티브로 전환합니다.

기본 Firepower Management Center - FMC1이 교체될 때까지 FMC2를 액티브 Firepower Management Center로 사용할 수 있습니다.

주의 Firepower Management Center 고가용성을 FMC2에서 분리하지 마십시오. (오류 발생 전) FMC1에서 FMC2에 동기화된 클래식 및 스마트 라이선스가 FMC2에서 제거되어 FMC2에서 구축 작업을 수행할 수 없게 됩니다.

단계 **3** FMC1과 동일한 소프트웨어 버전으로 Firepower Management Center을 리이미징하고 교체합니다.

단계 **4** FMC2와 일치시키기 위해 필수 Firepower Management Center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

단계 **5** Firepower Management Center - FMC2를 Cisco Smart Software Manager에서 등록 취소합니다. 자세한 내용은 Cisco Smart Software Manager에서 Firepower Management Center 등록 취소를 참고하십시오.

Firepower Management Center을 Cisco Smart Software Manager에서 등록 취소하면 가상 어카운트에서 Managememt Center가 제거됩니다. Firepower Management Center와 연결되는 모든 라이선스 엔타이틀먼트를 가상 어카운트에 다시 릴리스합니다. 등록 취소 후 라이선스 기능에 대한 어떤 업데이트 또는 변경도 허용되지 않는 부분에서 Firepower Management Center가 Enforcement(시행) 모드를 입력합니다.

단계 **6** 보조 Firepower Management Center - FMC2의 웹 인터페이스에 액세스하여 Firepower Management Center 고가용성을 해제합니다. 자세한 내용은 Firepower Management Center 고가용성 비활성화, 289 페이지를 참고하십시오. 관리되는 디바이스를 처리하기 위한 옵션 선택 메시지가 표시되면 이 콘솔에서 등록된 디바이스 관리를 선택합니다.

따라서 보조 Firepower Management Center - FMC2에서 동기화된 클래식 및 스마트 라이선스가 제거되고 FMC2에서 구축 작업을 수행할 수 없습니다.

단계 **7** Firepower Management Center - FMC2를 기본으로 설정하고 Firepower Management Center - FMC1을 보조로 설정하여 Firepower Management Center 고가용성을 다시 설정합니다. 자세한 내용은 Firepower Management Center 고가용성 설정, 284 페이지를 참조하십시오.

단계 **8** 새 Firepower Management Center - FMC1에서 수신된 기본 라이선스를 적용하고 기존 라이선스를 삭제합니다. 자세한 내용은 기본 라이선스 생성 및 추가 Firepower Management Center, 167 페이지를 참고하십시오.

단계 **9** 기본 Firepower Management Center - FMC2에 스마트 라이선스를 등록합니다. 자세한 내용은 스마트 라이선스 등록를 참조하십시오.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 Firepower Management Center이 정상적으로 작동합니다.

오류가 발생한 보조 FMC 교체(백업 성공)

두 Firepower Management Center, FMC1 및 FMC2는 고가용성 쌍의 일부입니다. FMC1은 기본이며 FMC2는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 보조 Firepower Management Center인 FMC2을 교체하는 단계를 설명합니다.

시작하기 전에

오류가 발생한 보조 Firepower Management Center의 데이터 백업이 성공했는지 확인합니다.

프로시저

단계 **1** 오류가 발생한 Firepower Management Center - FMC2에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 **2** 기본 Firepower Management Center - FMC1을 액티브 Firepower Management Center로 계속 사용합니다.

단계 **3** FMC2과 동일한 소프트웨어 버전으로 Firepower Management Center을 리이미징하고 교체합니다.

단계 **4** FMC2에서 생성한 데이터 백업을 새 Firepower Management Center에 복원합니다.

단계 **5** FMC1와 일치시키기 위해 필수 Firepower Management Center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

단계 **6** (중단된 경우) 기본 Firepower Management Center - FMC1의 최신 설정을 동기화하기 위해 새 Firepower Management Center의 웹 인터페이스에서 데이터 동기화를 재개합니다. 자세한 내용은 페어링된 Firepower Management Center 간 통신 재시작, 288 페이지를 참고하십시오.

클래식 및 스마트 라이선스가 원활하게 작동합니다.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 Firepower Management Center이 정상적으로 작동합니다.

오류가 발생한 보조 FMC 교체(백업 실패)

두 Firepower Management Center, FMC1 및 FMC2는 고가용성 쌍의 일부입니다. FMC1은 기본이며 FMC2는 보조입니다. 이 작업은 데이터 백업이 실패한 경우 오류가 발생한 보조 Firepower Management Center인 FMC2을 교체하는 단계를 설명합니다.

프로시저

단계 **1** 오류가 발생한 Firepower Management Center - FMC2에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 **2** 기본 Firepower Management Center - FMC1을 액티브 Firepower Management Center로 계속 사용합니다.

단계 **3** FMC2과 동일한 소프트웨어 버전으로 Firepower Management Center을 리이미징하고 교체합니다.

단계 **4** FMC1와 일치시키기 위해 필수 Firepower Management Center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

단계 **5** 기본 Firepower Management Center - FMC1의 웹 인터페이스에 액세스하여 Firepower Management Center 고가용성을 해제합니다. 자세한 내용은 Firepower Management Center 고가용성 비활성화, 289 페이지를 참고하십시오. 관리되는 디바이스를 처리하기 위한 옵션 선택 메시지가 표시되면 이 콘솔에서 등록된 디바이스 관리를 선택합니다.

단계 **6** Firepower Management Center - FMC1를 기본으로 설정하고 Firepower Management Center - FMC2를 보조로 설정하여 Firepower Management Center 고가용성을 다시 설정합니다. 자세한 내용은 Firepower Management Center 고가용성 설정, 284 페이지를 참조하십시오.

- 고가용성이 성공적으로 설정된 경우 기본 Firepower Management Center - FMC1의 최신 설정이 보조 Firepower Management Center - FMC2에 동기화됩니다.
- 클래식 및 스마트 라이선스가 원활하게 작동합니다.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 Firepower Management Center이 정상적으로 작동합니다.

FMC 고가용성 히스토리

기능	버전	세부 사항
VMWare에서 FMCv를 사용하는 FMC 고가용성	6.7	이제 VMWare에서 실행되는 FMCv를 사용하여 FMC 고가용성을 달성할 수 있습니다. 가상 플랫폼 요건, 281 페이지의 요구 사항을 참조하십시오. 지원되는 플랫폼: VMWare용 FMCv 10, 25 및 300

기능	버전	세부 사항
SSO(Single Sign-On)	6.7	SSO(Single Sign-On)를 위해 고가용성 쌍의 멤버 하나 또는 둘 다를 구성할 때는 특별한 고려 사항이 있습니다. 지원되는 플랫폼: FMC

13 장

디바이스 관리 기본 사항

다음 주제에서는 Firepower System에서 디바이스를 관리하는 방법을 설명합니다.

- 디바이스 관리 관련 정보, 297 페이지
- 디바이스 관리 요구 사항 및 사전 요건, 305 페이지
- FTD 초기 설정 완료, on page 305
- FMC에 디바이스 추가, 311 페이지
- FMC에서 디바이스 삭제, 315 페이지
- 디바이스 그룹 추가, 315 페이지
- 디바이스 설정 구성, 316 페이지
- 디바이스의 관리자 변경, 351 페이지
- 디바이스 정보 보기, 356 페이지

디바이스 관리 관련 정보

Firepower Management Center를 사용하여 디바이스를 관리합니다.

Firepower Management Center 및 디바이스 관리 관련 정보

Firepower Management Center는 디바이스를 관리할 때 자체와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. Firepower Management Center는 이 채널을 사용하여 네트워크 트래픽을 분석하고 관리하고자 하는 방법에 대한 정보를 디바이스로 전송합니다. 디바이스는 트래픽을 평가할 때 이벤트를 생성하고 동일한 채널을 사용하여 Firepower Management Center로 전송합니다.

Firepower Management Center를 사용하여 디바이스를 관리하면 다음을 수행할 수 있습니다.

- 단일 위치에서 모든 디바이스에 대한 정책을 구성하므로 설정을 좀 더 쉽게 변경할 수 있습니다.
- 디바이스에 각종 소프트웨어 업데이트를 설치할 수 있습니다.
- 관리되는 디바이스에 상태 정책을 푸시하고 에서 상태를 모니터링할 수 있습니다. Firepower Management Center

Firepower Management Center는 침입 이벤트, 네트워크 검색 정보 및 디바이스 성능 데이터를 집계하고 상호 연결하므로 사용자는 디바이스가 상호 관계에 대해 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가할 수 있습니다.

Firepower Management Center를 사용하면 디바이스 동작의 거의 모든 부분을 관리할 수 있습니다.

참고 하지만 Firepower Management Center은 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html에서 사용 가능한 호환성 매트릭스에서 지정된 일부 이전 릴리스가 실행되는 디바이스를 관리할 수 있으며 이런 이전 릴리스를 사용하는 디바이스에서는 새로운 기능을 사용할 수 없습니다.

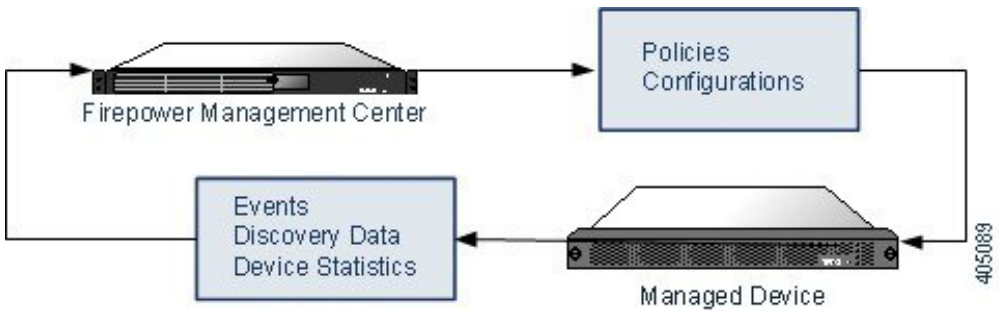
Firepower Management Center로 관리할 수 있는 내용

Firepower Management Center를 다음과 같은 디바이스를 관리하기 위한 Firepower System 구축의 중앙 관리 지점으로 사용할 수 있습니다.

- 7000 및 8000 Series 디바이스
- ASA FirePOWER 모듈
- NGIPSv 디바이스
- Firepower Threat Defense(물리적 하드웨어 및 가상)

디바이스를 관리할 때에는 Firepower Management Center와 디바이스 간에 안전한 SSL 암호화 TCP 터널을 통해 정보가 전송됩니다.

다음 그림에서는 Firepower Management Center 및 해당 매니지드 디바이스 간에 무엇이 전송되는지를 보여줍니다. 어플라이언스 간에 전송되는 이벤트와 정책의 유형은 디바이스 유형을 기반으로 합니다.



정책 및 이벤트 이상

디바이스에 정책을 구축하고 디바이스에서 이벤트를 수신하는 것 외에도 Firepower Management Center에서는 다른 디바이스 관련 작업을 수행할 수 있습니다.

디바이스 백업

NGIPSv 디바이스 또는 ASA FirePOWER 모듈에 대한 백업 파일을 만들거나 복원할 수 없습니다.

디바이스 자체에서 관리되는 물리적 디바이스의 백업을 수행할 경우 디바이스 설정만 백업됩니다. 설정 데이터 및 선택적으로 통합된 파일을 백업하려면 관리하는 Firepower Management Center를 사용하여 디바이스의 백업을 수행할 수 있습니다.

이벤트 데이터를 백업하기 위해서는 관리하는 Firepower Management Center의 백업을 수행합니다.

디바이스 업데이트

Cisco는 다음과 같은 Firepower System의 업데이트를 수시로 배포합니다.

- 새로운 침입 규칙과 업데이트된 침입 규칙이 포함되는 침입 규칙 업데이트
- 취약성 데이터베이스(VDB) 업데이트
- 지리위치 업데이트
- 소프트웨어 패치 및 업데이트

관리하는 디바이스에 업데이트를 설치하려면 Firepower Management Center를 사용할 수 있습니다.

디바이스 관리 인터페이스

각 디바이스는 FMC와 통신하기 위한 단일 전용 관리 인터페이스를 포함합니다. 선택적으로 전용 관리 인터페이스 대신 관리용 데이터 인터페이스를 사용하도록 디바이스를 구성할 수 있습니다.

관리 인터페이스 또는 콘솔 포트에서 초기 설정을 수행할 수 있습니다.

관리 인터페이스는 Smart Licensing 서버와 통신하고, 업데이트를 다운로드하고, 기타 관리 기능을 수행하는 작업에도 사용됩니다.

매니지드 디바이스의 관리 인터페이스

디바이스를 설정할 때 연결할 FMC IP 주소를 지정합니다. 관리 및 이벤트 트래픽은 초기 등록 시 이 주소로 이동합니다. 참고: 일부 경우에 FMC는 다른 관리 인터페이스에서 초기 연결을 설정할 수 있습니다. 후속 연결은 지정된 IP 주소가 있는 관리 인터페이스를 사용해야 합니다.

FMC에 별도의 이벤트 전용 인터페이스가 있는 경우, 네트워크가 허용하는 경우 매니지드 디바이스에서 후속 이벤트 트래픽을 FMC 이벤트 전용 인터페이스로 보냅니다. 또한 일부 매니지드 디바이스 모델에는 이벤트 전용 트래픽에 대해 구성할 수 있는 추가 관리 인터페이스가 포함되어 있습니다. 관리를 위해 데이터 인터페이스를 구성하는 경우 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다. 이벤트 네트워크가 다운되면 이벤트 트래픽은 FMC 및/또는 매니지드 디바이스의 일반 관리 인터페이스로 되돌아갑니다.

FTD 데이터 인터페이스를 사용하여 관리하는 방법에 대한 정보

FMC와의 통신에 전용 관리 인터페이스 또는 일반 데이터 인터페이스를 사용할 수 있습니다. 외부 인터페이스에서 원격으로 FTD를 관리하려는 경우 또는 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 FMC 액세스가 유용합니다.

데이터 인터페이스에서의 FMC 액세스에는 다음과 같은 제한이 있습니다.

- 하나의 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 FMC를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

디바이스 모델별 관리 인터페이스 지원

관리 인터페이스 위치에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.

각 매니지드 디바이스 모델에서 지원되는 관리 인터페이스는 다음 표를 참조하십시오.

표 ***11:*** 매니지드 디바이스의 관리 인터페이스 지원

모델	관리 인터페이스	선택적 이벤트 인터페이스
7000 Series	eth0	지원 안 함
8000 Series	eth0	eth1
NGIPSv	eth0	지원 안 함
ASA 5508-X 또는 5516-X의 ASA FirePOWER 서비스 모듈	eth0 참고 eth0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함

모델	관리 인터페이스	선택적 이벤트 인터페이스
ISA 3000의 ASA FirePOWER 서비스 모듈	eth0 참고 eth0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Firepower Threat Defense Firepower 1000	management0 참고 management0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Firepower Threat Defense Firepower 2100	management0 참고 management0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함

디바이스 관리 인터페이스의 네트워크 라우트

관리 인터페이스(이벤트 전용 인터페이스 포함)는 정적 경로만 지원하여 원격 네트워크에 연결할 수 있습니다. 매니지드 디바이스를 설정하면 설정 과정에서 지정한 게이트웨이 IP 주소에 대한 기본 경로가 생성됩니다. 이 경로는 삭제할 수 없으며 게이트웨이 주소만 수정할 수 있습니다.

참고 관리 인터페이스의 라우팅은 데이터 인터페이스에 대해 구성한 라우팅과는 완전히 분리됩니다. 전용 관리 인터페이스를 사용하는 대신 관리용 데이터 인터페이스를 설정하는 경우 데이터 라우팅 테이블을 사용하도록 트래픽이 백플레인을 통해 라우팅됩니다. 이 섹션의 정보는 적용되지 않습니다.

기본 경로는 항상 가장 낮은 번호의 관리 인터페이스(예: management0)를 사용합니다.

원격 네트워크에 액세스하기 위해서는 관리 인터페이스당 최소 1개의 정적 경로가 권장됩니다. 다른 디바이스에서 FTD 로의 라우팅 문제를 비롯하여 잠재적인 라우팅 문제를 방지하려면 각 인터페이스를 별도의 네트워크에 배치하는 것이 좋습니다. 동일한 네트워크의 인터페이스에서 문제가 발생하지 않으면 고정 경로를 올바르게 설정해야 합니다. 예를 들어 management0과 management1은 동일한 네트워크에 있지만 FMC 관리 및 이벤트 인터페이스는 서로 다른 네트워크에 있습니다. 게이트웨이는 192.168.45.1입니다. 10.6.6.1/24에서 management1을 FMC의 이벤트 전용 인터페이스에 연결하려는 경우 동일한 게이트웨이 192.168.45.1로 10.6.6.0/24에서 management1까지의 고정 경로를 생성할 수 있습니다. 10.6.6.0/24 트래픽은 기본 경로에 도달하기 전에 이 경로에 도달하므로 management1이 예상대로 사용됩니다.

또 다른 예는 FMC 및 매니지드 디바이스에 별도의 관리 및 이벤트 전용 인터페이스를 포함합니다. 이벤트 전용 인터페이스는 관리 인터페이스와 별도의 네트워크에 있습니다. 이 경우 원격 이벤트 전

용 네트워크를 대상으로 하는 트래픽에 대해 이벤트 전용 인터페이스를 통해 정적 경로를 추가할 수 있으며, 그 반대의 경우도 마찬가지입니다.

NAT 환경

NAT(Network Address Translation)는 소스 또는 대상 IP 주소를 재할당하는 작업에 관여하는 라우터를 통해 네트워크 트래픽을 보내고 받는 방법입니다. NAT는 일반적으로 프라이빗 네트워크와 인터넷이 통신하는 데 사용됩니다. 정적 NAT는 1:1 변환을 수행하여 디바이스와 FMC의 통신에 문제를 일으키지 않지만 포트 주소 변환(PAT)이 더욱 일반적입니다. PAT를 사용하면 단일 공용 IP 주소에 고유한 포트를 사용해 공용 네트워크에 접속할 수 있습니다. 이러한 포트는 필요에 따라 동적으로 할당되므로 PAT 라우터 뒤에 있는 디바이스에 연결을 시작할 수 없습니다.

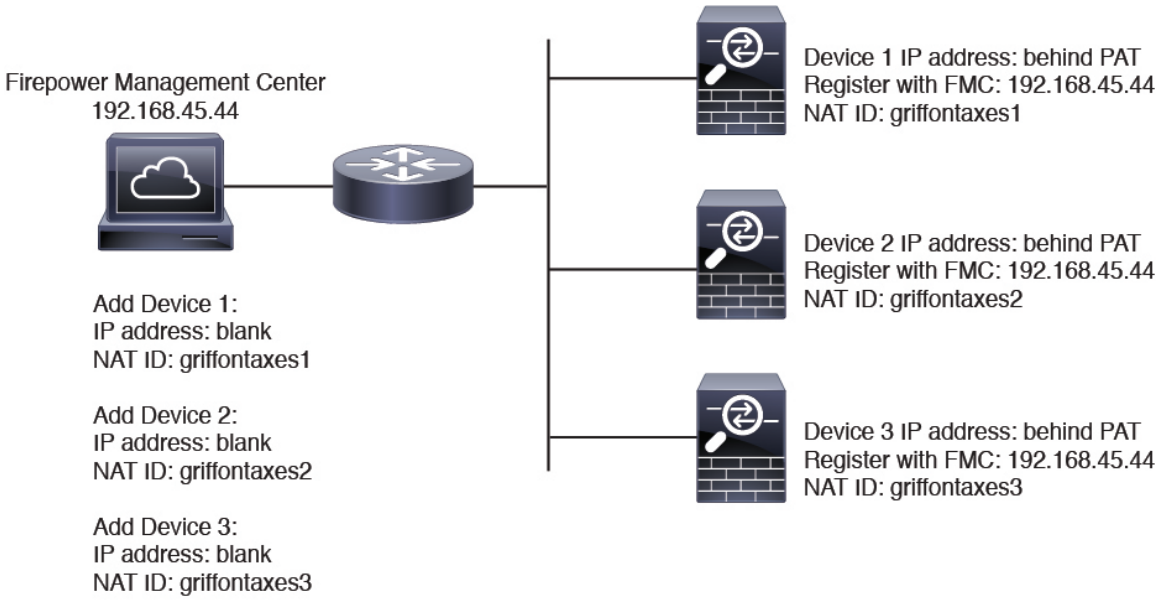
일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

예를 들어 FMC에 디바이스를 추가하지만 디바이스 IP 주소를 모르는 경우(디바이스가 PAT 라우터 뒤에 있는 경우) FMC에 NAT ID와 등록 키만 지정하고 IP 주소는 공백으로 둡니다. 디바이스에 FMC IP 주소, 동일한 NAT ID와 동일한 등록 키를 지정합니다. FMC의 IP 주소에 디바이스를 등록합니다. 이때 FMC은 IP 주소 대신 NAT ID를 사용해 디바이스를 인증합니다.

NAT 환경에서 NAT ID 사용은 일반적이지만 FMC에 많은 디바이스를 추가하려고 할 때에도 NAT ID를 선택할 수 있습니다. FMC에는 추가하려는 각 디바이스에 고유한 NAT ID를 지정하고 IP 주소를 공백으로 두고, 각 디바이스에서 FMC IP 주소 및 NAT ID를 지정하십시오. 주의: NAT ID는 디바이스별로 고유해야 합니다.

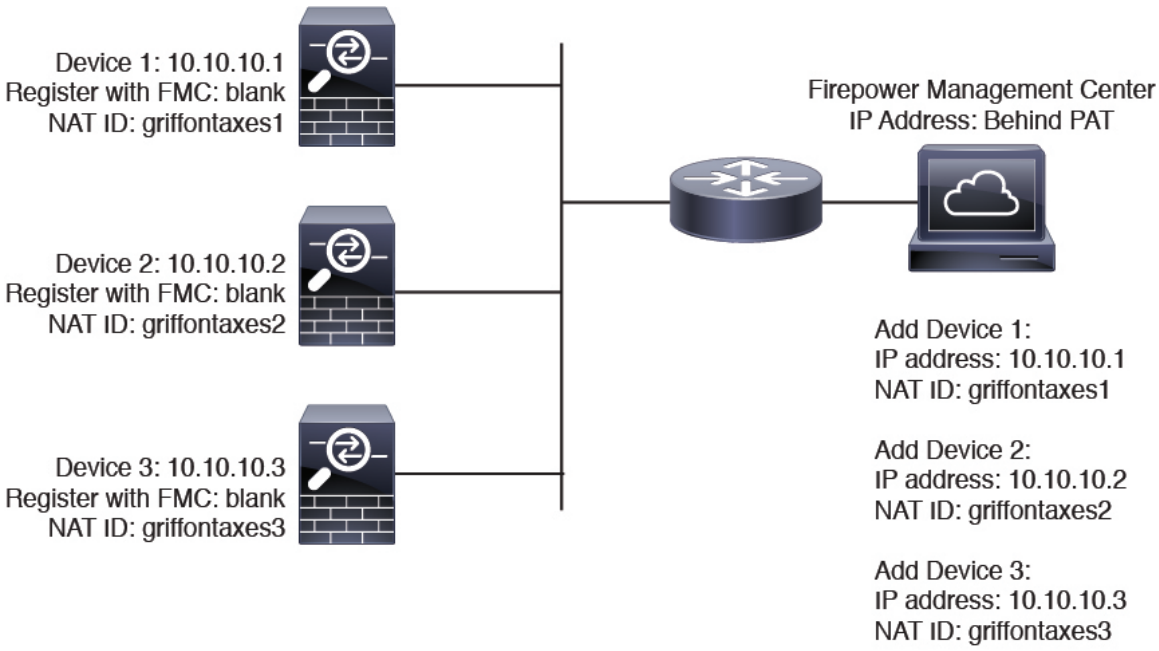
다음 예에서는 PAT IP 주소 뒤에 3개의 장치가 있음을 보여줍니다. 이 경우 FMC 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 디바이스에 FMC IP 주소를 지정하십시오.

그림 *1: PAT* 뒤의 관리되는 디바이스의 *NAT ID*



다음 예는 PAT ID 주소 뒤의 FMC을 보여줍니다. 이 경우 FMC 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 FMC에 디바이스 IP 주소를 지정하십시오.

그림 *2: PAT* 뒤의 *FMC*에 대한 *NAT ID*

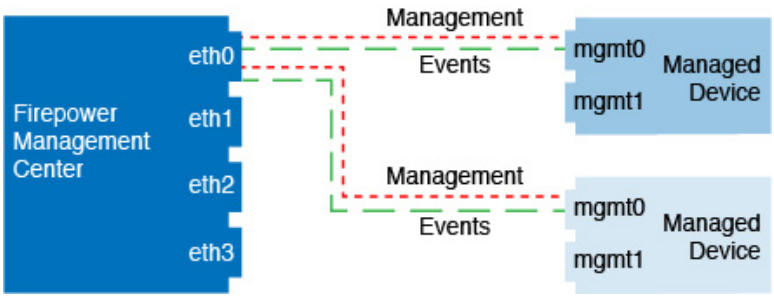


관리 및 이벤트 트래픽 채널 예시

참고 FTD에서 관리를 위해 데이터 인터페이스를 사용하는 경우 해당 디바이스에 대해 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다.

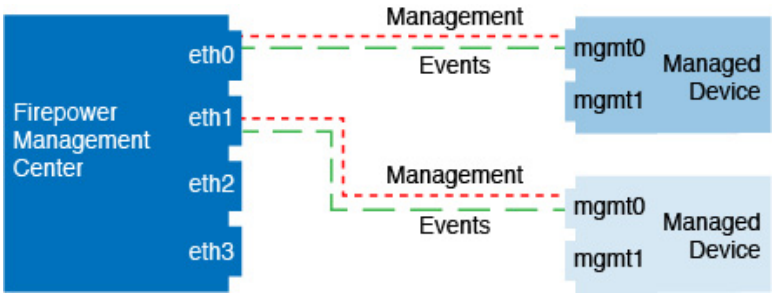
다음 예에서는 기본 관리 인터페이스만 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

그림 *3:* 단일 관리 인터페이스*: Firepower Management Center*



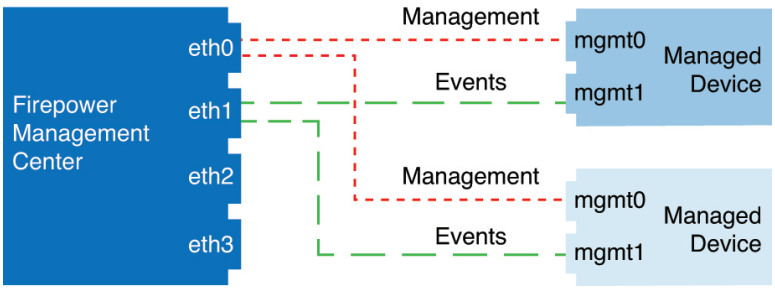
다음 예는 디바이스에 별도의 관리 인터페이스를 사용하는 Firepower Management Center를 보여 줍니다. 관리되는 각 디바이스는 1개의 관리 인터페이스를 사용합니다.

그림 *4:* 다중 관리 인터페이스*: Firepower Management Center*



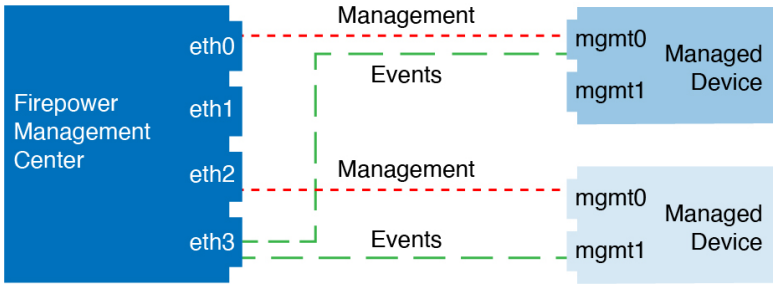
다음 예에서는 별도의 이벤트 인터페이스를 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

그림 *5: Firepower Management Center* 및 매니지드 디바이스에 대한 별도의 이벤트 인터페이스



다음 예는 별도의 이벤트 인터페이스를 사용하거나 단일 관리 인터페이스를 사용하는 Firepower Management Center 및 여러 매니지드 디바이스에 대한 다중 관리 인터페이스 및 별도의 이벤트 인터페이스를 보여 줍니다.

그림 *6:* 혼합 관리 및 이벤트 인터페이스 사용



디바이스 관리 요구 사항 및 사전 요건

모델 지원

모든 관리되는 디바이스(절차에 명시되지 않는 한)

지원되는 도메인

디바이스가 상주하는 도메인입니다.

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)

FTD 초기 설정 완료

FTD CLI에 연결하여 설정 마법사를 사용하여 관리 IP 주소, 게이트웨이 및 기타 기본 네트워킹 설정을 포함한 초기 설정을 수행합니다. 전용 관리 인터페이스는 자체 네트워크 설정이 있는 특수 인터페이스입니다. FMC 액세스에 관리 인터페이스를 사용하지 않으려는 경우, 대신 CLI를 사용하여 데이터 인터페이스를 설정할 수 있습니다. FMC 통신 설정도 구성합니다.

Before you begin

이 절차는 Firepower 4100/9300을(를) 제외한 모든 FTD 디바이스에 적용됩니다. Firepower 4100/9300의 경우, 용 독립형 Firepower Threat Defense 추가, on page 763의 내용을 참조하십시오.

Procedure

단계 **1** 콘솔 포트에서 또는 관리 인터페이스에 대한 SSH를 사용하여 FTD CLI에 연결합니다.이 인터페이스는 기본적으로 DHCP 서버에서 IP 주소를 가져옵니다. 네트워크 설정을 변경하려는 경우 연결이 끊어지지 않도록 콘솔 포트를 사용하는 것이 좋습니다.

(Firepower 1000/2100) 콘솔 포트는 FXOS CLI에 연결합니다. SSH 세션은 FTD CLI에 직접 연결됩니다.

단계 **2** 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

(Firepower 1000/2100) 콘솔 포트에서 사용자를 FXOS CLI에 연결합니다. FXOS에 처음 로그인하면 암호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 FTD 로그인에도 사용됩니다.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

단계 **3** (Firepower 1000/2100) 콘솔 포트에서 FXOS에 연결한 경우 FTD CLI에 연결합니다.

connect ftd

Example:

```
firepower# connect ftd
>
```

단계 **4** FTD에 처음 로그인할 경우, 최종 사용자 라이선스 계약(EULA)에 동의하고 SSH 연결을 사용 중인 경우 관리자 암호를 변경하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

Note 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 마법사를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network(**네트워크 구성**)** 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. FTD 명령 참조를 참조하십시오.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

Note 관리 인터페이스 설정은 데이터 인터페이스에서 FMC 액세스를 활성화한 경우에도 사용됩니다. 예를 들어 데이터 인터페이스를 통해 백플레인으로 라우팅되는 관리 트래픽은 데이터 인터페이스 DNS 서버가 아닌 관리 인터페이스 DNS 서버를 사용하여 FQDN을 확인합니다.

다음 지침을 참조하십시오.

- **Configure IPv4 via DHCP or manually?(DHCP**를 통해 또는 수동으로 **IPv4**를 설정하시겠습니까**?)** - 관리 인터페이스 대신 FMC 액세스용 데이터 인터페이스를 사용하려면 **manual(**수동**)**을 선택합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다. 이 IP 주소는 트래픽이 데이터 인터페이스로 전달될 때 NAT 처리됩니다. 관리 인터페이스가 DHCP로 설정된 경우 관리를 위해 데이터 인터페이스를 설정할 수 없습니다. 데이터 인터페이스**(**데이터 인터페이스**)**여야 하는 기본 경로(다음 글머리 기호 참조)가 DHCP 서버에서 수신한 기본 경로를 덮어 쓸 수 있기 때문입니다.
- **Enter the IPv4 default gateway for the management interface(**관리 인터페이스에 대한 **IPv4** 기본 게이트웨이 입력**)** - 관리 인터페이스 대신 FMC 액세스에 데이터 인터페이스를 사용하려면 게이트웨이를 데이터 인터페이스**(**데이터 인터페이스**)**로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 FMC 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다. FMC 액세스에 관리 인터페이스를 사용하려면 관리 1/1 네트워크에서 게이트웨이 IP 주소를 설정해야합니다.
- **If your networking information has changed, you will need to reconnect(**네트워킹 정보가 변경된 경우 다시 연결해야 합니다**)** — SSH를 통해 연결되어 있지만 최초 설정에서 IP 주소를 변경한 경우 연결이 끊깁니다. 새 IP 주소 및 비밀번호를 사용하여 다시 연결합니다. 콘솔 연결에는 영향을 미치지 않습니다.
- **Manage the device locally?(**디바이스를 로컬로 관리하시겠습니까**?)**—FMC을(를) 사용하려면 **no**를 입력합니다. 예를 입력하면 Firepower Device Manager를 대신 사용하게 됩니다.
- **Configure firewall mode?(**방화벽 모드를 설정하시겠습니까**?)**—초기 설정에서 방화벽 모드를 설정하는 것이 좋습니다. 초기 설정 후에 방화벽 모드를 변경하면 실행 중인 구성이 지워집니다.데이터 인터페이스 FMC 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
```

```
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

단계 **5** 이 FTD를 관리할 FMC을(를) 식별합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—FMC의 FQDN 또는 IP 주소를 지정합니다. FMC의 주소를 직접 지정할 수 없는 경우 **DONTRESOLVE**를 사용하고 *nat_id*도 지정합니다. 하나 이상의 디바이스(FMC 또는 FTD)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다. 이 명령에서 **DONTRESOLVE**를 지정하는 경우 FTD에 연결할 수 있는 IP 주소 또는 호스트 이름이 있어야 합니다.
- *reg_key* — FTD 등록시 FMC에 지정할 일회용 등록 키를 지정합니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다.
- *nat_id* — 한쪽이 연결할 수 있는 IP 주소 또는 호스트 이름을 지정하지 않은 경우 FTD를 등록할 때 FMC에 지정할 고유한 일회용 문자열을 지정합니다. FMC를 **DONTRESOLVE**로 설정하는 경우 반드시 필요합니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 FMC에 등록하는 다른 디바이스에 사용할 수 없습니다.

  Note 관리에 데이터 인터페이스를 사용하는 경우 등록을 위해 FTD 및 FMC 모두에서 NAT ID를 지정해야 합니다.

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

FMC이(가) NAT 디바이스 뒤에 있는 경우 등록 키와 고유한 NAT ID를 입력하고 호스트 이름 대신 DONTRESOLVE를 지정합니다. 예를 들면 다음과 같습니다.

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

FTD가 NAT 디바이스 뒤에 있는 경우 FMC IP 주소 또는 호스트 이름과 함께 고유한 NAT ID를 입력합니다. 예를 들면 다음과 같습니다.

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

단계 **6** (Optional) FMC 액세스를위한 데이터 인터페이스를 설정합니다.

configure network management-data-interface

그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

Note 이 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 관리 인터페이스에 SSH를 사용하는 경우 연결이 끊기고 콘솔 포트에 다시 연결해야 할 수 있습니다. SSH 사용량에 대한 자세한 내용은 아래를 참조하십시오.

이 명령 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 관리에 데이터 인터페이스를 사용하려는 경우 원래 관리 인터페이스에서 DHCP를 사용할 수 없습니다. 초기 설정 중에 IP 주소를 수동으로 설정하지 않은 경우 지금 **configure network** {**ipv4** | **ipv6**} **manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces**로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- 데이터 인터페이스에서의 FMC 액세스에는 다음과 같은 제한이 있습니다.
  - 하나의 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다.
  - 이 인터페이스는 관리 전용일 수 없습니다.
  - 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
  - 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
  - PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
  - 인터페이스는 전역 VRF에만 있어야 합니다.
  - 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.

  - SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 FMC를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

- FMC에 FTD를 추가하면 FMC는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 컨피그레이션을 검색하고 유지 관리합니다. DNS 서버 설정에 관한 자세한 내용은 아래를 참조하십시오. FMC에서 나중에 FMC 액세스 인터페이스 구성을 변경할 수 있지만, FTD 또는 FMC가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 FTD에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- DDNS 서버 업데이트 URL을 설정하는 경우 FTD가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 Cisco Trusted Root CA 번들에서 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. FTD는 DynDNS 원격 API 사양(https://help.dyn.com/remote-access-api/)을 사용하는 모든 DDNS 서버를 지원합니다.
- 이 명령은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 스크립트로 설정하거나 **configure network dns servers** 명령을 사용하여 설정한 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다.

  FMC에서 이 FTD에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. FMC에 FTD를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 구성을 포함하는 FTD에 플랫폼 설정 정책을 할당하면 해당 구성이 로컬 설정을 덮어씁니다. FMC와 FTD를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 설정하는 것이 좋습니다.

  또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 FMC에 의해 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 설정하는 경우 FTD 구성과 일치하도록 DNS 서버를 포함하여 FMC에서 이러한 모든 설정을 수동으로 설정해야 합니다.
- FTD를 FMC에 등록한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 구성을 지울 수 있습니다. 복구 시나리오에서는 이 옵션을 사용할 수 있지만 초기 설정 또는 정상 작동에는 이 옵션을 사용하지 않는 것이 좋습니다.
- 데이터 관리를 비활성화하려면 **configure network management-data-interface disable** 명령을 입력합니다.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

```
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 **7** (Optional) 특정 네트워크의 FMC에 대한 데이터 인터페이스 액세스를 제한합니다.

configure network management-data-interface client *ip_address netmask*

기본적으로 모든 네트워크가 허용됩니다.

What to do next

장치를 FMC에 등록합니다.

FMC에 디바이스 추가

단일 디바이스를 FMC에 추가하려면 이 절차를 사용합니다. 디바이스를 이중화 또는 성능을 위해 연결하려는 경우 다음을 염두에 두고 이 절차를 사용합니다.

- 8000 Series스택 - 이 절차를 사용해 각 디바이스를 Firepower Management Center에 추가하고 스택을 설정할 땐 디바이스 스택 설정의 내용을 참조하십시오.
- 7000 및 8000 Series고가용성 - 이 절차를 사용해 각 디바이스를 Firepower Management Center에 추가하고 고가용성을 설정할 땐 Firepower 7000/8000 시리즈 고가용성 설정의 내용을 참조하십시오. 고가용성 스택의 경우 먼저 디바이스를 스태킹하고 스택 간 고가용성을 설정합니다.

- FTD 클러스터 - 클러스터 추가에 대한 자세한 내용은 FMC: 클러스터 추가, 943 페이지의 내용을 참조하십시오.

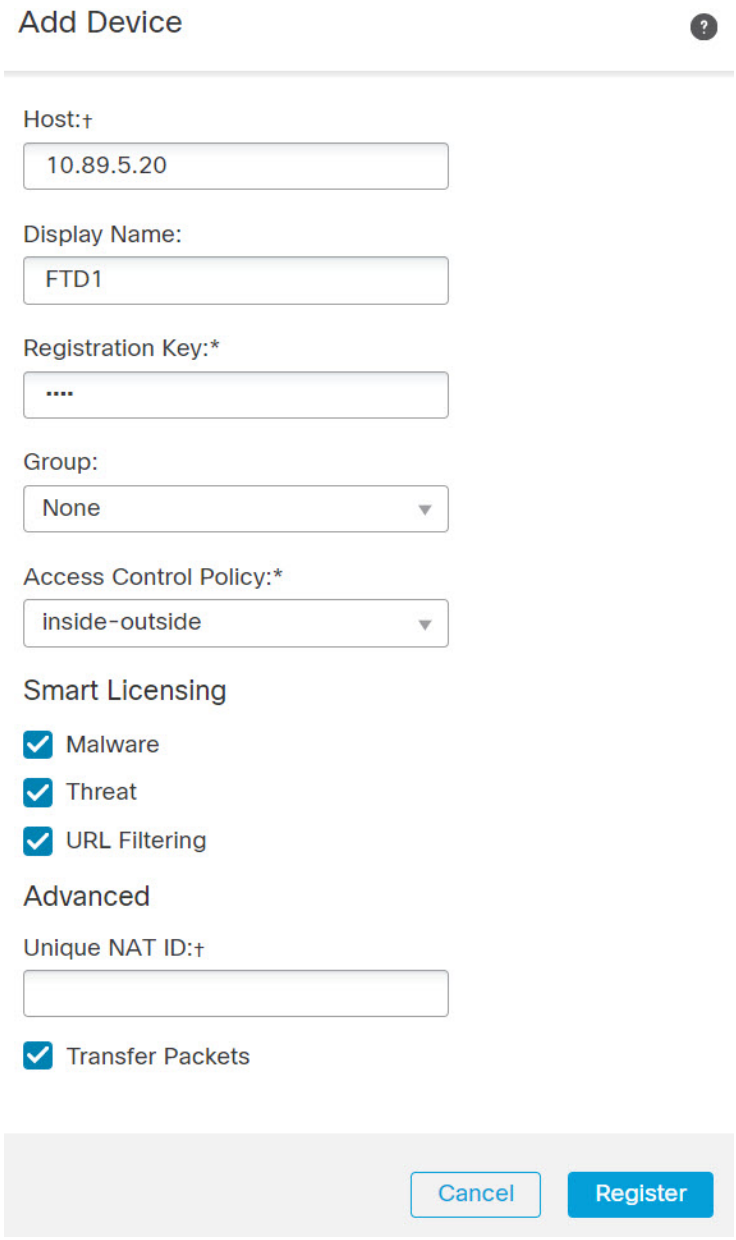
시작하기 전에

- FMC에서 관리할 수 있도록 디바이스를 설정합니다. 적절한 빠른 시작 가이드를 참조하십시오. 7000 및 8000 Series 디바이스에 대해서는 매니지드 디바이스에서 원격 관리 구성, 686 페이지의 내용도 참조하십시오.
- FTD 디바이스를 추가하는 경우, FMC를 Smart Licensing Server(CSSM)에 등록해야 합니다. 유효한 평가 라이선스는 충분하지만, 만료되면 등록에 성공할 때까지 새 디바이스를 추가할 수 없습니다.
- FMC 및 IPv4를 사용하는 디바이스를 등록했으며 IPv6으로 전환하려는 경우, 해당 디바이스를 삭제하고 다시 등록해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** **Add(**추가**)** 드롭다운 메뉴에서 **Device(**디바이스**)**를 선택합니다.



단계 **3** 추가할 디바이스의 IP 주소 또는 호스트 이름을 호스트 필드에 입력합니다.

디바이스의 호스트 이름은 FQDN(Fully Qualified Domain Name) 또는 유효한 IP 주소에 로컬 DNS를 통해 확인하는 이름입니다. 사용자 네트워크가 IP 주소를 할당하기 위해 DHCP를 사용하는 경우 IP 주소 대신 호스트 이름을 사용합니다.

NAT 환경에서는, FMC로 관리되는 디바이스를 구성할 때 FMC의 IP 주소 또는 호스트 이름을 이미 지정한 경우 디바이스의 IP 주소 또는 호스트 이름을 지정하지 않아도 될 수 있습니다. 자세한 내용은 NAT 환경, 302 페이지의 내용을 참고하십시오.

단계 **4** FMC에 표시할 디바이스의 이름을 표시 이름 필드에 입력합니다.

단계 **5** FMC로 관리할 디바이스를 구성할 때 사용한 것과 동일한 등록 키를 등록 키 필드에 입력합니다. 등록 키는 일회용 공유 암호입니다.

단계 **6** 다중 도메인 구축에서는 현재 도메인과 상관없이 디바이스를 리프 도메인으로 할당합니다.

현재 도메인이 리프 도메인인 경우 디바이스는 자동으로 현재 도메인에 추가됩니다. 현재 도메인이 리프 도메인이 아닌 경우나 이후 재등록을 한 경우라면 리프 도메인으로 전환하여 디바이스를 구성합니다.

단계 **7** (선택 사항) 디바이스 그룹에 디바이스를 추가합니다.

단계 **8** 등록 시 디바이스를 구축하기 위해 초기 액세스 제어 정책을 선택하거나 새 정책을 생성합니다.

디바이스가 선택한 정책과 호환되지 않는 경우 구축이 실패합니다. 이러한 문제는 라이선싱 불일치, 모델 제약 조건, 수동 대 인라인 문제, 기타 잘못된 구성을 비롯한 여러 가지 이유로 인해 발생할 수 있습니다. 오류 원인을 해결한 뒤 디바이스에 수동으로 설정을 구축합니다.

단계 **9** 디바이스에 적용할 라이선스를 선택합니다.

스마트 라이선싱

구축하려는 기능에 필요한 스마트 라이선스를 할당합니다.

- 악성코드(AMP 악성코드 검사를 사용하려는 경우)
- 위협(침입 방지를 사용하려는 경우)
- **URL**(범주 기반 URL 필터링을 구현하려는 경우)

Classic Licensing

- Control, Malware 및 URL Filtering 라이선스에는 Protection 라이선스가 필요합니다.
- VPN 라이선스는 하나의 7000 또는 8000 Series 디바이스를 요구합니다.
- NGIPSv와 ASA FirePOWER 디바이스에서는 제어 라이선스가 지원되지만, 8000 Series 빠른 경로 규칙, 전환, 라우팅, 스태킹, 디바이스 고가용성 구성을 허용하지 않습니다.

단계 **10** 디바이스 설정 중 NAT ID를 사용하는 경우 **Advanced(**고급**)** 섹션을 확장하고 **Unique NAT ID(**고유 **NAT ID)** 필드에 동일한 NAT ID를 입력합니다.

단계 **11** 패킷 전송 체크 박스를 선택하여 디바이스가 Firepower Management Center에 패킷을 전송하도록 합니다.

이 옵션은 기본적으로 활성화되어 있습니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 FMC에 전송합니다. 이벤트를 비활성화하면 이벤트 정보는 FMC에 전송되지만 패킷 데이터는 전송되지 않습니다.

단계 **12** **Register(**등록**)**를 클릭합니다.

FMC이 디바이스의 하트비트를 확인하고 통신을 설정하는 데 최대 2분이 소요될 수 있습니다. 등록에 성공하면 디바이스가 목록에 추가됩니다. 오류가 발생하면 오류 메시지가 표시됩니다. 디바이스가 등록에 실패하면 다음 항목을 확인하십시오.

- Ping - 다음 명령을 사용해 디바이스 CLI에 액세스하고 FMC IP 주소에 Ping을 보냅니다.

ping system *ip_address*

Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. 디바이스 IP 주소를 변경해야 하는 경우 **configure network** {**ipv4** | **ipv6**} **manual** 명령을 사용합니다.

- 등록 키, NAT ID 및 FMC IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add** 명령을 사용해 디바이스에서 등록 키 및 NAT ID를 설정할 수 있습니다.

자세한 문제 해결 정보는 https://cisco.com/go/fmc-reg-error를 참조하십시오.

FMC에서 디바이스 삭제

디바이스를 더 이상 관리하지 않으려면 FMC에서 삭제할 수 있습니다. 디바이스 삭제

- 모든 서버는 Firepower Management Center과 디바이스 간 통신합니다.
- 디바이스 관리 페이지에서 디바이스를 제거합니다.
- 디바이스가 NTP를 통해 FMC에서 시간을 수신하도록 플랫폼 정책 설정을 통해 구성된 경우 디바이스가 로컬 시간 관리로 반환됩니다.

이후 디바이스를 관리하려면 FMC에 다시 추가합니다.

참고 디바이스를 삭제하고 다시 추가하는 경우 FMC 웹 인터페이스에서 액세스 제어 정책을 재적용하라는 메시지가 표시됩니다. 그러나 재등록 시 NAT 및 VPN 정책을 다시 적용하는 옵션은 없습니다. 재등록 시 이전에 적용된 모든 NAT 또는 VPN 설정이 삭제되며 등록이 완료한 뒤에 이를 다시 적용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 삭제하려는 디바이스 옆에 있는 삭제( )을 클릭합니다.

단계 **3** 디바이스를 삭제하려면 확인합니다.

디바이스 그룹 추가

Firepower Management Center에서는 디바이스를 그룹화하여 편리하게 정책을 구축하고 여러 디바이스에 업데이트를 설치할 수 있습니다. 그룹에 있는 디바이스의 목록을 확장 및 축소할 수 있습니다.

다중 도메인 구축의 경우 리프 도메인 내에서만 디바이스 그룹을 생성할 수 있습니다. 멀티테넌시에 Firepower Management Center을 구성하는 경우 기존 디바이스 그룹이 제거되지만 리프 도메인 레벨에서 다시 추가할 수 있습니다.

스택이나 고가용성 쌍의 기본 디바이스를 그룹에 추가하면 두 디바이스 모두 그룹에 추가됩니다. 디바이스를 스택에서 제거하거나 고가용성 쌍을 중단하는 경우에도 두 디바이스는 해당 그룹에 남아 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 드롭다운 메뉴의 **Add(**추가**)**에서 **Add Group(**그룹 추가**)**를 선택합니다.

기존 그룹을 수정하려면 수정하려는 그룹에 대한 수정( )을 클릭합니다.

단계 **3** **Name(**이름**)**을 입력합니다.

단계 **4** **Available Devices(**사용 가능한 장치**)**에서 디바이스 그룹에 추가할 하나 이상의 디바이스를 선택합니다. 여러 디바이스를 선택하려면 Ctrl 또는 Shift 키를 누른 상태에서 클릭합니다.

단계 **5** 디바이스 그룹에서 선택한 디바이스를 포함하려면 **Add(**추가**)**를 클릭합니다.

단계 **6** 선택적으로 디바이스 그룹에서 디바이스를 제거하려면 제거하려는 디바이스 옆의 제거(삭제( ))를 클릭합니다.

단계 **7** 디바이스 그룹에 추가하려면 **OK(**확인**)**를 클릭합니다.

디바이스 설정 구성

디바이스를 추가한 후 디바이스의 **Device(**디바이스**)** 페이지에서 일부 설정을 구성 할 수 있습니다.

시스템 종료 관리

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	Any(모든)	ASA FirePOWER를 제외한 모든 디바이스	리프 전용	관리자/네트워크 관리자

참고 Firepower System 사용자 인터페이스에서 ASA FirePOWER을 종료하거나 다시 시작할 수 없습니다. 각 디바이스를 종료하는 방법에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 다시 시작할 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭합니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 디바이스 페이지에서 개별 디바이스를 종료하거나 다시 시작합니다.

단계 **4** 디바이스를 종료하려면 시스템 섹션에서 디바이스 종료( )를 클릭합니다.

단계 **5** 메시지가 표시되면 디바이스 종료를 확인합니다.

단계 **6** 디바이스를 다시 시작하려면 디바이스 재시작( )을 클릭합니다.

단계 **7** 메시지가 표시되면 디바이스 다시 시작을 확인합니다.

관리 설정 편집

Management(관리**)** 영역에서 관리 설정을 편집할 수 있습니다.

FMC에서 호스트 이름 또는 IP 주소 업데이트

디바이스의 호스트 이름 또는 IP 주소를 (디바이스의 CLI 등을 사용해) FMC에 추가했다면, 아래의 절차를 사용하여 관리 FMC의 호스트 이름 또는 IP 주소를 수동으로 업데이트해야 할 수 있습니다.

디바이스에서 디바이스 관리 IP 주소를 변경하려면를 참조하십시오.CLI에서 디바이스 관리 인터페이스 수정, 327 페이지

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

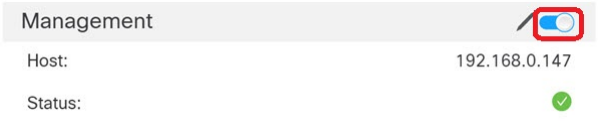
단계 **2** 관리 옵션을 수장할 디바이스 옆의 수정( )를 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

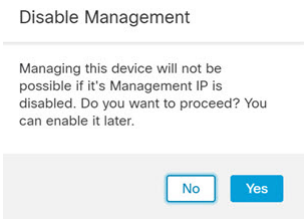
단계 **3** **Device(**디바이스**)**를 클릭하고 **Management(**관리**)** 영역을 확인합니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 디바이스 페이지에서 개별 디바이스의 관리 옵션을 수정할 수 있습니다.

단계 **4** 슬라이더 활성화됨( )을(를) 클릭하여 관리를 일시적으로 비활성화합니다.



관리 비활성화를 진행하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.



관리를 비활성화하면 Firepower Management Center와 디바이스 간 연결이 차단되지만 Firepower Management Center에서 디바이스가 삭제되지는 않습니다.

단계 **5** 수정( )를 클릭하여 **Host(**호스트**)** IP 주소 또는 호스트 이름을 수정합니다.

Management(관리**)** 대화상자에서 **Host(**호스트**)** 필드의 이름 또는 IP 주소를 수정하고 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관리에서 데이터로 FMC 액세스 인터페이스 변경

전용 관리 인터페이스 또는 데이터 인터페이스에서 FTD를 관리할 수 있습니다. 디바이스를 FMC에 추가 한 후 FMC 액세스 인터페이스를 변경하려면 다음 단계에 따라 관리 인터페이스에서 데이터 인터페이스로 마이그레이션합니다. 다른 방향으로 마이그레이션하려면 데이터에서 관리로 FMC 액세스 인터페이스 변경, 321 페이지의 내용 참조하십시오.

관리에서 데이터로의 FMC 액세스 마이그레이션을 시작하면 구축시 FTD에 차단을 적용합니다. 블록을 제거하려면 데이터 인터페이스에서 FMC 액세스를 활성화합니다.

데이터 인터페이스에서 FMC 액세스를 활성화하고 다른 필수 설정도 구성하려면 다음 단계를 참조하십시오.

시작하기 전에

모델 지원—FTD

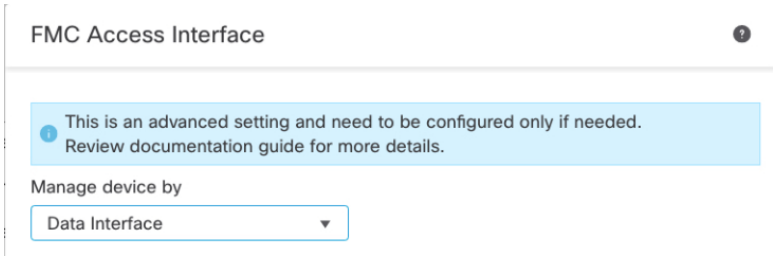
프로시저

단계 1 인터페이스 마이그레이션을 시작합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 디바이스에 대해 수정( )을 클릭합니다.

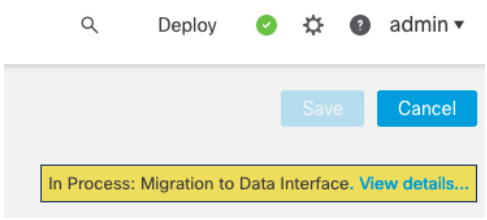
b) **Device(**디바이스**)** > **Management(**관리**)** 섹션으로 이동하여 **FMC Access Interface(FMC** 액세스 인터페이스**)** 링크를 클릭합니다.

FMC Access Interface(FMC 액세스 인터페이스**)** 필드에는 현재 관리 인터페이스가 표시됩니다. 링크를 클릭하면 **Manage device by(**디바이스 관리 기준**)** 드롭 다운 목록에서 새 인터페이스 유형인 **Data Interface(**데이터 인터페이스**)**를 선택합니다.



c) **Save(**저장**)**를 클릭합니다.

이제 데이터 인터페이스에서 FMC 액세스를 활성화하려면 이 절차의 나머지 단계를 완료해야 합니다. Devices(디바이스) 페이지의 오른쪽 상단에 관리 인터페이스를 마이그레이션하고 있음을 나타내는 노란색 배너가 표시됩니다.



View Details(세부 사항 보기**)**를 클릭하면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 세부 사항**)** 대화 상자가 열립니다. **FMC** 액세스 모드에는 In Process(처리 중) 마이그레이션이 표시됩니다.

Configuration		
Version	7.1.0	7.1.0 (Build 1760)
Configuration Cleared		No
FMC Access Mode	Data Interface (Deploy pending)	Management Interface
Connectivity Status	Connected	Connected

단계 2 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 편집**)** > **FMC Access(FMC** 액세스**)** 페이지에서 데이터 인터페이스에 대한 FMC 액세스를 활성화합니다.

라우팅 모드 인터페이스 구성, 817 페이지를 참조하십시오. 하나의 라우팅된 데이터 인터페이스에서 FMC 액세스를 활성화할 수 있습니다. 이 인터페이스가 이름 및 IP 주소로 완전히 구성되어 있고 활성화되어 있는지 확인합니다.

단계 **3** (선택 사항) 인터페이스에 DHCP를 사용하는 경우 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **DHCP** > **DDNS** 페이지에서 웹 유형 DDNS 방법을 활성화합니다.

동적 DNS 구성, 865 페이지를 참조하십시오. DDNS는 FTD의 IP 주소가 변경될 경우 FMC가 FQDN(Fully-Qualified Domain Name)에서 FTD에 연결할 수 있도록 합니다.

단계 **4** FTD가 데이터 인터페이스를 통해 FMC로 라우팅될 수 있는지 확인합니다. **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Static Route(**고정 경로**)**에서 필요한 경우 고정 경로를 추가합니다.

고정 경로 추가, 1038 페이지의 내용을 참조하십시오.

단계 **5** (선택 사항) 플랫폼 설정 정책에서 DNS를 구성하고 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **DNS**에서 이 디바이스에 적용합니다.

DNS 구성, 1425 페이지를 참조하십시오. DDNS를 사용하는 경우 DNS가 필요합니다. 보안 정책에서 FQDN에 대해 DNS를 사용할 수도 있습니다.

단계 **6** (선택 사항) 플랫폼 설정 정책에서 데이터 인터페이스에 대해 SSH를 활성화하고 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Secure Shell(**보안 셸**)**에서 이 디바이스에 적용합니다.

에서 SSH(Secure Shell) 설정, 1435 페이지를 참조하십시오. SSH는 데이터 인터페이스에서 기본적으로 활성화되어 있지 않으므로 SSH를 사용하여 FTD를 관리하려면 그를 명시적으로 허용해야 합니다.

단계 **7** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

FMC는 현재 관리 인터페이스를 통해 구성 변경 사항을 구축합니다. 구축 후에는 데이터 인터페이스를 사용할 수 있지만 관리에 대한 원래 관리 연결은 계속 활성화됩니다.

단계 **8** 콘솔 포트의 FTD CLI에서 관리 인터페이스가 고정 IP 주소를 사용하도록 설정하고 게이트웨이가 데이터 인터페이스를 사용하도록 설정합니다.

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask*-관리 인터페이스를 사용하지 않더라도 고정 IP 주소(예: 개인 주소)를 설정해야 합니다. 데이터 인터페이스 여야하는 기본 경로(다음 글 머리 기호 참조)가 DHCP 서버에서 수신한 경로로 덮어 쓰여질 수 있으므로 DHCP를 사용할 수 없습니다.
- **data-interfaces** —이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 FMC 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.

관리 인터페이스 네트워크 설정을 변경하면 SSH 세션의 연결이 끊어 지므로 SSH 연결 대신 콘솔 포트를 사용하는 것이 좋습니다. 다음과 같은 경우

단계 **9** 필요한 경우 데이터 인터페이스에서 FMC에 연결할 수 있도록 FTD를 다시 케이블로 연결합니다.

단계 **10** FMC에서 관리 연결을 비활성화하고 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)**섹션에서 FTD의 호스트 IP 주소를 업데이트한 다음 연결을 다시 활성화합니다.

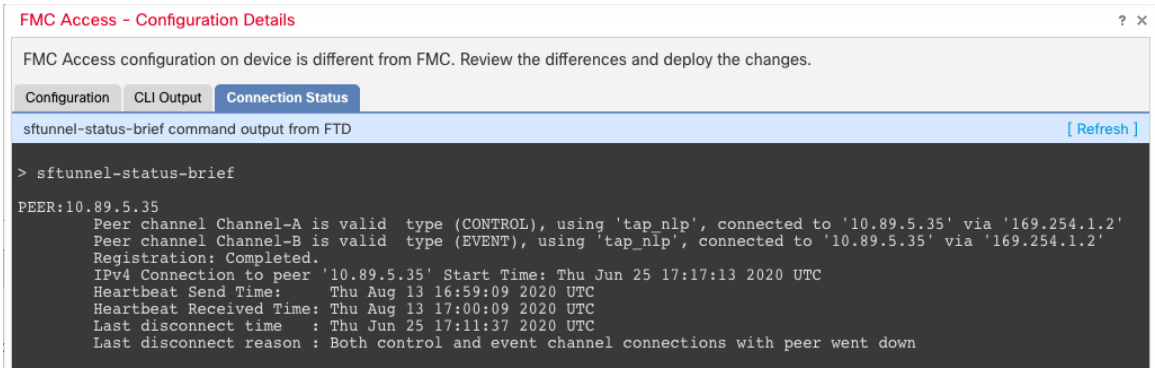
FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지의 내용을 참조하십시오. FTD를 FMC에 추가할 때 FTD 호스트 네임 또는 NAT ID만 사용한 경우, 값을 업데이트할 필요가 없습니다. 그러나 연결을 다시 시작하려면 관리 연결을 비활성화했다가 다시 활성화해야 합니다.

단계 **11** 관리 연결이 다시 설정되었는지 확인합니다.

FMC의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 디테일**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

다음 상태는 내부 "tap_nlp" 인터페이스를 보여주는 데이터 인터페이스의 성공적인 연결을 보여줍니다.



연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 337 페이지의 내용을 참조하십시오.

데이터에서 관리로 FMC 액세스 인터페이스 변경

전용 관리 인터페이스 또는 데이터 인터페이스에서 FTD를 관리할 수 있습니다. 디바이스를 FMC에 추가한 후 FMC 액세스 인터페이스를 변경하려면 다음 단계에 따라 데이터 인터페이스에서 관리 인터페이스로 마이그레이션합니다. 다른 방향으로 마이그레이션하려면 관리에서 데이터로 FMC 액세스 인터페이스 변경, 318 페이지의 내용 참조하십시오.

데이터에서 관리로 FMC 액세스 마이그레이션을 시작하면 FMC가 구축 시 FTD에 차단을 적용합니다. 차단을 제거하려면 데이터 인터페이스에서 FMC 액세스를 비활성화해야 합니다.

데이터 인터페이스에서 FMC 액세스를 비활성화하고 다른 필수 설정도 구성하려면 다음 단계를 참조하십시오.

시작하기 전에

모델 지원—FTD

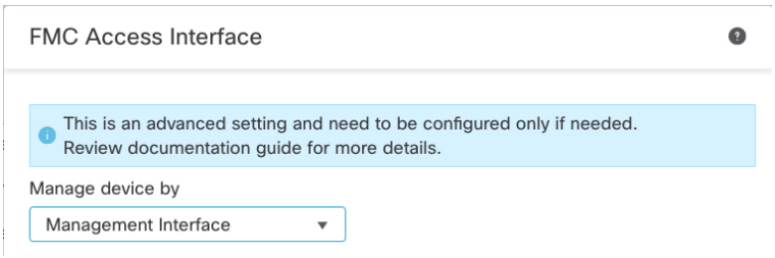
프로시저

단계 **1** 인터페이스 마이그레이션을 시작합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 디바이스에 대해 수정( )을 클릭합니다.

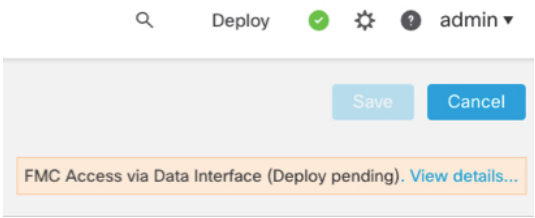
b) **Device(**디바이스**)** > **Management(**관리**)** 섹션으로 이동하여 **FMC Access Interface(FMC** 액세스 인터페이스**)** 링크를 클릭합니다.

FMC Access Interface(FMC 액세스 인터페이스**)** 필드에는 현재 관리 인터페이스가 표시됩니다. 링크를 클릭할 때 **Manage device by(**디바이스 관리 기준**)** 드롭다운 목록에서 새 인터페이스 유형인 **Management Interface(**관리 인터페이스**)**를 선택합니다.

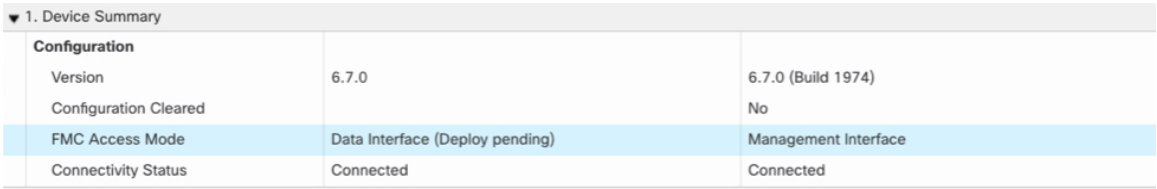


c) **Save(**저장**)**를 클릭합니다.

이제 이 절차의 나머지 단계를 완료하여 관리 인터페이스에서 FMC 액세스를 활성화해야 합니다. Devices(디바이스) 페이지의 오른쪽 상단에 관리 인터페이스를 마이그레이션하고 있음을 나타내는 노란색 배너가 표시됩니다.



View Details(세부 사항 보기**)**를 클릭하면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 세부 사항**)** 대화 상자가 열립니다. **FMC** 액세스 모드에는 In Process(처리 중) 마이그레이션이 표시됩니다.



단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 편집**)** > **FMC Access(FMC** 액세스**)** 페이지에서 데이터 인터페이스에 대한 FMC 액세스를 비활성화합니다.

라우팅 모드 인터페이스 구성, 817 페이지를 참조하십시오. 이 단계에서는 구축 시 차단을 제거합니다.

단계 3 아직 수행하지 않은 경우, 플랫폼 설정 정책에서 데이터 인터페이스에 대한 DNS 설정을 구성하고 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **DNS**에서 해당 디바이스에 적용합니다.

DNS 구성, 1425 페이지를 참조하십시오. 데이터 인터페이스에서 FMC 액세스를 비활성화하는 FMC 구축은 로컬 DNS 설정을 제거합니다. 해당 DNS 서버가 액세스 규칙의 FQDN과 같은 보안 정책에서 사용되는 경우, FMC를 통해 DNS 구성을 다시 적용해야 합니다.

단계 4 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

FMC는 현재 데이터 인터페이스를 통해 구성 변경 사항을 구축합니다.

단계 5 필요한 경우, 관리 인터페이스에서 FMC에 연결할 수 있도록 FTD를 다시 케이블로 연결합니다.

단계 6 FTD CLI에서 고정 IP 주소 또는 DHCP를 사용하여 관리 인터페이스 IP 주소 및 게이트웨이를 설정합니다.

원래 FMC 액세스용 데이터 인터페이스를 설정하면 관리 게이트웨이가 데이터 인터페이스로 설정되었습니다. 이 인터페이스는 관리 트래픽을 백플레인을 통해 전달하여 FMC 액세스 데이터 인터페이스를 통해 라우팅할 수 있도록 지원했습니다. 이제 관리 네트워크에서 게이트웨이의 IP 주소를 설정해야 합니다.

고정 **IP** 주소**:**

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network{**ipv4** | **ipv6**} **dhcp**

단계 7 FMC에서 관리 연결을 비활성화하고 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)**섹션에서 FTD의 호스트 IP 주소를 업데이트한 다음 연결을 다시 활성화합니다.

FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지의 내용을 참조하십시오. FTD를 FMC에 추가할 때 FTD 호스트네임 또는 NAT ID만 사용한 경우, 값을 업데이트할 필요가 없습니다. 그러나 연결을 다시 시작하려면 관리 연결을 비활성화했다가 다시 활성화해야 합니다.

단계 8 관리 연결이 다시 설정되었는지 확인합니다.

FMC의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Status(**상태**)** 필드에서 관리 연결 상태를 확인하거나 FMC에서 알림을 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 337 페이지의 내용을 참조하십시오.

데이터 인터페이스 관리를 위한 FMC 액세스 세부정보 보기

모델 지원—FTD

전용 관리 인터페이스를 사용하는 대신 FMC 관리용 데이터 인터페이스를 사용하는 경우, FMC에서 FTD에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다. 디바이스에서 로컬로 데이터 인터페이스 설정을 변경할 수도 있습니다. 이렇게 하려면 FMC에서 이러한 변경 사항을 수동으로 조정해야 합니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 세부정보**)** 대화 상자를 사용하면 FMC와 FTD 로컬 구성 간의 불일치를 해결할 수 있습니다.

일반적으로 FMC에 FTD를 추가하기 전에 초기 FTD 설정의 일부로 FMC 액세스 데이터 인터페이스를 구성합니다. FMC에 FTD를 추가하면 FMC는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 구성을 검색하고 유지 관리합니다. DNS 서버의 경우 구성이 등록 중에 검색된 경우 로컬로 유지되지만 FMC의 플랫폼 설정 정책에 추가되지 않습니다.

FTD를 FMC에 추가한 후 **configure network management-data-interface** 명령을 사용하여 FTD의 데이터 인터페이스 설정을 로컬로 변경하면 FMC는 구성 변경 사항을 탐지하고 FTD에 대한 구축을 차단합니다. FMC는 다음 방법 중 하나를 사용하여 구성 변경을 탐지합니다.

- FTD에 구축합니다. FMC는 구축하기 전에 구성 차이를 탐지하고 구축을 중지합니다.
- **Interface(**인터페이스**)** 페이지의 **Sync(**동기화**)** 버튼
- **FMC Access Details(FMC** 액세스 상세정보**)** 대화 상자의 **Refresh(**새로 고침**)** 버튼

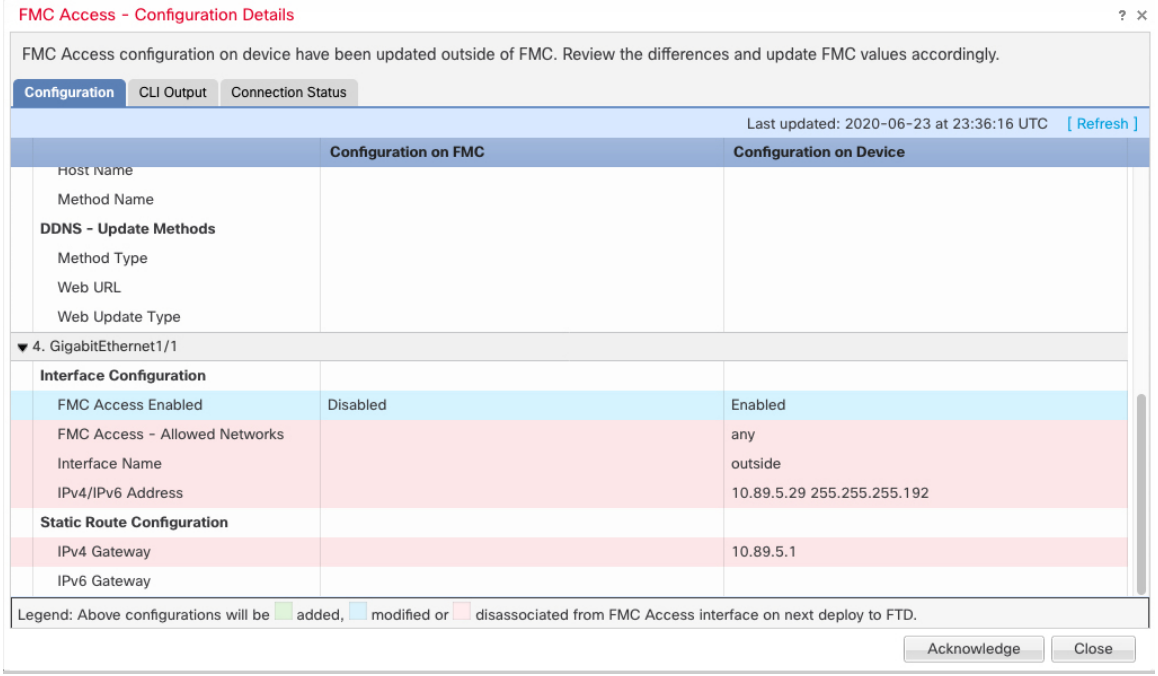
블록을 제거하려면 **FMC Access Details(FMC** 액세스 상세정보**)** 대화 상자로 이동하여 **Acknowledge(**확인**)**를 클릭해야 합니다. 다음에 구축할 때 FMC 컨피그레이션은 FTD의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 FMC에서 컨피그레이션을 수동으로 수정하는 것은 사용자의 책임입니다.

이 대화 상자에서 다음 페이지를 참조하십시오.

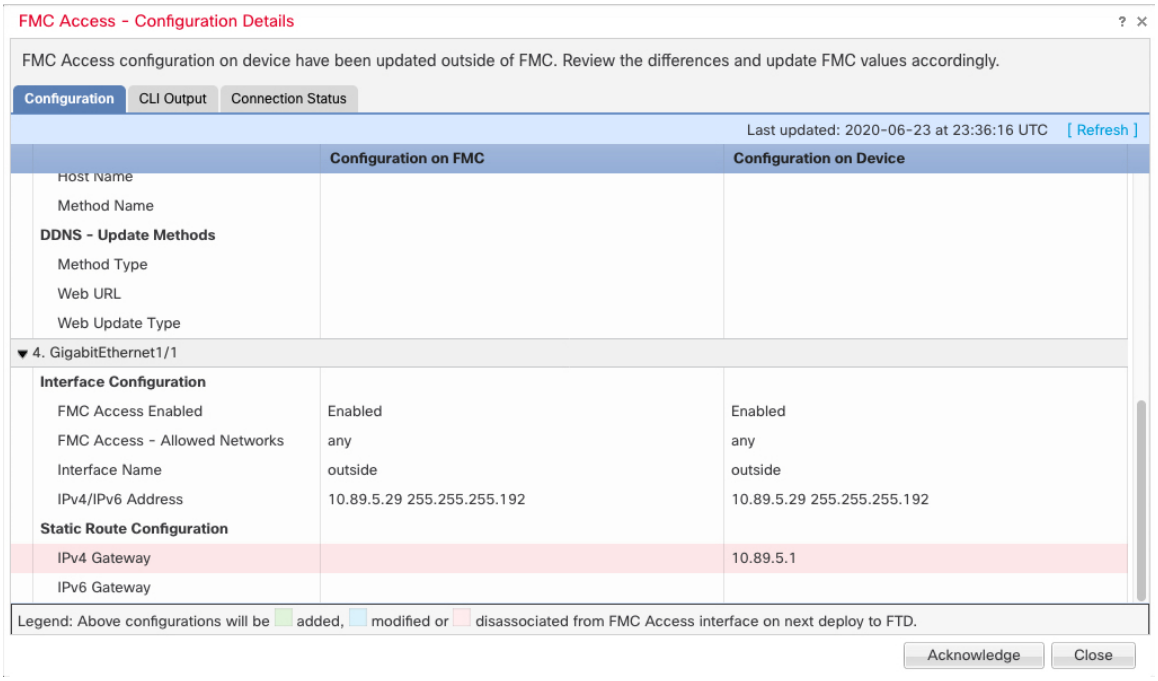
컨피그레이션

FMC 및 FTD에서 FMC 액세스 데이터 인터페이스의 구성 비교를 확인합니다.

다음 예에서는 FTD에서 **configure network management-data-interface** 명령이 입력된 FTD의 구성 세부 사항을 보여줍니다. 분홍으로 강조 표시된 부분은 차이점을 **Acknowledge(**확인**)** 하지만 FMC의 구성과 일치하지 않으면 FTD 구성이 제거됨을 나타냅니다. 파란색으로 강조 표시된 부분은 FTD에서 수정될 구성을 보여줍니다. 녹색으로 강조 표시된 부분은 FTD에 추가될 구성을 보여줍니다.

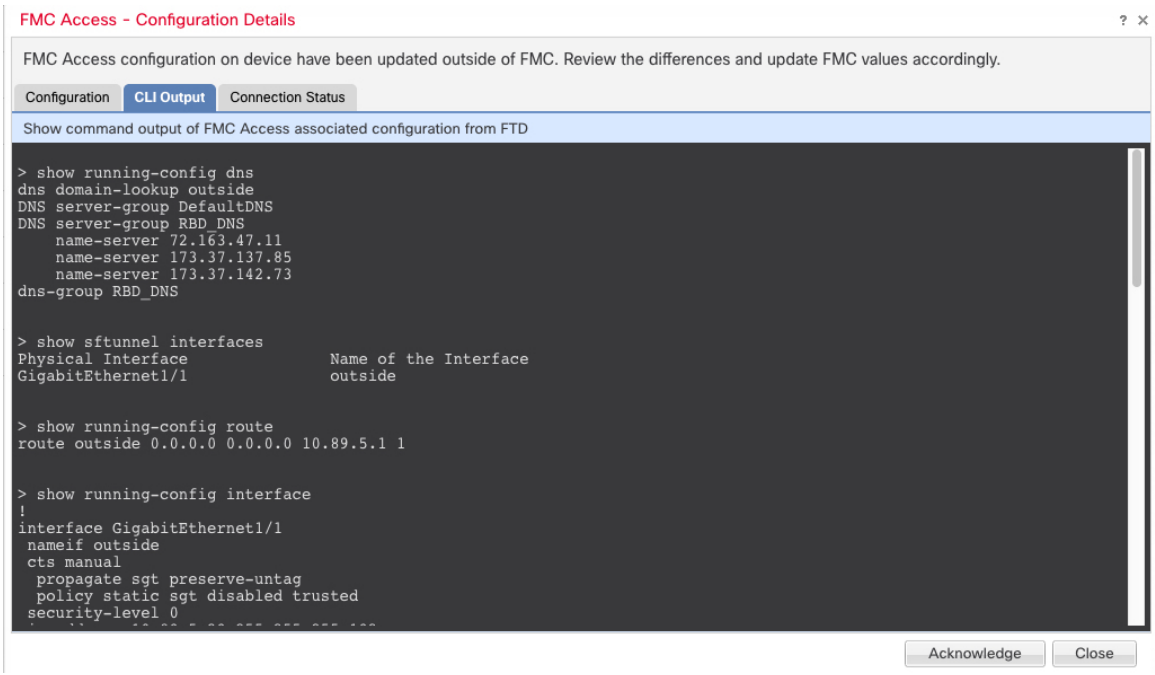


다음 예는 FMC에서 인터페이스를 구성한 후의 이 페이지를 보여줍니다. 인터페이스 설정이 일치하고 분홍색 강조 표시가 제거되었습니다.



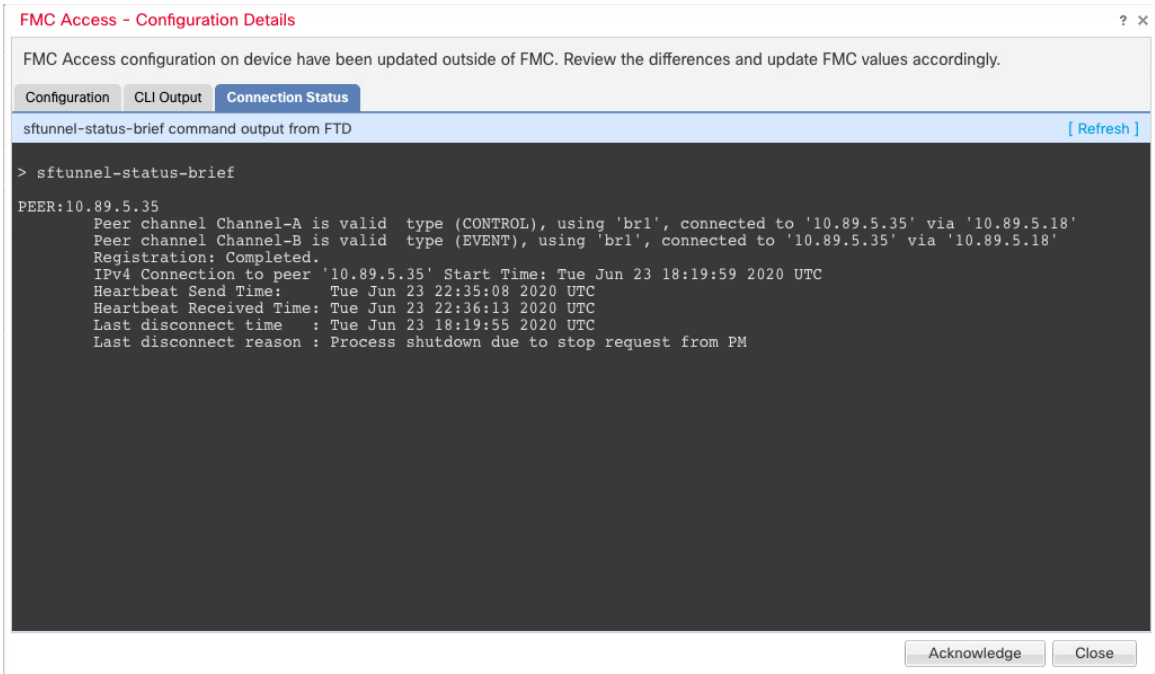
CLI 출력

FMC 액세스 데이터 인터페이스의 CLI 구성을 확인합니다. 이는 기본 CLI에 익숙한 경우 유용합니다.

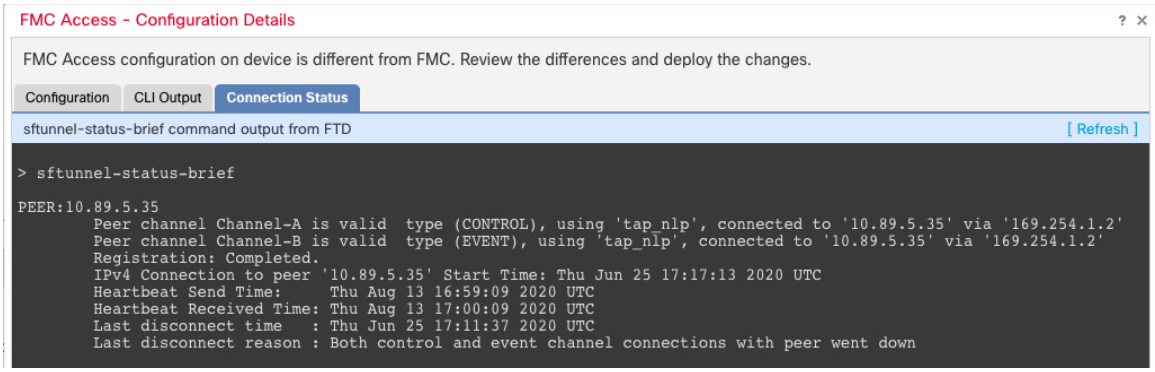


연결 상태

관리 연결 상태를 봅니다. 다음 예는 관리 연결이 여전히 관리 "br1"인터페이스를 사용하고 있음을 보여줍니다.



다음 상태는 내부 "tap_nlp" 인터페이스를 보여주는 데이터 인터페이스의 성공적인 연결을 보여줍니다.



작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

CLI에서 디바이스 관리 인터페이스 수정

CLI를 사용하여 매니지드 디바이스의 관리 인터페이스 설정을 수정합니다. 이러한 설정 중 대부분은 초기 설정을 수행할 때의 설정입니다. 이 절차를 통해 해당 설정을 변경하고 모델에서 지원하는 경우 이벤트 인터페이스를 활성화하거나 정적 경로를 추가하는 등의 추가 설정을 지정할 수 있습니다.

참고 이 항목은 전용 관리 인터페이스에 적용됩니다. 관리를 위해 데이터 인터페이스를 설정할 수도 있습니다. 해당 인터페이스의 네트워크 설정을 변경하려면 CLI가 아닌 FMC 내에서 변경해야 합니다. 중단된 관리 연결을 문제 해결해야 하고 FTD에서 직접 변경해야 하는 경우 CLI에서 관리에 사용되는 FTD 데이터 인터페이스 수정, 334 페이지의 내용을 참조하십시오.

FTD CLI에 대한 자세한 내용은 FTD 명령 참조를 참조하십시오.

클래식 디바이스 CLI에 대한 내용은 이 가이드의 명령줄 참조, 3113 페이지 섹션을 참조하십시오.

FTD 및 클래식 디바이스는 관리 인터페이스 설정에 대해 동일한 명령을 사용합니다. 다른 명령은 플랫폼에 따라 다를 수 있습니다.

참고 SSH를 사용하여 관리 인터페이스를 변경할 때는 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 디바이스 콘솔 포트에 액세스해야 합니다.

참고 디바이스 관리 IP 주소를 변경하는 경우 **configure manager add** 명령을 사용하여 초기 디바이스 설정 중에 FMC를 식별한 방법에 따라 FMC 연결에 대한 다음 작업을 참조하십시오(새 FMC 식별, 352 페이지 참조).

- **IP address(IP 주소)** - 작업이 없습니다**.** 연결 가능한 IP 주소를 사용하여 FMC를 식별한 경우 몇 분 후 관리 연결이 자동으로 다시 설정됩니다. 정보를 동기화 상태로 유지하려면 FMC에 표시되는 디바이스 IP 주소도 변경하는 것이 좋습니다. FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지의 내용을 참조하십시오. 이 작업은 연결을 더 빠르게 재설정하는 데 도움이 될 수 있습니다. 참고: 연결할 수 없는 FMC IP 주소를 지정한 경우 아래의 NAT ID 절차를 참조하십시오.
- **NAT ID**만 - 수동으로 연결을 재설정합니다**.** NAT ID만 사용하여 FMC를 식별한 경우 연결을 자동으로 재설정할 수 없습니다. 이 경우 FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지에 따라 FMC에서 디바이스 관리 IP 주소를 변경합니다.

참고 고가용성 설정에서 등록된 Firepower 디바이스의 관리 IP 주소를 디바이스 CLI 또는 FMC에서 수정하면 보조 FMC는 HA 동기화가 끝나도 변경 사항을 반영하지 않습니다. 보조 FMC도 업데이트되게 하려면 두 FMC의 역할을 바꿔 보조 FMC를 액티브 유닛으로 설정해야 합니다. 현재 액티브 FMC의 디바이스 관리 페이지에 등록한 Firepower 디바이스의 관리 IP 주소를 수정합니다.

시작하기 전에

- Firepower Threat Defense 디바이스의 경우, **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. FTD CLI용 로컬 사용자 계정 생성CLI에서 내부 사용자 추가, 137 페이지 섹션을 참조하십시오.
- 7000 및 8000 Series 디바이스의 경우, 사용자 어카운트 만들기에 설명된 대로 웹 인터페이스에서 사용자 어카운트를 생성할 수 있습니다.

프로시저

단계 **1** 콘솔 포트 또는 SSH를 사용하여 디바이스 CLI에 연결합니다.

7000/8000 시리즈, ASA FirePOWER, NGIPSv 디바이스에서 CLI에 로그인, 36 페이지를 참조하십시오.

단계 **2** 관리자 사용자 이름 및 비밀번호로 로그인합니다.

단계 **3** (Firepower 4100/9300만 해당) 이벤트 전용 인터페이스 사용.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

예제:

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

Firepower Management Center 이벤트 전용 인터페이스는 관리 채널 트래픽을 허용할 수 없으므로 디바이스 이벤트 인터페이스에서 관리 채널을 비활성화해야 합니다.

configure network management-interface disable-events-channel 명령을 사용하여 관리 인터페이스의 이벤트를 선택적으로 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다.

인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.

단계 **4** 관리 인터페이스 및/또는 이벤트 인터페이스의 네트워크 설정을 구성합니다.

management_interface 인수를 지정하지 않으면 기본 관리 인터페이스에 대한 네트워크 설정을 변경하면 됩니다. 이벤트 인터페이스를 구성할 때 *management_interface* 인수를 지정해야 합니다. 이벤트 인터페이스는 관리 인터페이스와 별도의 네트워크에 있거나 동일한 네트워크에 있을 수 있습니다. 구성 중인 인터페이스에 연결되어 있으면 연결이 끊어집니다. 새 IP 주소에 다시 연결할 수 있습니다.

a) IPv4 주소 구성:

- 수동 구성:

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  이 명령의 *gateway_ip*는 디바이스의 기본 경로를 만드는 데 사용됩니다. 이벤트 전용 인터페이스를 설정하는 경우 명령의 일부로 *gateway_ip*를 입력해야 합니다. 그러나 이 항목은 사용자가 지정한 값에 대한 기본 경로만 설정하며 이벤트 인터페이스에 대해 별도의 고정 경로를 생성하지 않습니다. 관리 인터페이스와 다른 네트워크에서 이벤트 전용 인터페이스를 사용하는 경우 관리 인터페이스와 함께 사용할 *gateway_ip*를 설정한 다음 **configure network static-routes** 명령을 사용하여 이벤트 전용 인터페이스에 대해 별도의 고정 경로를 생성하는 것이 좋습니다.

  예:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

- DHCP(기본 관리 인터페이스에서만 지원됨):

  configure network ipv4 dhcp

b) IPv6 주소 구성:

- 상태 비저장 자동 구성:

  configure network ipv6 router [*management_interface*]

  예:

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 수동 구성:

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  이 명령의 *ipv6_gateway_ip*는 디바이스의 기본 경로를 만드는 데 사용됩니다. 이벤트 전용 인터페이스를 설정하는 경우 명령의 일부로 *ipv6_gateway_ip*를 입력해야 합니다. 그러나 이 항목은 사용자가 지정한 값에 대한 기본 경로만 설정하며 이벤트 인터페이스에 대해 별도의 고정 경로를 생성하지 않습니다. 관리 인터페이스와 다른 네트워크에서 이벤트 전용 인터페이스를 사용하는 경우 관리 인터페이스와 함께 사용할 *ipv6_gateway_ip*를 설정한 다음 **configure network static-routes** 명령을 사용하여 이벤트 전용 인터페이스에 대해 별도의 고정 경로를 생성하는 것이 좋습니다.

  예:

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6(기본 관리 인터페이스에서만 지원됨):

  configure network ipv6 dhcp

단계 **5** IPv6의 경우 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 활성화하거나 비활성화합니다. 이러한 메시지는 기본적으로 활성화됩니다.

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 디바이스 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.

예제:

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

단계 **6** (FTD 전용) 기본 관리 인터페이스의 DHCP 서버가 연결된 호스트에 IP 주소를 제공할 수 있게 활성화합니다.

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

예제:

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

관리 인터페이스 IP 주소를 수동으로 설정할 때만 DHCP 서버를 구성할 수 있습니다. 이 명령은 Firepower Threat Defense Virtual에서 지원되지 않습니다. DHCP 서버 상태를 표시하려면 **show network-dhcp-server**:를 입력합니다.

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

단계 **7** Firepower Management Center가 원격 네트워크에 있는 경우 이벤트 전용 인터페이스에 정적 경로를 추가합니다. 그렇지 않으면 모든 트래픽이 관리 인터페이스를 통해 기본 경로와 일치하게 됩니다.

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

기본 경로의 경우 이 명령을 사용하지 마십시오. **configure network ipv4** 또는 **ipv6** 명령을 사용할 때만 기본 경로 게이트웨이 IP 주소를 변경할 수 있습니다(4단계 참조).

라우팅에 대한 내용은 디바이스 관리 인터페이스의 네트워크 라우트, 301 페이지 섹션을 참조하십시오.

예제:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

정적 경로를 표시하려면 **show network-static-routes**를 입력합니다(기본 경로는 표시되지 않음).

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : management1
Destination              : 192.168.6.0
Gateway                  : 10.10.10.1
Netmask                  : 255.255.255.0
[…]
```

단계 **8** 호스트네임 설정

configure network hostname *name*

예제:

```
> configure network hostname farscape1.cisco.com
```

시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.

단계 **9** 검색 도메인 설정:

configure network dns searchdomains *domain_list*

예제:

```
> configure network dns searchdomains example.com,cisco.com
```

디바이스에 대한 검색 도메인을 쉼표로 구분하여 설정합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.

단계 **10** 쉼표로 구분하여 최대 3개의 DNS 서버를 설정합니다.

configure network dns servers *dns_ip_list*

예제:

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

단계 **11** FMC와의 통신을 위한 원격 관리 포트를 설정합니다.

configure network management-interface tcpport *number*

예제:

```
> configure network management-interface tcpport 8555
```

FMC 및 매니지드 디바이스는 기본적으로 포트 8305에 있는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

참고 Cisco에서는 원격 관리 포트에 대해 기본 설정을 유지할 것을 적극 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 디바이스의 설정을 변경해야 합니다.

단계 **12** (FTD 전용) 관리 또는 이벤트 인터페이스 MTU를 설정합니다. MTU는 기본적으로 1500바이트입니다.

configure network mtu [*bytes*] [*interface_id*]

- *bytes* - MTU를 바이트 단위로 설정합니다. 관리 인터페이스의 경우 IPv4를 활성화하는 경우 값의 범위는 64 ~ 1500이고 IPv6를 활성화하는 경우 값은 1280 ~ 1500입니다. 이벤트 인터페이스의 경우 IPv4를 활성화하는 경우 값의 범위는 64 ~ 9000이고 IPv6를 활성화하는 경우 값은 1280 ~ 9000입니다. IPv4 및 IPv6를 모두 활성화하는 경우 최소값은 1280입니다. 바이트를 입력하지 않으면 값을 입력하라는 프롬프트가 표시됩니다.
- *interface_id* — MTU를 설정할 인터페이스 ID를 지정합니다. 플랫폼에 따라 사용 가능한 인터페이스 ID(예: management0, management1, br1, eth0)를 보려면 **show network** 명령을 사용합니다. 인터페이스를 지정하지 않으면 관리 인터페이스가 사용됩니다.

예제:

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

단계 **13** HTTP 프록시를 구성합니다. 디바이스는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다. 명령을 실행하면 HTTP 프록시 주소와 포트, 프록시 인증이 필요한지 여부에 대한 프롬프트가 표시되며, 해당 인증이 필요한 경우 프록시 사용자 이름, 프록시 비밀번호, 프록시 비밀번호의 확인에 대한 프롬프트가 표시됩니다.

참고 Cisco Firepower Threat Defense의 프록시 비밀번호의 경우 A-Z, a-z 및 0-9 문자만 사용할 수 있습니다.

configure network http-proxy

예제:

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

단계 **14** 디바이스 관리 IP 주소를 변경하는 경우 **configure manager add** 명령을 사용하여 초기 디바이스 설정 중에 FMC를 식별한 방법에 따라 FMC 연결에 대한 다음 작업을 참조하십시오(새 FMC 식별, 352 페이지 참조).

- **IP address(IP 주소)** - 작업이 없습니다. 연결 가능한 IP 주소를 사용하여 FMC를 식별한 경우 몇 분 후 관리 연결이 자동으로 다시 설정됩니다. 정보를 동기화 상태로 유지하려면 FMC에 표시되

는 디바이스 IP 주소도 변경하는 것이 좋습니다. FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지의 내용을 참조하십시오. 이 작업은 연결을 더 빠르게 재설정하는 데 도움이 될 수 있습니다. 참고: 연결할 수 없는 FMC IP 주소를 지정한 경우 FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지을(를) 사용하여 연결을 수동으로 다시 설정해야 합니다.

- **NAT ID**만 - 수동으로 연결을 재설정합니다**.** NAT ID만 사용하여 FMC를 식별한 경우 연결을 자동으로 재설정할 수 없습니다. 이 경우 FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지에 따라 FMC에서 디바이스 관리 IP 주소를 변경합니다.

CLI에서 관리에 사용되는 FTD 데이터 인터페이스 수정

FTD와 FMC 간의 관리 연결이 중단된 상태에서 기존 인터페이스를 대체할 새 데이터 인터페이스를 지정하려는 경우 FTD CLI를 사용하여 새 인터페이스를 설정합니다. 이 절차에서는 동일한 네트워크에서 기존 인터페이스를 새 인터페이스로 교체하려 한다고 가정합니다. 관리 연결이 활성 상태이면 FMC를 사용하여 기존 데이터 인터페이스를 변경해야 합니다. 데이터 관리 인터페이스의 초기 설정에 대해서는 FTD 초기 설정 완료, 305 페이지에서 **configure network management-data-interface** 명령을 참조하십시오.

참고 이 항목은 전용 관리 인터페이스가 아니라 관리용으로 설정한 데이터 인터페이스에 적용됩니다. 관리 인터페이스의 네트워크 설정을 변경하려면 CLI에서 디바이스 관리 인터페이스 수정, 327 페이지의 내용을 참조하십시오.

FTD CLI에 대한 자세한 내용은 FTD 명령 참조를 참조하십시오.

시작하기 전에

- **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 사용자 계정을 생성할 수 있습니다. CLI에서 내부 사용자 추가, 137 페이지의 내용을 참조하십시오. SSH에 대한 외부 인증 설정에 따라 AAA 사용자를 구성할 수도 있습니다.

프로시저

단계 **1** 데이터 관리 인터페이스를 새 인터페이스로 변경하는 경우 현재 인터페이스 케이블을 새 인터페이스로 이동합니다.

단계 **2** 디바이스 CLI에 연결합니다.

이러한 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 초기 설정을 수행하는 경우 관리 인터페이스에서 연결이 끊어질 수 있습니다. 관리 연결이 중단되어 구성을 수정하는 경우 전용 관리 인터페이스에 대한 SSH 액세스 권한이 있는 경우 해당 SSH 연결을 사용할 수 있습니다.

FTD디바이스의FTD 명령줄 인터페이스에 로그인의 내용을 참조하십시오.

단계 **3** 관리자 사용자 이름 및 비밀번호로 로그인합니다.

단계 **4** FMC 액세스 인터페이스의 이름을 설정하십시오.

configure network management-data-interface

그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

데이터 관리 인터페이스를 동일한 네트워크의 새 인터페이스로 변경할 때는 인터페이스 ID를 제외하고 이전 인터페이스와 동일한 설정을 사용합니다. 또한, 적용하기 전에 모든 디바이스 구성을 지우시겠습니까**? (y/n) [n]:** 옵션에 대해 **y**를 선택합니다. 이 옵션을 선택하면 이전 데이터 관리 인터페이스 구성이 지워지므로 새 인터페이스에서 IP 주소 및 인터페이스 이름을 성공적으로 재사용할 수 있습니다.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 **5** (선택 사항) 특정 네트워크에서 FMC에 대한 데이터 인터페이스 액세스를 제한합니다.

configure network management-data-interface client *ip_address netmask*

기본적으로 모든 네트워크가 허용됩니다.

단계 **6** 연결은 자동으로 재설정되지만 FMC에서 연결을 비활성화했다가 다시 활성화하면 연결을 더 빠르게 재설정하는 데 도움이 됩니다. FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지의 내용을 참조하십시오.

단계 **7** 관리 연결이 재설정되었는지 확인합니다.

sftunnel-status-brief

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

단계 **8** FMC에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 세부 정보**)**를 선택하고 **Refresh(**새로 고침**)**를 클릭합니다.

FMC는 인터페이스 및 기본 경로 구성 변경을 탐지하고 FTD에 대한 구축을 차단합니다. 디바이스에서 로컬로 데이터 인터페이스 설정을 변경하는 경우 FMC에서 수동으로 변경 사항을 조정해야 합니다. **Configuration(**구성**)** 탭에서 FMC와 FTD 간의 불일치를 볼 수 있습니다.

단계 **9** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택하고 다음을 변경합니다.

a) 이전 데이터 관리 인터페이스에서 IP 주소와 이름을 제거하고 이 인터페이스에 대해 FMC 액세스를 비활성화합니다.

b) 이전 인터페이스(CLI에서 사용한 인터페이스)의 설정으로 새 데이터 관리 인터페이스를 설정하고 FMC 액세스를 활성화합니다.

단계 **10** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Static Route(**고정 경로**)**를 선택하고 기존 데이터 관리 인터페이스에서 새 경로로 기본 경로를 변경합니다.

단계 **11** **FMC Access Details(FMC** 액세스 세부 정보**)** 대화 상자로 돌아가서 **Acknowledge(**확인**)**를 클릭하여 구축 블록을 제거합니다.

다음에 구축할 때 FMC 구성은 FTD의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 FMC에서 구성을 수동으로 수정하는 것은 사용자의 책임입니다.

"Config was cleared(구성이 지워졌습니다)" 및 "FMC Access changed and acknowledged(FMC 액세스가 변경되어 승인되었습니다)"라는 메시지가 표시됩니다.

FMC가 연결을 상실할 경우 컨피그레이션을 롤백

FMC 관리를 위해 FTD에서 데이터 인터페이스를 사용하고 네트워크 연결에 영향을 주는 FMC에서 구성 변경 사항을 구축하는 경우 관리 연결을 복원할 수 있도록 FTD의 구성을 마지막으로 구축된 구성으로 롤백할 수 있습니다. 그런 다음 네트워크 연결이 유지되도록 FMC에서 구성 설정을 조정하고 다시 구축할 수 있습니다. 연결이 끊기지 않아도 롤백 기능을 사용할 수 있습니다. 이는 이 문제 해결 상황으로 제한되지 않습니다.

다음 지침을 참조하십시오.

- 이전 구축만 FTD에서 로컬로 사용할 수 있습니다. 이전 구축으로 롤백할 수 없습니다.
- 고가용성 또는 클러스터링 구축에서는 롤백이 지원되지 않습니다.
- 롤백은 FMC에서 설정할 수 있는 구성에만 영향을 미칩니다. 예를 들어 롤백은 FTD CLI에서만 구성할 수 있는 전용 관리 인터페이스와 관련된 로컬 구성에 영향을주지 않습니다. **configure network management-data-interface** 명령을 사용하여 마지막 FMC 구축 후 데이터 인터페이스 설정을 변경한 다음 롤백 명령을 사용하면 해당 설정이 유지되지 않습니다. 마지막으로 구축된 FMC 설정으로 롤백됩니다.
- UCAPL/CC 모드는 롤백할 수 없습니다.
- 이전 구축 중에 업데이트된 OOB(Out of Band) SCEP 인증서 데이터는 롤백할 수 없습니다.

- 롤백 중에는 현재 구성이 지워지므로 연결이 삭제됩니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 **1** FTD CLI에서 이전 구성으로 롤백합니다.

configure policy rollback

롤백 후 FTD는 롤백이 성공적으로 완료되었음을 FMC에 알립니다. FMC에서 구축 화면에는 구성이 롤백되었음을 알리는 배너가 표시됩니다.

롤백에 실패한 경우, 일반적인 구축 문제에 대한 https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html의 내용을 참조하십시오. 경우에 따라 FMC 관리 액세스가 복원된 후 롤백이 실패할 수 있습니다. 이 경우 FMC 구성 문제를 해결하고 FMC에서 다시 구축할 수 있습니다.

예제:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

단계 **2** 관리 연결이 재설정되었는지 확인합니다.

FMC의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 디테일**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 337 페이지의 내용을 참조하십시오.

데이터 인터페이스에서 관리 연결성 문제 해결

모델 지원—FTD

전용 관리 인터페이스를 사용하는 대신 FMC 관리용 데이터 인터페이스를 사용하는 경우, FMC에서 FTD에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다. FMC에 FTD를 추가한 후 관리 인터페이스 유형을 데이터에서 관리로 또는 관리에서 데이터로 변경하는 경우, 인터페이스 및 네트워크 설정이 올바르게 설정되지 않으면 관리 연결이 끊어질 수 있습니다.

이 주제는 관리 연결 끊김 문제를 해결하는 데 도움이 됩니다.

관리 연결 상태 보기

FMC의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 디테일**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다. **sftunnel-status** 명령을 사용하여 전체 정보를 볼 수도 있습니다.

작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

FTD 네트워크 정보 보기

FTD CLI에서 관리 및 FMC 액세스 데이터 인터페이스 네트워크 설정을 확인합니다.

show network

```
> show network
===============[ System Information ]===============
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port         : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces
```

```
======================[ br1 ]=======================
State                        : Enabled
Link                         : Up
Channels                     : Management & Events
Mode                         : Non-Autonegotiation
MDI/MDIX                     : Auto/MDIX
MTU                          : 1500
MAC Address                  : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration                : Manual
Address                      : 10.99.10.4
Netmask                      : 255.255.255.0
Gateway                      : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration                : Disabled

===============[ Proxy Information ]================
State                        : Disabled
Authentication               : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers                  :
Interfaces                   : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                        : Enabled
Link                         : Up
Name                         : outside
MTU                          : 1500
MAC Address                  : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration                : Manual
Address                      : 10.89.5.29
Netmask                      : 255.255.255.192
Gateway                      : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration                : Disabled
```

FTD가 **FMC**에 등록되었는지 확인합니다**.**

FTD CLI에서 FMC 등록이 완료되었는지 확인합니다. 이 명령은 관리 연결의 현재 상태를 표시하지 않습니다.

show managers

```
> show managers
Type                         : Manager
Host                         : 10.89.5.35
Registration                 : Completed

>
```

FMC ping

FTD CLI에서 다음 명령을 사용하여 데이터 인터페이스에서 FMC를 ping합니다.

ping *fmc_ip*

FTD CLI에서 다음 명령을 사용하여 관리 인터페이스에서 FMC를 ping합니다. 이 인터페이스는 백플레인을 통해 데이터 인터페이스로 라우팅되어야 합니다.

ping system *fmc_ip*

FTD 내부 인터페이스에서 패킷 캡처

FTD CLI에서 내부 백플레인 인터페이스(nlp_int_tap)의 패킷을 캡처하여 관리 패킷이 전송되는지 확인합니다.

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture *name* **trace detail**

내부 인터페이스 상태, 통계 및 패킷 수 확인

FTD CLI에서 내부 백플레인 인터페이스, nlp_int_tap에 대한 정보를 참조하십시오.

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

라우팅 및 **NAT** 확인

FTD CLI에서 기본 경로(S *)가 추가되었고 관리 인터페이스(nlp_int_tap)에 대한 내부 NAT 규칙이 있는지 확인합니다.

show route

```
> show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

다른 설정 확인

다른 모든 설정이 있는지 확인하려면 다음 명령을 참조하십시오. FMC의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **FMC Access Details(FMC** 액세스 세부 사항**)** > **CLI Output(CLI** 출력**)** 페이지에서 이러한 명령을 많이 볼 수 있습니다.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
```

```
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

성공적인 **DDNS** 업데이트 확인

FTD CLI에서 DDNS 업데이트에 성공했는지 확인합니다.

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

업데이트가 실패하면 **debug http** 및 **debug ssl** 명령을 사용합니다. 인증서 검증에 실패한 경우, 다음을 통해 루트 인증서가 디바이스에 설치되어 있는지 확인합니다.

show crypto ca certificates *trustpoint_name*

DDNS 작업을 확인하려면 다음 명령을 사용하십시오.

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

FMC 로그 파일 확인

https://cisco.com/go/fmc-reg-error를 참조하십시오.

일반 설정 편집

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 수정할 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** 일반 섹션에서 수정( )을 클릭합니다.

단계 **5** 매니지드 디바이스의 이름을 입력합니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 스택 페이지에서 스택에 할당된 디바이스 이름을 편집합니다. 어플라이언스 편집기의 디바이스 페이지에서 개별 디바이스에 할당된 디바이스 이름을 편집할 수 있습니다.

단계 **6** **Transfer Packets(**패킷 전송**)** 설정을 변경합니다.

- 체크 박스를 선택하여 패킷 데이터가 이벤트와 함께 Firepower Management Center에 저장되도록 합니다.
- 관리되는 디바이스가 이벤트로 패킷 데이터를 전송하는 것을 방지하려면 체크 박스를 비워둡니다.

단계 **7** 디바이스에 현재 정책 및 디바이스 설정의 구축을 강제로 구축하려면 **Force Deploy(**강제 구축**)**을 클릭합니다.

참고 강제 구축은 FTD에 구축할 정책 규칙의 완전한 생성을 포함하므로 일반 구축보다 더 많은 시간을 소비합니다.

단계 **8** **Deploy(**구축**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

다른 디바이스에 구성 복사

새로운 디바이스가 네트워크에 구축되면 새 디바이스를 수동으로 다시 구성하는 대신 사전 구성된 디바이스에서 설정 및 정책을 쉽게 복사할 수 있습니다.

시작하기 전에

다음을 확인합니다.

- 소스 및 대상 Firepower Threat Defense 디바이스가 동일한 모델이며 동일한 버전의 Firepower 소프트웨어가 실행 중입니다.
- 소스는 독립형 Firepower Threat Defense 디바이스 또는 Firepower Threat Defense 고가용성 쌍입니다.
- 대상 디바이스는 독립형 Firepower Threat Defense 디바이스입니다.
- 소스 및 대상 Firepower Threat Defense 디바이스에는 동일한 수의 물리적 인터페이스가 있습니다.

- 소스 및 대상 Firepower Threat Defense 디바이스는 동일한 방화벽 모드(라우팅됨 또는 투명)를 사용합니다.
- 소스 및 대상 Firepower Threat Defense 디바이스는 동일한 보안 인증 규정 준수 모드 상태에 있습니다.
- 소스 및 대상 Firepower Threat Defense 디바이스가 동일한 도메인에 있습니다.
- 소스 및 대상 Firepower Threat Defense 디바이스에서 구성 구축이 진행되고 있지 않습니다.

모델 지원—FTD

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 수정할 디바이스 옆의 수정( )를 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** 일반 섹션에서 다음 중 하나를 수행합니다.

- 디바이스 컨피그레이션 가져오기( )를 클릭하여 다른 디바이스에서 새 디바이스로 디바이스 설정을 복사합니다. 디바이스 설정 가져오기 페이지의 디바이스 선택 드롭다운 목록에서 소스 디바이스를 선택합니다.
- 디바이스 컨피그레이션 푸시( )를 클릭하여 현재 디바이스에서 새 디바이스로 디바이스 설정을 복사합니다. 디바이스 설정 푸시 페이지의 대상 디바이스 드롭다운 목록에서 설정을 복사할 대상을 선택합니다.

단계 **5** (선택 사항) 정책을 복사하려면 **Include shared policies configuration(**공유 정책 구성 포함**)** 확인란을 선택합니다.

AC 정책, NAT, 플랫폼 설정 및 FlexConfig 정책 같은 공유 정책은 여러 디바이스에 공유할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

메시지 센터의 작업에서 디바이스 설정 작업 복사 상태를 모니터링할 수 있습니다.

디바이스 설정 복사 작업이 시작되면 대상 디바이스의 설정을 삭제하고 소스 디바이스의 설정을 대상 장치에 복사합니다.

경고! 디바이스 설정 복사 작업을 완료하면 대상 디바이스를 원래 설정으로 되돌릴 수 없습니다.

라이선스 설정 편집

Firepower Management Center에 사용 가능한 라이선스가 있으면 디바이스에서 라이선스를 활성화할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 라이선스를 활성화 또는 비활성화하려는 디바이스 옆에 있는 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭합니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 스택 페이지에서 스택에 대한 라이선스를 활성화 또는 비활성화합니다.

단계 **4** 라이선스 섹션 옆에 있는 수정( )을 클릭합니다.

단계 **5** 관리되는 디바이스에서 활성화 또는 비활성화 하려는 라이선스 옆의 체크 박스를 선택하거나 선택 취소합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

고급 설정 편집

다음 주제에서는 고급 디바이스 설정을 편집하는 방법에 대해 설명합니다.

참고 패킷 전송 설정에 대한 자세한 내용은 일반 설정 편집, 342 페이지를 참고하십시오.

AAB(Automatic Application Bypass) 구성

AAB(Automatic Application Bypass)를 사용하면 Snort가 다운된 경우 또는 클래식 디바이스의 경우 패킷 처리에 시간이 너무 오래 걸리는 경우 패킷이 탐지를 우회할 수 있습니다. AAB는 장애 발생 후 10분 이내에 Snort를 재시작하고, Snort 장애의 원인을 조사하기 위해 분석할 수 있는 문제 해결 데이터를 생성합니다.

주의 AAB 활성화는 Snort 프로세스를 일부 재시작하여 일부 패킷의 검사를 일시적으로 중단합니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

다음 동작을 참조하십시오.

FTD 동작: Snort가 중단된 경우 지정된 타이머 기간 후에 AAB가 트리거됩니다. Snort가 작동하면 패킷 처리가 설정된 타이머를 초과하더라도 AAB가 트리거되지 않습니다.

기본 디바이스 동작: AAB는 인터페이스를 통해 패킷을 처리하는 데 허용되는 시간을 제한합니다. 패킷 처리 지연을 패킷 대기 시간을 위한 네트워크의 허용 오차와 균형을 맞춥니다.

이 기능은 모든 배포에서 기능하지만, 인라인 배포에서 특히 유용합니다.

일반적으로 레이턴시 임계값이 초과된 후 빠른 경로 패킷에 대한 침입 정책에서 Rule Latency Thresholding을 사용합니다. 규칙 레이턴시 임계값은 엔진을 종료하거나 문제 해결 데이터를 생성하지 않습니다.

탐지가 우회되면 디바이스는 상태 모니터링 알림을 생성합니다.

기본적으로 AAB는 비활성화되어 있습니다. AAB를 활성화하려면 단계 설명을 따릅니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 고급 디바이스 설정을 수정할 디바이스 옆에 있는 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**(또는 스태킹된 디바이스의 경우 **Stack(**스택**)**)을 클릭하고, **Advanced Settings(**고급 설정**)** 섹션에서 수정( )을 클릭합니다.

단계 **4** **AAB(Automatic Application Bypass)**를 선택합니다.

단계 **5** 250~60000밀리초 사이의 우회 임계값을 입력합니다. 기본 설정은 3000밀리초(ms)입니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

로컬 라우터 트래픽 검사

로컬에서 바인딩된 트래픽이 레이어 3 구축의 모니터링 규칙과 일치하면 해당 트래픽은 검사를 우회할 수 있습니다. 트래픽의 검사를 위해 로컬 라우터 트래픽 검사를 활성화합니다.

시작하기 전에

모델 지원—7000 및 8000 Series

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 고급 디바이스 설정을 수정할 디바이스 옆에 있는 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭(또는 스태킹된 디바이스의 경우 **Stack(**스택**)**)한 다음 **Advanced Settings(**고급 설정**)** 섹션에서 수정( )을 클릭합니다.

단계 **4** 7000 또는 8000 Series 디바이스가 라우터로 구축된 경우 예외 트래픽을 검사하려면 로컬 라우터 트래픽 검사를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

빠른 경로 규칙(8000 Series) 설정

초기 트래픽 처리의 형태로 8000 Series 빠른 경로 규칙은 추가 검사나 로그인 없이 8000 Series 디바이스로 트래픽을 직접 보낼 수 있습니다. (수동 배포에서 8000 Series 빠른 경로 규칙은 단순히 분석을 중지합니다.) 각 8000 Series 빠른 경로 규칙은 특정 보안 영역 또는 인라인 인터페이스 세트에 적용됩니다. 8000 Series 빠른 경로 규칙은 하드웨어 레벨에서 기능하기 때문에 간단한 외부 헤더 기준을 따르기만 하면 빠른 경로 규칙을 사용할 수 있습니다.

- 이니시에이터 또는 응답자 IP 주소 또는 주소 블록
- TCP와 UDP에 대한 프로토콜, 이니시에이터 및 응답자 포트
- VLAN ID

기본적으로 8000 Series 빠른 경로 규칙은 특정 이니시에이터부터 특정 응답자의 연결에 영향을 줍니다. 호스트가 이니시에이터이거나 응답자인 것과 관계없이 규칙의 조건을 충족하는 모든 연결에 대한 빠른 경로를 만들기 위해 규칙을 양방향으로 만들 수 있습니다.

참고 TCP 또는 UDP 트래픽에 모든 이외의 포트를 지정하면 프래그먼트 트래픽에 일치하는 첫 프래그먼트만 빠른 경로로 지정됩니다. 다른 모든 프래그먼트는 추가 검사를 위해 전달됩니다. 8000 Series은 각 프래그먼트의 IP 헤더가 빠른 경로 규칙을 일치시키는 데 필요한 모든 IP 헤더 정보를 포함하고 하위 프래그먼트가 포트를 식별하는 필드를 포함하지 않았을 때에만 프래그먼트 트래픽을 빠른 경로로 지정하기 때문입니다.

시작하기 전에

모델 지원—8000 Series

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 규칙을 설정하려는 8000 Series 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭(또는 스태킹된 디바이스의 경우 **Stack(**스택**)**)한 다음 Advanced Settings(고급 설정) 섹션에서 수정( )을 클릭합니다.

단계 **4** 새 **IPv4** 규칙 또는 새 **IPv6** 규칙을 클릭합니다.

단계 **5** 도메인 드롭다운 목록에서 인라인 집합 또는 패시브 보안 영역을 선택합니다.

단계 **6** 빠른 경로로 지정하고 싶은 트래픽을 설정합니다. 트래픽은 빠른 경로로 지정되기 위한 모든 조건을 충족해야 합니다.

- 이니시에이터 및 응답자(필수): 이니시에이터 및 응답자의 IP 주소 또는 주소 블록을 입력합니다.
- 프로토콜: 프로토콜을 선택하거나 **All(**전체**)**을 클릭합니다.
- 이니시에이터 포트 및 응답자 포트: TCP 및 UDP 트래픽의 경우 이니시에이터 및 응답자 포트를 입력합니다. 필드를 공백으로 두거나 모든을 입력하여 모든 TCP 또는 UDP 트래픽을 일치시킵니다. 쉼표로 구분된 포트 목록은 입력할 수 있지만 포트 범위는 입력할 수 없습니다.
- VLAN: VLAN ID를 입력합니다. 필드를 공백으로 두거나 모든을 입력하여 VLAN 태그와 관계없이 모든 트래픽을 일치시킵니다.

단계 **7** (선택 사항) 규칙을 양방향으로 설정합니다.

단계 **8** 저장을 클릭하여 다시 저장합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

개체 그룹 검색 구성

작동하는 동안 FTD 디바이스는 액세스 규칙에 사용되는 모든 네트워크 또는 인터페이스 개체의 컨텐츠에 따라 액세스 컨트롤 규칙을 여러 액세스 컨트롤 목록 항목으로 확장합니다. 개체 그룹 검색을 활성화하여 액세스 컨트롤 규칙을 검색하는 데 필요한 메모리를 줄일 수 있습니다. 개체 그룹 검색을 사용하면 시스템이 네트워크 또는 인터페이스 개체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 개체 그룹 검색은 액세스 규칙이 정의된 방식 또는 Firepower 디바이스 관리자에 표시되는 방식에 영향을 주지 않습니다. 이는 액세스 컨트롤 규칙과의 연결을 일치시키는 동안 디바이스가 이를 해석 및 처리하는 방법에만 영향을 미칩니다.

개체 그룹 검색을 활성화하면 네트워크 또는 인터페이스 개체를 포함하는 액세스 컨트롤 정책에 대한 메모리 요구 사항이 감소합니다. 그러나 개체 그룹 검색은 또한 규칙 조회 성능을 저하시켜 CPU 사용률이 증가한다는 점에 유의해야 합니다. 특정 액세스 컨트롤 정책에 대한 감소된 메모리 요구 사항에 대한 CPU 영향의 균형을 유지해야 합니다. 대부분의 경우, 개체 그룹 검색을 활성화하면 네트워크 운영이 개선됩니다.

개체 그룹 검색은 기본적으로 비활성화되어 있습니다. 한 번에 하나의 디바이스에서 활성화할 수 있으며 전역적으로 활성화할 수 없습니다. 네트워크 또는 인터페이스 개체를 사용하는 액세스 규칙을 구축하는 모든 디바이스에서 이 기능을 활성화하는 것이 좋습니다.

참고 개체 그룹 검색을 활성화한 다음 잠시 동안 디바이스를 구성하고 작동할 경우 나중에 기능을 비활성화하면 원하지 않는 결과가 발생할 수 있습니다. 개체 그룹 검색을 비활성화할 경우 디바이스의 실행 중인 구성에서 기존 액세스 제어 규칙이 확장됩니다. 확장에 디바이스에서 사용할 수 있는 것보다 많은 메모리가 필요할 경우 디바이스는 일관적이지 않은 상태로 남아있을 수 있으며 성능에 영향을 미칠 수 있습니다. 디바이스가 정상적으로 작동중인 경우 활성화한 개체 그룹 검색을 비활성화해서는 안 됩니다.

시작하기 전에

- 모델 지원—FTD
- 각 디바이스에서 트랜잭션 커밋도 활성화하는 것이 좋습니다. 디바이스 CLI에서 **asp rule-engine transactional-commit access-group** 명령을 입력합니다.
- 이 설정을 변경하면 디바이스가 ACL을 다시 컴파일하는 동안 시스템 작동이 중단될 수 있습니다. 유지 보수 기간 중에 이 설정을 변경하는 것이 좋습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 규칙을 설정하려는 FTD 디바이스 옆의 수정( )을 클릭합니다.

단계 **3** **Device(**디바이스**)** 탭을 클릭한 다음 **Advanced Settings(**고급 설정**)**섹션에서 수정( )을 클릭합니다.

단계 **4** 개체 그룹 검색을 선택합니다.

단계 **5** 네트워크 개체 외에 인터페이스 개체에서도 개체 그룹 검색을 수행하려면 **Interface Object Optimization(**인터페이스 개체 최적화**)**을 선택합니다.

Interface Object Optimization(인터페이스 개체 최적화**)**을 선택하지 않으면 시스템은 각 소스/인터페이스 쌍에 대해 별도의 규칙을 구축합니다. 규칙에 사용되는 보안 영역 및 인터페이스 그룹을 사용합니다. 이는 인터페이스 그룹을 개체 그룹 검색 처리에 사용할 수 없음을 의미합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

인터페이스 개체 최적화 구성

구축 중 액세스 제어 및 사전 필터 정책에서 사용하는 인터페이스 그룹 및 보안 영역은 각 소스/대상 인터페이스 쌍에 대해 별도의 규칙을 생성합니다. 인터페이스 개체 최적화를 활성화하면 시스템은 대신 액세스 제어/사전 필터 규칙에 따라 단일 규칙을 구축하여 디바이스 설정을 간소화하고 구축 성능을 개선할 수 있습니다. 이 옵션을 선택하는 경우, **Object Group Search(**개체 그룹 검색**)** 옵션도 선택하여 디바이스의 메모리 사용량을 줄일 수 있습니다.

인터페이스 개체 최적화는 기본적으로 비활성화되어 있습니다. 한 번에 하나의 디바이스에서 활성화할 수 있으며, 전역적으로 활성화할 수 없습니다.

참고 인터페이스 개체 최적화를 비활성화하면 인터페이스 개체를 사용하지 않고 기존 액세스 제어 규칙이 구축되므로 구축 시간이 더 오래 걸릴 수 있습니다. 또한 개체 그룹 검색을 활성화하면 인터페이스 개체에 이점이 적용되지 않으며, 디바이스의 실행 중인 설정에서 액세스 제어 규칙이 확장되어 표시될 수 있습니다. 확장에 디바이스에서 사용할 수 있는 것보다 많은 메모리가 필요할 경우 디바이스는 일관적이지 않은 상태로 남아있을 수 있으며 성능에 영향을 미칠 수 있습니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 규칙을 설정하려는 FTD 디바이스 옆의 수정( )을 클릭합니다.

단계 **3** **Device(**디바이스**)** 탭을 클릭한 다음 **Advanced Settings(**고급 설정**)**섹션에서 수정( )을 클릭합니다.

단계 **4** **Interface Object Optimization(**인터페이스 개체 최적화**)**을 확인합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

디바이스의 관리자 변경

다음과 같은 상황에서는 디바이스에서 관리자를 변경해야 할 수 있습니다.

- 디바이스에서 FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다., 351 페이지 - FMC IP 주소 또는 호스트네임을 변경하는 경우, 디바이스의 새 IP 주소 또는 호스트네임과 일치하는 것이 좋습니다.
- 새 FMC 식별, 352 페이지- 이전 FMC에서 디바이스가 있다면 이를 삭제한 후 새 FMC에 대해 디바이스를 구성한 다음 FMC에 추가할 수 있습니다.
- Firepower Device Manager에서 FMC로 전환, 353 페이지- 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FDM에서 FMC로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.
- FMC에서 Firepower Device Manager로 전환, 354 페이지- 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FMC에서 FDM으로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.

디바이스에서 FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다.

FMC IP 주소 또는 호스트네임을 변경하는 경우, 설정이 일치하도록 디바이스 CLI의 값도 변경해야 합니다. 대부분 디바이스에서 FMC IP 주소 또는 호스트네임을 변경하지 않고 관리 연결이 다시 설정되지만, 적어도 FMC에 디바이스를 추가하고 NAT ID만 지정한 경우 연결을 다시 설정하려면 이 작업을 수행해야 합니다. 다른 경우에도 네트워크의 복원력을 높이려면 FMC IP 주소 또는 호스트네임을 최신 상태로 유지하는 것이 좋습니다

시작하기 전에

모델 지원—FTD

프로시저

단계 **1** FMC CLI에서 FTD 명령에 지정할 수 있도록 FMC의 고유한 UUID를 확인합니다.FMC CLI에 대한 자세한 내용은 Firepower Management Center 명령줄 참조, 3175 페이지의 내용을 참조하십시오.

show version

FMC UUID는 FMC를 명확하게 식별합니다. 예를 들어 FMC 고가용성의 경우 FTD에서 활성 FMC를 지정해야 합니다.

예제:

```
> show version
-------------------[ firepower ]--------------------
```

```
Model                     : Cisco Firepower Management Center for VMWare (66) Version 6.7.0
 (Build 1222)
UUID                       : f2a06484-9f7f-11ea-b9f4-541a108ebbb5
Rules update version       : 2020-05-26-001-vrt
VDB version                : 334
------------------------------------------------
```

단계 **2** FTD CLI에서 FMC IP 주소 또는 호스트네임을 수정합니다.

configure manager edit *fmc_uuid* {*ip_address* | *hostname*}

FMC가 원래 **DONTRESOLVE** 및 NAT ID로 식별된 경우 이 명령을 사용하여 값을 호스트네임 또는 IP 주소로 변경할 수 있습니다. IP 주소 또는 호스트네임은 **DONTRESOLVE**으로 변경할 수 없습니다.

관리 연결이 중단된 다음 다시 설정됩니다. **sftunnel-status** 명령을 사용하여 연결 상태를 모니터링할 수 있습니다.

예제:

```
> configure manager edit f2a06484-9f7f-11ea-b9f4-541a108ebbb5 10.10.5.1
```

새 FMC 식별

이 절차에서는 매니지드 디바이스의 새 FMC를 식별하는 방법을 보여줍니다. 새 FMC에서 이전 FMC의 IP 주소를 사용하는 경우에도 이러한 단계를 수행해야 합니다.

프로시저

단계 **1** 기존 FMC에서 매니지드 디바이스를 삭제합니다. FMC에서 디바이스 삭제, 315 페이지를 참조하십시오.

FMC와의 활성 연결이 있는 경우 FMC IP 주소를 변경할 수 없습니다.

단계 **2** 예를 들어 SSH를 사용하여 디바이스 CLI에 연결합니다.

단계 **3** 새 FMC를 구성합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address*} - FMC 호스트 이름, IPv4 주소 또는 IPv6 주소를 설정합니다
- **DONTRESOLVE** - FMC에서 주소를 직접 지정할 수 없는 경우, 호스트 이름 또는 IP 주소 대신 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 *nat_id*가 필요합니다. 이 디바이스를 FMC에 추가할 때는 디바이스 IP 주소와 *nat_id*를 모두 지정해야 합니다. 연결의 한쪽에서 IP 주소를 지정해야 하며, 양쪽에서 동일한 고유 NAT ID를 지정해야 합니다.
- *regkey*—등록 시 FMC와 디바이스 간에 공유할 등록 키를 입력합니다. 이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.

- *nat_id* - FMC와 디바이스에서 IP 주소를 지정하지 않은 경우, 둘 사이의 등록 프로세스 동안에만 사용되는 1~37자의 영문숫자 문자열로 구성됩니다. 이 NAT ID는 등록 시에만 사용되는 일회용 비밀번호입니다. NAT ID가 고유하고 등록 대기 중인 다른 디바이스에서 사용되지 않는지 확인하십시오. FTD를 추가할 때 FMC에 동일한 NAT ID를 지정합니다.

예제:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

단계 **4** FMC에 디바이스를 추가합니다. FMC에 디바이스 추가, 311 페이지의 내용을 참조하십시오.

Firepower Device Manager에서 FMC로 전환

이 절차에서는 관리자를 FDM(Firepower Device Manager)에서 로컬 디바이스 관리자인 FMC로 변경하는 방법을 설명합니다. 소프트웨어를 다시 설치하지 않고도 FDM과 FMC 간에 전환할 수 있습니다. 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FDM에서 FMC로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.

⚠

주의 관리자를 변경하면 FTD 컨피그레이션이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 컨피그레이션은 유지됩니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 **1** FDM에서 고가용성을 위해 고가용성 구성을 해제합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다.

단계 **2** FDM에서 스마트 라이선스 서버에서 디바이스를 등록 해제합니다.

단계 **3** 예를 들어 SSH를 사용하여 디바이스 CLI에 연결합니다.

단계 **4** 현재 관리 설정을 제거합니다.

configure manager delete

주의 로컬 관리자를 삭제하면 FTD 컨피그레이션이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 컨피그레이션은 유지됩니다.

예제:

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

단계 **5** 새 FMC를 구성합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address*}—FMC 호스트 이름, IPv4 주소 또는 IPv6 주소를 설정합니다
- **DONTRESOLVE**—FMC에서 주소를 직접 지정할 수없는 경우 호스트 이름 또는 IP 주소 대신 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 *nat_id*가 필요합니다. 이 디바이스를 FMC에 추가할 때는 디바이스 IP 주소와 *nat_id*를 모두 지정해야 합니다. 연결의 한쪽에서 IP 주소를 지정해야 하며, 양쪽에서 동일한 고유 NAT ID를 지정해야 합니다.
- *regkey*—등록 시 FMC와 디바이스 간에 공유할 등록 키를 입력합니다. 이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.
- *nat_id* - FMC와 디바이스에서 IP 주소를 지정하지 않은 경우, 둘 사이의 등록 프로세스 동안에만 사용되는 1~37자의 영문숫자 문자열로 구성됩니다. 이 NAT ID는 등록 시에만 사용되는 일회용 비밀번호입니다. NAT ID가 고유하고 등록 대기 중인 다른 디바이스에서 사용되지 않는지 확인하십시오. FTD를 추가할 때 FMC에 동일한 NAT ID를 지정합니다.

예제:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

단계 **6** FMC에 디바이스를 추가합니다. FMC에 디바이스 추가, 311 페이지 섹션을 참조하십시오.

FMC에서 Firepower Device Manager로 전환

이 절차에서는 관리자를 FMC에서 로컬 디바이스 관리자인 FDM(Firepower Device Manager)으로 변경하는 방법을 설명합니다. 소프트웨어를 다시 설치하지 않고도 FDM과 FMC 간에 전환할 수 있습니다. 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FMC에서 FDM으로 변경할 경우, FTD 컨피그레이션이 지워지며 처음부터 다시 시작해야 합니다.

주의 관리자를 변경하면 FTD 구성이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 구성은 유지됩니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 **1** FMC에서 고가용성을 위해 고가용성 구성을 해제합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다. 고가용성 쌍의 유닛 분리, 914 페이지 섹션을 참조하십시오.

단계 **2** FMC에서 매니지드 디바이스를 삭제합니다. FMC에서 디바이스 삭제, 315 페이지를 참조하십시오.

FMC와의 활성 연결이 있는 경우 관리자를 변경할 수 없습니다.

단계 **3** 예를 들어 SSH를 사용하여 디바이스 CLI에 연결합니다.

단계 **4** 현재 관리 설정을 제거합니다.

configure manager delete

주의 로컬 관리자를 삭제하면 FTD 구성이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 컨피그레이션은 유지됩니다.

예제:

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

단계 **5** 새 FMC를 구성합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address*}—FMC 호스트 이름, IPv4 주소 또는 IPv6 주소를 설정합니다
- **DONTRESOLVE**—FMC에서 주소를 직접 지정할 수없는 경우 호스트 이름 또는 IP 주소 대신 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 *nat_id*가 필요합니다. 이 디바이스를 FMC에 추가할 때는 디바이스 IP 주소와 *nat_id*를 모두 지정해야 합니다. 연결의 한쪽에서 IP 주소를 지정해야 하며, 양쪽에서 동일한 고유 NAT ID를 지정해야 합니다.

- *regkey*—등록 시 FMC와 디바이스 간에 공유할 등록 키를 입력합니다. 이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.
- *nat_id* - FMC와 디바이스에서 IP 주소를 지정하지 않은 경우, 둘 사이의 등록 프로세스 동안에만 사용되는 1~37자의 영문숫자 문자열로 구성됩니다. 이 NAT ID는 등록 시에만 사용되는 일회용 비밀번호입니다. NAT ID가 고유하고 등록 대기 중인 다른 디바이스에서 사용되지 않는지 확인하십시오. FTD를 추가할 때 FMC에 동일한 NAT ID를 지정합니다.

예제:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

단계 **6** FMC에 디바이스를 추가합니다. FMC에 디바이스 추가, 311 페이지 섹션을 참조하십시오.

디바이스 정보 보기

다중 도메인 구축에서 상위 도메인은 하위 도메인의 모든 디바이스에 대한 정보를 볼 수 있습니다. 디바이스를 편집하려면 리프 도메인에 있어야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 확인할 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축 시 상위 도메인에 있는 경우, 보기 ( )를 클릭하여 하위 도메인의 읽기 전용 모드에서 디바이스를 볼 수 있습니다.

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** 다음 정보를 볼 수 있습니다.

- 일반 - 디바이스의 일반 설정을 표시합니다. 일반 정보, 357 페이지의 내용을 참조하십시오.
- 라이선스 - 디바이스의 라이선스 정보를 표시합니다. 라이선스 정보, 358 페이지의 내용을 참조하십시오.
- 시스템 - 디바이스에 대한 시스템 정보를 표시합니다. 시스템 정보, 358 페이지의 내용을 참조하십시오.
- 상태 - 디바이스의 현재 상태에 대한 정보를 표시합니다. 상태 정보, 358 페이지의 내용을 참조하십시오.
- 관리 - Firepower Management Center과 디바이스 간 통신 채널에 대한 정보를 표시합니다. 관리 정보, 359 페이지를 참조합니다.

- 고급 - 고급 기능 설정에 대한 정보를 표시합니다. Advanced Settings(고급 설정), 359 페이지을 참조합니다.

디바이스 관리 페이지 정보

Device Management(디바이스 관리) 페이지에서는 Firepower 디바이스를 관리하는 데 사용할 수 있는 다양한 정보와 옵션을 제공합니다.

이 페이지를 사용하여 디바이스를 추가, 편집, 제거 및 그룹화하고 상태를 비롯한 기본 디바이스 속성을 확인할 수 있습니다. 다양한 특성별로 디바이스를 추가로 필터링할 수 있습니다.

이 페이지에서는 클릭 한 번으로 다음에 액세스할 수 있는 기능을 제공합니다.

- 디바이스에 구축한 액세스 제어 정책
- 문제 해결 파일을 생성할 수 있는 각 디바이스의 상태 모니터링 페이지
- Firepower 4100/9300 시리즈 디바이스의 경우, Firepower Chassis Manager 웹 인터페이스로 연결되는 링크

일반 정보

디바이스 탭의 일반 섹션은 아래 표의 설정을 표시합니다.

표 ***12:*** 일반 섹션 표 필드

필드	설명
이름	Firepower Management Center에 표시되는 디바이스의 이름입니다.
패킷 전송	관리되는 디바이스가 Firepower Management Center에 이벤트 및 패킷 데이터를 전송할지 여부를 표시합니다.
모드	디바이스에 대한 관리 인터페이스 모드로 라우팅 또는 투명을 선택할 수 있습니다. 참고 모드 필드는 Firepower Threat Defense 디바이스에만 표시됩니다.
컴플라이언스 모드	디바이스에 대한 보안 인증서 컴플라이언스를 표시합니다. 유효한 값은 CC, UCAPL, None(없음)입니다.

라이선스 정보

디바이스 페이지의 라이선스 섹션은 장치에 대해 활성화된 라이선스를 표시합니다.

시스템 정보

디바이스 페이지의 시스템 섹션은 다음 표에 나타난 시스템 정보의 읽기 전용 표를 표시합니다.

표 ***13:*** 시스템 섹션 표 필드

필드	설명
모델	관리되는 디바이스의 모델 이름 및 번호입니다.
일련 번호	관리되는 디바이스의 섀시의 일련 번호입니다.
시간	디바이스의 현재 시스템 시간입니다. 항상 UTC입니다. 아래의 시간 기반 규칙에 대한 표준 시간대 설정을 참조하십시오.
버전	매니지드 디바이스에 현재 설치된 소프트웨어 버전입니다.
시간 기반 규칙에 대한 표준 시간대 설정	디바이스 플랫폼 설정에 지정된 표준 시간대의 디바이스의 현재 시스템 시간입니다.
정책	관리되는 디바이스에 현재 구축된 플랫폼 설정 정책에 연결합니다.
인벤토리	연결된 디바이스에 대한 인벤토리 세부 정보를 연결합니다. 이 필드는 Firepower 2100 또는 Firepower 4100/9300 컨테이너 인스턴스 같은 일부 플랫폼에만 표시됩니다. 컨테이너 인스턴스에 대한 정보를 업데이트하려면 업데이트를 클릭합니다. 리소스 프로파일을 변경하면 고가용성 쌍의 불일치 문제를 방지하기 위해 인벤토리의 업데이트를 강제로 수행할 수 있습니다. 그렇지 않으면 정책 변경 사항을 구축할 때 이 정보가 업데이트됩니다.

디바이스를 종료하거나 다시 시작할 수 있습니다.

상태 정보

디바이스 페이지의 상태 섹션은 아래 표에서 설명한 정보를 표시합니다.

표 *14:* 상태 섹션 표 필드

필드	설명
상태	디바이스의 현재 상태를 나타내는 아이콘 아이콘을 클릭하면 어플라이언스에 대한 상태 모니터가 표시됩니다.
정책	디바이스에 현재 구축된 상태 정책에 대한 읽기 전용 링크입니다.
블랙리스트	상태 블랙리스트 모듈을 활성화하거나 비활성화할 수 있는 상태 블랙리스트 페이지의 링크입니다.

관리 정보

아래 테이블은 **Device(**디바이스**)** 페이지의 **Management(**관리**)** 섹션에 표시되는 필드를 표시합니다.

표 *15:* 관리 섹션 표 필드

필드	설명
호스트	디바이스의 IP 주소 또는 호스트네임입니다. 디바이스의 호스트네임 또는 IP 주소를 변경하려면 관리 설정 편집, 317 페이지의 내용을 참조하십시오.
상태	Firepower Management Center과 매니지드 디바이스 간 채널 통신 상태를 나타내는 아이콘입니다. 커서를 상태 아이콘에 올려 놓으면 Firepower Management Center이 디바이스와 연결한 마지막 시간을 볼 수 있습니다.
FMC 액세스 인터페이스	FMC 관리에 사용되는 인터페이스 유형(데이터 인터페이스 또는 관리 인터페이스)을 표시합니다. 인터페이스를 변경하려면 값을 클릭합니다. 관리 설정 편집, 317 페이지의 내용을 참조하십시오.
FMC 액세스 세부 사항	**Configuration(**설정**)** 링크를 클릭하여 FMC의 데이터 인터페이스 설정 및 연결 상태를 디바이스의 값과 비교합니다. 자세한 내용은 데이터 인터페이스 관리를 위한 FMC 액세스 세부정보 보기, 323 페이지를 참고하십시오.

Advanced Settings(고급 설정)

디바이스 페이지의 고급 설정 섹션은 고급 아래 표에 설명된 대로 고급 구성 설정을 표시합니다. 이러한 설정은 편집할 수 있습니다.

표 *16:* 고급 섹션 표 필드

필드	설명	지원되는 장치
애플리케이션 우회	디바이스에서 Automatic Application Bypass의 상태	7000 및 8000 Series NGIPSv ASA FirePOWER Firepower Threat Defense
우회 임계값	밀리초로 나타낸 Automatic Application Bypass(자동 애플리케이션 우회) 임계값입니다.	
로컬 라우터 트래픽 검사	디바이스가 라우티드 인터페이스에서 수신된 ICMP, DHCP, OSFP 트래픽과 같이 스스로를 향하는 트래픽을 검사할지 여부입니다.	7000 및 8000 Series
빠른 경로(Fast-Path) 규칙	디바이스에서 생성된 8000 Series 빠른 경로 규칙의 수입니다.	8000 Series
개체 그룹 검색	디바이스에서 개체 그룹 검색의 상태입니다. 작동하는 동안 FTD 디바이스는 액세스 규칙에 사용되는 모든 네트워크 또는 인터페이스 개체의 컨텐츠에 따라 액세스 컨트롤 규칙을 여러 액세스 컨트롤 목록 항목으로 확장합니다. 개체 그룹 검색을 활성화하여 액세스 컨트롤 규칙을 검색하는 데 필요한 메모리를 줄일 수 있습니다. 개체 그룹 검색을 사용하면 시스템이 네트워크 또는 인터페이스 개체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 개체 그룹 검색은 액세스 규칙이 정의된 방식 또는 Firepower 디바이스 관리자에 표시되는 방식에 영향을 주지 않습니다. 이는 액세스 컨트롤 규칙과의 연결을 일치시키는 동안 디바이스가 이를 해석 및 처리하는 방법에만 영향을 미칩니다.	Firepower Threat Defense
인터페이스 개체 최적화	디바이스에서 인터페이스 개체 최적화의 상태입니다. 구축 중 액세스 제어 및 사전 필터 정책에서 사용하는 인터페이스 그룹 및 보안 영역은 각 소스/대상 인터페이스 쌍에 대해 별도의 규칙을 생성합니다. 인터페이스 개체 최적화를 활성화하면 시스템은 대신 액세스 제어/사전 필터 규칙에 따라 단일 규칙을 구축하여 디바이스 설정을 간소화하고 구축 성능을 개선할 수 있습니다. 이 옵션을 선택하는 경우, **Object Group Search(**개체 그룹 검색**)** 옵션도 선택하여 디바이스의 메모리 사용량을 줄일 수 있습니다.	Firepower Threat Defense

III 부

시스템 모니터링 및 문제 해결

- 대시보드, 363 페이지
- 상태 모니터링, 387 페이지
- 시스템 모니터링, 431 페이지
- 시스템 감사, 449 페이지
- 시스템 문제 해결, 461 페이지

14 장

대시보드

다음 항목에서는 Firepower System에서 대시보드를 사용하는 방법을 설명합니다.

- 대시보드 정보, 363 페이지
- Firepower System 대시보드 위젯, 364 페이지
- 대시보드 관리, 378 페이지

대시보드 정보

Firepower System 대시보드는 시스템에 의해 수집 및 생성된 이벤트에 대한 데이터를 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기를 제공합니다. 또한 구축에서 어플라이언스의 전체적인 상태에 대한 정보를 확인하는 데에도 대시보드를 사용할 수 있습니다. 참고로 대시보드가 제공하는 정보는 시스템 라이선싱, 구성 및 구축 방법에 따라 달라집니다.

팁 대시보드는 철저한 데이터를 제공하는 복잡한 맞춤형 가능 모니터링 기능입니다. 모니터링되는 네트워크의 광범위하고 간결하고 다채로운 그림을 보려면 컨텍스트 탐색기를 사용하십시오.

대시보드는 Firepower Management Center 및 7000 및 8000 Series 디바이스에서 사용할 수 있습니다.

대시보드는 탭을 사용하여 위젯을 표시합니다. 위젯은 시스템의 여러 측면을 파악할 수 있는 자체 포함형 소형 구성 요소입니다. 예를 들어, 사전 정의된 Appliance Information(어플라이언스 정보) 위젯에서는 어플라이언스 이름, 모델 및 현재 실행 중인 Firepower System 소프트웨어의 버전을 확인할 수 있습니다. 시스템은 위젯을 대시보드 시간 범위로 제한합니다. 이 범위를 변경해 전 시간만큼 짧거나 지난해처럼 긴 기간을 반영할 수 있습니다.

이 시스템에는 사전 정의된 여러 대시보드가 함께 제공됩니다. 이 대시보드는 사용 및 수정할 수 있습니다. 사용자 역할이 대시보드(관리자, 유지 보수 사용자, 보안 분석가, 보안 분석가[읽기 전용] 및 대시보드 권한이 있는 맞춤형 역할)에 액세스 할 수 있는 경우, 기본적으로 홈페이지는 사전 정의된 요약 대시보드입니다. 그러나 비 대시보드를 포함하여 다른 기본 홈페이지를 구성할 수 있습니다. 기본 대시보드를 변경할 수도 있습니다. 사용자 역할이 대시보드에 액세스 할 수 없는 경우, 기본 홈페이지는 역할과 관련이 있습니다. 예를 들어, 검색 관리자는 Network Discovery(네트워크 검색) 페이지를 봅니다.

사전 정의된 대시보드를 맞춤형 대시보드의 기본으로 사용할 수도 있습니다. 이 대시보드는 공유하거나 비공개로 제한할 수 있습니다. 관리자 액세스 권한이 없으면 다른 사용자가 생성한 개인 대시보드를 보거나 수정할 수 없습니다.

참고 일부 드릴다운 페이지 및 이벤트의 테이블 보기에는 사전 정의된 관련 대시보드를 보기 위해 클릭할 수 있는 **Dashboard(**대시보드**)** 툴바 링크가 포함되어 있습니다. 사전 정의 대시보드 또는 탭을 삭제하면 연결된 툴바 링크가 작동하지 않습니다.

다중 도메인 구축에서는 상위 도메인의 대시보드를 볼 수 없습니다. 그러나 상위 대시보드의 복사본인 새 대시보드를 생성할 수 있습니다.

Firepower System 대시보드 위젯

대시보드는 하나 이상의 탭을 가지며, 각 탭은 3열 레이아웃에서 하나 이상의 위젯을 표시합니다. Firepower System에는 많은 사전 정의된 대시보드 위젯이 제공되며, 각 위젯은 Firepower System의 다른 측면에 대한 통찰력을 제공합니다. 위젯은 세 카테고리로 그룹화됩니다.

- *Analysis & Reporting widgets(*분석&보고 위젯*)*은 Firepower System에 의해 수집 및 생성된 이벤트를 표시합니다.
- *Miscellaneous widgets(*기타 위젯*)* 이벤트 데이터와 작업 데이터를 모두 표시하지 않습니다. 현재 이 카테고리의 유일한 위젯은 RSS 피드를 표시합니다.
- *Operations widgets(*운영 위젯*)*은 Firepower System의 상태 및 전체 상태에 대한 정보를 표시합니다.

표시되는 대시보드 위젯은 다음에 따라 달라집니다.

- 사용 중인 어플라이언스 유형
- 사용자 역할
- 현재 도메인(다중 도메인 구축의 경우)

또한, 각 대시보드에는 해당 작업을 결정하는 환경 설정 집합이 있습니다.

위젯을 최소화 및 최대화하고 탭에서 위젯을 추가하거나 제거하며, 탭에서위젯을 다시 정렬할 수도 있습니다.

참고 일정 기간 동안 이벤트 수를 표시하는 위젯의 경우, 전체 이벤트 수는 Analysis(분석) 메뉴 하단 페이지에 있는 테이블에서 상세 데이터를 사용할 수 있는 이벤트 수를 반영하지 않을 수 있습니다. 이는 디스크 공간 사용량을 관리하기 위해 때때로 오래된 이벤트의 세부사항을 삭제하기 때문입니다. 이벤트 세부사항이 삭제되는 경우를 최소화하기 위해 이벤트 로깅을 세밀하게 조정하여 구축에 가장 중요한 이벤트만 로깅하게 할 수 있습니다.

위젯 가용성

표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형, 사용자 역할 및 현재 도메인(다중 도메인 구축의 경우)에 따라 달라집니다.

다중 도메인 구축에서, 예상했던 위젯이 보이지 않으면 전역 도메인으로 전환하십시오. 도메인 전환 Firepower Management Center, 14 페이지의 내용을 참조하십시오.

다음을 참고하십시오.

- *invalid(*유효하지 않은*)* 위젯이란 잘못된 어플라이언스 유형을 사용하고 있기 때문에 볼 수 없는 위젯을 말합니다.
- *unauthorized(*무단*)* 뒤젯은 사용자 어카운트에 필요한 권한이 없기 때문에 볼 수 없는 위젯입니다.

예를 들어 어플라이언스 상태 위젯은 관리자, 유지 보수 사용자, 보안 분석가 또는 보안 분석가 (읽기 전용) 계정 권한이 있는 사용자만 FMC에서 사용할 수 있습니다.

무단 또는 유효하지 않은 위젯을 대시보드에 추가할 수는 없지만, 가져온 대시보드에는 무단 또는 유효하지 않은 위젯이 포함될 수 있습니다. 예를 들어, 가져온 대시보드가 다음에 해당되는 경우 그러한 위젯이 나타날 수 있습니다.

- 상이한 액세스 권한이 있는 사용자가 생성하였습니다.
- 상위 도메인에 속합니다.

사용할 수없는 위젯은 비활성화되며, 표시되지 않는 이유를 나타내는 오류 메시지가 표시됩니다.

위젯이 시간 초과되거나 다른 문제가 발생하는 경우에도 개별 위젯에 오류 메시지가 표시됩니다.

참고 무단 위젯이나 잘못된 위젯 또는 데이터가 표시되지 않는 위젯은 삭제하거나 최소화할 수 있습니다. 공유 대시보드에서 위젯을 수정하면 어플라이언스의 모든 사용자에 대해 수정됩니다.

사용자 역할별 대시보드 위젯 가용성

다음 표에는 각 위젯을 보기 위해 필요한 사용자 어카운트 권한이 나열되어 있습니다. 관리자, 유지 보수 관리자, 보안 분석가 또는 보안 분석가(읽기 전용) 액세스 권한이 있는 사용자 어카운트만 대시보드를 사용할 수 있습니다.

맞춤형 역할이 부여된 사용자는 사용자 역할이 허용하는 만큼 위젯 조합에 액세스할 수 있습니다. 전부일 수도 전혀 없을 수도 있습니다.

표 ***17:*** 사용자 역할 및 대시보드 위젯 가용성

위젯	관리자	유지 보수 사용자	보안 분석가	보안 분석가**(RO)**
어플라이언스 정보	예	예	예	예

위젯	관리자	유지 보수 사용자	보안 분석가	보안 분석가**(RO)**
어플라이언스 상태	예	예	예	아니요
Correlation Events	예	아니요	예	예
현재 인터페이스 상태	예	예	예	예
현재 세션	예	아니요	아니요	아니요
맞춤형 분석	예	아니요	예	예
디스크 사용	예	예	예	예
Interface Traffic	예	예	예	예
침입 이벤트	예	아니요	예	예
네트워크 컴플라이언스	예	아니요	예	예
제품 라이선싱	예	예	아니요	아니요
제품 업데이트	예	예	아니요	아니요
RSS 피드	예	예	예	예
시스템 로드	예	예	예	예
시스템 시간	예	예	예	예
화이트 이벤트 표시	예	아니요	예	예

사전 정의된 대시보드 위젯

Firepower System에는 대시보드에서 사용할 때 현재 시스템 상태를 한 눈에 볼 수 있는 몇 가지 사전 정의된 위젯이 제공됩니다. 볼 수 있는 항목은 다음과 같습니다.

- 시스템에서 수집하고 생성 한 이벤트에 대한 데이터
- 배포의 어플라이언스 상태 및 전반적인 상태에 대한 정보

참고 표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형, 사용자 역할, 다중 도메인 구축에서 현재 도메인에 따라 달라집니다.

어플라이언스 정보 위젯

Appliance Information(애플리케이션 정보) 위젯은 어플라이언스의 스냅샷을 제공합니다. 이는 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다. 위젯에서는 다음을 제공합니다.

- 어플라이언스 이름, IPv4 주소, IPv6 주소 및 모델
- Firepower System 소프트웨어 버전, 운영 체제, Snort, 규칙 업데이트, 규칙 팩, 모듈 팩, VDB(취약성 데이터베이스) 및 가상 Firepower Management Center을 제외한 대시보드를 포함한 어플라이언스에 설치된 지리위치 업데이트
- 관리되는 어플라이언스의 경우, 관리되는 어플라이언스와의 통신 링크 상태 및 이름

단순 보기 또는 고급 보기를 표시하는 위젯 환경 설정을 수정하여 더 많은 정보 또는 더 적은 정보를 표시하도록 위젯을 구성할 수 있습니다. 환경 설정에서는 또한 위젯 업데이트의 빈도를 제어합니다.

어플라이언스 상태 위젯

Appliance Status(어플라이언스 상태) 위젯은 어플라이언스 및 관리 중인 어플라이언스의 상태를 나타냅니다. Firepower Management Center는 매니지드 디바이스에 상태 정책을 자동으로 적용하지 않으므로 상태 정책을 디바이스에 수동으로 적용해야 합니다. 그렇지 않으면 상태가 `Disabled(비활성화)`로 표시됩니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 어플라이언스 상태를 원그래프 또는 테이블로 표시하도록 위젯을 구성할 수 있습니다.

환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

원그래프의 섹션을 클릭하거나 어플라이언스 상태 테이블의 숫자 중 하나를 클릭하여 Health Monitor(상태 모니터) 페이지로 이동한 다음 어플라이언스 및 관리 중인 어플라이언스의 컴파일된 상태를 볼 수 있습니다.

상관관계 이벤트 위젯

Correlation Events(상관관계 이벤트) 위젯은 대시보드 시간 범위 중 초당 상관관계 이벤트의 평균 개수를 우선순위 기준으로 보여줍니다. 이 위젯은 Detailed Dashboard(상세 대시보드)의 Correlation(상관관계) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 서로 다른 우선순위의 상관관계 이벤트를 표시하고, 선형(증분) 또는 로그(10배) 비율을 선택하도록 위젯을 구성할 수 있습니다.

하나 이상의 **Priorities(**우선순위**)** 확인란을 선택하고 특정 우선순위의 이벤트(우선순위가 없는 이벤트 포함)에 대해 별도의 그래프를 표시합니다. **Show All(**모두 표시**)**를 선택하고 우선순위와 상관없이 모든 상관관계 이벤트에 대해 추가 그래프를 표시합니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

특정 우선순위의 상관관계 이벤트를 보려면 그래프 하나를 클릭하고, 모든 상관관계 이벤트를 보려면 **All(**모두**)** 그래프를 클릭합니다. 어떤 경우든 이벤트는 대시보드 시간 범위에 의해 제한됩니다. 대

시보드를 통해 상관관계 이벤트에 액세스하면 어플라이언스에 대한 이벤트(또는 전역) 시간 창이 변경됩니다.

현재 인터페이스 상태 위젯

Current Interface Status(현재 인터페이스 상태) 위젯은 활성화되어 있거나 사용하지 않는 어플라이언스의 모든 인터페이스의 상태를 보여줍니다. Firepower Management Center에서 관리(`eth0`, `eth1` 등) 인터페이스를 표시할 수 잇습니다. 매니지드 디바이스에서 센싱(`s1p1` 등) 인터페이스만 표시하거나 관리 및 센싱 인터페이스를 모두 표시하도록 선택할 수 있습니다. 인터페이스는 관리, 인라인, 수동, 스위치드, 라우티드, 스태킹됨, 사용되지 않음 등의 유형별로 그룹화됩니다.

각 인터페이스의 경우, 위젯은 다음을 제공합니다.

- 인터페이스의 이름
- 인터페이스의 연결 상태
- 인터페이스의 연결 모드(예: 전이중 100Mb 또는 반이중 10Mb)
- 인터페이스 유형(즉, 구리 또는 파이버)
- 인터페이스로 수신(Rx) 및 전송(Tx)된 데이터 양

링크 상태를 나타내는 공 색상은 다음과 같이 현재 상태를 표시합니다.

- 녹색: 링크가 최대 속도로 작동 중
- 노란색: 링크가 최대 속도로 작동 중
- 빨간색: 링크가 작동하지 않음
- 회색: 링크가 관리 목적으로 비활성화됨
- 파란색: 연결 상태 정보를 사용할 수 없음(예: ASA)

위젯 환경 설정은 위젯 업데이트의 빈도를 제어합니다.

현재 세션 위젯

Current Sessions(현재 세션) 위젯은 어플라이언스에 현재 로그인한 사용자, 세션이 시작된 시스템과 관련된 IP 주소, 각 사용자가 어플라이언스에서 페이지에 액세스한 마지막 시간(어플라이언스의 현지 시간 기준)을 보여줍니다. 자신을 나타내는 사용자, 즉 현재 위젯을 보고 있는 사용자는 사용자 아이콘과 함께 굵은 글꼴로 표시됩니다. 세션은 로그 오프 1 시간 이내에이 위젯의 데이터에서 정리 됩니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

Current Sessions(현재 세션) 위젯에서 다음을 수행할 수 있습니다.

- 사용자 관리 페이지에서 사용자 어카운트를 관리하려면 사용자 이름을 클릭합니다.
- IP 주소 옆에 있는 호스트 아이콘 또는 손상된 호스트 아이콘을 클릭하여 연결된 컴퓨터의 호스트 프로필을 확인합니다.

- IP 주소나 액세스 시간을 클릭하여 해당 IP 주소에 의해, 그리고 웹 IP 주소와 연결된 사용자가 웹 인터페이스에 로그온한 시간에 의해 제한되는 감사 로그를 볼 수 있습니다

위젯 환경 설정은 위젯 업데이트의 빈도를 제어합니다.

맞춤형 분석 위젯

사용자 지정 기능이 뛰어난 위젯인 Custom Analysis(맞춤 분석) 위젯을 사용하면 Firepower System에 의해 수집 및 생성된 이벤트에 대한 자세한 정보를 표시할 수 있습니다.

위젯에는 구축에 대한 정보에 빠르게 액세스 할 수 있는 여러 사전 설정이 제공됩니다. 사전 정의된 대시보드가 이러한 사전 설정을 광범위하게 사용합니다. 이러한 사전 설정을 사용할 수도 있고 맞춤형 구성을 생성할 수도 있습니다. 맞춤형 구성에서는 최소한 사용자가 관심있는 데이터(테이블 및 필드)와 해당 데이터의 집계 방법을 지정합니다. 다른 디스플레이 관련 환경 설정도 지정할 수도 있습니다. 예를 들어, 이벤트를 상대적 발생(막대 그래프) 또는 시간 경과에 따라(선 그래프) 표시할 수 있습니다.

위젯은 로컬 시간을 기준으로 업데이트한 마지막 시간을 표시합니다. 위젯은 대시보드 시간 범위에 따른 빈도로 업데이트됩니다. 예를 들어 대시보드 시간 범위를 시로 설정하면 위젯은 5분마다 업데이트됩니다. 반면, 대시보드 시간 범위를 연도로 설정하면 위젯은 일주일에 한 번 업데이트됩니다. 대시보드의 다음번 업데이트 시기를 확인하려면 위젯의 왼쪽 아래에 있는 **Last updated(**마지막 업데이트**)** 알림으로 포인터를 이동합니다.

참고 빨간색으로 표시된 Custom Analysis(맞춤 분석) 위젯은 위젯 사용으로 시스템 성능이 저하되고 있음을 나타냅니다. 위젯이 계속해서 빨간색으로 표시되면 해당 위젯을 제거해야 합니다. 시스템 구성(**System(**시스템**)** > **Configuration(**구성**)** > **Dashboard(**대시보드**)**)의 Dashboard(대시보드) 설정에서 모든 Custom Analysis(맞춤 분석) 위젯을 비활성화할 수도 있습니다.

이벤트 상대적 발생**(**막대 그래프**)** 표시

Custom Analysis(맞춤 분석) 위젯의 막대 그래프의 경우, 위젯 배경에 있는 색상이 지정된 막대는 각 이벤트의 상대적 횟수를 표시합니다. 막대를 오른쪽에서 왼쪽으로 읽습니다.

방향 아이콘 은 표시의 정렬 순서를 나타내고 제어합니다. 아래로 향하는 아이콘은 내림차순, 위로 향하는 아이콘은 오름차순을 나타냅니다. 정렬 순서를 바꾸려면 아이콘을 클릭합니다.

각 이벤트 옆에는 최신 결과에서 변경된 내용을 나타내는 세 가지 아이콘 중 하나가 표시됩니다.

- 새 이벤트 아이콘 추가( )은 이벤트가 결과에 새로 추가되었음을 나타냅니다.
- 위쪽 화살표 아이콘은 위젯이 마지막으로 업데이트된 이후 이벤트 순위가 위로 이동했음을 나타냅니다. 이벤트가 몇 단계 올라갔는지 알려주는 숫자가 아이콘 옆에 나타납니다.
- 아래쪽 화살표 아이콘은 위젯이 마지막으로 업데이트된 이후 이벤트 순위가 아래로 이동했음을 나타냅니다. 이벤트가 몇 단계 내려갔는지 알려주는 숫자가 아이콘 옆에 나타납니다.

시간 경과에 따른 이벤트 표시**(**선형 그래프**)**

시간에 따라 발생한 이벤트 또는 기타 수집된 데이터에 대한 정보(예: 구축에서 시간에 따라 생성된 침입 이벤트의 총수)를 보려면 선 그래프를 표시하도록 Custom Analysis(맞춤 분석) 위젯을 구성할 수 있습니다.

맞춤 분석 위젯 제한 사항

Custom Analysis(맞춤 분석) 위젯에는 표시되도록 구성된 데이터를 사용자가 볼 권한이 없다고 나타날 수도 있습니다. 예를 들어, 유지 보수 사용자는 검색 이벤트를 볼 권한이 없습니다. 또 다른 예로, 이 위젯은 라이선스가 없는 기능과 관련된 정보를 표시하지 않습니다. 그러나 사용자(대시보드를 공유하는 모든 사용자)는 자신이 볼 수 있는 데이터를 표시하도록 위젯 환경 설정을 수정할 수 있으며 위젯을 삭제할 수도 있습니다. 이런 일이 발생하지 않도록 하려면 대시보드를 비공개로 저장하십시오.

사용자 데이터를 보는 경우, 시스템에는 권한 있는 사용자만 표시됩니다.

URL 카테고리 정보를 보는 경우, 시스템에는 분류되지 않은 URL이 표시되지 않습니다.

Count(개수**)**로 집계된 침입 이벤트를 보는 경우, 개수에는 침입 이벤트에 대한 검토된 이벤트가 포함됩니다. Analysis(분석) 메뉴 하단 페이지에 있는 테이블 개수를 보는 경우, 개수에는 검토된 이벤트가 포함되지 않습니다.

참고 다중 도메인 구축에서 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 따라서 리프 도메인은 네트워크 내에서는 고유하지만 다른 리프 도메인과 동일한 IP 주소를 포함할 수 있습니다. 상위 도메인에서 맞춤 분석(Custom Analysis) 위젯을 보는 경우, 반복되는 IP 주소의 여러 인스턴스가 표시될 수 있습니다. 처음에는 이것이 중복된 항목으로 보일 수 있습니다. 하지만 각 IP 주소의 호스트 프로파일 정보로 드릴다운하는 경우, 시스템은 이들이 서로 다른 리프 도메인에 속한다고 표시합니다.

예**:** 맞춤 구성

Intrusion Events(침입 이벤트**)** 테이블의 데이터를 표시하도록 위젯을 구성하여 최신 침입 이벤트 목록을 표시하도록 Custom Analysis(맞춤 분석) 위젯을 구성할 수 있습니다. **Classification(**분류**)**필드를 선택하고 **Count(**개수**)** 단위로 이 데이터를 결합하면 각 이벤트 유형이 생성된 방법을 파악할 수 있습니다.

반면 **Unique Events(**고유 이벤트**)** 단위로 결합하면 각 유형의 고유한 침입 이벤트가 발생한 횟수(예: 네트워크 트로이 목마, 회사 정책의 잠재적 위반, 서비스 거부 공격 시도 등의 탐지 횟수)를 파악할 수 있습니다.

저장된 검색(어플라이언스와 함께 제공된 사전 정의된 검색 중 하나 또는 자신이 생성한 사용자 지정 검색)을 사용하여 위젯을 더 제한할 수 있습니다. 예를 들어, **Dropped Events(**삭제된 이벤트**)** 검색으로 첫 번째 예제(**Classification(**분류**)** 필드를 사용하고 **Count(**개수**)**로 결합한 침입 이벤트)를 제한하면 각 유형의 침입 이벤트가 얼마나 삭제되었는지를 알 수 있습니다.

관련 항목

대시보드 시간 설정 수정, 383 페이지

맞춤형 분석 위젯 환경설정

다음 표에서는 Custom Analysis(맞춤 분석) 위젯에서 설정할 수 있는 환경 설정에 대해 설명합니다.

위젯을 구성하는 방법에 따라 다양한 환경 설정이 표시됩니다. 예를 들어, 이벤트의 상대적 발생(막대 그래프)과 시간 경과그래프(선형 그래프)를 표시하도록 위젯을 구성하면 여러 환경 설정 집합이 나타납니다. 필터와 같은 일부 환경 설정은 데이터를 표시하는 특정 테이블을 선택하는 경우에만 표시됩니다.

표 ***18:*** 맞춤 분석 위젯 환경설정

기본 설정	세부 사항
직함	위젯의 제목을 지정하지 않으면 시스템은 구성된 이벤트 유형을 제목으로 사용합니다.
프리셋	맞춤 분석(Custom Analysis) 사전 설정을 통해 구축에 대한 정보에 빠르게 액세스할 수 있습니다. 사전 정의된 대시보드가 이러한 사전 설정을 광범위하게 사용합니다. 이러한 사전 설정을 사용할 수도 있고 맞춤형 구성을 생성할 수도 있습니다.
테이블(필수)	위젯이 표시하는 데이터가 포함된 이벤트 또는 자산 테이블
필드(필수)	표시하려는 이벤트 유형의 특정 필드입니다. 시간에 따른 데이터를 표시하려면(선형 그래프) **Time(**시간**)**을 선택합니다. 이벤트의 상대적 발생(막대 그래프)을 표시하려면 다른 옵션을 선택하십시오.
집계(필수)	집계 방식은 위젯이 표시하는 데이터를 그룹화하는 방법을 구성합니다. 대부분의 이벤트 유형에 대해 기본 옵션은 **Count(**개수**)**입니다.
필터	애플리케이션 필터를 사용하여 Application Statistics(애플리케이션 통계) 및 Intrusion Event Statistics(침입 이벤트 통계) 데이터를 Application(애플리케이션) 테이블별로 제한할 수 있습니다.

기본 설정	세부 사항
검색	저장된 검색을 사용하여 위젯이 표시하는 데이터를 제한할 수 있습니다. 일부 프리셋에서는 사전 정의된 검색을 사용하지만, 검색을 지정해야 할 필요는 없습니다. 비공개로 저장한 검색에는 저장한 당사자만 액세스할 수 있습니다. 공유 대시보드에서 위젯을 구성하고 비공개 검색을 사용하도록 해당 이벤트를 제한하면, 다른 사용자가 로그인할 때 검색을 사용할 수 없도록 위젯이 재설정됩니다. 이것이 위젯 보기에도 영향을 줍니다. 이런 일이 발생하지 않도록 하려면 대시보드를 비공개로 저장하십시오. 연결 요약을 표시하는 필드만이 연결 이벤트를 기반으로 Custom Analysis(맞춤 분석) 대시보드 위젯을 제한할 수 있습니다. 유효하지 않은 저장된 검색은 흐리게 표시됩니다. 저장된 검색을 사용하여 Custom Analysis(맞춤 분석) 위젯을 제한한 다음 검색을 수정하면, 다음 업데이트 시간까지 위젯에 변경 사항이 반영되지 않습니다.
표시	가장 많이(**Top(**상단**)**) 또는 가장 적게(**Bottom(**하단**)**) 발생하는 이벤트를 표시할지 여부를 선택합니다.
결과	표시할 결과 행 수를 선택합니다.
변경 이벤트 표시	가장 최근 결과의 변경 사항을 나타내는 아이콘을 표시할지 여부를 선택합니다.
시간대	결과 표시에 사용할 시간대를 선택합니다.
색상	위젯의 막대 그래프에서 막대의 색상을 변경할 수 있습니다.

관련 항목

위젯 환경설정 구성, 380 페이지

맞춤형 분석 위젯에서 관련 이벤트 보기

Custom Analysis(맞춤 분석) 위젯에서 위젯에 표시된 이벤트에 대한 자세한 정보를 제공하는 이벤트 보기(워크플로)를 호출할 수 있습니다. 이벤트는 해당 이벤트 유형에 대한 기본 워크플로에 표시되며 대시보드 시간 범위로 제한됩니다. 또한 구성한 시간대 개수와 이벤트 유형에 따라 Firepower Management Center에서 해당 기간을 변경합니다.

예를 들면 다음과 같습니다.

- 여러 시간대를 구성한 다음 Custom Analysis(맞춤 분석) 위젯에서 상태 이벤트에 액세스하면, 이벤트는 기본 상태 이벤트 워크플로에 나타나고 상태 모니터링 시간대는 대시보드 시간 범위로 변경됩니다.

- 단일 시간대를 구성한 다음 Custom Analysis(맞춤 분석) 위젯에서 임의의 이벤트 유형에 액세스하면 그 이벤트는 해당 이벤트 유형의 기본 워크플로에 나타나고 전역 시간대는 대시보드 시간 범위로 변경됩니다.

프로시저

다음 옵션을 이용할 수 있습니다.

- Custom Analysis(맞춤 분석) 위젯에서 위젯 오른쪽 아래에 있는 보기 ( )을 클릭하면 위젯 환경 설정에 의해 제한되는 모든 관련 이벤트를 볼 수 있습니다.
- 이벤트의 상대적 발생을 보여주는 Custom Analysis(맞춤 분석) 위젯(막대 그래프)에서, 이벤트를 클릭하면 위젯 환경 설정 및 해당 이벤트로 제한된 관련 이벤트를 볼 수 있습니다.

디스크 사용량 위젯

Disk Usage(디스크 사용량) 위젯은 디스크 사용량 카테고리에 따라 하드 드라이브에서 사용된 공간의 백분율을 표시합니다. 이는 또한 어플라이언스 하드 드라이브의 각 파티션에 대한 용량 및 사용되는 공간의 백분율을 나타냅니다. 디바이스에 악성코드 스토리지 팩이 설치되어 있거나 Firepower Management Center가 악성코드 스토리지 팩이 포함된 디바이스를 관리하는 경우, Disk Usage(디스크 사용량) 위젯은 악성코드 스토리지 팩에 대해서도 동일한 정보를 표시합니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

By Category(By 카테고리) 누적 막대는 총 사용 가능한 디스크 공간 중 사용되고 있는 비율로 각 디스크 사용량 카테고리를 나타냅니다. 다음 표에서는 사용 가능한 카테고리를 설명합니다.

표 ***19:*** 디스크 사용량 카테고리

디스크 사용량 카테고리	설명
이벤트	시스템에서 로깅된 모든 이벤트
파일	시스템에서 저장된 모든 파일
백업	모든 백업 파일
업데이트	규칙 업데이트 및 시스템 업데이트와 같은 업데이트와 관련된 모든 파일
기타	시스템 문제 해결 파일 및 기타 파일
여유 공간	어플라이언스에 남아 있는 여유 공간

By Category(카테고리별) 누적 막대에서 디스크 사용량 카테고리 위로 포인터를 이동하면 해당 카테고리에 사용된 가용 디스크 공간의 비율, 디스크의 실제 저장 공간 및 해당 카테고리의 총 가용 디스

크 공간을 볼 수 있습니다. 악성코드 스토리지 팩이 설치되어 있으면, Files(파일) 카테고리에 대한 총 가용 디스크 공간은 악성코드 스토리지 팩의 가용 디스크 공간입니다.

악성코드 스토리지 팩이 설치된 경우, 위젯 설정을 수정하여 위젯이 By Category(By 카테고리) 누적 막대만 표시하도록 구성하거나 누적 막대와 관리(/), `/Volume`, 및 `/boot` 파티션 사용, 그리고 `/var/storage` 파티션을 함께 표시할 수 있습니다.

위젯 설정은 또한 위젯 업데이트의 빈도뿐 아니라 대시보드 시간 범위에 현재 디스크 사용량 또는 수집한 디스크 사용량 통계량을 표시 여부를 제어합니다.

인터페이스 트래픽 위젯

Interface Traffic(인터페이스 트래픽) 위젯은 수신된 트래픽(Rx) 및 어플라이언스의 관리 인터페이스에 전송된(Tx) 트래픽 비율을 표시합니다. 7000 및 8000 Series디바이스의 경우, 이 위젯은 센싱 인터페이스에 대한 정보도 표시합니다. 이 위젯은 사전 정의된 모든 대시보드에 기본적으로 표시되지는 않습니다.

악성코드 라이선스가 정기적으로 활성화되는 매니지드 디바이스는 사용자가 동적 분석을 구성하지 않은 경우에도 AMP 클라우드 연결을 시도합니다. 따라서 이러한 디바이스는 전송된 트래픽을 표시하는데, 이는 자연스러운 동작입니다. 아웃바운드(전송됨) 트래픽은 플로우 제어 패킷을 포함합니다. 따라서 7000 및 8000 Series 디바이스의 패시브 센싱 인터페이스는 전송된 트래픽을 표시할 수 있습니다. 이 또한 자연스러운 동작입니다.

위젯 환경 설정은 위젯 업데이트의 빈도를 제어합니다. 7000 및 8000 Series디바이스의 환경 설정에서는 사용되지 않은 인터페이스에 대한 트래픽 속도의 표시 여부도 제어할 수 있습니다(기본적으로 위젯에는 활성 인터페이스의 트래픽 속도만 표시됨).

침입 이벤트 위젯

Intrusion Events(침입 이벤트) 위젯은 대시보드 시간 범위 중에 발생한 침입 이벤트를 우선순위별로 구성하여 보여줍니다. 여기에는 삭제된 패킷 및 서로 다른 영향과 함께 침입 이벤트에 대한 통계도 포함됩니다. 이 위젯은 Summary Dashboard(요약 대시보드)의 Intrusion Events(침입 이벤트) 탭에 기본적으로 나타납니다.

위젯 환경 설정에서 다음을 선택할 수 있습니다.

- **Event Flags(**이벤트 플래그**)**는 삭제된 패킷, 삭제 가능성이 있는 패킷 또는 특정 영향이 있는 이벤트를 별도 그래프로 표시합니다. **All(**모두**)**를 선택하고 영향 또는 규칙 상태와 상관없이 모든 침입 이벤트에 대한 추가 그래프를 표시합니다.

  아이콘에 대한 설명은 침입 이벤트 작업, 2909 페이지를 참조하십시오. 영향 레벨 번호 위에 나타나는 화살표(해당되는 경우)는 인라인 결과를 설명하며 다음과 같이 정의됩니다.

  표 ***20:*** 워크플로 및 테이블 보기에서 인라인 결과 필드 내용

아이콘	표시 내용
검은색 아래쪽 화살표	시스템이 규칙을 트리거한 패킷을 삭제했음을 나타냅니다.

아이콘	표시 내용
회색 아래쪽 화살표	(인라인 구축에서) **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화하는 경우 또는 시스템 정리 중 Drop and Generate(삭제 및 생성) 규칙이 이벤트를 생성한 경우 IPS가 패킷을 삭제했음을 나타냅니다.
아이콘 없음(공란)	트리거된 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되지 않았음을 나타냅니다.

수동 구축에서 인라인 인터페이스가 탭 모드에 있는 경우를 포함하여 침입 정책의 규칙 상태 또는 인라인 삭제 작업에 상관없이 시스템은 패킷을 삭제하지 않습니다.

- **Show(**표시**)**는 **Average Events Per Second(**초당 평균 이벤트**)**(EPS) 또는 **Total Events(**총 이벤트**)**를 지정합니다.
- **Vervical Scale(**세로 비율**)**은 **Linear(**선형**)**(증분) 또는 **Logarithmic(**로그**)**(10배) 비율을 지정합니다.
- 위젯 업데이트 빈도입니다.

이 위젯에서 다음을 수행할 수 있습니다.

- 삭제된 패킷, 삭제 가능성이 있는 패킷 또는 특정 영향에 해당하는 그래프를 클릭하여 해당 유형의 침입 이벤트를 볼 수 있습니다.
- 삭제된 이벤트에 해당하는 그래프를 클릭하여 해당 이벤트를 볼 수 있습니다.
- 삭제 가능성이 있는 이벤트에 해당하는 그래프를 클릭하여 해당 이벤트를 볼 수 있습니다.
- **All(**모두**)** 그래프를 클릭하여 모든 침입 이벤트를 볼 수 있습니다.

결과 이벤트 보기는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 침입 이벤트에 액세스하면 어플라이언스에 대한 이벤트(또는 전역) 시간대가 변경됩니다. 참고로 침입 규칙 상태 또는 침입 정책의 인라인 삭제 동작과 상관없이, 패시브 구축의 패킷은 삭제되지 않습니다.

네트워크 컴플라이언스 위젯

Network Compliance(네트워크 컴플라이언스) 위젯은 사용자가 설정한 화이트리스트에 대한 호스트의 규정준수를 요약하여 보여줍니다. 기본적으로 이 위젯은 활성 상관관계 정책에 있는 모든 규정준수 화이트리스트에 대해 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 원도표를 표시합니다. 이 위젯은 Detailed Dashboard(상세 대시보드)의 Correlation(상관관계) 탭에 기본적으로 나타납니다.

위젯 환경설정을 수정하여 모든 화이트리스트 또는 특정 화이트리스트에 대한 네트워크 규정준수를 표시하도록 위젯을 설정할 수 있습니다.

모든 화이트리스트에 대한 네트워크 규정준수를 표시하도록 선택하는 경우, 호스트가 활성 상관관계 정책에서 임의의 화이트리스트를 따르지 않으면 위젯은 해당 호스트를 규정을 준수하지 않는 호스트로 간주합니다.

또한 위젯 환경 설정을 사용하여 네트워크 규정준수를 표시하기 위해 사용할 세 가지 서로 다른 스타일 중 하나를 지정할 수 있습니다.

Network Compliance(네트워크 컴플라이언스**)** 스타일(기본값)은 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 원 그래프를 표시합니다. 원도표를 클릭하면 호스트 위반 횟수를 볼 수 있습니다. 그러면 하나 이상의 화이트리스트를 위반하는 호스트가 나열됩니다.

Network Compliance over Time(시간에 따른 네트워크 컴플라이언스**)(%)** 스타일은 대시보드 시간 범위 중에 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 상대 비율을 보여주는 누적 영역 그래프를 표시합니다.

Network Compliance over Time(시간에 따른 네트워크 컴플라이언스**)**스타일은 대시보드 시간 범위 중에 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 선 그래프를 표시합니다.

환경 설정은 위젯 업데이트의 빈도를 제어합니다. **Show Not Evaluated(**평가되지 않은 이벤트 표시**)** 확인란을 선택하고 평가되지 않은 이벤트를 숨깁니다.

제품 라이선싱 위젯

Product Licensing(제품 라이선싱) 위젯은 현재 Firepower Management Center에 설치된 디바이스와 기능 라이선스를 보여줍니다. 또한 라이선싱된 항목 수 및 허용된 나머지 라이선싱된 항목 수를 나타냅니다. 미리 정의된 모든 대시보드에 기본적으로 표시되지는 않습니다.

위젯의 상단 섹션은 Firepower Management Center에 설치된 모든 디바이스 및 기능을 표시합니다. 여기에는 임시 라이선스가 포함되지만 Expiring Licenses(만료 라이선스) 섹션은 임시 라이선스와 만료된 라이선스만 표시합니다.

위젯 백그라운드의 막대는 사용 중인 라이선스의 각 유형에 대한 백분율을 나타냅니다. 막대는 오른쪽에서 왼쪽으로 읽어야 합니다. 만료된 라이선스는 취소 회선으로 표시됩니다.

위젯 환경 설정을 수정하여 현재 라이선싱된 기능 또는 라이선싱할 수 있는 모든 기능 중 하나를 표시하는 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

라이선스 유형을 클릭하여 로컬 구성의 License(라이선스) 페이지로 이동하거나 기능 라이선스를 추가 또는 삭제할 수 있습니다.

제품 업데이트 위젯

Product Updates(제품 업데이트) 위젯은 어플라이언스에 현재 설치된 소프트웨어의 요약과 함께 다운로드했지만 아직 설치하지 않은 업데이트에 대한 정보도 표시합니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯은 예약된 작업을 사용하여 최신 버전을 확인하기 때문에 업데이트를 다운로드, 푸시 또는 설치하는 예약된 작업을 구성할 때까지 `Unknwon(알 수 없음)`을 표시합니다.

위젯 설정을 수정하여 최신 버전을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

이 위젯에서는 소프트웨어를 업데이트할 수 있는 페이지의 링크도 제공합니다. 다음 작업을 수행할 수 있습니다.

- 현재 버전을 클릭하여 어플라이언스를 수동으로 업데이트합니다.
- 최신 버전을 클릭하여 업데이트를 다운로드하는 예약된 작업을 생성합니다.

RSS 피드 위젯

RSS Feed 위젯은 RSS 피드를 대시보드에 추가합니다. 기본적으로 이 위젯은 Cisco 보안 뉴스의 피드를 보여줍니다. 이는 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

회사 뉴스, Snort.org 블로그 또는 Cisco Threat Research 블로그의 사전 구성된 피드를 표시하도록 위젯을 구성할 수도 있고, 위젯 환경 설정에서 URL을 지정하여 다른 RSS 피드에 대한 사용자 지정 연결을 생성할 수도 있습니다. FMC는 FMC에서 인식하는 CA(Certificate Authority)에서 서명한 신뢰할 수 있는 서버 인증서를 사용하는 경우에만 암호화된 RSS 피드를 표시할 수 있습니다. CA를 사용하는 암호화된 RSS 피드를 FMC에서 인식하지 못하거나 자체 서명 인증서를 사용하는 RSS 피드 위젯을 표시하도록 구성하면 검증이 실패하고 위젯이 피드를 표시하지 않습니다.

피드는 24시간마다 업데이트되며(수동으로 업데이트 가능), 위젯은 어플라이언스의 현지 시간을 기반으로 피드가 업데이트된 마지막 시간을 표시합니다. 어플라이언스는 웹사이트(사전 구성된 두 피드의 경우) 또는 구성한 사용자 지정 피드에 액세스할 수 있어야 합니다.

위젯을 구성할 때에는 또한 위젯에 표시할 피드의 스토리 수는 물론 헤드라인과 함께 스토리의 설명을 표시할지 여부도 선택할 수 있습니다. 모든 RSS 피드가 설명을 사용하는 것은 아닙니다.

RSS Feed 위젯에서 다음을 수행할 수 있습니다.

- 스토리를 보려는 피드에서 스토리 중 하나를 클릭할 수 있습니다.
- **more** 링크를 클릭하여 피드의 웹사이트로 이동할 수 있습니다.
- 업데이트( )을 클릭하여 피드를 수동으로 업데이트할 수 있습니다.

시스템 로드 위젯

System Load(시스템 로드) 위젯은 CPU 사용량(각 CPU), 메모리(RAM) 사용량, 어플라이언스에서 시스템 로드(또한 실행을 기다리는 프로세스의 수로 측정된 로드 평균)를 보여줍니다. 이는 현재 및 대시보드 시간 범위 모두를 보여주는 것입니다. 이는 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 로드 평균을 보여주거나 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

시스템 시간 위젯

System Time(시스템 시간) 위젯은 어플라이언스의 로컬 시스템 시간, 가동 시간 및 부팅 시간을 보여줍니다. 이는 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 부팅 시간을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 어플라이언스의 시계와 위젯 동기화의 빈도를 제어합니다.

화이트 목록 이벤트 위젯

화이트 목록 이벤트 위젯은 대시보드 시간 범위 중에 우선순위별 초당 평균 이벤트 수를 보여줍니다. 이 위젯은 Default Dashboard(상세 대시보드)의 Correlation(상관관계) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 서로 다른 우선순위의 화이트 목록 이벤트를 표시하도록 위젯을 구성할 수 있습니다.

위젯 환경 설정에서 다음을 수행할 수 있습니다.

- 하나 이상의 **Priorities(**우선순위**)** 확인란을 선택하고 특정 우선순위의 이벤트(우선순위가 없는 이벤트 포함)에 대해 별도의 그래프를 표시합니다.
- **Show All(**모두 표시**)**를 선택하고 우선순위와 상관없이 모든 화이트 목록 이벤트에 대해 추가 그래프를 표시합니다.
- **Vervical Scale(**세로 비율**)**을 선택하고 **Linear(**선형**)**(증분) 또는 **Logarithmic(**로그**)**(10배) 비율을 선택합니다.

환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

특정 우선순위의 화이트 목록 이벤트를 보려면 그래프 하나를 클릭하고, 모든 화이트 목록 이벤트를 보려면 **All(**모두**)** 그래프를 클릭합니다. 어떤 경우든 이벤트는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 화이트 목록 이벤트에 액세스하면 Firepower Management Center에 대한 이벤트(또는 전역) 시간대가 변경됩니다.

대시보드 관리

프로시저

단계 **1** **Overview(**개요**)** > **Dashboards(**대시보드**)**를 선택한 후, 메뉴에서 수정하려는 대시보드를 선택합니다.

단계 **2** 대시보드 관리:

- Create Dashboards(대시보드 생성) — 맞춤형 대시보드를 생성합니다. 맞춤형 대시보드 생성, 381 페이지을 참조하십시오.
- Delete Dashboards(대시보드 삭제) - 대시보드를 삭제하려면 삭제하려는 대시보드 옆에 있는 삭제( )를 클릭합니다. 기본 대시보드를 삭제하는 경우 새 기본 대시보드를 정의해야 합니다. 그렇지 않으면 대시보드 보기를 시도할 때마다 대시보드를 선택하라는 메시지가 어플라이언스에 표시됩니다.
- Edit Options(편집 옵션) — 맞춤형 대시보드 옵션을 편집합니다. 대시보드 옵션 수정, 383 페이지을 참조하십시오.
- Modify Time Constraints(시간 제한 수정) — 대시보드 시간 설정 수정, 383 페이지에 설명된 대로 시간 표시를 수정하거나 대시보드를 일시중지/일시중지 취소합니다.

단계 **3** 대시 보드를 추가(대시보드 추가, 379 페이지 참조), 삭제(닫기( ) 클릭) 및 이름 변경(대시보드 이름 변경, 384 페이지 참조)합니다.

참고 대시보드 순서는 변경할 수 없습니다.

단계 **4** 대시보드 위젯 관리:

- Add Widgets(위젯 추가) — 대시보드에 위젯을 추가합니다. 대시보드에 위젯 추가, 379 페이지을 참조하십시오.
- Configure Preferences(환경설정 구성) — 위젯 환경설정을 구성합니다. 위젯 환경설정 구성, 380 페이지을 참조하십시오.
- Customize Display(디스플레이 맞춤화) — 위젯 디스플레이를 맞춤화합니다. 위젯 디스플레이 맞춤 설정, 382 페이지을 참조하십시오.
- View Events(이벤트 보기) — Custom Analysis(맞춤 분석) 위젯에서 관련 이벤트를 확인합니다. 맞춤형 분석 위젯에서 관련 이벤트 보기, 372 페이지을 참조하십시오.

팁 Cisco 사전 정의 대시보드에 있는 Custom Analysis(맞춤 분석) 위젯의 모든 구성은 해당 위젯에 대한 시스템 사전 설정과 일치합니다. 이러한 위젯 중 하나를 변경 또는 삭제하는 경우, 적절한 사전 설정을 기반으로 새 Custom Analysis(맞춤 분석) 위젯을 생성하여 복원할 수 있습니다.

대시보드 추가

프로시저

단계 **1** 수정하려는 대시보드를 확인니다. Viewing Dashboards, 385 페이지을 참조하십시오.

단계 **2** 추가(+) 버튼을 클릭합니다.

단계 **3** 이름을 입력합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

대시보드에 위젯 추가

각 탭은 3단 레이아웃에 하나 이상의 위젯을 표시할 수 있습니다. 대시보드에 위젯을 추가하는 경우, 위젯을 추가하려는 탭을 선택합니다. 시스템에서 위젯이 가장 적은 열에 자동으로 위젯을 추가합니다. 모든 열의 위젯 수가 동일하면 새 위젯은 맨 왼쪽 열에 추가됩니다. 대시보드 탭 하나에 최대 15개의 위젯을 추가할 수 있습니다.

팁 위젯을 추가한 후에는 탭에서 원하는 위치로 이동할 수 있습니다. 그러나 탭 간에는 위젯을 이동할 수 없습니다.

표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형, 사용자 역할 및 현재 도메인(다중 도메인 구축의 경우)에 따라 달라집니다. 모든 사용자 역할이 모든 대시보드 위젯에 액세스할 수 있는 것은 아니므로, 권한이 더 적은 사용자가 권한이 더 많은 사용자가 생성한 대시보드를 볼 때 대시보드의 위젯 중 일부가 표시되지 않을 수 있습니다. 무단 위젯이 대시보드에 나타날 수 있지만 비활성화된 상태로 나타납니다.

프로시저

단계 **1** 위젯을 추가하려는 대시보드를 확인합니다. Viewing Dashboards, 385 페이지을 참조하십시오.

단계 **2** 위젯을 추가하려는 탭을 클릭합니다.

단계 **3** **Add Widgets(**위젯 추가**)**를 클릭합니다. 카테고리 이름을 클릭하여 각 카테고리의 위젯을 볼 수 있습니다. 모든 위젯을 보려면 **All Categories(**모든 카테고리**)**를 클릭합니다.

단계 **4** 추가하려는 위젯 옆에 있는 **Add(**추가**)**를 클릭합니다. Add Widgets(위젯 추가) 페이지는 추가하려는 위젯을 포함하여 탭에 있는 각 유형의 위젯 수를 나타냅니다

팁 동일한 유형의 여러 위젯을 추가하려면(예: 여러 RSS Feed 위젯 또는 여러 Custom Analysis 위젯 추가) **Add(**추가**)**를 다시 클릭합니다.

단계 **5** 위젯 추가가 끝나면 **Done(**완료**)**를 클릭하고 대시보드로 돌아갑니다.

다음에 수행할 작업

- Custom Analysis(맞춤 분석) 위젯을 추가한 경우, 위젯 환경 설정을 구성합니다. 위젯 환경설정 구성, 380 페이지을 참조하십시오.

관련 항목

위젯 가용성, 365 페이지

위젯 환경설정 구성

각 위젯에는 해당 작업을 결정하는 환경 설정 집합이 있습니다.

프로시저

단계 **1** 환경 설정을 변경하고자 하는 위젯의 제목 표시줄에서 기본 설정 표시( )을 클릭합니다.

단계 **2** 필요에 따라 변경합니다.

단계 **3** 환경 설정 섹션을 숨기려면 위젯의 제목 표시줄에서 기본 설정 숨기기( )을 클릭합니다.

맞춤형 대시보드 생성

팁 새 대시보드를 생성하지 않고 다른 어플라이언스에서 대시보드를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 대시보드를 필요에 맞게 수정할 수 있습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Management(**관리**)**를 선택합니다.

단계 **2** **Create Dashboard(**대시보드 생성**)**를 클릭합니다.

단계 **3** 맞춤형 대시보드 옵션, 381 페이지에 설명된 대로 맞춤형 대시보드 옵션을 수정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

맞춤형 대시보드 옵션

아래 표에서는 맞춤형 대시 보드를 만들거나 편집할 때 사용할 수 있는 옵션을 설명합니다.

표 ***21:*** 맞춤형 대시보드 옵션

옵션	설명
대시보드 복사	맞춤형 대시보드를 생성 할 때 사용자 생성 또는 시스템 정의 여부와 상관없이 기존 대시보드를 기반으로 선택할 수 있습니다. 이 옵션을 사용하면 기존 대시보드를 복사하여 필요에 맞게 수정할 수 있습니다. 경우에 따라 **none (**없음**)**을 선택하여 비어 있는 새 대시보드를 생성할 수 있습니다. 이 옵션은 새 대시보드를 생성하는 경우에만 사용할 수 있습니다. 다중 도메인 구축에서는 상위 도메인의 모든 공개 대시보드를 복사할 수 있습니다.
이름	맞춤형 대시보드의 고유한 이름.
설명	맞춤형 대시보드에 대한 간략한 설명.
탭 변경 간격	대시보드가 탭을 순환하는 빈도를 지정합니다(분 단위). 대시보드를 일시 중지하거나 대시보드에 탭이 하나뿐인 경우가 아니면, 여기서 지정한 간격으로 보기가 다음 탭으로 이동합니다. 탭 순환을 비활성화하려면, **Change Tabs Every(**탭 변경 간격**)** 필드에 0을 입력합니다.

옵션	설명
페이지 새로 고침 간격:	전체 대시보드 페이지가 자동으로 새로 고쳐지는 빈도를 결정합니다. 전체 대시보드를 새로 고치면, 마지막 대시보드 새로 고침 이후 다른 사용자가 공유 대시보드에 대해 수행한 환경 설정 또는 레이아웃 변경 사항이나, 자신이 다른 컴퓨터에서 비공개 대시보드에 대해 수행한 변경 사항을 볼 수 있습니다. 빈번한 새로 고침은 예를 들어 대시보드가 항상 표시되는 NOC(네트워크 운영 센터)에서 유용 할 수 있습니다. 로컬 컴퓨터에서 대시보드를 변경하는 경우, NOC의 대시보드가 지정된 간격으로 자동으로 새로 고쳐져 수동 새로 고침이 필요하지 않습니다. 새로 고침은 데이터를 업데이트하지 않으며 데이터 업데이트를 보기 위해 전체 대시보드를 새로 고칠 필요는 없습니다. 개별 위젯은 환경 설정에 따라 업데이트됩니다. 이 값은 **Change Tabs Every(**탭 변경 간격**)** 설정보다 큰 수여야 합니다. 대시보드를 일시 중지하지 않는 한, 여기서 지정한 간격으로 전체 대시보드 새로 고침이 수행됩니다. 주기적인 페이지 새로 고침을 비활성화하려면, **Refresh Page Every(**페이지 새로 고침 간격**)** 필드에 `0`을 입력합니다. 참고 이 설정은 많은 개별 위젯에서 사용할 수 있는 업데이트 간격과는 별개입니다. 대시보드 페이지를 새로 고치면 개별 위젯의 업데이트 간격이 재설정되지만 **Refresh Page Every(**페이지 새로 고침 간격**)** 설정을 비활성화하더라도 위젯은 개별 환경 설정에 따라 업데이트됩니다.
비공개로 저장	어플라이언스의 모든 사용자가 맞춤형 대시보드를 보고 수정할 수 있는지 여부를 결정하거나 사용자 전용으로 사용자 어카운트에 연결됩니다. 참고로 역할과 상관없이 대시보드 액세스 권한이 있는 사용자는 공유 대시보드를 수정할 수 있습니다. 자신만이 특정 대시보드를 수정할 수 있도록 하려면 비공개로 저장해야 합니다.

위젯 디스플레이 맞춤 설정

위젯은 최대화/최소화할 수 있으며 탭에서 다시 정렬할 수도 있습니다.

프로시저

단계 **1** 대시보드를 확인합니다. Viewing Dashboards, 385 페이지을 참조하십시오.

단계 **2** 위젯 디스플레이 맞춤 설정:

- 탭에서 위젯을 다시 정렬하려면 이동시키려는 위젯의 제목 표시줄을 클릭한 다음, 새 위치로 끌어 놓습니다.

  참고 탭 간에는 위젯을 이동할 수 없습니다. 위젯이 다른 탭에 표시되기를 원하는 경우, 기존 탭에서 삭제하고 새 탭에 추가해야 합니다.

- 대시보드에서 위젯을 최소화하거나 최대화하려면 위젯의 제목 표시줄에서 최소화( ) 또는 최대화( )를 클릭합니다.
- 위젯을 삭제해서 더 이상 탭에서 보지 않으려면 위젯의 제목 표시줄에서 닫기( )를 클릭합니다.

대시보드 옵션 수정

프로시저

단계 **1** 편집하려는 대시보드를 확인합니다. Viewing Dashboards, 385 페이지을 참조하십시오.

단계 **2** 수정( ) 버튼을 클릭합니다.

단계 **3** 맞춤형 대시보드 옵션, 381 페이지에 설명된 대로 옵션을 변경합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

대시보드 시간 설정 수정

시간 범위를 변경하여 지난 시간처럼 짧은 기간(기본값) 또는 지난해처럼 긴 기간을 반영할 수 있습니다. 시간 범위를 변경할 때, 시간을 통해 자동 제한될 수 있는 위젯은 새로운 시간 범위를 반영하도록 업데이트합니다.

모든 위젯을 시간으로 제한할 수 있는 것은 아님에 유의하십시오. 예를 들어, 대시보드 시간 범위는 Firepower System 소프트웨어의 이름, 모델 및 최신 버전을 포함한 정보를 제공하는 Appliance Information(어플라이언스 정보) 위젯에 영향을 주지 않습니다.

Firepower System의 엔터프라이즈 구축에서 시간 범위를 긴 기간으로 변경하는 것은, 새 이벤트가 이전 이벤트를 교체하는 빈도에 따라 Custom Analysis(맞춤 분석) 등의 위젯에는 유용하지 않을 수 있습니다.

대시보드를 일시 중지할 수도 있는데, 그렇게 하면 표시를 변경하고 분석을 중단하지 않아도 위젯에서 제공하는 데이터를 검토할 수 있습니다. 대시보드 일시 중지는 다음과 같은 효과가 있습니다.

- **Update Every(**업데이트 간격**)** 위젯 환경 설정과 상관없이 개별 위젯의 업데이트가 중지됩니다.
- 대시보드 탭은 대시보드 속성의 **Cycle Tabs Every(**탭 순환 간격**)** 설정과 상관없이 순환을 중지합니다.
- 대시보드 속성의 **Refresh Page Every(**페이지 새로 고침 간격**)** 설정과 상관없이 대시보드 페이지 새로 고침이 중지됩니다.
- 시간 범위 변경이 영향을 미치지 않습니다.

분석을 마치면 대시보드의 일시 중지를 취소할 수 있습니다. 대시보드의 일시 중지를 취소하면 현재 시간 범위를 반영하여 페이지의 모든 해당 위젯이 업데이트됩니다. 또한 대시보드 속성에서 지정한 설정에 따라 대시보드 탭의 순환이 다시 시작되고, 대시보드 페이지의 새로 고침도 다시 시작됩니다.

시스템 정보를 대시보드로 보내는 플로우가 중단되는 연결 문제나 기타 문제가 발생하면, 대시보드가 자동으로 일시 중지되고 문제가 해결될 때까지 오류 알림이 나타납니다.

참고 대시보드의 일시 중지 여부와 상관없이, 비활성 상태가 1시간(또는 구성된 다른 간격 동안) 지속되면 일반적으로 세션에서 로그아웃됩니다. 대시보드를 오랫동안 수동으로 모니터링할 계획이면 세션 시간 초과에서 일부 사용자를 제외하거나 시스템 시간 초과 설정을 변경하는 방법을 고려해 보십시오.

프로시저

단계 **1** 위젯을 추가하려는 대시보드를 확인합니다. Viewing Dashboards, 385 페이지을 참조하십시오.

단계 **2** 경우에 따라 대시보드 시간 범위를 변경하려면 시간 범위를 **Show the Last(**마지막으로 표시**)** 드롭다운 목록에서 선택합니다.

단계 **3** 경우에 따라 일시 중지( ) 또는 재생( )를 사용하여 시간 범위 제어에서 대시보드를 일시 중지 또는 일시 중지 취소합니다.

대시보드 이름 변경

프로시저

단계 **1** 수정하려는 대시보드를 확인니다. Viewing Dashboards, 385 페이지을 참조하십시오.

단계 **2** 이름을 변경할 대시보드를 클릭합니다.

단계 **3** 이름을 입력합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

Viewing Dashboards

기본적으로 어플라이언스의 홈페이지에는 기본 대시보드가 표시됩니다. 기본 대시보드가 정의되어 있지 않은 경우, 홈페이지는 Dashboard Management(대시보드 관리) 페이지를 표시하는데, 여기에서 표시할 대시보드를 선택할 수 있습니다.

프로시저

언제든지 다음 중 하나를 수행할 수 있습니다.

- 어플라이언스에 대한 기본 대시보드를 보려면 **Overview(**개요**)** > **Dashboards(**대시보드**)**을 선택합니다.
- 특정 대시보드를 보려면 **Overview(**개요**)** > **Dashboards(**대시보드**)**을 선택하고 메뉴에서 해당 대시보드를 선택합니다.
- 모든 사용 가능한 대시보드를 보려면 **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Management(**관리**)**을 선택합니다. 그러면 개별 대시보드 옆에 있는 보기 ( )를 선택하여 대시보드를 볼 수 있습니다.

15 장

상태 모니터링

다음 항목에서는 Firepower System에서 상태 모니터링을 사용하는 방법에 대해 설명합니다.

- 상태 모니터링 요구 사항 및 사전 요건, 387 페이지
- 상태 모니터링 정보, 387 페이지
- 상태 정책, 398 페이지
- 상태 모니터 블랙리스트, 402 페이지
- 상태 모니터 알림, 404 페이지
- 상태 모니터 사용, 407 페이지
- 상태 이벤트 보기, 421 페이지
- 상태 모니터링 기록, 428 페이지

상태 모니터링 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

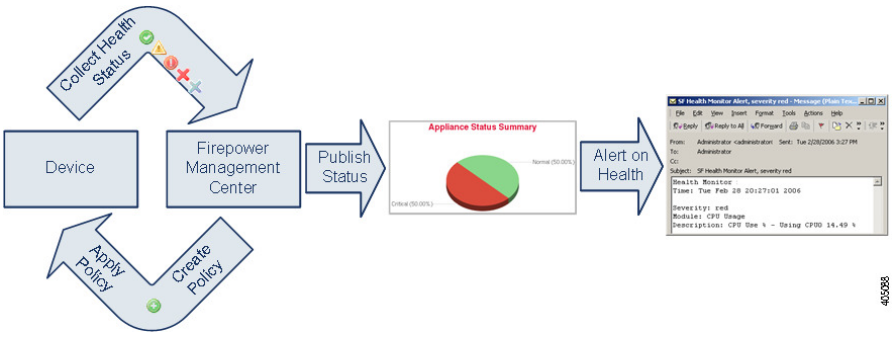
사용자 역할

관리자

유지 보수 사용자

상태 모니터링 정보

Firepower Management Center에서 상태 모니터는 다양한 상태 표시기를 추적하고 Firepower System의 하드웨어 및 소프트웨어가 올바르게 작동하는지 확인합니다. 상태 모니터를 사용하여 Firepower System 구축에서 중요한 기능의 상태를 확인할 수 있습니다.



상태 모니터를 사용하여 *health policy(*상태 정책*)*라고 하는 테스트 집합을 생성하고 하나 이상의 어플라이언스에 상태 정책을 적용할 수 있습니다. *health modules(*상태 모듈*)*라고도 하는 테스트는 지정한 기준을 테스트하는 스크립트입니다. 테스트를 활성화 또는 비활성화하거나 테스트 설정을 변경하여 상태 정책을 수정할 수 있으며, 더 이상 필요하지 않은 상태 정책을 삭제할 수 있습니다. 선택한 어플라이언스를 블랙리스트에 추가하여 해당 메시지를 억제할 수도 있습니다.

상태 정책의 테스트는 구성한 간격으로 자동 실행됩니다. 필요에 따라 모든 테스트 또는 특정 테스트를 실행할 수 있습니다. 상태 모니터는 구성한 테스트 조건을 기반으로 상태 이벤트를 수집합니다.

참고 모든 어플라이언스는 하드웨어 알람 상태 모듈을 통해 하드웨어 상태를 자동으로 보고합니다. Firepower Management Center도 기본 상태 정책에 구성된 모듈을 사용하여 상태를 자동으로 보고합니다. Appliance Heartbeat 모듈과 같은 일부 상태 모듈은 Firepower Management Center에서 실행되어 Firepower Management Center의 매니지드 디바이스의 상태를 보고합니다. 일부 상태 모듈은 해당 모듈로 구성된 상태 정책을 디바이스에 적용하지 않는 경우 매니지드 디바이스 상태를 제공하지 않습니다.

상태 모니터를 사용하여 전체 시스템, 특정 어플라이언스 또는 다중 도메인 구축에서 특정 도메인의 상태 정보에 액세스할 수 있습니다. Health Monitor(상태 모니터) 페이지의 원형 차트 및 상태 테이블은 Firepower Management Center를 포함해 네트워크의 모든 어플라이언스 상태를 시각적으로 요약하여 보여줍니다. 개별 어플라이언스 상태 모니터에서는 특정 어플라이언스의 상태로 드릴다운할 수 있습니다.

완전히 사용자 지정 가능한 이벤트 보기에서는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있습니다. 이러한 이벤트 보기에서는 이벤트 데이터를 검색하고 볼 수 있으며, 조사 중인 이벤트와 관련이 있을 수 있는 다른 정보에 액세스할 수 있습니다. 예를 들어 CPU 사용량이 특정 비율에 도달한 모든 경우를 보려면 CPU 사용량 모듈을 검색하고 비율 값을 입력합니다.

상태 이벤트에 대한 응답으로 이메일, SNMP 또는 syslog 알림을 구성할 수도 있습니다. *health alert(*상태 알림*)*는 표준 알림과 상태 레벨을 연결한 것입니다. 예를 들어, 하드웨어 과부하 때문에 어플라이언스가 실패하지 않도록 하려면 이메일 알림을 설정할 수 있습니다. 그런 다음 CPU, 디스크 또는 메모리 사용량이 어플라이언스에 적용된 상태 정책에서 구성한 경고(Warning) 레벨에 도달할 때마다 이메일 알림을 트리거하는 상태 알림을 생성할 수 있습니다. 반복해서 알림을 수신하는 횟수를 최소화하려면 알림 임계값을 설정할 수 있습니다.

또한 고객 지원에서 요청할 경우 어플라이언스에 대한 문제 해결 파일을 생성할 수도 있습니다.

상태 모니터링은 관리 활동이므로 관리자 사용자 역할 권한이 있는 사용자만 시스템 상태 데이터에 액세스할 수 있습니다.

상태 모듈

*Health modules(*상태 모듈*)* 또는 *health tests(*상태 테스트*)*는 상태 정책에서 지정한 기준을 테스트합니다.

표 ***22:*** 상태 모듈

모듈	어플라이언스	설명
AMP for Endpoints 상태	FMC	이 모듈은 FMC가 초기 연결에 성공한 후 AMP 클라우드 또는 Cisco AMP 프라이빗 클라우드에 연결할 수 없거나 프라이빗 클라우드가 공용 AMP 클라우드에 연결할 수 없는 경우에 경고를 보냅니다. 또한 엔드포인트용 AMP 관리 콘솔을 사용하여 AMP 클라우드 연결을 등록 취소하면 경고를 보냅니다.
Firepower용 AMP 상태 (AMP for Networks 상태)	FMC	이 모듈은 다음의 경우에 경고를 보냅니다. • FMC은 AMP 클라우드(퍼블릭 또는 프라이빗), Cisco Threat Grid 퍼블릭 클라우드 또는 온프레미스 어플라이언스에 연결할 수 없으며 또는 AMP 프라이빗 클라우드는 퍼블릭 AMP 클라우드에 연결할 수 없습니다. • 연결에 사용되는 암호화 키가 유효하지 않습니다. • 디바이스는 Cisco Threat Grid 클라우드 또는 Cisco Threat Grid 온프레미스 어플라이언스에 연결하여 동적 분석을 위한 파일을 제출할 수 없습니다. • 파일 정책 구성을 기반으로 네트워크 트래픽에서 과도한 수의 파일이 검색됩니다. FMC에서 인터넷 연결이 끊어지는 경우, 시스템이 상태 알림을 생성하는 데 최대 30분이 걸릴 수 있습니다.
어플라이언스 하트비트	Any(모든)	이 모듈은 어플라이언스에서 어플라이언스 하트비트가 전송되는지 확인하고, 어플라이언스 하트비트 상태를 기반으로 알림을 전송합니다.
자동 애플리케이션 우회 상태	7000 및 8000 Series	이 모듈은 어플라이언스가 우회 임계값에 설정된 시간(초 단위) 내에 응답하지 않아서 우회되었는지 확인하고, 우회가 발생하면 알림을 전송합니다.
카드 재설정	Any(모든)	이 모듈은 하드웨어 장애 때문에 다시 시작된 네트워크 카드를 확인하고, 재설정이 발생하면 알림을 전송합니다.
기존 라이선스 모니터	FMC	이 모듈은 기본 라이선스가 충분히 남아 있는지 확인합니다. 스택의 디바이스가 라이선스 세트와 일치하지 않는 경우에도 알림을 전송합니다. 모듈에 대해 자동으로 구성된 경고 레벨을 기반으로 알림이 전송됩니다. 이 모듈의 구성은 변경할 수 없습니다.

모듈	어플라이언스	설명
클러스터/페일오버 상태	FTD	이 모듈은 디바이스 클러스터의 상태를 모니터링합니다. 이 모듈은 다음의 경우 경고를 보냅니다. • 새 기본 유닛이 클러스터에 선택됩니다. • 새 보조 유닛에서 클러스터에 가입합니다. • 기본 또는 보조 유닛이 클러스터를 떠납니다.
구성 데이터베이스	FMC	이 모듈은 구성 데이터베이스 크기를 확인하고, 크기가 모듈에 대해 구성된 값(기가바이트)을 초과하면 알림을 보냅니다.
연결 통계	FTD	이 모듈은 연결 통계 및 NAT 변환 수를 모니터링합니다.
CPU 사용량(코어당)	FTD	이 모듈은 모든 코어의 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
CPU 사용 데이터 플레인	FTD	이 모듈은 디바이스에 있는 모든 데이터 플레인의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
CPU 사용량 Snort	FTD	이 모듈은 디바이스에 있는 Snort 프로세스의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
CPU 사용량 시스템	FTD	이 모듈은 디바이스에 있는 모든 시스템의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
중요한 프로세스 통계	FTD	이 모듈은 중요한 프로세스의 상태, 리소스 소비 및 재시작 횟수를 모니터링합니다.
구축된 컨피그레이션 통계	FTD	이 모듈은 구축된 설정에 대한 통계(예: ACE 수 및 IPS 규칙)를 모니터링합니다.

모듈	어플라이언스	설명
디스크 상태	Any(모든)	이 모듈은 하드 디스크의 성능과 어플라이언스의 악성코드 스토리지 팩(설치된 경우)을 점검합니다. 이 모듈에서는 하드 디스크와 RAID 컨트롤러(설치된 경우)가 실패할 위험이 있을 때 또는 악성코드 스토리지 팩이 아닌 추가 하드 드라이브가 설치된 경우 Warning(노란색) 상태 알림을 생성합니다. 설치된 악성코드 스토리지 팩을 탐지할 수 없는 경우에는 Alert(빨간색) 상태 알림이 생성됩니다.
디스크 사용	Any(모든)	이 모듈은 어플라이언스 하드 드라이브 및 악성코드 스토리지 팩의 디스크 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 비율을 초과하면 알림을 전송합니다. 또한 시스템이 모니터링되는 디스크 사용량 카테고리에서 과도하게 파일을 삭제하는 경우 또는 모듈 임계값을 기반으로 그러한 카테고리 외의 디스크 사용량이 과도한 수준에 도달하는 경우에도 알림을 전송합니다. 디스크 사용량 알림의 문제 해결 시나리오에 대한 내용은 이벤트 상태 모니터 알림의 디스크 사용량 및 소모, 469 페이지의 내용을 참조하십시오. 디스크 사용량 상태 모듈을 사용 하 여 기기에서 /및/ 또는 볼륨 파티션의 디스크 사용량을 모니터링 하 고 배수 빈도를 추적 합니다. 디스크 사용 모듈은 /boot 파티션을 모니터링되는 파티션으로 나열하지만 파티션의 크기는 정적이므로 모듈은 부팅 파티션에서 경고를 보내지 않습니다. 주의 파티션/볼륨에 대한 관리되지 않는 디스크 사용량이 높음에 대한 알림이 상태 정책에 지정된 위험 또는 경고 임계값보다 낮더라도 시스템에서 수동으로 삭제해야 하는 파일이 있음을 나타낼 수 있습니다. 이러한 알림을 받으면 TAC에 문의하십시오.
하드웨어 경보	7000 및 8000 Series Threat Defense(물리적)	이 모듈은 하드웨어의 교체가 필요한지 여부를 판단하고, 하드웨어 상태를 기반으로 알림을 전송합니다. 이 모듈은 또한 하드웨어 관련 데몬의 상태와 고가용성 구축에서 7000 및 8000 Series 디바이스의 상태에 대해 보고합니다.
HA 상태	FMC	이 모듈은 FMC의 고가용성 상태를 모니터링하고 경고합니다. FMC 고가용성이 설정되지 않은 경우, HA 상태는 Not in HA(HA가 아님) 입니다. 이 모듈은 매니지드 디바이스의 페어링 여부와 관계없이 해당 디바이스의 고가용성 상태를 모니터링하거나 경고하지 않습니다. 매니지드 디바이스의 HA 상태는 항상 Not in HA(HA가 아님) 입니다. 디바이스 관리 페이지**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 사용하여 고가용성 쌍의 디바이스를 모니터링합니다.
상태 모니터 프로세스	Any(모든)	이 모듈은 상태 모니터 자체의 상태를 모니터링하고, FMC에서 마지막으로 상태 이벤트를 수신한 후 시간(분 단위)이 Warning(경고) 또는 Critical(심각) 한도를 초과하면 알림을 전송합니다.

모듈	어플라이언스	설명
	FMC	이 모듈은 FMC가 모니터할 수있는 호스트의 수가 한계에 가까워지고 모듈에 구성된 경고 수준에 따라 경고를 할지 결정합니다. 자세한 내용은 Firepower System 호스트 제한, 2391 페이지의 내용을 참고하십시오.
인라인 링크 불일치 경보	다음을 제외한ASA FirePOWER 모든 매니지드 디바이스	이 모듈은 인라인 집합과 관련된 포트를 모니터링하고, 인라인 쌍의 두 인터페이스가 서로 다른 속도를 협상하는 경우 알림을 전송합니다.
인터페이스 상태	Any(모든)	이 모듈은 디바이스가 현재 트래픽을 수집하는지 확인하고, 물리적 인터페이스와 집계 인터페이스의 트래픽 상태를 기준으로 알림을 제공합니다. 물리적 인터페이스의 경우 정보에 인터페이스 이름, 링크 상태 및 대역폭이 포함됩니다. 집계 인터페이스의 경우 정보에 인터페이스 이름, 활성 링크의 수, 총 집계 대역폭이 포함됩니다. ASA FirePOWER의 경우, DataPlaneInterfacex라는 인터페이스(여기서 x는 숫자값)는 내부 인터페이스(사용자 정의 아님)이며 시스템 내 패킷 플로우에 관여합니다.
침입 및 파일 이벤트 비율	모든 매니지드 디바이스	이 모듈은 초당 침입 이벤트 수를 모듈에 대해 구성된 제한과 비교하고, 제한을 초과하는 경우 알림을 전송합니다. 침입 및 파일 이벤트 비율이 0이면 침입 프로세스가 다운되거나 매니지드 디바이스가 이벤트를 전송하지 못할 수 있습니다. **Analysis(분석)** > **Intrusions(침입)** > **Events(이벤트)**을 선택하고 이벤트가 디바이스에서 수신되는지 확인합니다. 일반적으로 네트워크 세그먼트의 이벤트 속도는 초당 이벤트 20개입니다. 이 평균 속도의 네트워크 세그먼트에서 Events per second(Critical)는 50, Events per second (Warning)는 30으로 설정해야 합니다. 시스템에 대한 제한을 확인하려면 디바이스의 Statistics(통계) 페이지에서 Events/Sec 값을 찾고(**System(시스템)** > **Monitoring(모니터링)** > **Statistics(통계)**), 다음 공식을 사용하여 제한을 계산합니다. • Events per second (Critical) = Events/Sec * 2.5 • Events per second (Warning) = Events/Sec * 1.5 두 가지 제한 중 하나에 대해 설정할 수 있는 최대 이벤트 수는 999이며, Critical 제한이 Warning 제한보다 높아야 합니다.
ISE 연결 상태 모니터	FMC	이 모듈은 Cisco ISE(Identity Services Engine)와 FMC간의 서버 연결 상태를 모니터링 합니다. ISE는 추가 사용자 데이터, 디바이스 유형 데이터, 디바이스 위치 데이터, SGT(Security Group Tags), SXP(Security Exchange Protocol) 서비스를 제공합니다.

모듈	어플라이언스	설명
링크 상태 전파	NGIPSv, ASA FirePOWER, Firepower 9300, Firepower 2100 Series, Firepower 1000 Series를 제외하고 모두	페어링된 인라인 집합의 링크가 실패하는 경우를 확인하고 링크 상태 전파 모드를 트리거합니다. 링크 상태가 쌍으로 전파되면 해당 모듈에 대한 상태 분류가 Critical로 변경되고 다음과 같은 메시지가 나타납니다. `Module Link State Propagation: ethx_ethy is Triggered` 여기서 `x`및 `y`는 쌍을 이룬 인터페이스 번호입니다.
메모리 사용	Any(모든)	이 모듈은 어플라이언스의 메모리 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 레벨을 초과하면 알림을 전송합니다. 메모리가 4GB를 넘는 어플라이언스의 경우 프리셋 알림 임계값은 시스템 문제를 일으킬 수 있는 사용 가능한 메모리의 비율을 고려하는 공식을 기반으로 합니다. 4GB를 넘는 어플라이언스에서는 Warning 임계값과 Critical 임계값 사이의 간격이 매우 좁기 때문에 Cisco에서는 **Warning Threshold %(**경고 임계값 **%)** 값을 `50`으로 수동으로 설정할 것을 권장합니다. 이렇게 하면 문제를 해결할 수 있도록 적시에 어플라이언스에 대한 메모리 알림을 받을 수 있습니다. 버전 6.6부터 FMCv를 버전 6.6.0 이상으로 업그레이드하는 데 필요한 최소 RAM은 28GB이며, FMCv 구축에 권장되는 RAM은 32GB입니다. 기본 설정을 줄이지 않는 것이 좋습니다. 대부분의 FMCv 인스턴스의 경우 32GB RAM, FMCv 300의 경우 64GB가 필요합니다(VMware만 해당). 주의 RAM이 부족하여 FMCv 구축에 할당되면 상태 모니터에서 중요 알림이 생성됩니다. 복잡한 액세스 제어 정책 및 규칙을 적용할 경우 상당한 리소스가 소모되어 성능이 저하될 수 있습니다.FirePOWER Services 소프트웨어이 포함된 일부 저사양 ASA 디바이스는 디바이스의 메모리 할당을 가능한 한 최대로 사용하기 때문에 수시로 메모리 사용 경고를 생성할 수 있습니다.
메모리 사용량 데이터 플레인	FTD	이 모듈은 데이터 플레인 프로세스에서 사용하는 할당된 메모리의 백분율을 확인하고 메모리 사용량이 모듈에 대해 설정된 백분율을 초과할 때 경고를 표시합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 `80`입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 `90`입니다.
메모리 사용량 Snort	FTD	이 모듈은 Snort 프로세스에서 사용하는 할당된 메모리의 백분율을 확인하고 메모리 사용량이 모듈에 대해 설정된 백분율을 초과할 때 경고를 표시합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 `80`입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 `90`입니다.

모듈	어플라이언스	설명
플랫폼 결함	Firepower 1000/2100	Firepower 2100 및 Firepower 1000 디바이스에서 결함은 FMC에서 관리하는 변경 가능한 개체입니다. 각 결함은 Firepower 1000/2100 인스턴스의 장애 또는 경고 임계값 증가를 나타냅니다. 결함의 라이프사이클 중에 상태 또는 심각도가 서로 변경될 수 있습니다. 각 결함에는 결함이 제기된 시점에 영향을 받은 개체의 운영 상태에 대한 정보가 포함됩니다. 결함이 과도적이고 실패가 해결될 경우, 개체가 기능적 상태로 전환됩니다. 자세한 내용은*Cisco Firepower 1000 /2100 FXOS* 결함 및 오류 메시지 가이드를 참조하십시오.
전력 공급 장치	물리적 FMC 7000 및 8000 Series	이 모듈은 디바이스의 전력 공급 장치를 교체해야 하는지 여부를 확인하고, 전력 공급 장치 상태를 기반으로 알림을 전송합니다. 참고 8000 Series 디바이스에 정전이 발생하면 알림을 생성하는 데 최대 20분이 소요될 수 있습니다.
프로세스 상태	Any(모든)	이 모듈은 어플라이언스의 프로세스가 프로세스 관리자 외부에서 종료되는지를 확인합니다. 프로세스가 프로세스 관리자 외부에서 고의로 종료되면 모듈 상태가 Warning으로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다. 프로세스가 프로세스 관리자 외부에서 비정상적으로 종료되거나 충돌되면 모듈 상태가 Critical로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다.
영역	모든 매니지드 디바이스	영역 또는 사용자 불일치에 대한 경고 임계값을 설정할 수 있습니다. • 사용자 불일치: 사용자가 다운로드되지 않고 Firepower Management Center에 보고됩니다. 사용자 불일치가 발생하는 일반적인 이유는 사용자가 Firepower Management Center 다운로드에서 제외된 그룹에 속하기 때문입니다. 영역 필드, 2467 페이지에서 논의된 정보를 검토합니다. • 영역 불일치: 사용자가 Firepower Management Center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다. 자세한 내용은 영역 또는 사용자 불일치 탐지, 2483 페이지의 내용을 참고하십시오.
탐지 재구성	모든 매니지드 디바이스	이 모듈은 디바이스 재구성이 실패한 경우 경고를 보냅니다.

모듈	어플라이언스	설명
RRD 서버 프로세스	FMC	이 모듈은 시계열 데이터를 저장하는 라운드 로빈 데이터 서버가 제대로 실행되고 있는지 확인합니다. 마지막으로 업데이트된 이후 RRD 서버가 다시 시작되면 알림이 전송됩니다. RRD 서버 다시 시작의 연속 업데이트 수가 모듈 컨피그레이션에 지정된 수에 도달하면 Critical 또는 Warning 상태로 들어가게 됩니다.
보안 인텔리전스	FMC	이 모듈은 보안 인텔리전스를 사용 중이고 FMC가 피드를 업데이트할 수 없거나 피드 데이터가 손상되었거나 인식할 수 없는 IP 주소를 포함하는 경우 알림을 표시합니다. 디바이스의 위협 데이터 업데이트 모듈도 참조하십시오.
스마트 라이선스 모니터	FMC	이 모듈은 다음의 경우에 경고를 보냅니다. • 스마트 라이선싱 에이전트(Smart Agent)와 스마트 소프트웨어 매니저 간에 통신 오류가 있습니다. • 제품 인스턴스 등록 토큰이 만료되었습니다. • 스마트 라이선스 사용량이 미준수 상태입니다. • 스마트 라이선스 권한 부여 또는 평가 모드 만료 되었습니다.
Snort ID 메모리 사용량	FTD	메모리 사용량이 모듈에 대해 설정된 레벨을 초과할 때 Snort ID 처리 및 알림에 대한 경고 임계값을 설정할 수 있습니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 80입니다.
Snort 통계	FTD	이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort 통계를 모니터링합니다.

모듈	어플라이언스	설명
디바이스에서 위협 데이터 업데이트	Any(모든 상태)	디바이스가 위협을 탐지하는 데 사용하는 특정 인텔리전스 데이터 및 구성은 30분마다 클라우드의 FMC에서 업데이트됩니다. 이 모듈은 사용자가 지정한 기간 내에 해당 정보가 디바이스에 업데이트되지 않은 경우 경고를 보냅니다. 모니터링되는 업데이트는 다음을 포함합니다. • 로컬 URL 카테고리 및 평판 데이터 • 보안 인텔리전스 URL 목록 및 피드. Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 URL이 포함됩니다. • 보안 인텔리전스 네트워크 목록 및 피드(IP 주소). Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 IP 주소가 포함됩니다. • 보안 인텔리전스 DNS 목록 및 피드. Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 도메인이 포함됩니다. • 에서 로컬 악성코드 분석 서명(ClamAV) • Threat Intelligence Director의 SHA 목록. **Objects(**개체**) > Object Management(**개체 관리**) > Security Intelligence(**보안 인텔리전스**) > Network Lists and Feeds(**네트워크 목록 및 피드**)** 페이지에 나와 있습니다. • 동적 분석 설정. **AMP > Dynamic Analysis Connections(**동적 분석 연결**)** 페이지에 구성되어 있습니다. • 캐시된 URL 만료와 관련한 Threat Configuration 설정. **System(**시스템**) > Integration(**통합**) > Cloud Services**페이지의 Cached URLs Expire 설정을 포함합니다. (URL 캐시에 대한 업데이트는 이 모듈에서 모니터링하지 않습니다.) • 이벤트 전송에서의 Cisco Cloud와의 통신 이슈 **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)** 페이지의 **Cisco Cloud** 상자를 참조하십시오. 참고 Threat Intelligence Director 업데이트는 TID가 시스템에 구성되어 있고 피드가 있는 경우에만 포함됩니다. 기본적으로 이 모듈은 1시간 후에 warning(경고) 알림을 보내고 24시간 후에 critical(심각) 알림을 보냅니다. 이 모듈에서 FMC 또는 어떠한 디바이스에 실패가 표시되는 경우, FMC가 디바이스에 연결되는지 확인합니다. URL 카테고리 및 평판 데이터 유형의 실패가 표시되는 메모리 부족 디바이스의 경우, 메모리 사용 문제 해결, 1707 페이지를 참조하십시오.

모듈	어플라이언스	설명
시계열 데이터 모니터링	FMC	이 모듈은 시계열 데이터(예: 상관관계 이벤트 카운트)가 저장된 디렉토리에 손상된 파일이 있는지를 추적하고, 손상되어 제거된 것으로 파일에 플래그가 표시되는 경우 알림을 전송합니다.
동기화 상태	Any(모든)	이 모듈은 NTP를 사용하여 시간을 가져오는 디바이스 시계와 NTP 서버에 있는 시계의 동기화를 추적하고, 두 시계 간 차이가 10초를 넘으면 알림을 전송합니다.
URL 필터링 모니터	FMC	FMC가 다음에 실패하는 경우 이 모듈이 경고를 보냅니다. • Cisco Cloud에 등록 • Cisco Cloud에서 URL 위협 데이터 업데이트 다운로드 • 완전한 URL 조회 이러한 경고에 대해 시간 임계값을 구성할 수 있습니다. 디바이스의 위협 데이터 업데이트 모듈도 참조하십시오.
VPN 상태	FMC	이 모듈은 Firepower 디바이스 간에 하나 이상의 VPN 터널이 다운되면 알림을 보냅니다. 이 모듈을 다음을 추적합니다. • 7000 및 8000 Series 디바이스에 대한 VPN) • Site-to-Site VPN Firepower Threat Defense 주의 VTI(Virtual Tunnel Interface)로 생성된 사이트 대 사이트 VPN 터널은 터널이 다운될 때 상태 알림을 생성하지 않습니다. VTI를 사용하는 VPN에서 패킷 손실이 발생하는 경우 VPN 설정을 확인하십시오. • 원격 액세스 VPN Firepower Threat Defense

상태 모니터링 구성

프로시저

단계 **1** 상태 모듈, 389 페이지에 설명된 대로 모니터링 하려는 상태 모듈을 결정합니다.

Firepower System에 있는 각 어플라이언스 종류에 대해 특정 정책을 설정하고 해당 어플라이언스에 맞는 테스트만 활성화할 수 있습니다.

팁 모니터링 동작을 사용자 지정하지 않고 빠르게 상태 모니터링을 활성화하려면 이 용도로 제공되는 기본 정책을 적용할 수 있습니다.

단계 **2** 상태 정책 생성, 398 페이지에 설명된 대로 상태를 추적하려는 각 어플라이언스에 상태 정책을 적용합니다.

단계 **3** (선택 사항). 상태 모니터 알림 생성, 405 페이지에 설명된 대로 상태 모니터 알림을 구성합니다.

상태 레벨이 특정 상태 모듈에 대해 특정 심각도에 도달할 때 트리거되는 이메일, syslog 또는 SNMP 알림을 설정할 수 있습니다.

상태 정책

상태 정책에는 여러 모듈용으로 구성된 상태 테스트 기준이 포함되어 있습니다. 각 어플라이언스에 대해 어떤 상태 모듈을 실행할지 제어할 수 있으며, 각 모듈에 의해 실행되는 테스트에서 사용할 특정 제한을 구성할 수 있습니다.

상태 정책을 구성할 때에는 해당 정책에 대해 각 상태 모듈을 활성화할지 여부를 결정합니다. 또한 각 사용 가능 모듈에서 프로세스의 상태를 평가 하는 때마다 보고할 상태를 제어 하는 조건을 선택합니다.

시스템의 모든 어플라이언스에 적용할 수 있는 하나의 상태 정책을 생성하거나, 특정 어플라이언스에 적용하고자 하는 각 상태 정책을 사용자 지정하거나, 제공되는 기본 상태 정책을 사용할 수 있습니다. 다중 도메인 구축에서, 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

기본 상태 정책

Firepower Management Center에서 상태 모니터는 기본 상태 정책을 제공하여 어플라이언스의 상태 모니터링을 신속하게 구현할 수 있습니다. 기본 상태 정책에서는 실행 중인 플랫폼에서 사용할 수 있는 상태 모듈이 대부분 자동으로 활성화됩니다. 기본 상태 정책은 자동으로 Firepower Management Center에 적용됩니다. 또한 매니지드 디바이스를 Firepower Management Center에 추가하는 경우 기본 상태 정책이 매니지드 디바이스에 적용됩니다. 기본 상태 정책은 수정할 수 없지만, 이를 복사하여 해당 컨피그레이션을 기반으로 사용자 지정 정책을 생성할 수 있습니다.

상태 정책 생성

어플라이언스와 함께 사용할 상태 정책을 사용자 지정하려면 새 정책을 생성할 수 있습니다. 초기에는 정책의 설정이 새 정책의 기반으로 선택한 상태 정책에서 오는 설정으로 채워집니다. 정책 내 모듈을 활성화 또는 비활성화할 수 있으며 필요에 따라 각 모듈의 알림 기준을 변경할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는

하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** 새 정책의 기본으로 사용할 기존 정책을 **Copy Policy(**정책 복사**)** 드롭다운 목록에서 선택합니다**.**

단계 **4** 정책의 이름을 입력합니다.

단계 **5** 이 정책에 대한 설명을 입력합니다.

단계 **6** **Save(**저장**)**를 선택하고 정책 정보를 저장합니다.

단계 **7** 사용하려는 모듈을 선택합니다.

단계 **8** **Enabled(**활성화**)**옵션에서 **On(**켬**)**을 선택하고 상태 테스트를 위한 모듈의 사용을 활성화합니다.

단계 **9** 해당되는 경우, **Critical(**심각**)**및 **Warning(**경고**)** 기준을 설정합니다.

단계 **10** 모듈에 대한 추가 설정을 구성합니다. 각 모듈에 7-10단계를 반복합니다.

단계 **11** 다음 3가지 옵션을 사용할 수 있습니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy(상태 정책) 페이지로 돌아가려면, **Save Policy and Exit(**정책 저장 및 종료**)**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy(상태 정책) 페이지로 돌아가려면 **Cancel(**취소**)**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 작업이 완료된 후 **Save Policy and Exit(**정책 저장 및 종료**)**를 클릭하면 모든 변경 사항이 저장됩니다. **Cancel(**취소**)**을 클릭하면 모든 변경 사항이 취소됩니다.

다음에 수행할 작업

- 상태 정책 적용, 399 페이지에 설명된 대로 각 어플라이언스에 상태 정책을 적용합니다. 이렇게 하면 변경 사항이 적용되고 영향을 받는 모든 정책에 대한 정책 상태가 업데이트됩니다.

상태 정책 적용

어플라이언스에 상태 정책을 적용하면, 정책에서 활성화한 모든 모듈에 대한 상태 테스트가 어플라이언스의 프로세스 및 하드웨어의 상태를 모니터링합니다. 상태 테스트는 정책에 구성된 간격으로 계속 실행되면서 어플라이언스에 대한 상태 데이터를 수집한 다음 Firepower Management Center로 전달합니다.

상태 정책에서 모듈을 활성화한 다음 상태 테스트가 필요하지 않은 어플라이언스에 정책을 적용하면, 상태 모니터는 해당 상태 모듈의 상태를 비활성으로 보고합니다.

모든 모듈이 비활성화된 정책을 어플라이언스에 적용하면, 적용된 모든 상태 정책이 어플라이언스에서 제거됩니다.

정책이 이미 적용된 어플라이언스에 다른 정책을 적용하면, 새로 적용된 테스트를 기반으로 새 데이터의 표시에 약간의 레이턴시가 발생합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** 적용하려는 정책 옆에 있는 적용( )를 클릭합니다.

팁 Health Policy(상태 정책) 열 옆의 상태( )는 어플라이언스의 현재 상태를 나타냅니다. System Policy(시스템 정책) 열 옆의 상태( )은(는) Firepower Management Center와(과) 디바이스 간 통신 상태를 나타냅니다. 제거(제거( ))를 클릭하면 현재 적용된 정책을 제거할 수 있습니다.

단계 **3** 상태 정책을 적용할 어플라이언스를 선택합니다.

단계 **4** **Apply(**적용**)**를 클릭하고 선택한 어플라이언스에 정책을 적용합니다.

다음에 수행할 작업

- 필요한 경우 작업 상태를 모니터링합니다. 작업 메시지 보기, 445 페이지를 참조하십시오.

  정책이 성공적으로 적용됨과 동시에 어플라이언스의 모니터링이 시작됩니다.

상태 정책 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** 수정하려는 NAT 정책 옆의 수정( )을 클릭합니다.

단계 **3** 원하는 대로 정책 또는 정책 설명 필드를 편집 합니다.

단계 **4** 수정하려는 상태 모듈을 클릭합니다.

단계 **5** 상태 모듈, 389 페이지에 설명된 대로 설정을 수정합니다.

단계 **6** 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy(상태 정책) 페이지로 돌아가려면, **Save Policy and Exit(**정책 저장 및 종료**)**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy(상태 정책) 페이지로 돌아가려면 **Cancel(**취소**)**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 작업이 완료된 후 **Save Policy and Exit(**정책 저장 및 종료**)**를 클릭하면 모든 변경 사항이 저장됩니다. **Cancel(**취소**)**을 클릭하면 모든 변경 사항이 취소됩니다.

다음에 수행할 작업

- 상태 정책 적용, 399 페이지에 설명된 대로 상태 정책을 다시 적용합니다. 이렇게 하면 변경 사항이 적용되고 영향을 받는 모든 정책에 대한 정책 상태가 업데이트됩니다.

상태 정책 삭제

더 이상 필요 없는 상태 정책을 삭제할 수 있습니다. 어플라이언스에 여전히 적용된 정책을 삭제하면, 다른 정책을 적용할 때까지 정책 설정이 그대로 유지됩니다. 또한 장치에 적용 되는 상태 정책을 삭제 하면 기본 연결 된 알림 응답을 비활성화할 때까지 장치에 적용 되는 모든 상태 모니터링 경고가 활성 상태로 유지 됩니다.

다중 도메인 구축에서는 현재 도메인에서 만든 상태 정책만 삭제할 수 있습니다.

팁 어플라이언스에 대한 상태 모니터링을 중지하려면 모든 모듈이 비활성화된 상태 정책을 생성하여 어플라이언스에 적용합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)** 을(를) 선택합니다.

단계 **2** 삭제하려는 정책 옆에 있는 삭제( )를 클릭합니다.
성공적으로 삭제했음을 알리는 메시지가 나타납니다.

상태 모니터 블랙리스트

일반적인 네트워크 유지 보수 과정에서 어플라이언스를 비활성화하거나 일시적으로 사용할 수 없도록 만들 수 있습니다. 이러한 중단은 고의적인 것이므로 해당 어플라이언스의 상태가 Firepower Management Center의 요약 상태에 영향을 미치지 않도록 할 수 있습니다.

어플라이언스나 모듈에 대한 상태 모니터링 상태 보고를 비활성화하려면 상태 모니터 블랙리스트 기능을 사용할 수 있습니다. 예를 들어, 네트워크의 한 세그먼트를 사용할 수 없게 될 것임을 알고 있는 경우 해당 세그먼트의 매니지드 디바이스에 대한 상태 모니터링을 일시적으로 비활성화할 수 있습니다. 그러면 디바이스에 대한 연결이 무효화되므로 Firepower Management Center의 상태가 Warning 또는 Critical 상태로 표시되지 않습니다.

상태 모니터링 상태를 비활성화하면 상태 이벤트는 여전히 생성되지만 비활성화된 상태를 갖게 되어 상태 모니터의 상태에 영향을 미치지 않습니다. 어플라이언스나 모듈을 블랙리스트에서 제거하면 블랙리스트에 있는 동안 생성된 이벤트는 계속해서 비활성 상태를 표시합니다.

어플라이언스에서 일시적으로 상태 이벤트를 비활성화하려면 블랙리스트 구성 페이지로 이동하고 블랙리스트에 어플라이언스를 추가합니다. 설정이 적용되면 시스템은 전체적인 상태를 계산할 때 블랙리스트의 어플라이언스를 더 이상 포함하지 않습니다. Health Monitor Appliance Status Summary(상태 모니터 어플라이언스 상태 요약)에는 어플라이언스가 비활성 상태로 나열됩니다.

때로는 어플라이언스에서 개별 상태 모니터링 모듈만 블랙리스트에 추가하는 것이 좀 더 실용적일 수 있습니다. 예를 들어 Firepower Management Center에서 호스트 제한에 도달하는 경우, FireSIGHT 호스트 상태 메시지를 블랙리스트에 추가할 수 있습니다.

기본 Health Monitor 페이지에서, 특정 상태 행의 화살표를 클릭하여 해당 상태의 어플라이언스 목록을 볼 수 있도록 확장하면 블랙리스트에 추가된 여러 어플라이언스를 구분할 수 있습니다.

블랙리스트에 추가되거나 부분적으로 추가된 어플라이언스의 보기를 확장하면 차단 목록( ) 및 표기법이 표시됩니다.

참고 Firepower Management Center에서 Health Monitor 블랙리스트 설정은 로컬 구성 설정입니다. 따라서 디바이스를 블랙리스트에 추가한 다음, 삭제 후 Firepower Management Center에서 다시 등록하는 경우 블랙리스트 설정이 계속 유지됩니다. 새롭게 다시 등록한 디바이스는 계속 블랙리스트에 유지됩니다.

다중 도메인 구축에서 상위 도메인의 관리자는 하위 도메인의 어플라이언스 또는 상태 모듈을 블랙리스트에 추가할 수 있습니다. 그러나 하위 도메인의 관리자는 상위 구성을 무시하고 해당 도메인의 디바이스에 대한 블랙리스트를 지울 수 있습니다.

어플라이언스를 블랙리스트에 추가

어플라이언스를 개별적으로 또는 그룹, 모델 또는 관련 상태 정책별로 블랙리스트에 추가할 수 있습니다.

블랙리스트 설정이 적용되면 어플라이언스가 Health Monitor Appliance Module Summary(상태 모니터 어플라이언스 모듈 요약) 및 Device Management(디바이스 관리) 페이지에서 비활성으로 표시됩니다. 어플라이언스에 대한 상태 이벤트에 상태가 Disabled(비활성화)로 표시됩니다.

개별 어플라이언스의 이벤트 및 상태를 비활성으로 설정하려면 어플라이언스를 블랙리스트에 추가할 수 있습니다. 블랙리스트 설정이 적용되면 어플라이언스가 Health Monitor Appliance Module Summary(상태 모니터 어플라이언스 모듈 요약)에서 Disabled(비활성)로 표시되고, 어플라이언스에 대한 상태 이벤트에 상태가 Disabled(비활성)로 표시됩니다.

다중 도메인 구축에서 상위 도메인의 어플라이언스를 블랙리스트에 추가하면 모든 하위 도메인에 대해 어플라이언스가 블랙리스트에 표시됩니다. 하위 도메인은 이 상속된 구성을 무시하고 블랙리스트를 지울 수 있습니다. 전역 수준에서 Firepower Management Center만 블랙리스트에 추가할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Blacklist(**블랙리스트**)**을 선택합니다.

단계 **2** 오른쪽에 있는 드롭다운 목록을 사용하여 그룹별, 모델별 또는 상태 정책별로 목록을 정렬합니다.

팁 Health Policy(상태 정책) 열 옆의 상태 아이콘(상태( ))은 어플라이언스의 현재 상태를 나타냅니다. System Policy(시스템 정책) 열 옆의 상태 아이콘(상태( ))은 Firepower Management Center와 디바이스 간 통신 상태를 나타냅니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 그룹, 모델 또는 정책 카테고리의 모든 어플라이언스를 블랙리스트에 추가하려면 해당 카테고리 확인란을 선택한 후, **Blacklist Selected Devices(**선택된 디바이스 블랙리스트 추가**)**를 클릭합니다.
- 그룹, 모델 또는 정책 카테고리의 모든 어플라이언스를 블랙리스트에서 지우려면 해당 카테고리 확인란을 선택한 후, **Clear Blacklist on Selected Devices(**선택된 디바이스의 블랙리스트 지우기**)**를 클릭합니다.

상태 정책 모듈을 블랙리스트에 추가

어플라이언스에서 개별 상태 정책 모듈을 블랙리스트에 추가할 수 있습니다. 모듈의 이벤트가 어플라이언스의 상태를 Warning(경고) 또는 Critical(심각)로 변경하지 못하게 하려면 이 기능을 사용할 수 있습니다.

블랙리스트 설정이 적용되면 Blacklist(블랙리스트) 페이지 및 Appliance Health Monitor Module Status Summary(어플라이언스 상태 모니터 모듈 상태 요약)에서 어플라이언스가 **Partially Blacklisted(**부분 블랙리스트 추가**)** 또는 **All Modules Blacklisted(**모든 모듈 블랙리스트 추가**)**로 표시됩니다. 단, Appliance Status Summary(어플라이언스 상태 요약) 메인 페이지에서는 확장된 보기에만 표시됩니다.

팁 개별적으로 블랙리스트에 추가한 모듈은 필요 시 다시 활성화할 수 있도록 계속 추적해야 합니다. 실수로 모듈을 비활성 상태로 남겨 두면 필요한 Warning(경고) 또는 Critical(심각) 메시지를 놓칠 수 있습니다.

다중 도메인 구축에서 상위 도메인의 관리자는 하위 도메인의 상태 모듈을 블랙리스트에 추가할 수 있습니다. 그러나 하위 도메인의 관리자는 이러한 상위 구성을 무시하고 해당 도메인의 디바이스에 대한 블랙리스트를 지울 수 있습니다. 전역 수준에서 Firepower Management Center 상태 모듈만 블랙리스트에 추가할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Blacklist(**블랙리스트**)**를 선택합니다.

단계 **2** 수정하려는 어플라이언스 옆에 있는 수정( )을 클릭합니다.

단계 **3** 블랙리스트에 추가하려는 상태 정책 모듈 옆의 확인란을 선택합니다. 특정 모듈은 특정 디바이스만 적용됩니다. 자세한 내용은 상태 모듈, 389 페이지을 참조 하십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

상태 모니터 알림

상태 정책에서 모듈에 대한 상태가 변경될 때 이메일, SNMP 또는 시스템 로그를 통해 알리도록 알림을 설정할 수 있습니다. 기존 알림 응답을 트리거할 상태 이벤트 레벨과 연결하고, 특별한 레벨의 상태 이벤트가 발생할 때 알릴 수 있습니다.

예를 들어 어플라이언스의 하드 디스크 공간이 부족해질 것이 우려되면, 남은 디스크 공간이 Warning(경고) 수준에 도달할 때 시스템 관리자에게 이메일을 자동으로 전송할 수 있습니다. 하드 디스크가 계속 채워지면 하드 드라이브가 Critical(심각) 수준에 도달할 때 두 번째 이메일을 전송할 수 있습니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

상태 모니터 알림 정보

상태 모니터에 의해 생성되는 알림에는 다음 정보가 포함됩니다.

- Severity(심각도) - 알림의 심각도를 나타냅니다.
- Module(모듈) - 테스트 결과가 알림을 트리거한 상태 모듈을 지정합니다.
- Description(설명) - 테스트 결과가 알림을 트리거한 상태 테스트를 포함합니다.

아래 표는 이러한 심각도 수준을 설명합니다.

표 *23:* 알림 심각도

심각도	설명
중대	상태 테스트 결과가 Critical(심각) 알림 상태를 트리거하는 기준을 충족함.
경고	상태 테스트 결과가 Warning(경고) 알림 상태를 트리거하는 기준을 충족함.
정상	상태 테스트 결과가 Normal(정상) 알림 상태를 트리거하는 기준을 충족함.
오류	상태 테스트가 실행되지 않음.
복원됨	상태 테스트 결과가 Critical(심각) 또는 Warning(경고) 알림 상태에 이어 Normal(정상) 알림 상태로 전환되는 기준을 충족함.

상태 모니터 알림 생성

이 절차를 수행하려면 관리자 사용자여야 합니다.

상태 모니터 알림을 생성할 때 심각도, 상태 모듈 및 알림 응답 간에 연결을 생성합니다. 기존 알림을 사용할 수도 있고 특별히 시스템 상태에 대해 보고하도록 새 알림을 구성할 수도 있습니다. 선택한 모듈에 대해 심각도가 발생하면 알림이 트리거됩니다.

기존 임계값을 복제하는 방식으로 임계값을 생성하거나 업데이트하는 경우 충돌이 발생합니다. 중복된 임계값이 존재하면 상태 모니터는 가장 적은 알림을 생성하는 임계값을 사용하고 나머지는 무시합니다. 임계값의 시간 제한 값은 범위가 5~4,294,967,295분이어야 합니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

시작하기 전에

- 상태 경고를 보내는 SNMP, syslog 또는 이메일 서버와 Firepower Management Center의 통신을 제어하는 알림 응답을 구성합니다. Firepower Management Center 알림 응답, 2681 페이지를 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**를 선택합니다.

단계 **2** **Health Alert Name(**상태 알림 이름**)** 필드에 상태 알림의 이름을 입력합니다.

단계 **3** **Severity(**심각도**)** 목록에서 알림을 트리거하기 위해 사용하려는 심각도 수준을 선택합니다.

단계 **4** **Module(**모듈**)** 목록에서 경고를 적용하려는 상태 정책 모듈을 선택합니다.

단계 **5** **Alert(**알림**)** 목록에서 지정된 심각도 수준에 도달할 때 트리거하려는 알림 응답을 선택합니다.

단계 **6** 경우에 따라 각 임계값 기간이 끝나고 임계값 카운트가 재설정되기까지의 시간(분 단위)을 **Threshold Timeout(**임계값 시간 초과**)** 필드에 입력합니다.

정책 실행 시간 간격 값이 임계값 시간 초과 값보다 작은 경우에도 지정된 모듈에서 보고된 두 가지 상태 이벤트 사이의 간격은 항상 더 큽니다. 예를 들어 임계값 시간 초과를 8 분으로 변경하고 정책 실행 시간 간격을 5분으로 설정하는 경우, 보고된 이벤트 사이의 간격은 10분(5 x 2)입니다.

단계 **7** **Save(**저장**)**를 클릭하고 상태 알림을 저장합니다.

상태 모니터 알림 수정

이 절차를 수행하려면 관리자 사용자여야 합니다.

상태 모니터 알림과 관련된 심각도, 상태 모듈 또는 알림 응답을 변경하려면 기존의 상태 모니터 알림을 수정할 수 있습니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**를 선택합니다.

단계 **2** **Active Health Alerts(**활성 상태 알림**)** 목록에서 수정하려는 알림을 선택합니다.

단계 **3** **Load(**로드**)**를 클릭하고 선택한 알림에 대한 구성된 설정을 로드합니다.

단계 **4** 필요에 따라 설정을 수정합니다.

단계 **5** **Save(**저장**)**를 클릭하고 수정된 상태 알림을 저장합니다.
구성이 성공적으로 저장되었음을 알리는 메시지가 나타납니다.

상태 모니터 알림 삭제

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**를 선택합니다.

단계 **2** 삭제하려는 활성 상태 알림을 선택한 후 **Delete(**삭제**)**를 클릭합니다.

다음에 수행할 작업

- 알림이 계속 전송되지 않도록 하려면 기본 알림 응답을 비활성화하거나 삭제해야 합니다. Firepower Management Center 알림 응답, 2681 페이지을 참조하십시오.

상태 모니터 사용

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모니터는 Firepower Management Center뿐만 아니라 Firepower Management Center에서 관리하는 모든 디바이스에 대한 편집된 상태를 제공합니다. 상태 모니터는 다음으로 구성됩니다.

- Health Status(상태) 요약 페이지 - FMC에서 관리하는 모든 디바이스 및 Firepower Management Center의 상태를 한눈에 볼 수 있습니다. 디바이스는 해당하는 경우 지리위치, 고가용성 또는 클러스터 상태에 따라 개별적으로 나열되거나 그룹화됩니다.
  - 디바이스 상태를 나타내는 육각형 위에 마우스를 올려놓으면 FMC 및 디바이스의 상태 요약을 확인할 수 있습니다.
  - 디바이스의 왼쪽에 있는 점은 해당 상태를 나타냅니다.
    - 녹색 - 알람 없음
    - 주황색 - 하나 이상의 상태 경고가 표시됨
    - 빨간색 - 하나 이상의 중대 상태 알람
- Monitoring(모니터링) 탐색창 - 디바이스 계층 구조를 탐색할 수 있습니다. 탐색창에서 개별 디바이스에 대한 상태 모니터를 볼 수 있습니다.

다중 도메인 구축에서 상위 도메인의 상태 모니터는 모든 하위 도메인의 데이터를 표시합니다. 하위 도메인에서 상태 모니터는 현재 도메인의 데이터만 표시합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** **Health Status(**상태**)** 랜딩 페이지에서 FMC 및 매니지드 디바이스의 상태를 확인합니다.

a) 디바이스의 상태 요약을 보려면 육각형 위로 마우스 포인터를 올려놓습니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부 사항 보기를 엽니다.

b) 디바이스 목록에서 확장(>) 및 축소(⌄)를 클릭하여 디바이스의 상태 알림 목록을 확장하고 축소합니다.

행을 확장하면 상태, 제목 및 상세 정보를 포함한 모든 상태 알림이 나열됩니다.

참고 상태 알림은 심각도 레벨을 기준으로 정렬됩니다.

단계 **3** Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다. Monitoring(모니터링) 탐색창을 사용하는 경우, 다음을 수행합니다.

a) **Home(**홈**)**을 클릭하여 Health Status(상태) 요약 페이지로 돌아갑니다.

b) Firepower Management Center 자체에 대한 상태 모니터를 보려면 **FMC**를 클릭합니다.

c) 디바이스 목록에서 확장( ) 및 축소( )를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

행을 확장하면 모든 디바이스가 나열됩니다.

d) 디바이스별 상태 모니터를 보려면 디바이스를 클릭합니다.

다음에 수행할 작업

- Firepower Management Center에서 관리하는 모든 디바이스의 편집된 상태 및 메트릭에 대한 자세한 내용은 디바이스 상태 모니터, 408 페이지의 내용을 참조하십시오.
- Firepower Management Center의 상태에 대한 자세한 내용은 FMC 상태 모니터 보기, 418 페이지의 내용을 참조하십시오.

  언제든지 **Home(홈)**을 클릭하여 Health Status(상태) 랜딩 페이지로 돌아갈 수 있습니다.

디바이스 상태 모니터

디바이스 상태 모니터는 Firepower Management Center에서 관리하는 모든 디바이스에 대한 편집된 상태를 제공합니다. 디바이스 상태 모니터는 Firepower 디바이스에 대한 상태 메트릭을 수집하여 시스템 이벤트를 예측하고 이에 응답합니다. 디바이스 상태 모니터는 다음 구성 요소로 이루어집니다.

- System Details(시스템 세부 사항) - 설치된 Firepower 버전 및 기타 구축 세부 사항을 포함하여 매니지드 디바이스에 대한 정보를 표시합니다.
- Troubleshooting & Links(문제 해결 및 링크) - 자주 사용하는 문제 해결 주제 및 절차에 대한 편리한 링크를 제공합니다.
- Health Alerts(상태 알림) - 상태 알림 모니터에서 디바이스의 상태를 한눈에 볼 수 있습니다.
- Time Range(시간 범위) - 다양한 디바이스 메트릭 창에 표시되는 정보를 제한하도록 조정할 수 있는 시간 창입니다.
- Device Metrics(디바이스 메트릭) - 다음을 포함하여 사전 정의된 대시보드에서 범주화된 주요 Firepower 디바이스 상태 메트릭의 어레이입니다.
  - CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
  - 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
  - Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
  - Connections(연결) - 연결 통계 및 NAT 변환 횟수
  - Snort - Snort 프로세스와 관련된 통계.
  - Disk Usage(디스크 사용량) - 파티션별 디스크 크기 및 디스크 사용률을 포함한 디바이스 디스크 사용량

- Critical Processes(중요 프로세스) - 프로세스 재시작과 CPU 및 메모리 사용률과 같이 기타 선택된 상태 모니터를 포함하여 관리 프로세스와 관련된 통계

시스템 세부 사항 및 문제 해결 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

System Details(시스템 세부 사항) 섹션에서는 선택한 디바이스에 대한 일반 시스템 정보를 제공합니다. 해당 디바이스에 대한 문제 해결 작업을 시작할 수도 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 확장(>) 및 축소(⌄)를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

단계 **3** 디바이스별 상태 모니터를 보려면 디바이스를 클릭합니다.

단계 **4** **View System & Troubleshoot Details** …**(**시스템 및 문제 해결 세부 사항 보기**...)** 링크를 클릭합니다.

이 패널은 기본적으로 축소되어 있습니다. 링크를 클릭하면 축소된 섹션이 확장되어 디바이스의 **System Details(**시스템 세부 사항**)** 및 **Troubleshooting & Links(**문제 해결 및 링크**)**가 표시됩니다. 시스템 세부 사항은 다음으로 구성됩니다.

- **Version(**버전**):** Firepower 소프트웨어 버전
- **Model(**모델**):** 디바이스 모델
- **Mode(**모드**):** 방화벽 모드 Firepower Threat Defense 디바이스는 일반 방화벽 인터페이스에 대해 라우팅 방화벽 모드 및 투명 방화벽 모드의 두 가지 방화벽 모드를 지원합니다.
- **VDB:** Cisco VDB(취약성 데이터베이스) 버전
- **SRU:** 침입 규칙 집합 버전
- **Snort:** Snort 버전

단계 **5** 다음 문제 해결 옵션을 이용할 수 있습니다.

- 문제 해결 파일 생성(다음 참조) 특정 시스템 기능에 대한 문제 해결 파일 생성, 473 페이지
- 고급 문제 해결 파일을 생성하고 다운로드합니다. 고급 문제 해결 파일 다운로드, 474 페이지의 내용을 참조하십시오.
- 상태 정책을 생성하고 수정합니다. 상태 정책 생성, 398 페이지의 내용을 참조하십시오.
- 상태 모니터 알림을 생성하고 수정합니다. 상태 모니터 알림 생성, 405 페이지의 내용을 참조하십시오.

디바이스 상태 모니터 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

디바이스 상태 모니터는 Firepower 디바이스의 상태에 대한 자세한 보기를 제공합니다. 디바이스 상태 모니터는 디바이스 메트릭을 컴파일하고 대시보드 어레이에 있는 디바이스의 상태 및 추세를 제공합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 확장(>) 및 축소(⌄)를 클릭하여 매니지드 디바이스 목록을 확장하고 축소합니다.

단계 **3** 페이지 상단에서 디바이스 이름의 바로 오른쪽에 있는 알림에서 디바이스의 **Health Alerts(**상태 알림**)**를 확인합니다.

Health Alerts(상태 알림**)** 위에 포인터를 올려놓으면 디바이스의 상태 요약이 표시됩니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

단계 **4** 오른쪽 상단의 드롭다운에서 시간 범위를 설정할 수 있습니다. 시간 범위는 지난 시간처럼 짧은 기간(기본값) 또는 지난 주처럼 긴 기간을 반영할 수 있습니다. 드롭다운에서 **Custom(**사용자 지정**)**을 선택하여 사용자 지정 시작 및 종료 날짜를 설정합니다.

새로 고침 아이콘을 클릭하여 자동 새로 고침을 5분으로 설정하거나 자동 새로 고침을 해제합니다.

단계 **5** 선택한 시간 범위와 관련하여 추세 그래프에서 구축 오버레이를 보려면 구축 아이콘을 클릭합니다.

구축 아이콘은 선택한 시간 범위 동안의 구축 수를 나타냅니다. 세로 줄은 구축 시작 및 종료 시간을 나타냅니다. 다수의 구축이 있는 경우, 여러 대역/라인이 나타납니다. 점선 위에 있는 아이콘을 클릭하여 구축 세부 사항을 확인합니다.

단계 **6** 디바이스 모니터는 기본적으로 사전 정의된 여러 대시보드에서 상태 및 성능 메트릭을 보고합니다. 메트릭 대시보드에는 다음이 포함됩니다.

- Overview(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.
- CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- Connections(연결) - 연결 통계 및 NAT 변환 횟수
- Snort - Snort 프로세스와 관련된 통계

레이블을 클릭하여 다양한 메트릭 대시보드를 탐색할 수 있습니다. 지원되는 디바이스 메트릭의 전체 목록은 Firepower 디바이스 메트릭, 412 페이지의 내용을 참조하십시오.

단계 **7** 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 지정 상관 관계 대시보드를 생성하려면 디바이스 모니터의 오른쪽 상단 모서리에 있는 더하기 기호(+)를 클릭합니다. 디바이스 메트릭 연계, 411 페이지의 내용을 참조하십시오.

디바이스 메트릭 연계

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

디바이스 상태 모니터에는 시스템 이벤트를 예측하고 응답하는 데 사용되는 주요 Firepower 디바이스 메트릭 어레이가 포함되어 있습니다. 보고된 메트릭을 통해 모든 Firepower 디바이스의 상태를 확인할 수 있습니다. 디바이스 모니터는 기본적으로 여러 미리 정의된 대시보드에서 이러한 메트릭을 보고합니다. 이러한 대시보드에는 다음이 포함됩니다.

- Overview(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.
- CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- Connections(연결) - 연결 통계 및 NAT 변환 횟수
- Snort - Snort 프로세스와 관련된 통계.

사용자 정의 대시보드를 추가하여 상호 연결된 메트릭을 상호 연결할 수 있습니다. 사전 정의된 상관 관계 그룹(예: CPU 및 Snort) 중에서 선택합니다. 또는 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 정의 상관 관계 대시보드를 생성할 수도 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 확장(>) 및 축소(⌄)를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

단계 **3** 디바이스 모니터의 오른쪽 상단 모서리에 있는 더하기 기호(+)를 클릭하여 새 대시보드를 추가합니다.

단계 **4** **Select Correlation Group(**상관 관계 그룹 선택**)** 드롭다운에서 미리 정의된 상관 관계 그룹을 선택하거나 사용자 정의 그룹을 생성합니다.

단계 **5** 미리 정의된 상관 관계 그룹에서 대시보드를 생성하려면 그룹을 선택하고 **Add(**추가**)**를 클릭합니다.

- CPU – 데이터 플레인

- CPU – Snort
- CPU – 기타
- 메모리 – 데이터 플레인
- 패킷 삭제

단계 **6** 사용자 정의 상관 관계 대시보드를 생성하려면:

a) **Custom(**사용자 정의**)**을 선택합니다.

b) 필요에 따라 **Dashboard Name(**대시보드 이름**)** 필드에 고유한 이름을 입력하거나 기본값을 수락합니다.

c) 그런 다음 **Select Metric Group(**메트릭 그룹 선택**)** 드롭다운에서 그룹을 선택한 다음 **Select Metrics(**메트릭 선택**)** 드롭다운에서 해당 메트릭을 선택합니다.

- 연결; 사용 가능한 메트릭은 연결 그룹 메트릭, 414 페이지의 내용을 참조하십시오.
- CPU; 사용 가능한 메트릭은 CPU 그룹 메트릭, 412 페이지의 내용을 참조하십시오.
- 중요 프로세스; 사용 가능한 메트릭은 중요 프로세스 그룹 메트릭, 417 페이지의 내용을 참조하십시오.
- 구축된 구성; 사용 가능한 메트릭은 구축된 컨피그레이션 그룹 메트릭, 416 페이지의 내용을 참조하십시오.
- 디스크; 사용 가능한 메트릭은 디스크 그룹 메트릭, 416 페이지의 내용을 참조하십시오.
- 인터페이스; 사용 가능한 메트릭은 인터페이스 그룹 메트릭, 414 페이지의 내용을 참조하십시오.
- Snort; 사용 가능한 메트릭은 Snort 그룹 메트릭, 415 페이지의 내용을 참조하십시오.

단계 **7** **Add Metrics(**메트릭 추가**)**를 클릭하여 다른 그룹에서 메트릭을 추가하고 선택합니다.

단계 **8** 개별 메트릭을 제거하려면 항목의 오른쪽에있는 **x**를 클릭합니다. 전체 그룹을 제거하려면 삭제 아이콘(휴지통)을 클릭합니다.

단계 **9** **Add(**추가**)**를 클릭하여 워크플로우를 완료하고 상태 모니터에 대시보드를 추가합니다.

단계 **10** 사용자 정의 상관 관계 대시보드를 편집하거나 삭제할 수 있습니다.

Firepower 디바이스 메트릭

다음 섹션에서는 Firepower Threat Defense 디바이스에서 사용 가능한 상태 메트릭에 대해 설명합니다.

CPU 그룹 메트릭

상태 모니터는 프로세스 및 물리적 코어별 CPU 사용률을 포함하여 CPU 이용률과 관련된 통계를 추적합니다.

표 ***24: CPU*** 그룹 메트릭

메트릭	설명	형식
컨트롤 플레인	지난 1분 동안 제어 플레인의 평균 CPU 사용률입니다.	백분율

메트릭	설명	형식
데이터 플레인	지난 1분 동안 데이터 플레인의 평균 CPU 사용률입니다.	백분율
Snort	지난 1분 동안 Snort 프로세스의 평균 CPU 사용률입니다.	백분율
System	지난 1분 동안 시스템 프로세스의 평균 CPU 사용률입니다.	백분율
물리적 코어	지난 1분 동안의 모든 코어에 대한 평균 CPU 사용률입니다.	백분율

메모리 그룹 메트릭

상태 모니터는 데이터 플레인 및 Snort 메모리 사용량을 포함하여 디바이스 메모리 사용률과 관련된 통계를 추적합니다.

표 ***25:*** 메모리 그룹 메트릭

메트릭	설명	형식
버퍼 캐시	버퍼 캐시입니다.	바이트
여유 공간	사용 가능한 총 메모리입니다.	바이트
최대 데이터 플레인	데이터 플레인에서 사용하는 최대 메모리입니다.	바이트
최대 Snort	Snort 프로세스에서 사용하는 최대 메모리입니다.	바이트
Snort에 대한 최대 스왑	Snort 프로세스에서 사용하는 최대 스왑 메모리입니다.	바이트
남은 메모리 블록(1550)	1550 바이트 블록의 사용 가능한 메모리입니다.	숫자
남은 메모리 블록(256)	256 바이트 블록의 사용 가능한 메모리입니다.	숫자
사용된 시스템	시스템에서 사용한 총 메모리입니다.	바이트
합계	사용 가능한 총 메모리입니다.	바이트
총 스왑	스왑에 사용 가능한 총 메모리입니다.	바이트
데이터 플레인	데이터 플레인에서 사용된 총 메모리입니다.	바이트
데이터 플레인에서 사용된 비율	데이터 플레인에 사용된 메모리의 비율입니다.	백분율
Snort에서 사용된 비율	Snort 프로세스에 사용된 메모리의 비율입니다.	백분율
스왑에서 사용된 비율	스왑에 사용된 메모리의 비율입니다.	백분율

메트릭	설명	형식
시스템에서 사용된 비율	시스템에 사용된 메모리의 비율입니다.	백분율
시스템 및 스왑에서 사용된 비율	시스템 및 스왑에 사용된 메모리의 비율입니다.	백분율
Snort	Snort 프로세스에 사용된 총 메모리입니다.	바이트
사용된 스왑	스왑에 사용된 총 메모리입니다.	바이트
Snort에서 사용된 스왑	Snort 프로세스에 사용된 총 스왑 메모리입니다.	바이트

인터페이스 그룹 메트릭

상태 모니터는 인터페이스 상태 및 집계 트래픽 통계를 포함하여 디바이스 인터페이스와 관련된 통계를 추적합니다.

표 ***26:*** 인터페이스 그룹 메트릭

메트릭	설명	형식
패킷 삭제	드롭된 패킷 수입니다.	숫자
평균 입력 패킷 크기	수신 패킷의 평균 크기입니다.	바이트
입력 속도	총 수신 바이트 수입니다.	바이트
입력 패킷	총 수신 패킷 수입니다.	숫자
평균 출력 패킷 크기	발신 패킷의 평균 크기입니다.	바이트
출력 속도	총 발신 바이트 수입니다.	바이트
출력 패킷	총 발신 패킷 수입니다.	숫자
상태	인터페이스의 상태로, 1은 up(가동), 0은 down(중지)입니다.	1 또는 0

연결 그룹 메트릭

상태 모니터는 연결 및 NAT 변환 수와 관련된 통계를 추적합니다.

표 ***27:*** 연결 그룹 메트릭

메트릭	설명	형식
사용 중인 연결	사용 중인 연결 수를 표시합니다.	숫자
최대 연결 수	최대 동시 연결 수를 표시합니다.	숫자
초당 전체 연결 수	모든 연결 유형에 대한 초당 연결 수입니다.	숫자

메트릭	설명	형식
초당 TCP 연결 수	TCP 연결 유형의 초당 연결 수입니다.	숫자
초당 UDP 연결 수	UDP 연결 유형의 초당 연결 수입니다.	숫자
활성화된 연결 유지	Snort 프로세스가 중단될 경우 라우팅 및 투명 인터페이스에서 기존 TCP/UDP 연결을 유지합니다.	숫자
유지되는 연결	현재 유지되는 연결이 활성화된 연결 수입니다.	숫자
가장 활성화된 연결 유지	지금까지 유지되는 가장 많은 연결 수입니다.	숫자
유지되는 최대 연결 수	지금까지 유지되는 가장 많은 최대 연결 수입니다.	숫자
NAT 변환	변환 수를 표시합니다.	숫자
최대 NAT 변환	동시 변환의 기록 최대 값을 한 번에 표시합니다.	숫자

Snort 그룹 메트릭

상태 모니터는 Snort 프로세스와 관련된 통계를 추적합니다.

표 ***28: Snort*** 그룹 메트릭

메트릭	설명	형식
차단된 목록 플로우	Snort에서 삭제한 정책 설정의 플로우 수입니다.	숫자
차단된 패킷	차단된 패킷 수입니다.	숫자
거부된 플로우	거부된 플로우 이벤트 수입니다. 데이터 플레인은 Snort로 전송하기 전에 플로우를 삭제하기로 결정하면 거부된 플로우 이벤트를 Snort로 전송합니다.	숫자
플로우 종료	데이터 플레인은 빠른 경로 플로우가 종료되면 Snort에 플로우 종료 이벤트를 전송합니다.	숫자
빠른 전달 플로우	정책에 의해 빨리 전달되어 검사되지 않은 플로우 수입니다.	숫자
데이터 플레인에서 전달된 삭제된 프레임	데이터 플레인에서 전달된 삭제된 프레임 수입니다.	숫자
삽입된 패킷 삭제됨	Snort가 삭제된 트래픽 스트림에 추가한 패킷 수입니다.	숫자

메트릭	설명	형식
삽입된 패킷	Snort가 생성하여 트래픽 스트림에 추가한 패킷 수입니다. 예를 들어 재설정 작업으로 파단을 구성하는 경우, Snort는 연결을 재설정할 패킷을 생성합니다.	숫자
인스턴스	Snort 인스턴스(프로세스) 수입니다.	숫자
패킷 수신 대기열 사용률	데이터 플레인 수신 대기열의 대기열 사용률입니다.	백분율
Snort가 사용 중이어서 패킷 우회됨	Snort 사용량이 너무 많아 패킷을 처리할 수 없을 때 검사를 우회한 패킷 수입니다.	숫자
Snort 다운으로 인해 패킷 우회됨	Snort가 중단되었을 때 검사를 우회한 패킷 수입니다.	숫자
RX 대기열이 꽉 차서 패킷 우회됨	수신 대기열이 꽉 차서 우회된 패킷 수입니다.	숫자
TX 대기열이 꽉 차서 패킷 우회됨	전송 대기열이 꽉 차서 우회된 패킷 수입니다.	숫자
통과된 패킷	데이터 플레인에서 Snort로 전송된 패킷 수입니다.	숫자
플로우 시작	플로우 시작 이벤트 수입니다. 이러한 이벤트는 Snort가 연결을 추적하고 연결 이벤트를 보고하는 데 도움이 됩니다.	숫자

구축된 컨피그레이션 그룹 메트릭

상태 모니터는 구축된 설정과 관련된 통계(예: IPS 규칙 수 및 ACE 수)를 추적합니다.

표 ***29:*** 구축된 설정 그룹 메트릭

메트릭	설명	형식
ACE의 수	ACE(Access Control Entry) 또는 규칙의 수입니다. ACL(액세스 제어 목록)은 하나 이상의 ACE 또는 규칙으로 구성됩니다.	숫자
규칙의 수	침입 정책에 있는 규칙의 수입니다.	숫자

디스크 그룹 메트릭

상태 모니터는 디스크 크기 및 파티션별 디스크 사용률을 포함하여 디바이스 디스크 사용과 관련된 통계를 추적합니다.

표 ***30:*** 디스크 그룹 메트릭

메트릭	설명	형식
합계	디바이스 디스크의 총 크기입니다.	바이트
사용됨	디바이스 디스크에서 사용된 총 공간입니다.	바이트
/ngfw에서 사용된 %	/ngfw 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/Ngfw/Volume에서 사용된 %	/ngfw/Volume 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/Dev/cgroups에서 사용된 %	/dev/cgroups 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/Mnt/disk0에서 사용된 %	/mnt/disk0 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/Var/volatile에서 사용된 %	/var/volatile 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율

중요 프로세스 그룹 메트릭

상태 모니터는 관리되는 프로세스의 프로세스 재시작과 관련된 통계를 추적합니다. 또한 각 중요 프로세스에 대해 상태 모니터는 CPU 사용률, 메모리 사용률, 업타임 및 상태를 추적합니다.

표 ***31:*** 중요 프로세스 그룹 메트릭

메트릭	설명	형식
CPU 사용률	마지막 1분 동안 제어 플레인 및 데이터 플레인의 평균 CPU 사용률입니다.	백분율
재시작 횟수	지난 1분 동안 제어 플레인의 평균 CPU 사용률입니다.	백분율
상태	지난 1분 동안 데이터 플레인의 평균 CPU 사용률입니다.	백분율
업타임	지난 1분 동안 Snort 프로세스의 평균 CPU 사용률입니다.	백분율
사용된 메모리	지난 1분 동안 시스템 프로세스의 평균 CPU 사용률입니다.	백분율

FMC 상태 모니터 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

FMC Health Monitor(FMC 상태 모니터)는 Firepower Management Center의 상태에 대한 자세한 보기를 제공합니다. 상태 모니터는 다음으로 구성됩니다.

- 상태 테이블 - Firepower Management Center의 전체 상태를 제공합니다.
- 원형 차트 - 활성화된 상태 모듈의 백분율을 나타냅니다.
- 경고 세부 사항 목록-상태 경고의 개요를 제공합니다.

팁 비활성 상태가 1시간(또는 구성된 다른 간격 동안) 지속되면 일반적으로 세션에서 로그아웃됩니다. 상태를 오랫동안 수동으로 모니터링할 계획이면 세션 시간 초과에서 일부 사용자를 제외하거나 시스템 시간 초과 설정을 변경하는 방법을 고려해 보십시오. 자세한 내용은 사용자 어카운트 로그인 옵션 및 세션 시간 제한 구성, 1388 페이지를 참고하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 FMC 및 디바이스별 상태 모니터에 액세스합니다.

단계 **2** **Health Status(**상태**)** 랜딩 페이지에서 FMC의 상태를 확인합니다.

a) FMC의 상태 요약을 보려면 마우스 포인터를 FMC 육각형 모양 위에 둡니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

b) 디바이스 목록에서 **FMC**을 클릭하여 상태 모니터를 봅니다.

행을 확장하면 상태, 제목 및 상세 정보를 포함한 모든 상태 알림이 나열됩니다.

참고 상태 알림은 심각도 레벨을 기준으로 정렬됩니다.

단계 **3** 경우에 따라, **Module Status Summary(**모듈 상태 요약**)** 그래프에서 확인하려는 이벤트 상태 카테고리의 색상을 클릭합니다.

Alert Detail(알림 세부정보) 목록은 디스플레이를 토글하여 이벤트를 표시하거나 숨깁니다.

어플라이언스에 대해 모든 모듈 실행

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 어플라이언스에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 모든 상태 모듈 테스트를 실행할 수도 있습니다.

다중 도메인 구축에서 현재 도메인 및 모든 하위 도메인의 어플라이언스에 대한 상태 모듈 테스트를 실행할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다.의 내용을 참조하십시오.

단계 **2** **Run All Modules(**모든 모듈 실행**)**를 클릭합니다. 상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance(상태 모니터 어플라이언스) 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

특정 상태 모듈 실행

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 모듈에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 해당 상태 모듈 테스트를 실행할 수도 있습니다.

다중 도메인 구축에서 현재 도메인 및 모든 하위 도메인의 어플라이언스에 대한 상태 모듈 테스트를 실행할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다.의 내용을 참조하십시오.

단계 **2** **Module Status Summary(**모듈 상태 요약**)** 그래프에서 확인하려는 상태 알림 카테고리의 색상을 클릭합니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)**열에서 **Run(**실행**)**을 클릭합니다.

상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance(상태 모니터 어플라이언스) 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

상태 모듈 알림 그래프 생성

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

특정 어플라이언스에 대한 특별한 상태 테스트 기간 중에 발생한 결과를 그래프로 표시할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다의 내용을 참조하십시오.

단계 **2** Health Monitor Appliance(상태 모니터 어플라이언스) 페이지의 **Module Status Summary** 그래프에서 확인하려는 상태 알림 상태 카테고리의 색상을 클릭합니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)**열에서 **Graph(**그래프**)**를 클릭합니다.

팁 이벤트가 나타나지 않으면 시간 범위를 조정해야 합니다.

상태 모니터 상태 카테고리

사용 가능한 상태 카테고리가 아래 표에 심각도별로 나열됩니다.

표 ***32:*** 상태 표시기

상태 레벨	상태 아이콘	원 그래프의 상태 색상	설명
오류	오류( )	검은색	어플라이언스에서 하나 이상의 상태 모니터링 모듈이 실패했으며, 실패 이후 성공적으로 다시 실행되지 않았습니다. 상태 모니터링 모듈의 업데이트를 얻으려면 기술 지원 담당자에게 문의하십시오.
중대	중요( )	빨간색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Critical(심각) 한도가 초과되었으며 문제가 해결되지 않았음을 나타냅니다.
경고	경고( )	노란색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Warning(경고) 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다.

상태 레벨	상태 아이콘	원 그래프의 상태 색상	설명
정상	일반( )	녹색	어플라이언스의 모든 상태 모듈이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있습니다.
복원됨	복구됨( )	녹색	어플라이언스의 모든 상태 모듈(Critical(심각) 또는 Warning(경고) 상태에 있던 모듈 포함)이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있음을 나타냅니다.
Disabled(비활성화)	비활성화됨( )	파란색	어플라이언스가 비활성화되었거나 블랙리스트에 추가되었거나, 어플라이언스에 상태 정책이 적용되지 않았거나, 어플라이언스에 현재 도달할 수 없음을 나타냅니다.

상태 이벤트 보기

상태 이벤트 보기(Health Event View) 페이지에서는 Firepower Management Center로그 상태 이벤트의 상태 모니터가 기록한 상태 이벤트를 볼 수 있습니다. 완전하게 맞춤화가 가능한 이벤트 보기에서는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있습니다. 조사하는 이벤트와 관련된 기타 정보에 쉽게 액세스 할 수 있도록 이벤트 데이터를 검색 할 수 있습니다. 각 상태 모듈이 테스트하는 조건을 이해하면 상태 이벤트에 대한 알림을 좀 더 효과적으로 구성할 수 있습니다.

상태 이벤트 보기 페이지에서 많은 표준 이벤트 보기 기능을 수행할 수 있습니다.

상태 이벤트 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

Health Events(상태 이벤트) 페이지의 Table View(테이블 보기)에는 지정된 어플라이언스의 모든 상태 이벤트가 나열됩니다.

Firepower Management Center의 Health Monitor(상태 모니터) 페이지에서 상태 이벤트에 액세스하면 모든 관리되는 어플라이언스에 대한 모든 상태 이벤트가 검색됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

팁 Health Events(상태 이벤트) 테이블이 포함된 상태 이벤트 워크플로의 페이지로 돌아가려면 이 보기에 북마크를 지정할 수 있습니다. 북마크 지정된 보기는 현재 보고 있는 시간 범위 내에서 이벤트를 검색하지만, 필요한 경우 시간 범위를 수정하여 좀 더 최신 정보로 테이블을 업데이트할 수 있습니다.

프로시저

System(시스템**)** > **Health(**상태**)** > **Events(**이벤트**)**를 선택합니다.

팁 상태 이벤트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭하십시오. Select Workflow(워크플로 선택) 페이지에서 **Health Events(**상태 이벤트**)**를 클릭합니다.

참고 이벤트가 나타나지 않으면 시간 범위를 조정해야 합니다.

모듈 및 어플라이언스별로 상태 이벤트 보기

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다. 디바이스 상태 모니터 보기, 410 페이지을 참조하십시오.

단계 **2** **Module Status Summary(**모듈 상태 요약**)** 그래프에서 확인하려는 이벤트 상태 카테고리의 색상을 클릭합니다.

Alert Detail(알림 세부정보) 목록은 디스플레이를 토글하여 이벤트를 표시하거나 숨깁니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)** 열에서 **Events(**이벤트**)**를 클릭합니다.

어플라이언스의 이름 및 제약 조건으로써 지정된 상태 알림 모듈의 이름과 함께 쿼리에 대한 결과가 포함된 Health Events(상태 이벤트) 페이지가 나타납니다. 이벤트가 나타나지 않으면 시간 범위를 조정해야 합니다.

단계 **4** 지정한 어플라이언스에 대한 모든 상태 이벤트를 보려면 **Search Constraints(**검색 제약 조건**)**를 확장하고 **Module Name(**모듈 이름**)** 제약 조건을 클릭하여 제거합니다.

상태 이벤트 테이블 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Bookmark(즐겨찾기) — 현재 페이지에 즐겨찾기에 등록해 빠르게 돌아오려면, **Bookmark This Page(**이 페이지를 즐겨찾기에 등록**)**를 클릭하고 즐겨찾기 이름을 지정한 후 **Save(**저장**)**를 클릭합니다.
- Change Workflow(워크플로 변경) — 다른 상태 이벤트 워크플로 선택하려면, **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- Delete Events(이벤트 삭제) — 상태 이벤트를 삭제하려, 삭제하려는 이벤트 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다. 현재 제한된 보기에서 모든 이벤트를 삭제하려면 **Delete All(**모두 삭제**)**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
- Generate Reports(보고서 생성) — 테이블 보기에서 데이터를 기반으로 보고서를 생성하고 **Report Designer(**리포트 디자이너**)**를 클릭합니다.
- Modify(수정) — 상태 테이블 보기에 나열된 이벤트의 시간 및 날짜 범위를 수정합니다. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
- Navigate(탐색) — 이벤트 보기 페이지를 탐색합니다.
- Navigate Bookmark(즐겨찾기 탐색) — 즐겨찾기 관리 페이지로 이동하려면 이벤트 보기에서 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.
- Navigate Other(기타 탐색) — 관련 이벤트를 보기 위해 다른 이벤트 테이블로 이동합니다.
- Sort(정렬) — 표시되는 이벤트를 정렬하고, 이벤트 테이블에 표시되는 열을 변경하며, 표시되는 이벤트를 제한합니다.
- View All(모두 보기) — 보기에서 모든 이벤트에 대한 이벤트 세부 정보를 보려면, **View All(**모두 보기**)**를 클릭합니다.
- View Details(세부 정보 보기) — 단일 상태 이벤트와 관련된 세부 사항을 보려면, 이벤트의 왼쪽에 있는 아래쪽 화살표 링크를 클릭합니다.
- View Multiple(다중 보기) — 여러 상태 이벤트의 이벤트 세부 정보를 보려면, 세부 정보를 보려는 이벤트에 해당하는 행 옆의 확인란을 선택한 후 **View(**보기**)**를 클릭합니다.
- View Status(상태 보기) - 특정 상태의 모든 이벤트를 보려면 Status(상태) 열의 상태를 클릭하여 해당 상태의 이벤트를 찾습니다.

7000 및 **8000 Series** 디바이스에 대한 하드웨어 알림 세부 정보

참고 8350 하드웨어 플랫폼에는 6개의 팬이 있으며 FAN2~FAN7으로 표시됩니다. 이는 정상적인 동작입니다. 8350 플랫폼에서 FAN1 또는 팬 번호지정과 관련된 하드웨어 알림을 받으면 이 알림을 무시할 수 있습니다.

표 *33: 7000* 및 *8000 Series* 디바이스 모니터링 조건

모니터링되는 상태	노란색 또는 빨간색 오류 조건의 원인
디바이스 고가용성 상태	고가용성 쌍으로 된 7000 또는 8000 Series 디바이스가 더 이상 서로 통신하지 않는 경우(예: 케이블 연결 문제), Hardware Alarms(하드웨어 알림) 모듈이 빨간색으로 바뀝니다.
`ftwo` 데몬 상태	`ftwo` 데몬이 다운되는 경우, Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조가 포함됩니다.
NFE 카드 탐지됨	시스템에서 탐지된 NFE 카드의 수를 나타냅니다. 이 값이 어플라이언스의 예상 NFE 카운트와 일치하지 않으면 Hardware Alarms(하드웨어 알림) 모듈이 빨간색으로 변경됩니다.
NFE 하드웨어 상태	하나 이상의 NFE 카드가 통신하지 않으면 Hardware Alarms(하드웨어 알림) 모듈은 빨간색으로 변경되고 메시지 세부사항에 해당 카드가 나타납니다.
NFE 하트비트	시스템이 NFE 하트비트를 탐지하면 Hardware Alarms(하드웨어 알림) 모듈이 빨간색으로 변경되고 메시지 세부사항에 관련 카드에 대한 참조가 포함됩니다.
NFE 내부 링크 상태	NMSB 및 NFE 카드 간 링크가 다운되면 Hardware Alarms(하드웨어 알림) 모듈이 빨간색으로 변경되고 메시지 세부사항에 관련 포트에 대한 참조가 포함됩니다.
NFE Message 데몬	NFE Message 데몬이 다운되면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.

모니터링되는 상태	노란색 또는 빨간색 오류 조건의 원인
NFE 온도	NFE 온도가 섭씨 36.2도(화씨 97도)를 넘으면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 노란색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다. NFE 온도가 섭씨 38.9도(화씨 102도)를 넘으면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조가 포함됩니다. (해당 되는 경우 NFE 카드 번호 포함).
NFE 온도 상태	특정 NFE 카드의 현재 온도 상태를 나타냅니다. Hardware Alarms(하드웨어 알림) 모듈은 OK(정상)가 녹색, Warning(경고)이 노란색, Critical(심각)이 빨간색을 나타냅니다(해당되는 경우 NFE 카드 번호 포함).
NFE `TCAM` 데몬	NFE `TCAM` 데몬이 다운되면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
`nfm_ipfragd` (호스트 조각) 데몬	`nfm_ipfragd` 데몬이 다운되면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
NFE Platform 데몬	NFE Platform 데몬이 다운되면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
NMSB 커뮤니케이션	Media 어셈블리가 없거나 통신하지 않으면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
`psls` 데몬 상태	`psls` 데몬이 다운되는 경우, Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조가 포함됩니다.

모니터링되는 상태	노란색 또는 빨간색 오류 조건의 원인
`Rulesd`(호스트 규칙) 데몬	`Rulesd` 데몬이 다운되면 Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
`scmd` 데몬 상태	`scmd` 데몬이 다운되는 경우, Hardware Alarms(하드웨어 알림) 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 데몬에 대한 참조가 포함됩니다.

상태 이벤트 테이블

상태 정책에서 활성화하기 위해 선택하는 Health Monitor(상태 모니터) 모듈은 다양한 테스트를 실행하여 어플라이언스 상태를 결정합니다. 상태가 지정된 기준을 충족하면 상태 이벤트가 생성됩니다.

아래 표에서는 상태 이벤트 테이블에서 보고 검색 할 수 있는 필드를 설명합니다.

표 ***34:*** 상태 이벤트 필드

필드	설명
모듈 이름	보려는 상태 이벤트를 생성한 모듈의 이름을 지정합니다. 예를 들어 CPU 성능을 측정하는 이벤트를 보려면, `CPU`를 입력합니다. 그러면 해당 CPU Usage 및 CPU 온도 이벤트가 검색됩니다.
테스트 이름 (검색만 해당)	이벤트를 생성한 상태 모듈의 이름입니다.
시간 (검색만 해당)	상태 이벤트의 타임스탬프.
설명	이벤트를 생성한 상태 모듈의 설명. 예를 들어, 프로세스를 실행할 수 없을 때 생성되는 상태 이벤트에는 `Unable to Execute`라는 레이블이 지정됩니다.
값	이벤트를 생성한 상태 테스트에서 얻은 결과의 값(단위의 수). 예를 들어 Firepower Management Center에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때마다 상태 이벤트가 생성된다면 값은 80~100의 숫자가 될 수 있습니다.

필드	설명
단위	결과의 단위 설명자. 와일드카드 검색을 생성하려면 별표(*)를 사용할 수 있습니다. 예를 들어 Firepower Management Center에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때 상태 이벤트가 생성된다면 단위 설명자는 퍼센트 기호(%)입니다.
상태	어플라이언스에 대해 보고된 상태(Critical(심각), Yellow(노란색), Green(녹색) 또는 Disabled(비활성화)).
도메인	매니지드 디바이스에서 보고한 상태 이벤트의 경우, 상태 이벤트를 보고한 디바이스의 도메인. Firepower Management Center에서 보고한 상태 이벤트의 경우, `Global(전역)`. 이 필드는 다중 도메인 구축에서만 나타납니다.
디바이스	상태 이벤트가 보고된 어플라이언스.

상태 모니터링 기록

기능	버전	세부 사항
새로운 상태 모듈 도입	6.7	CPU 사용 모듈은 더 이상 사용되지 않습니다. 대신 다음 CPU 사용 모듈을 참조하십시오. • **CPU** 사용**(**코어 당**)**: 모든 코어의 CPU 사용을 모니터링합니다. • **CPU** 사용 데이터 플레인: 디바이스에서 모든 데이터 플레인 프로세스의 평균 CPU 사용을 모니터링합니다. • **CPU** 사용 데이터 **Snort**: 디바이스에서 Snort 프로세스의 평균 CPU 사용을 모니터링합니다. • **CPU** 사용량 시스템: 디바이스에 있는 모든 시스템 프로세스의 평균 CPU 사용량을 모니터링합니다. 통계를 추적하기 위해 다음 모듈이 추가되었습니다. • 연결 통계: 연결 통계 및 NAT 변환 수를 모니터링합니다. • 중요 프로세스 통계: 이 모듈은 중요한 프로세스의 상태, 리소스 소비 및 재시작 횟수를 모니터링합니다. • 구축된 구성 통계: 구축 된 구성에 대한 통계(예: ACE 및 IPS 규칙 수)를 모니터링합니다. • **Snort** 통계: 이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort 통계를 모니터링합니다. 메모리 사용을 추적하기 위해 다음 모듈이 추가되었습니다. • 메모리 사용 데이터 플레인: 데이터 플레인 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다. • 메모리 사용량 **Snort**: Snort 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다.

기능	버전	세부 사항
상태 모니터 개선 사항	6.7	상태 모니터에는 다음과 같은 향상된 기능이 추가되었습니다. • 상태 요약 페이지는 Firepower Management Center 및 FMC가 관리하는 모든 디바이스의 상태를 한눈에 볼 수 있도록 합니다. • Monitoring(모니터링) 탐색 창에서는 디바이스 계층 구조를 탐색할 수 있습니다. • 매니지드 디바이스는 개별적으로 나열되거나 해당하는 경우 지리적 위치, 고 가용성 또는 클러스터 상태에 따라 그룹화됩니다. • 탐색창에서 개별 디바이스에 대한 상태 모니터를 볼 수 있습니다. • 상호 관련된 메트릭을 상호 연결하는 맞춤형 대시 보드입니다. 사전 정의된 상관 관계 그룹(예: CPU 및 Snort) 중에서 선택합니다. 또는 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 정의 상관 관계 대시보드를 생성할 수도 있습니다.
기능이 디바이스의 위협 데이터 업데이트 모듈로 이동됨	6.7	로컬 악성 코드 분석 모듈은 더 이상 사용되지 않습니다. 대신 이 정보는 디바이스의 위협 데이터 업데이트 모듈을 참조하십시오. 이전에는 보안 인텔리전스 모듈 및 URL 필터링 모듈에서 제공한 일부 정보가 디바이스의 위협 데이터 업데이트 모듈에서 제공되었습니다.
URL 필터링 모니터링 개선 사항	6.5	이제 URL 필터링 모니터 모듈은 FMC가 Cisco Cloud에 등록하지 못하면 알림을 보냅니다.
URL 필터링 모니터링 개선 사항	6.4	이제 URL 필터링 모니터 경고에 대한 시간 임계값을 구성할 수 있습니다. 수정된 화면: **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)** > **URL Filtering Monitor(URL** 필터링 모니터**)** 페이지의 새로운 옵션. 지원되는 플랫폼: Firepower Management Center
새 상태 모듈: Threat Data Updates on Devices(디바이스에서 위협 데이터 업데이트)	6.3	새 모듈 **Threat Data Updates on Devices(**디바이스에서 위협 데이터 업데이트**)**이 삭제되었습니다. 이 모듈은 디바이스가 위협 탐지에 사용하는 특정 인텔리전스 데이터 및 구성이 사용자가 지정한 기간 내에 디바이스에서 업데이트되지 않은 경우 알림을 보냅니다. 새 화면: **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)**에서의 새 상태 정책 수정된 화면: **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**에서의 새 모니터 결과 지원되는 플랫폼: 6.3 이상 버전을 실행하는 Firepower Management Center 및 매니지드 디바이스.
상태 모니터링	—	버전 6.0 이전에 도입된 기능. 새 화면: **System(**시스템**)** > **Health(**상태**)** 아래 메뉴 옵션 지원되는 플랫폼: Firepower Management Center 및 매니지드 디바이스.

16 장

시스템 모니터링

다음 항목에서는 Firepower 시스템을 모니터링 하는 방법을 설명합니다.

- 시스템 통계 관련 정보, 431 페이지
- 시스템 메시지, 441 페이지
- 시스템 메시지 관리, 444 페이지

시스템 통계 관련 정보

Firepower Management Center 및 7000 및 8000 Series 디바이스 모두에서 시스템 통계를 볼 수 있습니다.

Statistics(통계) 페이지에는 디스크 사용 및 시스템 프로세스, Data Correlator(데이터 상관 처리)(FMC에만 해당) 통계 및 침입 이벤트 정보(FMC에만 해당)를 포함한 일반 어플라이언스 통계의 현재 상태가 나와 있습니다.

호스트 통계 섹션

다음 표는 Statistics(통계 자료) 페이지에 나열된 호스트 통계 자료에 대해 설명합니다.

표 ***35:*** 호스트 통계 자료

카테고리	설명
시간	시스템의 현재 시간
실행 시간	시스템이 마지막으로 시작된 후 경과한 날짜 수(해당되는 경우), 시간 및 분
메모리 사용	사용 중인 시스템 메모리의 백분율
로드 평균	지난 1분, 5분 15분 동안 CPU 큐 프로세스의 평균 수.

카테고리	설명
디스크 사용	사용 중인 디스크의 백분율 자세한 호스트 통계 자료를 보려면 화살표를 클릭합니다.
프로세스	시스템에서 실행 중인 프로세스의 요약.

Disk Usage(디스크 사용량) 섹션

Statistics(통계 자료) 페이지의 Disk Usage(디스크 사용) 섹션에서는 디스크 사용에 대한 즉각적인 개요를 카테고리 및 파티션 상태별로 제공합니다. 디바이스에 악성코드 스토리지 팩이 설치되어 있는 경우, 스토리지 팩의 파티션 상태도 확인할 수 있습니다. 이 페이지를 자주 모니터링하여 시스템 프로세스와 데이터베이스에 충분한 디스크 공간을 사용할 수 있는지 확인할 수 있습니다.

팁 또한 디스크 사용량 상태 모니터를 통해 Firepower Management Center 디스크 사용량을 모니터링하고 디스크 공간 부족에 대해 알림을 보낼 수도 있습니다.

Processes(프로세스) 섹션

통계 페이지의 Processes(프로세스) 섹션에서는 현재 어플라이언스에서 실행 중인 프로세스를 볼 수 있습니다. 이 섹션에서는 실행되고 있는 각 프로세스에 대한 일반 처리 정보 및 특정 정보를 제공합니다. Firepower Management Center의 웹 인터페이스를 사용해 관리되는 모든 디바이스의 프로세스 상태를 볼 수 있습니다.

어플라이언스에서는 데몬 및 실행 파일이라는 두 가지 유형의 프로세스가 실행됩니다. 데몬은 항상 실행되며, 실행 파일은 필요한 경우 실행됩니다.

프로세스 상태 필드

통계 페이지의 프로세스 섹션을 확장하는 경우 다음을 확인할 수 있습니다.

CPU

다음 CPU 사용 정보를 확인할 수 있습니다.

- 사용자 처리 사용 백분율
- 시스템 처리 사용 백분율
- nice 사용 백분율(더 높은 우선 순위를 나타내는 음수인 nice 값을 지닌 프로세스의 CPU 사용량) nice 값은 시스템 프로세스에 대해 예약된 우선 순위를 나타내며 그 범위는 -20(가장 높은 우선 순위)에서 19(가장 낮은 우선 순위)까지입니다.
- 유휴 사용 백분율

MEM

다음 메모리 사용 정보를 확인할 수 있습니다.

- 메모리 내 총 킬로바이트 수
- 메모리 내 사용된 킬로바이트의 총 수
- 메모리 내 무료 킬로바이트의 총 수
- 메모리 내 버퍼된 킬로바이트의 총 수

Swap(스왑)

다음 스왑 사용 정보를 확인할 수 있습니다.

- 스왑 내 총 킬로바이트 수
- 스왑 내 사용된 킬로바이트의 총 수
- 스왑 내 무료 킬로바이트의 총 수
- 스왑 내 캐시된 킬로바이트의 총 수

다음 테이블은 프로세스 섹션의 각 열에 대해 설명합니다.

표 ***36:*** 프로세스 목록 열

열	설명
Pid	프로세스 ID 번호
사용자 이름	프로세스를 실행하는 사용자 또는 그룹 이름
Pri	프로세스 우선 순위
Nice	*nice* 값. 프로세스의 예약 우선 순위를 나타내는 값입니다. 그 범위는 -20(가장 높은 우선 순위)에서 19(가장 낮은 우선 순위)까지입니다.
크기	프로세스가 사용하는 메모리 크기(메가바이트를 나타내는 `m`표시가 없는 경우 킬로바이트 값)
Res	메모리에 상주하는 페이징 파일의 양(메가바이트를 나타내는 `m`이 값 뒤에 오지 않는 한 킬로바이트 단위)

열	설명
상태	프로세스 상태: • D — 프로세스가 중단할 수 없는 잠자기 상태에 있습니다(일반적으로 입력/출력). • N — 프로세스가 양수인 nice 값을 지닙니다. • R — 프로세스가 실행 가능합니다(실행을 위해 큐에서 대기). • S — 프로세스가 절전 모드에 있습니다. • T — 프로세스가 추적 또는 중지되고 있습니다. • W — 프로세스가 호출되고 있습니다. • X — 프로세스가 작동하지 않습니다. • Z — 프로세스가 작동하지 않습니다. • < — 프로세스가 음수인 nice 값을 지닙니다.
시간	프로세스가 실행되고 있는 시간(시간:분:초 단위)
Cpu	프로세스가 사용하고 있는 CPU의 백분율
명령	프로세스의 실행 가능한 이름

관련 항목

시스템 데몬, 434 페이지
실행 파일 및 시스템 유틸리티, 436 페이지

시스템 데몬

데몬은 어플라이언스에서 계속 실행됩니다. 데몬은 필요한 경우 서비스의 가용성을 확인하고 프로세스를 생성합니다. 다음 표에서는 Process Status(처리 상태) 페이지에서 볼 수 있는 데몬을 나열하고 해당 기능에 대한 간단한 설명을 제공합니다.

참고 아래 표는 어플라이언스에서 실행할 수 있는 모든 프로세스의 전체 목록이 아닙니다.

표 ***37:*** 시스템 데몬

데몬	설명
crond	예약된 명령의 실행을 관리합니다(cron 작업).

데몬	설명
dhclient	동적 호스트 IP 주소 부여를 관리합니다.
fpcollect	클라이언트 및 서버 지문의 컬렉션을 관리합니다.
httpd	HTTP(Apache 웹 서버) 프로세스를 관리합니다.
httpsd	HTTPS(SSL을 사용하는 Apache 웹 서버) 서비스를 관리하고 작동하는 SSL 및 유효한 인증서 인증을 확인하며, 어플라이언스에 보안 웹 액세스를 제공하는 백그라운드에서 실행됩니다.
keventd	Linux 커널 이벤트 알림 메시지를 관리합니다.
klogd	Linux 커널 메시지의 차단 및 로깅을 관리합니다.
kswapd	Linux 커널 스왑 메모리를 관리합니다.
kupdated	디스크 동기화를 수행하는 Linux 커널 업데이트 프로세스를 관리합니다.
mysqld	데이터베이스 프로세스를 관리합니다.
ntpd	NTP(Network Time Protocol)프로세스를 관리합니다
pm	Firepower System의 모든 프로세스를 관리하고, 필요한 프로세스를 시작하며 예기치 않게 실패한 모든 프로세스를 다시 시작합니다.
reportd	보고서를 관리합니다.
safe_mysqld	데이터베이스의 안전 모드 운영을 관리하고 오류가 발생하고 파일에 런타임 정보를 로깅할 경우 데이터베이스 데몬을 다시 시작합니다.
SFDataCorrelator	데이터 전송을 관리합니다.
sfestreamer(FMC만)	Event Streamer를 사용하는 서드파티 클라이언트 애플리케이션에 대한 연결을 관리합니다.
sfmgr	어플라이언스로 향하는 sftunnel 연결을 사용하여 어플라이언스의 원격 관리 및 구성을 위한 RPC 서비스를 제공합니다.
SFRemediateD(FMC만)	교정 응답을 관리합니다.
sftimeserviced(FMC만)	시간 동기화 메시지를 관리되는 디바이스에 전달합니다.

데몬	설명
sfmbservice	어플라이언스에 대한 sftunnel 연결을 사용하여 원격 어플라이언스에서 실행되는 sfmb 메시지 브로커 프로세스에 대한 액세스를 제공합니다. 현재는 상태 모니터가 관리되는 디바이스에서 Firepower Management Center로 상태 이벤트 및 알림을 전송하는 데 사용됩니다.
sftroughd	수신 소켓에서 연결을 수신한 후 요청을 처리하기 위해 올바른 실행 파일(일반적으로 Cisco 메시지 브로커, sfmb)을 호출합니다.
sftunnel	원격 어플라이언스와의 통신이 필요한 모든 프로세스에 안전한 커뮤니케이션 채널을 제공합니다.
sshd	SSH(Secure Shell) 프로세스를 관리하고 어플라이언스에 SSH 액세스를 제공하는 백그라운드에서 실행됩니다.
syslogd	시스템 로깅(syslog) 프로세스를 관리합니다.

실행 파일및 시스템 유틸리티

다른 프로세스에 의해 또는 사용자 작업을 통해 수행될 때 실행되는 시스템에는 많은 실행 파일이 있습니다. 다음 표는 Process Status(처리 상태) 페이지에서 볼 수 있는 실행 파일에 대해 설명합니다.

표 ***38:*** 시스템 실행 파일 및 유틸리티

실행 파일	설명
awk	`awk` 프로그래밍 언어로 작성된 프로그램을 실행하는 유틸리티입니다.
bash	GNU Bourne-Again 셸
cat	파일을 읽고 표준 출력에 콘텐츠를 작성하는 유틸리티입니다.
chown	사용자 및 그룹 파일 권한을 변경하는 유틸리티입니다.
chsh	기본 로그인 셸을 변경하는 유틸리티입니다.
SFDataCorrelator(FMC만)	이벤트, 연결 데이터, 네트워크 맵을 생성하기 위해 시스템이 생성한 이진 파일을 분석합니다.
cp	파일을 복제하는 유틸리티입니다.

실행 파일	설명
df	어플라이언스의 여유 공간에 대한 볼륨을 나열하는 유틸리티입니다.
echo	표준 출력에 콘텐츠를 작성하는 유틸리티입니다.
egrep	지정된 입력에 대한 파일 및 폴더를 검색하는 유틸리티이며, 표준 grep에서 지원되지 않는 확장된 정규식 집합을 지원합니다.
find	지정된 입력에 대한 디렉토리를 되풀이하여 검색하는 유틸리티입니다.
grep	지정된 입력에 대한 파일 및 디렉토리를 검색하는 유틸리티입니다.
halt	서버를 중지하는 유틸리티입니다.
httpsdctl	보안 Apache 웹 프로세스를 처리합니다.
hwclock	하드웨어 클럭에 대한 액세스를 허용하는 유틸리티입니다.
ifconfig	네트워크 구성 실행 파일을 나타냅니다. MAC 주소가 일정한 상태를 유지하는지 확인합니다.
iptables	Access Configuration(액세스 구성) 페이지에 적용된 변경 사항에 기반하여 액세스 제한을 처리합니다.
iptables-restore	iptables 파일 복원을 처리합니다
iptables-save	iptables에 저장된 변경 사항을 처리합니다.
kill	세션 및 프로세스를 종료하는 데 사용할 수 있는 유틸리티입니다.
killall	모든 세션 및 프로세스를 종료하는 데 사용할 수 있는 유틸리티입니다
ksh	Korn 셸의 공개 도메인 버전입니다.
logger	명령줄에서 syslog 데몬에 액세스하는 방법을 제공하는 유틸리티입니다.
md5sum	지정된 파일에 대한 체크섬 및 블록 횟수를 인쇄하는 유틸리티입니다.
mv	파일을 옮기는 (이름을 바꾸는) 유틸리티입니다

실행 파일	설명
myisamchk	데이터베이스 표 확인 및 복구를 나타냅니다.
mysql	데이터베이스 프로세스를 나타내며 여러 인스턴스가 표시될 수 있습니다.
openssl	인증서 인증 생성을 나타냅니다.
perl	perl 프로세스를 나타냅니다.
ps	표준 출력에 처리 정보를 작성하는 유틸리티입니다.
sed	하나 이상의 텍스트 파일을 수정하는 데 사용하는 유틸리티입니다.
sfheartbeat	어플라이언스가 활성 상태임을 나타내는 하트비트 브로드캐스트를 식별합니다. 하트비트는 디바이스와 Firepower Management Center 사이의 연결을 유지하는 데 사용됩니다. Firepower Management Center
sfmb	메시지 브로커 프로세스를 나타내며 Firepower Management Center과 디바이스 간 통신을 처리합니다.
sh	Korn 셸의 공개 도메인 버전입니다.
shutdown	어플라이언스를 종료하는 유틸리티입니다.
sleep	지정된 시간(초) 동안 프로세스를 중지하는 유틸리티입니다.
smtpclient	이메일 이벤트 알림 기능이 활성화된 경우 이메일 전송을 처리하는 메일 클라이언트입니다.
snmptrap	SNMP 알림 기능이 활성화된 경우 지정된 SNMP 트랩 서버에 SNMP 트랩 데이터를 전달합니다.
snort	Snort가 실행되고 있음을 나타냅니다.
ssh	어플라이언스로 향하는 SSH(Secure Shell) 연결을 나타냅니다.
sudo	관리자가 아닌 사용자가 실행 파일을 실행할 수 있는 sudo 프로세스를 나타냅니다.
top	상위 CPU 프로세스에 대한 정보를 표시하는 유틸리티입니다.

실행 파일	설명
touch	지정된 파일의 액세스 및 변경 횟수를 변경하는 데 사용할 수 있는 유틸리티입니다.
vim	텍스트 파일을 수정하는 데 사용하는 유틸리티입니다.
wc	지정된 파일에서 회선, 단어 및 바이트 계산을 수행하는 유틸리티입니다.

관련 항목

액세스 목록 구성, 1370 페이지

The SFDataCorrelator 프로세스 통계 섹션

Firepower Management Center에서 현재 날짜까지의 Data Correlator 및 네트워크 검색 프로세스에 대한 통계를 볼 수 있습니다. 관리되는 디바이스가 데이터 수집, 디코딩 및 분석을 수행하는 동안 네트워크 검색 프로세스는 데이터를 지문 및 취약성 데이터베이스와 상호 연결한 다음, Firepower Management Center에서 실행되는 Data Correlator에 의해 처리되는 이진 파일을 생성합니다. The Data Correlator는 이진 파일의 정보를 분석하고 이벤트를 생성하고 네트워크 맵을 만듭니다.

네트워크 검색 및 Data Correlator에 표시되는 통계는 현재 날짜의 평균으로 오전 12:00부터 오후 11:59 사이에 각 기기에서 수집된 통계가 사용됩니다.

다음 테이블은 Data Correlator 프로세스에 표시되는 통계에 대해 설명합니다.

표 ***39: Data Correlator*** 프로세스 통계

카테고리	설명
이벤트/초	Data Correlator에서 초당 수신하여 처리하는 검색 이벤트의 수
연결/초	Data Correlator에서 초당 수신하여 처리하는 연결의 수
CPU 사용량 — 사용자(%)	현재 날짜에 대해 사용자 프로세스에 소비되는 평균 CPU 시간의 비율
CPU 사용량 — 시스템(%)	현재 날짜에 대해 시스템 프로세스에 소비되는 평균 CPU 시간의 비율
VmSize(KB)	현재 날짜에 대해 Data Correlator에 할당된 평균 메모리의 크기(킬로바이트 단위)
VmRSS	현재 날짜에 대해 Data Correlator에서 사용하는 평균 메모리의 양(킬로바이트 단위)

침입 이벤트 정보 섹션

Firepower Management Center 및 관리되는 디바이스의 통계 페이지에서 침입 이벤트에 대한 요약 정보를 볼 수 있습니다. 이 정보에는 마지막 침입 이벤트 날짜 및 시간, 이전 시간 및 날짜에 발생한 총 이벤트 수, 데이터베이스의 총 이벤트 수가 포함됩니다.

참고 통계 페이지 내 침입 이벤트 정보 섹션의 정보는 Firepower Management Center에 전송된 침입 이벤트가 아니라 관리되는 디바이스에 저장된 침입 이벤트를 기반으로 합니다. 만약 관리되는 디바이스가 로컬에서 침입 이벤트를 저장할 수 없는 (또는 저장하지 않도록 설정된) 경우 이 페이지에 침입 이벤트가 표시되지 않습니다.

다음 테이블은 통계 페이지의 침입 이벤트 정보 섹션에 표시되는 통계에 대해 설명합니다.

표 ***40:*** 침입 이벤트 정보

통계	설명
최근 경보	마지막 이벤트가 발생한 날짜 및 시간을 나타냅니다.
최근 1시간의 전체 이벤트	최근 1시간 동안 발생한 전체 이벤트 수를 나타냅니다.
최근 1일의 전체 이벤트	지난 24시간 동안 발생한 전체 이벤트 수를 나타냅니다.
데이터베이스의 전체 이벤트	이벤트 데이터베이스에 있는 전체 이벤트 수를 나타냅니다.

시스템 통계 보기

Firepower Management Center 및 관련 매니지드 디바이스에 대한 통계도 표시됩니다.

Firepower Management Center의 웹 인터페이스는 관리하는 FMC 및 디바이스에 대한 통계를 표시합니다. 7000 및 8000 Series 디바이스의 경우 시스템은 해당 디바이스에만 통계를 표시합니다.

시작하기 전에

시스템 통계를 보려면 관리자 또는 유지 보수 사용자여야 하며 전역 도메인에 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Monitoring(**모니터링**)** > **Statistics(**통계**)**를 선택합니다.

단계 **2** (FMC에만 해당) **Select Device(s)(**디바이스 선택**)** 목록에서 디바이스를 선택하고 **Select Devices(**디바이스 선택**)**을 클릭합니다.

단계 **3** 사용 가능한 통계를 봅니다.

단계 **4** 디스크 사용량 섹션에서 다음을 수행할 수 있습니다.

- 다음을 보려면 **By Category(**카테고리별로**)** 누적 막대의 디스크 사용량 카테고리 위에 포인터를 올려 놓습니다. (순서대로)
  - 해당 카테고리에 사용된 사용 가능한 디스크 공간의 백분율
  - 디스크의 실제 저장 공간
  - 해당 카테고리에 사용 가능한 모든 디스크 공간
- **By Partiion(**파티션별**)** 옆의 아래로 화살표를 클릭하여 확대합니다. 악성코드 스토리지 팩을 설치했다면 `/var/storage` 파티션 사용량이 표시됩니다.

단계 **5** (선택 사항) 프로세스 상태 필드, 432 페이지에 설명된 정보를 보려면 **Processes(**프로세스**)** 옆의 화살표를 클릭합니다.

시스템 메시지

Firepower System에서 발생한 문제를 추적하려면 메시지 센터에서 조사를 시작하십시오. 이 기능을 사용하면 Firepower System에서 지속적으로 생성하는 시스템 활동 및 상태에 대한 메시지를 볼 수 있습니다.

메시지 센터를 열려면 메인 메뉴의 Deploy(구축) 메뉴 옆에 있는 시스템 상태 아이콘을 클릭합니다. 이 아이콘은 시스템 상태에 따라 다음 중 하나의 형태를 취합니다.

- **Indicates One or More Errors(**오류가 하나 이상임을 표시**)** — 시스템에 하나 이상의 오류 및 경고가 발생했음을 나타냅니다.
- **Indicates One or More Warnings(**경고가 하나 이상임을 표시**)** — 시스템에 오류 없이 하나 이상의 경고가 발생했음을 나타냅니다.
- **Indicates No Warnings(**경고 없음 표시**)** — 시스템에 발생한 오류 및 경고가 없음을 나타냅니다.

아이콘에 표시된 숫자는 전체 오류 및 경고 메시지의 수를 나타냅니다.

메시지 센터를 닫으려면 Firepower System 웹 인터페이스에서 메시지 센터의 범위를 벗어난 아무 곳이나 클릭합니다.

메시지 센터 외에도 웹 인터페이스는 사용자 활동 및 현재 진행 중인 시스템 활동에 대해 즉시 팝업 알림을 표시합니다. 일부 팝업 알림은 5초 후 자동으로 사라지지만 "스티커" 알림은 해제 (✕)을 클릭해 취소하기 전까지 표시됩니다. 모든 알림을 취소하려면 알림 목록 상단의 취소 링크를 클릭합니다.

팁 비 스티커 팝업 알림 위에 커서를 올려 놓으면 알림이 고정됩니다.

시스템은 라이선스, 도메인, 액세스 역할에 따라 사용자에게 팝업 알림과 메시지 센터 중 하나를 선택하여 메시지를 표시합니다.

메시지 유형

메시지 센터의 시스템 활동 및 상태를 보고하는 메시지는 세 가지 탭으로 구성됩니다.

구축

이 탭에는 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 설정 구축과 관련된 현재 상태가 표시됩니다. 이 탭에서 Firepower System은 다음 구축 상태 값을 보고합니다.

- 실행 중(회전 중인) - 설정이 구축 중입니다.
- 성공 - 설정이 성공적으로 구축되었습니다.
- 경고( ) - 경고 구축 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 실패 - 설정 구축에 실패했습니다. 만료된 정책, 516 페이지의 내용을 참조하시기 바랍니다. 구축 실패는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

상태

이 탭은 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 현재 상태 정보가 표시됩니다. 상태는 상태 모니터링 정보, 387 페이지에서 설명한 상태 모듈에 의해 생성됩니다. 이 탭에서 Firepower System은 다음 상태 값을 보고합니다.

- 경고( ) - 어플라이언스의 상태 모듈에 대한 경고 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 노란색 삼각형( )을 사용하여 이 상태를 표시합니다. 경고 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 중요( ) - 어플라이언스의 상태 모듈에 대한 위험 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 중요( ) 아이콘을 사용하여 이 상태를 표시합니다. 위험 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 오류( ) - 어플라이언스에서 상태 모니터링 모듈의 오류가 발생했으며 오류 발생 이후 성공적으로 다시 실행되지 않았음을 나타냅니다. 상태 모니터링 페이지는 오류 아이콘을 사용하여 이 상태를 표시합니다. 오류 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

상태 모니터링 페이지에서 관련 상세정보를 보려면 상태 탭의 링크를 클릭하십시오. 현재 상태 조건이 없는 경우 상태 탭은 메시지를 표시하지 않습니다.

작업

Firepower System에서 일부 작업(구성 백업 또는 업데이트 설치)을 완료하는 데 시간이 걸릴 수 있습니다. 이 탭은 이러한 장기 작업 및 사용자 또는 적절한 액세스가 가능한 시스템의 다른 사용자가 시작한 작업 상태를 표시합니다. 이 탭은 각 메시지의 최신 업데이트를 기준으로 시간 반대순으로 메시지를 표시합니다. 일부 작업 상태 메시지는 문제의 작업에 대한 자세한 정보를 안내하는 링크를 포함합니다. 이 탭에서 Firepower System은 다음 작업 상태 값을 보고합니다.

- 대기() - 실행 중인 다른 작업이 완료될 때까지 작업이 실행 대기 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 실행 중 - 작업이 실행 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 재시도() - 작업이 자동으로 재시도함을 나타냅니다. 모든 작업의 재시도가 허용되는 것은 아니라는 점에 유의하십시오. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 성공() - 작업이 성공적으로 완료됨을 나타냅니다.
- 실패() - 작업이 성공적으로 완료되지 않음을 나타냅니다. 오류 작업은 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 중단 또는 정지() - 작업이 시스템 업데이트 때문에 중단됨을 나타냅니다. 중단된 작업은 다시 시작할 수 없습니다. 정상 작업이 복구되면 작업을 다시 시작합니다.
- 건너뜀 - 진행 중인 프로세스 때문에 작업을 시작할 수 없었습니다. 다시 시도해 작업을 시작하십시오.

새 작업이 시작되면 이 탭에 새 메시지가 표시됩니다. 작업이 완료(상태 성공, 실패, 중단)되면 이 탭은 사용자가 제거할 때까지 최종 상태 메시지를 표시합니다. 작업 탭 및 메시지 데이터베이스가 불필요하게 복잡해지지 않도록 메시지를 제거하는 것이 좋습니다.

메시지 관리

메시지 센터에서 다음을 수행할 수 있습니다.

- 팝업 알림 동작을 설정합니다(표시할 것인지 선택).
- 시스템 데이터베이스에서 추가 작업 상태 메시지를 표시합니다(제거되지 않아 사용 가능한 경우).
- 작업 상태 메시지를 하나씩 제거합니다. (제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)
- 작업 상태 메시지를 한꺼번에 제거합니다. (제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)

팁 데이터베이스 및 표시가 불필요하게 복잡해지지 않도록 작업 탭에서 누적된 작업 상태 메시지를 정기적으로 제거하는 것이 좋습니다. 데이터베이스의 메시지 수가 100,000개에 근접하면 시스템이 자동으로 제거한 작업 상태 메시지를 삭제합니다.

시스템 메시지 관리

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 구성 구축과 관련된 메시지를 보려면 배포를 클릭합니다. 구축 메시지 보기, 444 페이지의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 구성 구축 권한이 있어야합니다.
- Firepower Management Center 및 등록된 디바이스의 상태와 관련된 메시지를 보려면 상태를 클릭합니다. 상태 메시지 보기, 445 페이지의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.
- 장기 작업과 관련된 메시지를 보려면 작업를 클릭합니다. 작업 메시지 보기, 445 페이지 또는 작업 메시지 관리, 446 페이지를 참조하십시오. 누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.
- 팝업 알림 동작을 설정하려면 메시지 센터의 오른쪽 상단 모서리의 톱니바퀴( )를 클릭합니다. 알림 동작 설정, 446 페이지의 내용을 참조하십시오.

구축 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 컨피그레이션 구축 권한이 있어야합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Deployments(**구축**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- **total(**전체**)**을 클릭하여 모든 현재 구축 상태를 확인합니다.
- 특정 상태 값을 클릭하여 해당 구축 상태의 메시지만 확인합니다.

- 경과된 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **1m 5s(1**분 **5**초**)**)에서 구축의 경과된 시간과 시작 및 중지 시간을 확인합니다.

관련 항목

컨피그레이션 변경 사항 구축, 498 페이지

상태 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Health(**상태**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 모든 현재 상태를 확인하려면 **total(**전체**)**을 클릭합니다.
- 특정 상태 메시지만을 확인하려면 상태 메시지를 클릭합니다.
- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3**일 전**)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 특정 메시지에 대한 자세한 상태 정보를 보려면 메시지를 클릭합니다.
- 상태 모니터링 페이지에서 전체 상태를 보려면 상태 모니터를 클릭합니다.

관련 항목

상태 모니터링 정보, 387 페이지

작업 메시지 보기

누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Tasks(**작업**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- **total(**전체**)**을 클릭하여 모든 현재 작업 상태를 확인합니다.
- 특정 상태 값을 클릭하여 해당 상태의 작업에 대한 메시지만 확인합니다.

참고 중지된 작업에 대한 메시지는 작업 상태 메시지의 전체 목록에만 표시됩니다. 중지된 작업을 필터링할 수는 없습니다.

- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3**일 전**)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 메시지 내의 링크를 클릭하여 작업에 대한 자세한 정보를 확인합니다.
- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(**메시지 더 가져오기**)**를 클릭하여 해당 메시지를 검색합니다.

작업 메시지 관리

누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** Tasks(작업)를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(**메시지 더 가져오기**)**를 클릭하여 해당 메시지를 검색합니다.
- 완료된 작업(상태 중단, 성공, 실패)에 대한 단일 메시지를 제거하려면 메시지 옆의 제거( )를 클릭합니다.
- 모든 완료된 작업(상태 중간, 성공, 실패)에 대한 전체 메시지를 제거하려면 **Total(**전체**)**에서 메시지를 필터링하 고 **Remove all completed tasks(**모든 완료된 작업 제거**)**를 클릭합니다.
- 성공적으로 완료된 모든 작업에 대한 전체 메시지를 제거하려면 **Success(**성공**)** 메시지를 필터링하고 **Remove all completed tasks(**모든 성공적인 작업 제거**)**를 클릭합니다.
- 실패한 모든 작업에 대한 전체 메시지를 제거하려면 **Failure(**실패**)** 메시지를 필터링하고 **Remove all failed tasks(**모든 실패한 작업 제거**)**를 클릭합니다.

알림 동작 설정

참고 이 설정은 모든 팝업 알림에 영향을 주고 로그인 세션 동안 유지됩니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** 메시지 센터 오른쪽 상단 구석의 톱니바퀴( )를 클릭합니다.

단계 **3** 팝업 알림 표시를 활성화 또는 비활성화하려면 알림 표시 슬라이더를 클릭 합니다.

단계 **4** 슬라이더를 다시 숨기려면 톱니바퀴( )를 클릭합니다.

단계 **5** 메시지 센터를 닫으려면 시스템 상태를 다시 클릭합니다.

17 장

시스템 감사

다음 주제에서는 시스템에서의 활동을 감사하는 방법을 설명합니다.

- 시스템 로그, 449 페이지
- 시스템 감사 정보, 451 페이지

시스템 로그

시스템 로그(syslog) 페이지에서는 어플라이언스에 대한 시스템 로그 정보를 제공합니다.

시스템에서의 활동은 다음 두 가지 방법으로 감사할 수 있습니다. Firepower System에 속하는 어플라이언스는 사용자와 웹 인터페이스의 각 상호 작용에 대한 감사 기록을 생성하고 시스템 로그에 시스템 상태 메시지도 로깅합니다.

시스템 로그는 시스템에서 생성된 각 메시지를 표시합니다. 다음 항목이 순서대로 나열됩니다.

- 메시지가 생성된 날짜
- 메시지가 생성된 시간
- 메시지를 생성한 호스트
- 메시지 자체

시스템 로그 보기

시스템 로그 정보는 로컬입니다. 예를 들어 Firepower Management Center를 사용하여 매니지드 디바이스에서 시스템 로그의 시스템 상태 메시지를 볼 수 없습니다.

UNIX 파일 검색 유틸리티 Grep에서 허용되는 대부분의 구문을 사용하여 메시지를 필터링할 수 있습니다. 이에 따라 패턴 매칭에 Grep 호환 정규식을 사용할 수 있습니다.

시작하기 전에

시스템 통계를 보려면 관리자 또는 유지 보수 사용자여야 하며 전역 도메인에 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Monitoring(**모니터링**)** > **Syslog**을(를) 선택합니다.

단계 **2** 시스템 로그에서 특정 메시지 내용을 검색하려면

a) 시스템 로그 필터 구문, 450 페이지에 설명된 대로 필터 필드에 단어 또는 쿼리를 입력합니다.

Grep 호환 검색 구문만 지원됩니다.

예:

사용자 이름 "Admin"이 포함된 모든 로그 항목을 검색하려면 `Admin`을 사용합니다.

11월 27일에 생성된 모든 로그 항목을 검색하려면 `Nov[[:space:]]*27` 또는 `Nov.*27`을 사용합니다(하지만 `Nov 27` 또는 `Nov*27` 은 사용하지 마십시오).

11월 5일의 권한 부여 디버깅 정보를 포함하는 모든 로그 항목을 검색하려면 `Nov[[:space:]]*5.*AUTH.*DEBUG`를 사용합니다.

b) 검색에서 대소문자를 구분하려면 **Case-sensitive**를 선택합니다. (기본적으로 필터는 대소문자를 구분하지 않습니다.)

c) 입력한 기준을 충족하지 않는 모든 시스템 로그 메시지를 검색하려면 **Exclusion**을 선택합니다.

d) **Go(**이동**)**를 클릭합니다.

시스템 로그 필터 구문

다음 표에서는 System Log 필터에서 사용할 수 있는 정규식 구문을 보여줍니다.

표 ***41:*** 시스템 로그 필터 구문

구문 구성 요소	설명	예
.	문자나 공백과 일치	`Admi.`는 `Admin`, `AdmiN`, `Admi1`, `Admi&`와 일치
`[[:alpha:]]`	알파벳 문자와 일치	`[[:alpha:]]dmin`은 `Admin`, `bdmin`, `Cdmin`과 일치
`[[:upper:]]`	알파벳 대문자와 일치	`[[:upper:]]dmin`은 `Admin`, `Bdmin`, `Cdmin`과 일치
`[[:lower:]]`	알파벳 소문자와 일치	`[[:lower:]]dmin`은 `admin`, `bdmin`, `cdmin`과 일치
`[[:digit:]]`	숫자와 일치	`[[:digit:]]dmin`은 `0dmin`, `1dmin`, `2dmin`과 일치
`[[:alnum:]]`	영숫자 문자와 일치	`[[:alnum:]]dmin`은 `1dmin`, `admin`, `2dmin`, `bdmin`과 일치

구문 구성 요소	설명	예
`[[:space:]]`	탭을 포함한 공백과 일치	`Feb[[:space:]]29`는 2월 29일의 로그와 일치
*	앞에 오는 0개 이상의 문자 또는 식 인스턴스와 일치	`ab*`는 `a`, `ab`, `abb`, `ca`, `cab`, `cabb`과 일치 `[ab] *`는 모두 일치
?	0개 또는 1개 인스턴스와 일치	`ab?`는 `a` 또는 `ab`와 일치
\	일반적으로 정규식 구문으로 해석되는 문자에 대한 검색 허용	`alert\?`는 `alert?`와 일치

시스템 감사 정보

Firepower System에 속하는 어플라이언스는 사용자와 웹 인터페이스의 각 상호 작용에 대한 감사 레코드를 생성합니다.

관련 항목

Introduction to Reports(보고서 소개), 2653 페이지

감사 기록

Firepower Management Center 및 7000 및 8000 Series 디바이스는 사용자 활동에 대한 읽기 전용 감사 정보를 로깅합니다. 감사 로그는 감사 보기의 항목을 기준으로 감사 로그 메시지를 보고, 정렬하고, 필터링할 수 있는 표준 이벤트 보기에서 제공됩니다. 감사 정보를 손쉽게 삭제하고 보고할 수 있으며, 사용자가 변경한 내용에 대한 자세한 보고서를 볼 수 있습니다.

감사 로그에는 최대 100,000개의 항목이 저장됩니다. 감사 로그 항목 수가 100,000개를 초과하면 어플라이언스는 데이터베이스에서 가장 오래된 기록을 삭제하여 항목 수를 100,000개로 줄입니다.

참고 7000 또는 8000 Series 디바이스를 재부팅하고 가능한 한 빨리 보조 CLI에 로그인하는 경우, 로컬 웹 인터페이스를 사용할 수 있을 때까지는 실행하는 명령이 감사 로그에 기록되지 않습니다.

관련 항목

FMC에 대한 SSO 지침, 74 페이지

감사 레코드 보기

Firepower Management Center 또는 7000 및 8000 Series 디바이스에서 감사 레코드의 테이블을 볼 수 있습니다. 사전 정의된 감사 워크플로에는 이벤트의 단일 테이블 보기가 포함되어 있습니다. 찾고 있

는 정보에 따라 테이블 보기를 조작할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **System**(시스템) > **Monitoring**(모니터링) > **Audit**(감사)를 사용하여 감사 로그 워크플로에 액세스합니다.

단계 **2** 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다. 자세한 내용은 이벤트 시간 제약 조건, 2811 페이지를 참고하십시오.

참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 테이블의 열 내용을 자세히 알아보려면 시스템 로그, 449 페이지를 참조하십시오.
- 현재 워크플로 페이지에서 이벤트를 정렬하고 제한하려면 테이블 보기 페이지 사용, 2802 페이지를 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다. 자세한 내용은 워크플로 사용, 2793 페이지를 참고하십시오.
- 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용, 2801 페이지 섹션을 참조하십시오.
- 특정 값으로 제한하려면 행 내의 값을 클릭합니다. 드릴다운 페이지에서 값을 클릭하면 다음 페이지로 이동하며 해당 값으로 제한됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다. 자세한 내용은 이벤트 보기 제약 조건, 2818 페이지를 참조하십시오.

  팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

- 감사 레코드를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete**(삭제)를 클릭하거나 **Delete All**(모두 삭제)을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page**(이 페이지 즐겨찾기)를 클릭합니다. 자세한 내용은 북마크, 2822 페이지를 참고하십시오.
- 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks**(즐겨찾기 보기)를 클릭합니다. 자세한 내용은 북마크, 2822 페이지를 참고하십시오.
- 현재 보기의 데이터를 기반으로 보고서를 생성하려면 **Report Designer**(리포트 디자이너)를 클릭합니다. 자세한 내용은 이벤트 보기에서 보고서 템플릿 생성, 2657 페이지를 참고하십시오.

- 감사 로그에 기록된 변경의 요약을 보려면 **Message(**메시지**)** 열의 해당 이벤트 옆에 있는 **Compare(**비교**)**를 클릭합니다. 자세한 내용은 감사 로그를 사용하여 변경 검사, 454 페이지를 참고하십시오.

관련 항목

이벤트 보기 제약 조건, 2818 페이지

감사 로그 워크플로 필드

다음 표는 보고 검색할 수 있는 감사 로그 필드를 설명합니다.

표 *42:* 감사 로그 필드

필드	설명
시간	어플라이언스가 감사 레코드를 생성한 시간과 날짜.
User	감사 이벤트를 트리거한 사용자의 사용자 이름.
하위 시스템	감사 레코드를 생성하기 위해 사용자가 따른 전체 메뉴 경로. 예를 들어 **System(**시스템**)** > **Monitoring(**모니터링**)** > **Audit(**감사**)**는 감사 로그를 보기 위한 메뉴 경로입니다. 메뉴 경로와 관련이 없는 몇몇 경우에는 Subsystem(하위 시스템) 필드에 이벤트 유형만 표시됩니다. 예를 들어 **Login(**로그인**)**은 사용자 로그인 시도를 분류합니다.
Message	사용자가 수행한 작업 또는 사용자가 페이지에서 클릭한 버튼. 예를 들어 `Page View(페이지 보기)`는 단순히 사용자가 Subsystem(하위 시스템)에 표시된 페이지를 봤음을 의미하는 반면, `Save(저장)`는 사용자가 페이지에서 **Save(**저장**)** 버튼을 클릭했음을 의미합니다. Firepower System에 대한 변경 사항은 클릭하면 변경 사항 요약을 볼 수 있는 비교 아이콘과 함께 나타납니다.
Source IP(소스 IP)	사용자가 사용한 호스트와 연결된 IP 주소. 참고: 이 필드를 검색할 때는 특정 IP 주소를 입력해야 합니다. 로그 감사를 검색할 때는 IP 범위를 사용할 수 없습니다.

필드	설명
도메인	감사 이벤트가 트리거되었을 때 사용자의 현재 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
구성 변경 (검색만 해당)	검색 결과에서 구성 변경의 감사 레코드를 볼지 여부를 지정합니다. (`yes` 또는 `no`)
Count(개수)	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색, 2825 페이지

감사 이벤트 테이블 보기

이벤트 보기의 레이아웃을 변경하거나 보기의 이벤트를 필드 값으로 제한할 수 있습니다. 열을 비활성화할 때 나타나는 팝업 윈도우에서 숨기려는 컬럼 헤드의 닫기(✕)를 클릭한 다음 **Apply(적용)**를 클릭합니다. 비활성화한 열은 나중에 다시 추가하지 않는 한 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화하면 Count(카운트) 열이 추가됩니다.

다른 열을 숨기거나 표시하려면, 또는 비활성화된 열을 다시 보기에 추가하려면, 해당 확인란을 선택하거나 선택 취소한 후 **Apply(적용)**를 클릭하십시오.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되고 워크플로의 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

관련 항목

워크플로 사용, 2793 페이지

감사 로그를 사용하여 변경 검사

시스템 변경 사항에 대한 자세한 보고서를 보려면 감사 로그를 사용할 수 있습니다. 이러한 보고서는 시스템의 현재 구성을 특정 변경 이전의 최신 구성과 비교합니다.

Compare Configurations 페이지에는 차이점을 쉽게 파악할 수 있도록 변경 이전의 시스템 구성과 실행 중인 구성이 나란히 배치됩니다. 감사 이벤트 유형, 마지막 수정 시간 및 변경을 수행한 사용자의 이름이 각 구성 위의 제목 표시줄에 표시 됩니다.

두 구성의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 구성 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.

- 녹색은 강조 표시된 설정이 둘 중 한 구성에만 나타남을 의미합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Monitoring(**모니터링**)** > **Audit(**감사**)**을(를) 선택합니다.

단계 **2** **Message(**메시지**)** 열의 해당 감사 로그 이벤트 옆에 있는 **Compare(**비교**)**를 클릭합니다.

팁 제목 표시줄 위에 있는 **Previous(**이전**)** 또는 **Next(**다음**)**를 클릭하여 변경 사항을 개별적으로 탐색할 수 있습니다. 변경 요약의 길이가 한 페이지를 넘으면 오른쪽에 있는 스크롤바를 이용해 추가 변경 내용을 볼 수 있습니다.

감사 레코드 억제

감사 정책에서 Firepower System과의 특정 사용자 상호 작용 유형을 감사하도록 요구하지 않는 경우, 그러한 상호 작용이 Firepower Management Center 또는 7000 및 8000 Series 디바이스에서 감사 레코드를 생성하는 것을 차단할 수 있습니다. 예를 들어 기본적으로 사용자가 온라인 도움말을 볼 때마다 Firepower System은 감사 레코드를 생성합니다. 이러한 상호 작용 레코드를 유지할 필요가 없으면 자동으로 억제할 수 있습니다.

감사 이벤트 억제를 구성하려면 어플라이언스의 `admin` 사용자 계정에 대한 액세스 권한이 있어야 하며, 어플라이언스의 콘솔에 액세스하거나 SSH(Secure Shell)를 열 수 있어야 합니다.

주의 권한이 있는 사용자만 어플라이언스 및 `admin` 계정에 액세스할 수 있습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

`/etc/sf` 디렉터리에서 다음 형식으로 `AuditBlock` 파일을 생성합니다. 여기서 type은 감사 블록 유형, 456 페이지에 설명된 유형 중 하나입니다.

`AuditBlock.type`

참고 특정 유형의 감사 메시지에 대해 `AuditBlock.type` 파일을 생성한 후 억제를 해제하려는 경우 `AuditBlock.type` 파일의 내용을 삭제하되 파일 자체는 Firepower System에 남겨두어야 합니다.

감사 블록 유형

각 감사 블록 유형의 내용은 다음 표에 설명한 것처럼 특정 형식으로 지정해야 합니다. 파일 이름에 대/소문자를 정확하게 사용해야 합니다. 파일의 내용 역시 대/소문자를 구분합니다.

`AuditBlock` 파일을 추가하면 `Audit` 하위 시스템과 `Audit Filter type Changed` 메시지가 있는 감사 레코드가 감사 이벤트에 추가됩니다. 보안상의 이유로 이 감사 레코드는 억제할 수 없습니다.

표 ***43:*** 감사 블록 유형

유형	설명
주소	`AuditBlock.address` 파일을 생성하고, 감사 로그에서 억제하려는 각 IP 주소를 한 줄에 하나씩 포함합니다. 주소의 시작 부분부터 매핑되는 경우, 부분적인 IP 주소를 사용할 수 있습니다. 예를 들어 부분 주소 `10.1.1`은 `10.1.1.0~10.1.1.255` 범위의 주소와 일치합니다.
메시지	이름이 `AuditBlock.message`인 파일을 생성하고, 억제하려는 메시지 하위 문자열을 한 줄에 하나씩 포함합니다. 파일에 `backup`을 포함하면 `backup`이라는 단어가 포함된 모든 메시지가 억제되도록 하위 문자열이 매칭됩니다.
하위 시스템	이름이 `AuditBlock.subsystem`인 파일을 생성하고, 억제하려는 각 하위 시스템을 한 줄에 하나씩 포함합니다. 하위 문자열은 매칭되지 않습니다. 정확한 문자열을 사용해야 합니다. 감사 대상 하위 시스템 목록은 감사 하위 시스템, 457 페이지를 참조하십시오.
사용자	이름이 `AuditBlock.user`인 파일을 생성하고, 억제하려는 각 사용자 계정을 한 줄에 하나씩 포함합니다. 사용자 이름의 시작 부분부터 매핑되는 것이라면 부분적인 문자열 매칭을 사용할 수 있습니다. 예를 들어 부분적 사용자 이름 `IPSAnalyst`는 사용자 이름 `IPSAnalyst1` 및 `IPSAnalyst2`과 일치합니다.

감사 하위 시스템

다음 표에는 감사 대상 하위 시스템이 나열되어 있습니다.

표 ***44:*** 하위 시스템 이름

이름	포함되는 사용자 상호 작용
Admin(관리자)	시스템 및 액세스 구성, 시간 동기화, 백업 및 복원, 디바이스 관리, 사용자 계정 관리, 예약 등의 관리 기능
알림	이메일, SNMP, syslog 알림 등의 알림 기능
감사 로그	감사 이벤트 보기
감사 로그 검색	감사 이벤트 검색
명령행	명령줄 인터페이스
구성	이메일 알림
상황별로 크로스 실행	시스템에 추가되거나 대시보드 및 이벤트 보기에서 액세스한 외부 리소스
COOP	운영 연속성 기능
날짜	이벤트 보기의 날짜 및 시간 범위
기본 하위 시스템	할당된 하위 시스템이 없는 옵션
탐지 및 예방 정책	침입 정책에 대한 메뉴 옵션
오류	시스템 레벨 오류
eStreamer	eStreamer 구성
최종 사용자 라이선스 계약	최종 사용자 라이선스 계약 검토
이벤트	침입 및 검색 이벤트 보기
이벤트 클립보드	침입 이벤트 클립보드
검토된 이벤트	검토된 침입 이벤트
이벤트 검색	모든 이벤트 검색
규칙 업데이트 `rule_update_id` 설치 실패	규칙 업데이트 설치 중
헤더	사용자 로그인 후 유저 인터페이스의 초기 표시
상태	상태 모니터링

이름	포함되는 사용자 상호 작용
상태 이벤트	상태 모니터링 이벤트 보기
도움말	온라인 도움말
고가용성	고가용성 쌍에서 Firepower Management Center 설정 및 관리
IDS 영향 플래그	침입 이벤트에 대한 영향 플래그 구성
IDS 정책	침입 정책
IDSRule sid:`sig_id` rev:`rev_num`	SID 기준 침입 규칙
인시던트	침입 인시던트
설치	업데이트 설치
침입 이벤트	침입 이벤트
로그인	웹 인터페이스 로그인 및 로그 아웃 기능
메뉴	모든 메뉴 옵션
Configuration export > `config_type` > `config_name`	특정 유형 및 이름의 구성가져오기
권한 에스컬레이션	사용자 역할 에스컬레이션
선호	사용자 계정의 표준 시간대와 개별 이벤트 환경 설정 등의 사용자 환경 설정
정책	침입 정책을 비롯한 모든 정책
등록	다음에서 디바이스 등록: FMC
RemoteStorageDevice	원격 스토리지 디바이스 구성
보고서	보고서 나열 및 리포트 디자이너 기능
규칙	침입 규칙 편집기 및 규칙 가져오기 프로세스를 비롯한 침입 규칙
규칙 업데이트 가져오기 로그	규칙 업데이트 가져오기 로그 보기
규칙 업데이트 설치	규칙 업데이트 설치
상태	Syslog, 호스트 및 성능 통계
시스템	다양한 시스템 전체 설정
작업 대기열	백그라운드 프로세스 상태 보기

이름	포함되는 사용자 상호 작용
사용자	사용자 계정과 역할 생성 및 수정

18 장

시스템 문제 해결

다음 주제에서는 Firepower System에서 발생할 수 있는 문제를 진단하는 방법을 설명합니다.

- 문제 해결의 첫 번째 단계, 461 페이지
- 시스템 메시지, 462 페이지
- 기본 시스템 정보 보기, 464 페이지
- 시스템 메시지 관리, 465 페이지
- 상태 모니터 알림의 메모리 사용량 임계값, 468 페이지
- 이벤트 상태 모니터 알림의 디스크 사용량 및 소모, 469 페이지
- 문제 해결을 위한 상태 모니터 보고서, 473 페이지
- 일반 문제 해결, 475 페이지
- 연결 기반 문제 해결, 475 페이지
- Firepower Threat Defense 디바이스의 고급 문제 해결, 476 페이지
- 기능별 문제 해결, 477 페이지

문제 해결의 첫 번째 단계

- 문제 해결을 위해 변경을 수행하기 전에 원래 문제를 캡처하기 위한 문제 해결 파일을 생성합니다. 문제 해결을 위한 상태 모니터 보고서, 473 페이지 및 그 하위 섹션을 참조하십시오.

  Cisco TAC에 지원 문의를 하는 경우 이 문제 해결 파일이 필요한 경우가 있습니다.

- 메시지 센터에서 오류 및 경고 메시지를 확인하여 검사를 시작합니다. 시스템 메시지, 441 페이지의 내용을 참조하십시오.

- 제품의 제품 문서 중 "문제 해결 및 알림"에 수록된 관련 기술 노트 및 다른 문제 해결 자료를 참고하십시오. FMC 구축에 대한 최상위 문서 목록 페이지, 17 페이지의 내용을 참조하십시오.

시스템 메시지

Firepower System에서 발생한 문제를 추적하려면 메시지 센터에서 조사를 시작하십시오. 이 기능을 사용하면 Firepower System에서 지속적으로 생성하는 시스템 활동 및 상태에 대한 메시지를 볼 수 있습니다.

메시지 센터를 열려면 메인 메뉴의 Deploy(구축) 메뉴 옆에 있는 시스템 상태 아이콘을 클릭합니다. 이 아이콘은 시스템 상태에 따라 다음 중 하나의 형태를 취합니다.

- **Indicates One or More Errors(**오류가 하나 이상임을 표시**)** — 시스템에 하나 이상의 오류 및 경고가 발생했음을 나타냅니다.
- **Indicates One or More Warnings(**경고가 하나 이상임을 표시**)** — 시스템에 오류 없이 하나 이상의 경고가 발생했음을 나타냅니다.
- **Indicates No Warnings(**경고 없음 표시**)** — 시스템에 발생한 오류 및 경고가 없음을 나타냅니다.

아이콘에 표시된 숫자는 전체 오류 및 경고 메시지의 수를 나타냅니다.

메시지 센터를 닫으려면 Firepower System 웹 인터페이스에서 메시지 센터의 범위를 벗어난 아무 곳이나 클릭합니다.

메시지 센터 외에도 웹 인터페이스는 사용자 활동 및 현재 진행 중인 시스템 활동에 대해 즉시 팝업 알림을 표시합니다. 일부 팝업 알림은 5초 후 자동으로 사라지지만 "스티커" 알림은 해제 ( )을 클릭해 취소하기 전까지 표시됩니다. 모든 알림을 취소하려면 알림 목록 상단의 취소 링크를 클릭합니다.

팁 비 스티커 팝업 알림 위에 커서를 올려 놓으면 알림이 고정됩니다.

시스템은 라이선스, 도메인, 액세스 역할에 따라 사용자에게 팝업 알림과 메시지 센터 중 하나를 선택하여 메시지를 표시합니다.

메시지 유형

메시지 센터의 시스템 활동 및 상태를 보고하는 메시지는 세 가지 탭으로 구성됩니다.

구축

이 탭에는 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 설정 구축과 관련된 현재 상태가 표시됩니다. 이 탭에서 Firepower System은 다음 구축 상태 값을 보고합니다.

- 실행 중(회전 중인) - 설정이 구축 중입니다.
- 성공 - 설정이 성공적으로 구축되었습니다.
- 경고( ) - 경고 구축 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

- 실패 - 설정 구축에 실패했습니다. 만료된 정책, 516 페이지의 내용을 참조하시기 바랍니다. 구축 실패는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

상태

이 탭은 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 현재 상태 정보가 표시됩니다. 상태는 상태 모니터링 정보, 387 페이지에서 설명한 상태 모듈에 의해 생성됩니다. 이 탭에서 Firepower System은 다음 상태 값을 보고합니다.

- 경고( ) - 어플라이언스의 상태 모듈에 대한 경고 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 노란색 삼각형( )을 사용하여 이 상태를 표시합니다. 경고 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 중요( ) - 어플라이언스의 상태 모듈에 대한 위험 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 중요( ) 아이콘을 사용하여 이 상태를 표시합니다. 위험 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 오류( ) - 어플라이언스에서 상태 모니터링 모듈의 오류가 발생했으며 오류 발생 이후 성공적으로 다시 실행되지 않았음을 나타냅니다. 상태 모니터링 페이지는 오류 아이콘을 사용하여 이 상태를 표시합니다. 오류 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

상태 모니터링 페이지에서 관련 상세정보를 보려면 상태 탭의 링크를 클릭하십시오. 현재 상태 조건이 없는 경우 상태 탭은 메시지를 표시하지 않습니다.

작업

Firepower System에서 일부 작업(구성 백업 또는 업데이트 설치)을 완료하는 데 시간이 걸릴 수 있습니다. 이 탭은 이러한 장기 작업 및 사용자 또는 적절한 액세스가 가능한 시스템의 다른 사용자가 시작한 작업 상태를 표시합니다. 이 탭은 각 메시지의 최신 업데이트를 기준으로 시간 반대순으로 메시지를 표시합니다. 일부 작업 상태 메시지는 문제의 작업에 대한 자세한 정보를 안내하는 링크를 포함합니다. 이 탭에서 Firepower System은 다음 작업 상태 값을 보고합니다.

- 대기() - 실행 중인 다른 작업이 완료될 때까지 작업이 실행 대기 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 실행 중 - 작업이 실행 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 재시도() - 작업이 자동으로 재시도함을 나타냅니다. 모든 작업의 재시도가 허용되는 것은 아니라는 점에 유의하십시오. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 성공() - 작업이 성공적으로 완료됨을 나타냅니다.
- 실패() - 작업이 성공적으로 완료되지 않음을 나타냅니다. 오류 작업은 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

- 중단 또는 정지() - 작업이 시스템 업데이트 때문에 중단됨을 나타냅니다. 중단된 작업은 다시 시작할 수 없습니다. 정상 작업이 복구되면 작업을 다시 시작합니다.
- 건너뜀 - 진행 중인 프로세스 때문에 작업을 시작할 수 없었습니다. 다시 시도해 작업을 시작하십시오.

새 작업이 시작되면 이 탭에 새 메시지가 표시됩니다. 작업이 완료(상태 성공, 실패, 중단)되면 이 탭은 사용자가 제거할 때까지 최종 상태 메시지를 표시합니다. 작업 탭 및 메시지 데이터베이스가 불필요하게 복잡해지지 않도록 메시지를 제거하는 것이 좋습니다.

메시지 관리

메시지 센터에서 다음을 수행할 수 있습니다.

- 팝업 알림 동작을 설정합니다(표시할 것인지 선택).
- 시스템 데이터베이스에서 추가 작업 상태 메시지를 표시합니다(제거되지 않아 사용 가능한 경우).
- 작업 상태 메시지를 하나씩 제거합니다. (제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)
- 작업 상태 메시지를 한꺼번에 제거합니다. (제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)

팁 데이터베이스 및 표시가 불필요하게 복잡해지지 않도록 작업 탭에서 누적된 작업 상태 메시지를 정기적으로 제거하는 것이 좋습니다. 데이터베이스의 메시지 수가 100,000개에 근접하면 시스템이 자동으로 제거한 작업 상태 메시지를 삭제합니다.

기본 시스템 정보 보기

About(정보) 페이지에는 Firepower System의 모델, 일련 번호, 다양한 구성 요소에 대한 버전 정보 등 어플라이언스에 대한 정보가 표시됩니다. 또한 Cisco 저작권 정보도 포함되어 있습니다.

프로시저

단계 **1** 페이지 상단에 있는 툴바에서 **Help(**도움말**)**를 클릭합니다.

단계 **2** **About(**정보**)**를 선택합니다.

어플라이언스 정보 보기

프로시저

System(시스템**)** > **Configuration(**구성**)**을 선택합니다.

시스템 메시지 관리

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 구성 구축과 관련된 메시지를 보려면 배포를 클릭합니다. 구축 메시지 보기, 444 페이지의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 구성 구축 권한이 있어야합니다.
- Firepower Management Center 및 등록된 디바이스의 상태와 관련된 메시지를 보려면 상태를 클릭합니다. 상태 메시지 보기, 445 페이지의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.
- 장기 작업과 관련된 메시지를 보려면 작업를 클릭합니다. 작업 메시지 보기, 445 페이지 또는 작업 메시지 관리, 446 페이지를 참조하십시오. 누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.
- 팝업 알림 동작을 설정하려면 메시지 센터의 오른쪽 상단 모서리의 톱니바퀴( )를 클릭합니다. 알림 동작 설정, 446 페이지의 내용을 참조하십시오.

구축 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 컨피그레이션 구축 권한이 있어야합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Deployments(**구축**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- **total(**전체**)**을 클릭하여 모든 현재 구축 상태를 확인합니다.

- 특정 상태 값을 클릭하여 해당 구축 상태의 메시지만 확인합니다.
- 경과된 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **1m 5s(1**분 **5**초**)**)에서 구축의 경과된 시간과 시작 및 중지 시간을 확인합니다.

관련 항목

컨피그레이션 변경 사항 구축, 498 페이지

상태 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Health(**상태**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 모든 현재 상태를 확인하려면 **total(**전체**)**을 클릭합니다.
- 특정 상태 메시지만을 확인하려면 상태 메시지를 클릭합니다.
- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3**일 전**)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 특정 메시지에 대한 자세한 상태 정보를 보려면 메시지를 클릭합니다.
- 상태 모니터링 페이지에서 전체 상태를 보려면 상태 모니터를 클릭합니다.

관련 항목

상태 모니터링 정보, 387 페이지

작업 메시지 보기

누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Tasks(**작업**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- **total(**전체**)**을 클릭하여 모든 현재 작업 상태를 확인합니다.
- 특정 상태 값을 클릭하여 해당 상태의 작업에 대한 메시지만 확인합니다.

참고 중지된 작업에 대한 메시지는 작업 상태 메시지의 전체 목록에만 표시됩니다. 중지된 작업을 필터링할 수는 없습니다.

- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3**일 전**)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 메시지 내의 링크를 클릭하여 작업에 대한 자세한 정보를 확인합니다.
- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(**메시지 더 가져오기**)**를 클릭하여 해당 메시지를 검색합니다.

작업 메시지 관리

누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** Tasks(작업)를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(**메시지 더 가져오기**)**를 클릭하여 해당 메시지를 검색합니다.
- 완료된 작업(상태 중단, 성공, 실패)에 대한 단일 메시지를 제거하려면 메시지 옆의 제거( )를 클릭합니다.
- 모든 완료된 작업(상태 중간, 성공, 실패)에 대한 전체 메시지를 제거하려면 **Total(**전체**)**에서 메시지를 필터링하 고 **Remove all completed tasks(**모든 완료된 작업 제거**)**를 클릭합니다.
- 성공적으로 완료된 모든 작업에 대한 전체 메시지를 제거하려면 **Success(**성공**)** 메시지를 필터링하고 **Remove all completed tasks(**모든 성공적인 작업 제거**)**를 클릭합니다.
- 실패한 모든 작업에 대한 전체 메시지를 제거하려면 **Failure(**실패**)** 메시지를 필터링하고 **Remove all failed tasks(**모든 실패한 작업 제거**)**를 클릭합니다.

알림 동작 설정

참고 이 설정은 모든 팝업 알림에 영향을 주고 로그인 세션 동안 유지됩니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** 메시지 센터 오른쪽 상단 구석의 톱니바퀴( )를 클릭합니다.

단계 **3** 팝업 알림 표시를 활성화 또는 비활성화하려면 알림 표시 슬라이더를 클릭 합니다.

단계 **4** 슬라이더를 다시 숨기려면 톱니바퀴( )를 클릭합니다.

단계 **5** 메시지 센터를 닫으려면 시스템 상태를 다시 클릭합니다.

상태 모니터 알림의 메모리 사용량 임계값

Memory Usage 상태 모듈은 어플라이언스의 메모리 사용량을 모듈에 대해 설정된 제한과 비교하고, 사용량이 레벨을 초과하면 알림을 전송합니다. 모듈은 매니지드 디바이스 및 FMC 자체의 데이터를 모니터링합니다.

메모리 사용에 대해 설정 가능한 두 가지 임계값인 Critical(심각) 및 Warning(경고)을 사용된 메모리의 백분율로 설정할 수 있습니다. 이러한 임계값을 초과하면 심각도 레벨이 지정된 상태 알람이 생성됩니다. 그러나 상태 경보 시스템은 이러한 임계 값을 정확한 방식으로 계산하지 않습니다.

높은 메모리 디바이스를 사용하는 경우 특정 프로세스에서는 낮은 메모리 공간 디바이스에서보다 전체 시스템 메모리의 비율이 더 많이 사용됩니다. 이 설계에서는 보조 프로세스에 사용할 수있는 작은 메모리 값을 남겨 두면서 최대한 많은 물리적 메모리를 사용합니다.

두 개의 디바이스(하나는 32GB 메모리, 다른 하나는 4GB 메모리)를 비교합니다. 32GB의 메모리가 있는 디바이스에서 메모리의 5%(1.6GB)는 4GB의 메모리가 있는 디바이스(4GB의 5% = 200MB)보다 보조 프로세스에서 남겨야 할 메모리 값이 훨씬 더 큽니다.

특정 프로세스에서 시스템 메모리를 더 많이 사용하는 비율을 고려하기 위해 FMC는 총 물리적 메모리와 총 스왑 메모리를 모두 포함하도록 총 메모리를 계산합니다. 따라서 사용자가 설정한 임계값 입력에 대해 시행된 메모리 임계값은 이벤트의 "Value(값)" 열이 초과된 임계값을 결정하기 위해 입력한 값과 일치하지 않는 상태 이벤트를 초래할 수 있습니다.

다음 표에는 설치된 시스템 메모리에 따라 사용자 입력 임계값 및 시행 된 임계값의 예가 나와 있습니다.

참고 이 표의 값은 예시입니다. 이 정보를 사용하여 여기에 표시된 설치된 RAM과 일치하지 않는 디바이스에 대한 임계값을 추정할 수 있습니다. 또는 더 정확한 임계값 계산을 위해 Cisco TAC에 문의할 수 있습니다.

표 ***45:*** 설치된 ***RAM*** 기반 메모리 사용량 임계값

사용자 입력 임계값	설치된 메모리당 시행된 임계값**(RAM)**			
	4GB	**6 GB**	**32GB**	**48GB**
10%	10%	34%	72%	81%
20%	20%	41%	75%	83%
30%	30%	48%	78%	85%
40%	40%	56%	81%	88%
50%	50%	63%	84%	90%
60%	60%	70%	88%	92%
70%	70%	78%	91%	94%
80%	80%	85%	94%	96%
90%	90%	93%	97%	98%
100%	100%	100%	100%	100%

이벤트 상태 모니터 알림의 디스크 사용량 및 소모

디스크 사용량 상태 모듈은 매니지드 디바이스의 하드 드라이브 및 악성코드 스토리지 팩의 디스크 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 비율을 초과하면 알림을 전송합니다. 또한 시스템이 모니터링되는 디스크 사용량 카테고리에서 과도하게 파일을 삭제하는 경우 또는 모듈 임계값을 기반으로 그러한 카테고리 외의 디스크 사용량이 과도한 수준에 도달하는 경우에도 알림을 전송합니다.

이 주제에서는 디스크 사용량 상태 모듈에서 생성되는 두 가지 상태 경고에 대한 증상 및 문제 해결 지침에 대해 설명합니다.

- 이벤트의 빈번한 드레인
- 처리되지 않은 이벤트의 드레인

디스크 관리자 프로세스는 디바이스의 디스크 사용량을 관리합니다. 디스크 관리자가 모니터링하는 각 파일 유형에는 사일로가 할당됩니다. 시스템에서 사용 가능한 디스크 공간의 양에 따라 디스크 관리자는 각 사일로에 대해 HWM(상위 워터마크) 및 LWM(하위 워터마크)을 계산합니다.

시스템의 각 부분(silo, LWM 및 HWM 등)에 대한 자세한 디스크 사용량 정보를 표시하려면 **show disk-manager** 명령을 사용합니다.

예

다음은 디스크 관리자 정보의 예입니다.

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

상태 알림 형식

FMC의 상태 모니터 프로세스가 실행되면(5분마다 또는 수동 실행이 트리거될 때) 디스크 사용량 모듈이 diskmanager.log 파일을 살펴보고 올바른 조건이 충족되면 해당 상태 알림이 트리거됩니다.

이러한 상태 알림의 구조는 다음과 같습니다.

- <사일로 이름>의 빈번한 드레인
- <사일로 이름>에서 처리되지 않은 이벤트의 드레인

예를 들면 다음과 같습니다.

- 낮은 우선순위 이벤트의 빈번한 드레인
- 낮은 우선순위 이벤트에서 처리되지 않은 이벤트의 드레인

사일로에서 <사일로 이름>의 빈번한 드레인 상태 알림을 생성할 수 있습니다. 그러나 이벤트와 관련된 알림이 가장 일반적으로 표시됩니다. 이벤트 사일로 중에는 이러한 유형의 이벤트가 디바이스에서 더욱 빈번하게 생성되므로 낮은 우선순위 이벤트가 자주 표시됩니다.

<사일로 이름>의 빈번한 드레인 이벤트는 이벤트가 FMC로 전송되도록 대기하기 때문에 이벤트 관련 사일로에 대해서 표시할 때 **Warning(**경고**)** 심각도 레벨을 갖습니다. 백업 사일로와 같이 이벤트와 관련이 없는 사일로의 경우, 이 정보가 손실되므로 경고의 심각도는 **Critical(**중대**)**입니다.

중요 이벤트 사일로만이 <사일로 이름> 에서 처리되지 않은 이벤트의 드레인 상태 알림을 생성합니다. 이 알림의 심각도 레벨은 항상 **Critical(**중대**)**입니다.

알림 외에 추가 증상은 다음과 같습니다.

- FMC 사용자 인터페이스의 속도 저하
- 이벤트 손실

일반적인 문제 해결 시나리오

<사일로 이름>의 빈번한 드레인 이벤트가 그 크기로 인해 사일로에 너무 많이 입력되어 발생합니다. 이 경우, 디스크 관리자는 마지막 5분 간격으로 해당 파일을 두 번 이상 비우거나 제거합니다. 이벤트 유형 사일로에서 이는 일반적으로 해당 이벤트 유형의 과도한 로깅으로 인해 발생합니다.

<사일로 이름>의 처리되지 않은 이벤트의 드레인 상태 알림의 경우, 이벤트 처리 경로의 병목 현상으로 인해 발생할 수도 있습니다.

이러한 디스크 사용량 알림과 관련하여 발생 가능한 세 가지 병목 현상이 있습니다.

- 과도한 로깅 - FTD의 EventHandler 프로세스가 초과 서브스크립션됩니다(Snort가 쓰는 것보다 느리게 읽음).
- Sftunnel 병목 현상 - Eventing 인터페이스가 불안정하거나 초과 서브스크립션됩니다.
- SFDataCorrelator 병목 현상 - FMC와 매니지드 디바이스 간의 데이터 전송 채널이 초과 서브스크립션됩니다.

과도한 로깅

이 유형의 상태 알림의 가장 일반적인 원인 중 하나는 과도한 입력입니다. **show disk-manager** 명령에서 수집한 LWM(하위 워터마크)과 HWM(상위 워터마크)의 차이점은 LWM(새로 드레인됨)에서 HWM 값으로 이동하기 위해 해당 사일로에서 사용할 수 있는 공간의 양을 나타냅니다. 처리되지 않은 이벤트의 유무에 관계없이 이벤트가 자주 비워지는 경우, 로깅 설정을 가장 먼저 검토해야 합니다.

- 이중 로깅 확인 - FMC에서 상관기 *perfstats*를 보면 이중 로깅 시나리오를 확인할 수 있습니다.

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- ACP에 대한 로깅 설정 확인 - ACP(Access Control Policy, 액세스 제어 정책)의 로깅 설정을 검토합니다. 연결의 "시작" 및 "종료"를 모두 로깅하는 경우, 시작을 기록할 때 포함된 모든 항목을 포함하고 이벤트의 양을 줄이므로 종료만 기록합니다.

  연결 로깅 모범 사례, 2868 페이지에 설명된 모범 사례를 따라야 합니다.

통신 병목 현상 **- Sftunnel**

sftunnel은 FMC와 매니지드 디바이스 간의 암호화된 통신을 담당합니다. 이벤트는 터널을 통해 FMC로 전송됩니다. 매니지드 디바이스와 FMC 간의 통신 채널(sftunnel)에서 연결 문제 및/또는 불안정은 다음과 같은 원인으로 발생할 수 있습니다.

- sftunnel이 다운되었거나 불안정합니다(플랩).

  FMC와 매니지드 디바이스가 TCP 포트 8305의 관리 인터페이스 간에 연결 가능한지 확인합니다.

  sftunnel 프로세스는 안정적이어야 하며 예기치 않게 재시작되지 않아야 합니다. **/var/log/message** 파일을 점검하여 이를 확인하고 ***sftunneld*** 문자열이 포함된 메시지를 검색합니다.

- sftunnel이 초과 서브스크립션되었습니다.

상태 모니터에서 추세 데이터를 검토하고 관리 트래픽이 급증하거나 지속적인 초과 서브스크립션이 될 수 있는 FMC 관리 인터페이스의 초과 서브스크립션 징후를 확인합니다.

Firepower 이벤트를 위한 보조 관리 인터페이스로 사용합니다. 이 인터페이스를 사용하려면 **configure network management-interface** 명령을 사용하여 FTD CLI에서 해당 IP 주소 및 기타 매개변수를 구성해야 합니다.

통신 병목 현상 - SFDataCorrelator

SFDataCorrelator는 FMC와 매니지드 디바이스 간의 데이터 전송을 관리합니다. FMC는 시스템에서 생성된 이진 파일을 분석하여 이벤트, 연결 데이터 및 네트워크 맵을 생성합니다. 첫 번째 단계는 **diskmanager.log** 파일에서 다음과 같이 수집할 중요한 정보를 검토하는 것입니다.

- 드레인의 빈도
- 처리되지 않은 이벤트가 드레인된 파일의 수
- 처리되지 않은 이벤트가 있는 드레인의 발생

디스크 관리자 프로세스가 실행될 때마다 **[/ngfw]/var/log/diskmanager.log**에 있는 자체 로그 파일에서 각기 다른 사일로에 대한 항목을 생성합니다. diskmanager.log에서 수집한 정보(CSV 형식)를 사용하면 원인을 찾는 범위를 좁힐 수 있습니다.

추가 문제 해결 단계:

- **stats_unified.pl** 명령을 사용하면 매니지드 디바이스에 FMC로 전송해야 하는 데이터가 있는지 확인할 수 있습니다. 이 상태는 매니지드 디바이스와 FMC에 연결 문제가 있을 때 발생할 수 있습니다. 매니지드 디바이스는 로그 데이터를 하드 드라이브에 저장합니다.

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- **manage_proc.pl** 명령은 FMC 측의 상관기를 재설정할 수 있습니다.

  ```
  root@FMC:~# manage_procs.pl
  ```

Cisco TAC(Technical Assistance Center)에 연락하기 전에

Cisco TAC에 연락하기 전에 다음 항목을 수집하는 것이 좋습니다.

- 표시되는 상태 알림의 스크린샷
- FMC에서 생성된 문제 해결 파일
- 영향을 받는 매니지드 디바이스에서 생성된 문제 해결 파일

  문제가 처음 확인된 날짜 및 시간

- 정책에 적용된 최근 변경 사항에 대한 정보(해당되는 경우)

  통신 병목 현상 - SFDataCorrelator, 472 페이지에 설명된 stats_unified.pl 명령의 출력

문제 해결을 위한 상태 모니터 보고서

경우에 따라 어플라이언스에 문제가 발생하면 support(지원팀)가 문제 진단에 도움이 될 수 있도록 문제 해결 파일을 생성하도록 요청할 수 있습니다. 아래 표에 나열된 옵션 중 하나를 선택하여 상태 모니터가 보고하는 문제 해결 데이터를 맞춤화할 수 있습니다.

일부 옵션은 보고하는 데이터의 측면에서 겹치지만, 문제 해결 파일은 선택하는 옵션에 관계없이 중복된 사본을 포함하지 않는다는 점에 유의하십시오.

표 ***46:*** 선택 가능한 문제 해결 옵션

옵션	보고 내용
Snort 성능 및 구성	어플라이언스의 Snort에 관련된 데이터 및 구성 설정
하드웨어 성능 및 로그	어플라이언스 하드웨어의 성능에 관련된 데이터 및 로그
시스템 구성, 정책 및 로그	어플라이언스의 현재 시스템 구성에 관련된 구성 설정, 데이터 및 로그
탐지 구성, 정책 및 로그	어플라이언스의 탐지에 관련된 구성 설정, 데이터 및 로그
인터페이스 및 네트워크 관련 데이터	어플라이언스의 인라인 집합 및 네트워크 구성에 관련된 구성 설정, 데이터 및 로그
검색, 인식, VDB 데이터 및 로그	어플라이언스의 현재 검색 및 인식 구성에 관련된 구성 설정, 데이터 및 로그
데이터 및 로그 업그레이드	어플라이언스의 이전 업그레이드와 관련된 데이터 및 로그
모든 데이터베이스 데이터	문제 해결 보고서에 포함된 모든 데이터베이스 관련 데이터
모든 로그 데이터	어플라이언스 데이터베이스에 의해 수집된 모든 로그
네트워크 맵 정보	현재 네트워크 토폴로지 데이터

특정 시스템 기능에 대한 문제 해결 파일 생성

지원 시 전송할 수 있는 맞춤 문제 해결 파일을 생성 및 다운로드할 수 있습니다.

다중 도메인을 구축한 경우, 하위 도메인의 디바이스에서 문제 해결 파일을 생성하고 다운로드할 수 있습니다.

주의 메모리가 적은 디바이스에서 문제 해결 파일을 생성하는 경우 자동 애플리케이션 우회(AAB)가 활성화되어 있는 경우 AAB가 발생할 수 있습니다. 적어도 AAB가 작동하면 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. 일부 경우에는 AAB가 작동하여 디바이스가 일시적으로 동작하지 않을 수 있습니다. 만약 동작 정지 상태가 지속되면 Cisco TAC(Technical Assistance Center)에 문의할 경우 구축 시 적절한 솔루션을 제시할 것입니다. 영향을 받기 쉬운 디바이스에는 Firepower 7010, 7020 및 7030, 5508-X, 5516-X NGIPSv가 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 유지 보수, 보안 분석가 또는 보안 분석가(읽기 전용) 사용자여야 합니다.

프로시저

단계 **1** 디바이스 상태 모니터 보기, 410 페이지의 단계를 수행합니다.

단계 **2** **Generate Troubleshooting Files(**문제 해결 파일 생성**)**를 클릭합니다.

단계 **3** 모든 생성 가능한 문제 해결 날짜의 파일을 생성하려면 모든 데이터를 선택하거나 작업 메시지 보기, 445 페이지의 설명에 따라 개별 상자를 체크합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** Message Center에서 작업 메시지를 확인하려면 작업 메시지 보기, 445 페이지를 참고하십시오.

단계 **6** 사용자가 생성한 문제 해결 파일에 해당하는 작업을 찾습니다.

단계 **7** 어플라이언스가 문제 해결 파일을 생성하고 작업 상태가 `Completed(완료)`로 변경된 후 **Click to retrieve generated files(**생성된 파일을 검색하려면 클릭**)**를 클릭합니다.

단계 **8** 파일을 다운로드하려면 브라우저의 프롬프트를 따릅니다. (문제 해결 파일은 단일 `.tar.gz` 파일에 다운로드 됩니다.)

단계 **9** Cisco에 문제 해결 파일을 보내려면 Support(지원팀)의 지시에 따르십시오.

고급 문제 해결 파일 다운로드

다중 도메인을 구축한 경우, 하위 도메인의 디바이스에서 문제 해결 파일을 생성하고 다운로드할 수 있습니다. 파일의 다운로드는 글로벌 도메인의 Firepower Management Center에서만 할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 유지 보수, 보안 분석가 또는 보안 분석가(읽기 전용) 사용자여야 합니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 보려면 디바이스 상태 모니터 보기, 410 페이지을 참고하십시오.

단계 **2** **Advanced Troubleshooting(**고급 문제 해결**)**을 클릭하십시오.

단계 **3** **File Download(**파일 다운로드**)**에서 지원팀이 제공한 파일 이름을 입력합니다.

단계 **4** **Download(**다운로드**)**를 클릭합니다.

단계 **5** 파일을 다운로드하려면 브라우저의 프롬프트를 따릅니다.

참고 매니지드 디바이스의 경우, 시스템 이름 앞에 장치 이름을 추가하여 파일의 이름을 바꿉니다.

단계 **6** Cisco에 문제 해결 파일을 보내려면 Support(지원팀)의 지시에 따르십시오.

일반 문제 해결

내부 전원 장애(하드웨어 장애, 전원 서지) 또는 외부 전원 장애(플러그 뽑힘)로 인해 예기치 않은 시스템 셧다운 또는 재부팅이 발생할 수 있습니다. 이러한 경우 결국 데이터 손상이 발생할 수 있습니다.

연결 기반 문제 해결

연결 기반 문제 해결 또는 디버깅은 특정 연결에 대한 적절한 로그를 수집하기 위해 모듈에 균일한 디버깅을 제공합니다. 또한 최대 레벨 7까지 레벨 기반 디버깅을 지원하고 액세스 모듈에 대한 균일한 로그 수집 메커니즘을 활성화합니다. 연결 기반 디버깅은 다음을 지원합니다.

- Firepower Threat Defense에서 문제를 해결하는 공통 연결 기반 디버깅 하위 시스템
- 모듈에서 일관된 디버그 메시지 형식
- 재부팅에서 지속적인 디버그 메시지
- 모듈에서 기존 연결 기반 엔드 투 엔드 디버깅
- 진행 중인 연결 디버깅

참고 연결 기반 디버깅은 Firepower 2100 시리즈 디바이스에서는 지원되지 않습니다.

문제 해결 연결에 대한 자세한 내용은 연결 문제 해결 , 476 페이지를 참조하십시오.

연결 문제 해결

프로시저

단계 **1** **debug packet-condition** 명령을 사용하여 연결을 식별하는 필터를 구성합니다.

예:

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

단계 **2** 관심 있는 모듈 및 해당 레벨에 대한 디버그를 활성화합니다. **debug packet** 명령을 사용합니다.

예:

```
Debug packet acl 5
```

단계 **3** 다음 명령을 사용하여 패킷 디버깅을 시작합니다.

```
debug packet-start
```

단계 **4** 다음 명령을 사용하여 데이터베이스에서 디버그 메시지를 가져오고 디버그 메시지를 분석합니다.

```
show packet-debugs
```

단계 **5** 다음 명령을 사용하여 패킷 디버깅을 중지합니다.

```
debug packet-stop
```

Firepower Threat Defense 디바이스의 고급 문제 해결

Firepower Threat Defense 디바이스의 자세한 문제 해결 분석을 수행하기 위해 패킷 트레이서 및 패킷 캡처 기능을 사용할 수 있습니다. 패킷 트레이서는 방화벽 관리자가 가상 패킷을 보안 어플라이언스에 삽입하고 인그레스에서 이그레스로의 흐름을 추적하도록 합니다. 그 과정에서 패킷은 흐름 및 경로 조회, ACL, 프로토콜 검사, NAT, 침입 탐지에 대해 평가됩니다. 유틸리티 전원은 프로토콜 및 포트 정보로 소스 및 대상 주소를 지정하여 실제 트래픽을 시뮬레이션하는 기능에서 가져옵니다. 패킷 캡처는 패킷의 성공 실패 판정을 제공하는 추적 옵션을 통해 사용 가능합니다.

문제 해결 파일에 대한 자세한 내용은 고급 문제 해결 파일 다운로드, 474 페이지의 내용을 참조하십시오.

웹 인터페이스에서 FTD CLI 사용

Firepower Management Center 웹 인터페이스에서 선택한 FTD 명령줄 인터페이스(CLI)를 실행할 수 있습니다. 이러한 명령은 **ping**, **packet-tracer**, **traceroute** 및 **show**(**show history** 및 **show banner** 제외)입니다.

다중 도메인 구축 시 하위 도메인에서 관리되는 디바이스를 위한 Firepower Management Center 웹 인터페이스를 통해 FTD CLI 명령을 입력할 수 있습니다.

참고 Firepower Management Center의 고가용성을 활용한 배포의 경우 이 기능은 활성화된 Firepower Management Center에서만 사용할 수 있습니다.

FTD CLI에 대한 자세한 정보는, *Firepower Threat Defense*용 명령 참조 가이드를 참조하십시오.

시작하기 전에

CLI를 사용하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 보려면 디바이스 상태 모니터 보기, 410 페이지을 참고하십시오.
단계 **2** **Advanced Troubleshooting(**고급 문제 해결**)**을 클릭하십시오.
단계 **3** **Threat Defense CLI(**위협 방어 **CLI)**를 클릭합니다.
단계 **4** **Command(**명령**)** 드롭다운 목록에서 명령을 선택합니다.
단계 **5** 선택 사항으로 매개 변수 텍스트 상자에 명령 매개 변수를 입력할 수도 있습니다.
단계 **6** 명령 출력을 보려면 **Execute(**실행**)**를 클릭합니다.

기능별 문제 해결

기능 관련 문제 해결 팁과 기술은 다음 표를 참조하십시오.

표 ***47:*** 기능 관련 문제 해결 주제

기능	관련 문제 해결 정보
애플리케이션 제어	애플리케이션 제어 규칙 문제 해결, 544 페이지
LDAP 외부 인증	LDAP 인증 연결 문제 해결 LDAP 인증 연결 문제 해결, 132 페이지
라이선싱	FTD 라이선싱 문제 해결 특정 라이선스 예약 문제 해결
FMC 고가용성	Firepower Management Center 고가용성 문제 해결, 280 페이지
7000 및 8000 Series 디바이스 고가용성 상태 공유	문제 해결을 위한 디바이스 고가용성 상태 공유 통계

기능	관련 문제 해결 정보
사용자 규칙 조건	사용자 제어 문제 해결, 549 페이지
사용자 ID 소스	ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결, 2500 페이지 캡티브 포털(captive portal) ID 소스 문제 해결, 2518 페이지 원격 액세스 VPN ID 소스 문제 해결, 2523 페이지 LDAP 인증 연결 문제 해결 LDAP 인증 연결 문제 해결, 132 페이지
영역 및 사용자 데이터 다운로드	영역 및 사용자 다운로드 문제 해결, 2480 페이지
네트워크 검색	네트워크 검색 전략 문제 해결, 2560 페이지
SSL 규칙	TLS/SSL 규칙 문제 해결, 1851 페이지
Firepower Threat Defense syslog	시스템 로그 구성 관련 정보, 1445 페이지
침입 성능 통계	침입 성능 통계 로깅 구성, 2196 페이지
7000 및 8000 Series NGIPSv ASA 및 FirePOWER Services	generate-troubleshoot, 3168 페이지 (명령줄 인터페이스(CLI)의 명령)
연결 기반 문제 해결	연결 기반 문제 해결, 475 페이지

IV 부

구축 관리

- 도메인 관리, 481 페이지
- 정책 관리, 491 페이지
- 규칙 관리: 일반 특성, 523 페이지
- 재사용 가능 개체, 557 페이지
- Firepower Threat Defense 인증서 기반 인증, 675 페이지

19 장

도메인 관리

다음 주제는 도메인을 사용해 멀티 테넌시를 관리하는 방법을 설명합니다.

- 도메인을 사용하는 다중 테넌시 소개, 481 페이지
- 도메인 요구 사항 및 사전 요건, 485 페이지
- 도메인 관리, 485 페이지
- 새 도메인 생성, 486 페이지
- 도메인 간 데이터 이동, 487 페이지
- 도메인 간 디바이스 이동, 487 페이지
- 도메인 관리 기록, 489 페이지

도메인을 사용하는 다중 테넌시 소개

Firepower System을 사용 하면 도메인을 사용 하는 멀티 테 넌 시를 구현할 수 있습니다. 도메인에 따라 매니지드 디바이스, 구성 및 이벤트에 대한 사용자 액세스가 구분됩니다. 최고 수준 글로벌 도메인에 2~3개의 레벨로 최대 100개의 하위 도메인을 생성할 수 있습니다.

Firepower Management Center에 로그인하는 경우, *current domain(*현재 도메인*)*이라고 하는 단일 도메인에 로그인합니다. 사용자 어카운트에 따라 다른 도메인으로 전환할 수 있습니다.

사용자 역할에 의해 부과된 제한 외에도 현재 도메인 레벨이 다양한 Firepower System 구성을 수정할 수 있는 기능을 제한할 수 있습니다. 시스템은 시스템 소프트웨어 업데이트와 같은 대부분의 관리 작업을 전역 도메인으로 제한합니다.

시스템은 다른 작업을 하위 도메인이 없는 리프 도메인으로 제한합니다. 예를 들어 각 매니지드 디비아스를 리프 도메인과 연결하고 해당 리프 도메인의 컨텍스트에서 디바이스 관리 작업을 수행해야 합니다.

각 리프 도메인은 해당 리프 도메인의 디바이스에서 수집한 검색 데이터를 기반으로 자체 네트워크 맵을 작성합니다. 매니지드 디바이스에서 보고한 이벤트(연결, 침입, 악성코드 등)도 디바이스의 리프 도메인에 연결됩니다.

도메인 레벨 **1:** 전역

멀티 테넌시를 구성하지 않는 경우, 모든 디바이스, 설정 및 이벤트가 전역 도메인에 속하며 이 시나리오에서는 리프 도메인이기도 합니다. 도메인 관리를 제외하고 시스템은 하위 도메인이 추가될 때까지 도메인별 구성 및 분석 옵션을 숨깁니다.

두 개의 도메인 레벨**:** 전역 및 **2**차 레벨

2단계 다중 도메인 구축에서 전역 도메인에는 직계 하위 도메인만 있습니다. 예를 들어 MSSP(매니지드 보안 서비스 제공자)는 여러 고객에 대한 네트워크 보안을 관리하기 위해 단일 Firepower Management Center를 사용할 수 있습니다.

- 전역 도메인에 로그인하는 MSSP 관리자는 고객의 구축을 보거나 편집할 수 없습니다. 고객의 구축을 관리하려면 각각 두 번째 수준의 명명된 하위 도메인에 로그인해야 합니다.
- 각 고객의 관리자는 두 번째 수준의 이름이 지정된 하위 도메인에 로그인하여 조직에 적용 가능한 디바이스, 구성 및 이벤트만 관리할 수 있습니다. 이런 로컬 관리자는 MSSP 내 다른 고객의 구축을 보거나 영향을 줄 수 없습니다.

세 개의 도메인 레벨**:** 전역**, 2**차 레벨 및 **3**차 레벨

3단계 다중 도메인 구축에서 전역 도메인에는 하위 도메인이 있으며, 그 중 적어도 하나가 자체 하위 도메인입니다. 앞의 예를 확장해, 이미 하위 도메인으로 제한되어 있는 MSSP 고객이 구축을 더욱 세분화하려는 시나리오를 생각해 보겠습니다. 이 고객은 디바이스 두 부류를 따로 관리하고자 합니다(네트워크 에지에 배치된 디바이스 및 내부에 배치된 디바이스).

- 두 번째 수준 하위 도메인에 로그인하는 고객의 관리자는 고객의 엣지 네트워크 구축을 보거나 편집할 수 없습니다. 네트워크 엣지에 구축된 디바이스를 관리하려면 해당 리프 도메인에 로그인해야 합니다.
- 고객의 엣지 네트워크 관리자는 세 번째 수준(리프) 도메인에 로그인하여 네트워크 엣지에 구축된 디바이스에 적용 가능한 디바이스, 구성 및 이벤트만 관리할 수 있습니다. 마찬가지로 고객의 내부 네트워크 관리자는 내부 디바이스, 구성 및 이벤트를 관리하기 위해 다른 3차 도메인에 로그인할 수 있습니다. 엣지 및 내부 관리자는 서로의 구축을 볼 수 없습니다.

참고 멀티테넌시를 사용하는 FMC에서 SSO 설정은 전역 도메인 수준에서만 적용할 수 있으며, 전역 도메인과 모든 하위 도메인에 적용됩니다.

관련 항목

SAML SSO(Single Sign-On) 구성, 74 페이지

도메인 용어

이 문서에서는 도메인 및 다중 도메인 배포에 대해 다음 용어를 사용합니다.

전역 도메인

다중 도메인 구축의 경우, 최상위 도메인을 표시 합니다. 멀티 테넌시를 구성하지 않는 경우 모든 디바이스, 설정 및 이벤트는 전역 도메인에 해당됩니다. 관리자가 전역 도메인의 전체 Firepower System 구축을 관리할 수 있습니다.

서브도메인

이차 또는 삼차 도메인입니다.

이차 도메인

전역 도메인의 하위 도메인입니다. 이차 도메인은 리프 도메인 또는 하위 도메인이 될 수 있습니다.

삼차 도메인

이차 도메인의 하위 도메인입니다. 삼차 도메인은 항상 리프 도메인입니다.

리프 도메인

하위 도메인이 없는 도메인입니다. 각 디바이스는 리프 도메인에 속해야 합니다.

하위 도메인

계층 구조에서 현재 도메인의 하위 단계에 있는 도메인입니다.

하위 도메인

도메인의 직접 하위 도메인입니다.

최상위 도메인

현재 도메인을 하위 도메인으로 갖는 도메인입니다.

상위 도메인

도메인의 직접 상위 도메인입니다.

동기 도메인

상위 도메인이 동일한 도메인입니다.

현재 도메인

현재 로그인한 도메인입니다. 시스템은 웹 인터페이스의 오른쪽 상단 사용자 이름 앞에 현재 도메인의 이름을 표시합니다. 사용자 역할이 제한된 경우가 아니라면 현재 도메인의 설정을 수정할 수 있습니다.

도메인 속성

도메인 속성을 수정하려면 해당 도메인의 상위 도메인에서 관리자 권한이 있어야 합니다.

이름 및 설명

각 도메인의 이름은 계층 내에서 고유해야 합니다. 설명은 선택 사항입니다.

상위 도메인

두 번째 및 세 번째 레벨 도메인에는 상위 도메인이 있습니다. 도메인을 생성한 후에는 도메인의 상위 항목을 변경할 수 없습니다.

디바이스

리프 도메인만 디바이스를 포함할 수 있습니다. 즉, 도메인은 하위 도메인이나 디바이스 중 하나만 포함할 수 있으며 둘 다 포함할 수는 없습니다. 리프가 아닌 도메인이 디바이스를 직접 제어하는 구축은 저장할 수 없습니다.

도메인 편집기에서 웹 인터페이스에는 도메인 계층 내의 현재 위치에 따라 사용 가능한 디바이스와 선택한 디바이스가 표시됩니다.

호스트 제한

Firepower Management Center에서 모니터링할 수 있는 호스트, 즉 네트워크 맵에 저장할 수 있는 호스트 수는 해당 모델에 따라 다릅니다. 다중 도메인 구축에서 리프 도메인은 모니터링되는 호스트의 사용 가능 풀을 공유하지만, 네트워크 맵은 각기 다릅니다.

각 리프 도메인이 네트워크 맵을 채울 수 있도록 각 하위 도메인 레벨에서 호스트 제한을 설정할 수 있습니다. 도메인의 호스트 제한을 **0**으로 설정하면 도메인이 일반 풀을 공유합니다.

호스트 제한을 설정할 때 각 도메인 레벨에 미치는 영향은 서로 다릅니다.

- 리프 - 리프 도메인의 경우 호스트 제한은 리프 도메인이 모니터링할 수 있는 호스트 수에 대한 단순한 제한입니다.
- 두 번째 레벨 - 세 번째 레벨 리프 도메인을 관리하는 두 번째 레벨 도메인의 경우 호스트 제한은 리프 도메인이 모니터링할 수 있는 총 호스트 수를 나타냅니다. 리프 도메인은 사용 가능한 호스트 풀을 공유합니다.
- 글로벌 - 글로벌 도메인의 경우 호스트 제한은 Firepower Management Center에서 모니터링할 수 있는 총 호스트 수와 같습니다. 이 값은 변경할 수 없습니다.

하위 도메인의 호스트 제한을 합한 값이 상위 도메인의 호스트 제한보다 커질 수 있습니다. 예를 들어 글로벌 도메인 호스트 제한이 150,000이면 각기 호스트 제한이 100,000인 하위 도메인을 여러 개 구성할 수 있습니다. 이러한 각 도메인은 100,000개의 호스트를 모니터링할 수 있지만 모든 도메인이 100,000개의 호스트를 모니터링할 수 있는 것은 아닙니다.

네트워크 검색 정책은 호스트 제한에 도달한 후 새 호스트가 탐지될 때 수행되는 작업을 제어합니다. 새 호스트를 삭제하거나 가장 오랫동안 비활성 상태였던 호스트를 교체할 수 있습니다. 각 리프 도메인에 자체 네트워크 검색 정책이 있으므로, 각 리프 도메인은 시스템에서 새 호스트를 검색할 때 고유한 동작을 관리합니다.

도메인의 호스트 제한을 줄이는 경우 네트워크 맵에 새 제한보다 많은 호스트가 포함되어 있으면 가장 오랫동안 비활성 상태였던 호스트가 삭제됩니다.

관련 항목

Firepower System 호스트 제한, 2391 페이지
네트워크 검색 데이터 스토리지 설정, 2556 페이지

도메인 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

도메인 관리

도메인 속성을 수정하려면 해당 도메인의 상위 도메인에서 관리자 권한이 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Domains(**도메인**)**를 선택합니다.

단계 **2** 도메인을 관리합니다.

- Add(추가) - **Add Domain(**도메인 추가**)**을 클릭하거나 상위 도메인 옆에 있는 **Add Subdomain(**하위 도메인 추가**)**을 클릭합니다. 새 도메인 생성, 486 페이지를 참조하십시오.
- Edit(수정) - 수정할 도메인 옆에 있는 아이콘(수정( ))을 클릭합니다. 도메인 속성, 483 페이지를 참조하십시오.
- Delete(삭제) - 삭제할 빈 도메인 옆에 있는 아이콘(삭제( ))을 클릭한 다음 선택 내용을 확인합니다. 대상 도메인을 수정하여 삭제할 도메인에서 디바이스를 이동합니다.

단계 **3** 도메인 구조를 변경하고 모든 디바이스를 리프 도메인과 연결한 후에 **Save(**저장**)**를 클릭하여 변경사항을 구현합니다.

단계 **4** 메시지가 표시되면 추가로 다음과 같이 변경합니다.

- 리프 도메인을 상위 도메인으로 변경한 경우 이전 네트워크 맵을 이동하거나 삭제합니다. 도메인 간 데이터 이동, 487 페이지를 참조하십시오.
- 도메인 간에 디바이스를 이동했으며 새 정책과 보안 영역 을 할당해야 하는 경우 도메인 간 디바이스 이동, 487 페이지를 참조하십시오.

다음에 수행할 작업

- 모든 새 도메인에 대한 사용자 역할 및 정책(액세스 제어, 네트워크 검색 등)을 구성합니다. 필요한 경우 디바이스 속성을 업데이트합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

새 도메인 생성

최고 수준 글로벌 도메인에 2~3개의 레벨로 최대 100개의 하위 도메인을 생성할 수 있습니다.

모든 디바이스를 리프 도메인에 할당해야 도메인 컨피그레이션을 구현할 수 있습니다. 리프 도메인에 하위 도메인을 추가하면 도메인은 더 이상 리프 도메인이 아니며, 해당 도메인의 디바이스를 재할당해야 합니다.

프로시저

단계 **1** 글로벌 또는 두 번째 수준 도메인에서 **System(**시스템**)** > **Domains(**도메인**)**를 선택합니다.

단계 **2** **Add Domain(**도메인 추가**)**을 클릭하거나 상위 도메인 옆에 있는 **Add Subdomain(**하위 도메인 추가**)**을 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Parent Domain(**상위 도메인**)**을 선택합니다.

단계 **5** **Devices(**디바이스**)**에서 도메인에 추가할 **Available Devices(**사용 가능한 디바이스**)**를 선택한 다음 **Add to Domain(**도메인에 추가**)**을 클릭하거나 **Selected Devices(**선택한 디바이스**)** 목록으로 끌어다 놓습니다.

단계 **6** 필요한 경우 **Advanced(**고급**)**을 클릭하여 새 도메인이 모니터링할 수 있는 호스트 수를 제한합니다. 도메인 속성, 483 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭하여 도메인 관리 페이지로 돌아갑니다.

리프 도메인이 아닌 도메인에 할당된 디바이스가 있는지 확인하라는 경고가 표시됩니다. **Create New Domain(**새 도메인 생성**)**을 클릭하여 해당 디바이스용으로 새 도메인을 생성합니다. 디바이스를 기존 도메인으로 이동하려는 경우에는 **Keep Unassigned(**미할당 상태 유지**)**를 클릭합니다.

단계 **8** 도메인 구조를 변경하고 모든 디바이스를 리프 도메인과 연결한 후에 **Save(**저장**)**를 클릭하여 변경사항을 구현합니다.

단계 **9** 메시지가 표시되면 추가로 다음과 같이 변경합니다.

- 리프 도메인을 상위 도메인으로 변경한 경우 이전 네트워크 맵을 이동하거나 삭제합니다. 도메인 간 데이터 이동, 487 페이지를 참조하십시오.
- 도메인 간에 디바이스를 이동했으며 새 정책과 보안 영역 을 할당해야 하는 경우 도메인 간 디바이스 이동, 487 페이지를 참조하십시오.

다음에 수행할 작업

- 모든 새 도메인에 대한 사용자 역할 및 정책(액세스 제어, 네트워크 검색 등)을 구성합니다. 필요한 경우 디바이스 속성을 업데이트합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

도메인 간 데이터 이동

이벤트 및 네트워크 맵은 리프 도메인과 연결되므로 리프 도메인을 상위 도메인으로 변경하는 경우 다음 두 가지 작업 중에서 선택할 수 있습니다.

- 네트워크 맵과 연결된 이벤트를 새 리프 도메인으로 이동합니다.
- 네트워크 맵을 삭제하되 이벤트는 유지합니다. 이 경우 시스템이 필요에 따라 또는 구성된 대로 이벤트를 정리할 때까지 이벤트는 상위 도메인과 연결된 상태로 유지됩니다. 또는 기존 이벤트를 수동으로 삭제할 수 있습니다.

시작하기 전에

이전의 리프 도메인이 이제 상위 도메인이 되는 도메인 컨피그레이션을 구현합니다. 도메인 관리, 485 페이지를 참조하십시오.

프로시저

단계 **1** 현재는 상위 도메인인 이전의 각 리프 도메인에 대해 다음 작업을 수행합니다.

- **Parent Domain(**상위 도메인**)**의 이벤트와 네트워크 맵을 상속할 새 **Leaf Domain(**리프 도메인**)**을 선택합니다.
- **None(**없음**)**을 선택하여 상위 도메인의 네트워크 맵을 삭제하되 기존 이벤트는 유지합니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

도메인 간 디바이스 이동

글로벌 도메인 또는 두 번째 레벨 도메인에 있을 때 도메인 간에 디바이스를 이동할 수 있습니다. 도메인 간에 디바이스를 이동하면 해당 디바이스에 적용된 컨피그레이션과 정책에 영향을 줄 수 있습니다. 시스템은 자동으로 가능한 내용을 유지하고 업데이트합니다. 업데이트할 수 없는 항목, 즉 개체 재정의, 동적 라우팅 구성, 고정 경로, 진단 인터페이스와 연결된 IP 풀, DDNS를 삭제합니다.

디바이스에 원격 액세스 VPN 정책을 할당할 경우, 한 도메인에서 다른 도메인으로 동일한 디바이스를 이동할 수 없습니다.

디바이스를 이동할 때 다음과 같은 새 필수 컨피그레이션을 선택하라는 프롬프트가 표시될 수 있습니다.

- 액세스 제어 정책 - 이동한 디바이스에 할당된 액세스 제어 정책이 새 도메인에서 유효하지 않거나 액세스할 수 없는 경우 새 정책을 선택합니다. 각 디바이스에 액세스 제어 정책이 할당되어 있어야 합니다.
- 상태 정책 - 이동한 디바이스에 적용된 상태 정책이 새 도메인에서 액세스할 수 없는 경우 새 상태 정책을 선택할 수 있습니다.
- 보안 영역 - 이동한 디바이스의 인터페이스가 새 도메인에서 액세스할 수 없는 보안 영역에 속해 있는 경우 새 영역을 선택할 수 있습니다.

디바이스에서 정책을 업데이트해야 하는데 영역 간에 인터페이스를 이동할 필요가 없는 경우에는 영역 컨피그레이션이 최신 상태라는 메시지가 표시됩니다. 예를 들어 디바이스의 인터페이스가 공통 상위 도메인에 구성된 보안 영역에 속해 있는 경우에는 하위 도메인 간에 디바이스를 이동할 때 영역 컨피그레이션을 업데이트할 필요가 없습니다.

시작하기 전에

- 도메인 간에 디바이스를 이동했으며 이제 새 정책과 보안 영역을 할당해야 하는 도메인 컨피그레이션을 구현합니다. 도메인 관리, 485 페이지를 참조하십시오.

프로시저

단계 **1** **Move Devices(**디바이스 이동**)** 대화 상자의 **Select Device(s) to Configure(**구성할 디바이스 선택**)** 아래에서 구성할 디바이스를 선택합니다.

동일한 상태 및 액세스 제어 정책을 할당할 디바이스를 여러 개 선택합니다.

단계 **2** 디바이스에 적용할 **Access Control Policy(**액세스 제어 정책**)**를 선택하거나 **New Policy(**새 정책**)**를 선택하여 새 정책을 생성합니다.

단계 **3** 디바이스에 적용할 **Health Policy(**상태 정책**)**를 선택하거나 **None(**없음**)**을 선택하여 상태 정책이 없는 상태로 디바이스를 유지합니다.

단계 **4** 새 영역에 인터페이스를 할당하라는 메시지가 표시되면 나열된 각 인터페이스에 대해 **New Security Zone(**새 보안 영역**)**을 선택하거나 **None(**없음**)**을 선택하여 나중에 인터페이스를 할당합니다.

단계 **5** 영향받는 모든 디바이스를 구성한 후 **Save(**저장**)**를 클릭하여 정책 및 영역 할당을 저장합니다.

단계 **6** **Save(**저장**)**를 클릭하여 도메인 컨피그레이션을 구현합니다.

다음에 수행할 작업

- 이동의 영향을 받은 이동한 디바이스의 기타 컨피그레이션을 업데이트합니다.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

도메인 관리 기록

기능	버전	세부 사항
지원되는 최대 도메인 수 증가	6.5	이제는 도메인을 100개까지 추가할 수 있습니다. 이전에는 최대 50개의 도메인만 구축할 수 있었습니다. 지원되는 플랫폼: Firepower Management Center

20 장

정책 관리

다음 주제는 Firepower Management Center의 다양한 정책을 관리하는 방법에 대해 설명합니다.

- 정책 관리를 위한 요구 사항 및 사전 요건, 491 페이지
- 정책 구축, 491 페이지
- 정책 비교, 513 페이지
- 정책 보고서, 515 페이지
- 만료된 정책, 516 페이지
- 제한된 구축에 대한 성능 고려 사항, 516 페이지
- 정책 관리 히스토리, 519 페이지

정책 관리를 위한 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)
- 보안 승인자

정책 구축

구축 설정을 완료하거나 구성을 변경한 뒤 영향받는 디바이스에 변경 사항을 구축해야 합니다. 메시지 센터에서 배포 상태를 확인할 수 있습니다.

다음 구성 요소 업데이트를 배포합니다.

- 디바이스 및 인터페이스 컨피그레이션
- 장치 관련 정책: NAT, VPN, QoS, 플랫폼 설정
- 액세스 제어 및 관련 정책: DNS, 파일, ID, 침입, 네트워크 분석, SSL
- 네트워크 검색 정책
- 침입 규칙 업데이트
- 설정 및 해당 요소와 관련된 개체

배포 작업을 예약하거나 침입 규칙 업데이트를 가져올 때 시스템 배포로 설정하여 자동으로 구축 시스템을 구성할 수 있습니다. 자동화 정책을 구축하는 것은 특히 침입 및 네트워크 분석에 대한 시스템 제공 기본 정책을 수정하는 침입 규칙 업데이트를 허용하는 경우에 유용합니다. 또한 침입 규칙 업데이트는 액세스 제어 정책의 고급 전처리 및 성능 옵션에 대한 기본값을 변경할 수 있습니다.

다중 도메인 구축에서 사용자 계정에 속해있는 모든 도메인에 대한 변경 사항을 구축할 수 있습니다.

- 상위 도메인이 모든 하위 도메인에 동시에 변경 사항을 구축하도록 전환합니다.
- 리프 도메인이 해당 도메인에만 변경 사항을 구축하도록 전환합니다.

구성 변경 사항 구축을 위한 모범 사례

다음은 컨피그레이션 변경 사항 구축을 위한 지침입니다.

인라인 구축과 패시브 구축 비교

수동으로 구축된 디바이스에 인라인 컨피그레이션을 적용하거나 인라인으로 구축된 디바이스에 수동 컨피그레이션을 적용하지 마십시오.

구축 시간 및 메모리 제한

구축 소요 시간은 다음을 비롯한 여러 요인에 따라 달라집니다.

- 디바이스로 전송하는 컨피그레이션. 예를 들어 차단할 보안 인텔리전스 항목의 수를 크게 늘리면 구축이 더 오래 걸릴 수 있습니다.
- 디바이스 모델 및 메모리. 메모리가 적은 디바이스에서는 구축이 더 오래 걸릴 수 있습니다. 예를 들어 Firepower 7010, 7020 또는 7030 디바이스 구축은 최대 5분이 소요될 수 있습니다.

디바이스의 기능을 초과하는 작업을 수행하지 마십시오. 대상 디바이스에서 지원하는 최대 규칙 또는 정책 수를 초과하면 경고가 표시됩니다. 최대치는 디바이스의 프로세서 수와 메모리뿐 아니라 정책 및 규칙의 복잡성과 같은 여러 가지 요인에 따라 달라집니다. 정책 및 규칙 최적화에 대한 정보는 액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지를 참조하십시오.

구축 중에 트래픽 흐름 및 검사 중단

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. Snort® 재시작 트래픽 동작, 507 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지의 내용을 참조하십시오.

주의 중단의 영향이 가장 적은 시간이나 유지 보수 기간에 구축을 수행하는 것이 좋습니다.

애플리케이션 탐지기 자동 활성화

애플리케이션 제어를 수행할 때 필요한 탐지기를 비활성화할 경우 정책 구축 시 적절한 시스템 제공 탐지기가 자동으로 활성화됩니다. 시스템 제공 탐지기가 없으면 애플리케이션에 대해 가장 최근에 수정된 사용자 정의 탐지기가 활성화됩니다.

네트워크 검색 정책 변경이 있는 자산 재검색

네트워크 검색 정책에 대한 변경 사항을 구축할 때는 시스템이 모니터링되는 네트워크의 호스트에 대한 네트워크 맵에서 MAC 주소, TTL 및 홉 정보를 삭제한 후 다시 검색합니다. 또한, 영향을 받는 매니지드 디바이스는 아직 Firepower Management Center로 전송되지 않은 검색 데이터를 모두 삭제합니다.

관련 항목

Snort® 재시작 시나리오, 505 페이지

구축 상태

Deployment(구축) 페이지에서 **Status(**상태**)** 열은 각 디바이스의 구축 상태를 제공합니다. 구축이 진행 중인 경우 구축 진행률의 라이브 상태가 표시됩니다. 그렇지 않으면 다음 상태 중 하나가 표시됩니다.

- Pending(보류 중) - 구축할 디바이스에 변경 사항이 있음을 나타냅니다.
- Warnings or errors(경고 또는 오류) - 사전 구축 확인에서 구축에 대한 경고 또는 오류를 식별했으며 구축을 진행하지 않았음을 나타냅니다. 경고가 있는 경우 구축을 계속할 수 있지만 오류가 있는 경우에는 구축을 계속할 수 없습니다.

참고 상태 열은 구축 페이지의 단일 사용자 세션에 대해서만 경고 또는 오류 상태를 제공합니다. 페이지에서 다른 페이지로 이동하거나 페이지를 새로 고치면 상태가 보류 중으로 변경됩니다.

- Failed(실패) - 이전 구축 시도가 실패했음을 나타냅니다. 세부 사항을 보려면 상태를 클릭합니다.
- In queue(대기열) - 구축이 시작되었으며 시스템이 아직 구축 프로세스를 시작하지 않았음을 나타냅니다.

• Completed(완료됨) - 구축이 성공적으로 완료되었음을 나타냅니다.

구축 견적

디바이스, 정책 또는 구성을 선택한 후에는 구축 페이지에서가 가견적 링크를 사용할 수 있습니다. 가견적 링크를 클릭하여 구축 기간의 가견적을 확인합니다. 소요 시간은 대략적인 가견적(약 70% 정확도)이며 구축에 소요되는 실제 시간은 몇 가지 시나리오에서 달라질 수 있습니다. 일부 FTD에 대한 구축은 예상 구축 기간을 참조하십시오. 가견적은 최대 20개의 FTD 디바이스를 구축할 때 신뢰할 수 있습니다.

가견적을 사용할 수 없으면 선택한 디바이스에서 첫 번째로 성공한 구축이 보류 중이므로 데이터를 사용할 수 없음을 나타냅니다. 이 상황은 FMC 버전 업그레이드 후 또는 새로 설치한 후에 발생할 수 있습니다.

참고 가견적은 휴리스틱 기술을 기반으로 하므로 대량 정책 변경(대량 정책 마이그레이션의 경우) 및 선택적 구축에 대한 가견적이 올바르지 않으며 신뢰할 수 없습니다.

구축 미리보기

미리보기에서는 디바이스에 구축할 모든 정책 및 개체 변경 사항의 스냅샷을 제공합니다. 정책 변경 사항에는 새 정책, 기존 정책의 변경 사항 및 삭제된 정책이 포함됩니다. 개체 변경 사항에는 정책에 사용되는 추가 및 수정된 개체가 포함됩니다. 사용되지 않는 개체 변경 사항은 디바이스에 구축되지 않으므로 표시되지 않습니다.

Deployment(구축) 페이지에서 Preview(미리보기) 열은 나열된 각 디바이스에 대한 미리보기( ) 아이콘을 제공합니다. 미리보기 아이콘을 클릭하면 FMC에서 모든 정책 및 개체 변경 사항을 나열하는 UI 페이지를 표시합니다. 미리보기 페이지의 왼쪽 창에는 디바이스에서 변경된 모든 정책 유형이 트리 구조로 구성되어 있습니다. 오른쪽 창에는 정책의 모든 추가, 변경 또는 삭제된 항목이나 왼쪽 창에서 선택한 개체가 나열됩니다. 오른쪽 창에 있는 2개의 열은 마지막으로 구축한 구성 설정(**Version on Device(**디바이스 버전**)** 열)과 구축 예정인 변경 사항(**Version on FMC(FMC** 버전**)** 열)을 제공합니다. 마지막으로 구축된 구성 설정은 디바이스가 아니라 FMC에 마지막으로 저장된 구축의 스냅샷에서 가져옵니다. 설정의 배경색은 페이지 오른쪽 상단에 있는 범례에 따라 색상으로 구분됩니다.

참고

- 구축 변경 사항을 미리 보려면 Firepower REST API에서 Firepower Management Center에 액세스해야 합니다. REST API 액세스를 활성화하려면 REST API 액세스 활성화의 단계를 수행합니다.
- 미리보기에는 여러 정책 간 규칙의 재정렬이 표시되지 않습니다.
- 변경되지 않은 경우에도 인터페이스 또는 플랫폼 설정 정책을 처음 추가할 때 구성된 다른 설정과 함께 모든 기본값이 미리보기에 표시됩니다. 마찬가지로, 설정에 대한 고가용성 관련 정책 및 기본값은 변경되지 않은 경우에도 고가용성 쌍이 설정되거나 중단된 후 첫 번째 미리보기에 표시됩니다.
- 일부 개체의 경우, 미리보기가 지원되지 않습니다.
- 개체가 디바이스 또는 인터페이스와 연결된 경우에만 개체 추가 및 속성 변경 사항이 미리보기에 표시됩니다. 개체 삭제는 표시되지 않습니다.
- 다음 정책에 대해서는 미리보기가 지원되지 않습니다.
  - 고가용성
  - 네트워크 검색
  - 네트워크 분석
  - 디바이스 설정
  - Flex 설정

선택적 정책 구축

FMC를 사용하면 구축할 예정인 디바이스의 모든 변경 사항 목록에서 특정 정책을 선택하고 선택한 정책만 구축할 수 있습니다. 선택적으로, 다음 정책에 대해서만 구축을 사용할 수 있습니다.

- 액세스 제어 정책
- 침입 정책
- 악성코드 및 파일 정책
- DNS 정책
- ID 정책
- SSL 정책
- QoS 정책
- 사전 필터 정책
- 네트워크 검색
- NAT 정책

- 라우팅 정책

구축 페이지에서 디바이스별 설정 변경 사항을 보려 확장 화살표( )를 클릭하면 정책 선택( ) 아이콘이 표시됩니다. 정책 선택 아이콘을 사용하면 나열된 나머지 변경 사항을 구축하지 않고 보류하면서 구축할 개별 정책 또는 설정을 선택할 수 있습니다. 이 옵션은 FTD에만 사용할 수 있으며 센서에는 사용할 수 없습니다. 이 옵션을 통해 특정 정책 또는 설정에 대한 상호 의존적인 변경 사항을 볼 수도 있습니다. FMC는 정책 간(예: 액세스 제어 정책과 침입 정책 간), 공유 개체와 정책 간의 종속성을 동적으로 탐지합니다. 상호 의존적인 변경 사항은 상호 의존적인 구축 변경 사항을 식별할 수 있도록 색상 코드 태그를 사용하여 표시됩니다. 구축 변경 사항 중 하나를 선택하면 상호 의존적인 변경 사항이 자동으로 선택됩니다.

참고

- 공유 개체의 변경 사항을 구축할 때는 영향을 받는 정책도 함께 구축해야 합니다. 구축 중에 공유 개체를 선택하면 영향을 받는 정책이 자동으로 선택됩니다.
- 예약된 구축 및 REST API를 사용하는 구축의 경우에는 선택적 구축이 지원되지 않습니다. 이때는 모든 변경 사항을 완전히 구축하도록 선택할 수만 있습니다.
- 경고 및 오류에 대한 사전 구축 검사는 선택한 정책뿐만 아니라 오래된 모든 정책에 대해서도 수행됩니다. 따라서 경고 또는 오류 목록에는 선택 취소된 정책도 표시됩니다.
- 마찬가지로 Deployment(구축) 페이지의 **Inspect Interruption(**검사 중단**)** 열 표시는 선택한 정책뿐 아니라 모든 오래된 정책을 고려합니다. **Inspect Interruption(**검사 중단**)** 열에 대한 자세한 내용은 Firepower Threat Defense 디바이스의 재시작 경고의 내용을 참조하십시오.

선택적으로 정책을 구축하는 데는 몇 가지 제한 사항이 있습니다. 아래 테이블의 내용에 따라 선택적 정책 구축을 사용할 수 있는 시점을 파악하십시오.

표 ***48:*** 선택적 구축에 대한 제한 사항

유형	설명	시나리오
전체 구축	전체 구축은 특정 구축 시나리오에 필요하며, FMC는 이러한 시나리오에서 선택적 구축을 지원하지 않습니다. 이러한 시나리오에서 오류가 발생하는 경우, 디바이스에서 구축할 모든 변경 사항을 골라서 진행하도록 선택할 수 있습니다.	전체 구축이 필요한 시나리오는 다음과 같습니다. • FTD 또는 FMC를 업그레이드한 후 첫 번째 구축 • FTD를 복원한 후의 첫 번째 구축 • FTD 인터페이스 설정 수정 후 첫 번째 구축 • 가상 라우터 설정 수정 후 첫 번째 구축 • FTD 디바이스가 새 도메인(전역에서 하위 도메인으로 또는 하위 도메인에서 전역으로)으로 이전하는 경우

유형	설명	시나리오
연결된 정책 구축	FMC는 서로 연결된 상호 의존적인 정책을 식별합니다. 상호 연결된 정책 중 하나를 선택하면 나머지 상호 연결된 정책이 자동으로 선택됩니다.	연결된 정책이 자동으로 선택되는 시나리오는 다음과 같습니다. • 새 개체가 기존 정책과 연결된 경우 • 기존 정책의 개체가 수정된 경우 여러 정책이 자동으로 선택되는 시나리오는 다음과 같습니다. • 새 개체가 기존 정책과 연결되어 있고 동일한 개체가 이미 다른 정책과 연결되어 있으면 연결된 모든 정책이 자동으로 선택됩니다. • 공유 개체가 수정되면 연결된 모든 정책이 자동으로 선택됩니다.
상호 의존적 정책 변경(색상으로 구분된 태그를 사용하여 표시)	FMC는 정책 간 및 공유 개체와 정책 간의 종속성을 동적으로 탐지합니다. 개체 또는 정책의 상호 종속성은 색상으로 구분된 태그를 사용하여 표시됩니다.	색상으로 구분된 상호 의존적 정책 또는 개체가 자동으로 선택되는 시나리오는 다음과 같습니다. • 모든 오래된 정책에 상호 의존적인 변경 사항이 있는 경우 예를 들어, 액세스 제어 정책, 침입 정책 및 NAT 정책이 오래된 경우입니다. 액세스 제어 정책과 NAT 정책은 개체를 공유하므로 구축을 위해 모든 정책이 함께 선택됩니다. • 모든 오래된 정책이 하나의 개체를 공유하고 해당 개체가 수정된 경우

유형	설명	시나리오
액세스 정책 그룹 사양	액세스 정책 그룹 정책은 정책 표시 또는 숨기기( )를 클릭하면 **Access Policy Group(**액세스 정책 그룹**)** 아래의 미리보기 창에 함께 나열됩니다.	액세스 정책 그룹 정책에 대한 시나리오 및 예상되는 동작은 다음과 같습니다. • 액세스 제어 정책이 만료된 경우, 파일 그룹 및 침입 정책을 제외하고 이 그룹에 속한 다른 모든 오래된 정책은 액세스 제어 정책이 구축하도록 선택될 때 설정됩니다. 단, 액세스 제어 정책이 만료된 경우, 종속적인 변경이 없는 한 액세스 제어 정책의 선택 여부와 관계없이 침입 및 파일 정책을 개별적으로 선택하거나 선택을 취소할 수 있습니다. 예를 들어, 새 침입 정책이 액세스 제어 규칙에 할당된 경우, 종속 변경 사항이 있음을 나타내며, 둘 중 하나를 선택하면 액세스 제어 정책과 침입 정책이 모두 자동으로 선택됩니다. • 만료된 액세스 제어 정책이 없는 경우, 이 그룹의 다른 만료된 정책을 개별적으로 선택하여 구축할 수 있습니다.

컨피그레이션 변경 사항 구축

컨피그레이션을 변경한 후 해당하는 디바이스에 구축합니다. 컨피그레이션 변경 사항은 트래픽 흐름 및 검사 중단의 영향이 가장 적은 시간이나 유지 보수 기간에 구축하는 것이 좋습니다.

⚠

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. Snort® 재시작 트래픽 동작, 507 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지의 내용을 참조하십시오.

시작하기 전에

- 구성 변경 사항 구축을 위한 모범 사례, 492 페이지에 설명되어 있는 지침을 검토합니다.
- 모든 매니지드 디바이스가 동일한 수정 버전의 보안 영역 개체를 사용하는지 확인합니다. 보안 영역 개체를 수정한 경우 동기화하려는 모든 디바이스에서 인터페이스에 대한 영역 설정을 수정하기 전에는 구성 변경 사항을 디바이스에 구축하지 마십시오. 모든 매니지드 디바이스에 동시에 구축해야 합니다. 보안 영역 개체의 수정 버전 동기화, 695 페이지의 내용을 참조하십시오.

프로시저

단계 **1** Firepower Management Center 메뉴 모음에서 **Deploy(구축)**를 클릭한 다음 **Deployment(구축)**를 선택합니다.

GUI 페이지에는 오래된 상태의 구성이 보류중인 디바이스가 나열됩니다.

- **Inspect Interruption(검사 중단)** 열은 구축 중에 디바이스에서 트래픽 검사 중단이 발생할 수 있는지 여부를 나타냅니다.

  디바이스에 대한 이 열의 항목이 비어 있으면 구축 중에 해당 디바이스에서 트래픽 검사가 중단되지 않음을 나타냅니다.

- 마지막 수정 시간 열은 구성을 마지막으로 변경한 시간을 나타냅니다.
- **Preview(미리보기)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다. 자세한 내용은 구축 미리보기, 494 페이지를 참고하십시오.
- **Status(상태)** 열은 각 구축의 상태를 제공합니다. 자세한 내용은 구축 상태, 493 페이지를 참고하십시오.

단계 **2** 컨피그레이션 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스 별 구성 변경 사항을 보려면 확장 화살표( )을 클릭합니다.

디바이스 확인란을 선택하면 디바이스 아래에 나열된 디바이스에 대한 모든 변경 사항이 푸시되어 구축됩니다. 그러나 정책 선택( )를 사용하면 구축하지 않고 나머지 변경 사항을 보류하면서 구축할 개별 정책 또는 구성을 선택할 수 있습니다. 자세한 내용은 선택적 정책 구축, 495 페이지 섹션을 참조해 주십시오.

선택적으로, 수정되지 않은 관련 정책을 선택적으로 보거나 숨기는 데 정책 표시 또는 숨기기( )을(를) 사용할 수 있습니다.

참고

- **Inspect Interruption(검사 중단)** 열의 상태가 (Yes(예))인 경우(컨피그레이션을 구축하면 Firepower Threat Defense 디바이스에서 검사가 중단되며 트래픽도 중단될 수 있는 경우) 확장된 목록에 중단을 야기하는 특정 컨피그레이션이 검사 중단( )으로 표시됩니다.
- 인터페이스 그룹, 보안 영역 또는 개체가 변경되면 영향을 받는 디바이스는 FMC(Firepower Management Center)에서 오래된 것으로 표시됩니다. 이러한 변경 사항을 적용하려면 이러한 인터페이스 그룹, 보안 영역 또는 개체가 포함된 정책도 이러한 변경 사항과 함께 구축해야 합니다. 영향을 받는 정책은 FMC의 미리보기 페이지에서 만료된 것으로 표시됩니다.

단계 **3** (선택 사항) 대략적인 구축 기간을 확인하려면 **Estimate(견적)**를 클릭합니다.

자세한 내용은 구축 견적, 494 페이지를 참조하십시오.

단계 **4** **Deploy(**구축**)**를 클릭합니다.

단계 **5** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- Deploy(구축) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

다음에 수행할 작업

- (선택 사항) 구축 상태를 모니터링합니다. 구축 메시지 보기, 444 페이지를 참조하십시오.
- 구축에 실패하는 경우 구성 변경 사항 구축을 위한 모범 사례, 492 페이지를 참조하십시오.

관련 항목

Snort® 재시작 시나리오, 505 페이지

디바이스에 기존 구성을 재구축하십시오

관리되는 단일 디바이스에 기존의 (변경되지 않은) 구성을 강제 구축할 수 있습니다. 컨피그레이션 변경 사항은 트래픽 흐름 및 검사 중단의 영향이 가장 적은 시간이나 유지 보수 기간에 구축하는 것이 좋습니다.

⚠

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. Snort® 재시작 트래픽 동작, 507 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지의 내용을 참조하십시오.

시작하기 전에

구성 변경 사항 구축을 위한 모범 사례, 492 페이지에 설명되어 있는 지침을 검토합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 강제 구축을 원하는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 디바이스를 클릭합니다.

단계 **4** **General(**일반**)** 섹션 옆에 있는 수정( )을 클릭합니다.

단계 **5** 강제 구축( ) 버튼을 클릭합니다.

참고 강제 구축은 FTD에 구축할 정책 규칙의 완전한 생성을 포함하므로 일반 구축보다 시간이 더 오래 걸립니다.

단계 **6** **Deploy(**구축**)**를 클릭합니다.

시스템은 구축하려는 설정과 관련된 모든 오류나 경고를 식별합니다. 경고 상황을 해결하지 않고 계속하려면 **Proceed(**진행**)**를 클릭합니다. 그러나 시스템이 오류를 식별하는 경우 계속 진행할 수 없습니다.

다음에 수행할 작업

- (선택 사항) 구축 상태를 모니터링합니다. 구축 메시지 보기, 444 페이지를 참조하십시오.
- 구축에 실패하는 경우 구성 변경 사항 구축을 위한 모범 사례, 492 페이지를 참조하십시오.

관련 항목

Snort® 재시작 시나리오, 505 페이지

구축 히스토리 보기

프로시저

단계 **1** Firepower Management Center 메뉴 표시줄에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment History(**구축 기록**)**를 선택합니다.

모든 이전 구축 및 롤백 작업의 목록이 역순으로 표시됩니다.

단계 **2** 필요한 구축 작업 옆의 확장 화살표( )를 클릭하여 작업에 포함된 디바이스 및 구축 상태를 확인합니다.

단계 **3** (선택 사항) 디바이스로 전송된 명령 및 수신된 응답을 보려면 대화 내용 상세정보( )를 클릭합니다.

기록은 다음 섹션으로 구성되어 있습니다.

- **Snort Apply(Snort** 적용**)** - Snort 관련 정책에서 장애 또는 응답이 발생하는 경우, 이 섹션에 메시지가 표시됩니다. 일반적으로 이 섹션은 비어 있습니다.
- **CLI Apply(CLI** 적용**)** - 이 섹션에서는 디바이스로 전송되는 명령을 사용하여 설정한 기능에 대해 설명합니다.

참고 롤백 작업의 기록은 CLI 명령 정보를 제공하지 않습니다. 롤백 명령을 보려면 구축 롤백 기록 보기, 505 페이지의 내용을 참조하십시오.

- **Infrastructure Messages(**인프라 메시지**)** - 이 섹션에는 여러 구축 모듈의 상태가 표시됩니다.

CLI Apply(CLI 적용**)** 섹션의 구축 기록에는 디바이스로 전송된 명령과 디바이스에서 반환된 응답이 포함되어 있습니다. 이러한 응답은 정보 메시지 또는 오류 메시지일 수 있습니다. 장애가 발생한 구축의 경우 명령 오류를 나타내는 메시지를 확인합니다. FlexConfig 정책을 사용하여 맞춤화된 기능을 구성하는 경우 이러한 오류를 검사하면 특히 유용할 수 있습니다. 이 오류를 확인하여 명령을 구성하려는 FlexConfig 개체의 스크립트를 수정할 수 있습니다.

참고 관리 기능에 대해 전송된 명령과 FlexConfig 정책에서 생성된 명령이 기록에서 구분되지는 않습니다.

예를 들어, 다음 시퀀스는 Firepower Management Center(FMC)가 외부에서 논리적 이름으로 GigabitEthernet0/0을 설정하기 위해 명령을 전송했음을 보여줍니다. 디바이스에서 보안 수준을 0으로 자동 설정했다고 응답했습니다. FTD에서는 어떠한 경우에도 보안 수준을 사용하지 않습니다.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

구축 롤백

롤백은 FTD 디바이스에서 기존 구축을 지우고 이전에 구축한 구성으로 디바이스를 재구성하기 위해 제공되는 구축 기능입니다.

주의 롤백은 베타 기능입니다. 그러나 이 기능은 완전히 지원됩니다.

정책 구축 후 FTD를 통과하는 트래픽이 의도하지 않은 방식으로 영향을 받는 경우 롤백이 디바이스를 결함 있는 구축 이전의 상태로 되돌릴 수 있는 옵션을 제공합니다.

구축이 잘못되어 의도하지 않은 방식으로 트래픽이 중단된 경우에는 구축의 변경 사항을 확인하여 문제를 해결하는 것이 좋습니다. 이전 구축의 변경 사항을 확인하려면 **Deploy(**구축**)** > **Deployment History(**구축 기록**)**로 이동하여 마지막 구축의 기록을 확인합니다. 이전 구축과 관련된 추가 변경 사항은 감사 레코드를 참조하십시오(감사 기록, 451 페이지 참조). 문제를 일으키는 변경 사항을 식별한 후 구성을 수정하고 디바이스에 다시 구축합니다. 이것이 권장되는 접근 방식입니다. 그러나 문제를 일으킨 변경 사항을 식별할 수 없는 경우 디바이스에서 마지막으로 구축된 안정적인 버전으로 롤백합니다.

롤백 작업이 정상적으로 완료되면 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 롤백된 디바이스 옆의 **Preview(**미리보기**)** 아이콘을 클릭합니다. 롤백 구성과 FMC의 현재 변경 사항 간의 변경 사항을 확인합니다. 문제를 일으킨 변경 사항을 식별하고 수정합니다.

롤백은 일부를 제외하고 디바이스의 모든 구성을 되돌립니다. 자세한 내용은 아래 표를 참조하십시오.

롤백 중에 복귀되는 구성	롤백 중에 복귀되지 않은 구성
• 모든 정책 구성 • 인터페이스 구성 • SRU 구성 • VDB 구성 • VPN 구성 • FXOS 구성	• Snort 이진 • Geo DB

중요

- 롤백은 중단 작업입니다. 이 작업을 수행하는 동안 모든 기존 연결 및 경로가 삭제되고 트래픽이 중단됩니다. 롤백은 선택한 모든 FTD 디바이스에서 현재 구성을 제거하고 선택한 롤백 버전으로 재구성합니다.
- 최적의 성능을 위해 낮은 트래픽 조건에서 롤백을 시작합니다.
- 특정 버전으로의 롤백은 한 번만 수행할 수 있습니다.
- 현재 구축된 버전 직전 버전으로만 롤백할 수 있습니다. 이전 버전으로의 롤백은 지원되지 않습니다. 지원되지 않는 버전의 경우 롤백 아이콘이 회색으로 표시됩니다.
- 2회 연속 롤백 작업은 허용되지 않습니다. 그러나 구축 후에는 다시 롤백할 수 있습니다.
- 롤백은 선택한 FTD에서만 설정을 되돌립니다. FMC는 모든 변경 사항을 유지합니다. FMC에서 구성 변경 사항이 유지되면 롤백 작업 후 디바이스가 FMC에서 오래된 것으로 표시됩니다. 디바이스의 구성과 FMC에서 유지되는 변경 사항을 보려면 **Deploy(**구축**)** > **Deployment(**구축**)**으로 이동하고 롤백된 디바이스 옆에 있는 **Preview(**미리 보기**)** 아이콘을 클릭합니다.
- 전체 구축이므로 롤백한 후 첫 번째 구축에서 구축할 변경 사항에 유의해야 합니다. 그러면 롤백된 버전으로 다시 롤백할 수 없습니다.
- **Object Group Search(**개체 그룹 검색**)** 설정이 비활성화된 경우 큰 액세스 목록이 있는 FTD에 대해서는 롤백 작업을 완료하는 데 더 오래 걸릴 수 있습니다. 이 **Object Group Search(**개체 그룹 검색**)** 설정을 확인하려면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**로 이동하여 디바이스를 선택하고 **Edit Advanced Settings(**고급 설정 편집**)**을 클릭합니다.

참고

- 롤백은 FTD 버전 6.7.0 이상에서만 지원됩니다.
- 롤백은 FTD 클러스터 및 NGIPS 디바이스에서 지원되지 않습니다.
- FMC와 FTD 간의 연결 인터페이스가 관리에서 데이터로 또는 그 반대로 변경되는 경우 롤백이 지원되지 않습니다.
- Firepower 4100/9300에서는 이전 구축의 FCM(Firepower Chassis Manager)에서 인터페이스를 변경한 다음 FCM을 사용하여 인터페이스를 동기화한 후 롤백을 시작합니다. 이렇게 하지 않으면 트래픽이 중단될 수 있습니다.
- 독립 인증서 등록도 Deployment History(구축 기록) 페이지에 구축 작업으로 나열됩니다. 그러나 이러한 버전으로 롤백할 수는 없습니다. 인증서 등록 이후에 생성된 구축 버전의 롤백은 인증서 연결도 되돌립니다. 롤백 후 다음 구축에서는 구축을 진행하기 전에 인증서를 수동으로 연결합니다.
- FMC 또는 FTD 업그레이드 후 첫 번째 버전에서는 롤백이 지원되지 않습니다. 예를 들어 FMC가 6.7.0에서 6.7.0.1로 업그레이드된 경우 6.7.0과 연결된 구축 패키지로 롤백할 수 없습니다.
- 구축 빈도가 **Once(**한 번**)**로 설정된 상태로 구성된 FlexConfig 개체가 있는 디바이스에 대한 구축이 롤백되는 경우, Preview (미리보기) 페이지에서 해당 객체가 오래된 것으로 표시되더라도 해당 구축을 재구축할 수 없습니다. 롤백 후에는 다음 구축 전에 FlexConfig 개체를 수동으로 할당 해제한 다음 디바이스에 다시 할당해야합니다.

HA 시나리오의 롤백

다음 HA 시나리오에서는 롤백이 지원되지 않습니다.

- 롤백하려는 버전에 FTD HA 부트 스트랩 구성이 포함된 경우.
- 롤백하려는 버전에 FTD HA 중단 구성이 포함된 경우.
- 현재 독립형 모드인 FTD가 이전 구축 버전에서 HA 또는 클러스터의 일부인 경우.

디바이스에서 구축 롤백

프로시저

단계 **1** Firepower Management Center 메뉴 표시줄에서 **Deploy(**구축**)** > **Deployment History(**구축 기록**)**를 선택합니다.

모든 이전 구축 작업 목록이 역순으로 표시됩니다.

단계 **2** 필요한 구축 작업 옆의 롤백 아이콘()을 클릭하여 작업에 포함된 디바이스 및 구축 상태를 확인합니다.

단계 **3** 롤백할 디바이스를 선택합니다.

단계 **4** **Rollback(**롤백**)**을 클릭합니다.

다음에 수행할 작업

롤백 상태를 확인하려면 **Deploy(**구축**)** > **Deployment(**구축**)**를 클릭합니다. 디바이스 옆의 롤백 상태를 볼 수 있습니다.

구축 롤백 기록 보기

롤백 기록은 디바이스에서 반환되는 응답과 함께 디바이스로 전송되는 명령이 작성된 버전입니다. 롤백 작업이 실패한 경우, **Deploy(**구축**)** > **Deployment History(**구축 기록**)** 페이지의 기록에 실패 이유가 표시됩니다. 단, 롤백 작업을 성공적으로 수행하기 위해 실행된 CLI 명령을 확인하려면 롤백 작업이 완료된 후 아래 단계를 수행하십시오. 이 정보는 다음 구축까지만 확인할 수 있습니다.

참고 CLI 명령 정보는 롤백이 완료된 후에 확인할 수 있으며, 다음 구축까지만 살펴볼 수 있습니다. 롤백 작업 후 첫 번째 구축에서는 모든 롤백 관련 정보가 지워집니다.

프로시저

단계 **1** Firepower Management Center 메뉴 표시줄에서 **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** 왼쪽 창에서 롤백된 디바이스를 선택합니다.

단계 **3** **View System & Troubleshooting Details(**시스템 및 문제 해결 세부 사항 보기**)** 링크를 클릭합니다.

단계 **4** **Advanced Troubleshooting(**고급 문제 해결**)**을 클릭하십시오.

단계 **5** **Threat Defense CLI(**위협 방어 **CLI)**를 클릭합니다.

단계 **6** **Command(**명령**)** 드롭다운 상자에서 **show**를 클릭합니다.

단계 **7** **Parameter(**매개변수**)** 필드에 **`running`**을 입력합니다.

단계 **8** **Execute(**실행**)**를 클릭합니다.

Snort® 재시작 시나리오

Snort 프로세스라는 트래픽 검사 엔진이 매니지드 디바이스에서 재시작되면, 프로세스가 다시 시작될 때까지 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. 또한, 구축 시에는 Snort 프로세스가 재시작되는지와 관계없이 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다.

다음 표의 시나리오 중 하나가 발생하는 경우 Snort 프로세스가 재시작됩니다.

표 ***49: Snort*** 재시작 시나리오

시나리오 다시 시작	추가 정보
Snort 프로세스를 재시작해야 하는 특정 설정을 구축합니다.	구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지
즉시 Snort 프로세스를 재시작해야 하는 특정 설정을 수정합니다.	즉시 Snort 프로세스를 재시작시키는 변경 사항, 513 페이지
현재 구축된 자동 애플리케이션 우회(AAB) 설정을 활성화하는 트래픽을 활성화합니다.	AAB(Automatic Application Bypass) 구성, 345 페이지

관련 항목

액세스 제어 정책 고급 설정, 1637 페이지
구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지

정책 적용 중에 트래픽 검사

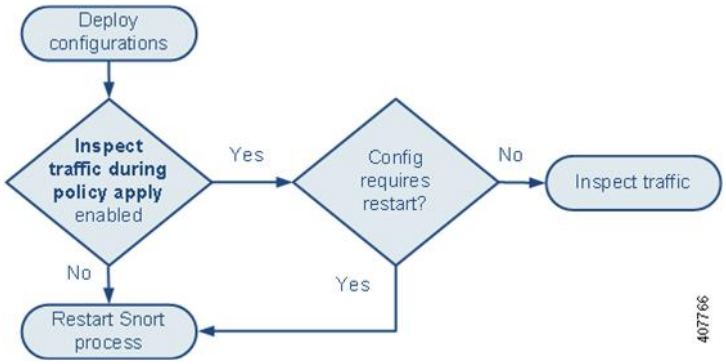
정책 적용 중 트래픽 검사는 고급 액세스 제어 정책 일반 설정으로서 설정 변경이 구축되는 동안 관리되는 디바이스가 트래픽을 검사하도록 허용합니다. 단 구축하려는 설정이 Snort 프로세스를 재시작할 필요가 없는 경우에 한정됩니다. 이 옵션은 다음과 같이 구성할 수 있습니다.

- 활성화 — 재시작 시 특정 설정이 Snort 프로세스를 요구하지 않는 한 구축 시 트래픽을 검사합니다.

  구축하려는 구성이 Snort 재시작을 요구하지 않는 경우 시스템은 현재 구축된 액세스 제어 정책을 사용해 트래픽을 검사하고 구축 시 구축하려는 액세스 제어 정책으로 전환합니다.

- 비활성화 — 구축 중 트래픽을 검사하지 않습니다. 구축 시 항상 Snort 프로세스를 재시작합니다.

다음 그래픽은 정책 적용 중 트래픽 검사 활성화에 따라 Snort가 재시작되는 방식을 나타냅니다.



주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. Snort® 재시작 트래픽 동작, 507 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지의 내용을 참조하십시오.

Snort® 재시작 트래픽 동작

다음 표에서는 Snort 프로세스가 재시작될 때 각 디바이스가 트래픽을 처리하는 방법을 설명합니다.

표 ***50: FTD*** 및 ***FTD*** 가상 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음
라우팅, Transparent(EtherChannel, 이중화, Transparent 포함)	차단

표 ***51: 7000*** 및 ***8000, NGIPSv*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음
라우팅, 스위칭 (7000 및 8000 Series 전용)	차단

표 ***52: ASA FirePOWER*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅 또는 fail-open 상태의 Transparent	검사 없이 통과됨
라우팅 또는 fail-close 상태의 Transparent	차단

표 ***53: FTD*** 및 ***FTD*** 가상 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Snort Fail Open: Down(Snort Fail-Open:** 중단**)**: 활성화	검사 없이 통과됨
인라인: **Snort Fail Open: Down(Snort Fail-Open:** 중단**)**: 비활성화	차단
라우팅, Transparent(EtherChannel, 이중화, 하위 인터페이스 포함) 버전 6.2.2에서는 **configure snort preserve-connection {enable | disable}** CLI 명령을 지원하지 않으며 이 명령이 활성화되어 있을 때(기본값) 검사 없이 통과하도록 기존 TCP/UDP 연결을 허용했습니다. 버전 6.2.2 기준으로, FMC 및 FTD 모두 버전 6.2.0.2 또는 후속 6.2.0.x 패치를 실행하고 있지 않으면 패킷이 삭제됩니다. 자세한 내용은 Cisco Firepower Threat Defense 명령 참조의 내용을 참고하십시오.	차단
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음

표 ***54: 7000*** 및 ***8000, NGIPSv*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅, 스위칭 (7000 및 8000 Series 전용)	차단

표 ***55: ASA FirePOWER*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅 또는 fail-open 상태의 Transparent	검사 없이 통과됨
라우팅 또는 fail-close 상태의 Transparent	차단

표 ***56: FTD*** 및 ***FTD*** 가상 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Snort Fail Open: Down(Snort Fail-Open: 중단)**: 비활성화	차단
인라인: **Snort Fail Open: Down(Snort Fail-Open: 중단)**: 활성화	검사 없이 통과됨
라우팅, Transparent(EtherChannel, 이중화, 하위 인터페이스 포함): **preserve-connection** 활성화 (**configure snort preserve-connection enable**, 기본값) 자세한 내용은 Cisco Firepower Threat Defense 명령 참조의 내용을 참고하십시오.	기존 TCP / UDP 플로우 : Snort가 중단된 상태에서 하나 이상의 패킷이 도착하는 한 검사 없이 통과됨 새 TCP/UDP 플로우와 모든 비TCP/UDP 플로우: 삭제됨 다음 트래픽은 **preserve-connection** 활성화 시에도 삭제됩니다. • **Analyze** 규칙 작업 또는 **Analyze all tunnel traffic** 기본 정책 작업과 일치하는 plaintext, passthrough prefilter 터널 트래픽 • 연결은 액세스 제어 규칙과 일치하지 않으며 대신 기본 작업에 의해 처리됩니다. • 암호 해독된 TLS/SSL 트래픽 • 안전한 검색 흐름 • 캡티브 포털 흐름
라우팅, Transparent(EtherChannel, 이중화, 하위 인터페이스 포함): **preserve-connection** 비활성화 (**configure snort preserve-connection disable**)	차단
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회

인터페이스 컨피그레이션	재시작 트래픽 동작
패시브	중단되지 않음, 검사되지 않음

표 ***57: NGIPSv*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음

표 ***58: ASA FirePOWER*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅 또는 fail-open 상태의 Transparent	검사 없이 통과됨
라우팅 또는 fail-close 상태의 Transparent	차단

참고 Snort 프로세스가 재시작되는 동안 중단되는 경우의 트래픽 처리 이외에 Failsafe 옵션의 컨피그레이션에 따라 Snort 프로세스가 사용 중인 경우에도 트래픽이 검사 없이 통과하거나 삭제될 수 있습니다. Firepower System의 인라인 집합, 703 페이지의 내용을 참조하십시오.

참고 컨피그레이션 구축 중에 Snort 프로세스가 사용 중이지만 중단되지는 않은 경우, 총 CPU 로드가 50%를 초과하면 라우팅, 스위칭 또는 Transparent 인터페이스에서 일부 패킷이 삭제될 수 있습니다.

구축 또는 활성화 시 **Snort** 프로세스를 재시작하는 컨피그레이션

AAB를 제외한 다음 구성을 구축할 때는 설명대로 Snort 프로세스가 재시작됩니다. AAB를 구축할 때는 프로세스가 재시작되지 않지만, 과도한 패킷 레이턴시로 인해 현재 구축된 AAB 컨피그레이션이 활성화되어 Snort 프로세스가 부분적으로 재시작됩니다.

액세스 제어 정책 고급 설정

- **Inspect Traffic During Policy Apply(**정책 적용 중에 트래픽 검사**)**가 비활성화되었을 때 구축합니다.

- SSL 정책을 추가하거나 제거합니다.

보안 인텔리전스

여러 보안 인텔리전스 화이트리스트 또는 블랙리스트 네트워크나 네트워크 개체를 추가 또는 삭제합니다. 변경 사항은 맞춤형 목록 또는 시스템 제공 목록이 될 수 있으며 Snort 프로세스의 재시작 여부는 검사에 사용할 수 있는 메모리에 따라 디바이스별로 달라질 수 있습니다.

파일 정책

다음 컨피그레이션 중 하나의 첫 번째 또는 마지막 항목을 구축합니다. 이러한 파일 정책 컨피그레이션을 다른 방식으로 구축할 때는 프로세스가 재시작되지 않지만, 비 파일 정책 컨피그레이션을 구축할 때는 프로세스가 재시작될 수 있습니다.

- **Inspect Archives(**아카이브 검사**)**를 활성화하거나 비활성화합니다.
- 다음 작업 중 하나를 수행합니다.
  - 구축된 액세스 컨트롤 정책에 파일 정책이 하나 이상 포함되어 있으면 **Inspect Archives(**아카이브 검사**)**를 활성화하거나 비활성화합니다.
  - **Inspect Archives(**아카이브 검사**)**가 활성화되어 있으면 첫 번째 정책 규칙을 추가하거나 마지막 파일 정책을 제거합니다. **Inspect Archives(**아카이브 검사**)**가 적용되려면 규칙이 하나 이상 필요합니다.
- **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 **Store Files(**파일 저장**)**를 활성화하거나 해제합니다.
- **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)**, **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**)**, **Unknown(**알 수 없음**)**, **Clean(**정상**)**, **Custom(**맞춤형**))**과 결합하는 첫 번째 활성 파일 규칙을 추가하거나 마지막 활성 파일 규칙을 제거합니다.

이러한 파일 정책 컨피그레이션을 보안 영역이나 터널 영역에 구축하는 액세스 컨트롤 규칙의 경우 컨피그레이션이 다음 조건을 충족할 때만 프로세스가 재시작됩니다.

- 액세스 컨트롤 규칙의 소스 또는 대상 보안 영역이 대상 디바이스의 인터페이스와 연결된 보안 영역과 일치해야 합니다.
- 액세스 컨트롤 규칙의 대상 영역이 *any*(임의)가 아니면 규칙의 소스 터널 영역은 사전 필터 정책의 터널 규칙에 할당된 터널 영역과 일치해야 합니다.

ID 정책

- SSL 암호 해독이 비활성화되어 있으면(액세스 제어 정책에 SSL 정책이 포함되지 않음) 첫 번째 활성 인증 규칙을 추가하거나 마지막 활성 인증 규칙을 제거합니다.

활성 인증 규칙에는 **Active Authentication(**활성 인증**)** 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)**가 선택된 **Passive Authentication(**패시브 인증**)** 규칙 작업이 있습니다.

네트워크 검색

- 네트워크 검색 정책을 사용하여 HTTP, FTP 또는 MDNS 프로토콜을 통한 신뢰할 수 없는 트래픽 기반 사용자 탐지를 활성화하거나 비활성화합니다.

디바이스 관리

- 라우팅: 7000 또는 8000 Series 디바이스에 라우팅된 인터페이스 쌍 또는 가상 라우터를 추가합니다.
- VPN: 7000 또는 8000 Series 디바이스에서 VPN을 추가하거나 제거합니다.

  주의 7000 또는 8000 Series 디바이스에서 VPN을 추가하거나 제거할 때는 Snort 프로세스가 재시작된다는 경고가 표시되지 않습니다.

- MTU: 디바이스의 모든 비 관리 인터페이스 중에서 가장 높은 MTU 값을 변경합니다.
- 7000/8000 시리즈 고가용성: 고가용성 상태 공유 옵션을 변경합니다. 기본 디바이스와 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고가 표시되지 않습니다.
- AAB(자동 애플리케이션 바이패스): Snort 프로세스 오작동 또는 잘못된 디바이스 컨피그레이션으로 인해 단일 패킷이 과도한 처리 시간을 사용하면 현재 구축되어 있는 AAB 컨피그레이션이 활성화됩니다. 이 경우 매우 긴 레이턴시를 완화하거나 완전한 트래픽 정지를 방지하기 위해 Snort 프로세스가 부분적으로 재시작됩니다. 이처럼 프로세스가 부분적으로 재시작되면 디바이스가 트래픽을 처리하는 방법에 따라 일부 패킷이 검사 없이 통과되거나 삭제됩니다.

업데이트

- 시스템 업데이트: Snort 이진 또는 데이터 획득 라이브러리(DAQ)의 새 버전을 포함하는 소프트웨어 업데이트 후에 처음으로 구성을 구축합니다.
- VDB: 매니지드 디바이스에 적용 가능한 변경 사항을 포함하는 VDB(취약성 데이터베이스) 업데이트를 설치한 후 처음으로 구성을 구축하려면 탐지 엔진 재시작이 필요하며 그러면 일시적인 트래픽 중단이 발생할 수 있습니다. 이러한 경우, 설치를 시작하기 위해 Firepower Management Center를 선택하면 경고 메시지가 표시됩니다. VDB 변경 사항이 보류 중인 경우 구축 대화 상자에서 Firepower Threat Defense 디바이스에 대한 추가 경고를 제공합니다. Firepower Management Center에만 적용되는 VDB 업데이트로는 탐지 엔진이 재시작되지 않으므로 해당 업데이트는 구축할 수 없습니다.

관련 항목

컨피그레이션 변경 사항 구축, 498 페이지
Snort® 재시작 시나리오, 505 페이지

즉시 **Snort** 프로세스를 재시작시키는 변경 사항

다음 변경 사항은 구축 단계를 거치지 않고 즉시 Snort 프로세스를 재시작합니다. 재시작으로 인해 어떻게 트래픽이 영향을 받는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

- 애플리케이션 또는 애플리케이션 탐지기와 관련된 다음 작업 중 하나를 수행합니다.
  - 시스템 또는 사용자 정의 애플리케이션 탐지기를 활성화하거나 비활성화합니다.
  - 활성화된 사용자 정의 탐지기를 삭제합니다.
  - 활성화된 사용자 정의 탐지기를 저장하고 다시 활성화합니다.
  - 사용자 정의 애플리케이션 생성

  Snort 프로세스를 재시작한다는 경고 메시지가 표시되며 진행을 취소할 수 있습니다. 현재 도메인 또는 하위 도메인의 관리되는 디바이스가 재시작됩니다.
- Firepower Threat Defense 고가용성 쌍을 생성하거나 중단 - 고가용성 쌍을 생성하면 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지가 표시되며 사용자가 취소할 수 있습니다.
- 7000 또는 8000 Series 유저 인터페이스(시스템 > 설정 > 프로세스)에서 Snort 프로세스를 재시작 - 시스템이 사용자의 승인 여부를 확인하며 사용자는 취소할 수 있습니다.

정책 비교

조직의 표준 규정을 준수하는지에 대한 정책 변경을 검토하고 시스템 성능을 최적화하기 위해 두 정책 또는 저장된 정책과 실행 설정 간 차이를 검토할 수 있습니다.

다음 정책 유형을 비교할 수 있습니다.

- DNS
- 파일
- 상태
- ID
- 침입
- 네트워크 분석
- SSL

비교 보기는 옵션 요약 비교 형식으로 두 정책을 표시합니다. 두 정책 간 차이점은 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.

- 녹색은 강조 표시된 설정이 한 정책에서는 나타나지만 다른 정책에서는 나타나지 않음을 표시합니다.

정책 비교

특정 정책에 대한 액세스 권한 및 필요한 라이선스가 있고 정책을 구성하기 위한 올바른 도메인에 있는 경우에만 정책을 비교할 수 있습니다.

프로시저

단계 **1** 비교할 정책의 관리 페이지에 액세스합니다.

- DNS—**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**
- 파일 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)**
- 상태 — **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)**
- ID — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)**
- 침입 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**
- 네트워크 분석 — **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**

  참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

- SSL — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**

단계 **2** **Compare Policies(**정책 비교**)**를 클릭합니다.

단계 **3** **Compare Against(**비교 대상**)** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 가지의 서로 다른 정책을 비교하려면, **Other Policy(**다른 정책**)**를 선택합니다.
- 동일한 정책의 두 가지 수정 버전을 비교하려면, **Other Revision(**다른 수정 버전**)**을 선택합니다.
- 현재 활성화된 정책과 다른 정책을 비교하려면, **Running Configuration(**실행 중인 컨피그레이션**)**을 선택합니다.

단계 **4** 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 가지 서로 다른 정책을 비교하는 경우 **Policy A(**정책 **A)** 및 **Policy B(**정책 **B)** 드롭다운 목록에서 비교할 정책을 각각 선택합니다.
- 실행 중인 컨피그레이션을 다른 정책과 비교하는 경우 **Policy B(**정책 **B)** 드롭다운 목록에서 두 번째 정책을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 비교 결과를 검토합니다.

- 비교 뷰어—비교 뷰어를 사용하여 정책 차이점을 개별적으로 탐색하려면 제목 바 위의 **Previous(**이전**)** 또는 **Next(**다음**)**를 클릭합니다.

- 비교 보고서 — 두 정책 간의 차이점을 나열하는 PDF 보고서를 생성하려면 **Comparison Report(**비교 보고서**)**를 클릭합니다.

정책 보고서

대부분의 정책에 대해 두 종류의 보고서를 생성할 수 있습니다. 보고서 목록은 두 정책 간 차이를 비교하는 반면, 단일 정책에 대한 보고서는 정책에 현재 저장된 설정의 세부 정보를 제공합니다. 상태를 제외한 모든 정책 유형에 대한 단일 정책 보고서를 생성할 수 있습니다.

참고 침입 정책 보고서는 기본 정책 설정과 정책 레이어의 설정을 결합하며 기본 정책 또는 정책 레이어 중 기반이 되는 설정이 무엇인지 구분하지 않습니다.

현재 정책 보고서 생성

특정 정책에 대한 액세스 권한 및 필요한 라이선스가 있고 정책을 설정하기 위한 올바른 도메인에 있는 경우에만 정책을 생성할 수 있습니다.

프로시저

단계 **1** 보고서를 생성할 정책의 관리 페이지에 액세스합니다.

- 액세스 제어 —**Policies(**정책**)** > **Access Control(**액세스 제어**)**
- DNS—**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**
- 파일 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)**
- 상태 — **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)**
- ID — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)**
- 침입 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**
- 7000 및 8000 Series 디바이스용 NAT — **Devices(**디바이스**)** > **NAT**
- 네트워크 분석 — **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**

  참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

- SSL — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**

단계 **2** 보고서를 생성하려는 정책 옆에 있는 보고서( )를 클릭합니다.

만료된 정책

The Firepower System marks out-of-date policies with red status text that indicates how many of its targeted devices need a policy update. 이 상태를 지우려면 다시 디바이스에 정책을 구축 해야 합니다.

Configuration changes that require a policy re-deploy include:

- 액세스 제어 정책을 수정하는 경우: 액세스 제어 규칙, 기본 작업, 정책 대상, 보안 인텔리전스 필터링, 전처리를 포함한 고급 옵션 등의 모든 변경 사항
- 액세스 제어 정책이 호출하는 모든 정책을 변경하는 경우: SSL 정책, 네트워크 분석 정책, 침입 정책, 파일 정책, ID 정책 또는 DNS 정책
- 액세스 제어 정책 또는 호출 정책에 사용된 재사용 가능한 개체 또는 구성의 변경:
  - 네트워크, 포트, VLAN 태그, URL 및 지리위치 개체
  - 보안 인텔리전스 목록 및 피드
  - 애플리케이션 필터 또는 탐지기
  - 침입 정책 변수 집합
  - 파일 목록
  - 암호 해독 관련 개체 및 보안 영역
- 시스템 소프트웨어, 침입 규칙 또는 취약성 데이터베이스(VDB)의 업데이트

웹 인터페이스 내 여러 위치에서 이러한 구성 중 일부를 변경할 수 있다는 점에 주의하십시오. 예를 들어, 개체 관리자(**Objects(**개체**)** > **Object Management(**개체 관리**)**)를 사용하여 보안 영역을 수정할 수 있습니다. 그러나, 디바이스의 구성(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**)에서 인터페이스 유형을 수정하면 영역도 변경될 수 있으며 정책 재구축이 필요합니다.

참고로 다음 업데이트에는 정책 재구축이 필요하지 않습니다.

- 보안 인텔리전스 피드에 대한 자동 업데이트 그리고 컨텍스트 메뉴를 사용하여 보안 인텔리전스 차단 또는 차단 금지 목록에 추가
- URL 필터링 데이터에 대한 자동 업데이트
- 예약된 GeoDB(지정학적 위치 데이터베이스) 업데이트

제한된 구축에 대한 성능 고려 사항

호스트, 애플리케이션, 사용자 검색 데이터는 시스템이 네트워크 전체의 최신 프로파일을 생성하도록 허용합니다. 또한 시스템은 침입 및 공격 네트워크 트래픽을 분석하고 선택적으로 공격 패킷을 제거하는 침입 탐지 및 예방 시스템(IPS)으로 작용합니다.

검색 및 IPS를 결합하면 네트워크 활동에 대한 컨텍스트를 제공하며 다음과 같은 다양한 기능을 활용할 수 있습니다.

- 영향 플래그 및 보안 침해 지표는 특정 익스플로잇, 공격, 악성코드에 취약한 호스트가 무엇인지 나타냅니다
- 적응형 프로파일 Firepower 권장 사항은 대상 호스트에 따라 트래픽을 다른 방법으로 검사할 수 있습니다
- 상관관계는 영향을 받은 호스트에 따라 침입(및 기타 이벤트)에 다른 방식으로 대응합니다

그러나 조직이 IPS 수행 또는 검색 수행에만 관심이 있는 경우 다음 설정으로 시스템의 설정을 최적화할 수 있습니다.

침입 방지 없이 검색

검색 기능은 네트워크 트래픽을 모니터링하고 네트워크의 (네트워크 디바이스를 포함한) 호스트 유형 개수 및 운영 시스템, 활성 애플리케이션, 해당 호스트에 개방된 포트 정보를 확인할 수 있습니다. 또한 네트워크의 사용자 활동을 모니터링하도록 관리되는 디바이스를 구성할 수 있습니다. 검색 데이터를 사용해 트래픽 프로파일링을 수행하고 네트워크 규정 준수를 평가하고 정책 위반에 대응할 수 있습니다.

기본 구축(검색 및 단순한 네트워크 기반 액세스 제어만 수행)의 경우 액세스 제어 정책을 구성할 때 몇 가지 중요 지침을 따름으로서 디바이스의 성능을 향상할 수 있습니다.

참고 모든 트래픽을 허용하는 경우에도 액세스 제어 정책을 사용해야 합니다. 네트워크 검색 정책은 액세스 제어 정책이 통과를 허용하는 트래픽에 한해서만 검사할 수 있습니다.

우선 액세스 제어 정책에 복잡한 프로세스가 필요하지 않으며 단순한 네트워크 기반 조건을 사용하여 네트워크 트래픽을 처리할 수 있는지 확인합니다. 다음 지침을 모두 시행해야 합니다. 이런 옵션 중 하나의 구성 오류가 발생할 경우 성능 이점이 사라집니다.

- 보안 인텔리전스 기능을 사용하지 마십시오. 정책의 보안 인텔리전스 설정에서 생성된 전역 차단 또는 차단 금지 목록을 제거합니다.
- 차단 활동을 모니터링하거나 상호 작용과 관련된 액세스 제어 규칙을 포함하지 마십시오. 허용되고 신뢰할 수 있는 차단 규칙만 사용합니다. 허용된 트래픽은 검색을 통해서만 검사할 수 있으며 신뢰할 수 있는 차단된 트래픽은 검사할 수 없습니다.
- 애플리케이션, 사용자, URL, ISE 속성, 위치 정보에 기반한 네트워크 조건과 관련된 제어 규칙을 포함하지 않습니다. 단순한 네트워크 기반 조건인 영역, IP 주소, VLAN 태그, 포트만 사용합니다.
- 파일, 악성코드, 침입 검사를 수행하는 액세스 제어 규칙을 포함하지 않습니다. 즉 파일 또는 침입 정책을 액세스 제어 규칙과 연결하지 마십시오.

- 액세스 제어 정책의 Advanced(고급) 설정에서 **Access Control(**액세스 제어**)** 규칙이 결정되기 전에 사용되는 Intrusion Policy(침입 정책)가 **No Rules Active(**활성 규칙 없음**)**로 설정되어 있는지 확인합니다.
- **Network Discovery Only(**네트워크 검색만**)**를 정책의 기본 활동으로 선택합니다. 침입 검사를 수행하는 정책을 기본 활동으로 선택하지 않습니다.

액세스 제어 정책을 결합하면 시스템이 세그먼트, 포트, 영역에서 발견된 검색 데이터, 호스트, 애플리케이션, 사용자에 대한 검색을 수행하는 네트워크 세그먼트, 포트, 영역을 특정하는 네트워크 검색 정책을 설정하고 구축할 수 있습니다.

관련 항목

트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지

검색 없이 침입 방지

필요하지 않을 경우 (IPS 전용 구축 등) 검색을 비활성화하면 성능을 향상시킬 수 있습니다. 검색을 비활성화하려면 다음의 모든 변경 사항을 구현해야 합니다.

- 네트워크 검색 정책의 모든 규칙을 삭제합니다.
- 영역, IP 주소, VLAN 태그, 포트의 액세스 제어를 수행하는 단순한 네트워크 기반 조건만 사용합니다.

  모든 유형의 어플리케이션, 사용자, URL, 지리 위치 제어, 보안 인텔리전스를 수행하지 마십시오. 검색 데이터의 스토리지를 비활성화할 수 있지만 시스템은 이런 기능을 수행하기 위해 수집 및 검사를 수행합니다.
- 기본 전역 목록을 포함해 액세스 제어 정책의 보안 인텔리전스 설정에서 모든 차단 및 차단 안 함 목록을 삭제하면 네트워크 및 URL 기반 보안 인텔리전스를 비활성화합니다.
- DNS 규칙에 대해 DNS 및 전역 차단 목록에 대한 기본 전역 차단 안 함 목록을 포함해 DNS 정책과 관련된 모든 규칙을 삭제 또는 비활성화하여 DNS 기반 보안 인텔리전스를 비활성화합니다.

구축 후 대상 디바이스에서 새 검색을 중지합니다. 시스템은 시간 초과 환경 설정에 따라 네트워크 맵에서 점진적으로 정보를 삭제합니다. 또는 사용자가 모든 데이터를 즉시 제거할 수 있습니다.

정책 관리 히스토리

기능	버전	세부 사항
FTD 디바이스의 롤백 구축	6.7	롤백은 FTD 디바이스에서 기존 구축을 제거하고 이전에 구축한 구성으로 디바이스를 재구성하기 위해 제공되는 구축 기능입니다. New/modified(신규 / 수정) 페이지: **Deploy(**구축**)** > **Deployment History(**구축 히스토리**)** 페이지에 롤백 아이콘이 있는 새로운 롤백 열이 제공됩니다. 작업이 확장되어도 디바이스 레벨에서 롤백을 시작하기 위해 유사한 롤백 아이콘을 찾을 수 있습니다. 지원되는 플랫폼: Firepower Management Center

기능	버전	세부 사항
Firepower Management Center의 구축 섹션을 개정합니다.	6.6	

기능	버전	세부 사항
		FMC 메뉴 모음의 **Deploy(**구축**)** 버튼이 **Deploy(**구축**)** 메뉴로 변경됩니다. 그 아래에는 2개의 새로운 하위 메뉴 옵션이 있습니다. 이들은 **Deployment(**구축**)** 및 **Deployment History(**구축 히스토리**)**입니다. 새로 구축된 기능과 함께 구축 페이지가 개선되었으며, 새로운 구축 히스토리 페이지에서는 모든 이전 구축의 범례를 제공합니다. 구축 페이지에는 다음과 같은 기능이 새로 추가되었습니다. • 구축 상태-구축 페이지의 Status(상태) 열에서 각 디바이스의 구축 상태를 제공합니다. • 구축 견적-디바이스, 정책 또는 구성을 선택한 후 구축 페이지에서 견적 링크를 사용할 수 있습니다. 견적 링크를 한 번 클릭하면 구축 기간의 견적이 제공됩니다. • 구축 미리보기-미리보기는 디바이스에 구축할 모든 정책 및 개체 변경 사항의 스냅샷을 제공합니다. 정책 변경 사항에는 새 정책, 기존 정책의 변경 사항 및 삭제된 정책이 포함됩니다. 개체 변경 사항에는 정책에 사용되는 추가 및 수정된 개체가 포함됩니다. • 선택적 정책 구축-FMC를 사용하면 구축해야 하는 디바이스의 모든 변경 사항 목록에서 특정 정책을 선택하고 선택한 정책만 구축할 수 있습니다. 지원되는 플랫폼: Firepower

기능	버전	세부 사항
		Management Center

21 장

규칙 관리: 일반 특성

다음 주제에서는 Firepower Management Center의 다양한 정책에 있는 규칙의 일반 특성을 관리하는 방법에 대해 설명합니다.

- 규칙 관리 요구 사항 및 사전 요건, 523 페이지
- 규칙 소개, 524 페이지
- 규칙 조건 유형, 525 페이지
- 날짜 및 시간 기준 규칙 적용, 551 페이지
- 규칙 검색, 551 페이지
- 디바이스별 규칙 필터링, 552 페이지
- 문제가 있는 규칙 식별, 553 페이지
- 규칙 및 기타 정책 경고, 554 페이지
- 규칙 관리 기록: 일반 특성, 555 페이지

규칙 관리 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

규칙 소개

다양한 정책의 규칙은 네트워크 트래픽에 대해 세분화된 제어를 시행합니다. 시스템은 사용자가 지정한 순서에 따라 첫 번째 일치 알고리즘을 사용해 규칙에 대한 트래픽을 평가합니다.

이러한 규칙은 다음과 같은 기본 특성 및 설정 메커니즘을 공유하는 일치하지 않는 정책 간의 다른 설정을 포함할 수 있습니다.

- 조건: 규칙 조건은 각 규칙을 처리하는 특정 트래픽을 지정합니다. 규칙마다 여러 조건을 구성할 수 있습니다. 트래픽은 규칙과 일치하는 모든 조건과 일치해야 합니다.
- 작업: 규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 규칙에 선택할 수 있는 작업 목록이 포함되지 않더라도 규칙과 관련된 작업이 있습니다. 예를 들어 사용자 지정 네트워크 분석 규칙은 "작업"으로 네트워크 분석 정책을 사용합니다. 다른 예로 모든 QoS 규칙이 동일하게 제한 트래픽을 평가하므로 QoS 규칙에는 명시적인 작업이 없습니다
- 위치: 규칙의 위치는 평가 순서를 결정합니다. 트래픽 평가에 정책을 사용할 경우 시스템은 트래픽이 사용자가 지정한 순서에 따른 규칙과 일치하는지 확인합니다. 일반적으로 시스템은 모든 규칙 조건이 트래픽과 일치하는 첫 번째 규칙에 따라 트래픽을 처리합니다. (추적 및 기록용인 모니터링 규칙은 예외입니다.) 적절한 규칙 순서는 네트워크 트래픽 처리에 필요한 리소스를 줄여 규칙 선점을 방지합니다.
- 범주: 일부 규칙 유형을 구조화하기 위해 각 상위 정책에서 사용자 지정 규칙 카테고리를 만들 수 있습니다.
- 로깅: 많은 규칙의 경우 로깅 설정은 규칙에 의해 처리되는 시스템 로그 연결 여부 및 그 방법을 제어합니다. 규칙이 최종 연결 속성을 결정하거나 특별히 연결을 기록하도록 되어있지 않으므로 일부 규칙(ID 및 네트워크 분석 규칙 등)은 로깅 설정을 포함하지 않습니다. 다른 예로 QoS 규칙은 로깅 설정을 포함하지 않습니다. 속도 제한이 있으므로 연결 기록을 할 수 없습니다.
- 설명: 일부 규칙 유형은 변경 사항을 저장할 때마다 설명을 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다.

팁 여러 정책 편집기의 오른쪽 클릭 메뉴는 편집, 삭제, 이동, 활성화 및 비활성화를 비롯해 많은 규칙 관리 옵션에 대한 바로 가기를 제공합니다.

공유 특성이 포함된 규칙

이 장에서 다음 규칙 및 구성에 대한 여러 공통 측면을 다룹니다. 비공유 설정에 대한 내용은 다음을 참조하십시오.

- 액세스 제어 규칙: 액세스 제어 규칙, 1645 페이지
- SSL 규칙: TLS/SSL 규칙 생성 및 수정, 1810 페이지
- DNS 규칙: DNS 규칙 생성 및 편집, 1714 페이지

- ID 규칙: ID 규칙 생성, 2531 페이지
- 네트워크 분석 규칙: 네트워크 분석 규칙 설정, 2206 페이지
- QoS 규칙: QoS 규칙 구성, 883 페이지
- IAB(Intelligent Application Bypass): IAB(Intelligent Application Bypass), 1745 페이지
- 애플리케이션 필터: 애플리케이션 필터, 574 페이지

공유 속성 없는 규칙 -

이 장에 설명되지 않은 설정 규칙은 다음과 같습니다.

- 침입 규칙: 규칙을 사용하여 침입 정책 조정, 2007 페이지
- 파일 및 악성코드 규칙: 파일 규칙, 1885 페이지
- 상관관계 규칙: 상관관계 규칙 설정, 2587 페이지
- NAT 규칙(기본): 7000 및 8000 Series 디바이스용 NAT
- NAT 규칙(Firepower Threat Defense): Firepower Threat Defense용 NAT(네트워크 주소 변환), 1487 페이지
- 8000 Series 빠른 경로(Fast-Path) 규칙: 빠른 경로 규칙(8000 Series) 설정, 347 페이지

규칙 조건 유형

다음 표에는 이 장에 나오는 일반 규칙 조건이 설명되어 있으며, 이러한 조건이 사용되는 컨피그레이션이 나열되어 있습니다.

조건	트래픽 제어 기준	지원되는 규칙/컨피그레이션
보안 영역 조건, 528 페이지	소스 및 대상 보안 영역	액세스 제어 규칙 SSL 규칙 DNS 규칙 ID 규칙 네트워크 분석 규칙

조건	트래픽 제어 기준	지원되는 규칙/컨피그레이션
네트워크 조건, 530 페이지	소스 및 대상 IP 주소, (지원되는 경우) 지리위치	액세스 제어 규칙 SSL 규칙 DNS 규칙 ID 규칙 네트워크 분석 규칙 QoS 규칙
VLAN 조건, 531 페이지	VLAN 태그	액세스 제어 규칙 참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. 방화벽 인터페이스에 적용된 액세스 규칙에는 사용할 수 없습니다. SSL 규칙 DNS 규칙 ID 규칙 네트워크 분석 규칙
포트 및 ICMP 코드 조건, 532 페이지	소스 및 대상 포트, 프로토콜, ICMP 코드	액세스 제어 규칙 SSL 규칙 ID 규칙 QoS 규칙
애플리케이션 조건(애플리케이션 컨트롤), 535 페이지	애플리케이션 또는 애플리케이션 특성(유형, 위험, 사업 타당성, 카테고리 및 태그)	액세스 제어 규칙 SSL 규칙 ID 규칙 QoS 규칙 애플리케이션 필터 IAB(Intelligent Application Bypass)
URL 조건(URL 필터링), 545 페이지	URL, 지원되는 영역, URL 특성(카테고리 및 평판)	액세스 제어 규칙 SSL 규칙 QoS 규칙

조건	트래픽 제어 기준	지원되는 규칙/컨피그레이션
사용자, 영역 및 ISE 속성 조건(사용자 제어), 545 페이지	호스트의 로그인한 권한 있는 사용자 또는 사용자의 영역, 그룹 또는 ISE 속성	액세스 제어 규칙 SSL 규칙(ISE 속성 없음) QoS 규칙

규칙 조건 메커니즘

규칙 조건은 각 규칙이 처리하는 트래픽을 지정합니다. 다양한 조건에 맞는 각 규칙을 설정하고 트래픽은 규칙과 일치하는 모든 조건에 일치해야 합니다. 사용할 수 있는 조건 유형은 규칙 유형에 따라 다릅니다.

규칙 편집기에는 각 조건 유형의 탭이 있습니다. 일치시키려는 트래픽 속성을 선택하여 조건을 구성합니다. 일반적으로 왼쪽에서 하나 또는 두 목록의 사용 가능한 항목 중 기준을 선택한 뒤 해당 기준을 오른쪽에서 선택한 하나 또는 두 항목의 조건에 추가하거나 결합합니다. 예를 들어 액세스 제어 규칙의 URL 조건에서 URL 카테고리와 평판 기준을 결합하여 블록할 단일 웹 사이트 그룹을 생성할 수 있습니다.

조건을 구축하기 위해 영역, ISE 속성, 다양한 유형의 개체 및 개체 그룹을 포함해 시스템이 제공하는 다양한 사용자 지정 설정을 사용해 트래픽을 일치시킬 수 있습니다. 종종 사용자가 수동으로 규칙 기준을 지정할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

⚠

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

소스 및 대상 기준

소스 및 대상 기준(영역, 네트워크, 포트)과 관련된 규칙의 경우 일반적으로 둘 중 하나 또는 두 제약 기준 모두를 사용할 수 있습니다. 두 제약 기준 모두를 사용하는 경우 일치하는 트래픽은 지정된 소스 영역, 네트워크, 포트 중 하나에서 생성되고 대상 영역, 네트워크, 포트를 통과해야 합니다.

조건당 항목

각 조건에 최대 50개의 항목을 추가할 수 있습니다. 소스 및 대상 기준 규칙은 각각 최대 50개까지 사용할 수 있습니다. 선택된 항목과 일치하는 트래픽은 조건과 일치해야 합니다.

간단한 규칙 메커니즘

규칙 편집기에서 다음과 같은 일반적인 선택을 할 수 있습니다. 조건 구성에 대한 자세한 지침은 각 조건 유형에 대한 항목을 참고하십시오.

- 항목 선택 - 항목을 클릭하거나 해당 항목의 확인란을 선택합니다. Ctrl 또는 Shift를 사용해 여러 항목을 선택하거나 모두 선택하려면 오른쪽 클릭을 사용할 수 있습니다.
- 검색 - 검색 필드에 기준을 입력합니다. 입력하면 항목이 업데이트됩니다. 시스템은 항목 이름 및 개체, 개체 그룹, 그 값을 검색합니다. 다시 로드( ) 또는 지우기( )을 클릭하여 검색 내용을 삭제합니다.
- 사전 정의된 항목 추가 - 하나 이상의 사용 가능한 항목을 선택한 후 추가 버튼을 클릭하거나 드래그 앤 드롭을 사용합니다. 시스템은 중복, 유효하지 않은 조합 등 유효하지 않은 항목을 추가하지 않도록 방지합니다.
- 직접 항목 추가 - 선택한 항목 목록의 필드를 클릭하고 유효한 값을 입력한 뒤 추가를 클릭합니다. 포트를 추가하는 경우 드롭다운 목록에서 프로토콜을 선택할 수도 있습니다.
- 개체 생성 - 추가( )을 클릭하여 구성 중인 조건에 즉시 사용할 수 있는 새롭거나 재사용할 수 있는 개체를 생성하고 개체 관리자에서 관리할 수 있습니다. 상황에 따라 애플리케이션 필터를 추가하기 위해 이 방법을 사용할 경우 다른 사용자 생성 필터를 포함하는 필터를 저장할 수 없습니다.
- 삭제 - 한 항목을 삭제하는 경우 삭제( )을 클릭하거나 선택한 항목 삭제를 하려는 경우 오른쪽 클릭으로 하나 이상의 항목을 선택합니다.

보안 영역 조건

보안 영역은 네트워크를 세그멘테이션화하여 여러 디바이스에 걸쳐 인터페이스를 그룹화하는 방법을 통해 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다.

영역 규칙의 조건은 소스 및 대상 보안 영역을 통해 트래픽을 제어합니다. 소스 및 대상 영역 모두 영역 조건에 추가할 경우 소스 영역 중 하나의 인터페이스에서 트래픽 매치를 시작하고 대상 영역 중 하나의 인터페이스에서 종료해야 합니다.

영역의 모든 인터페이스가 동일한 유형이어야 하는 것과 마찬가지로(모든 인라인, 수동, 스위칭, 라우팅 또는 ASA FirePOWER), 영역 조건에 사용된 모든 영역도 동일한 유형이어야 합니다. 패시브 방식으로 구축된 디바이스는 트래픽을 전송하지 않으므로 패시브 인터페이스를 대상 영역으로 하면서 영역을 사용할 수 없습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

팁 영역으로 규칙을 제한하는 것은 시스템 성능을 개선할 수 있는 가장 좋은 방법 중 하나입니다. 규칙이 디바이스의 인터페이스를 통과하는 트래픽에 적용되지 않을 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

보안 영역 조건 및 멀티테넌시

다중 도메인 구축에서, 상위 도메인에 생성된 영역은 다른 도메인의 디바이스에 있는 인터페이스를 포함할 수 있습니다. 하위 도메인의 영역 조건을 구성할 경우, 컨피그레이션은 사용자가 볼 수 있는 인터페이스에만 적용됩니다.

보안 영역 조건이 포함된 규칙

다음 규칙은 보안 영역 조건을 지원합니다.

- 액세스 제어
- SSL
- DNS(소스 영역 제약 조건만)
- ID
- 네트워크 분석

예: 보안 영역을 사용한 액세스 제어

호스트에 인터넷에 대한 무제한 액세스를 허용하더라도 수신 트래픽에서 침입 및 악성코드를 검사하여 호스트를 보호하는 경우의 구축을 고려하십시오.

우선, 내부 및 외부의 보안 영역 2개를 생성합니다. 그런 다음, 하나 이상의 디바이스에 있는 인터페이스 쌍을 이러한 영역에 할당합니다. 각 쌍의 인터페이스 하나는 내부 영역에, 다른 인터페이스 하나는 외부 영역에 할당합니다. 내부에서 네트워크에 연결된 호스트는 보호된 자산을 나타냅니다.

참고 모든 내부 (또는 외부) 인터페이스를 단일 영역으로 그룹화할 필요는 없습니다. 구축 및 보안 정책에 알맞은 그룹화를 선택합니다.

그런 다음 대상 영역 조건을 Internal로 설정한 액세스 제어 규칙을 구성합니다. 이 단순한 규칙은 내부 영역 내의 모든 인터페이스에서 디바이스를 나가는 트래픽과 일치됩니다. 일치하는 트래픽에서 침입 및 악성코드를 검사하려면 **Allow(**허용**)** 규칙 작업을 선택한 다음 해당 규칙을 침입 및 파일 정책과 연결합니다.

네트워크 조건

네트워크 규칙 조건은 내부 헤더를 사용하여 트래픽의 소스 및 대상 IP 주소를 기준으로 삼아 트래픽을 제어합니다. 외부 헤더를 사용하는 터널 규칙에는 네트워크 조건 대신 터널 엔드포인트 조건이 있습니다.

사전 정의된 개체를 사용하여 네트워크 조건을 작성하거나, 수동으로 개별 IP 주소 또는 주소 블록을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

네트워크 조건의 지리위치

어떤 규칙은 소스 또는 대상의 지리위치 정보를 사용하여 트래픽을 매치할 수 있습니다. 규칙 유형이 지리위치를 지원할 경우, 네트워크와 지리위치 기준을 혼합할 수 있습니다. 최신 지리위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(Geolocation Database)를 정기적으로 업데이트하는 것이 좋습니다.

네트워크 조건이 포함된 규칙

규칙 유형	지리위치 제약 조건 지원 여부
액세스 제어	예
SSL	예
DNS(소스 네트워크만)	아니요
Identity(ID)	예
네트워크 분석	아니요

네트워크 조건 구성

프로시저

단계 **1** 규칙 편집기에서 **Networks(**네트워크**)**를 클릭합니다.

단계 **2** **Available Networks(**사용 가능한 네트워크**)** 목록에서 추가하려는 사전 정의된 네트워크를 찾아 선택합니다.

규칙이 지리위치를 지원할 경우 네트워크와 지리위치 기준을 동일 규칙에 병합할 수 있습니다.

- 네트워크 - 네트워크를 선택하려면 **Networks(**네트워크**)**를 클릭합니다.
- 지리위치 - 지리위치 개체를 선택하려면 **Geolocation(**지리위치**)**를 클릭합니다.

단계 **3** **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**를 클릭하거나 드래그 앤 드롭을 사용합니다.

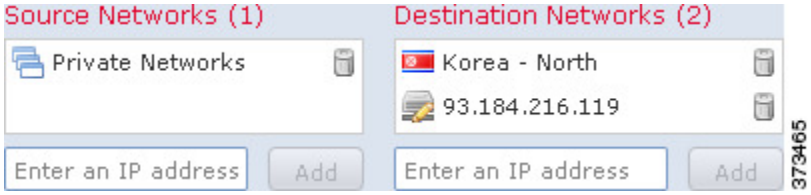
단계 **4** 수동 지정을 원하는 네트워크를 추가합니다. 소스 또는 대상 IP 주소 또는 주소 블록을 입력하고 추가를 클릭합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

예: 액세스 제어 규칙의 네트워크 조건

다음 그림은 사용자의 내부 네트워크에서 시작해 북한 또는 93.184.216.119(example.com)의 리소스에 액세스를 시도하는 연결을 차단하는 액세스 제어 규칙에 대한 네트워크 조건을 보여줍니다.



이 예에서 (보이지 않는 IPv4 및 IPv6 Private Networks 네트워크 개체로 구성된) Private Networks라는 네트워크 개체 그룹은 사용자의 내부 네트워크를 나타냅니다. 또한 이 예에서는 example.com의 IP 주소를 수동으로 특정하고 북한 IP 주소를 대신해 시스템이 제공한 북한 지리위치 개체를 사용합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

VLAN 조건

VLAN 규칙 조건은 Q-in-Q(스택 VLAN) 트래픽을 포함한 VLAN 태그가 있는 트래픽을 제어합니다. 시스템은 가장 안쪽의 VLAN 태그를 사용하여 VLAN 트래픽을 필터링하며.

다음 Q-in-Q 지원에 유의하십시오.

- NGIPSv, Firepower 7000, Firepower 8000 - 모든 인터페이스 유형에 Q-in-Q를 지원합니다.

- ASA FirePOWER 모듈 - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- Firepower 4100/9300의 FTD - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- 기타 모든 모델의 FTD:
  - 인라인 집합 및 패시브 인터페이스 - Q-in-Q를 지원합니다(최대 2개의 VLAN 태그 지원).
  - 방화벽 인터페이스 - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).

사전 정의된 개체를 사용하여 VLAN 조건을 작성하거나, **1**에서 **4094** 사이의 VLAN 태그를 수동으로 입력할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

최대 50개의 VLAN 조건을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

VLAN 조건이 포함된 규칙

다음 규칙 유형은 VLAN 조건을 지원합니다.

- 액세스 제어

  참고 , 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. 방화벽 인터페이스에 적용된 액세스 규칙에는 사용할 수 없습니다.

- SSL
- DNS
- ID
- 네트워크 분석

포트 및 ICMP 코드 조건

포트 조건을 사용하면 소스 및 대상 포트를 기준으로 트래픽을 제어할 수 있습니다. 규칙 유형에 따라, "포트"는 다음 중 하나를 나타낼 수 있습니다.

- TCP 및 UDP — 전송 레이어 프로토콜을 기준으로 TCP 및 UDP 트래픽을 제어할 수 있습니다. 시스템은 괄호 내 프로토콜 번호와 선택적으로 결합된 포트 또는 포트 범위를 사용하여 이 구성을 나타냅니다. 예: TCP(6)/22

- ICMP — 인터넷 레이어 프로토콜과 선택적 유형 및 코드에 따라 ICMP 및 ICMPv6(IPv6-ICMP) 트래픽을 제어할 수 있습니다. 예: ICMP(1):3:3
- 포트 없음 — 포트를 사용하지 않는 다른 프로토콜을 사용하여 트래픽을 제어할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

포트 기반 규칙 모범 사례

포트를 지정하는 것은 애플리케이션을 대상으로 하는 기존의 방법입니다. 그러나 고유한 포트를 사용하여 액세스 제어 블록을 우회하도록 애플리케이션을 설정할 수 있습니다. 따라서 트래픽을 대상으로 지정하려면 가능한 경우 항상 포트 기준 대신 애플리케이션 필터링 기준을 사용하십시오.

FTD와 같이 제어와 데이터 흐름을 위해 별도의 채널을 동적으로 여는 애플리케이션에도 애플리케이션 필터링이 권장됩니다. 포트 기반 액세스 제어 규칙을 사용하면 이러한 종류의 애플리케이션이 올바르게 작동하지 못하게 되어 적절한 연결이 차단될 수 있습니다.

소스 및 대상 포트 제약 조건 사용

소스 및 대상 포트 제약 조건을 모두 추가할 경우 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어, 소스 포트로 DNS over TCP를 추가한 경우, 대상 포트에 Yahoo 메신저 음성 채팅(TCP)을 추가할 수 있지만 Yahoo 메신저 음성 채팅(UDP)은 해당되지 않습니다.

소스 포트만 또는 대상 포트만 추가할 경우 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어, DNS over TCP 및 DNS over UDP 모두를 단일 액세스 제어 규칙의 소스 포트 조건으로 추가할 수 있습니다.

비 **TCP** 트래픽을 포트 조건과 일치

비 TCP 트래픽과 일치하도록 포트 조건을 구성할 수 있지만, 몇 가지 제한 사항이 있습니다.

- 액세스 제어 규칙 - GRE(47) 프로토콜을 대상 포트 조건으로 사용하는 방법으로 GRE 캡슐화 트래픽을 액세스 제어 규칙과 매치할 수 있습니다. GRE 제한 규칙에는 네트워크 기반 조건(영역, IP 주소, 포트, VLAN 태그)만 추가할 수 있습니다. 또한, 시스템은 외부 헤더를 사용하여 액세스 제어 정책의 모든 트래픽을 GRE 제한 규칙과 일치시킵니다.
- SSL 규칙 — SSL 규칙은 TCP 포트 조건만 지원합니다.

- ⚠

  주의 SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거함 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

  액티브 인증 규칙에는 **Active Authentication(**액티브 인증**)** 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)**가 선택된 **Passive Authentication(**패시브 인증**)** 규칙 작업이 있음에 유의하십시오.

- IMCP 에코 - 대상 ICMP 포트의 유형이 0으로 설정되었거나 대상 ICMPv6 포트의 유형이 129로 설정된 경우 요청하지 않은 에코 응답만 매치합니다. ICMP 에코 요청에 대한 응답으로 전송된 ICMP 에코 응답은 무시됩니다. 모든 ICMP 에코에 일치하는 규칙의 경우, ICMP 유형 8 또는 ICMPv6 유형 128을 사용합니다.

포트 조건이 포함된 규칙

다음 규칙은 포트 조건을 지원합니다.

- 액세스 제어
- SSL(TCP 트래픽만 지원)
- ID(액티브 인증은 TCP 트래픽만 지원)
- QoS

포트 조건 구성

프로시저

단계 **1** 규칙 편집기에서 **Ports(**포트**)**를 클릭합니다.

단계 **2** **Available Ports(**사용 가능한 포트**)** 목록에서 추가하려는 사전 정의된 포트를 찾아 선택합니다.

단계 **3** **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**을 클릭하거나 끌어서 놓습니다.

단계 **4** 직접 지정하려는 소스 포트 또는 대상 포트를 추가합니다.

- 소스—프로토콜을 선택하고 0 ~ 65535 범위에서 단일 포트를 입력한 다음 **Add(**추가**)**를 클릭합니다.
- 대상(비 ICMP)—프로토콜을 선택하거나 입력합니다. 프로토콜을 지정하고 싶지 않거나 **TCP** 또는 **UDP**를 선택할 경우 0 ~ 65535 범위에서 단일 포트를 입력합니다. **Add(**추가**)**를 클릭합니다.

- 대상(ICMP)— **Protocol(프로토콜)** 드롭다운 목록에서 **ICMP** 또는 **IPv6-ICMP**를 선택한 다음 팝업 창이 나타나면 유형 및 코드를 선택합니다. ICMP 유형 및 코드에 대한 자세한 내용은 IANA(Internet Assigned Numbers Authority) 웹사이트를 참조하십시오.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

애플리케이션 조건(애플리케이션 컨트롤)

시스템에서 IP 트래픽을 분석할 때, 사용자의 네트워크에서 자주 사용되는 애플리케이션을 식별하여 분류할 수 있습니다. 이 검색 기반 애플리케이션 인식은 애플리케이션 컨트롤을 위한 기본 요소로, 애플리케이션 트래픽을 제어하는 기능입니다.

시스템에서 제공되는 애플리케이션 필터는 유형, 위험, 사업 타당성, 카테고리, 태그라는 기본 특성에 따라 애플리케이션을 구성하여 애플리케이션 컨트롤을 수행할 수 있도록 지원합니다. 시스템에서 제공되는 필터를 조합하거나 애플리케이션을 맞춤형으로 조합하여 재사용 가능한 사용자 정의 필터를 생성할 수 있습니다.

정책의 애플리케이션 규칙 조건마다 적어도 하나의 탐지기가 활성화되어야 합니다. 애플리케이션에 탐지기가 활성화되지 않은 경우, 시스템은 시스템에서 제공된 모든 탐지기를 해당 애플리케이션에 자동으로 활성화합니다. 시스템에서 제공된 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 활성화합니다. 애플리케이션 탐지기에 대한 자세한 내용은 애플리케이션 탐지기 기초, 2440 페이지을 참조하십시오.

두 애플리케이션 필터를 모두 사용하거나 개별적으로 지정된 애플리케이션을 사용하여 완전한 커버리지를 보장할 수 있습니다. 그러나 액세스 제어 규칙 순서를 지정하기 전에 다음을 참고하십시오.

⚠

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

애플리케이션 필터의 이점

애플리케이션 필터는 애플리케이션 컨트롤을 신속하게 구성하는 데 도움이 됩니다. 예를 들어 시스템에서 제공되는 필터를 손쉽게 사용하여 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하고 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 시스템에서는 해당 세션을 차단합니다.

애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템이 애플리케이션 트래픽을 정상적으로 제어할 수 있습니다. Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 애플리케이션 탐지기를 자주 업데이트하고 추가하므로, 시스템에서는 최신 탐지기를 사용하여 애플리케이션 트래픽을 모니터링할 수 있습니다. 자체 탐지기를 생성하고 이러한 탐지기로 탐지한 애플리케이션에 특성을 할당할 수도 있으며, 이는 기존 필터에 자동으로 추가됩니다.

애플리케이션 조건이 포함된 컨피그레이션

다음 표의 컨피그레이션은 애플리케이션 컨트롤을 수행하는 데 도움이 됩니다. 이 표에는 컨피그레이션에 따라 애플리케이션 컨트롤을 제한할 수 있는 방법도 나와 있습니다.

컨피그레이션	유형,위험,타당성,카테고리	태그	사용자 정의 필터
액세스 제어 규칙	예	예	예
SSL 규칙	예	아니요. SSL 프로토콜 태그를 통해 암호화된 애플리케이션 트래픽에 자동으로 제한됨	아니요
IID 규칙(액티브 인증에서 애플리케이션을 제외할 목적)	예	아니요. User-Agent Exclusion 태그를 통해 자동으로 제한됨	아니요
개체 관리자의 사용자 정의 애플리케이션 필터	예	예	아니요. 사용자 정의 필터는 중첩할 수 없음
IAB(Intelligent Application Bypass)	예	예	예

관련 항목

개요: 애플리케이션 탐지, 2439 페이지

애플리케이션 조건 및 필터 구성

애플리케이션 조건 또는 필터를 구성하려면 사용 가능한 애플리케이션 목록에서 제어를 원하는 트래픽의 애플리케이션을 선택합니다. 선택적으로(권장 사항), 필터를 사용해 사용 가능한 애플리케이션을 제약합니다. 동일한 조건에서 필터 및 개별적으로 지정된 애플리케이션을 사용할 수 있습니다.

시작하기 전에

- 적응형 프로파일은 애플리케이션 제어를 수행하기 위해 적응형 프로파일 구성, 2374 페이지의 설명대로 액세스 제어 규칙에 대해 반드시 활성화가 되어 있어야 합니다.
- 클래식 디바이스 모델의 경우 이러한 조건을 설정하려면 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** 규칙 또는 구성 편집기를 호출합니다.

- 액세스 제어, SSL, QoS 규칙 조건 - 규칙 편집기에서 **Applications(**애플리케이션**)**을 클릭합니다.
- ID 규칙 조건 - 규칙 편집기에서 **Realms & Settings(**영역 및 설정**)**을 클릭하고 액티브 인증을 활성화하려면 ID 규칙 생성, 2531 페이지를 참조합니다.
- 애플리케이션 필터 - 개체 관리자의 애플리케이션 필터 페이지에서 애플리케이션 필터를 추가하거나 편집합니다. 필터의 고유 이름을 제공합니다.
- 인텔리전트 애플리케이션 우회(IAB) - 액세스 제어 정책 편집기에서 **Advanced(**고급**)**을 클릭하고 IAB 세팅을 편집한 뒤 **Bypassable Applications and Filters(**우회 가능한 애플리케이션 및 필터**)**를 클릭합니다.

단계 **2** **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 추가하려는 애플리케이션을 찾아 선택합니다.

Available Applications(사용 가능한 애플리케이션**)**에 표시된 애플리케이션을 제한하기 위해 하나 이상의 **Application Filters(**애플리케이션 필터**)**를 선택하거나 개별 애플리케이션을 검색합니다.

팁 요약 정보 및 내부 검색 링크를 표시하기 위해 애플리케이션 옆의 정보() 을 클릭합니다. **Unlock(**잠금 해제**)**은 시스템이 암호화된 트래픽에서만 확인할 수 있는 애플리케이션을 표시합니다.

하나 또는 여러 필터를 선택할 때 사용 가능한 애플리케이션 목록은 조건에 맞는 애플리케이션만 표시합니다. 시스템에서 제공된 여러 필터를 선택할 수 있지만 사용자 지정 필터는 선택할 수 없습니다.

- 동일한 속성(위험, 비즈니스 연관성 등)에 대한 여러 필터 - 애플리케이션 트래픽은 하나의 필터에만 일치해야 합니다. 중간 또는 고위험 필터를 선택하는 경우 사용 가능한 애플리케이션 목록은 모든 중간 및 고위험 애플리케이션을 표시합니다.
- 다른 애플리케이션 속성에 대한 필터 - 애플리케이션 트래픽은 두 필터 유형에 모두 일치해야합니다. 예를 들어 고위험 및 비즈니스 연관성이 낮은 필터를 선택하는 경우 사용 가능한 애플리케이션 목록은 두 조건을 모두 만족하는 애플리케이션만을 표시합니다.

단계 **3** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

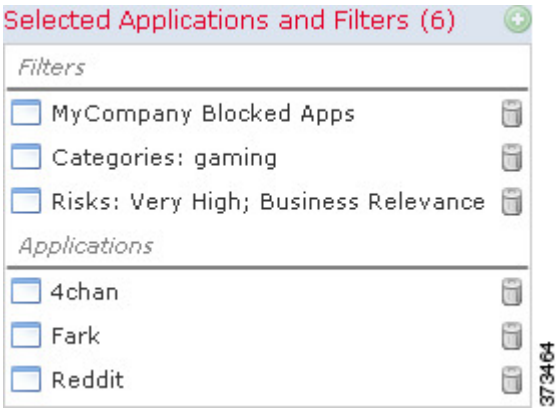
팁 더 많은 필터 및 애플리케이션을 추가하기 전에 현재 선택 사항을 지우려면 **Clear Filters(**필터 지우기**)**를 클릭합니다.

웹 인터페이스는 위의 조건에 추가된 필터 및 개별적으로 추가된 애플리케이션을 표시합니다.

단계 **4** 규칙 또는 설정을 저장하거나 편집합니다.

예: 액세스 제어 규칙의 애플리케이션 조건

다음 그림은 MyCompany, 위험도가 높고 비즈니스 연관성이 낮은 모든 애플리케이션, 게임 애플리케이션, 일부 개별 선택 애플리케이션에 대해 사용자 정의된 애플리케이션 필터를 차단하는 액세스 제어 규칙의 애플리케이션 조건을 표시합니다.



다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

애플리케이션 특성

시스템은 다음 표에서 설명하는 조건을 사용해 탐지하는 각 애플리케이션을 구별합니다. 애플리케이션 필터로 이러한 특성을 사용합니다.

표 ***59:*** 애플리케이션 특성

특성	설명	예
유형	애플리케이션 프로토콜은 호스트 간 통신을 나타냅니다. 클라이언트는 호스트에서 실행 중인 소프트웨어를 나타냅니다. 웹 애플리케이션은 HTTP 트래픽에 대한 콘텐츠 또한 요청 URL을 나타냅니다.	HTTP 및 SSH는 애플리케이션 프로토콜입니다. 웹 브라우저 및 이메일 클라이언트는 클라이언트입니다. MPEG 비디오 및 Facebook은 웹 애플리케이션입니다.
위험	애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성입니다.	피어 투 피어 애플리케이션은 고위험 경향이 있습니다.

특성	설명	예
사업 타당성	애플리케이션이 오락이 아닌 조직의 비즈니스 운영 컨텍스트 내에서 사용될 가능성입니다.	게임 애플리케이션은 비즈니스 연관성이 매우 낮은 경향이 있습니다.
Category(카테고리)	가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.	Facebook은 소셜 네트워킹 카테고리에 포함됩니다.
Tag(태그)	애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.	비디오 스트리밍 웹 애플리케이션은 종종 높은 대역폭 및 광고 표시 태그가 지정됩니다.

애플리케이션 제어 모범 사례

애플리케이션 제어와 관련해서 다음의 지침과 제한 사항에 유의해야 합니다.

애플리케이션 탐지기 자동 활성화

탐지하려는 애플리케이션에 대해 탐지기를 사용하고 있지 않으면 시스템은 해당 애플리케이션에 대해 모든 시스템 제공 탐지기를 자동으로 사용합니다. 시스템 제공 탐지기가 없으면 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 대해 사용합니다.

애플리케이션이 식별되기 전에 통과해야 하는 패킷을 검사하도록 정책 설정

시스템은 다음의 두 가지 조건을 만족하지 않는 경우 인텔리전트 애플리케이션 우회(IAB) 및 속도 제한을 포함한 애플리케이션 제어를 수행할 수 없습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 시스템이 세션에서 애플리케이션 식별

이 식별은 3~5개 패킷 내에서 이루어지거나 트래픽이 암호화된 경우 SSL 핸드셰이크의 서버 인증 교환 이후에 이루어져야 합니다.

중요! 시스템에서 이러한 초기 패킷을 검사하도록 하려면 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정, 2203 페이지의 내용을 참조하십시오.

초기 트래픽이 기타 모든 기준과는 일치하는데 애플리케이션 식별이 불완전한 경우 시스템은 패킷 통과 및 연결 설정 또는 SSL 핸드셰이크 완료를 허용합니다. 시스템은 식별을 완료하면 나머지 세션 트래픽에 적절한 작업을 적용합니다.

URL 및 애플리케이션 필터링용 별도의 규칙 생성

애플리케이션과 URL 기준을 결합하면 특히 암호화된 트래픽에 대해 예기치 않은 결과가 발생할 수 있으므로 가능하면 URL 및 애플리케이션 필터링에 대한 별도의 규칙을 만듭니다.

애플리케이션+URL 규칙이 더 일반적인 애플리케이션 전용 또는 URL 전용 규칙에 대한 예외 역할을 하지 않는 한, 애플리케이션 및 URL 기준을 모두 포함하는 규칙은 애플리케이션 전용 또는 URL 전용 규칙 뒤에 와야 합니다.

애플리케이션 및 기타 규칙 이전의 **URL** 규칙

가장 효과적인 URL 일치를 위해 특히 URL 규칙이 차단 규칙이고 다른 규칙이 다음 조건을 모두 만족하는 경우 다른 규칙 전에 URL 조건을 포함하는 규칙을 배치합니다.

- 애플리케이션 조건을 포함합니다.
- 검사할 트래픽은 암호화되어야 합니다.

암호화된 트래픽과 암호 해독된 트래픽에 대한 애플리케이션 제어

시스템은 암호화된 트래픽과 암호 해독된 트래픽을 식별하고 필터링할 수 있습니다.

- 암호화된 트래픽 - 시스템은 SMTPS, POPS, FTPS, TelnetS, IMAPS를 비롯하여 StartTLS로 암호화된 애플리케이션 트래픽을 탐지할 수 있습니다. 또한, TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서의 주체로 구별되는 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다. 이러한 애플리케이션은 `SSL` 프로토콜 태그가 지정됩니다. SSL 규칙에서는 이런 애플리케이션만 선택할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다.
- 암호 해독된 트래픽 - 시스템은 암호화되거나 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에 `decrypted traffic` 태그를 할당합니다.

TLS 서버 **ID** 검색 및 애플리케이션 제어

RFC 8446에서 정의한 TLS(Transport Layer Security) 프로토콜 1.3의 최신 버전은 보안 통신을 제공하기 위해 많은 웹 서버에서 선호하는 프로토콜입니다. TLS 1.3 프로토콜은 추가 보안을 위해 서버의 인증서를 암호화하며, 액세스 제어 규칙의 애플리케이션 및 URL 필터링 기준과 일치하는 데 인증서가 필요하므로 Firepower System은 전체 패킷의 암호를 해독하지 않고 서버 인증서를 추출하는 방법을 제공합니다.

애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.

자세한 내용은 액세스 제어 정책 고급 설정, 1637 페이지를 참고하십시오.

활성 권한 부여에서 애플리케이션 제외

ID 정책에서는 특정 애플리케이션을 액티브 인증에서 제외하여 트래픽이 액세스 제어로 계속 이동하도록 허용할 수 있습니다. 이러한 애플리케이션에는 `User-Agent Exclusion` 태그가 지정됩니다. ID 규칙에서는 이러한 애플리케이션만 선택할 수 있습니다.

페이로드 없이 애플리케이션 트래픽 패킷 처리

액세스 제어를 수행할 때 시스템은 애플리케이션이 식별된 연결에서 페이로드가 없는 패킷에 기본 정책 작업을 적용합니다.

참조된 애플리케이션 트래픽 처리

광고물 트래픽과 같이 웹 서버에서 참조된 트래픽을 처리하려면 참조하는 애플리케이션이 아닌 참조되는 애플리케이션의 일치 여부를 확인합니다.

다중 프로토콜을 사용하는 애플리케이션**(Skype, Zoho)**의 애플리케이션 트래픽 제어

일부 애플리케이션은 다중 프로토콜을 사용합니다. 해당 트래픽을 제어하려면 액세스 제어 정책이 모든 관련 옵션을 포함하는지 확인합니다. 예를 들면 다음과 같습니다.

- Skype - Skype 트래픽을 제어하려면 개별 애플리케이션을 선택하는 대신 **Application Filters(**애플리케이션 필터**)** 항목에서 **Skype** 태그를 선택합니다. 이렇게 하면 시스템이 동일한 방법으로 모든 Skype 트래픽을 탐지하고 제어할 수 있도록 할 수 있습니다.
- Zoho - Zoho 메일을 제어하려면 사용 가능한 애플리케이션 목록에서 **Zoho** 및 **Zoho mail**을 모두 선택합니다.

콘텐츠 제한 기능용으로 지원되는 검색 엔진

시스템은 특정 검색 엔진에 대해서만 안전 검색 필터링을 지원합니다. 이러한 검색 엔진의 애플리케이션 트래픽에는 `safesearch supported` 태그가 할당됩니다.

우회 애플리케이션 트래픽 제어

애플리케이션 관련 참고 사항 및 제한 사항, 543 페이지의 내용을 참조하십시오.

애플리케이션 제어 순서 지정에 대한 추가 규칙

애플리케이션 제어 순서를 결정하는 규칙에 대한 지침은 애플리케이션 제어 구성 모범 사례, 541 페이지을 참조하십시오.

관련 항목

트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지
애플리케이션 탐지 특별 고려 사항, 2443 페이지

애플리케이션 제어 구성 모범 사례

다음과 같이 네트워크에 대한 애플리케이션의 액세스를 제어하는 것이 좋습니다.

- 보안 수준이 낮은 네트워크에서 보안 수준이 높은 네트워크로 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Port(**포트**)** (Selected Destination Port)(선택한 대상 포트) 조건을 사용합니다.

  예를 들어, 인터넷(보안 수준 낮음)에서 내부 네트워크(보안 수준 높음)으로 ICMP 트래픽을 허용합니다.

- 사용자 그룹의 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Application(**애플리케이션**)** 조건을 사용합니다.

  예를 들어, 계약업체 그룹 구성원의 Facebook 액세스를 차단합니다.

⚠

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

다음 표에서 액세스 제어 규칙을 설정하는 방법에 대한 예시가 제공됩니다.

제어의 유형	조치	영역, 네트워크, **VLAN** 태그	사용자	애플리케이션	포트	**URL**	**SGT/ISE** 속성	검사, 로깅, 코멘트
애플리케이션에서 포트(예: SSH)를 사용하는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow(**허용**)**)	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	사용 가능한 포트: **SSH** **Selected Destination Ports(**선택한 대상 포트**)**에 추가	Any(모든)	ISE/ISE-PIC에만 사용합니다.	Any(모든)
애플리케이션에서 포트(예: ICMP)를 사용하지 않는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow(**허용**)**)	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	선택한 대상 포트 프로토콜: **ICMP** **Type(**유형**)**: **Any (**모든**)**	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	Any(모든)

제어의 유형	조치	영역, 네트워크, **VLAN** 태그	사용자	애플리케이션	포트	**URL**	**SGT/ISE** 속성	검사, 로깅, 코멘트
사용자 그룹의 애플리케이션 액세스	선택(이 예에서는 **Block(**차단**)**)	선택	사용자 그룹(이 예에서는 계약업체 그룹)을 선택합니다.	애플리케이션의 이름(이 예에서는 **Facebook**)을 선택합니다.	설정하지 마십시오.	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	선택

애플리케이션 관련 참고 사항 및 제한 사항

- Office 365 관리자 포털:

  제한 사항: 액세스 정책이 시작 및 종료 시 로깅을 활성화한 경우 첫 번째 패킷은 Office 365로 감지되고 연결 종료는 Office 365 관리자 포털로 감지됩니다. 이는 블로킹에 영향을 주지 않습니다.

- Skype:

  애플리케이션 제어 모범 사례, 539 페이지의 내용을 참조하십시오.

- GoToMeeting

  GoToMeeting을 완벽하게 탐지하려면 규칙에 다음 애플리케이션이 모두 있어야 합니다.

  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting 플랫폼
  - LogMeIn
  - STUN

- Zoho:

  애플리케이션 제어 모범 사례, 539 페이지의 내용을 참조하십시오.

- Bittorrent, Tor, Psyphon, Ultrasurf 등의 우회 애플리케이션:

  우회 애플리케이션의 경우 기본적으로 가장 신뢰도가 높은 시나리오만 인식됩니다. 이 트래픽의 활동(차단 또는 QoS 구현 등)이 필요한 경우 효율성을 높이기 위해 더 적극적인 탐지 설정이 필요합니다. 이런 변경으로 오탐이 발생할 수 있으므로 이 작업을 수행하기 위해서는 설정을 검토하기 위한 TAC에 연결합니다.

- WeChat:

  WeChat을 허용하는 경우 선택적으로 WeChat Media를 차단할 수 없습니다.

애플리케이션 제어 규칙 문제 해결

애플리케이션 제어 규칙이 예상대로 작동하지 않는 경우 이 섹션에서 설명한 지침을 사용합니다.

다음과 같이 네트워크에 대한 애플리케이션의 액세스를 제어하는 것이 좋습니다.

- 보안 수준이 낮은 네트워크에서 보안 수준이 높은 네트워크로 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Port(**포트**)** (Selected Destination Port)(선택한 대상 포트) 조건을 사용합니다.

  예를 들어, 인터넷(보안 수준 낮음)에서 내부 네트워크(보안 수준 높음)으로 ICMP 트래픽을 허용합니다.

- 사용자 그룹의 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Application(**애플리케이션**)** 조건을 사용합니다.

  예를 들어, 계약업체 그룹 구성원의 Facebook 액세스를 차단합니다.

⚠

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

다음 표에서 액세스 제어 규칙을 설정하는 방법에 대한 예시가 제공됩니다.

제어의 유형	조치	영역, 네트워크, **VLAN** 태그	사용자	애플리케이션	포트	**URL**	**SGT/ISE** 속성	검사, 로깅, 코멘트
애플리케이션에서 포트(예: SSH)를 사용하는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow(**허용**)**)	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	사용 가능한 포트: **SSH** **Selected Destination Ports(**선택한 대상 포트**)**에 추가	Any(모든)	ISE/ISE-PIC에만 사용합니다.	Any(모든)

제어의 유형	조치	영역, 네트워크, VLAN 태그	사용자	애플리케이션	포트	URL	SGT/ISE 속성	검사, 로깅, 코멘트
애플리케이션에서 포트(예: ICMP)를 사용하지 않는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow**(허용))	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	선택한 대상 포트 프로토콜: **ICMP** **Type**(유형): **Any**(모든)	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	Any(모든)
사용자 그룹의 애플리케이션 액세스	선택(이 예에서는 **Block**(차단))	선택	사용자 그룹(이 예에서는 계약업체 그룹)을 선택합니다.	애플리케이션의 이름(이 예에서는 **Facebook**)을 선택합니다.	설정하지 마십시오.	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	선택

초기 패킷이 검사되지 않고 통과됨

트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지 및 하위 항목을 참조하십시오.

관련 항목

규칙 순서 지정 모범 사례, 1618 페이지

URL 조건(URL 필터링)

네트워크의 사용자가 액세스할 수 있는 웹 사이트를 제어하기 위해 URL 조건을 사용합니다.

자세한 내용은 URL 필터링, 1665 페이지를 참조하십시오.

사용자, 영역 및 ISE 속성 조건(사용자 제어)

Firepower System에서 수집한 권한 있는 사용자 *ID* 데이터로 사용자 제어를 수행할 수 있습니다.

ID 소스는 로그인 및 로그아웃하는 사용자를 모니터링하거나, 사용자가 Microsoft AD(Active Directory) 또는 LDAP 접속 정보를 사용하여 인증하는 사용자를 모니터링합니다. 그런 다음 이렇게 수집된 ID 데이터를 사용하는 규칙을 구성하여, 모니터링된 호스트와 관련된 로그인한 권한 있는 사용자를 기준으로 트래픽을 처리할 수 있습니다. 사용자가 로그오프하거나(ID 소스를 통해 보고됨), 영역의 세

션 시간이 초과되거나, 시스템의 데이터베이스에서 사용자 데이터를 삭제할 때까지 사용자는 호스트에 계속 연결되어 있습니다.

현재 보유한 버전의 Firepower System에서 지원되는 권한 있는 사용자 ID 소스에 대한 자세한 내용은 사용자 ID 소스 정보를 참조하십시오.

다음 규칙 조건을 사용하여 사용자 제어를 수행할 수 있습니다.

- 사용자 및 영역 조건 — 호스트의 로그인한 권한 있는 사용자를 기준으로 트래픽을 일치시킵니다. 영역, 개별 사용자 또는 해당 사용자가 속한 그룹을 기준으로 트래픽을 제어할 수 있습니다.
- ISE 속성 조건 — 사용자의 ISE 할당 SGT(Security Group Tag), 디바이스 유형(엔드포인트 프로파일이라고도 함) 또는 위치 IP(엔드포인트 위치라고도 함)를 기준으로 트래픽을 일치시킵니다. ISE를 ID 소스로 구성해야 합니다.

참고 ISE-PIC ID 소스는 ISE 속성 데이터를 제공하지 않습니다.

사용자 조건이 포함된 규칙

규칙 유형	사용자 및 영역 조건 지원 여부	**ISE** 속성 조건 지원 여부
액세스 제어	예	예
SSL	예	아니요
QoS	예	예 SGT 매칭은 소스 매칭 기준으로만 지원되며, 대상 일치 기준은 지원되지 않습니다.

관련 항목

ISE/ISE-PIC ID 소스, 2485 페이지
캡티브 포털 ID 소스, 2505 페이지

사용자 제어 사전 요구 사항

ID 소스/인증 방법 구성

수행하려는 인증 유형에 대한 ID 소스를 구성합니다. 자세한 내용은 사용자 ID 소스 정보를 참고하십시오.

여러 사용자 그룹을 모니터링하기 위한 ISE 디바이스를 설정하는 경우, 또는 네트워크의 호스트에 다수의 사용자가 매핑된 경우, 시스템은 Firepower Management Center 사용자 제한에 따라 그룹을 기반으로 한 사용자 매핑이 삭제될 수 있습니다. 그 결과 영역, 사용자, 사용자 그룹 조건의 규칙은 정상적인 트래픽과 일치하지 않을 수 있습니다.

여러 사용자 그룹을 모니터링하기 위한 ISE/ISE/PIC 또는 TS 에이전트, ISE/ISE-PIC 디바이스를 설정하는 경우, 또는 네트워크의 호스트에 다수의 사용자가 매핑된 경우, 시스템은 Firepower Management Center 사용자 제한에 따라 그룹을 기반으로 한 사용자 매핑이 삭제될 수 있습니다. 그 결과 영역, 사용자, 사용자 그룹 조건의 규칙은 정상적인 트래픽과 일치하지 않을 수 있습니다.

영역 설정

ISE 서버를 포함해 모니터링하려는 각 AD 또는 LDAP 서버 영역을 설정하고 사용자 다운로드를 수행합니다. 자세한 내용은 영역 생성, 2466 페이지를 참고하십시오.

ISE/ISE-PIC 및 TS 에이전트 서버를 포함해 모니터링하려는 각 AD 또는 LDAP 서버 영역을 설정하고 사용자 다운로드를 수행합니다. 자세한 내용은 영역 생성, 2466 페이지를 참고하십시오.

영역을 설정할 때 활동을 모니터링할 사용자 및 사용자 그룹을 지정할 수 있습니다. 사용자 그룹을 포함하면 해당 그룹의 모든 멤버(보조 그룹 멤버 포함)가 자동으로 포함됩니다. 그러나 규칙 기준으로 보조 그룹을 사용하려면 영역 설정에 보조 그룹을 명시적으로 포함해야 합니다.

각 영역에 대해 신뢰할 수 있는 사용자 또는 사용자 그룹의 데이터를 새로 고침하거나 사용자 데이터의 자동 다운로드를 활성화할 수 있습니다.

ID 정책 생성

인증 방법과 영역을 연결하고 해당 정책을 액세스 제어와 연결하는 ID 정책을 생성합니다. 자세한 내용은 ID 정책 생성, 2534 페이지를 참고하십시오.

디바이스에 사용자 제어를 수행하는 정책(액세스 제어, SSL, QoS)은 ID 정책을 공유합니다. ID 정책은 해당 디바이스의 트래픽에 영향을 미치는 규칙에서 사용할 수 있는 영역, 사용자, 그룹을 결정합니다.

QoS 규칙에서 사용자 조건을 설정하기 전에 QoS 정책의 대상이 되는 디바이스가 반드시 디바이스가 구축한 액세스 제어 정책에서 정의된 것과 같은 올바른 ID 정책을 사용해야 합니다. 동일한 디바이스에 배포된 QoS 정책 및 액세스 제어 정책이 명시적으로 연결된 것은 아니기 때문에 QoS 규칙 편집기를 사용해 유효하지 않은 영역, 사용자, 그룹을 선택할 수 있습니다. 유효하지 않은 이런 요소는 Firepower Management Center의 ID 정책에는 존재하지만 QoS 대상 디바이스에는 적용되지 않습니다. 이러한 요소를 사용하는 경우 시스템은 구축 시간 이전에 사용자가 유효하지 않은 선택을 했는지 식별할 수 없습니다.

사용자 및 영역 조건 구성

영역, 또는 해당 영역에 속한 사용자 그룹 및 사용자에 따른 규칙을 제한할 수 있습니다.

시작하기 전에

- 사용자, 영역 및 ISE 속성 조건(사용자 제어), 545 페이지에서 설명된 사용자 제어 전제 조건을 충족합니다.
- 클래식 디바이스 모델의 경우 이러한 조건을 설정하려면 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** 규칙 편집기에서 **Users(**사용자**)**를 클릭합니다.

단계 **2** (선택 사항) **Available Realms(**사용 가능한 영역**)**에서 사용하려는 영역을 찾아 선택합니다.

단계 **3** (선택 사항) **Available Users(**사용 가능한 사용자**)** 목록에서 사용자 및 그룹을 선택하여 규칙을 추가로 제한할 수 있습니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

ISE 속성 조건 구성

시작하기 전에

- 사용자, 영역 및 ISE 속성 조건(사용자 제어), 545 페이지에서 설명한 사용자 제어 전제 조건을 충족합니다.
- 클래식 디바이스 모델의 경우 이러한 조건을 구성하려면 제어 라이센스가 있어야 합니다.

프로시저

단계 **1** 규칙 편집기에서 ISE 속성 조건에 대해 다음을 클릭합니다.

- 액세스 제어 - **SGT/ISE Attributes(SGT/ISE** 속성**)**를 클릭합니다.

ISE가 할당된 SGT(보안 그룹 태그)를 사용하면 ISE 속성 조건을 제한할 수 있습니다.

단계 **2** 항목의 **Available ISE Session Attributes(**사용 가능한 **ISE** 세션 속성**)**에서 사용하려는 ISE 속성을 찾아 선택합니다.

- 보안 그룹 태그(SGT)
- 디바이스 유형(또는 엔드포인트 프로파일)
- QoS - **ISE Attributes(ISE** 속성**)**를 클릭합니다.
- 위치 IP(또는 엔드포인트 위치)

단계 **3** 항목의 **Available ISE Metadata(**사용 가능한 **ISE** 메타데이터**)**의 속성 메타데이터를 선택하여 규칙을 추가로 제한합니다. 또는 기본값 모든을 유지합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

단계 **5** (선택 사항) **Add a Location IP Address(IP** 주소 위치 추가**)** 필드의 IP 주소 규칙을 제한하고 **Add(**추가**)**를 클릭합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **6** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

사용자 제어 문제 해결

사용자 규칙 동작이 정상적이지 않을 경우 규칙, ID 소스 또는 영역 컨피그레이션을 조정하는 방법을 고려하십시오. 기타 관련 문제 해결 정보를 보려면 다음을 참조하십시오.

- ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결, 2500 페이지
- 캡티브 포털(captive portal) ID 소스 문제 해결, 2518 페이지
- 영역 및 사용자 다운로드 문제 해결, 2480 페이지

영역, 사용자 또는 사용자 그룹을 대상으로 하는 규칙이 트래픽과 일치하지 않음

다수의 사용자 그룹을 모니터링하는 ISE 디바이스를 설정하거나 네트워크의 호스트에 매우 많은 사용자가 매핑된 경우, Firepower Management Center 사용자 제한으로 인해 사용자 레코드가 삭제될 수 있습니다. 그 결과, 사용자 조건이 있는 규칙은 정상적으로 트래픽과 일치하지 않을 수 있습니다.

다수의 사용자 그룹을 모니터링하는 TS 에이전트, 또는 ISE/ISE-PIC 디바이스를 설정하거나 네트워크의 호스트에 매우 많은 사용자가 매핑된 경우, Firepower Management Center 사용자 제한으로 인해 사용자 레코드가 삭제될 수 있습니다. 그 결과, 사용자 조건이 있는 규칙은 정상적으로 트래픽과 일치하지 않을 수 있습니다.

사용자 그룹 내의 사용자 그룹 또는 사용자를 대상으로 하는 규칙이 정상적으로 트래픽과 일치하지 않음

사용자 그룹 조건이 포함된 규칙을 구성할 경우, LDAP 또는 Active Directory 서버에 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.

보조 그룹의 사용자를 대상으로 하는 규칙이 정상적으로 트래픽과 일치하지 않음

Active Directory 서버에 있는 보조 그룹의 구성원인 사용자를 포함하거나 제외하는 사용자 그룹 조건이 포함된 규칙을 구성할 경우, 서버에서는 보고하는 사용자 수를 제한할 수 있습니다.

기본적으로 Active Directory 서버는 보조 그룹에서 보고하는 사용자 수를 제한합니다. 보조 그룹의 모든 사용자를 Firepower Management Center에 보고하고 사용자 조건이 포함된 규칙에서 사용할 수 있도록 하려면 이 제한을 맞춤설정해야 합니다.

사용자가 최초로 확인된 경우 규칙이 해당 사용자와 일치하지 않음

이전에 확인되지 않은 사용자의 활동이 탐지되면 시스템은 서버에서 해당 사용자에 대한 정보를 검색합니다. 시스템이 이러한 정보를 성공적으로 검색할 때까지 해당 사용자가 보여준 활동이 일치하는 규칙으로 처리되지 않습니다. 그 대신, 일치하는 다음 규칙(또는 해당하는 경우 정책의 기본 작업)에 따라 사용자 세션이 처리됩니다.

다음과 같은 경우를 예로 들 수 있습니다.

- 사용자 그룹의 구성원인 사용자가 사용자 그룹 조건이 포함된 규칙과 일치하지 않음
- 사용자 데이터 회수에 사용된 서버가 액티브 디렉토리 서버인 경우, 또는 ISE/ISE-PIC 디바이스가 보고한 사용자가 규칙과 일치하지 않습니다.

이 경우 시스템에서 이벤트 보기 및 분석 툴에 사용자 데이터를 표시하는 것이 지연될 수 있습니다.

규칙이 모든 **ISE** 사용자와 일치하지 않음

이는 정상적인 동작입니다. Active Directory 도메인 컨트롤러에서 인증된 ISE 사용자에 대해 사용자 제어를 수행할 수 있습니다. LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.

규칙이 모든 **ISE/ISE-PIC** 사용자와 일치하지 않음

이는 정상적인 동작입니다. Active Directory 도메인 컨트롤러에서 인증된 ISE/ISE-PIC 사용자에 대해 사용자 제어를 수행할 수 있습니다. LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE/ISE-PIC 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.

너무 많은 메모리를 사용하는 사용자 및 그룹

처리 중인 사용자 및 그룹이 너무 많은 메모리를 사용하는 경우 상태 알림이 표시됩니다. 모든 사용자 세션은 FMC에서 관리하는 모든 디바이스로 전파됩니다. FMC가 메모리가 다른 디바이스를 관리하는 경우, 메모리가 가장 적은 디바이스가 시스템이 오류 없이 처리할 수 있는 사용자 세션 수를 결정합니다.

문제가 지속되는 경우 다음 옵션 중 하나를 선택합니다.

- 서브넷에서 저용량 관리 디바이스를 분리하고 패시브 인증 데이터를 해당 서브넷에 보고하지 않도록 ISE/ISE-PIC를 설정합니다.

  Cisco ISE(Identity Services Engine) 관리자 설명서의 네트워크 디바이스 관리 장을 참조하십시오.

- SGT(Security Group Tag)에서 구독을 취소합니다.

  자세한 내용은 사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지를 참고하십시오.

- 더 많은 메모리를 사용하여 매니지드 디바이스를 모델로 업그레이드합니다.

날짜 및 시간 기준 규칙 적용

다음 유형의 정책에서는 날짜와 시간에 따라 규칙을 적용할 수 있습니다.

- 액세스 제어
- 사전 필터
- VPN 그룹

연속 시간 범위 또는 반복 기간을 지정할 수 있습니다.

예를 들어 규칙은 주중 근무 시간 중 또는 매주 또는 공휴일 셧다운 기간에만 적용할 수 있습니다.

시간 기반 규칙은 트래픽을 처리하는 디바이스의 로컬 시간을 기준으로 적용됩니다.

시간 기반 규칙은 FTD 디바이스에서만 지원됩니다. 시간 기반 규칙이 있는 정책을 다른 유형의 디바이스에 할당하는 경우 해당 디바이스에서 규칙과 연결된 시간 제한이 무시됩니다. 이 경우 경고가 표시됩니다.

프로시저

단계 **1** (선택 사항) 각 디바이스에 로컬 표준 시간대를 할당합니다. 기본적으로 디바이스는 UTC 표준 시간대를 사용합니다.

Devices(디바이스**)** > **Platform Settings(**플랫폼 설정**)**로 이동하여 표준 시간대 개체를 생성하고 할당합니다.

단계 **2** 지원되는 규칙에서 적용 가능한 시간 범위를 지정합니다.

규칙을 구성하는 동안 시간 범위 개체를 생성하고 선택합니다.

단계 **3** 변경 사항을 구축합니다.

규칙 검색

많은 정책 및 규칙 내에서 검색할 수 있습니다. 시스템은 개체 및 개체 그룹의 이름 및 조건 값을 제어하는 입력에 일치시킵니다.

보안 인텔리전스 또는 URL 목록이나 피드의 값을 검색할 수 없습니다.

프로시저

단계 **1** 정책 편집기에서 **Rules(**규칙**)**를 클릭합니다.

단계 **2** (액세스 제어 규칙만 해당) **Search Rules(**검색 규칙**)**를 클릭하고 하나 이상의 필드에 전체 또는 부분 검색 문자열을 입력한 다음 Enter 키를 누릅니다.

여러 필드에 기준을 입력할 경우, 검색 결과에는 입력한 모든 기준(논리적 "AND" 검색)과 일치하는 규칙이 포함됩니다.

단일 필드에 여러 검색 기준을 포함하려면 값을 쉼표로 구분합니다. 검색 결과에는 입력한 값과 일치하는 규칙(논리적 "OR" 검색)이 포함됩니다.

단계 **3** (기타 규칙 유형) **Search Rules(**검색 규칙**)**를 클릭하고 전체 또는 부분 검색 문자열을 입력한 뒤 Enter 키를 누릅니다.
일치 값은 각 일치하는 규칙에 강조 표시됩니다. 상태 메시지는 현재 일치하는 규칙과 일치하는 총 수를 나타냅니다.

단계 **4** 관심 있는 규칙을 확인합니다.

일치하는 규칙을 탐색하려면 **Next-Match(**다음 일치**)** 또는 **Previous-Match(**이전 일치**)**를 클릭합니다.

(액세스 제어 규칙만 해당) 일치하는 규칙의 목록만 표시하거나 일치하는 규칙이 강조 표시된 모든 규칙의 목록을 표시하려면 다음을 클릭합니다. 검색 규칙( )

다음에 수행할 작업

- 새 검색을 시작하기 전에 검색 또는 강조 표시를 지우려면 지우기( )를 클릭합니다.

디바이스별 규칙 필터링

일부 정책 편집기를 사용하면 영향 받는 디바이스에 따른 규칙 보기를 필터링할 수 있습니다.

디바이스별 필터링은 영역 또는 인터페이스 그룹을 사용하는 규칙에 대해서만 작동합니다. (그렇지 않으면 모든 디바이스에 규칙이 적용됩니다.)

시스템은 규칙의 인터페이스 제약 조건을 사용하여 규칙이 디바이스에 영향을 미치는지 결정합니다. (보안 영역 조건) 인터페이스로 규칙을 제한하는 경우, 해당 인터페이스가 위치한 디바이스는 해당 규칙에 영향을 받습니다. 인터페이스 제약 조건이 없는 규칙은 모든 인터페이스에 적용되므로 모든 디바이스에 적용됩니다.

QoS 규칙은 항상 인터페이스에 의해 제한됩니다.

프로시저

단계 **1** 정책 편집기에서 **Rules(**규칙**)**를 클릭하고 **Filter by Device(**디바이스로 필터링**)**를 클릭합니다.
대상 디바이스 및 디바이스 그룹의 목록이 표시됩니다.

단계 **2** 이런 디바이스 또는 그룹에 적용되는 규칙만을 표시하려면 하나 이상의 체크 박스에 체크합니다. 또는 재설정하여 모든 규칙을 표시하려는 경우 모두를 체크합니다.

팁 해당 값을 확인하려면 규칙 기준으로 마우스 포인터를 이동합니다. 기준이 디바이스 한정 오버라이드가 포함된 개체를 나타내는 경우 시스템은 해당 디바이스에 한정한 규칙 목록을 필터링할 때 오버라이드 값을 표시합니다. 기준이 도메인 한정 오버라이드가 포함된 개체를 나타내는 경우 시스템은 해당 도메인의 디바이스의 규칙 목록을 필터링할 때 오버라이드 값을 표시합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

관련 항목

액세스 제어 규칙 생성 및 수정, 1651 페이지
QoS 규칙 구성, 883 페이지
Threat Defense NAT 구성, 1502 페이지

문제가 있는 규칙 식별

시스템은 규칙 순서의 다른 상위 규칙이 대신 일치하므로(노란색 아이콘으로 표시) 구축을 예방하는 각 규칙에 플래그를 지정하거나(빨간색 아이콘으로 표시) 트래픽을 일치시키지 않습니다.

중요 시스템은 다른 규칙과 일부 일치하고 하위 규칙과 일치하지 않도록 하는 규칙에 플래그를 지정하지 않습니다.

프로시저

단계 **1** **Policies(**정책**) > Access Control(**액세스 컨트롤**) > Access Control(**액세스 컨트롤**)**을 선택합니다.

단계 **2** 정책 이름을 클릭합니다.

단계 **3** 다음 중 하나를 또는 둘 다 수행합니다.

- 창의 상단 근처에 있는 **Show Warnings(**경고 표시**)**를 찾습니다.

  시스템이 문제를 식별하지 않는 경우 이 버튼이 표시되지 않습니다.

  문제가 있는 경우 이 버튼을 눌러 문제와 관련된 모든 규칙 목록을 표시합니다.

  모든 문제를 보려면 두 탭(규칙 오류 및 규칙 경고)을 클릭합니다.

  아래의 규칙 테이블의 규칙을 찾으려면 오류 또는 경고 목록에서 규칙 이름을 클릭합니다.

- **Show Rule Conflicts(**규칙 충돌 표시**)** 체크 박스를 선택합니다.

  목록에서 오류(빨간색) 또는 경고(노란색)로 각 문제 규칙을 나타냅니다.

  필요한 경우 정책의 모든 규칙을 보려면 아래로 스크롤하십시오.

단계 **4** 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

단계 **5** 일부만 일치하고 이를 처리하여 플래그로 지정되지 않은 중복을 검색합니다.

단계 **6** 변경하는 경우 **Save(**저장**)**를 클릭하거나 **Show Rule Conflicts(**규칙 충돌 보기**)**를 다시 선택 또는 선택 취소하여 충돌하는 규칙 변경을 다시 평가합니다.

다음에 수행할 작업

- 문제가 되는 규칙을 제거 또는 수정하여 관련 문제를 처리합니다.
- 유사한 오류 및 경고에 대한 SSL 또는 QoS 정책을 평가하고 이러한 문제를 처리합니다.

규칙 및 기타 정책 경고

정책 및 규칙 편집기는 아이콘을 사용하여 트래픽 분석 및 흐름에 부정적인 영향을 미칠 수 있는 설정을 표시합니다. 문제에 따라 구축 시 시스템이 경고하거나 완전 구축을 차단할 수 있습니다.

팁 경고, 오류 또는 정보를 제공하는 텍스트를 읽을 아이콘에 마우스 포인터를 놓습니다.

표 ***60:*** 정책 오류 아이콘

아이콘	설명	예
오류(✖) 오류	규칙 또는 설정에 오류가 있는 경우, 영향을 받는 규칙을 비활성화해도 문제를 수정하기 전까지는 구축할 수 없습니다.	카테고리 및 평판 기반 URL 필터링을 수행하는 규칙은 URL 필터링 라이선스가 없는 디바이스를 대상으로 하기 전까지 유효합니다. 이 경우 규칙 옆에 오류 아이콘이 표시되며 규칙을 편집 또는 삭제하거나 정책의 대상을 다시 설정하거나 라이선스를 활성화하기 전까지 구축할 수 없습니다.
경고(⚠) 경고	규칙 또는 다른 경고를 표시하는 정책을 구축할 수 있습니다. 그러나, 경고가 표시된 오류 구성은 적용되지 않습니다. 경고가 표시된 규칙을 비활성화하는 경우, 경고 아이콘이 사라집니다. 경고 아이콘은 근본적인 문제를 해결하지 않고 규칙을 활성화하는 경우 다시 나타납니다.	선점된 규칙 또는 설정 오류로 트래픽과 일치하지 않는 규칙은 효과가 없습니다. 이는 제외된 LDAP 사용자, 유효하지 않은 포트 등 애플리케이션과 일치하지 않는 빈 개체 그룹, 애플리케이션 필터를 사용한 조건을 포함합니다. 그러나 경고 아이콘이 라이선싱 오류 또는 모델 불일치를 표시하는 경우 해당 문제를 해결하기 전까지 구축할 수 없습니다.

아이콘	설명	예
정보() 정보	정보 아이콘은 트래픽의 흐름에 영향을 줄 수 있는 구성에 대한 유용한 정보를 제공합니다. 이 문제는 구축을 방해하지 않습니다.	애플리케이션 제어이 있는 경우, 시스템은 연결 애플리케이션 또는 웹 트래픽을 식별하기 전까지 일부 규칙과 다른 초기 연결 패킷을 일치시키는 작업을 건너 뛸 수 있습니다. 이는 애플리케이션 및 HTTP 요청을 확인할 수 있도록 연결을 설정할 수 있게 합니다.

관련 항목

애플리케이션 제어 모범 사례, 539 페이지
URL 필터링 모범 사례, 1667 페이지

규칙 관리 기록: 일반 특성

기능	버전	세부 사항
사전 필터 정책에서 개체 세부 사항 보기	6.6	이제 사전 필터 정책의 규칙에서 소스 및 대상 네트워크(IP 주소), 포트, VLAN 태그 개체 및 개체 그룹을 볼 수 있습니다. 적합한 개체를 마우스 오른쪽 버튼으로 클릭하고 **Object Details(**개체 세부 사항**)**를 선택합니다. 신규/수정된 페이지: Prefilter rules(사전 필터 규칙) 페이지 지원되는 플랫폼: FMC
설정된 규칙에 대한 향상된 검색	6.6	이제 여러 열에서 설정된 규칙을 검색할 수 있습니다(액세스 제어 정책만 해당). 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지 지원되는 플랫폼: FMC
사전 필터 규칙에 대한 시간 범위 지원	6.6	적용할 규칙에 대해 절대적이거나 반복되는 시간 또는 시간 범위를 지정할 수 있습니다. 규칙은 트래픽을 처리하는 디바이스의 표준 시간대에 따라 적용됩니다. 신규/수정된 페이지: Prefilter rule configuration(사전 필터 규칙 설정) 페이지 지원되는 플랫폼: FTD 디바이스 전용

기능	버전	세부 사항
URL 조건에 대한 정보는 새 URL 필터링 장으로 이동	6.3	URL 조건에 관한 전용 항목을 포함해 URL 필터링에 대한 정보는 URL 필터링, 1665 페이지을 참고하십시오.

22 장

재사용 가능 개체

다음 주제에서는 Firepower System에서 재사용 가능한 개체를 관리하는 방법을 설명합니다.

- 재사용 가능한 개체 소개, 558 페이지
- 개체 관리자, 560 페이지
- 네트워크 개체, 571 페이지
- 포트 개체, 572 페이지
- 애플리케이션 필터, 574 페이지
- VLAN 태그 개체, 574 페이지
- URL 개체, 575 페이지
- 지리위치 개체, 576 페이지
- 보안 영역, 577 페이지
- 시간 범위 개체, 578 페이지
- 표준 시간대 개체, 580 페이지
- 변수 집합, 580 페이지
- 보안 인텔리전스 목록 및 피드, 597 페이지
- 싱크홀 개체, 609 페이지
- 파일 목록, 610 페이지
- 암호 그룹 목록, 615 페이지
- 고유 이름 개체, 616 페이지
- PKI 개체, 618 페이지
- 키 체인 개체, 635 페이지
- DNS 서버 그룹 개체, 637 페이지
- SLA 모니터 개체, 638 페이지
- 접두사 목록, 639 페이지
- 경로 맵, 641 페이지
- 액세스 목록, 644 페이지
- AS 경로 개체, 647 페이지
- 커뮤니티 목록, 648 페이지
- 정책 목록, 649 페이지
- VPN 개체, 650 페이지

• 주소 풀, 666 페이지
• FlexConfig 개체, 667 페이지
• RADIUS 서버 그룹, 667 페이지
• SSO(Single Sign-On) 서버 추가, 670 페이지
• 재사용 가능 개체 히스토리, 672 페이지

재사용 가능한 개체 소개

향상된 유연성 및 웹 인터페이스 사용 편의성을 위해 Firepower System은 이름과 값을 연결하는 재사용 가능한 설정으로 명명된 개체를 사용합니다. 해당 값을 사용하려는 경우 명명된 개체를 사용합니다. 시스템은 다양한 정책 및 규칙, 이벤트 검색, 보고서, 대시보드 등을 포함해 웹 인터페이스의 다양한 위치에서 개체 사용을 지원합니다. 시스템은 자주 사용된 설정을 대표하는 여러 개의 사전 정의된 개체를 제공합니다.

개체 관리자를 사용하여 개체를 생성하고 관리합니다. 개체를 사용하는 많은 설정도 즉석에서 필요에 따라 개체를 생성할 수 있도록 합니다. 다음에 개체 관리자를 사용할 수 있습니다.

- 네트워크, 포트, VLAN 또는 URL 개체를 사용하는 정책, 설정 및 기타 개체를 확인합니다. 자세한 내용은 개체 및 사용 현황 보기, 564 페이지의 내용을 참조하십시오.
- 여러 개체가 단일 설정을 참조하도록 개체를 그룹화하려면 개체 그룹, 566 페이지의 내용을 참조하십시오.
- 선택한 디바이스, 다중 도메인 구축, 선택된 도메인에서 개체 값을 오버라이드하려면 개체 재정의, 568 페이지의 내용을 참조하십시오.

액티브 정책에서 사용된 개체를 편집한 뒤 변경 설정을 재구축해야 변경 사항이 적용됩니다. 활성 정책에서 사용 되는 개체를 삭제할 수 없습니다.

참고 관리되는 디바이스에 할당된 정책에서 사용되는 경우에만 디바이스에 개체를 설정할 수 있습니다. 특정 디바이스에 할당된 모든 정책에서 개체를 제거하는 경우 개체는 다음 구축의 디바이스 설정에서 제거되고 개체에 대한 후속 변경 사항은 디바이스 설정에 반영되지 않습니다.

개체 유형

다음 표는 Firepower System에서 생성할 수 있는 개체 및 각 개체 유형이 그룹화 또는 오버라이드가 허용되는지 여부를 나타냅니다.

개체 유형	그룹화 가능?	오버라이드 허용?
네트워크	예	예
Port(포트)	예	예
보안 영역	아니요	아니요

개체 유형	그룹화 가능?	오버라이드 허용?
애플리케이션 필터	아니요	아니요
VLAN Tag	예	예
URL	예	예
지리위치	아니요	아니요
시간 범위	아니요	아니요
변수 세트	아니요	아니요
Security Intelligence(보안 인텔리전스): 네트워크, DNS, URL 목록 및 피드	아니요	아니요
싱크홀	아니요	아니요
파일 목록	아니요	아니요
암호 그룹 목록	아니요	아니요
고유 이름	예	아니요
PKI(Public Key Infrastructure): • 내부 및 신뢰할 수 있는 CA • 내부 및 외부 인증	예	아니요
키 체인	아니요	예
DNS 서버 그룹	아니요	아니요
SLA 모니터링	아니요	아니요
접두사 목록: IPv4 및 IPv6	아니요	예
경로 맵	아니요	예
액세스 목록: 표준 및 확장	아니요	예
AS 경로	아니요	예
커뮤니티 목록	아니요	예
정책 목록	아니요	예
FlexConfig: 텍스트 및 FlexConfig 개체	아니요	예

개체 및 멀티 테넌시

다중 도메인 구축에서 전역 및 하위 도메인에 개체를 만들 수 있습니다. 시스템은 현재 도메인에 생성되어 편집할 수 있는 개체를 표시합니다. 또한 상위 도메인에 생성된 개체 중 보안 영역을 제외하고 편집이 불가능한 개체를 표시합니다.

참고 보안 영역 은 리프 레벨에서 구성하는 디바이스 인터페이스와 연결되어 있으므로 하위 도메인의 관리자는 상위 도메인에 생성된 보안 영역을 보고 편집할 수 있습니다. 서브도메인 사용자는 상위 영역에서 인터페이스를 추가하고 삭제할 수 있지만 영역을 삭제하거나 이름을 변경할 수 없습니다.

개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

그룹화를 지원하는 개체의 경우 상위 도메인에서 상속된 개체를 포함해 현재 도메인에 있는 개체를 그룹화할 수 있습니다.

개체 오버라이드는 네트워크, 포트, VLAN 태그, URL 등 특정 유형의 개체에 대해 디바이스별 또는 도메인별 값을 정의하도록 합니다. 다중 도메인 구축에서 상위 도메인의 개체에 대한 기본값을 정의할 수 있지만 하위 도메인의 관리자가 해당 개체에 대한 오버라이드 값을 추가할 수 있습니다.

개체 관리자

개체 관리자를 사용해 개체 및 개체 그룹을 생성하고 관리할 수 있습니다.

개체 관리자는 페이지당 20개의 개체 또는 그룹을 표시합니다. 모든 유형의 개체 또는 그룹이 20개 이상 있는 경우, 추가 페이지를 보려면 페이지 하단의 탐색 링크를 사용합니다. 또한 특정 페이지로 이동하거나 새로 로침( )을 클릭하여 보기를 새로 고칠 수 있습니다.

기본적으로, 페이지는 개체 및 그룹을 이름의 알파벳 순으로 나열합니다. 그러나, 표시되는 모든 열에 따라 각 유형의 개체 또는 그룹을 정렬할 수 있습니다. 또한 페이지의 개체를 이름 또는 값으로 필터링할 수 있습니다.

개체 가져오기

쉼표로 구분된 값 파일에서 개체를 가져올 수 있습니다. 한 번에 최대 1,000개의 개체를 가져올 수 있습니다. 쉼표로 구분된 값 파일의 내용은 특정 형식을 따라야 합니다. 형식은 개체 유형마다 다릅니다. 몇 가지 유형의 개체만 가져올 수 있습니다. 지원되는 개체 유형 및 해당 규칙을 확인하려면 다음 표를 참조하십시오.

개체 유형	규칙

개별 개체	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • DN
	• 항목을 가져오려면 NAME 및 DN 열 항목이 모두 필요합니다.
	• 개별 개체를 기존의 고유 이름 개체 그룹으로 직접 가져올 수 있습니다.

네트워크 개체	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • 설명
	  • 유형
	  • 값
	  • 조회
	• 호스트, 범위 또는 네트워크 개체 유형의 항목을 가져오려면 NAME 및 VALUE 열 항목은 필수입니다.
	• FQDN 개체의 경우 TYPE 열 항목은 'fqdn'을 언급하고 LOOKUP 열 항목은 'ipv4,' 'ipv6,'또는 'ipv4_ipv6'으로 지정해야 합니다.
	• FQDN 개체의 LOOKUP 열 항목에 콘텐츠가 제공되지 않으면 개체는 ipv4_ipv6 필드 값과 함께 저장됩니다.

개체 유형	규칙

포트	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • PROTOCOL
	  • PORT
	  • ICMPCODE
	  • ICMPTYPE
	• NAME 열 항목은 필수입니다.
	• 'tcp' 및 'udp' 프로토콜 유형의 경우 PORT 열 항목은 필수입니다.
	• 'icmp' 및 'icmp6' 프로토콜 유형의 경우 ICMPCODE 및 ICMPTYPE 열 항목은 필수입니다.

URL	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • 설명
	  • URL
	• NAME 및 URL 열 항목은 필수 항목입니다.

VLAN Tag	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • 설명
	  • 태그
	• 항목을 가져오려면 NAME 및 TAG 열 항목은 필수입니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** 왼쪽 창에서 다음 개체 유형 중 하나를 선택합니다.

- **Distinguished Name(**고유 이름**)** > **Individual Objects(**개별 개체**)** >
- 네트워크 개체
- **Port(**포트**)**
- **URL**
- **VLAN Tag**

단계 **3** **Add [Object Type]([**개체 유형**]** 추가**)** 드롭다운 목록에서 **Import Object(**개체 가져오기**)**를 선택합니다.

참고 이전 단계에서 **Individual Objects(**개별 개체**)**를 선택한 경우 **Import(**가져오기**)**를 클릭합니다.

단계 **4** **Browse(**찾아보기**)**를 클릭합니다.

단계 **5** 시스템에서 쉼표로 구분된 파일을 찾아 선택합니다.

단계 **6** **Open(**열기**)**을 클릭하십시오.

참고 **Distinguished Name(**고유 이름**)** 개체를 가져오는 동안 필요에 따라 **Add imported Distinguished Name objects to the below object group(**가져온 고유 이름 개체를 아래 개체 그룹에 추가 확인란을 선택하고 드롭 다운 상자에서 그룹 이름을 선택하여 개체를 기존의 고유 이름 개체 그룹으로 직접 가져올 수 있습니다.

단계 **7** **Import(**가져오기**)**를 클릭합니다.

개체 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 목록에서 개체 유형을 선택하려면 재사용 가능한 개체 소개, 558 페이지을 참조하십시오.

단계 **3** 편집하려는 개체 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 개체가 상위 도메인에 속하며 재정의를 허용하지 않도록 설정되었거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 필요에 맞게 개체 설정을 수정합니다.

단계 **5** 변수 집합을 편집하는 경우 집합의 변수를 관리하려면 변수 관리, 593 페이지을 참조하십시오.

단계 **6** 오버라이드를 허용하도록 구성할 수 있는 개체는 다음과 같습니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오. 현재 도메인에 속한 개체에 대해서만 이 설정을 변경할 수 있습니다.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 570 페이지의 내용을 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 변수 집합을 편집하고 해당 집합이 액세스 제어 정책에서 사용 중인 경우 변경 사항을 저장하려면 **Yes(**예**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참조하십시오.

개체 및 사용 현황 보기

Object Management(개체 관리) 페이지에서 개체의 사용량 세부 정보를 볼 수 있습니다. Firepower Management Center는 여러 개체 유형에 이 기능을 제공합니다. 그러나 일부 개체 유형은 지원되지 않습니다.

참고 다중 도메인 구축에서는 다른 도메인의 개체를 확인할 수 있습니다. 하지만 하위 도메인의 개체 사용량을 확인하려면 해당 도메인으로 전환해야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** 지원되는 다음 개체 유형 중 하나를 선택합니다.

- 액세스 목록 > 확장
- 액세스 목록 > 표준
- AS 경로
- 커뮤니티 목록
- 인터페이스
- 네트워크

- 정책 목록
- 포트
- 접두사 목록> IPv4 접두사 목록
- 접두사 목록> IPv6 접두사 목록
- 경로 맵
- SLA 모니터링
- URL
- VLAN Tag

단계 **3** 개체 옆에 있는 사용량 찾기( ) 아이콘을 클릭합니다.

Object Usage(개체 사용량) 창에는 개체가 사용 중인 모든 정책, 개체 및 기타 설정 목록이 표시됩니다. 목록에 있는 항목을 클릭하면 개체 사용량 추가 정보를 확인할 수 있습니다. 개체를 사용하는 정책 및 일부 기타 설정의 경우, 해당 링크를 클릭하면 대응하는 UI 페이지를 방문할 수 있습니다.

개체 또는 개체 그룹 필터링

다중 도메인 구축에서 시스템은 필터링 가능한 현재 및 상위 도메인에서 생성된 개체를 표시합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **Filter(**필터**)** 필드에 필터 기준을 입력합니다.

일치하는 항목을 입력하여 표시하면 페이지가 업데이트됩니다.

다음 와일드카드를 사용할 수 있습니다.

- 별표(*)는 0번 이상 나타나는 문자에 해당합니다.
- 캐럿 (^) 은 문자열의 시작 부분에 있는 내용에 해당합니다.
- 달러 기호 ($)는 문자열의 끝 부분에 있는 내용에 해당합니다.

단계 **3** 시스템에서 사용되지 않는 개체 및 개체 그룹을 보려면 **Show Unused Object(**사용하지 않은 개체 표시**)** 확인란을 선택합니다.

참고
- 개체가 사용되지 않은 개체 그룹의 일부인 경우, 개체는 사용된 것으로 간주됩니다. 그러나 **Show Unused Object(**사용되지 않은 개체 표시**)** 확인란을 선택하면 사용되지 않은 개체 그룹이 표시됩니다.
- **Show Unused Object(**사용되지 않은 개체 표시**)** 확인란은 네트워크, 포트, URL 및 VLAN 태그 개체 유형에만 사용할 수 있습니다.

개체 정렬

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 열 제목을 클릭합니다. 반대 방향으로 정렬하려면, 제목을 다시 클릭합니다.

개체 그룹

개체 그룹화는 단일 컨피그레이션으로 여러 개체를 참조하도록 허용합니다. 시스템을 통해 웹 인터페이스에서 개체 및 개체 그룹을 같은 의미로 사용할 수 있습니다. 예를 들어, 포트 개체를 사용하는 모든 곳에서 포트 개체 그룹을 사용할 수 있습니다.

네트워크, 포트, VLAN 태그, URL, PKI 개체를 그룹화할 수 있습니다.

유형이 동일한 개체 및 개체 그룹이 동일한 이름을 가질 수 없습니다. 다중 도메인 구축에서 개체 그룹 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 그룹 이름과의 충돌을 식별합니다.

정책에서 사용되는 개체 그룹(액세스 제어 정책의 네트워크 개체 그룹 등)을 편집할 때는 변경 설정을 재구축해야 변경 사항이 적용됩니다.

그룹을 삭제해도 그룹 내 개체는 삭제되지 않으며, 개체 간 연결만 삭제됩니다. 또한 활성 정책에서 사용 중인 그룹을 삭제할 수 없습니다. 예를 들어 저장한 액세스 제어 정책의 VLAN 조건에서 사용 중인 VLAN 태그 그룹은 삭제할 수 없습니다.

재사용 가능 개체 그룹화

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인에서 상속된 개체를 포함해 현재 도메인의 개체를 그룹화할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 그룹화할 개체 유형이 네트워크, 포트, **URL**, **VLAN** 태그인 경우:

a) 개체 유형 목록에서 개체 유형을 선택합니다.

b) 드롭다운 목록의 **Add [Object Type]([**개체 유형**]** 추가**)**에서 **Add Group(**그룹 추가**)**를 선택합니다.

단계 **3** 그룹화하려는 개체 유형이 **Distinguished Name(**고유 이름**)**인 경우:

a) **Distinguished Name(**고유 이름**)** 노드를 확장합니다.

b) **Object Group(**개체 그룹**)**을 선택합니다.

c) **Add Distinguished Name Group(**고유 이름 그룹 추가**)**을 클릭합니다.

단계 **4** 그룹화하려는 개체 유형이 **PKI**인 경우:

a) **PKI** 노드를 확장합니다.

b) 다음 중 하나를 선택합니다.

- 내부 **CA** 그룹
- 신뢰하는 **CA** 그룹
- 내부 인증서 그룹
- 외부 인증서 그룹

c) **Add [Object Type] Group([**개체 유형**]** 그룹 추가**)**을 클릭합니다.

단계 **5** 고유한 이름을 입력합니다.

단계 **6** 목록에서 하나 이상의 개체를 선택하고 **Add(**추가**)**를 클릭합니다.

다음 작업도 가능합니다.

- 기존 개체를 포함하여 검색하려면 필터 필드 검색( )를 사용합니다. 입력 시 일치하는 항목이 업데이트됩니다. 검색 필드 위의 다시 로드( )을 클릭하거나 검색 필드에서 지우기( )을 클릭하여 검색 문자열을 삭제합니다.
- 어떤 기존 개체도 요구 사항을 충족하지 않는 경우 추가( )을 클릭하여 상황에 따라 개체를 생성합니다.

단계 **7** 네트워크, 포트, **URL**, **VLAN** 태그 그룹일 경우:

- **Description(**설명**)**을 입력합니다.
- 개체 그룹의 오버라이드를 허용하려면 체크 박스에서 **Allow Overrides(**오버라이드 허용**)**을 선택합니다. 개체 재정의 허용, 570 페이지를 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체 그룹을 참조하는 경우 설정 변경을 구축하는 방법은 컨피그레이션 변경 사항 구축, 498 페이지을 참조하십시오.

개체 재정의

개체 오버라이드는 시스템이 지정한 장치에 대해 사용하는 개체에 대한 대체 값을 정의하도록 합니다.

대부분의 디바이스에 대한 정의가 해당하는 개체를 생성하고 다른 정의가 필요한 일부 디바이스의 개체에 대한 특정 변경 사항을 지정하는 오버라이드를 사용할 수 있습니다. 모든 디바이스에 오버라이드가 필요한 개체를 생성할 수도 있습니다. 하지만 이 경우 모든 디바이스에 단일 정책을 생성할 수 있습니다. 개체 오버라이드는 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성하도록 합니다.

예를 들어 다른 네트워크에 연결된 회사 내 다른 부서의 ICMP 트래픽을 거부하는 경우가 있습니다. 이런 경우 부서 네트워크라는 네트워크 개체가 포함된 규칙이 있는 액세스 제어 정책을 정의합니다. 이 개체에 대한 오버라이드를 허용함으로써 디바이스가 연결된 실제 네트워크를 지정하는 각 관련 디바이스의 오버라이드를 생성할 수 있습니다.

다중 도메인 구축에서 상위 도메인의 개체에 대한 기본값을 정의할 수 있지만 하위 도메인의 관리자가 해당 개체에 대한 오버라이드 값을 추가할 수 있습니다. 예를 들어 관리되는 보안 서비스 제공자(MSSP)는 여러 고객에 대한 네트워크 보안을 관리하기 위해 단일 Firepower Management Center를 사용할 수 있습니다. MSSP의 관리자는 모든 고객의 배포에 사용하기 위한 전역 도메인의 개체를 정의할 수 있습니다. 각 고객의 관리자는 조직에 대한 개체를 오버라이드하기 위해 하위 도메인에 로그인할 수 있습니다. 이런 로컬 관리자는 MSSP 내 다른 고객의 오버라이드 값을 보거나 영향을 줄 수 없습니다.

특정 도메인에 개체 오버라이드를 지정할 수 없습니다. 이 경우 시스템은 사용자가 디바이스 수준에서 오버라이드하지 않는 경우 대상 도메인의 모든 디바이스에 개체 오버라이드 값을 사용합니다.

개체 관리자에서 오버라이드 가능한 개체를 선택하고 개체에 대해 디바이스 수준 또는 도메인 수준의 오버라이드 목록을 정의할 수 있습니다.

다음 개체 유형에만 개체 오버라이드를 사용할 수 있습니다.

- 네트워크
- Port(포트)
- VLAN 태그
- URL
- SLA 모니터링
- 접두사 목록

- 경로 맵
- 액세스 목록
- AS 경로
- 커뮤니티 목록
- 정책 목록
- PKI 등록
- 키 체인

개체를 오버라이드할 수 있는 경우 개체 관리자의 개체 유형에 **Override(**재정의**)** 열이 나타납니다. 이 열에서 사용 가능한 값은 다음과 같습니다.

- 녹색 확인 표시 - 개체에 대한 오버라이드를 만들 수 있으며 오버라이드가 추가된 적이 없음을 나타냅니다.
- 빨간색 X - 해당 개체에는 오버라이드를 생성할 수 없음을 나타냅니다.
- 숫자 - 해당 개체에 추가된 오버라이드의 수를 나타냅니다. (예를 들어 "2"는 2개의 오버라이드가 추가됐음을 나타냅니다.)

개체 재정의 관리

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 선택합니다. 재사용 가능한 개체 소개, 558 페이지을 참조하십시오.

단계 **3** 편집하려는 개체 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 개체가 상위 도메인에 속하며 재정의를 허용하지 않도록 설정되었거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 개체 오버라이드 관리

- 추가 - 개체 오버라이드를 추가합니다. 개체 재정의 추가, 570 페이지을 참조하십시오.
- 허용 - 개체 오버라이드를 허용합니다. 개체 재정의 허용, 570 페이지을 참조하십시오.
- 삭제 - 개체 편집기에서 제거하려는 오버라이드 옆의 삭제( )를 클릭합니다.
- 편집 - 오버라이드를 편집합니다. 개체 오버라이드 편집, 571 페이지을 참조하십시오.

개체 재정의 허용

프로시저

단계 **1** 개체 편집기에서 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

개체 재정의 값을 추가합니다. 개체 재정의 추가, 570 페이지를 참조하십시오.

개체 재정의 추가

시작하기 전에

개체 재정의를 허용합니다. 개체 재정의 허용, 570 페이지를 참조하십시오.

프로시저

단계 **1** 개체 편집기에서 **Override(**재정의**)** 섹션을 확장합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Targets(**타겟**)**에서 **Available Devices and Domains(**사용 가능한 디바이스 및 도메인**)** 목록에서 도메인 또는 디바이스를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **4** Override(재정의) 탭에서 **Name(**이름**)**을 입력합니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** 재정의 값을 입력합니다.

예제**:**

네트워크 개체의 경우 네트워크 값을 입력합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

개체 오버라이드 편집

기존 오버라이드 값과 설명은 수정할 수 있지만 기존 대상 목록은 수정할 수 없습니다. 대신 기존 오버라이드를 대체하는 새 대상에 새 오버라이드를 추가해야합니다.

프로시저

단계 **1** 개체 편집기에서 **Override(**재정의**)** 섹션을 확장합니다.

단계 **2** 수정할 오버라이드 옆의 수정( )을 클릭합니다.

단계 **3** 필요에 따라 설명을 수정합니다.

단계 **4** 오버라이드 값을 수정합니다.

단계 **5** **Save(**저장**)**를 클릭하여 오버라이드를 저장합니다.

단계 **6** **Save(**저장**)**를 클릭하여 개체를 저장합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참조하십시오.

네트워크 개체

네트워크 개체는 개별적으로 또는 주소 블록으로 지정할 수 있는 하나 이상의 IP 주소를 나타냅니다. 액세스 제어 정책, 네트워크 변수, ID 규칙, 네트워크 검색 규칙, 이벤트 검색, 보고서, 등 시스템 내 웹 인터페이스의 여러 위치에서 네트워크 개체 및 그룹을 사용할 수 있습니다.

네트워크 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Network(**네트워크**)**를 선택합니다.

단계 **3** **Add Network(**네트워크 추가**)** 드롭다운 메뉴에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** **Network(**네트워크**)** 필드에서 개체에 추가할 IP 주소 또는 주소 블록을 입력합니다.

단계 **7** (FQDN 개체 한정) FQDN과 관련된 IPv4, IPv6 또는 IPv4 및 IPv6 주소를 선택해 사용하려면 **Lookup(**검색**)** 드롭다운 메뉴에서 DNS 확인을 선택합니다.

단계 **8** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 570 페이지의 내용을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

네트워크 개체 가져오기

네트워크 개체 가져오기에 대한 자세한 내용은 개체 가져오기, 560 페이지의 내용을 참조하십시오.

포트 개체

포트 개체는 여러 프로토콜을 조금씩 다른 방법으로 나타냅니다.

TCP 및 **UDP**

투명 레이어 프로토콜로서 괄호 안에 프로토콜 번호 및 관련 포트 또는 포트 범위가 선택적으로 표시되는 포트 개체입니다. 예: `TCP(6)/22`

ICMP, ICMPv6 (IPv6-ICMP)

인터넷 레이어 프로토콜 및 유형과 코드가 선택적으로 표시되는 포트 개체입니다. 예: `ICMP(1):3:3`

유형이나 가능한 경우 코드로 ICMP 또는 IPV6-ICMP 포트 개체를 제한할 수 있습니다. ICMP 유형 및 코드에 대한 자세한 내용은 다음을 참조하십시오.

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

기타

포트를 사용하지 않는 다른 프로토콜을 나타내는 포트 개체입니다.

Firepower System은 잘 알려진 포트에 기본 포트 개체를 제공합니다. 이런 포트 개체는 수정하거나 삭제할 수 없습니다. 기본 개체에 추가해 사용자 정의 포트 개체를 만들 수 있습니다.

액세스 제어 정책, ID 규칙, 네트워크 검색 규칙, 포트 변수, 이벤트 검색 등 시스템 웹 인터페이스의 다양한 위치에서 포트 개체 및 그룹을 사용할 수 있습니다. 예를 들어, 조직에서 특정 포트 범위를 사

용하는 사용자 지정 클라이언트를 사용하며 시스템에서 잘못된 이벤트를 과도하게 생성하는 경우, 이러한 포트의 모니터링을 제외하도록 네트워크 검색 정책을 구성할 수 있습니다.

포트 개체를 사용할 경우 다음 지침을 준수합니다.

- 액세스 제어 규칙에서 소스 포트 조건의 TCP 또는 UDP 이외의 다른 프로토콜을 추가할 수 없습니다. 또한, 규칙에서 소스 및 대상 포트 조건을 모두 설정할 때 전송 프로토콜을 조합할 수 없습니다.
- 소스 포트 조건에서 사용되는 포트 개체 그룹에 지원되지 않는 프로토콜을 추가한 경우 정책 적용 시 사용되는 규칙은 관리되는 디바이스에 반영되지 않습니다.
- 또한, TCP와 UDP 포트를 모두 포함하는 포트 개체를 만들고 이를 규칙의 소스 포트 조건으로 추가하는 경우 대상 포트를 추가할 수 없으며, 그 반대도 마찬가지입니다.

포트 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Port(**포트**)**를 선택합니다.

단계 **3** 드롭다운 목록의 **Add Port(**포트 추가**)**에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** **Protocol(**프로토콜**)**을 선택합니다.

단계 **6** 선택한 프로토콜에 따라 제한할 포트또는 ICMP 유형 및 코드를 선택합니다.

1 에서 **65535**까지의 포트를 입력할 수 있습니다. 포트 범위를 지정하려면 하이픈을 사용합니다. 기타 드롭다운 목록을 사용해 모든 프로토콜에 일치하도록 선택한 경우 포트에 따라 개체를 제한해야 합니다.

단계 **7** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 570 페이지의 내용을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

포트 개체 가져오기

포트 개체 가져 오기에 대한 자세한 내용은 개체 가져오기, 560 페이지를 참고하십시오.

애플리케이션 필터

시스템에서 제공되는 애플리케이션 필터는 유형, 위험, 사업 타당성, 카테고리, 태그라는 기본 특성에 따라 애플리케이션을 구성하여 애플리케이션 컨트롤을 수행할 수 있도록 지원합니다. 개체 관리자에서는 시스템에서 제공되는 필터 조합 또는 사용자 정의 애플리케이션 조합을 기반으로 재사용 가능한 사용자 정의 애플리케이션 필터를 생성 및 관리할 수 있습니다. 자세한 내용은 애플리케이션 조건(애플리케이션 컨트롤), 535 페이지를 참조하십시오.

VLAN 태그 개체

구성하는 각 VLAN 태그 객체는 VLAN 태그 또는 태그 범위를 나타냅니다.

VLAN 태그 개체를 그룹화할 수 있습니다. 그룹은 여러 개체를 나타냅니다. 단일 개체의 VLAN 태그 범위를 사용하는 것은 그룹으로 간주되지 않습니다.

규칙 및 이벤트 검색을 포함해 시스템 웹 인터페이스의 여러 위치에서 VLAN 태그 개체 및 그룹을 사용할 수 있습니다. 예를 들어 특정 VLAN에만 적용되는 액세스 제어 규칙을 작성할 수 있습니다.

VLAN 태그 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **VLAN tag(VLAN** 태그**)**를 선택합니다.

단계 **3** 드롭다운 목록의 **Add VLAN tag(VLAN** 태그 추가**)**에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** **VLAN** 태그 필드에 값을 입력합니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

단계 **7** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 570 페이지의 내용을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참조하십시오.

URL 개체

중요 보안 인텔리전스 설정에서 이 옵션 및 이와 유사한 옵션을 사용하는 방법 및 액세스 제어 및 QoS 정책의 URL 규칙에 대한 모범 사례는 수동 URL 필터링 옵션, 1680 페이지의 내용을 참조하십시오.

사용자가 구성한 각 URL 개체는 단일 URL 또는 IP 주소를 나타냅니다. 액세스 제어 정책 및 이벤트 검색을 포함해 시스템 웹 인터페이스의 여러 위치에서 URL 개체 및 그룹을 사용할 수 있습니다.

시스템은 사용자가 입력하는 URL에 대해 간단한 하위 문자열 일치를 확인합니다. 이는 반드시 예상한 값이 아닐 수도 있습니다. 수동 URL 필터링 옵션, 1680 페이지에서 일치하는 URL 예를 참조하십시오.

특히 암호화된 트래픽을 해독하거나 차단하는 SSL 검사를 설정하지 않고 URL 개체를 생성할 때 다음에 유의해야 합니다.

- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.
- URL 조건과 함께 액세스 제어 규칙을 사용하여 웹 트래픽을 매칭할 경우 시스템은 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹사이트를 차단하는 경우 규칙을 세분화하는 애플리케이션 조건을 사용하지 않는 한 해당 웹사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 이를테면 `http://example.com` 대신 `example.com`을 사용하십시오.

URL 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **URL**을 선택합니다.

단계 **3** 드롭다운 목록의 **Add URL(URL** 추가**)**에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** **URL** 또는 IP 주소를 입력합니다.

단계 **7** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 570 페이지의 내용을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

지리위치 개체

사용자가 구성한 각 지리위치 개체는 시스템이 사용자의 모니터링된 네트워크에서 트래픽의 소스 또는 대상으로 파악한 하나 이상의 국가 또는 대륙을 나타냅니다. 액세스 제어 정책, SSL 정책, 이벤트 검색 등 시스템 웹 인터페이스의 여러 위치에서 지리위치 개체를 사용할 수 있습니다. 예를 들어, 특정 국가를 오가는 트래픽을 차단하는 액세스 제어 규칙을 작성할 수 있습니다.

네트워크 트래픽을 필터링하기 위해 최신 정보를 사용하려면 정기적으로 지리위치 데이터베이스(GeoDB)를 업데이트할 것을 강력하게 권장합니다.

지리위치 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Geolocation(**지리위치**)**를 선택합니다.

단계 **3** **Add Geolocation(**지리위치 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 지리위치 개체에 포함할 국가와 대륙의 확인란을 선택합니다. 대륙을 선택하면 해당 대륙 내의 모든 국가와 GeoDB 업데이트가 향후 해당 대륙에 추가하는 모든 국가를 선택합니다. 대륙에 속한 모든 국가를 선택 취소하려면 대륙을 선택 취소합니다. 국가 및 대륙의 모든 조합을 선택할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참조하십시오.

보안 영역

보안 영역는 네트워크를 세그멘테이션하여 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다. 보안 영역는 인터페이스를 그룹화합니다. 이러한 그룹의 범위는 여러 디바이스를 포괄할 수 있으며, 단일 디바이스에서 여러 영역 를 구성할 수도 있습니다.

보안 영역의 모든 인터페이스는 모든 인라인, 수동, 스위칭, 라우팅 또는 ASA FirePOWER가 동일한 유형이어야 합니다. 보안 영역를 생성한 후에는 여기에 포함하는 인터페이스의 유형을 변경할 수 없습니다. 하나의 인터페이스는 하나의 영역에만 속할 수 있습니다.

개체 관리자의 보안 영역 페이지에는 매니지드 디바이스에 구성된 영역이 나열됩니다. 이 페이지에는 각 영역의 인터페이스 유형도 표시되며, 사용자는 각 영역를 확장하여 어느 디바이스의 어떤 인터페이스가 각 영역에 속하는지 볼 수 있습니다.

참고 인라인 집합에서 인터페이스용 보안 영역을 추가하기 전에 인라인 집합을 생성합니다. 그렇지 않으면 보안 영역이 제거되므로 다시 추가해야 합니다.

모델별 참고 사항 및 경고

7000 또는 8000 Series 디바이스의 초기 컨피그레이션 도중, 시스템에서는 사용자가 디바이스에 대해 선택한 탐지 모드를 기준으로 보안 영역을 생성합니다. 예를 들어 시스템이 패시브 구축에서는 Passive 영역을 생성하는 반면, 인라인 구축에서는 External 및 Internal 영역을 생성합니다. 디바이스를 Firepower Management Center에 등록하면 이러한 보안 영역이 FMC에 추가됩니다.

영역 및 멀티테넌시

다중 도메인 구축의 경우, 모든 수준에서 보안 영역를 생성할 수 있습니다. 상위 도메인에 생성된 영역는 다른 도메인의 디바이스에 상주하는 인터페이스를 포함할 수 있습니다. 이 경우, 개체 관리자에서 상위 영역 컨피그레이션을 보는 서브도메인 사용자는 해당 도메인에서 인터페이스만 볼 수 있습니다.

역할별로 제한하지 않는 한, 서브도메인 사용자는 상위 도메인에 생성된 영역를 보고 수정할 수 있습니다. 서브도메인 사용자는 이러한 영역에서 인터페이스를 추가하고 삭제할 수 있습니다. 그러나 영역를 삭제하거나 이름을 바꿀 수는 없습니다. 하위 도메인에 생성된 영역는 보거나 수정할 수 없습니다.

보안 영역 개체 생성

팁 빈 보안 영역를 만들고 여기에 인터페이스를 추가할 수 있습니다. 인터페이스를 추가하려면 인터페이스에 이름이 있어야 합니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 인터페이스를 구성하는 동안 보안 영역을 생성할 수도 있습니다.

시작하기 전에

- 각 보안 영역 유형의 사용 요구 사항 및 제한 사항을 이해합니다. 보안 영역, 577 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Security Zones(**보안 영역**)**를 선택합니다.

단계 **3** **Add Security Zone(**보안 영역 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** **Interface Type(**인터페이스 유형**)**을 선택합니다.

단계 **6** **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 드롭다운 목록에서 추가할 인터페이스가 포함된 디바이스를 선택합니다.

단계 **7** 하나 이상의 인터페이스를 선택합니다.

단계 **8** **Add(**추가**)**를 클릭하여 디바이스별로 그룹화된 선택한 인터페이스를 추가합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

시간 범위 개체

규칙을 적용할 시기를 결정하는 데 사용할 기간을 정의하려면 시간 범위 개체를 사용합니다.

시간 범위 개체 생성

특정 시간 범위에만 적용되는 정책을 원하는 경우 시간 범위 개체를 생성하고 정책에서 해당 개체를 지정합니다. 이 개체는 FTD 디바이스에서만 작동합니다.

이 항목의 하단에 나열된 정책 유형에서만 시간 범위 개체를 지정할 수 있습니다.

시작하기 전에

시간 범위는 트래픽을 처리하는 디바이스와 연결된 표준 시간대를 기준으로 적용됩니다. 기본적으로 UTC입니다. 디바이스와 연결된 표준 시간대를 변경하려면 **Device(**디바이스**) > Platform Settings(**플랫폼 설정**)**로 이동합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택합니다.

단계 **2** 개체 유형 목록에서 **Time Range(**시간 범위**)**를 선택합니다.

단계 **3** **Add Time Range(**시간 범위 추가**)**를 클릭합니다.

단계 **4** 값을 입력합니다.

다음 지침을 참조하십시오.

- 입력한 개체 이름 주변에 붉은색 오류 상자가 등장하는 경우 이름 필드 위로 마우스를 이동하여 이름 지정 제한 사항을 확인하십시오.
- **Device(**디바이스**) > Platform Settings(**플랫폼 설정**)**에서 디바이스의 표준 시간대를 지정하지 않는 한 모든 시간은 UTC로 표시됩니다.
- 24시간을 사용하여 시간을 입력합니다. 예를 들어 오후 1시 30분은 13시30분으로 입력합니다.
- 일반적인 주말 시간(저녁과 밤을 포함해 금요일 오후 5시부터 월요일 오전 8시까지)같은 단일 연속 범위를 지정하려면 범위 유형에서 **Range(**범위**)**를 선택합니다.
- 월요일부터 금요일까지 오전 8시부터 오후 5시까지(매일 저녁, 밤, 이른 아침 포함)와 같은 여러 날짜의 일부분만 지정하려면 범위 유형에서 **Daily Interval(**매일 간격**)**을 선택합니다.
- 단일 개체에서 최대 28개의 기간을 지정할 수 있습니다.
- 하루 중 연속되지 않는 시간 또는 며칠 동안 다른 시간대를 지정하려면 복수의 반복 간격을 생성합니다. 예를 들어 표준 근무 시간 외 항상 정책을 적용하려면 다음과 같은 두 가지 반복 간격을 포함하는 단일 시간 범위 개체를 생성합니다.
  - 월요일부터 금요일 오전 9시부터 오후 5시까지 매일 간격
  - 금요일 오후 5시부터 월요일 오전 8시까지 범위 반복 간격

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

다음 중 하나에서 시간 범위를 설정합니다.

- 액세스 제어 규칙

- 사전 필터 규칙
- 터널 규칙
- VPN 그룹 정책

VPN 그룹 정책 개체에서 **Access Hours(**액세스 시간**)** 필드를 사용하여 시간 범위 개체를 지정합니다. 자세한 내용은 그룹 정책 개체 설정, 656 페이지 및 그룹 정책 고급 옵션, 662 페이지 섹션을 참조해 주십시오.

표준 시간대 개체

매니지드 디바이스의 로컬 표준 시간대를 지정하려면 표준 시간대 개체를 생성하고 디바이스에 할당된 디바이스 플랫폼 설정 정책에 해당 개체를 지정합니다.

이 디바이스 로컬 시간은 액세스 제어, 사전 필터 및 VPN 그룹 정책과 같이 시간 범위를 지원하는 정책의 규칙에 시간 범위를 적용하는 데만 사용됩니다. 디바이스에 표준 시간대를 할당하지 않으면 이러한 정책에서 시간 범위를 적용할 때 UTC가 기본적으로 사용됩니다. Firepower 시스템의 다른 기능은 표준 시간대 개체에 지정된 표준 시간대를 사용하지 않습니다.

표준 시간대 개체는 Firepower Threat Defense 디바이스에서만 지원됩니다.

변수 집합

변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 규칙 삭제, 적응형 프로파일, 동적 규칙 상태의 IP 주소를 나타내려면 침입 정책 내 변수를 사용할 수도 있습니다.

팁 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다.

변수 집합을 사용하여 변수를 관리하고, 사용자 정의하며, 정렬합니다. 시스템이 제공하는 기본 변수 집합을 사용하거나 사용자 정의 집합을 생성할 수 있습니다. 모든 집합에서 사전 정의된 기본 변수를 수정하고 사용자가 정의한 변수를 추가하거나 수정할 수 있습니다.

Firepower System이 제공하는 대부분의 공유 개체 규칙 및 표준 텍스트 규칙은 사전 정의된 기본 변수를 사용하여 네트워크 및 포트 번호를 정의합니다. 예를 들어, 대부분의 규칙은 `$HOME_NET` 변수를 사용하여 보호된 네트워크를 지정하고 `$EXTERNAL_NET` 변수를 사용하여 보호되지 않은(또는 외부) 네트워크를 지정합니다. 또한, 전문 규칙은 종종 미리 정의된 다른 변수를 사용합니다. 예를 들어, 웹 서버에 대한 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

규칙은 변수가 더 정확하게 네트워크 환경을 반영할 때 더욱 효과적입니다. 적어도 기본 집합의 기본 변수를 수정해야 합니다. `$HOME_NET`과 같은 변수가 올바르게 네트워크를 정의하고 `$HTTP_SERVERS`가 네트워크에서 모든 웹 서버를 포함한다는 것을 확인함으로써 프로세스가 최적화되고 모든 관련 시스템에서 의심스러운 활동이 감시됩니다.

변수를 사용하려면, 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 관련된 침입 정책에 변수 집합을 연결합니다. 기본적으로, 기본 변수 집합은 액세스 제어 정책에 의해 사용된 모든 침입 정책에 연결됩니다.

어느 집합이든 변수를 추가하면 모든 집합에 변수가 추가됩니다. 즉 각 변수 집합은 시스템에서 현재 구성된 모든 변수의 집합입니다. 모든 변수 집합에서 사용자 정의 변수를 추가하거나 모든 변수의 값을 사용자 정의할 수 있습니다.

초기에 Firepower System은 사전 정의된 기본 값으로 구성된 단일 기본 변수 집합을 제공합니다. 기본 집합의 각 변수는 초기 기본값으로 설정되는데, 이때 사전 정의된 변수의 경우 Cisco Talos Intelligence Group(Talos)이 설정하고 규칙 업데이트에서 제공되는 값입니다.

미리 정의된 기본 변수가 해당 기본값으로 구성된 상태로 둘 수도 있지만, Cisco는 사용자가 미리 정의된 변수의 하위 집합을 변경할 것을 권장합니다.

기본 집합에서만 변수를 사용할 수 있지만 대부분의 경우 하나 이상의 사용자 지정 집합을 추가하고, 다양한 집합에서 여러 변수 값을 구성하며, 새로운 변수를 추가하는 것이 유용할 수 있습니다.

여러 집합을 사용할 때, 기본 집합 내 모든 변수의 현재 값이 다른 모든 집합 내 변수의 기본값을 결정한다는 점을 기억하는 것이 중요합니다.

개체 관리자 페이지에서 **Variable Sets(**변수 집합**)**을 선택할 때 개체 관리자는 기본 변수 집합 및 사용자가 생성한 모든 사용자 정의 집합을 나열합니다.

새롭게 설치된 시스템에서 기본 변수 집합은 Cisco가 사전에 정의한 기본 변수만으로 구성됩니다.

각 변수 집합은 시스템이 제공하는 기본 변수와 사용자가 모든 변수 집합에서 추가한 모든 사용자 변수를 포함합니다. 기본 집합을 수정할 수 있지만, 기본 집합을 변경하거나 삭제할 수 없다는 점을 참고하십시오.

다중 도메인 구축의 경우 시스템은 각 하위 도메인에 기본 변수 집합을 생성합니다.

주의 액세스 제어 정책 또는 침입 정책을 가져오는 경우, 기본 변수 집합의 기존 기본 변수를 가져온 기본 변수로 덮어씁니다. 기존 기본 변수 값 집합이 가져온 기본 변수 값 집합에 없는 사용자 지정 변수를 포함하는 경우, 고유 변수는 유지됩니다.

관련 항목

변수 관리, 593 페이지
변수 집합 관리, 592 페이지

침입 정책 내 변수 집합

기본적으로 Firepower System은 액세스 제어 정책에서 사용되는 모든 침입 정책에 기본 변수 집합을 연결합니다. 침입 정책을 사용하는 액세스 제어 정책을 구축하면 침입 정책에서 활성화한 침입 규칙이 연결된 변수 집합의 변수 값을 사용합니다.

액세스 제어 정책의 침입 정책에서 사용하는 사용자 정의 변수 집합을 수정하면 시스템은 액세스 제어 정책 페이지에서 해당 정책의 상태를 오래된 것으로 표시합니다. 사용자 변수 집합의 변경 내용을 반영하려면 액세스 제어 정책을 재구축해야 합니다. 기본 집합을 변경하면 시스템은 침입 정책을 사

용한 모든 액세스 제어 정책의 상태를 오래된 것으로 표시하며 변경 사항을 반영하려면 사용자는 모든 액세스 제어 정책을 재구축해야 합니다.

변수

변수는 다음 범주 중 하나에 속합니다.

기본 변수

Firepower System에서 제공한 변수 기본 변수의 이름을 변경하거나 삭제할 수 없으며, 해당 기본값을 변경할 수 없습니다. 그러나 기본 변수의 사용자 정의 버전을 만들 수 있습니다.

사용자 정의 변수

사용자가 생성한 변수 다음과 같은 변수를 포함합니다.

- 사용자 지정 기본 변수

  기본 변수 값을 수정할 때, 시스템은 변수를 Default Variables(기본 변수) 영역에서 Customized Variables(사용자 지정 변수) 영역으로 옮깁니다. 기본 집합의 변수 값이 사용자 지정 집합 내 변수의 기본값을 결정하기 때문에, 기본 집합의 기본 변수를 사용자 지정하면 다른 모든 집합 내 변수의 기본값을 수정합니다.

- 사용자 정의 변수

  사용자 고유의 변수를 추가 및 삭제할 수 있으며, 그 값을 다른 변수 집합 내에서 사용자 정의하고, 기본값에 사용자 지정 변수를 재설정할 수 있습니다. 사용자 정의된 변수를 재설정해도 사용자 정의된 변수 영역에 남아 있습니다.

  사용자 정의 변수의 유형은 다음과 같습니다.

  - *network* 변수는 네트워크 트래픽에서 호스트 IP 주소를 지정합니다.
  - *port* 변수는 각 유형에 대한 `any` 값을 포함하여 네트워크 트래픽에서 TCP 또는 UDP 포트를 지정합니다.

예를 들어 사용자 정의 표준 텍스트 규칙을 생성한 경우 트래픽을 정확하게 반영하기 위해 사용자 정의된 변수 또는 규칙 생성 프로세스를 간소화하는 바로가기를 추가하려고 할 수 있습니다. 또는 "비무장 지대"(또는 DMZ)의 트래픽만 검사하는 규칙을 생성하는 경우 해당 값이 노출된 서버 IP 주소를 나열하는 `$DMZ`라는 이름의 변수를 생성할 수 있습니다. 그러면 이 영역에 작성된 모든 규칙에서 `$DMZ` 변수를 사용할 수 있습니다.

고급 변수

Firepower System이 특정 조건에서 제공하는 변수 이러한 변수는 매우 제한적으로 구축됩니다.

사전 정의된 기본 변수

기본적으로 Firepower System은 사전 정의된 기본 값으로 구성된 단일 기본 변수 집합을 제공합니다. Cisco Talos Intelligence Group(Talos)은 기본 변수를 포함해 신규 및 업데이트된 침입 규칙과 다른 침입 규칙 요소를 제공하기 위해 규칙 업데이트를 사용합니다.

그러나 시스템이 제공하는 대부분의 침입 규칙은 사전 정의된 기본 변수를 사용하므로 이러한 변수에 대해 적절한 값을 설정해야 합니다. 네트워크의 트래픽을 확인하기 위해 변수 집합을 사용하는 방법에 따라 일부 또는 전체 변수 집합에서 이 기본 변수의 값을 수정할 수 있습니다.

주의 액세스 제어 정책 또는 침입 정책을 가져오는 경우, 기본 변수 집합의 기존 기본 변수를 가져온 기본 변수로 덮어씁니다. 기존 기본 변수 값 집합이 가져온 기본 변수 값 집합에 없는 사용자 지정 변수를 포함하는 경우, 고유 변수는 유지됩니다.

다음 표는 시스템이 제공하는 변수 및 일반적으로 수정하는 변수를 나타냅니다. 네트워크에 맞게 변수를 조정하는 방법을 확인하는 데 대한 지원을 받으려면 Professional Services(전문 서비스) 또는 Support(지원부)에 문의하십시오.

표 ***61:*** 시스템 제공 변수

변수 이름	설명	수정 여부
`$AIM_SERVERS`	알려진 AIM(AOL Instant Messenger) 서버에 대해 정의하며 채팅 기반 규칙 및 AIM 익스플로잇을 검색하는 규칙에서 사용됩니다.	필요하지 않음
`$DNS_SERVERS`	DNS(Domain Name Service) 서버에 대해 정의합니다. 특히 DNS 서버에 영향을 미치는 규칙을 작성하는 경우, `$DNS_SERVERS` 변수를 대상 또는 소스 IP 주소로 사용할 수 있습니다.	현재 규칙 집합에서 필요하지 않습니다.
`$EXTERNAL_NET`	Firepower System이 보호되지 않는 네트워크로 간주하는 네트워크에 대해 정의하며 외부 네트워크에 대한 많은 규칙에서 사용됩니다.	예, `$HOME_NET`을 적절하게 정의한 후 `$EXTERNAL_NET`에 대한 값에서 `$HOME_NET`을 제외해야 합니다.
`$FILE_DATA_PORTS`	암호화되지 않은 포트에 대해 정의하며 네트워크 스트림에서 파일을 탐지하는 침입 규칙에서 사용됩니다.	필요하지 않음
`$FTP_PORTS`	네트워크에서 FTP 서버의 포트에 대해 정의하고, FTP 서버 익스플로잇 규칙에 사용됩니다.	FTP 서버가 기본 포트 이외의 포트를 사용할 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음).
`$GTP_PORTS`	패킷 디코더가 GTP(GPRS[General Radio Packet Service] 터널링 프로토콜) PDU 내의 페이로드를 추출하는 데이터 채널 포트에 대해 정의합니다.	필요하지 않음

변수 이름	설명	수정 여부
$HOME_NET	관련된 침입 정책이 모니터링하는 네트워크에 대해 정의하며, 내부 네트워크를 정의하는 많은 규칙에서 사용됩니다.	예(내부 네트워크에 대한 IP 주소를 포함할 경우)
$HTTP_PORTS	네트워크에서 웹 서버의 포트에 대해 정의하고, 웹 서버 익스플로잇 규칙에 사용됩니다.	웹 서버가 기본 포트 이외의 포트를 사용하는 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음).
$HTTP_SERVERS	네트워크에서 웹 서버에 대해 정의합니다. 웹 서버 익스플로잇 규칙에 사용합니다.	예(HTTP 서버를 실행하는 경우)
$ORACLE_PORTS	네트워크에서 Oracle(오라클) 데이터베이스 서버 포트에 대해 정의하고, Oracle(오라클) 데이터베이스 공격을 검색하는 규칙에서 사용됩니다.	예(Oracle(오라클) 서버를 실행하는 경우)
$SHELLCODE_PORTS	시스템이 셸 코드 코드 익스플로잇을 검색하기를 원하는 포트에 대해 정의하고, 셸 코드를 사용하는 익스플로잇을 탐지하는 규칙에서 사용됩니다.	필요하지 않음
$SIP_PORTS	네트워크에서 SIP 서버 포트에 대해 정의하고, SIP 익스플로잇 규칙에 사용됩니다.	필요하지 않음
$SIP_SERVERS	네트워크에서 SIP 서버에 대해 정의하고, SIP 대상 익스플로잇을 처리하는 규칙에서 사용됩니다.	예(SIP 서버를 실행하는 경우), $HOME_NET을 적절하게 정의한 후 $HOME_NET을 $SIP_SERVERS에 대한 값으로 포함해야 합니다.
$SMTP_SERVERS	네트워크에서 SMTP 서버에 대해 정의하고, 메일 서버를 대상으로 하는 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SMTP 서버를 실행하는 경우)
$SNMP_SERVERS	네트워크에서 SNMP 서버에 대해 정의하고, SNMP 서버에서 공격을 검색하는 규칙에 사용됩니다.	예(SNMP 서버를 실행하는 경우)
$SNORT_BPF	이후에 5.3.0 이상으로 업그레이드한 Firepower System 소프트웨어 릴리스 5.3.0 이하 시스템에 레거시 고급 변수가 등장하는 경우를 식별합니다.	아니요, 이 변수를 보거나 삭제하는 것만 가능합니다. 삭제한 다음 수정하거나 복원할 수 없습니다.

변수 이름	설명	수정 여부
$SQL_SERVERS	네트워크의 데이터베이스 서버에 대해 정의하고 데이터베이스 대상 익스플로잇을 처리하는 규칙에서 사용됩니다.	예(SQL Server를 실행하는 경우)
$SSH_PORTS	네트워크에서 SSH 서버의 포트에 대해 정의하고, SSH 서버 익스플로잇 규칙에 사용됩니다.	SSH 서버가 기본 포트 이외의 포트를 사용하는 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음)
$SSH_SERVERS	네트워크의 SSH 서버에 대해 정의하고 SSH를 대상으로 한 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SSH 서버를 실행하는 경우), $HOME_NET을 적절하게 정의한 후 $HOME_NET을 $SSH_SERVERS에 대한 값으로 포함해야 합니다.
$TELNET_SERVERS	네트워크에서 알려진 텔넷 서버에 대해 정의하고 텔넷 서버를 대상으로 한 익스플로잇을 해결하는 규칙에 사용됩니다.	예(텔넷 서버를 실행하는 경우)
$USER_CONF	웹 인터페이스를 통해 사용이 불가능한 하나 이상의 기능을 구성하는 일반 도구를 제공합니다. 충돌 또는 중복 $USER_CONF 구성은 시스템을 중단시킵니다.	아니요(기능 설명의 지침에 따른 경우 또는 Support(지원부)의 안내에 따른 경우에만 해당)

네트워크 변수

네트워크 변수는 침입 정책 및 침입 정책 규칙 억제, 다이내믹 규칙 상태 및 적응형 프로파일에서 활성화할 수 있는 침입 규칙에서 사용할 수 있는 IP 주소를 나타냅니다. 네트워크 개체 및 네트워크 개체 그룹과 다른 네트워크 변수는 침입 정책 및 침입 규칙에 특정되며 사용자는 네트워크 개체 및 그룹을 사용하여 액세스 제어 정책, 네트워크 변서, 침입 규칙, 네트워크 검색 규칙, 이벤트 검색, 보고서 등 시스템 웹 인터페이스 내 여러 위치의 IP 주소를 대표합니다.

다음 구성의 네트워크 변수를 사용하여 네트워크에 호스트의 IP 주소를 지정할 수 있습니다.

- 침입 규칙 - 침입 규칙 **Source IPs(**소스 **IP)** 및 **Destination IPs(**대상 **IP)** 헤더 필드는 특정 IP 주소에서 시작되었거나 특정 IP 주소로 향하는 패킷 검사를 제한할 수 있습니다.
- 억제 - 소스 또는 대상 침입 규칙 억제의 **Network(**네트워크**)** 필드는 특정 IP 주소 또는 IP 주소 범위가 침입 규칙 또는 프리프로세서를 트리거할 때 침입 이벤트 알림을 억제하도록 할 수 있습니다.
- 다이내믹 규칙 상태 - 소스 또는 대상 다이내믹 규칙 상태의 **Network(**네트워크**)** 필드는 지정된 기간 동안 하나의 침입 규칙 또는 프리프로세서 규칙에 대한 일치가 과도하게 발생하는 경우를 탐지합니다.
- 적응형 프로파일 - 적응형 프로파일 네트워크 필드는 패킷 프래그먼트 및 TCP 스트림의 리어셈블리를 개선하는 호스트를 식별합니다.

이 섹션에서 식별된 필드에 변수를 사용할 때, 사용자가 침입 정책에 연결하는 변수 집합은 침입 정책을 사용하는 액세스 제어 정책에 의해 처리된 네트워크 트래픽에서 변수 값을 결정합니다.

변수에 다음 네트워크 구성의 모든 조합을 추가할 수 있습니다:

- 네트워크 변수, 네트워크 개체 및 사용 가능한 네트워크 목록에서 선택하는 네트워크 개체 그룹의 조합
- New Variable(새 변수) 페이지 또는 Edit Variable(변수 수정) 페이지에서 추가한 후 사용자 변수 및 기타 기존 및 이후 변수에 추가할 수 있는 개별 네트워크 개체
- 리터럴, 단일 IP 주소 또는 주소 블록

  여러 리터럴 IP 주소 및 주소 블록 각각을 개별적으로 추가하여 나열할 수 있습니다. IPv4 및 IPv6 주소와 주소 블록을 단독으로 또는 조합하여 나열할 수 있습니다. IPv6 주소를 지정할 때, RFC 4291에 정의된 주소 지정 규칙을 사용할 수 있습니다.

추가한 모든 변수의 네트워크에 포함된 기본값은 `any`이며, 이는 모든 IPv4 또는 IPv6 주소를 나타냅니다. 제외된 네트워크 기본값은 `없으며` 이는 네트워크 없음을 나타냅니다. 또한 포함된 네트워크 목록에서 모든 IPv6 주소를 나타내는 리터럴 값으로, 또는 제외 목록에서 IPv6 주소 없음으로 주소 `::`를 지정할 수 있습니다.

제외한 목록에 네트워크를 추가하면 지정된 주소 및 주소 블록을 무효화합니다. 즉 제외된 IP 주소 또는 주소 블록을 제외한 모든 IP 주소와 일치시킬 수 있습니다.

예를 들어, 리터럴 주소 `192.168.1.1`을 제외하면 192.168.1.1을 제외한 모든 IP 주소가 지정되며, `2001:db8:ca2e::fa4c`를 제외하면 2001:db8:ca2e::fa4c를 제외한 모든 IP 주소가 지정됩니다.

리터럴 또는 가용 네트워크를 사용하여 모든 네트워크의 조합을 제외할 수 있습니다. 리터럴 값 `192.168.1.1`과 `192.168.1.5`를 제외하면 192.168.1.1 또는 192.168.1.5 이외의 IP 주소를 포함합니다. 즉 시스템은 이를 "192.168.1.1이 아니고 192.168.1.5도 아닌 것"으로 해석하며, 이는 괄호 사이에 나열된 IP 주소를 제외한 모든 IP 주소에 일치하는 것입니다.

네트워크 변수를 추가하거나 수정할 때는 다음 사항에 유의하십시오.

- 논리적으로 `any` 값을 제외할 수 없습니다. 제외할 경우, 이는 어떤 주소도 나타내지 않습니다. 예를 들면 제외된 네트워크의 목록에 값 `any`의 변수를 추가할 수 없습니다.
- 네트워크 변수는 지정된 침입 규칙 및 침입 정책 기능의 트래픽을 식별합니다. 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다.
- 제외된 값은 포함된 값의 하위 집합을 확인해야 합니다. 예를 들어, 192.168.5.0/24 주소 블록을 포함하거나 192.168.6.0/24를 제외할 수 없습니다.

포트 변수

포트 변수는 사용자가 침입 정책에서 활성화한 침입 규칙 내 **Source Port(**소스 포트**)** 및 **Destination Port(**대상 포트**)** 헤더 필드에서 사용할 수 있는 TCP 및 UDP 포트를 나타냅니다. 포트 변수는 포트 개체 및 포트 개체 그룹과 달리 침입 규칙에 특정적입니다. TCP 및 UDP에 대한 포트 개체를 생성할 수

있고 포트 변수, 액세스 제어 정책, 네트워크 검색 규칙, 이벤트 검색 등 시스템 웹 인터페이스의 여러 위치에서 포트 개체를 사용할 수 있다.

특정 TCP 또는 UDP 포트에서 오거나 그 포트로 이동하는 패킷으로 패킷 검사를 제한하려면 **Source Port** 및 **Destination Port** 헤더 필드의 침입 규칙에서 포트 변수를 사용할 수 있습니다.

이 필드에 변수를 사용할 때, 액세스 제어 규칙 또는 정책과 관련된 침입 정책에 연결한 변수 집합은 액세스 제어 정책을 적용하는 네트워크 트래픽에서 해당 변수의 값을 결정합니다.

변수에 다음 포트 구성의 모든 조합을 추가할 수 있습니다

- 사용 가능한 포트 목록에서 선택하는 포트 변수 및 포트 개체의 모든 조합

  사용 가능한 포트 목록이 포트 개체 그룹을 표시하지 않는다는 점과 변수에 이를 추가할 수 없다는 점에 주의하십시오.

- New Variable(새 변수) 페이지 또는 Edit Variable(변수 수정) 페이지에서 추가한 후 사용자 변수 및 기타 기존 및 이후 변수에 추가할 수 있는 개별 포트 개체

  각 유형의 `any` 값을 포함하여 TCP 및 UDP 포트만이 유효한 변수 값입니다. 유효한 변수 값이 아닌 유효한 포트 개체를 추가하기 위해 새 변수 페이지 또는 변수 수정 페이지를 사용할 경우, 개체는 시스템에 추가되지만 가용 개체 목록에 표시되지 않습니다. 개체 관리자를 사용하여 변수에 사용되는 포트 개체를 수정할 때, 유효한 변수 값에 대해 값을 변경하기만 할 수 있습니다.

- 단일, 리터럴 포트 값 및 포트 범위

  대시(-)로 포트 범위를 구분해야 합니다. 콜론(:)으로 표시된 포트 범위는 이전 버전 호환성을 위해 지원되지만 사용자가 생성하는 포트 변수에 콜론을 사용할 수 없습니다.

  여러 리터럴 포트 값 및 범위를 어떤 조합에서나 각각 개별적으로 추가하여 나열할 수 있습니다.

포트 변수를 추가하거나 수정할 때는 다음 사항에 유의하십시오.

- 추가한 모든 변수의 포트에 포함된 기본값은 `any`이며, 이는 모든 포트 또는 포트 범위를 나타냅니다. 제외한 포트에 대한 기본값은 `none`이며, 이는 아무 포트도 없음을 나타냅니다.

  팁 값 `any`의 변수를 생성하려면 특정 값을 추가하지 않은 채 변수의 이름을 지정하고 저장하십시오.

- 논리적으로 `any` 값을 제외할 수 없습니다. 제외할 경우, 이는 어떤 포트도 나타내지 않습니다. 예를 들어 제외된 포트의 목록에 값 `any`의 변수를 추가하면 변수 집합을 저장할 수 없습니다.
- 제외한 목록에 포트를 추가하면 지정된 포트 및 포트 범위가 무효화됩니다. 즉 제외된 포트 또는 포트 범위를 제외한 모든 포트와 일치시킬 수 있습니다.
- 제외된 값은 포함된 값의 하위 집합을 확인해야 합니다. 예를 들어, 포트 범위 10-50을 포함하거나 포트 60을 제외할 수 없습니다.

고급 변수

고급 변수는 웹 인터페이스를 통해 구성해야 하는 기능을 구성할 수 있습니다. Firepower System은 현재 하나의 고급 변수인 USER_CONF 변수만 제공합니다.

USER_CONF

USER_CONF는 웹 인터페이스를 통해 구성해야 하는 하나 이상의 기능을 구성하는 일반 도구를 제공합니다.

주의 기능 설명에서 또는 Support(지원부)를 통해 침입 정책 기능을 구성하라는 안내를 받지 않은 한 침입 정책 기능을 구성하기 위해 USER_CONF 고급 변수를 사용하지 마십시오. 충돌이나 이중 설정은 시스템을 중단시킵니다.

USER_CONF를 수정할 때, 단일 회선에 총 최대 4096개의 문자를 입력할 수 있습니다. 회선은 자동으로 래핑됩니다. 디스크 공간과 같은 변수 또는 물리적 제한을 위한 8192개의 최대 문자 길이에 도달할 때까지 유효한 지침 또는 회선을 원하는 만큼 포함할 수 있습니다. 명령 지시어의 모든 전체 인수 뒤에 백슬래시(\) 줄 연속 문자를 사용합니다.

USER_CONF를 재설정하면 빈 상태로 남게 됩니다.

변수 재설정

새 변수 페이지 또는 변수 수정 페이지에서 변수 집합의 기본값에 변수를 재설정할 수 있습니다. 다음 표는 변수 재설정의 기본 원칙에 대해 요약합니다.

표 ***62:*** 변수 재설정 값

재설정할 변수 유형	집합 유형	재설정
기본	기본값	규칙 업데이트 값
사용자 정의	기본값	`any`
기본 또는 사용자 정의	사용자 지정	현재 기본 설정값(변경되거나 변경되지 않은)

사용자 지정 집합의 변수를 재설정하면 기본 집합에서 해당 변수의 현재 값으로 재설정되기만 합니다.

반대로, 기본 집합의 변수 값을 재설정하거나 변경하면 모든 사용자 지정 집합에서 해당 변수의 기본값이 항상 업데이트됩니다. 재설정 아이콘이 회색으로 비활성화된 경우, 이는 변수를 재설정할 수 없음을 나타내므로, 이는 해당 설정에서 변수에 사용자 정의된 값이 없음을 의미합니다. 사용자 지정 집합의 변수 값을 사용자 정의하지 않는 한, 기본 집합의 변수를 수정하면 변수 집합에 연결한 침입 정책에서 사용되는 값이 업데이트됩니다.

참고 변경 사항이 연결된 사용자 지정 집합의 변수를 사용하는 침입 정책에 영향을 미치는 방식을 평가하기 위해 기본 집합의 변수를 변경해 보는 것이 좋습니다. 사용자 지정 집합의 변수 값을 사용자 지정하지 않은 경우 특히 그렇습니다.

재설정 값을 보려면 변수 집합에서 재설정 아이콘 위에 마우스 포인터를 올려놓으면 됩니다. 사용자 지정 값과 재설정 값이 동일한 경우, 이는 다음 중 하나를 나타냅니다.

- 값 `any`로 변수를 추가한 맞춤형 또는 기본 집합에 있는 것임
- 고유한 값을 가진 변수를 추가하고 기본값으로 구성된 값을 사용하도록 선택한 사용자 지정 집합에 있는 것입니다

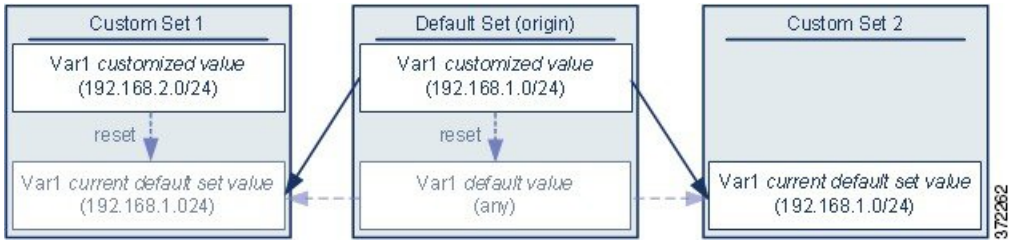
집합에 변수 추가

변수 집합에 변수를 추가하면 다른 모든 집합에 추가됩니다. 사용자 지정 집합에서 변수를 추가할 때 구성된 값을 기본 집합의 사용자 지정 값으로 사용할지 선택해야 합니다.

- 설정된 값**(**예**: 192.168.0.0/16)**을 사용하는 경우, 변수가 설정된 값을 기본값 `any`와 함께 사용자 지정 값으로 사용하는 기본 집합에 추가됩니다. 기본 집합의 현재 값이 다른 집합의 기본값을 결정하기 때문에, 다른 사용자 지정 집합의 초기 기본값은 구성된 값(예에서는 192.168.0.0/16)입니다.
- 설정된 값을 사용하지 않는 경우**,** 기본값 `any`만을 사용하여 변수가 기본 집합에 추가되므로 다른 사용자 지정 집합의 초기 기본값은 `any`가 됩니다.

예**:** 기본 집합에 사용자 정의 변수 추가

다음 다이어그램은 `192.168.1.0/24` 값이 있는 기본 집합에 사용자 정의 변수 `Var1`을 추가할 때의 집합 상호 작용에 대해 설명합니다.



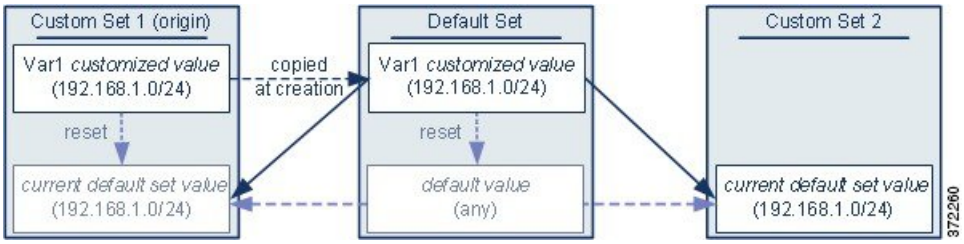
모든 집합에서 `Var1` 의 값을 사용자 지정할 수 있습니다. `Var1`이 사용자 정의되지 않은 사용자 지정 집합 2에서 해당 값은 `192.168.1.0/24`입니다. 사용자 지정 집합 1에서 `Var1`의 사용자 정의 값 `192.168.2.0/24`은 기본값을 오버라이드합니다. 기본 집합에서 사용자 정의 변수를 재설정하면 모든 집합에서 기본값을 `any`로 재설정합니다.

이 예에서 특히 주의해야 할 점은, 사용자가 `Var1`을 사용자 지정 집합 2에서 업데이트하지 않는 경우, 기본 집합에서 `Var1`을 사용자 지정하거나 재설정하면 결과적으로 사용자 지정 집합 2의 현재 `Var1` 기본값이 업데이트되며, 따라서 변수 집합에 연결된 모든 침입 규칙에 영향을 준다는 점입니다.

예에 표시되지 않지만 집합 간의 상호작용은 기본 집합의 기본 변수를 재설정하여 현재 규칙 업데이트에 의해 구성된 값을 재설정하지 않는 경우 사용자 정의 변수와 기본 변수에 대해 동일합니다.

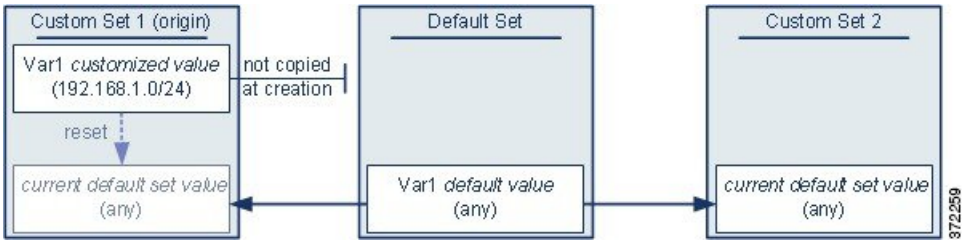
예: 맞춤형 집합에 사용자 정의 변수 추가

다음 두 가지 예는 사용자 정의 집합에 사용자 정의 변수를 추가할 때의 변수 집합 상호 작용에 대해 설명합니다. 새로운 변수를 저장할 때, 다른 집합에 대해 구성된 값을 기본값으로 사용하도록 설정할지 묻는 메시지가 표시됩니다. 다음 예에서, 구성된 값을 사용하도록 선택합니다.



사용자 지정 집합 1에서 `Var1`의 출처를 제외하고 이 예는 사용자가 기본 집합에 `Var1`을 추가한 위 예와 동일합니다. `Var1`에 대한 사용자 지정 값 `192.168.1.0/24`를 사용자 지정 집합 1에 추가하면 해당 값을 기본값 `any`와 함께 사용자 지정 값으로 기본 집합에 복사합니다. 따라서, `Var1` 값과 상호 작용은 사용자가 `Var1`을 기본 집합에 추가한 경우와 동일합니다. 이전 예와 마찬가지로, 기본 집합에서 `Var1`을 사용자 지정하거나 재설정하면 결과적으로 사용자 지정 집합 2의 현재 `Var1` 기본값이 업데이트되며, 따라서 변수 집합에 연결된 모든 침입 정책에 영향을 준다는 점에 유의하십시오.

다음 예에서는 이전 예처럼 값 192.168.1.0/24의 `Var1`을 Custom Set 1에 추가하되, `Var1`의 구성된 값을 다른 집합의 기본값으로 사용하지 않기로 선택합니다.



이 접근 방식은 `Var1`을 기본값 `any`를 가진 모든 집합에 추가합니다. `Var1`을 추가한 후 모든 집합의 값을 사용자 정의할 수 있습니다. 이 접근 방식의 이점은 기본 집합에서 `Var1`을 초기에 사용자 정의하지 않음으로써 기본 집합에서 값을 사용자 정의하여 `Var1`을 사용자 정의하지 않은 사용자 지정 집합 2와 같은 집합에서 현재 값을 부주의하게 변경하는 것의 위험을 줄일 수 있다는 것입니다.

중첩 변수

중첩 순환이 아닌 경우 변수를 중첩할 수 있습니다. 중첩된 부정 변수는 지원하지 않습니다.

유효한 중첩 변수

이 예에서는 SMTP_SERVERS, HTTP_SERVERS, OTHER_SERVERS가 유효한 중첩 변수입니다.

변수	유형	포함된 네트워크	제외된 네트워크
SMTP_SERVERS	사용자 지정 기본	10.1.1.1	—
HTTP_SERVERS	사용자 지정 기본	10.1.1.2	—
OTHER_SERVERS	사용자 정의	10.2.2.0/24	—
HOME_NET	사용자 지정 기본	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

유효하지 않은 중첩 변수

이 예에서는 HOME_NET의 중첩이 순환되므로 유효하지 않은 중첩 변수입니다. 즉 이는 HOME_NET을 포함한 OTHER_SERVERS을 정의하며 그 안에서 HOME_NET이 중첩됩니다.

변수	유형	포함된 네트워크	제외된 네트워크
SMTP_SERVERS	사용자 지정 기본	10.1.1.1	—
HTTP_SERVERS	사용자 지정 기본	10.1.1.2	—
OTHER_SERVERS	사용자 정의	10.2.2.0/24 HOME_NET	—
HOME_NET	사용자 지정 기본	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

지원되지 않는 중첩 부정 변수

중첩된 부정 변수는 지원되지 않기 때문에 이 예에서 보호된 네트워크 외부의 IP 주소를 나타내는 NONCORE_NET 변수를 사용할 수 없습니다.

변수	유형	포함된 네트워크	제외된 네트워크
HOME_NET	사용자 지정 기본	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	사용자 지정 기본	—	HOME_NET
DMZ_NET	사용자 정의	10.4.0.0/16	—
NOT_DMZ_NET	사용자 정의	—	DMZ_NET

변수	유형	포함된 네트워크	제외된 네트워크
NONCORE_NET	사용자 정의	EXTERNAL_NET NOT_DMZ_NET	—

다른 지원되지 않는 중첩 부정 변수

위의 다른 예에서는 이 예에 표시된 대로 NONCORE_NET 변수를 생성해 보호된 네트워크 외부의 IP 주소를 표시할 수 있습니다.

변수	유형	포함된 네트워크	제외된 네트워크
HOME_NET	사용자 지정 기본	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	사용자 정의	10.4.0.0/16	—
NONCORE_NET	사용자 정의	—	HOME_NET DMZ_NET

변수 집합 관리

변수 집합을 사용하려면 위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Variable Set(**변수 집합**)**을 선택합니다.

단계 **3** 변수 세트 관리:

- 추가 - 사용자 정의 변수 집합을 추가하려면 **Add Variable Set(**변수 집합 추가**)**를 클릭합니다. 변수 집합 생성, 593 페이지를 참조하십시오.
- 삭제 - 사용자 지정 변수 집합을 삭제하려면 변수 집합 옆의 삭제( )을 클릭하고 예를 클릭합니다. 기본 변수 집합 또는 상위 도메인에 속한 변수 집합을 삭제할 수 없습니다.

  참고 삭제한 변수 집합에서 생성된 변수는 삭제되거나 다른 집합에 영향을 받지 않습니다.

- 편집 - 변수 세트를 편집하려면 수정하려는 변수 집합 옆의 수정( )을 클릭합니다. 개체 수정, 563 페이지의 내용을 참조하십시오.
- 필터 - 이름으로 변수 집합을 필터링하려면 이름을 입력합니다. 입력하는 동안 페이지가 새로 고침되며 일치하는 이름을 표시합니다. 이름 필터링을 삭제하고 싶은 경우 필터 필드의 지우기( )을 클릭합니다.
- 변수 관리 - 변수 집합에 포함된 변수를 관리하려면 변수 관리, 593 페이지의 내용을 참조하십시오.

변수 집합 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Variable Set(**변수 집합**)**을 선택합니다.

단계 **3** **Add Variable Set(**변수 집합 추가**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** 집합의 변수를 관리하려면 변수 관리, 593 페이지의 내용을 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

변수 관리

위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Variable Set(**변수 집합**)**을 선택합니다.

단계 **3** 편집하려는 변수 집합 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 변수 관리

- 표시 - 변수에 대한 완전한 값을 표시하려는 경우 변수 옆 값 열의 값 위로 마우스를 이동합니다.
- 추가 - 변수를 추가하려면 **Add(**추가**)**를 클릭합니다. 변수 추가, 594 페이지를 참조하십시오.
- 삭제 - 변수 옆의 삭제( )를 클릭합니다. 변수를 추가한 뒤 변수 집합을 저장한 경우 변수를 삭제하려면 **Yes(**예**)**를 클릭합니다.

  다음은 삭제가 불가능합니다.

  - 기본 변수
  - 침입 규칙 또는 다른 변수에서 사용되는 사용자 정의 변수
  - 상위 도메인에 속하는 변수

- 편집 - 편집하려는 변수 옆에 있는 수정( )을 클릭합니다. 변수 편집, 595 페이지의 내용을 참조하십시오.
- 재설정 - 수정된 변수를 기본값으로 재설정하려는 경우, 수정된 변수 옆의 **Reset(**재설정**)**을 클릭합니다. 재설정 아이콘이 흐리게 표시되는 경우, 다음 중 하나에 해당합니다.
  - 현재 값은 이미 기본 값입니다.
  - 설정이 상위 도메인에 속합니다.

  팁 기본값을 표시하려면 활성 재설정 위에 마우스 포인터를 올려놓습니다.

단계 **5** 변수 집합을 저장하려면 **Save(**저장**)**을 클릭합니다. 변수 집합이 액세스 제어 정책에서 사용 중인 경우 변경 사항을 저장하려면 **Yes(**예**)**를 클릭합니다.

기본 집합의 현재 값이 다른 모든 집합의 기본값을 결정하기 때문에 기본 집합의 변수를 수정하거나 재설정하면 기본값을 사용자 정의하지 않은 집합에서 현재 값이 변경됩니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참조하십시오.

변수 추가

위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

프로시저

단계 **1** 변수 집합 편집기에서 **Add(**추가**)**를 클릭합니다.

단계 **2** 고유한 변수 **Name(**이름**)**을 입력합니다.

단계 **3** **Type(**유형**)** 드롭다운 목록에서 **Network(**네트워크**)** 또는 **Port(**포트**)**를 선택합니다.

단계 **4** 변수 값을 지정합니다.

- 사용 가능한 네트워크 또는 포트 목록에서 항목을 포함 또는 제외 항목으로 이동하려면 하나 이상의 항목을 선택하고 드래그앤드롭을 사용하거나 **Include(**포함**)** 또는 **Exclude(**제외**)**를 클릭합니다.

  팁 네트워크 또는 포트 변수에 대해 포함되거나 제외된 목록에서 주소 또는 포트가 중복되는 경우, 제외된 주소 또는 포트가 우선합니다.

- 단일 리터럴 값을 입력한 다음 **Add(**추가**)**를 클릭합니다. 네트워크 변수에 대해, 단일 IP 주소 또는 주소 블록을 입력할 수 있습니다. 포트 변수의 경우 단일 포트 또는 포트 범위를 추가할 수 있는데, 하이픈(-)으로 높은 값과 낮은 값을 나눕니다. 여러 문자 값을 입력하기 위해 필요한 만큼 이 단계를 반복합니다.
- 포함되거나 제외된 목록에서 항목을 제거하려면 항목 옆의 삭제( )를 클릭합니다.

참고 포함 또는 제외할 항목 목록은 리터럴 문자열 및 기존 변수, 개체, 네트워크 변수일 경우 네트워크 개체 그룹의 모든 조합으로 구성될 수 있습니다.

단계 **5** **Save(**저장**)**을 클릭하여 변수를 저장합니다. 사용자 지정 집합에서 새로운 변수를 추가하는 경우 다음과 같은 옵션을 사용할 수 있습니다.

- 구성된 값을 기본 집합의 맞춤화된 값으로 사용하는 변수를 추가하여 다른 맞춤형 집합의 기본값이 되도록 하려면 **Yes(**예**)**를 클릭합니다.
- 변수를 기본 집합 및 다른 사용자 정의 집합에 `Any(모든)` 기본값으로 추가하려면 **No(**아니오**)**를 클릭합니다.

단계 **6** 변수 집합을 저장하려면 **Save(**저장**)**을 클릭합니다. 변경 사항이 저장되며 변수 집합이 연결된 모든 액세스 제어 정책이 오래된 상태로 표시됩니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참조하십시오.

변수 편집

위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

사용자 정의 및 기본 변수를 편집할 수 있습니다.

기존 변수의 이름 또는 유형을 변경할 수 없습니다.

프로시저

단계 **1** 변수 집합 편집기에서 수정하려는 변수 옆의 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **2** 변수를 수정합니다.

- 사용 가능한 네트워크 또는 포트 목록에서 항목을 포함 또는 제외 항목으로 이동하려면 하나 이상의 항목을 선택하고 드래그앤드롭을 사용하거나 **Include(**포함**)** 또는 **Exclude(**제외**)**를 클릭합니다.

  팁 네트워크 또는 포트 변수에 대해 포함되거나 제외된 목록에서 주소 또는 포트가 중복되는 경우, 제외된 주소 또는 포트가 우선합니다.

- 단일 리터럴 값을 입력한 다음 **Add(**추가**)**를 클릭합니다. 네트워크 변수에 대해, 단일 IP 주소 또는 주소 블록을 입력할 수 있습니다. 포트 변수의 경우 단일 포트 또는 포트 범위를 추가할 수 있는데, 하이픈(-)으로 높은 값과 낮은 값을 나눕니다. 여러 문자 값을 입력하기 위해 필요한 만큼 이 단계를 반복합니다.
- 포함되거나 제외된 목록에서 항목을 제거하려면 항목 옆의 삭제( )를 클릭합니다.

참고 포함 또는 제외할 항목 목록은 리터럴 문자열 및 기존 변수, 개체, 네트워크 변수일 경우 네트워크 개체 그룹의 모든 조합으로 구성될 수 있습니다.

단계 **3** **Save(**저장**)**을 클릭하여 변수를 저장합니다.

단계 **4** 변수 집합을 저장하려면 **Save(**저장**)**을 클릭합니다. 변수 집합이 액세스 제어 정책에서 사용 중인 경우 변경 사항을 저장하려면 **Yes(**예**)**를 클릭합니다. 변경 사항이 저장되며 변수 집합이 연결된 모든 액세스 제어 정책이 오래된 상태로 표시됩니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참조하십시오.

보안 인텔리전스 목록 및 피드

보안 인텔리전스 기능을 사용하려면 위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

보안 인텔리전스 목록 및 피드는 목록 또는 피드의 항목과 일치하는 트래픽을 빠르게 필터링하는 데 사용할 수 있는 IP 주소, 도메인 이름 및 URL의 모음입니다.

- 목록은 수동으로 관리하는 정적 컬렉션입니다.
- 피드는 HTTP 또는 HTTPS의 간격에 따라 업데이트되는 동적 컬렉션입니다.

보안 인텔리전스 목록/피드는 다음과 같이 그룹화됩니다.

- DNS(도메인 이름)
- 네트워크(IP 주소)
- URL

시스템에서 제공한 피드

Cisco에서는 다음과 같은 피드를 보안 인텔리전스 개체로 제공합니다.

- 보안 인텔리전스 피드가 Talos에서 최신 위협 인텔리전스로 정기적으로 업데이트됩니다.
  - Cisco-DNS-and-URL-Intelligence-Feed(DNS 목록 및 피드 아래)
  - Cisco-Intelligence-Feed(IP 주소의 경우, 네트워크 목록 및 피드 아래)

  시스템에서 제공한 피드는 삭제할 수 없지만 업데이트 빈도는 변경(또는 비활성화)할 수 있습니다.

사전 정의된 목록: 전역 차단 목록 및 전역 차단 안 함 목록

시스템은 도메인(DNS), IP 주소(네트워크) 및 URL에 대해 사전 정의된 전역 차단 목록 및 차단 안 함 목록과 함께 제공됩니다.

이러한 목록은 사용자가 입력할 때까지 비어 있습니다. 이러한 목록을 작성하려면 글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지의 내용을 참조하십시오.

기본적으로, 액세스 제어 및 DNS 정책은 이러한 목록을 보안 인텔리전스의 일부로 사용합니다.

커스텀 피드

타사 피드를 사용하거나 내부 맞춤형 피드를 통해 여러 Firepower Management Center 어플라이언스를 포함하는 대규모 구축에서 전사적인 차단 목록을 손쉽게 유지 관리할 수 있습니다.

맞춤형 보안 인텔리전스 피드, 605 페이지의 내용을 참조하십시오.

맞춤형 목록

맞춤형 목록은 피드 및 Global(전역) 목록을 보강 및 세부 조정할 수 있습니다.

맞춤형 보안 인텔리전스 목록, 607 페이지의 내용을 참조하십시오.

보안 인텔리전스 목록 및 피드 사용처

- IP 주소 및 주소 블록 — 액세스 제어 정책에서 보안 인텔리전스의 일부로 차단 및 차단 안 함 목록을 사용합니다.
- 도메인 이름 — DNS 정책에서 보안 인텔리전스의 일부로 차단 및 차단 안 함 목록을 사용합니다.
- URL — 액세스 제어 정책에서 보안 인텔리전스의 일부로 차단 및 차단 안 함 목록을 사용합니다. 보안 인텔리전스 이후에 분석 및 트래픽 처리 단계가 발생하는 액세스 제어 규칙에서도 URL 목록을 사용할 수 있습니다.

보안 인텔리전스 개체 수정 방법

차단 목록, 차단 금지 목록, 피드 또는 싱크홀 개체에서 항목을 추가하거나 삭제하려면 다음을 수행합니다.

개체 유형	기능 편집	편집 후 재구축이 필요합니까?
기본(단 사용자가 생성한) 차단 및 차단 금지 목록: 전역, 하위, 도메인별	컨텍스트 메뉴를 사용해 항목을 추가합니다. 개체 관리자를 사용해 항목을 삭제합니다.	항목을 추가한 후 No(아니오)를 선택합니다. 항목을 삭제한 후 Yes(예)를 선택합니다.
맞춤형 차단 및 차단 금지 목록	개체 관리자를 사용해 새 항목 또는 교체 항목을 업로드합니다.	Yes(예)
시스템에서 제공한 인텔리전스 피드	개체 관리자를 사용해 빈도 업데이트를 변경 또는 비활성화합니다.	No(아니요)
맞춤 피드	개체 관리자를 사용해 완전히 수정합니다.	No(아니요)
싱크홀	개체 관리자를 사용해 완전히 수정합니다.	예

글로벌 및 도메인 보안 인텔리전스 목록

Firepower Management Center는 네트워크의 이벤트에서 언제든지 URL, 도메인 및 IP 주소를 즉시 추가할 수 있는 빈 전역 차단 및 차단 안 함 목록과 함께 제공됩니다. 이러한 목록을 사용하면 보안 인텔

리전스를 통해 특정 연결을 항상 차단하거나 보안 인텔리전스로 인해 특정 연결이 차단되지 않도록 하여 설정한 다른 위협 탐지 프로세스에서 해당 연결을 평가할 수 있습니다.

익스플로잇 시도와 결합된 침입 이벤트에서 라우팅 가능한 IP 주소 집합이 발견되면 해당 IP 주소를 즉시 차단할 수 있습니다. 변경 사항을 전파하기까지 몇 분 정도 걸릴 수 있으나, 재구축하지 않아도 됩니다.

기본적으로, 액세스 제어 및 DNS 정책은 모든 보안 영역에 적용되는 이러한 전역 목록을 사용합니다. 정책별 기준으로 이러한 목록을 사용하지 않도록 선택할 수 있습니다.

참고 이러한 옵션은 보안 인텔리전스에만 적용됩니다. 보안 인텔리전스는 이미 단축 경로가 지정된 트래픽을 차단할 수 없습니다. 마찬가지로, 보안 인텔리전스의 차단 안 함 목록에 항목을 추가해도 일치하는 트래픽을 자동으로 신뢰하거나 단축 경로 지정을 수행하지 않습니다. 자세한 내용은 보안 인텔리전스 정보, 1695 페이지를 참고하십시오.

다중 도메인 구축의 경우, 도메인 목록은 물론 전역 목록에 항목을 추가하여 차단 또는 보안 인텔리전스 차단에서 제외를 시행하려는 Firepower System 도메인을 선택할 수 있습니다(보안 인텔리전스 목록 및 멀티테넌시, 599 페이지 참조).

보안 인텔리전스 목록 및 멀티테넌시

다중 도메인 구축에서 전역 도메인은 전역 차단 목록 및 차단 안 함 목록을 소유합니다. 전역 관리자만 전역 목록에 항목을 추가하거나 전역 목록에서 항목을 제거할 수 있습니다. 따라서 서브도메인 사용자는 네트워크, 도메인 이름, URL을 차단 및 차단 안 함 목록에 추가할 수 있도록 멀티테넌시는 다음을 추가합니다.

- 도메인 목록 — 특정 서브도메인에만 적용되는 콘텐츠가 있는 차단 또는 차단 안 함 목록입니다. 전역 목록은 전역 도메인에 대한 도메인 목록입니다.
- 하위 도메인 목록 — 현재 도메인이 보유한 하위 항목의 도메인 목록을 집계하는 차단 또는 차단 안 함 목록입니다.

도메인 목록

전역 목록에 액세스할 수 있는 기능(단, 수정 안 됨) 외에도, 각 서브도메인에는 해당 서브도메인에만 적용되는 콘텐츠인 자체 명명된 목록이 있습니다. 예를 들어 Company A로 명명된 서브도메인은 다음을 소유합니다.

- 도메인 차단 목록 - Company A 및 도메인 차단 안 함 목록 - Company A
- DNS에 대한 도메인 차단 목록 - Company A, DNS에 대한 도메인 차단 안 함 목록 - Company A
- URL에 대한 도메인 차단 목록 - Company A, URL에 대한 도메인 차단 안 함 목록 - Company A

현재 도메인 수준 또는 그 이상에 있는 모든 관리자는 이 목록을 입력할 수 있습니다. 콘텍스트 메뉴를 사용하여 현재 및 모든 하위 도메인의 항목을 차단 또는 차단 안 함 목록에 추가할 수 있습니다. 그러나 연결된 도메인의 관리자만 도메인 목록에서 항목을 제거할 수 있습니다.

예를 들어 전역 관리자는 전역 도메인 및 Company A의 도메인에 있는 동일한 IP 주소를 차단 목록에 추가하도록 선택할 수 있으나, Company B의 도메인에 있는 IP 주소는 차단 목록에 추가할 수 없습니다. 이 작업을 수행하면 동일한 IP 주소가 다음 목록에 추가됩니다.

- 전역 차단 목록(전역 관리자만 제거할 수 있는 목록임)
- 도메인 차단 목록 - Company A(Company A 관리자만 제거할 수 있는 목록임)

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

하위 도메인 목록

하위 도메인 목록은 현재 도메인이 보유한 하위 항목의 도메인 목록을 집계하는 차단 안 함 또는 차단 목록입니다. 리프 도메인은 하위 도메인 목록을 보유하지 않습니다.

하위 도메인 목록은 더 높은 수준의 도메인 관리자가 일반적인 보안 인텔리전스 설정을 시행할 수 있는 동시에, 서브도메인 사용자가 자체 구축 시 차단 또는 차단 안 함 목록에 항목을 추가할 수 있으므로 유용합니다.

예를 들어 전역 도메인은 다음과 같은 하위 도메인 목록을 보유합니다.

- 하위 차단 목록 - 전역, 하위 차단 안 함 목록 - 전역
- DNS에 대한 하위 차단 목록 - 전역, DNS에 대한 하위 차단 목록 - 전역
- URL에 대한 하위 차단 목록 - 전역, URL에 대한 하위 차단 목록 - 전역

참고 하위 도메인 목록은 수동으로 입력된 목록이 아니라 심볼릭 집계이므로 개체 관리자에 표시되지 않습니다. 하위 도메인 목록은 이를 사용할 수 있는 곳인 액세스 제어 및 DNS 정책에 표시됩니다.

전역 보안 인텔리전스 목록에 항목 추가

이벤트 및 대시 보드를 검토할 때 미리 정의된 차단 목록에 추가하여 해당 이벤트에 나타나는 IP 주소, 도메인 및 URL과 관련된 향후 트래픽을 즉시 차단할 수 있습니다.

마찬가지로 보안 인텔리전스 차단 이후에 위협 탐지 프로세스에서 평가하려는 트래픽을 차단하는 경우 사전 정의된 Do Not Block(차단 금지) 목록에 이벤트의 IP 주소, 도메인 및 URL을 추가할 수 있습니다.

트래픽은 위협 탐지의 보안 인텔리전스 단계에서 이러한 목록의 항목과 비교하여 평가됩니다.

이 목록에 대한 자세한 내용은 글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지의 내용을 참조하십시오.

시작하기 전에

보안 인텔리전스 목록에 항목을 추가하면 액세스 제어에 영향을 미치므로, 다음 사용자 역할 중 한 가지를 보유하고 있어야 합니다.

- 관리자
- 역할의 조합: Network Admin(네트워크 관리자) 또는 Access Admin(액세스 관리자), Security Analyst(보안 분석가) 및 Security Approver(보안 승인자)
- Modify Access Control Policy(액세스 제어 정책 수정) 및 Deploy Configuration to Devices(디바이스에 컨피그레이션 구축) 권한이 모두 있는 맞춤형 역할

해당하는 경우, 이러한 목록이 사용될 것으로 예상되는 정책에 사용되는지 확인합니다.

프로시저

단계 **1** 보안 인텔리전스를 사용하여 항상 차단하거나 보안 인텔리전스 차단에서 제외할 IP 주소, 도메인 또는 URL을 포함하는 이벤트로 이동합니다.

단계 **2** IP 주소, 도메인 또는 URL을 마우스 오른쪽 버튼으로 클릭하고 적절한 옵션을 선택합니다.

대상 항목	상황 메뉴 옵션	영향을 받는 전역 목록
IP 주소	Blacklist Now(지금 블랙리스트에 추가) Whitelist Now(지금 화이트리스트에 추가)	글로벌 차단 목록 전역 화이트리스트
URL	Blacklist HTTP/S Connections to URL Now(지금 URL에 대한 HTTP/S 연결을 블랙리스트에 추가) Whitelist HTTP/S Connections to URL Now(지금 URL에 대한 HTTP/S 연결을 화이트리스트에 추가)	URL에 대한 전역 차단 목록 URL에 대한 전역 화이트리스트
전체 도메인	Blacklist HTTP/S Connections to Domain Now(지금 도메인에 대한 HTTP/S 연결을 블랙리스트에 추가) Whitelist HTTP/S Connections to Domain Now(지금 도메인에 대한 HTTP/S 연결을 화이트리스트에 추가)	URL에 대한 전역 차단 목록 URL에 대한 전역 화이트리스트
전체 도메인에 대한 DNS 요청	Blacklist DNS Requests to Domain Now(지금 도메인에 대한 DNS 요청을 블랙리스트에 추가) Whitelist DNS Requests to Domain Now(지금 도메인에 대한 DNS 요청을 화이트리스트에 추가)	DNS에 대한 전역 차단 목록 DNS에 대한 전역 화이트리스트

다음에 수행할 작업

이러한 변경 사항을 적용하기 위해 재구축할 필요는 없습니다.

목록에서 항목을 삭제하려면 전역 보안 인텔리전스 목록에서 항목 삭제, 602 페이지의 내용을 참조하십시오.

전역 보안 인텔리전스 목록에서 항목 삭제

참고

- 다중 도메인 구축에서 이러한 목록의 이름은 "Global"이 아닐 수 있습니다. 자세한 내용은 보안 인텔리전스 목록 및 멀티테넌시, 599 페이지를 참고하십시오.
- 이러한 목록에 항목을 추가하려면 전역 보안 인텔리전스 목록에 항목 추가, 600 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

단계 **3** 적절한 옵션을 클릭합니다.

- **Network Lists and Feeds(**네트워크 목록 및 피드**)**(IP 주소용)
- **DNS** 목록 및 피드(도메인 이름용)
- **URL Lists and Feeds(URL** 목록 및 피드**)**

단계 **4** Global Block(전역 차단) 또는 Global Do-Not-Block(전역 차단 안 함) 목록 옆의 연필을 클릭합니다.

단계 **5** 삭제할 항목 옆의 휴지통 버튼을 클릭합니다.

보안 인텔리전스 목록 및 피드 업데이트

목록 및 피드 업데이트는 기존 목록을 대체하거나 파일에 새 파일의 내용을 피드합니다. 기존 및 새로운 파일의 내용은 병합되지 않습니다.

시스템이 손상된 피드 또는 인식할 수 있는 항목이 없는 피드를 다운로드하는 경우, (처음 다운로드가 아니라면) 시스템은 오래된 피드 데이터를 사용하여 계속 진행합니다. 그러나 시스템이 피드에서 항목을 하나라도 인식할 수 있는 경우, 인식할 수 있는 항목을 사용합니다.

기본적으로 피드는 매 2시간마다 Management Center를 업데이트합니다. 빈도는 수정할 수 있습니다. Management Center가 수신하는 모든 업데이트는 즉시 매니지드 디바이스로 전달됩니다. 또한 매니지드 디바이스는 30분마다 FMC를 폴링하여 변경 사항을 확인합니다. 이 빈도는 수정할 수 없습니다.

다중 도메인 구축에서 시스템이 제공한 피드 전역 도메인에 속하고 해당 도메인의 관리자만 수정할 수 있습니다. 사용자의 도메인에 속한 사용자 정의 피드의 업데이트 빈도는 수정할 수 있습니다.

피드 업데이트 간격을 수정하려면 보안 인텔리전스 피드에 대한 업데이트 빈도 변경, 603 페이지의 내용을 참조하십시오.

보안 인텔리전스 피드에 대한 업데이트 빈도 변경

Firepower Management Center가 보안 인텔리전스 피드를 업데이트하는 간격을 지정할 수 있습니다.

피드 업데이트에 대한 자세한 내용은 보안 인텔리전스 목록 및 피드 업데이트, 602 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 빈도를 변경하고 싶은 피드 유형을 선택합니다.

시스템에서 제공하는 URL 피드는 **DNS Lists and Feeds(DNS** 목록 및 피드**)** 아래의 도메인 피드와 결합됩니다.

단계 **3** 업데이트하고자 하는 피드 옆에 있는 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** **Update Frequency(**업데이트 빈도**)**를 수정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

사용자 지정 보안 인텔리전스 목록 및 피드

사용자 지정 목록 및 피드: 요구 사항

목록 및 피드 포맷

각 목록 또는 피드는 500MB 이하의 간단한 텍스트 파일이어야 합니다. 목록 파일은 .txt 확장자를 사용해야 합니다. 한 줄당 하나의 항목 또는 코멘트를 포함합니다(IP 주소 1개, URL 1개, 도메인 이름 1개).

팁 포함할 수 있는 항목 수는 파일의 최대 크기에 따라 제한됩니다. 예를 들어 코멘트가 없고 평균 URL 길이가 100자(Punycode 또는 퍼센트 Unicode 표시 및 줄바꿈 포함)인 URL 목록에는 524만 개 이상의 항목을 포함할 수 있습니다.

DNS 목록 항목에서 도메인 라벨에 별표(*) 와일드카드 문자를 지정할 수 있습니다. 모든 라벨이 와일드카드와 일치됩니다. 예를 들어 `www.example.*` 항목은 `www.example.com` 및 `www.example.co`와 모두 일치됩니다.

소스 파일 내에 코멘트 행을 추가할 경우, 해당 행은 파운드(#) 문자로 시작해야 합니다. 코멘트가 있는 소스 파일을 업로드할 경우, 업로드 과정에서 코멘트가 제거됩니다. 다운로드하는 소스 파일에는 코멘트 없이 모든 항목이 포함됩니다.

피드 **URL**

피드를 구성할 때 URL을 사용하여 해당 위치를 지정합니다. URL은 Punycode로 인코딩된 것이 아니어야 합니다.

URL 목록 및 피드: URL 구문 및 일치 기준

보안 인텔리전스 URL 목록 및 피드(맞춤형 목록, 피드 및 전역 차단 목록 및 차단 금지 목록의 항목 포함)에는 다음과 같은 내용이 포함될 수 있으며 설명된 바와 같이 일치 동작이 있습니다.

- 호스트 이름

  예를 들어, **www.example.com**이 있습니다.

- URL

  example.com은 **example.com**과 그의 모든 하위 도메인과(**www.example.com**, **eu.example.com**, **example.com/abc** 그리고 **www.example.com/def**을 포함) 일치하지만 **example.co.uk**, **examplexyz.com**, **example.com.malicious-site.com**과는 일치하지 않습니다.

  전체 URL 경로를 포함할 수도 있습니다. 예를 들면 **https://www.cisco.com/c/en/us/products/security/firewalls/index.html**.

- 정확한 일치를 나타내는 URL 끝에 있는 슬래시

  example.com/는 **example.com**과만 일치합니다. **www.example.com** 또는 다른 URL과는 일치하지 않습니다.

- URL의 도메인을 나타내는 와일드 카드(*)

  별표는 점으로 구분된 전체 도메인 문자열을 나타낼 수 있지만 부분 도메인 문자열은 사용할 수 없으며 첫 번째 슬래시 다음에 오는 URL의 어떤 부분도 될 수 없습니다.

  유효한 예:

  - ***.example.com**
  - **www.*.com**
  - 예. *****

    (이는 **example.com** 및 **example.org** 및 **example.de**와 일치하지만 **example.co.uk**와는 일치하지 않습니다.)

  - ***.example.***

- 예. ***/**

잘못된 예:

- **example*.com**
- **example.com/***

- IP 주소(IPv4)

  IPv6 주소의 경우 또는 범위 또는 CIDR 표기법을 사용하려면 보안 인텔리전스 네트워크 개체를 사용합니다.

  옥텟을 나타내는 하나 이상의 와일드 카드를 포함할 수 있습니다(예: 10.10.10. * 또는 10.10. *. *).

맞춤형 보안 인텔리전스 목록, 607 페이지도 참조하십시오.

맞춤형 보안 인텔리전스 피드

사용자 지정 또는 서드파티 보안 인텔리전스 피드를 사용하면 정기적으로 업데이트되며 평판이 좋은 인터넷의 다른 차단 안 함 목록 및 차단 목록으로 시스템이 제공한 인텔리전스 피드를 보강할 수 있습니다. 하나의 소스 목록을 사용하여 구축 시 여러 Firepower Management Center 어플라이언스를 업데이트할 때 유용한 내부 피드를 설정할 수도 있습니다.

참고 보안 인텔리전스 피드의 `/0` 넷마스크를 사용하여 주소 블록에 차단 또는 차단 안 함 목록을 추가할 수 없습니다. 정책이 대상으로 하는 모든 트래픽을 모니터링하거나 차단하려는 경우 **Monitor(**모니터링**)** 또는 **Block(**차단**)**인 액세스 제어 규칙을 사용하고 **Source Networks(**소스 네트워크**)** 및 **Destination Networks(**대상 네트워크**)**에는 기본값은 `any(모든)`을 사용합니다.

사용자 지정 목록 및 피드: 요구 사항, 603 페이지의 요구 사항을 참조하십시오.

시스템이 md5 체크섬을 사용하도록 구성하여 업데이트된 피드를 다운로드할지 결정할 수도 있습니다. 시스템이 피드를 마지막으로 다운로드한 이후로 체크섬이 변경되지 않는 경우 시스템이 이를 다시 다운로드할 필요는 없습니다. 특히 내부 피드가 클 경우 md5 체크섬을 사용할 수 있습니다. md5 체크섬은 오직 체크섬으로만 간편한 텍스트 파일로 저장해야 합니다. 코멘트가 지원되지 않습니다.

참고 시스템은 사용자 지정 피드를 다운로드할 때 피어 SSL 인증서 확인을 수행하지 않습니다. 또한 시스템은 원격 피어를 확인하는 인증서 번들 또는 자체 서명된 인증서를 사용하도록 지원하지 않습니다.

시스템이 인터넷에서 피드를 업데이트할 때 엄격한 제어를 원할 경우, 해당 피드에 대한 자동 업데이트를 비활성화할 수 있습니다. 그러나 자동 업데이트는 가장 연관성 있는 최신 데이터를 지원합니다.

수동으로 보안 인텔리전스 피드를 업데이트하면 인텔리전스 피드를 비롯한 모든 피드가 업데이트됩니다.

보안 인텔리전스 피드 생성

위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 추가하려는 피드 유형을 선택합니다.

단계 **3** 위에서 선택한 피드 유형에 적절한 옵션을 클릭합니다.

- **Add Network Lists and Feeds(**네트워크 목록 및 피드 추가**)**(IP 주소)
- **ADD DNS Lists and Feeds(DNS** 목록 및 피드 추가**)**
- **URL Lists and Feeds(URL** 목록 및 피드 추가**)**

단계 **4** 피드의 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 목록에서 **Feed(**피드**)**를 선택합니다.

단계 **6** 피드 **URL**을 입력합니다.

단계 **7** **MD5 URL**을 입력합니다.

이는 피드 콘텐츠가 마지막 업데이트 이후에 변경되었는지를 확인하는 데 사용되므로 시스템은 변경되지 않은 피드를 다운로드하지 않습니다.

30분 미만의 업데이트 간격에는 MD5 URL이 필요합니다.

피드 서버에서 MD5 URL을 제공하지 않는 경우 30분 이상의 간격을 선택해야 합니다.

단계 **8** **Update Frequency(**업데이트 빈도**)**를 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.
피드 업데이트를 비활성화하지 않는 한, 시스템은 피드를 다운로드하고 확인하려고 시도합니다.

보안 인텔리전스 피드 수동 업데이트

위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

시작하기 전에

하나 이상의 디바이스가 관리 센터에 추가되어 있어야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 피드 유형을 선택합니다.

단계 **3** 업데이트 피드를 클릭하고 확인합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

Firepower Management Center는 피드 업데이트를 다운로드 및 확인한 후 변경 사항을 관리되는 디바이스로 전달합니다. 업데이트된 피드를 사용하여 트래픽 필터링이 시작됩니다.

맞춤형 보안 인텔리전스 목록

보안 인텔리전스 목록은 사용자가 시스템에 수동으로 업로드하는 IP 주소와 주소 블록, URL, 도메인 이름에 대한 간단한 정적 목록입니다. Firepower Management Center의 단일 관리되는 디바이스에 대해 전역 목록 중 하나 또는 피드를 보강하고 세부적으로 조정하려는 경우에는 사용자 지정 목록이 유용합니다.

예를 들어, 평판이 좋은 피드가 중요한 리소스에 액세스하는 것을 잘못 차단하고 있지만 사용자 조직에 전반적으로 유용한 경우, IP 주소 피드 개체를 액세스 제어 정책의 차단 목록에서 제거하는 대신 잘못 분류된 IP 주소만 포함하는 사용자 지정 차단 안 함 목록을 생성할 수 있습니다.

참고 보안 인텔리전스 목록의 `/0` 넷마스크를 사용하여 주소 블록에 차단 또는 차단 안 함 목록을 추가할 수 없습니다. 정책이 대상으로 하는 모든 트래픽을 모니터링하거나 차단하려는 경우 **Monitor(**모니터링**)** 또는 **Block(**차단**)**인 액세스 제어 규칙을 사용하고 **Source Networks(**소스 네트워크**)** 및 **Destination Networks(**대상 네트워크**)**에는 기본값은 `any(모든)`을 사용합니다.

목록 항목 서식에 대해서는 다음을 참조하십시오.

- 주소 블록에 대한 넷마스크는 IPv4 및 IPv6의 경우 각각 `0~32` 또는 `0~128`의 정수일 수 있습니다.
- 도메인 이름의 유니코드는 Punycode 형식으로 인코딩되어야 하고 대소문자를 구분하지 않습니다.
- 도메인 이름은 대소문자를 구분하지 않습니다.
- URL의 유니코드는 % 인코딩 형식으로 인코딩되어야 합니다.
- URL의 하위 디렉터리는 대소문자를 구분하지 않습니다.
- 파운드 기호(`#`)로 시작하는 목록 항목은 설명으로 처리됩니다.
- 사용자 지정 목록 및 피드: 요구 사항, 603 페이지에서 추가 형식 요구 사항을 참조하십시오.

일치 목록 항목은 다음을 참조하십시오.

- 시스템은 URL 또는 DNS 목록에 더 높은 수준의 도메인이 존재하는 경우 하위 도메인을 일치시킵니다. 예를 들어 `example.com`을 DNS 목록에 추가하는 경우 시스템은 `www.example.com` 및 `test.example.com`을 일치시킵니다.
- 시스템은 DNS 또는 URL 목록 항목의 DNS 조회(전달 또는 역방향)은 수행하지 않습니다. 예를 들어 `http://192.168.0.2`를 URL 목록에 추가하고 `http://www.example.com`에서 해제하는 경우 시스템은 `http://192.168.0.2`만 일치시키고 `http://www.example.com`은 일치시키지 않습니다.

새 보안 인텔리전스 목록을 다음에 업로드 Firepower Management Center

보안 인텔리전스 목록을 수정하려면 소스 파일을 변경하고 새 복사본을 업로드해야 합니다. 웹 인터페이스를 사용해 파일 내용을 수정할 수 없습니다. 소스 파일에 액세스할 수 없는 경우 시스템에서 복사본을 다운로드할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 목록 유형을 선택합니다.

단계 **3** 위에서 선택한 목록에 적절한 옵션을 클릭합니다.

- **Add Network Lists and Feeds(**네트워크 목록 및 피드 추가**)**(IP 주소)
- **ADD DNS Lists and Feeds(DNS** 목록 및 피드 추가**)**
- **URL Lists and Feeds(URL** 목록 및 피드 추가**)**

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 목록에서 **List(**목록**)**를 선택합니다.

단계 **6** **Browse(**찾아보기**)**를 클릭하여 목록에서 `.txt` 파일을 탐색한 후 **Upload(**업로드**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

보안 인텔리전스 목록 업데이트

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 목록 유형을 선택합니다.

단계 **3** 업데이트하려는 목록 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 목록 복사본을 편집해야 하는 경우 **Download(**다운로드**)**를 클릭하고 항목을 텍스트 파일로 저장하려면 브라우저 프롬프트를 따릅니다.

단계 **5** 필요에 따라 목록을 변경합니다.

단계 **6** 보안 인텔리전스 팝업 창에서 수정된 목록을 검색하려면 **Browse(**찾아보기**)**를 클릭하고 **Upload(**업로드**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

싱크홀 개체

싱크홀 개체는 싱크홀 내의 모든 도메인 이름용으로 라우팅할 수 없는 주소를 제공하는 DNS 서버나 서버로 확인되지 않는 IP 주소를 나타냅니다. DNS 정책 규칙 내의 싱크홀 개체를 참조하여 일치하는 트래픽을 싱크홀로 리디렉션할 수 있습니다. 개체에는 IPv4 주소와 IPv6 주소를 모두 할당해야 합니다.

싱크홀 개체 생성

위협 라이선스(FTD 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Sinkhole(**싱크홀**)**을 선택합니다.

단계 **3** **Add Sinkhole(**싱크홀 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 싱크홀의 **IPv4** 주소 및 **IPv6** 주소를 입력합니다.

단계 **6** 다음 옵션을 이용할 수 있습니다.

- 싱크홀 서버로 트래픽을 리디렉션하려면 **Log Connections to Sinkhole(**싱크홀에 대한 연결 로깅**)**을 선택합니다.
- 확인되지 않은 IP 주소로 트래픽을 리디렉션하려면 **Block and Log Connections to Sinkhole(**싱크홀에 대한 연결 차단 및 로깅**)**을 선택합니다.

단계 **7** 싱크홀에 IoC(보안 침해 지표) 유형을 할당하려면 **Type(**유형**)** 드롭다운에서 유형 하나를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

파일 목록

AMP for Networks 를 사용하고 AMP 클라우드가 파일의 속성을 잘못 식별하는 경우 향후 파일을 더 잘 탐지하기 위해 파일 목록에 파일을 추가할 수 있습니다. 이러한 파일은 SHA-256 해시 값을 사용해 지정됩니다. 각 파일 목록은 최대 10000개의 고유한 SHA-256 값을 포함할 수 있습니다.

파일 목록에는 두 개의 사전 정의된 카테고리가 있습니다.

안전 목록

이 목록에 파일을 추가하는 경우 시스템은 AMP 클라우드가 파일을 안전 속성으로 할당했다고 간주합니다.

사용자 지정 탐지 목록

이 목록에 파일을 추가하는 경우 시스템은 AMP 클라우드가 악성코드 속성으로 할당했다고 간주합니다.

다중 도메인 구축 시 안전 목록 및 사용자 지정 탐지 목록은 각 도메인마다 표시됩니다. 하위 도메인에서는 볼 수 있지만 상위 도메인의 항목은 수정할 수 없습니다.

이 목록에 포함된 파일에 대한 차단을 수동으로 지정하므로 시스템은 이런 파일의 속성에 대해 AMP 클라우드에 쿼리하지 않습니다. 파일 정책을 구성할 때는 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 작업 중 하나 및 파일의 SHA 값을 계산하는 일치 파일 유형을 포함한 규칙을 구성해야 합니다.

⚠

주의 안전 목록에 악성코드를 포함하지 마십시오. 안전 목록은 AMP 클라우드 및 사용자 지정 탐지 목록에 오버라이드됩니다.

파일 목록에 대한 소스 파일

SHA-256 값 및 설명이 포함된 쉼표로 구분된 값(CSV) 소스 파일을 업로드하여 파일 목록에 복수의 SHA-256 값을 추가할 수 있습니다. Firepower Management Center은 콘텐츠를 확인하고 파일 목록에 유효한 SHA-256 값을 입력합니다.

소스 파일은 .csv 파일 이름 확장자를 가진 간편한 텍스트 파일이어야 합니다. 모든 헤더는 파운드 기호(#)로 시작해야 합니다. 이는 코멘트로 처리되어 업로드되지 않습니다. 각 항목은 `LF` 또는 `CR+LF` 줄 바꿈 문자로 끝나며 설명이 있는 단일 SHA-256 값을 포함해야 합니다. 시스템은 항목의 추가 정보는 모두 무시합니다.

다음 사항을 참고하십시오.

- 파일 목록에서 소스 파일을 삭제하면 이는 또한 파일 목록에서 모든 관련 SHA-256 해시를 제거합니다.

- 성공적인 소스 파일 업로드의 결과 파일 목록이 10000개 이상의 명시적 SHA-256 값을 포함하는 경우 파일 목록에 여러 파일을 업로드할 수 없습니다.
- 시스템은 업로드 시 256개의 문자를 초과하는 설명이 있으면 이를 줄여서 처음 256개 문자만 남깁니다. 설명에 쉼표가 포함되어 있는 경우, 이스케이프 문자(\,)를 사용해야 합니다. 어떤 설명도 포함되지 않은 경우, 소스 파일 이름을 대신 사용합니다.
- 모든 비복제 SHA-256 값이 파일 목록에 추가됩니다. 파일 목록이 SHA-256 값을 포함하고 해당 값이 포함된 소스 파일을 업로드할 경우, 새로 업로드한 값은 기존 SHA-256 값을 변경하지 않습니다. 캡처 파일, 파일 이벤트 또는 SHA-256 값과 관련된 악성코드 이벤트를 볼 때, 모든 위협 이름 또는 설명은 개별 SHA-256 값에서 파생됩니다.
- 시스템은 소스 파일에 유효하지 않은 SHA-256 값을 업로드하지 않습니다.
- 업로드된 여러 소스 파일이 동일한 SHA-256 값에 대한 항목을 포함할 경우 시스템은 가장 최근 값을 사용합니다.
- 소스 파일이 동일한 SHA-256 값에 대한 여러 항목을 포함할 경우, 시스템은 가장 최근 값을 사용합니다.
- 개체 관리자 내 소스 파일을 직접 수정할 수 없습니다. 변경하려면, 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제한 후, 수정된 소스 파일을 업로드해야 합니다.
- 소스 파일과 관련된 항목 수는 명시적 SHA-256 값의 수를 나타납니다. 파일 목록에서 소스 파일을 삭제하는 경우, 파일 목록이 포함하는 SHA-256 항목의 총 수는 소스 파일 내 유효한 항목 수에 따라 감소합니다.

파일 목록에 개별 **SHA-256** 값 추가

이 절차를 수행하려면 악성 코드 라이선스가 있어야 합니다.

파일의 SHA-256 값을 제출하여 파일 목록에 추가할 수 있습니다. 중복된 SHA-256 값은 추가할 수 없습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

시작하기 전에

- 이벤트 보기에서 파일 또는 악성코드 이벤트를 오른쪽 클릭하고 컨텍스트 메뉴에서 **Show Full Text(**전체 텍스트 보기**)**를 선택하여 파일 항목에 붙여넣기 할 전체 SHA-256 값을 복사합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **File List(**파일 목록**)**을 선택합니다.

단계 **3** 파일을 추가하려는 정상 목록 또는 사용자 정의 탐지 목록 옆의 수정( )을 클릭하세요.

보기 ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 드롭다운 목록에서 **Add by(**추가 기준**)**의 `Enter SHA Value(SHA 값 입력)`를 선택합니다.

단계 **5** **Description(**설명**)** 필드에 소스 파일에 대한 설명을 입력합니다.

단계 **6** 파일의 전체 값을 **SHA-256** 필드에 입력하거나 붙여 넣습니다. 시스템은 일치하는 부분 값을 지원하지 않습니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

참고 설정 변경을 구축한 뒤 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에 개별 파일 업로드

이 절차를 수행하려면 악성 코드 라이선스가 있어야 합니다.

파일 목록에 추가하려는 파일의 사본이 있는 경우 분석을 위해 Firepower Management Center에 파일을 업로드할 수 있습니다. 시스템은 파일의 SHA-256 값을 계산하고 목록에 파일을 추가합니다. 시스템은 SHA-256 계산을 위한 파일 크기에 제한을 두지 않습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **File List(**파일 목록**)**을 선택합니다.

단계 **3** 파일을 추가하려는 정상 목록 또는 사용자 정의 탐지 목록 옆의 수정( )을 클릭하세요.

보기 ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 드롭다운 목록의 **Add(**추가**)**에서 **Calculate SHA(SHA** 계산**)**을 선택합니다.

단계 **5** 또는, **Description(**설명**)** 필드에 파일에 대한 설명을 입력합니다. 설명을 입력하지 않은 경우, 업로드 시 설명에 파일 이름이 사용됩니다.

단계 **6** **Browse(**탐색**)**를 클릭하여 업로드할 파일을 선택합니다.

단계 **7** **Calculate and Add SHA(SHA** 계산 및 주가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

참고 설정 변경을 구축한 뒤 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에 소스 파일 업로드

이 절차를 수행하려면 악성 코드 라이선스가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **File List(**파일 목록**)**를 클릭합니다.

단계 **3** 소스 파일의 값을 추가할 파일 목록 옆에 있는 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 드롭다운 목록의 **Add(**추가**)**에서 `List of SHAs(SHA 목록)`을 선택합니다.

단계 **5** 또는, **Description(**설명**)** 필드에 소스 파일에 대한 설명을 입력합니다. 설명을 입력하지 않을 경우, 시스템은 파일 이름을 사용합니다.

단계 **6** **Browse(**찾아보기**)**를 클릭하여 소스 파일을 탐색한 후 **Upload and Add List(**목록 업로드 및 주가**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

참고 정책을 구축한 후 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에서 SHA-256 값 수정

이 절차를 수행하려면 악성 코드 라이선스가 있어야 합니다.

파일 목록에서 개별 SHA-256 값을 편집하거나 삭제할 수 있습니다. 개체 관리자 내 소스 파일을 직접 수정할 수 없다는 점에 유의하십시오. 변경하려면, 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제한 후, 수정된 소스 파일을 업로드해야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **File List(**파일 목록**)**를 클릭합니다.

단계 **3** 수정하려는 파일이 포함된 정상 목록 또는 사용자 정의 탐지 목록 옆의 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 다음 작업을 수행할 수 있습니다.

- 변경하려는 SHA-256 값 옆의 수정( )을 클릭하고 원하는 **SHA-256** 또는 설명 값을 수정합니다.
- 삭제할 SHA-256 값 옆의 삭제( )을 클릭합니다.

단계 **5** 목록에서 파일 항목을 업데이트하려면 **Save(**저장**)**을 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭하여 파일 목록을 저장합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

참고 설정 변경을 구축한 뒤 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에서 소스 파일 다운로드

이 절차를 수행하려면 악성 코드 라이선스가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **File List(**파일 목록**)**을 선택합니다.

단계 **3** 소스 파일을 다운로드하려는 정상 목록 또는 사용자 정의 탐지 목록 옆의 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 다운로드할 소스 파일 옆에 있는 보기 ( )을 클릭합니다.

단계 **5** **Download SHA List(SHA** 목록 다운로드**)**를 클릭하고 프롬프트에 따라 소스 파일을 저장합니다.

단계 **6** **Close(**닫기**)**를 클릭합니다.

암호 그룹 목록

암호 그룹 목록은 여러 암호 그룹으로 구성된 개체입니다. 사전 정의된 각 암호 그룹 값은 SSL 또는 TLS 암호화 세션을 협상하는 데 사용되는 암호 그룹을 나타냅니다. 클라이언트와 서버가 해당 암호 그룹을 사용하여 SSL 세션을 협상했는지 여부를 기반으로 암호화된 트래픽을 제어하기 위해 SSL 규칙의 암호 그룹 및 암호 그룹 목록을 사용할 수 있습니다. SSL 규칙에 암호 그룹 목록을 추가하면 목록의 암호 그룹 중 하나와 협상한 SSL 세션이 규칙을 매칭합니다.

참고 암호 그룹 목록과 동일한 위치에 있는 웹 인터페이스의 암호 그룹을 사용할 수 있지만 암호 그룹을 추가, 수정, 삭제할 수는 없습니다.

암호 그룹 목록 생성

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Cipher Suite List(**암호 모음 목록**)**을 선택합니다.

단계 **3** **Add Cipher Suites**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Available Ciphers(**사용 가능한 암호**)** 목록에서 하나 이상의 암호 그룹을 선택합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** 선택적으로 **Selected Ciphers(**선택한 암호**)** 목록 내 삭제하려는 암호 그룹 옆의 삭제( )을 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

고유 이름 개체

각 고유 이름(DN) 개체는 공개 키 인증서의 주체 또는 발행자에 대해 나열된 고유 이름(DN)을 나타냅니다. 클라이언트 및 서버가 주체 또는 발행자로서 고유 이름과 함께 서버 인증서를 사용하여 SSL 세션을 협상했는지 여부를 기반으로 암호화된 트래픽을 제어하기 위해 SSL 규칙 내 고유 이름 개체 및 그룹을 사용할 수 있습니다.

고유 이름(DN) 개체는 공용 이름 특성(**CN**)을 포함할 수 있습니다. "CN=" 없이 공용 이름(CN)을 추가하면 개체를 저장하기 전에 시스템이 "CN="을 앞에 추가합니다.

다음 표에 나열된 각 특성 중 하나와 함께 쉼표로 구분하여 고유 이름(DN)을 추가할 수 있습니다.

표 ***63:*** 고유 이름***(DN)*** 특성

속성	설명	허용 값
전체	국가 코드	영문자 2개
CN	공용 이름(CN)	최대 64자의 영숫자, 백슬래시(/), 하이픈(-), 따옴표('), 별표(*) 문자 또는 공백

속성	설명	허용 값
O	조직	최대 64자의 영숫자, 백슬래시(/), 하이픈(-), 따옴표('), 별표(*) 문자 또는 공백
OU	조직 단위	최대 64자의 영숫자, 백슬래시(/), 하이픈(-), 따옴표('), 별표(*) 문자 또는 공백

특성에서 하나 이상의 별표(*)를 와일드카드로 정의할 수 있습니다. 공용 이름 특성(CN)에서 도메인 이름 레이블당 하나 이상의 별표를 정의할 수 있습니다. 와일드카드로 여러 레이블을 정의할 수도 있지만 와일드카드는 해당 레이블 내에서만 매칭합니다. 다음 표의 예를 참고하십시오.

표 ***64:*** 공용 이름 특성***(CN)*** 와일드카드 예

특성	일치	일치하지 않음
CN="*ample.com"	example.com	mail.example.com example.text.com ampleexam.com
CN="exam*.com"	example.com	mail.example.com example.text.com ampleexam.com
CN="*xamp*.com"	example.com	mail.example.com example.text.com ampleexam.com
CN="*.example.com"	mail.example.com	example.com example.text.com ampleexam.com
CN="*.com"	example.com ampleexam.com	mail.example.com example.text.com
CN="*.*.com"	mail.example.com example.text.com	example.com ampleexam.com

고유 이름(DN) 개체 생성

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **Distinguished Name(**고유 이름**)** 노드를 확장하고 **Individual Objects(**개별 개체**)**를 선택합니다.

단계 **3** **Add Distinguished Name(**고유 이름**(DN)** 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **DN** 필드에 고유 이름 또는 공통 이름의 값을 입력합니다. 다음 옵션을 이용할 수 있습니다.

- 고유 이름(DN)을 추가하면 고유 이름 개체, 616 페이지에 나열된 각 특성 중 하나를 쉼표로 구분하여 포함할 수 있습니다.
- 공용 이름(CN)을 추가하는 경우 여러 레이블과 와일드카드를 포함할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

PKI 개체

SSL 애플리케이션에 대한 **PKI** 개체

PKI 개체는 구축을 지원하는 데 필요한 공개 키 인증서 및 페어링된 개인 키를 나타냅니다. 내부 및 신뢰받는 CA 개체는 CA(인증 기관) 인증서로 구성되며, 내부 CA 개체는 인증서와 페어링된 개인 키도 포함합니다. 내부 및 외부 인증서 개체는 서버 인증서로 구성되며, 내부 인증서 개체는 인증서와 페어링된 개인 키도 포함합니다.

신뢰할 수 있는 인증 기관 개체 및 내부 인증 개체를 사용해 ISE/ISE-PIC에 대한 연결을 설정하는 경우 ISE/ISE-PIC를 ID 소스로 사용할 수 있습니다.

내부 인증 개체를 사용해 캡티브 포털을 설정하는 경우 시스템은 사용자의 웹 드라우저에 연결할 때 캡티브 포털 디바이스의 ID를 인증할 수 있습니다.

신뢰할 수 있는 인증 기관 개체를 사용해 영역을 구성하는 경우 LDAP 또는 AD 서버에 보안 연결을 구성할 수 있습니다.

SSL 규칙에서 PKI 개체를 사용하는 경우 다음을 사용해 암호화된 트래픽을 일치시킬 수 있습니다.

- 외부 인증서 개체의 인증서
- 신뢰받는 CA 개체에서 또는 CA의 신뢰 체인 내에서 CA에 의해 서명된 인증서

SSL 규칙에서 PKI 개체를 사용하는 경우 다음을 사용해 암호 해독을 할 수 있습니다.

- 발신 트래픽 - 내부 CA 개체로 서버 인증서를 다시 서명
- 수신 트래픽 - 내부 인증서 개체에서 알려진 개인 키를 사용하여

인증서와 키 정보를 수동으로 입력하거나, 해당 정보를 포함하는 파일을 업로드하거나, 경우에 따라 새 CA 인증서와 개인 키를 생성할 수 있습니다.

개체 관리자에서 PKI 개체의 목록을 볼 때 인증서의 주체 DN이 개체 값으로서 표시됩니다. 전체 인증서 주체 DN을 보려면 값 위로 포인터를 이동하십시오. 다른 인증서 세부사항을 보려면 PKI 개체를 수정하십시오.

참고 Firepower Management Center 및 관리되는 디바이스는 저장하기 전에 무작위로 생성된 키를 이용하여 내부 CA 개체 및 내부 인증서 개체에 저장된 모든 개인 키를 암호화합니다. 비밀번호로 보호된 개인 키를 업로드하면 어플라이언스는 사용자 제공 비밀번호를 사용해 키를 암호 해독한 다음 저장 전에 무작위로 생성된 키를 사용하여 다시 암호화합니다.

내부 인증 기관 개체

사용자가 구성하는 각 내부 CA(인증 기관) 개체는 조직에서 제어하는 CA의 CA 공개 키 인증서를 나타냅니다. 개체는 개체 이름, CA 인증서 및 페어링된 개인 키로 구성됩니다. SSL 규칙의 내부 CA 개체 및 그룹을 사용해 내부 CA로 서버 인증서를 다시 서명하면 암호화된 발신 트래픽을 암호 해독할 수 있습니다.

참고 **Decrypt - Resign(**암호 해독 - 다시 서명**)** SSL 규칙에서 내부 CA 개체를 참조하고 규칙이 암호화된 세션과 일치하는 경우, 사용자의 브라우저에 SSL 핸드셰이크를 협상하는 동안 인증서가 신뢰되지 않는다는 경고 메시지가 표시될 수 있습니다. 이 문제를 피하려면 내부 CA 개체 인증서를 신뢰받는 루트 인증서의 클라이언트 또는 도메인 목록에 추가하십시오.

다음과 같은 방법으로 내부 CA 개체를 생성할 수 있습니다.

- 기존의 RSA 기반 또는 EC(Elliptic Curve) 기반 CA 인증서와 개인 키 가져오기
- 새로운 자체 서명 RSA 기반 CA 인증서 및 개인 키 생성
- 서명되지 않은 RSA 기반 CA 인증서 및 개인 키 생성 내부 CA 개체를 사용하려면 우선 인증서 서명을 위해 CSR(certificate signing request)을 다른 CA에 제출해야 합니다.

서명된 인증서를 포함하는 내부 CA 개체를 생성한 후에 CA 인증서 및 개인 키를 다운로드할 수 있습니다. 시스템은 다운로드된 인증서 및 개인 키를 사용자 제공 비밀번호로 암호화합니다.

시스템 또는 사용자 생성 여부와 관계없이 내부 CA 개체 이름은 수정할 수 있지만 다른 개체 속성은 수정할 수 없습니다.

사용 중인 내부 CA 개체는 삭제할 수 없습니다. 또한 SSL 정책에서 사용되는 내부 CA 개체를 편집하면 관련 액세스 제어 정책이 오래된 상태가 됩니다. 변경 사항을 적용하려면 액세스 제어 정책을 재구축해야 합니다.

CA 인증서 및 개인 키 가져오기

X.509 v3 CA 인증서 및 개인 키를 가져와서 내부 CA 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

개인 키 파일이 비밀번호로 보호되는 경우 암호 해독 비밀번호를 제공할 수 있습니다. 인증서와 키가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

적절한 인증서 또는 키 정보를 포함하며 상호 페어링된 파일만 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 페어링을 검증합니다.

참고 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 인증 알고리즘 유형을 기반으로 트래픽을 매칭합니다. 예를 들어 EC(Elliptic Curve) 기반 알고리즘으로 암호화된 발신 트래픽을 암호 해독 하려면 EC 기반 CA 인증서를 업로드해야 합니다.

CA 인증서 및 개인 키 가져오기

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 **3** **Import CA**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Certificate Data** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드합니다.

단계 **6** **Key** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 페어링된 개인 키 파일을 업로드합니다.

단계 **7** 업로드 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크박스를 선택하고 비밀번호를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

새 **CA** 인증서 및 개인 키 생성

이러한 개체는 NGIPSv를 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

자체 서명 RSA 기반 CA 인증서 및 개인 키를 생성하기 위한 식별 정보를 제공하여 내부 CA 개체를 구성할 수 있습니다.

생성된 CA 인증서는 10년간 유효합니다. Valid From 날짜는 생성 이전의 주입니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 **3** **Generate CA(CA** 생성**)**를 클릭하고

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 식별 속성을 입력합니다.

단계 **6** **Generate self-signed CA(**자체 서명된 **CA** 생성**)**를 클릭합니다.

새로 서명된 인증서

CA에서 서명된 인증서를 가져와서 내부 CA 개체를 구성할 수 있습니다. 여기에는 두 단계가 관련됩니다.

- 내부 CA 개체를 구성하기 위한 식별 정보를 제공합니다. 그러면 서명되지 않은 인증서와 페어링된 개인 키, 그리고 사용자가 지정한 CA에 대한 CSR(certificate signing request)이 생성됩니다.

- CA가 서명된 인증서를 발행하면 이를 내부 CA 개체에 업로드하여 서명되지 않은 인증서를 교체합니다.

SSL 규칙에서 내부 CA 개체만 참조할 수 있습니다(해당 개체에 서명된 인증서가 포함된 경우).

서명되지 않은 CA 인증서 및 CSR 생성

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

프로시저

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 2 **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 3 **Generate CA(CA** 생성**)**를 클릭하고

단계 4 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 5 식별 속성을 입력합니다.

단계 6 **Generate CSR**을 클릭합니다.

단계 7 CA에 제출할 CSR을 복사합니다.

단계 8 **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 에 설명된 대로 CA에서 발급한 서명된 인증서를 업로드해야 합니다. CSR에 응답하여 발행된 서명된 인증서 업로드, 622 페이지

CSR에 응답하여 발행된 서명된 인증서 업로드

이러한 개체는 NGIPSv를 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

업로드가 끝나면 SSL 규칙에서 서명된 인증서를 참조할 수 있습니다.

프로시저

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 2 **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 **3** CSR을 기다리는 서명되지 않은 인증서가 포함된 CA 개체 옆에 있는 수정( )을 클릭합니다.

단계 **4** **Install Certificate(**인증서 설치**)**를 클릭합니다.

단계 **5** DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드하려면 **Browse(**찾아보기**)**를 클릭합니다.

단계 **6** 업로드된 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크 박스를 선택하고 비밀번호를 입력합니다.

단계 **7** CA 개체에 서명된 인증서를 업로드하려면 **Save(**저장**)**을 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

CA 인증서 및 개인 키 다운로드

내부 CA 개체의 인증서 및 키 정보를 포함하는 파일을 다운로드하여 CA 인증서 및 페어링된 개인 키를 백업하거나 전송할 수 있습니다.

주의 다운로드한 키 정보는 항상 안전한 장소에 저장하십시오.

시스템은 내부 CA 개체에 저장된 개인 키를 무작위로 생성된 키로 암호화한 후 디스크에 저장합니다. 내부 CA 개체에서 인증서와 개인 키를 다운로드하면 시스템은 인증서 및 개인 키 정보를 포함하는 파일을 생성하기 전에 먼저 해당 정보를 해독합니다. 그런 다음 시스템이 다운로드한 파일을 암호화하는 데 사용할 비밀번호를 제공해야 합니다.

주의 시스템 백업 과정에서 다운로드된 개인 키는 해독된 후 암호화되지 않은 백업 파일에 저장됩니다.

CA 인증서 및 개인 키 다운로드

이러한 개체는 NGIPSv를 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

현재 도메인 및 상위 도메인에 대한 CA 인증서를 다운로드할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 **3** 다운로드할 인증서 및 개인 키에 해당하는 내부 CA 개체 옆의 수정( )을 클릭합니다.

다중 도메인 구축의 경우, 보기 ( )을 클릭하면 상위 도메인의 개체에 대한 인증서 및 개인 키를 다운로드할 수 있습니다.

단계 **4** **Download(**다운로드**)**를 클릭합니다.

단계 **5** **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 암호화 비밀번호를 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

신뢰할 수 있는 인증 기관 개체

사용자가 구성하는 신뢰받는 인증 기관(CA) 개체는 신뢰받는 CA에 속한 CA 공개 키 인증서를 나타냅니다. 개체는 개체 이름 및 CA 공개 키 인증서로 구성됩니다. 다음의 경우에 외부 CA 개체 및 그룹을 사용할 수 있습니다.

- 트래픽을 제어하기 위한 SSL 정책이 신뢰받는 CA 또는 신뢰 체인의 CA가 서명한 인증서로 암호화된 경우
- LDAP 또는 AD 서버에 보안 연결을 설정하기 위한 영역 설정
- ISE/ISE-PIC 연결 **pxGrid** 서버 **CA** 및 **MNT** 서버 **CA** 필드에 대해 신뢰받는 인증 기관 개체를 선택합니다.

신뢰받는 CA 개체를 생성한 후에는 이름을 수정하고 CRL(certificate revocation lists)을 추가할 수 있지만 다른 개체 속성은 수정할 수 없습니다. 개체에 추가할 수 있는 CRL의 수에는 제한이 없습니다. 개체에 업로드한 CRL을 수정하려면 개체를 삭제하고 다시 생성해야 합니다.

참고 개체가 ISE/ISE-PIC 통합 설정에서 사용될 경우 개체에 CRL을 추가하는 것은 효과가 없습니다.

사용 중인 신뢰받는 CA 개체는 삭제할 수 없습니다. 또한 사용되는 신뢰받는 CA 개체를 편집하면 관련 액세스 제어 정책이 오래된 상태가 됩니다. 변경 사항을 적용하려면 액세스 제어 정책을 재구축해야 합니다.

신뢰할 수 있는 **CA** 개체

X.509 v3 CA 인증서를 업로드하여 외부 CA 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

파일이 비밀번호로 보호된 경우 암호 해독 비밀번호를 제공해야 합니다. 인증서가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

파일에 적절한 인증서 정보가 포함된 경우에만 CA 인증서를 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 인증서를 검증합니다.

신뢰할 수 있는 CA 개체 추가

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

프로시저

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 2 **PKI** 노드를 확장하고 신뢰받는 **CA**를 선택합니다.

단계 3 **Add Trusted CAs**를 클릭합니다.

단계 4 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 5 DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드하려면 **Browse(**찾아보기**)**를 클릭합니다.

단계 6 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크 박스를 선택하고 비밀번호를 입력합니다.

단계 7 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

신뢰할 수 있는 CA 개체의 인증서 해지 목록

CRL을 신뢰받는 CA 개체에 업로드할 수 있습니다. SSL 정책에서 해당 신뢰받는 CA 개체를 참조하는 경우, 세션 암호화 인증서를 발행한 CA가 그 이후 인증서를 폐기했는지 여부에 따라 암호화된 트래픽을 제어할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

CRL을 추가한 후에는 폐기된 인증서의 목록을 볼 수 있습니다. 개체에 업로드한 CRL을 수정하려면 개체를 삭제하고 다시 생성해야 합니다.

적절한 CRL을 포함하는 파일만 업로드할 수 있습니다. 신뢰받는 CA 개체에 추가할 수 있는 CRL의 수에는 제한이 없습니다. 그러나 CRL을 업로드할 때마다 또 다른 CRL을 추가하기 전에 개체를 저장해야 합니다.

참고 개체가 ISE/ISE-PIC 통합 설정에서 사용될 경우 개체에 CRL을 추가하는 것은 효과가 없습니다.

신뢰할 수 있는 CA 개체에 인증서 해지 목록 추가

이러한 개체는 NGIPSv를 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

참고 개체가 ISE/ISE-PIC 통합 설정에서 사용될 경우 개체에 CRL을 추가하는 것은 효과가 없습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 신뢰받는 **CA**를 선택합니다.

단계 **3** 신뢰받는 CA 개체 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** DER 또는 PEM으로 인코딩된 CRL 파일을 업로드하려면 **Add CRL(CRL** 추가**)**를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

외부 인증서 개체

사용자가 구성하는 각 외부 인증서 개체는 조직에 속하지 않은 서버 공개 키 인증서를 나타냅니다. 개체는 개체 이름 및 인증서로 구성됩니다. 서버 인증서로 암호화된 트래픽을 제어하려면 SSL 규칙에서 외부 인증서 개체 및 그룹을 사용할 수 있습니다. 예를 들어 사용자는 신뢰하는 자체 서명 서버 인증서를 업로드할 수는 있지만 신뢰할 수 있는 CA 인증서로 확인할 수는 없습니다.

X.509 v3 서버 인증서를 업로드하여 외부 인증서 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)

- PEM(Privacy-enhanced Electronic Mail)

적절한 서버 인증서 정보가 포함된 파일만 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 파일을 검증합니다. 인증서가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

외부 인증서 개체 추가

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 외부 인증서를 선택합니다.

단계 **3** **Add External Cert**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Certificate Data(**인증서 데이터**)** 필드 위에서 **Browse(**찾아보기**)**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 서버 인증서 파일을 업로드합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

내부 인증서 개체

사용자가 구성하는 각 내부 인증서 개체는 조직에 속한 서버 공개 키 인증서를 나타냅니다. 개체는 개체 이름, 공개 키 인증서 및 페어링된 개인 키로 구성됩니다. 다음의 경우 내부 인증서 개체 및 그룹을 사용할 수 있습니다.

- 알려진 개인 키를 사용하여 조직의 서버 중 하나로 들어오는 트래픽을 해독하려는 SSL 규칙
- ISE/ISE-PIC 연결 **MC** 서버 인증서 필드에 내부 인증서 개체를 선택합니다.
- 사용자의 웹 브라우저에 연결할 때 캡티브 포털 디바이스의 ID를 인증하는 캡티브 포털 설정 서버 인증서 필드에 내부 인증서 개체를 선택합니다.

X.509 v3 RSA 기반 또는 EC(Elliptic Curve) 기반 서버 인증서 및 페어링된 개인 키를 업로드하여 내부 인증서 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)

- PEM(Privacy-enhanced Electronic Mail)

파일이 비밀번호로 보호된 경우 암호 해독 비밀번호를 제공해야 합니다. 인증서와 키가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

적절한 인증서 또는 키 정보를 포함하며 상호 페어링된 파일만 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 페어링을 검증합니다.

내부 인증서 개체를 생성한 후에는 이름을 수정할 수 있지만 다른 개체 속성은 수정할 수 없습니다.

사용 중인 내부 인증서 개체는 삭제할 수 없습니다. 또한 사용 중인 내부 인증서 개체를 편집하면 관련 액세스 제어 정책이 오래된 상태가 됩니다. 변경 사항을 적용하려면 액세스 제어 정책을 재구축해야 합니다.

내부 인증서 개체 추가

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 인증서를 선택합니다.

단계 **3** **Add Internal Cert**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Certificate Data(**인증서 데이터**)** 필드 위에서 **Browse(**찾아보기**)**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 서버 인증서 파일을 업로드합니다.

단계 **6** **Key** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 페어링된 개인 키 파일을 업로드합니다.

단계 **7** 업로드된 개인 키 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크 박스를 선택하고 비밀번호를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

인증서 등록 개체

신뢰 지점을 사용하여 CA와 인증서를 관리하고 추적할 수 있습니다. 신뢰 지점은 CA 또는 ID 쌍을 나타낸 것입니다. 신뢰 지점에는 CA의 ID, CA별 구성 파라미터, 하나의 등록된 ID 인증서와의 연결 관계가 포함되어 있습니다.

인증서 등록 개체에는 CSR(Certificate Signing Requests)을 생성하고 지정된 CA(Certification Authority)에서 ID 인증서를 가져오기 위해 필요한 CA 서버 정보 및 등록 파라미터가 포함되어 있습니다. 이러한 활동은 PKI(Private Key Infrastructure)에서 발생합니다.

인증서 등록 개체에는 인증서 해지 정보도 포함될 수 있습니다. PKI, 디지털 인증서, 인증서 등록에 대한 자세한 내용은 PKI 인프라 및 디지털 인증서을 참조하십시오.

인증서 등록 개체의 사용 방법

인증서 등록 개체는 PKI 인프라에 관리되는 디바이스를 등록하고 다음을 통해 VPN 연결을 지원하는 디바이스에 트러스트 포인트(CA 개체)를 생성합니다.

1. CA 인증 및 인증서 등록 개체 등록에 대한 파라미터를 정의합니다. 공유 파라미터를 지정하고 다른 디바이스에 대해 고유한 개체 설정을 지정하기 위해 오버라이드 기능을 사용합니다.
2. ID 인증서를 요구하는 관리되는 각 디바이스에 개체를 설치 및 연결합니다. 디바이스에서 이는 트러스트 포인트가 됩니다.

   인증서 등록 개체이 연결된 후 디바이스에 설치되면 인증서 등록 프로세스가 즉시 시작됩니다. 이 프로세스는 자체 서명 및 SCEP 등록 유형의 경우 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록 및 PKCS12 파일 가져오기의 경우 관리자의 추가 작업이 필요합니다.
3. VPN 구성에서 생성된 트러스트 포인트를 지정합니다.

인증서 등록 개체 관리

인증서 등록 개체을 관리하려면 개체 > 개체 관리로 이동하고 탐색창에서 **PKI** > 인증서 등록을 선택합니다. 다음 정보가 표시됩니다.

- 기존 인증서 등록 개체는 **Name(**이름**)** 열에 표시됩니다.

  검색 필드(돋보기)를 사용해 목록을 필터링합니다.
- 각 개체의 등록 유형은 **Type(**유형**)** 열에 표시됩니다. 다음 등록 방법을 사용할 수 있습니다.
  - 자체 서명 - 관리되는 디바이스가 자체 서명된 루트 인증서를 생성합니다.
  - **SCEP** - (기본) SCEP(Simple Certificate Enrollment Protocol)은 디바이스가 CA로부터 ID 인증서를 가져올 때 사용합니다.
  - 수동 - 관리자가 수동으로 등록 프로세스를 수행합니다.
  - **PKCS12** 파일 - VPN 연결을 지원하는 Firepower Threat Defense 관리 디바이스에 PKCS12 파일을 가져옵니다. PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다.
- **Override(**오버라이드**)** 열은 개체가 오버라이드를 허용(녹색 확인 표시) 또는 허용 불가(빨간색 X)하는지 여부를 나타냅니다. 숫자가 표시되는 경우 오버라이드의 수를 나타냅니다.

  VPN 구성의 일부인 각 디바이스에 개체 설정을 사용자 정의하려면 오버라이드 옵션을 사용합니다. 오버라이드는 각 디바이스의 트러스트 포인트 세부 정보를 고유하게 만듭니다. 보통 VPN 구성 시 각 디바이스의 일반 이름 또는 제목이 오버라이드됩니다.

  모든 유형의 개체 오버라이드 절차에 대해서는 개체 재정의, 568 페이지를 참조하십시오.

- 편집 아이콘(연필)을 클릭하여 이전에 생성한 인증서 등록 개체를 **Edit(**편집**)**합니다. 등록 개체가 관리되는 디바이스와 연결되지 않은 경우만 편집할 수 있습니다. 편집에 대한 추가 지침은 인증서 등록 개체을 참조하십시오.
- 삭제 아이콘(휴지통)을 클릭하여 이전에 생성한 인증서 등록 개체를 **Delete(**삭제**)**합니다. 관리되는 디바이스와 연결된 경우 인증서 등록 개체을 삭제할 수 없습니다.

Add Cert Enrollment(인증서 등록 추가**)** 대화 상자를 열고 인증서 등록 개체을 구성하려면 **(+) Add Cert Enrollment(**인증서 등록 추가**)**를 누릅니다. 인증서 등록 개체 추가, 630 페이지를 참조하십시오. 각 관리되는 헤드엔드 디바이스에 인증서를 설치합니다.

관련 항목

자체 서명 등록을 사용한 인증서 설치 , 678 페이지
SCEP 등록을 사용한 인증서 설치, 679 페이지
수동 등록을 사용한 인증서 설치, 680 페이지
PKCS12 파일을 가져오는 방법으로 인증서 설치, 681 페이지

인증서 등록 개체 추가

이러한 개체는 FTD 디바이스와 함께 사용할 수 있습니다. 이 작업을 수행하려면 관리자 또는 네트워크 관리자 권한이 있어야 합니다.

프로시저

단계 **1** **Add Cert Enrollment(**인증서 등록 추가**)** 대화 상자를 엽니다.

- 개체 관리자에서 직접 하려는 경우 개체 > 개체 관리 화면에서 탐색창의 **PKI** > 인증서 등록을 선택하고 인증서 등록 추가를 누릅니다.
- 관리되는 디바이스를 구성하는 도중이라면 장치 > 인증서 화면에서 추가 > 새 인증서 추가를 선택하고 **(+)**를 클릭해 인증서 등록 필드를 엽니다.

단계 **2** 개체의 이름과 필요한 경우 설명을 입력합니다.

등록이 완료되면 이 이름은 연결된 관리되는 디바이스의 트러스트 포인트의 이름이 됩니다.

단계 **3** **CA Information(CA** 정보**)** 탭을 열고 **Enrollment Type(**등록 유형**)**을 선택합니다.

- 자체 서명 - 관리되는 디바이스가 CA가 되어 자체 서명된 루트 인증서를 생성합니다. 이 창에서는 기타 정보가 필요하지 않습니다.

  참고 자체 서명 인증서를 등록할 경우 인증서 파라미터에서 CN(Common Name)을 지정해야 합니다.

- **SCEP** - (기본) 단순 인증 등록 프로토콜(Simple Certificate Enrollment Protocol) SCEP 정보를 지정합니다. 인증서 등록 개체 SCEP 옵션, 632 페이지의 내용을 참조하십시오.
- 수동

- **CA Only(CA** 전용**)** - 선택한 CA에서 CA 인증서만 생성하려면 이 체크 박스를 선택합니다. 이 인증서에 대해 ID 인증서가 생성되지 않습니다.

  이 체크 박스를 선택하지 않으면 CA 인증서가 필수가 아닙니다. CA 인증서 없이 CSR을 생성하고 ID 인증서를 얻을 수 있습니다.

- **CA Certificate(CA** 인증서**)** - CA 인증서 정보를 상자에 붙여 넣습니다. 다른 디바이스에서 복사하여 CA 인증서를 가져올 수도 있습니다.

  CA 인증서 없이 CSR을 생성하도록 선택하는 경우 이 상자를 비워둘 수 있습니다.

- **PKCS12** 파일 - VPN 연결을 지원하는 FTD 관리 디바이스에 PKCS12 파일을 가져옵니다. PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다.
- **Skip Check for CA flag in basic constraints of the CA Certificate(CA** 인증서의 기본 제약 조건에서 **CA** 플래그 확인 건너뛰기**)** -

  트러스트 포인트 인증서에서 기본 제약 조건 확장 및 CA 플래그 검사를 건너 뛰려면 이 체크 박스를 선택합니다.

단계 **4** (선택 사항) **Certificate Parameters(**인증서 파라미터**)** 탭을 열고 인증서 내용을 지정합니다. 인증서 등록 개체 인증서 매개변수, 633 페이지의 내용을 참조하십시오.

이 정보는 인증서에 저장되고 라우터에서 인증서를 수신하는 측에서 읽을 수 있습니다.

단계 **5** (선택 사항) **Key(**키**)** 탭을 열고 키 정보를 지정합니다. 인증서 등록 개체 키 옵션, 634 페이지의 내용을 참조하십시오.

단계 **6** (선택 사항) **Revocation(**해지**)** 탭을 클릭하고 해지 옵션을 지정합니다. 인증서 등록 개체 폐기 옵션, 634 페이지를 참조하십시오.

단계 **7** 원하는 경우 개체에 대한 오버라이드를 허용합니다. 개체 오버라이드에 대한 전체 설명은 개체 재정의, 568 페이지을 참조하십시오.

다음에 수행할 작업

디바이스에 트러스트 포인트를 생성하려면 등록 개체를 연결 및 설치합니다.

관련 항목

자체 서명 등록을 사용한 인증서 설치 , 678 페이지
SCEP 등록을 사용한 인증서 설치, 679 페이지
수동 등록을 사용한 인증서 설치, 680 페이지
PKCS12 파일을 가져오는 방법으로 인증서 설치, 681 페이지

인증서 등록 개체 **SCEP** 옵션

Firepower Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > PKI** 등록을 선택합니다. **PKI** 등록 추가 대화 상자를 열고 **CA** 정보 탭을 선택하려면 **(+) Add PKI Enrollment(PKI** 등록 추가**)**를 누릅니다.

필드

등록 유형 - **SCEP**로 설정합니다.

등록 **URL** - 디바이스가 등록을 시도하는 CA 서버의 URL입니다.

CA_name이 CA 서버의 호스트 DNS 이름 또는 IP 주소인 **`http://CA_name:port`** 형태의 HTTP URL을 사용합니다. 포트 번호는 필수입니다.

CA의 CA cgi-bin 스크립트 위치가 기본(/cgi-bin/pkiclient.exe)이 아닌 경우 URL에 http://CA_name:port/script_location 형태로 비표준 스크립트 위치를 포함해야 하며, 이 때 script_location은 CA 스크립트의 전체 경로입니다.

비밀 번호 검사/확인 - 디바이스의 ID를 검증하도록 CA 서버에서 사용되는 비밀번호입니다. CA 서버에 직접 연결하거나 웹 브라우저에 **`http://URLHostName/certsrv/mscep/mscep.dll`**을 입력하여 비밀번호를 얻을 수 있습니다. 비밀번호는 CA 서버에서 가져온 뒤 60분 동안 유효합니다. 따라서 생성 후 최대한 빨리 비밀번호를 구축하는 것이 중요합니다.

재시도 간격 - 인증 요청 시도 재시도 간격으로 분 단위로 되어 있습니다. 값은 1~60분입니다. 기본값은 1분입니다.

재시도 수 - 첫 번째 요청에 인증서가 발행되지 않은 경우 재시도 횟수입니다. 값은 1~100입니다. 기본값은 10입니다.

CA 인증서 소스 - CA 인증서를 얻는 방법을 지정합니다.

- **SCEP**를 사용해 검색(기본, 지원되는 경우) - CA 서버에서 SCEP(단순 인증서 등록 프로세스)를 사용해 인증서를 검색합니다. SCEP를 사용하려면 디바이스와 CA 서버 간의 연결이 필요합니다. 등록 프로세스를 시작하기 전 디바이스가 CA 서버에 연결되었는지 확인하십시오.
- 수동으로 **CA** 인증서 입력 - (브라우저의 복사 기능 또는 Ctrl + V 키보드 바로 가기를 사용하여) **Certificate(**인증서**)** 필드에 다른 디바이스의 CA 서버 인증서를 복사합니다. 각 인증서는 "certificate"라는 단어로 시작해야 하며 "quit"이라는 단어로 끝나야 합니다.

  디바이스가 CA 서버에 직접 연결을 설정할 수 없는 경우 이 방법을 사용합니다.

핑거프린트 - SCEP를 사용하여 CA 인증서를 검색하는 경우 CA 서버에 핑거프린트를 입력할 수 있습니다. CA 서버 인증서의 신뢰성을 확인하기 위해 핑거프린트를 사용하면 권한이 없는 사용자가 실제 대신 가짜 인증서를 대체하는 것을 방지할 수 있습니다. 16진수 형태로 CA 서버의 핑거프린트를 입력합니다. 입력한 값이 인증서의 핑거프린트와 일치하지 않으면 인증서가 거부됩니다. 서버에 직접 연결하거나 웹 브라우저에 **`http://<URLHostName>/certsrv/mscep/mscep.dll`**의 주소를 입력하여 CA의 핑거프린트를 얻을 수 있습니다.

인증서 등록 개체 인증서 매개변수

CA 서버에 전송되는 인증서 요청의 추가 정보를 지정합니다. 이 정보는 인증서에 저장되고 라우터에서 인증서를 수신하는 측에서 읽을 수 있습니다.

Firepower Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > PKI** 등록을 선택합니다. **PKI** 등록 추가 대화 상자를 열고 **(+) PKI** 등록 추가를 누른 뒤 인증서 파라미터 탭을 누릅니다.

필드

표준 LDAP X.500 형식을 사용해 모든 정보를 입력합니다.

- **FQDN** 포함 - 인증서 요청에 FQDN(Fully Qualified Domain Name)을 포함할지 여부를 설정합니다. 다음을 선택할 수 있습니다.
  - 디바이스 호스트 이름을 **FQDN**으로 사용
  - 인증서에 **FQDN** 사용 안 함
  - 사용자 정의 **FQDN** - 이 옵션을 선택하고 표시되는 사용자 정의 **FQDN** 필드에서 지정합니다.
- 디바이스의 **IP** 주소 포함 - 인증서 요청에 IP 주소가 포함되는 인터페이스입니다.
- 일반 이름**(CN)** - 인증서에 포함할 X.500 일반 이름입니다.

  참고 자체 서명 인증서를 등록할 경우 인증서 파라미터에서 CN(Common Name)을 지정해야 합니다.
- 조직 단위**(OU)** - 인증서에 포함될 조직 단위(부서 등)의 이름입니다.
- 조직**(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- 구/군/시**(L)** - 인증서에 포함될 구/군/시입니다.
- 주/도**(ST)** - 인증서에 포함될 주/도입니다.
- 국가 코드**(C)** - 인증서에 포함될 국가입니다. 이 코드는 ISO 3166의 국가 약어를 준수하므로 미국의 경우 "US"로 표시됩니다.
- 이메일**(E)** - 인증서에 포함될 이메일 주소입니다.
- 디바이스의 일련 번호 포함 - 인증서에 디바이스의 인련 번호를 포함할지의 여부입니다. CA는 인증서 인증 또는 추후 특정 디바이스와 인증서를 연결하기 위해 일련 번호를 사용합니다. 확실하지 않은 경우 일련 번호를 포함하면 디버깅 시 유용합니다.

인증서 등록 개체 키 옵션

Firepower Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > Cert Enrollment(**인증서 등록**)**를 선택합니다. **Add Cert Enrollment(**인증서 등록 추가**)** 대화 상자를 열고 **(+) Add Cert Enrollment(**인증서 등록 추가**)**를 누른 뒤 **Key(**키**)** 탭을 누릅니다.

필드

- 키 유형—RSA, ECDSA, EDDSA
- **Key Name(**키 이름**)** - 인증서와 연결할 키 쌍이 이미 있는 경우, 이 필드는 해당 키 쌍의 이름을 지정합니다. 키 쌍이 존재하지 않는 경우, 이 필드는 등록 중에 생성될 키 쌍에 할당할 이름을 지정합니다. 이름을 지정하지 않으려면 FQDN(Fully Qualified Domain Name) 키 페어를 대신 사용합니다.
- 키 크기 - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. 권장 값은 1024비트입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)

인증서 등록 개체 폐기 옵션

방법을 선택 및 구성하여 인증서의 폐기 상태 확인 여부를 지정합니다. 인증서 폐기 확인은 기본적으로 사용하지 않으며 두 방법(CRL 또는 OSCP) 모두 체크 해제되어 있습니다.

Firepower Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > PKI** 등록을 선택합니다. **PKI** 등록 추가 대화 상자를 열고 **(+) PKI** 등록 추가를 누른 뒤 폐기 탭을 누릅니다.

필드

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.
  - 인증서에서 **CRL** 배포 지점 사용 - 인증서에서 폐기 목록 배포 URL을 사용하는지 확인합니다.
  - 정적 **URL** 구성 사용 - 폐기 목록에 정적, 사전 정의 배포 URL을 추가하려는 경우 선택합니다. 이어서 URL을 추가합니다.

    CRL 서버 **URL** - CRL을 다운로드할 수 있는 LDAP 서버의 URL입니다. 이 URL은 **`ldap://`**로 시작하고 포트 번호가 포함되어야 합니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  OCSP 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다. 이 URL은 **`http://`**로 시작해야 합니다.

- 폐기 정보를 찾을 수 없는 경우 인증서를 유효한 것으로 간주 - 기본적으로 선택되어 있습니다. 이를 허용하지 않으려면 선택을 취소합니다.

참고 **Consider the certificate valid if revocation information can not be reached(**폐기 정보를 찾을 수 없는 경우 인증서를 유효한 것으로 간주**)** 체크 박스 설정은 FTD 6.4 이하 버전에만 적용됩니다. FTD 6.5 이상 버전의 경우 이 설정이 무시되고 바이패스가 작동하지 않습니다.

키 체인 개체

데이터 보안 및 디바이스 보호 기능을 강화하기 위해 IGP 피어 인증용 회전 키는 최대 180일간 사용할 수 있습니다. 회전 키는 악의적인 사용자가 라우팅 프로토콜 인증에 사용되는 키를 추측하는 것을 방지하므로 네트워크가 잘못된 경로를 알리고 트래픽을 리디렉션하지 못하도록 보호합니다. 키를 자주 변경하면 결국에는 추측되는 위험이 줄어듭니다. 키 체인을 제공하는 라우팅 프로토콜에 대한 인증을 구성할 때 키 체인의 키 수명이 겹치도록 구성합니다. 이렇게 하면 액티브 키가 없기 때문에 키 보안 통신이 손실되는 것을 방지하는 데 도움이 됩니다. 회전 키는 OSPFv2 프로토콜에만 적용될 수 있습니다. 키 수명이 만료되고 액티브 키를 찾을 수 없는 경우 OSPF는 피어와의 인접성을 유지 관리하기 위해 마지막으로 유효한 키를 사용합니다.

참고 인증에는 MD5 암호화 알고리즘만 사용됩니다.

키 수명

안정적인 통신을 유지하기 위해 각 디바이스는 키 체인 인증 키를 저장하고 동시에 한 개 이상의 키를 사용합니다. 키 체인 관리는 키 전송 및 수신 수명을 기반으로 키의 롤오버를 처리하는 보안 메커니즘을 제공합니다. 디바이스는 키의 수명을 사용해 키 체인에서 활성화될 키를 결정합니다.

키 체인의 각 키에는 두 개의 수명이 있습니다.

- 수신 수명 - 다른 디바이스와 키를 교환할 때 디바이스가 키를 수신하는 데 걸리는 시간 간격입니다.
- 전송 수명 - 다른 디바이스와 키를 교환할 때 디바이스가 키를 전송하는 데 걸리는 시간 간격입니다.

키 전송 수명 동안 디바이스는 키로 라우팅 업데이트 패킷을 전송합니다. 디바이스는 전송된 키가 디바이스의 키 수신 수명을 벗어난 경우 다른 디바이스의 통신을 수신하지 않습니다.

키 수명이 구성되지 않은 경우 타임라인 없이 MD5 인증 키를 구성하는 것과 같습니다.

키 선택

- 키 체인에 하나 이상의 유효한 키가 있는 경우 OSPF는 최대 수명을 가지고 있는 키를 선택합니다.
- 키의 수명은 무한인 것이 좋습니다.
- 키가 동일한 수명을 가진 경우 키 ID가 높은 키가 좋습니다.

키 체인 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Key Chain(**키 체인**)**을 선택합니다.

단계 **3** **Add Key Chain(**키 체인 추가**)**를 클릭합니다.

단계 **4** 키 체인 개체 추가 대화 상자의 이름 필드에 키 체인의 이름을 입력합니다.

이름은 밑줄 또는 알파벳으로 시작해야 하며 이후에는 영숫자 및 특수 문자(-, _, +, .)로 구성되어야 합니다.

단계 **5** 키 체인에 키를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **6** **Key ID** 필드에 키 식별자를 지정합니다.

키 ID 값은 0~255 범위의 값일 수 있습니다. 유효하지 않은 키를 표시하려는 경우에만 0을 사용합니다.

단계 **7** 알고리즘 필드 및 암호화 유형 필드는 MD5 및 일반 텍스트로 지원되는 알고리즘 및 암호화 유형을 표시합니다.

단계 **8** 암호화 키 문자열 필드에 암호를 입력하고 암호화 키 문자열 확인 필드에 암호를 다시 입력합니다.

- 암호의 길이는 최대 80자입니다.
- 한 자리 숫자이거나 숫자 뒤에 공백이 오는 암호는 지정할 수 없습니다. 예를 들어 "0 pass" 또는 "1"은 유효하지 않습니다.

단계 **9** 다른 디바이스와 키 교환 시 키를 수신/전송하는 시간 간격을 설정하려면 수신 수명 및 전송 수명 필드에 수명 값을 제공합니다.

참고 날짜 및 시간 값은 UTC 표준 시간대를 기본으로 사용합니다.

종료 시간은 수신/전송 수명이 종료되거나 영원히 만료되지 않는 경우의 기간, 즉 절대 시간이 될 수 있습니다. 기본 종료 시간은 날짜 및 시간입니다.

다음은 시작 및 종료 값에 대한 검증 규칙입니다.

- 최종 수명이 지정된 경우 시작 수명은 null이 될 수 없습니다.

- 수신 또는 전송 수명의 시작 수명은 종료 수명보다 이전이어야 합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

키를 생성하려면 5~10단계를 반복합니다. 키 체인에 수명이 중복되는 키를 최소 2개 생성합니다. 이렇게 하면 액티브 키가 없기 때문에 키 보안 통신이 손실되는 것을 방지하는 데 도움이 됩니다.

단계 **11** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 570 페이지의 내용을 참조하십시오.

단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

DNS 서버 그룹 개체

DNS(Domain Name System) 서버는 www.example.com 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인합니다.

DNS 서버 그룹 개체 생성

이러한 개체는 NGIPSv을(를) 제외한 모든 디바이스 유형과 함께 사용할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** 네트워크 개체 목록에서 **DNS Server Group(DNS** 서버 그룹**)**을 클릭합니다.

단계 **3** **Add DNS Server Group(DNS** 서버 그룹 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요에 따라 정규화되지 않은 호스트 이름에 추가하는 데 사용될 기본 도메인을 입력합니다.

단계 **6** 기본 시간 초과 및 재시도 값은 사전 입력되어 있습니다. 필요한 경우 이 값을 변경합니다.

- Retries(재시도 횟수) - 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수(0~10회)입니다. 기본값은 2입니다.
- Timeout(시간한) — 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 초과 값이 두 배로 늘어납니다.

단계 **7** 쉼표로 구분된 항목으로 IPv4 또는 IPv6 형식으로 이 그룹의 일부가 될 **DNS** 서버를 입력합니다.

하나의 그룹에 최대 6개의 DNS 서버가 포함될 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

DNS 서버 그룹의 DNS 서버 구성은 DNS 플랫폼 설정의 인터페이스 개체에 할당되어야 합니다. 자세한 내용은 DNS 구성, 1425 페이지를 참고하십시오.

SLA 모니터 개체

각 인터넷 프로토콜 SLA(Service Level Agreement)는 모니터링되는 주소에 대한 연결 정책을 정의하며 주소에 대한 경로의 가용성을 추적합니다. 경로는 ICMP 에코 요청을 전송하고 응답을 기다리며 주기적으로 가용성을 확인합니다. 요청이 시간 초과되면 경로는 라우팅 테이블에서 제거되고 백업 경로로 교체됩니다. SLA 모니터링 작업은 구축 후 즉시 시작되고 SLA 모니터를 디바이스 설정에서 제거하지 않는 이상 계속 실행됩니다. (즉 노후화가 되지 않습니다.) 인터넷 프로토콜 SLA(Service Level Agreement) 모니터링 개체는 IPv4 정적 경로 정책의 경로 추적 필드에 사용됩니다. IPv6 경로에는 경로 추적을 통해 SLA 모니터를 사용하기 위한 옵션이 없습니다.

이러한 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **SLA** 모니터링을 선택합니다.

단계 **2** **ADD SLA Monitor(SLA** 모니터링 추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 개체의 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)** 필드에 개체의 설명을 입력합니다.

단계 **5** **Frequency(**빈도**)** 필드에 초 단위로 ICMP 에코 요청 전송의 간격을 입력합니다. 유효한 값은 1~604800초(7일)입니다. 기본값은 60초입니다.

참고 빈도는 시간 초과 값보다 작을 수 없습니다. 값을 비교하려면 빈도를 밀리초 단위로 변경해야 합니다.

단계 **6** **SLA** 모니터 **ID** 필드에 SLA 작업의 ID 번호를 입력합니다. 유효한 값은 1~2147483647입니다. 최대 2000개의 SLA 작업을 생성할 수 있습니다. 각 ID 번호는 정책 및 디바이스 설정에 대해 고유해야 합니다.

단계 **7** 임계값 필드에서 ICMP 에코 요청 후 임계값 증가 선언 전 통과해야 하는 시간을 입력합니다. 유효한 값은 0~2147483647밀리초입니다. 기본값은 5000밀리초입니다. 임계값은 정의된 값을 초과하는 이벤트를 표시할 때만 사용됩니다. 적절한 시간 초과 값을 평가하기 위해 이러한 이벤트를 사용할 수 있습니다. 모니터링되는 주소의 연결성을 직접 표시하지 않습니다.

참고 임계값은 시간 초과 값을 넘지 않아야 합니다.

단계 **8** 시간 초과 필드에 SLA 작업이 ICMP 에코 요청 응답을 대기하는 시간을 밀리초 단위로 입력합니다. 유효한 값은 0~604800000밀리초(7일)입니다. 기본값은 5000밀리초입니다. 이 필드에 정의된 시간 안에 모니터링되는 주소에서 응답이 수신되지 않으면 고정 경로는 라우팅 테이블에서 제거되고 백업 경로로 교체됩니다.

참고 시간 초과 값은 빈도 값을 초과할 수 없습니다. (수치를 비교하기 위해 빈도 값을 밀리초 단위로 조정합니다.)

단계 **9** 데이터 크기 필드에 ICMP 요청 패킷 페이로드의 크기를 바이트 단위로 입력합니다. 유효한 값의 범위는 0~16384바이트입니다. 기본값은 28바이트이며 총 64바이트의 ICMP 패킷을 생성합니다. 프로토콜 또는 경로 최대 전송 단위(PMTU)에 의해 허용되는 최대값보다 큰 값을 설정하지 마십시오. 소스와 대상의 PMTU 변경을 탐지하려면 연결성을 위해 기본 데이터 크기를 늘려야 할 수 있습니다. 낮은 PMTU는 세션 성능에 영향을 미칠 수 있으며 탐지되는 경우 보조 경로를 사용해야 함을 나타냅니다.

단계 **10** **ToS** 필드에 ICMP 요청 패킷의 IP 헤더에서 정의된 서비스 유형(ToS) 값을 입력합니다. 유효한 값의 범위는 0~255입니다. 기본값은 0입니다. 이 필드에는 지연, 우선 순위, 신뢰성 등의 정보가 포함됩니다. 네트워크의 다른 디바이스가 커밋된 액세스 속도 등 정책 라우팅 및 기능에 이를 사용할 수 있습니다.

단계 **11** 패킷 수 필드에 전송되는 패킷 수를 입력합니다. 유효한 값의 범위는 1~100입니다. 기본값은 1패킷입니다.

참고 패킷 손실로 인해 Firepower Threat Defense 디바이스가 모니터링되는 주소에 연결할 수 없다고 잘못 인식하는 것이 우려되는 경우 기본 패킷 수를 늘립니다.

단계 **12** 모니터링 되는 주소 필드에는 SLA 작업을 통해 가용성이 모니터링되는 IP 주소를 입력합니다.

단계 **13** 가용 영역 목록은 영역 및 인터페이스 그룹을 표시합니다. 영역/인터페이스 목록에는 디바이스가 관리 스테이션과 통신하는 인터페이스가 포함된 영역 및 인터페이스 그룹을 추가합니다. 단일 인터페이스를 지정하려면 인터페이스에 영역 또는 인터페이스 그룹을 생성해야 합니다. 보안 영역 개체 생성, 578 페이지을 참조하십시오. 디바이스에 선택된 인터페이스 또는 영역이 포함되는 경우에만 디바이스에서 호스트가 구성됩니다.

단계 **14** **Save(**저장**)**를 클릭합니다.

접두사 목록

경로 맵, 정책 맵, OSPF 필터링 또는 BGP 네이버 필터링을 구성할 때 사용할 IPv4 및 IPv6용 접두어 목록 개체를 만들 수 있습니다.

IPv6 접두사 목록 구성

IPv6 접두사 목록 구성 페이지를 사용하여 접두사 목록 개체를 생성, 복사, 편집합니다. 경로 맵, 정책 맵, OSPF 필터링 또는 BGP 네이버 필터링을 구성할 때 사용할 접두어 목록 개체를 만들 수 있습니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 접두사 목록 > **IPv6** 접두사 목록을 선택합니다.

단계 **2** **Add Prefix List(**접두사 목록 추가**)**를 선택합니다.

단계 **3** 새 접두사 목록 개체 창에서 이름 필드에 접두사 목록 개체에 대한 이름을 입력합니다.

단계 **4** 새 접두사 목록 개체 창에서 **Add(**추가**)**를 클릭합니다.

단계 **5** 작업 드롭다운 목록에서 재배포 액세스를 표시하기 위해 허용 또는 차단 등 적절한 작업을 선택합니다.

단계 **6** 개체에 이미 구성된 접두사 목록 항목의 목록 내 새 접두사 목록 항목의 위치를 나타내는 고유한 번호를 시퀀스 번호 필드에 입력합니다. 비워 둘 경우 시퀀스 번호는 현재 사용되는 시퀀스 번호보다 5로 기본 설정됩니다.

단계 **7** **IP** 주소 필드에 IP 주소/마스크 길이 형식의 IPv6 주소를 지정합니다. 마스크 길이는 1~128 사이의 유효한 값이어야 합니다.

단계 **8** 최소 접두사 길이 필드에 최소 접두사 길이를 입력합니다. 이 값은 마스크 길이보다 커야하며 최대 접두사 길이를 지정한 경우 이와 같거나 짧아야 합니다.

단계 **9** 최대 접두사 길이 필드에 최대 접두사 길이를 입력합니다. 최소 접두사 길이를 지정한 경우 이 값은 최소 접두사 길이와 같거나 길어야 하며 최소 접두사 길이가 지정되지 않은 경우 마스크 길이보다 길어야 합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

단계 **11** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **12** **Save(**저장**)**를 클릭합니다.

IPv4 접두사 목록 구성

IPv4 접두사 목록 구성 페이지를 사용하여 접두사 목록 개체를 생성, 복사, 편집합니다. 경로 맵, 정책 맵, OSPF 필터링 또는 BGP 네이버 필터링을 구성할 때 사용할 접두어 목록 개체를 만들 수 있습니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 접두사 목록 > **IPv4** 접두사 목록을 선택합니다.

단계 **2** **Add Prefix List(**접두사 목록 추가**)**를 선택합니다.

단계 **3** 새 접두사 목록 개체 창에서 이름 필드에 접두사 목록 개체에 대한 이름을 입력합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** 작업 드롭다운 목록에서 재배포 액세스를 표시하기 위해 허용 또는 차단 등 적절한 작업을 선택합니다.

단계 **6** 개체에 이미 구성된 접두사 목록 항목의 목록 내 새 접두사 목록 항목의 위치를 나타내는 고유한 번호를 시퀀스 번호 필드에 입력합니다. 비워 둘 경우 시퀀스 번호는 현재 사용되는 시퀀스 번호보다 5로 기본 설정됩니다.

단계 **7** **IP** 주소 필드에 IP 주소/마스크 길이 형식의 IPv4 주소를 지정합니다. 마스크 길이 1~32 사이의 유효한 값이어야 합니다.

단계 **8** 최소 접두사 길이 필드에 최소 접두사 길이를 입력합니다. 이 값은 마스크 길이보다 커야하며 최대 접두사 길이를 지정한 경우 이와 같거나 짧아야 합니다.

단계 **9** 최대 접두사 길이 필드에 최대 접두사 길이를 입력합니다. 최소 접두사 길이를 지정한 경우 이 값은 최소 접두사 길이와 같거나 길어야 하며 최소 접두사 길이가 지정되지 않은 경우 마스크 길이보다 길어야 합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

단계 **11** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **12** **Save(**저장**)**를 클릭합니다.

경로 맵

경로 맵은 경로를 라우팅 프로세스에 재분배할 때 사용됩니다. 또한 라우팅 프로세스로 기본 경로를 생성할 때도 사용됩니다. 경로 맵은 지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 정의합니다. 경로 맵을 구성하여 경로 맵 개체에 대한 새 경로 맵 항목을 생성하거나 기존 경로 맵을 편집합니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

시작하기 전에

A 경로 맵은 이러한 개체를 하나 이상 사용할 수 있습니다. 이런 개체를 모두 추가하는 것은 필수 사항이 아닙니다. 경로 맵을 구성하려면 필요에 따라 이런 개체를 생성하고 사용합니다.

- ACL 추가
- 접두사 목록 추가
- AS 경로 추가
- 커뮤니티 목록 추가
- 정책 목록 추가

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 경로 맵을 선택합니다.

단계 **2** **Add Route Map(**경로 맵 추가**)**를 클릭합니다.

단계 **3** **New Route Map Object(**새 경로 맵 개체**)** 창에서 **Add(**추가**)**를 클릭합니다.

단계 **4** 시퀀스 번호 필드에 0~65535 사이의 숫자를 입력합니다. 이는 경로 맵 개체에 이미 구성된 경로 맵 항목 목록 내 새 경로 맵 항목의 위치를 표시합니다.

참고 나중에 절을 추가해야 할 경우에 대비하여 최소 10 간격의 숫자 절을 추천합니다.

단계 **5** 재배포 드롭다운 목록에서 재배포 액세스를 표시하기 위해 허용 또는 차단 등 적절한 작업을 선택합니다.

단계 **6** (경로/트래픽을) 일치시키기 위해 목차에서 다음 기준에 따라 **Match Clauses(**절 일치**)** 탭을 클릭합니다.

- 보안 영역 - (인그레스/이그레스) 인터페이스를 기준으로 트래픽에 일치시킵니다. 영역을 선택하여 추가하거나 인터페이스 이름에 입력해 추가합니다.
- **IPv4** - 다음 기준을 기반으로 IPv4(경로/트래픽)을 일치시킵니다. 기준을 정의하려면 탭을 선택합니다.
  1. 경로 주소를 기반으로 경로를 일치시키려면 주소 탭을 클릭합니다. IPv4 주소를 드롭다운 목록에서 일치시키는 데 액세스 목록 또는 접두사 목록을 사용할지 선택하고 이때 사용할 ACL 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.
  2. 경로의 다음 홉 주소를 기반으로 경로를 일치시키려면 다음 홉 탭을 클릭합니다. IPv4 주소를 드롭다운 목록에서 일치시키는 데 액세스 목록 또는 접두사 목록을 사용할지 선택하고 이때 사용할 ACL 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.
  3. 경로의 알림 소스 주소를 기반으로 경로를 일치시키려면 경로 소스 탭을 클릭합니다. IPv4 주소를 드롭다운 목록에서 일치시키는 데 액세스 목록 또는 접두사 목록을 사용할지 선택하고 이때 사용할 ACL 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.
- **IPv6** - 라우팅 주소, 다음 홉 주소, 경로의 알림 소스 주소를 기반으로 IPv6(경로/트래픽)를 일치시킵니다.
- **BGP** - 다음 기준을 기반으로 BGP(경로/트래픽)을 일치시킵니다. 기준을 정의하려면 탭을 선택합니다.
  1. 특정 경로 액세스 목록과 BGP 자율 시스템 경로 액세스 목록 일치를 활성화하려면 **AS** 경로 탭을 클릭합니다. 경로 액세스 목록을 하나 이상 지정하는 경우 경로가 아무 경로 액세스 목록과도 일치할 수 있습니다.
  2. 특정 커뮤니티와 BGP 커뮤니티 일치를 활성화하려면 커뮤니티 목록 탭을 클릭합니다. 하나 이상의 커뮤니티를 지정하는 경우 경로가 아무 커뮤니티나 일치할 수 있습니다. 하나 이상의 Match 커뮤니티와 일치하지 않는 경로는 아웃바운드 경로 맵에 대해 알려지지 않습니다.

3. BGP 정책을 평가하고 처리하도록 경로 맵을 구성하려면 정책 목록 탭을 클릭합니다. 여러 정책 목록이 하나의 경로 맵 항목 내에서 일치를 수행하는 경우 모든 정책 목록은 들어오는 특성에 대해서만 확인됩니다.

- 기타 - 다음 기준에 따라 경로 또는 트래픽을 일치시킵니다.

1. 경로 메트릭 일치를 활성화하려면 메트릭 경로 값 필드에 일치에 사용할 메트릭 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 통해 지정된 메트릭이 있는 어떤 값과도 일치시킬 수 있습니다. 메트릭 값의 범위는 0~4294967295입니다.
2. 태그 값 필드에 일치에 사용할 태그 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 사용하면 특정 보안 그룹 태그가 있는 모든 경로를 일치시킬 수 있습니다. 태그 값의 범위는 0~4294967295입니다.
3. 경로 유형 일치를 활성화하려면 적절한 경로 유형 옵션을 체크합니다. 유효한 경로 유형은 External1, External2, Internal, Local, NSSA-External1 및 NSSA-External2입니다. 목록에서 하나 이상의 경로 유형을 선택할 수 있습니다.

단계 **7** 목차에서 선택한 다음 조건에 따라 경로/트래픽을 설정하려면 절 설정 탭을 클릭합니다.

- 메트릭 값 - 대역폭을 설정하기 위해 모든 값을 입력하거나 값을 입력하지 않습니다.

1. 대역폭 필드에 초당 Kbits 단위로 메트릭 값 또는 대역폭을 입력합니다. 유효한 값은 0~4294967295 범위의 정수 값입니다.
2. 대상 라우팅 프로토콜에 대한 메트릭 유형을 지정하려면 메트릭 유형 드롭다운 목록에서 선택합니다. 유효한 값은 내부, 유형 1, 유형 2입니다.

- **BGP** 절 - 다음 조건에 따라 BGP 경로를 설정합니다. 조건을 정의하려면 탭을 선택합니다.

1. BGP 경로에 대한 자율 시스템 경로를 변경하려면 **AS** 경로 탭을 클릭합니다.
    1. BGP 경로에 임의의 시스템 자율 경로 문자열을 첨부하려면 첨부된 **AS** 경로 필드에 AS 경로 번호를 입력합니다. 일반적으로 로컬 AS 번호가 여러 번 부착되어 자율 시스템 경로 길이가 늘어납니다. AS 경로 번호를 하나 이상 지정하면 경로는 아무 AS 번호나 추가할 수 있습니다.
    2. 최종 AS 번호를 AS 경로에 첨부하려면 최종 **AS**를 **AS** 경로에 첨부 필드에 AS 경로 번호를 입력합니다. AS 번호로 1 ~ 10의 값을 입력하십시오.
    3. **Convert route tag into AS Path(AS** 경로로 경로 태그 변환**)** 확인란을 선택하여 경로의 태그를 자율 시스템 경로로 변환하십시오.
2. 커뮤니티 특성을 설정하려면 커뮤니티 목록 탭을 클릭합니다.
    1. **None(**없음**)**을 클릭하여 경로 맵을 전달하는 접두사에서 커뮤니티 속성을 제거합니다.
    2. **Specify Community(**커뮤니티 설정**)**를 클릭하여 적용 가능한 경우 커뮤니티 번호를 입력합니다. 유효한 값은 1~4294967295입니다.

3. **Add to the existing communities(**기존 커뮤니티에 추가**)**를 선택하여 커뮤니티를 이미 존재하는 커뮤니티에 추가합니다.
4. **Internet(**인터넷**)**, **No-advertise(**알림 없음**)** 또는 **No-export(**내보내지 않음**)** 체크 박스를 선택하여 잘 알려진 커뮤니티 중 하나를 사용합니다.

3. 추가 특성을 설정하려면 기타 탭을 클릭합니다.
   1. 자동으로 태그 값을 계산하려면 자동 태그 설정을 선택합니다.
   2. 로컬 환경설정 설정 필드에 자동 시스템 경로에 대한 환경설정 값을 입력합니다. 0~4294967295 사이의 값을 입력합니다.
   3. 가중치 설정 필드에 라우팅 테이블에 대한 BGP 가중치를 입력합니다. 0에서 65535 사이의 값을 입력합니다.
   4. BGP 출처 코드를 지정하려면 선택합니다. 유효한 값은 **Local IGP** Local IGP와 **Incomplete** 입니다.
   5. IPv4 설정 섹션에서 패킷이 출력될 다음 홉의 다음 홉 IPv4 주소를 지정합니다. 인접 라우터일 필요는 없습니다. IPv4 주소를 하나 이상 지정하면 패킷이 아무 IP 주소로나 출력될 수 있습니다.

      접두사 목록 드롭다운 목록에서 IPv4 접두사 목록을 지정하려면 이 옵션을 선택합니다.
   6. IPv6 설정 섹션에서 하 여 패킷이 출력 되 next hop next hop IPv6 주소를 지정 합니다. 인접 라우터일 필요는 없습니다. IPv6 주소를 하나 이상 지정하면 패킷이 아무 IP 주소로나 출력될 수 있습니다.

      접두사 목록 드롭다운 목록에서 IPv6 접두사를 지정하려면 이 옵션을 선택합니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **10** **Save(**저장**)**를 클릭합니다.

액세스 목록

ACL(Access Control List)이라고도 알려진 액세스 목록 개체는 서비스를 적용할 트래픽을 선택합니다. FTD 디바이스에 대해 경로 맵과 같은 특별한 기능을 설정할 때 이러한 개체를 사용합니다. ACL에 의해 허용으로 식별된 트래픽은 서비스가 제공되는 반면 "차단된" 트래픽은 서비스에서 제외됩니다. 서비스에서 제외된 트래픽은 반드시 삭제된다는 의미는 아닙니다.

다음 유형의 ACL을 구성할 수 있습니다.

- 확장 - 소스 및 대상 주소와 포트를 기반으로한 트래픽을 식별합니다. 특정 규칙을 혼합할 수 있는 IPv4 및 IPv6 주소를 지원합니다.

• 표준 - 대상 주소만을 기반으로 트래픽을 식별합니다. IPv4만 지원합니다.

ACL은 하나 이상의 ACE(액세스 제어 항목) 또는 규칙으로 구성됩니다. ACE의 순서는 중요합니다. 패킷이 "허용된" ACE와 일치하는지 평가하는 데 ACL이 사용되면, 패킷은 각 ACE 항목에 대해 항목이 나열된 순서에 따라 점검됩니다. 일치가 발견되면 ACE가 더 이상 점검되지 않습니다. 예를 들어 10.100.10.1을 "허용"하지만 10.100.10.0/24의 나머지는 "차단"하려는 경우 허용 항목은 차단 항목 앞에 위치해야 합니다. 일반적으로 더 구체적인 규칙이 ACL의 상단에 배치됩니다.

"허용" 항목과 일치하지 않는 패킷은 차단해야 할 패킷으로 간주됩니다.

다음 주제는 ACL 개체를 구성하는 방법을 설명합니다.

확장 **ACL** 개체 설정

소스, 대상 주소, 프로토콜, 포트를 기반으로 트래픽을 일치시키려고 하거나 트래픽이 IPv6인 경우 확장 ACL 개체를 사용합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 액세스 제어 목록 > 확장을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 **Add Extended ACL(**확장 **ACL** 추가**)**를 클릭합니다.
- 수정( )을 클릭하여 기존 개체를 편집합니다.

단계 **3** 확장 ACL 개체 대화 상자에서 개체의 이름을 입력(공백은 허용되지 않음)하고 액세스 제어 항목을 구성합니다.

a) 다음 중 하나를 수행합니다.

- **Add(**추가**)**를 클릭하여 새 엔트리를 만듭니다.
- 수정( )을 클릭해서 기존 항목을 편집합니다.

마우스 오른쪽 버튼 클릭 메뉴에는 항목 잘라내기, 복사, 붙여넣기, 삭제 옵션이 포함되어 있습니다.

b) 작업을 선택하여 트래픽 조건을 허용(일치) 또는 차단(불일치)합니다.

참고 로그인, 로그 레벨, 로그 간격 옵션은 액세스 규칙에만 사용됩니다. (인터페이스에 속한 ACL 또는 전역으로 적용된 ACL) 액세스 규칙에 ACL 개체가 사용되지 않으므로 이 값을 기본값으로 유지합니다.

c) 다음 방법 중 하나를 사용하여 네트워크 탭에서 소스 및 대상 주소를 구성합니다.

- 사용 가능한 목록에서 원하는 네트워크 개체 또는 그룹을 선택하고 **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**를 클릭합니다. 목록 위의 +를 클릭하여 새 개체를 생성할 수 있습니다. IPv4 및 IPv6 주소를 혼합할 수 있습니다.

- 소스 또는 대상 목록 아래의 편집 상자에 주소를 입력하고 **Add(**추가**)**를 클릭합니다. 단일 호스트 주소(10.100.10.5 또는 2001:DB8::0DB8:800:200C:417A 등)나 서브넷(10.100.10.0/24 또는 10.100.10.0 255.255.255.0 형식, 또는 IPv6의 경우 2001:DB8:0:CD30::/60)를 지정할 수 있습니다.

d) 포트 탭을 클릭하고 다음 방법 중 하나를 사용하여 서비스를 구성합니다.

- 사용 가능한 목록에서 원하는 포트 개체를 선택하고 **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**를 클릭합니다. 목록 위의 +를 클릭하여 새 개체를 생성할 수 있습니다. 개체는 TCP/UDP 포트, ICMP/ICMPv6 메시지 유형, ("any" 포함) 다른 프로토콜을 지정할 수 있습니다. 그러나 일반적으로 비워 두는 소스 포트는 TCP/UDP만 수락합니다. 포트 그룹은 선택할 수 없습니다.
- 소스 또는 대상 목록 아래의 편집 상자에 포트 또는 프로토콜을 입력하거나 선택하고 **Add(**추가**)**를 클릭합니다.

참고 모든 IP 트래픽에 적용되는 항목을 얻기 위해 "all(모든)" 프로토콜을 지정하는 대상 포트 개체를 선택합니다.

e) 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.
f) 필요한 경우 항목을 클릭한 뒤 위나 아래로 드래그하여 규칙 순서에서 원하는 위치로 이동합니다.

개체에 추가 항목을 생성하거나 편집하려면 프로세스를 반복합니다.

단계 **4** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

표준 **ACL** 개체 설정

대상 IPv4 주소만에 기반해 트래픽을 일치시키려면 표준 ACL 개체를 사용합니다. 그 외에는 확장 ACL을 사용합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 액세스 제어 목록 > 표준을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 **Add Standard ACL(**표준 **ACL** 추가**)**를 클릭합니다.
- 수정( )을 클릭하여 기존 개체를 편집합니다.

단계 **3** 표준 ACL 개체 대화 상자에서 개체의 이름을 입력(공백은 허용되지 않음)하고 액세스 제어 항목을 구성합니다.

a) 다음 중 하나를 수행합니다.

- **Add(**추가**)**를 클릭하여 새 엔트리를 만듭니다.
- 수정( )을 클릭해서 기존 항목을 편집합니다.

마우스 오른쪽 버튼 클릭 메뉴에는 항목 잘라내기, 복사, 붙여넣기, 삭제 옵션이 포함되어 있습니다.

b) 각 액세스 제어 항목에 대해 다음 속성을 구성합니다.

- 작업 - 트래픽 조건을 허용(일치) 또는 차단(불일치)합니다.
- 네트워크 - IPv4 네트워크 개체 또는 트래픽 대상을 식별하는 그룹을 추가합니다.

c) 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.

d) 필요한 경우 항목을 클릭한 뒤 위나 아래로 드래그하여 규칙 순서에서 원하는 위치로 이동합니다.

개체에 추가 항목을 생성하거나 편집하려면 프로세스를 반복합니다.

단계 **4** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

AS 경로 개체

AS 경로는 BGP를 설정하기 위한 필수 속성입니다. 이는 네트워크에 액세스할 수 있는 일련의 AS 번호입니다. AS 경로는 소스와 대상 라우터 간 AS 번호 시퀀스로 패킷이 이동할 방향을 형성합니다. 인접한 자율 시스템(AS)는 BGP를 사용하여 다른 AS 접두사에 도달하는 방법에 대한 메시지를 교환하고 업데이트합니다. 각 라우터가 대상까지 최선의 경로에 대한 새 로컬 결정을 내리면 각 피어에 해당 경로, 경로 정보를 비롯해 거리 메트릭 및 경로 속성을 전송합니다. 이 정보가 네트워크를 통해 이동할 때 경로의 각 라우터는 고유한 AS 번호를 BGP 메시지의 AS 목록에 첨부합니다. 이 목록은 경로의 AS 경로입니다. AS 접두사가 있는 AS 경로는 네트워크를 통해 단방향 트랜짓 경로에 대한 특정 핸들을 제공합니다. AS 경로 설정 페이지를 사용해 자율 시스템(AS) 경로 정책 개체를 생성, 복사, 편집합니다. 경로 맵, 정책 맵, BGP 네이버 필터링을 구성할 때 사용할 AS 경로 개체를 생성할 수 있습니다. AS 경로 필터를 사용하면 정규식을 사용하여 라우팅 업데이트 메시지를 필터링할 수 있습니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **AS** 경로를 선택합니다.

단계 **2** **Add AS Path(AS** 경로 추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)**필드에 AS 경로 개체 이름을 입력합니다. 유효한 값은 1~500입니다.

단계 **4** 새 **AS** 경로 개체 창에서 **Add(**추가**)**를 클릭합니다.

a) 재배포 액세스를 나타내기 위해 작업 드롭다운 목록에서 허용 또는 차단 옵션을 선택합니다.

b) 정규식 필드에 AS 경로 필터를 정의하는 정규식을 지정합니다.

c) **Add(**추가**)**를 클릭합니다.

단계 **5** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

커뮤니티 목록

커뮤니티는 선택적 전이 BGP 속성입니다. 커뮤니티는 공통 속성을 공유하는 목적지 그룹입니다. 경로 태그 지정에 사용됩니다. BGP 커뮤니티 속성은 특정 접두사에 할당되고 다른 네이버에 전달되는 숫자 값입니다. 커뮤니티는 공통 특성을 공유하는 접두사 집합 표시로 사용될 수 있습니다. 업스트림 제공자는 이런 표시를 사용하여 필터링, 특정 로컬 환경설정 할당, 다른 속성 수정 등 일반 라우팅 정책을 적용할 수 있습니다. 커뮤니티 목록 구성 페이지를 사용해 커뮤니티 목록 정책 개체를 생성, 복사, 편집할 수 있습니다. 경로 맵 또는 정책 맵을 구성할 때 사용할 커뮤니티 목록 개체를 생성할 수 있습니다. 커뮤니티 목록을 사용하여 경로 맵의 일치 조항에서 사용할 커뮤니티 그룹을 만들 수 있습니다. 커뮤니티 목록은 일치하는 문장의 순서가 지정된 목록입니다. 일치가 발견될 때까지 규칙을 기준을 대상을 매칭합니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 커뮤니티 목록을 선택합니다.

단계 **2** **Add Community List(**커뮤니티 목록 추가**)**를 클릭합니다.

단계 **3** 이름 필드에 커뮤니티 목록 개체의 이름을 지정합니다.

단계 **4** 새 커뮤니티 목록 개체 창에서 **Add(**추가**)**를 클릭합니다.

단계 **5** 커뮤니티 규칙 유형을 표시하기 위해 **Standard(**표준**)** 라디오 버튼을 선택합니다.

표준 커뮤니티 목록은 잘 알려진 특정 커뮤니티 또는 커뮤니티 수를 구성하는 데 사용합니다.

참고 표준 커뮤니티 규칙 유형을 사용한 항목과 확장 커뮤니티 규칙 유형을 사용한 항목을 동일한 커뮤니티 목록 개체에 포함시킬 수 없습니다.

a) 재배포 액세스를 나타내기 위해 작업 드롭다운 목록에서 허용 또는 차단 옵션을 선택합니다.

b) **Communities(**커뮤니티**)** 필드에서 커뮤니티 번호를 지정합니다. 유효한 값은 1~4294967295 또는 0:1부터 65534:65535입니다.

c) 적절한 경로 유형을 선택합니다.

- **Internet(**인터넷**)** - 잘 알려진 인터넷 커뮤니티를 지정하려면 선택합니다. 이 커뮤니티 경로는 모든 피어(내부 및 외부)에게 알려집니다.

- **No-advertise(**알림 없음**)** - 잘 알려진 커뮤니티의 알림을 하지 않는 경우 선택합니다. 이 커뮤니티 경로는 모든 피어(내부 또는 외부)에게 알려지지 않습니다.
- **No Export(**내보내지 않음**)** - 잘 알려진 커뮤니티를 내보내지 않는 경우 선택합니다. 이 커뮤니티 경로는 같은 자율 시스템 안에 있는 피어 또는 연합 내에 다른 하위 자율 시스템으로만 알려집니다. 이 경로는 외부 피어에 알려지지 않습니다.

단계 **6** 커뮤니티 규칙 유형을 표시하기 위해 **Expanded(**확장**)** 라디오 버튼을 선택합니다.

확장 커뮤니티 목록은 정규식을 사용하여 커뮤니티를 필터링합니다. 정규식은 커뮤니티 속성과 일치하는 패턴을 지정하는 데 사용됩니다.

a) 재배포 액세스를 나타내기 위해 작업 드롭다운 목록에서 허용 또는 차단 옵션을 선택합니다.

b) 식 필드에 정규식을 지정합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

정책 목록

정책 목록 설정 페이지를 사용해 정책 목록 정책 개체를 생성, 복사, 편집할 수 있습니다. 경로 맵을 구성할 때 정책 목록 개체를 생성할 수 있습니다. 경로 맵 내에서 정책 목록이 참조되는 경우 정책 목록의 모든 일치 문장이 평가 및 처리됩니다. 경로 맵 내에 둘 이상의 정책 목록을 구성할 수 있습니다. 정책 목록은 같은 경로 맵 내에 있으나 정책 목록 밖에서 구성된 기존 일치 항목 및 설정 명령문과도 공존할 수 있습니다. 여러 정책 목록이 하나의 경로 맵 항목 내에서 일치를 수행하는 경우 모든 정책 목록은 들어오는 특성에 대해서만 확인됩니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 정책 목록을 선택합니다.

단계 **2** **Add Policy List(**정책 목록 추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 정책 목록 개체의 이름을 입력합니다. 개체 이름은 대소문자를 구분하지 않습니다.

단계 **4** 작업 드롭다운 목록에서 조건 일치에 대해 액세스를 허용 또는 차단할지 여부를 선택합니다.

단계 **5** 인터페이스 탭을 클릭하여 다음 홉이 지정된 인터페이스 중 하나를 벗어난 경로를 배포합니다.

Zones/Interfaces(영역/인터페이스**)** 목록에서 디바이스가 관리 스테이션과 통신하는 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Zone/Interface(**선택한 영역/ 인터페이스**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 선택한 인터페이스 또는 영역이 디바이스에 포함되어 있는 경우에만 디바이스에서 호스트가 구성됩니다.

단계 **6** 주소 탭에서 표준 액세스 목록 또는 접두사 목록에서 허용한 대상 주소가 있는 모든 경로를 재배포합니다.

일치시키는 데 사용할 액세스 목록 또는 접두사 목록 중 하나를 선택하고 이때 사용할 표준 액세스 목록 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.

단계 **7** 다음 홉 탭을 클릭하여 지정된 액세스 목록 또는 접두사 목록이 전달한 다음 홉 라우터 주소가 있는 모든 경로를 재배포합니다.

일치시키는 데 사용할 액세스 목록 또는 접두사 목록 중 하나를 선택하고 이때 사용할 표준 액세스 목록 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.

단계 **8** 경로 소스 탭을 클릭하여 액세스 목록 또는 접두사 목록에서 지정된 주소의 라우터 및 액세스 서버가 알려준 경로를 재배포합니다.

일치시키는 데 사용할 액세스 목록 또는 접두사 목록 중 하나를 선택하고 이때 사용할 표준 액세스 목록 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.

단계 **9** BGP 자율 시스템 경로를 일치시키려면 **AS** 경로 탭을 클릭합니다. 하나 이상의 AS 경로를 지정하면 경로는 모든 AS 경로에 대해 일치시킬 수 있습니다.

단계 **10** 특정 커뮤니티와 BGP 커뮤니티 일치를 활성화하려면 커뮤니티 규칙 탭을 클릭합니다. 하나 이상의 커뮤니티를 지정하는 경우 경로가 아무 커뮤니티나 일치할 수 있습니다. 특정 커뮤니티와 BGP 커뮤니티를 정확하게 일치시키려면 **Match the specified community exactly(**지정된 커뮤니티 정확하게 일치**)** 확인란을 선택합니다.

단계 **11** 경로의 메트릭 및 보안 그룹 태그와 일치시키려면 메트릭 **&** 태그 탭을 클릭합니다.

a) 메트릭 필드에 일치에 사용할 메트릭 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 통해 지정된 메트릭이 있는 어떤 값과도 일치시킬 수 있습니다. 메트릭 값의 범위는 0~4294967295입니다.

b) 태그 필드에 일치에 사용할 태그 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 사용하면 특정 보안 그룹 태그가 있는 모든 경로를 일치시킬 수 있습니다. 태그 값의 범위는 0~4294967295입니다.

단계 **12** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 570 페이지의 내용을 참조하십시오.

단계 **13** **Save(**저장**)**를 클릭합니다.

VPN 개체

FTD 디바이스에서 다음 VPN 개체를 사용할 수 있습니다. 이러한 개체를 사용하려면 관리자 권한이 있어야 하며, 스마트 라이선스 계정이 내보내기 제어를 충족해야 합니다. 이러한 개체는 리프 도메인에서만 설정할 수 있습니다.

FTD IKE 정책

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다. IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKEv1의 경우, IKE 제안에는 단일 알고리즘 집합과 모듈러스 그룹이 포함됩니다. 적어도 하나 이상의 정책이 원격 피어의 정책과 일치하도록 우선 순위가 지정된 여러 정책을 생성할 수 있습니다. IKEv1과는 달리 IKEv2 제안의 경우, 한 그룹에서 여러 알고리즘과 모듈러스 그룹을 선택할 수 있습니다. 피어가 1단계 협상 중에 선택하기 때문에 단일 IKE 제안을 생성할 수 있도록 하지만 가장 원하는 옵션에 더 높은 우선 순위를 부여하는 여러 다른 제안을 고려하십시오. IKEv2의 경우 정책 개체가 인증을 지정하지 않으면 다른 정책이 인증 요건을 정의해야 합니다.

사이트 대 사이트 IPsec VPN을 구성할 때 IKE 정책이 필요합니다. 자세한 내용은 Firepower Threat Defense VPN, 1119 페이지를 참고하십시오.

IKEv1 정책 개체 구성

IKEv1 정책 페이지를 사용하여 IKEv1 정책 개체를 생성, 삭제, 편집합니다. 이러한 정책 개체는 IKEv1 정책에 필요한 파라미터를 포함합니다.

프로시저

단계 1 개체 > 개체 관리를 선택하고 목차에서 **VPN** > **IKEv1** 정책을 선택합니다.

이전에 구성된 정책이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 제안을 수정( )하거나 보거나(보기 ( )) 삭제( )할 수 있습니다.

단계 2 (선택 사항) 추가( )**Add IKEv1 Policy(IKEv1** 정책 추가**)**를 선택해 새 정책 개체를 만들 수 있습니다.

단계 3 이 정책의 이름을 입력합니다. 최대 128자를 입력할 수 있습니다.

단계 4 (선택 사항) 이 제안의 설명을 입력하십시오. 최대 1,024자를 입력할 수 있습니다.

단계 5 IKE 정책의 우선 순위 값을 입력합니다.

우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어가 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 유효한 값의 범위는 1~65535입니다. 번호가 낮을수록 우선 순위가 높습니다. 이 필드를 공백으로 두면 Management Center는 1, 5 순으로 5씩 증가시키며 할당되지 않은 가장 낮은 값을 할당합니다

단계 6 **Encryption(**암호화**)** 방법을 선택합니다.

IKEv1 정책에 사용할 암호화 및 해시 알고리즘을 정의할 때 피어 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스의 경우 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. IKEv1의 경우 다음 옵션 중 하나를 선택합니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정, 1125 페이지를 참조하십시오.

단계 **7** 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하는 해시 알고리즘을 선택합니다.

IKEv1 제안에 사용할 암호화 및 해시 알고리즘을 정의할 때 관리되는 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스의 경우 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. 옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정, 1126 페이지를 참조하십시오.

단계 **8** **Diffie-Hellman** 그룹을 설정합니다.

Diffie-Hellman 그룹은 암호화에 사용됩니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. VPN에서 허용하려면 그룹을 선택합니다. 옵션에 대한 자세한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 1127 페이지를 참조하십시오.

단계 **9** 보안 연결(SA)의 수명을 초 단위로 설정합니다. 120~2147483647초 사이의 값을 지정할 수 있습니다. 기본값은 86400입니다.

라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 (특정 지점까지는) 수명이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다.

단계 **10** 두 피어 간에 사용할 인증 방법을 선택합니다.

- 사전 공유 키 - 사전 공유 키를 사용하면 두 피어 간 보안 키를 공유할 수 있으며 인증 단계에서 IKE가 사용할 수 있습니다. 피어에 구성된 피어 중 하나가 동일한 사전 공유 키로 구성되지 않은 경우 IKE SA를 설정할 수 없습니다.
- 인증서 - VPN 연결 인증 방법으로 인증서를 사용하는 경우 피어는 인증을 위해 PKI 인프라의 CA 서버에서 디지털 인증서를 가져와 거래합니다.

참고 IKEv1을 지원하는 VPN 토폴로지에서는 선택한 IKEv1 정책 개체에서 지정된 **Authentication Method(**인증 방법**)**가 IKEv1 **Authentication Type(**인증 유형**)** 설정의 기본값이 됩니다. 이러한 값은 서로 일치해야 하며, 그렇지 않을 경우 컨피그레이션에 오류가 발생합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.
새 IKEv1 정책이 목록에 추가됩니다.

IKEv2 정책 개체 구성

IKEv2 정책 대화 상자를 사용하여 IKEv2 정책 개체를 생성, 삭제, 편집합니다. 이러한 정책 개체는 IKEv2 정책에 필요한 파라미터를 포함합니다.

프로시저

단계 1 개체 > 개체 관리를 선택하고 목차에서 **VPN** > **IKEv2** 정책을 선택합니다.

이전에 구성된 정책이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 정책을 수정( ), 보기 ( ), 삭제( )할 수 있습니다.

단계 2 추가( )**Add IKEv2 Policy(IKEv2** 정책 추가**)**를 선택해 새 정책을 생성합니다.

단계 3 이 정책의 이름을 입력합니다.

정책 개체의 이름입니다. 최대 128자를 입력할 수 있습니다.

단계 4 이 정책에 대한 설명을 입력합니다.

정책 개체의 설명입니다. 최대 1024자를 입력할 수 있습니다.

단계 5 우선 순위를 입력합니다.

IKE 제안의 우선 순위 값입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 제안의 순서가 결정됩니다. 원격 IPsec 피어가 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 유효한 값의 범위는 1 ~ 65535입니다. 번호가 낮을수록 우선 순위가 높습니다. 이 필드를 공백으로 두면 Management Center는 1, 5 순으로 5씩 증가시키며 할당되지 않은 가장 낮은 값을 할당합니다

단계 6 보안 연결(SA)의 수명을 초 단위로 설정합니다. 120~2147483647초 사이의 값을 지정할 수 있습니다. 기본값은 86400입니다.

라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 (특정 지점까지는) 수명이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다.

단계 7 IKE 정책에 사용되는 해시 알고리즘의 무결성 알고리즘 부분을 선택합니다. 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하는 해시 알고리즘을 선택합니다.

IKEv2 제안에 사용할 암호화 및 해시 알고리즘을 정의할 때 관리되는 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스를 위해 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. VPN에서 허용하려는 모든 알고리즘을 선택합니다.옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정, 1126 페이지를 참조하십시오.

단계 8 2단계 협상 보호를 위한 1단계 SA를 설정하는 데 사용되는 암호화 알고리즘을 선택합니다.

IKEv2 제안에 사용할 암호화 및 해시 알고리즘을 정의할 때 관리되는 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스를 위해 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. VPN에서 허용하려는 모든 알고리즘을 선택합니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정, 1125 페이지를 참조하십시오.

단계 9 **PRF** 알고리즘을 선택합니다.

IKE 정책에 사용되는 해시 알고리즘의 의사 난수 함수(PRF) 부분입니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습

니다. VPN에서 허용하려는 모든 알고리즘을 선택합니다. 옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정, 1126 페이지를 참조하십시오.

단계 **10** **DH** 그룹을 선택하고 추가합니다.

Diffie-Hellman 그룹은 암호화에 사용됩니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. VPN에서 허용할 그룹을 선택합니다. 옵션에 대한 자세한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 1127 페이지를 참조하십시오.

단계 **11** **Save(**저장**)**를 클릭합니다.
유효한 선택 조합이 선택된 경우 새 IKEv2 정책이 목록에 추가됩니다. 그렇지 않으면 오류가 표시되며 정책을 성공적으로 저장하기 위해 변경해야 합니다.

FTD IPSec 제안

IPsec 제안(또는 변형 집합)은 VPN 토폴로지를 구성할 때 사용됩니다. ISAKMP와의 IPsec 보안 연계 협상에서 피어는 특정 데이터 흐름을 보호하기 위해 특정 제안을 사용하는 데 동의합니다. 제안은 두 피어 모두에 동일해야 합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안(변형 집합)을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성합니다.
- IKEv2 IPsec 제안 개체를 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. IKEv2 협상 중에 피어는 서로 도움이 되는 가장 적절한 옵션을 선택합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

참고 IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

IKEv1 IPsec 제안 개체 설정

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **VPN** > **IPsec IKev1** 제안을 선택합니다.

이전에 구성된 제안이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 제안을 수정( )하거나 보거나(보기 ( )) 삭제( )할 수 있습니다.

단계 **2** 추가( )**Add IPsec IKEv1 Proposal(IPsec IKEv1** 제안 추가**)**를 선택하여 새 제안을 만들 수 있습니다.

단계 **3** 이 제안의 이름을 입력합니다.

정책 개체의 이름입니다. 최대 128자를 입력할 수 있습니다.

단계 **4** 이 제안의 설명을 입력하십시오.

정책 개체의 설명입니다. 최대 1024자를 입력할 수 있습니다.

단계 **5** **ESP** 암호화 방법을 선택합니다. 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다.

IKEv1의 경우 다음 옵션 중 하나를 선택합니다. IPsec 제안에 사용할 암호화 및 해시 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정, 1125 페이지를 참조하십시오.

단계 **6** **ESP** 해시에 대한 옵션을 선택합니다.

옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정, 1126 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.
새 제안이 목록에 추가됩니다.

IKEv2 IPsec 제안 개체 설정

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **VPN** > **IKev2 IPsec** 제안을 선택합니다.

이전에 구성된 제안이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 제안을 편집(수정( ))), 보기(보기 ( ))), 삭제(삭제( ))할 수 있습니다.

단계 **2** 추가( )**Add IPsec IKEv2 Proposal(IPsec IKEv2** 제안 추가**)**를 선택하여 새 제안을 만들 수 있습니다.

단계 **3** 이 제안의 이름을 입력합니다.

정책 개체의 이름입니다. 최대 128자를 입력할 수 있습니다.

단계 **4** 이 제안의 설명을 입력하십시오.

정책 개체의 설명입니다. 최대 1024자를 입력할 수 있습니다.

단계 **5** 인증에 대한 제안에 사용되는 해시 또는 무결성 알고리즘인 **ESP** 해시 방법을 선택합니다.

참고 FTD NULL 암호화를 사용하는 IPSec 터널을 지원하지 않습니다. IPSec IKEv2 제안에 대해 NULL 암호화를 선택하지 않아야 합니다.

IKEv2의 경우 **ESP** 해시를 지원하려는 모든 옵션을 선택합니다. 옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정, 1126 페이지를 참조하십시오.

단계 **6** **ESP** 암호화 방법을 선택합니다. 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다.

IKEv2의 경우 선택을 클릭하여 지원하려는 모든 옵션을 선택할 수 있는 대화 상자를 엽니다. IPsec 제안에 사용할 암호화 및 해시 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정, 1125 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.
새 제안이 목록에 추가됩니다.

FTD 그룹 정책 개체

그룹 정책은 원격 액세스 VPN 경험을 정의하는 그룹 정책 개체가 저장된 속성 및 값 쌍의 집합입니다. 예를 들어 그룹 정책 개체에서는 주소, 프로토콜, 연결 설정 등 일반 속성을 구성합니다.

VPN 터널이 설정된 경우 사용자에게 적용되는 그룹 정책이 결정됩니다. RADIUS 권한 서버는 그룹 정책을 할당하거나 현재 연결 프로파일에서 그룹 정책을 가져옵니다.

참고 FTD에 그룹 정책 속성 상속이 없습니다. 그룹 정책 개체 전체가 사용자에 대해 사용됩니다. 로그인 시 AAA 서버에서 식별된 그룹 정책 개체가 사용됩니다. 이를 지정하지 않은 경우, VPN 연결을 위해 구성된 기본 그룹 정책이 사용됩니다. 제공된 기본 그룹 정책은 기본값으로 설정할 수 있으나, 해당 정책이 연결 프로파일에 할당되어 있고 사용자의 다른 그룹 정책이 식별되지 않은 경우에만 사용됩니다.

그룹 개체를 사용하려면 Export Controlled Features(내보내기 제어 기능)가 있는 Smart License(스마트 라이선스) 계정과 연결된 이러한 AnyConnect 라이선스 중 하나를 활성화해야 합니다.

- AnyConnect VPN만
- AnyConnect Plus
- AnyConnect Apex

관련 항목
그룹 정책 개체 설정, 656 페이지

그룹 정책 개체 설정

FTD 그룹 정책 개체, 656 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**을 선택합니다.

이전에 구성된 정책이 시스템 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 편집, 보기 또는 그룹 정책 삭제를 할 수 있습니다.

단계 **2** **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다.

단계 **3** 이 정책의 이름을 입력하고 필요한 경우 설명을 입력합니다.

이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다. 설명은 최대 1,024자까지 입력할 수 있습니다.

단계 **4** 그룹 정책에 그룹 정책 일반 옵션, 657 페이지에 설명된 **General(**일반**)** 파라미터를 지정합니다.

단계 **5** 그룹 정책에 그룹 정책 AnyConnect 옵션, 659 페이지에 설명된 **AnyConnect(**모든 연결**)** 파라미터를 지정합니다.

단계 **6** 그룹 정책에 그룹 정책 고급 옵션, 662 페이지에 설명된 **Advanced(**고급**)** 파라미터를 지정합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.
새 그룹 정책이 목록에 추가됩니다.

다음에 수행할 작업

그룹 정책 개체를 원격 액세스 VPN 연결 프로파일에 추가합니다.

그룹 정책 일반 옵션

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**는 **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다.을 클릭하고 **General(**일반**)** 탭을 선택합니다.

VPN 프로토콜 필드

이 그룹 정책을 적용할 때 사용할 수 있는 원격 액세스 VPN 터널 유형을 지정합니다. **SSL** 또는 **IPsec IKEv2**

배너 필드

로그인 시 사용자에게 표시될 배너 텍스트를 지정합니다. 최대 491자까지 가능합니다. 기본값은 없습니다. IPsec VPN 클라이언트는 배너에 대해 전체 HTML을 지원하지만 AnyConnect 클라이언트는 부분 HTML만을 지원합니다. 원격 사용자에게 배너가 올바르게 표시되도록 하려면 IPsec 클라이언트에 /n 태그를 사용하고 SSL 클라이언트에는
 태그를 사용합니다.

DNS/WINS 필드

DNS(Domain Naming System) 및 WINS(Windows Internet Naming System) 서버입니다. AnyConnect 클라이언트 이름 전송에 사용합니다.

- 기본 **DNS** 서버 및 보조 **DNS** 서버 - 그룹에서 사용하려는 DNS 서버의 IPv4 또는 IPv6 주소를 정의하는 네트워크 개체를 선택 또는 생성합니다.

- 기본 **WINS** 서버 및 보조 **WINS** 서버 - 그룹에서 사용하려는 WINS 서버의 IP 주소를 포함하는 네트워크 개체를 선택 또는 생성합니다.
- **DHCP** 네트워크 범위 - 그룹에 대한 DHCP 네트워크의 IPv4 주소를 포함하는 네트워크 개체를 선택 또는 생성합니다. 이 설정은 IPv6, 주소 범위 또는 서브넷 사양을 지원하지 않습니다. 설정이 올바르지 않은 경우 VPN 정책 구축이 실패합니다.

  참고 DHCP 네트워크 범위는 라우팅 가능한 IP 주소여야 하며, DHCP 풀의 서브넷이 아니어야 합니다. DHCP 서버는 이 IP 주소가 속한 서브넷을 확인하고 해당 풀에서 IP 주소를 할당합니다. 어떤 IP 주소든 dhcp 네트워크 범위로 사용할 수 있지만 네트워크에 정적 경로를 추가해야 할 수 있습니다.

  LINK-SELECTION(RFC 3527) 및 SUBNET-SELECTION(RFC 3011)은 현재 지원되지 않습니다.

- 디폴트 도메인 - 기본 도메인의 이름입니다. 예를 들어 최상위 도메인으로 **example.com**을 지정합니다.

스플릿 터널링 필드

스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 "일반 텍스트 형식")로 보냅니다.

- **IPv4** 스플릿 터널링 / **IPv6** 스플릿 터널링 - 기본적으로 스플릿 터널링은 활성화되어 있지 않습니다. IPv4 및 IPv6 모두 터널을 통해 모든 트래픽을 허용하도록 설정됩니다. 그대로 둘 경우 엔드포인트의 모든 트래픽은 VPN 연결을 통해 이동합니다.

  스플릿 터널링을 구성하려면 아래에 지정된 터널 네트워크 또는 아래에 지정된 제외 네트워크 정책을 선택합니다. 그런 다음 해당 정책에 대해 액세스 제어 목록을 구성합니다.

- 스플릿 터널 네트워크 목록 유형 - 사용하는 액세스 목록의 유형을 선택합니다. 표준 액세스 목록 또는 확장 액세스 목록을 선택 또는 생성합니다. 자세한 내용은 액세스 목록, 644 페이지를 참조하십시오.
- **DNS** 요청 스플릿 터널링 - 스플릿 DNS라고도 합니다. 사용자 환경에서 예상 DNS 행동을 구성합니다.

  기본적으로 스플릿 DNS가 활성화되어 있지 않고 스플릿 터널 정책에 따라 **DNS** 요청 전송으로 설정됩니다. 항상 터널을 통해 **DNS** 요청 전송을 선택하면 모든 DNS 요청을 강제로 터널을 통해 프라이빗 네트워크에 전송합니다.

  스플릿 DNS를 구성하려면 지정된 도메인만 터널을 통해 전송을 선택하고 도메인 목록 필드에 도메인 이름 목록을 입력합니다. 이 요청은 스플릿 터널을 통해 프라이빗 네트워크로 전송됩니다. 다른 이름은 공용 DNS 서버를 통해 전송됩니다. 도메인 목록은 쉼표로 구분하여 최대 10개의 항목을 입력할 수 있습니다. 전체 문자열은 255자를 초과할 수 없습니다.

관련 항목

그룹 정책 개체 설정, 656 페이지

그룹 정책 AnyConnect 옵션

이러한 사양은 AnyConnect VPN 클라이언트의 작업에 적용됩니다.

탐색

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**. **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다. 이어 **AnyConnect** 탭을 선택합니다.

프로파일 필드

프로파일 - AnyConnect 클라이언트 프로파일를 포함하는 파일 개체를 선택 또는 생성합니다. 개체 생성에 대한 자세한 내용은 FTD 파일 개체, 663 페이지을 참조하십시오.

AnyConnect 클라이언트 프로파일은 하나의 XML 파일에 설정 파라미터가 저장된 그룹입니다. AnyConnect 소프트웨어 클라이언트는 클라이언트의 사용자 인터페이스에 표시되는 연결 항목을 구성하는 데 사용합니다. 이러한 파라미터(XML 태그)는 더 많은 AnyConnect 기능을 활성화하는 설정을 구성합니다.

독립 설정 도구인 GUI 기반의 AnyConnect 프로파일 편집기을 사용하여 AnyConnect 클라이언트 프로파일를 생성합니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client Administrator Guide의 해당 릴리스의 *AnyConnect* 프로파일 편집기장을 참조하십시오.

관리 프로파일 필드

관리 VPN 터널은 엔드 유저가 VPN에 연결하지 않는 경우라도 엔트포인트가 켜져 있을 때마다 기업 네트워크에 대한 연결을 제공합니다.

관리 **VPN** 프로파일 - 관리 프로파일에는 엔드포인트에서 관리 VPN 터널을 자동으로 활성화하고 설정하기 위한 설정이 포함되어 있습니다.

독립형 관리 VPN 터널 프로파일 편집기를 사용하여 새 프로파일 파일을 생성하거나 기존 파일을 수정할 수 있습니다. Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드할 수 있습니다.

프로파일 파일 추가에 대한 자세한 내용은 FTD 파일 개체, 663 페이지의 내용을 참조하십시오.

클라이언트 모듈 필드

Cisco AnyConnect VPN 클라이언트는 다양한 내장 모듈을 통해 향상된 보안을 제공합니다. 이러한 모듈은 웹 보안, 엔드 포인트 플로우에 대한 네트워크 가시성, 네트워크 외부 로밍 보호와 같은 서비스를 제공합니다. 각 클라이언트 모듈에는 요구 사항에 따라 사용자 지정 구성 그룹이 포함된 클라이언트 프로파일이 포함되어 있습니다.

다음 AnyConnect 모듈은 선택 사항이며, VPN 사용자가 AnyConnect를 다운로드할 때 이러한 모듈을 다운로드하도록 설정할 수 있습니다.

- **AMP Enabler** — 엔드포인트용 AMP(Advanced Malware Protection)를 구축합니다.
- **DART** - 문제 해결을 위해 Cisco TAC로 전송할 수 있는 시스템 로그 및 기타 진단 정보의 스냅샷을 캡처합니다.

- **ISE Posture** — OPSWAT v3 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다.
- **Network Access Manager** - 802.1X(계층 2)와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
- **Network Visibility(**네트워크 가시성**)** — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다.
- **Start Before Login(**로그인 전 시작**)** - Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그온하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.
- **Umbrella** 로밍 보안 — 활성 VPN이 없을 때 DNS 레이어 보안을 제공합니다.
- 웹 보안 - 정의된 보안 정책에 따라 웹 페이지의 요소를 분석하고 허용되는 콘텐츠를 허용하며 악성 또는 허용되지 않는 콘텐츠를 차단합니다.

Add(추가**)**를 클릭하고 각 클라이언트 모듈에 대해 다음을 선택합니다.

- 클라이언트 모듈 - 목록에서 AnyConnect 모듈을 선택합니다.
- 다운로드할 프로파일 - AnyConnect 클라이언트 프로파일를 포함하는 파일 개체를 선택 또는 생성합니다. 개체 생성에 대한 자세한 내용은 FTD 파일 개체, 663 페이지을 참조하십시오.
- **Enable module download(**모듈 다운로드 활성화**)** - 엔드포인트가 프로파일과 함께 클라이언트 모듈을 다운로드하도록 하려면 선택합니다. 선택하지 않으면 엔드포인트는 클라이언트 프로파일만 다운로드할 수 있습니다.

독립 컨피규레이션 도구인 GUI 기반의 AnyConnect 프로파일 편집기을 사용하여 각 모듈에 대한 클라이언트 프로파일을 생성합니다. Cisco 소프트웨어 다운로드 센터에서 AnyConnect 프로파일 편집기를 다운로드합니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client Administrator Guide의 해당 릴리스의 *AnyConnect* 프로파일 편집기장을 참조하십시오.

SSL 설정 필드

- **SSL** 압축 - 데이터 압축 활성화 여부를 선택하고, 활성화하는 경우 압축 해제 또는 LZS 중 사용할 데이터 압축 방법을 선택합니다. SSL 압축은 기본적으로 Disabled(비활성화) 상태입니다.

  데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 그렇게 보안 어플라이언스의 전체 처리량이 감소합니다.
- **DTLS** 압축 - LZS를 사용해 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.
- **MTU** 크기 - Cisco AnyConnect VPN 클라이언트에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit) 크기입니다. 기본값은 1406바이트이며 유효범위는 576~1462바이트입니다.
  - **DF** 비트 무시 - 단편화가 필요한 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. DF 비트가 설정된 패킷의 강제 조각화를 허용하여 터널을 통과할 수 있게 합니다.

연결 설정 필드

- **AnyConnect** 클라이언트와 **VPN** 게이트웨이 간에 연결 유지 메시지를 활성화합니다. 간격 설정 - 피어 간 연결 유지 메시지를 교환하여 터널에서 데이터 송수신이 가능한지 시연 여부를 선택합니다. 기본적으로 활성화되어 있습니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 활성화된 경우 IKE 연결 유지 패킷을 전송하고 원격 클라이언트가 대기하는 시간 간격(초 단위)을 입력합니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.
- 데드 피어 탐지 활성화**....** 간격 설정 - DPD(Dead Peer Detection)을 사용하면 VPN 보안 게이트웨이 또는 VPN 클라이언트는 피어가 응답하지 않으며 연결이 실패했음을 신속하게 감지합니다. 게이트웨이 및 클라이언트 모두에 기본적으로 활성화되어 있습니다. DPD 메시지는 설정된 간격에 따라 전송됩니다. 활성화된 경우 DPD 메시지를 전송하고 원격 클라이언트가 대기하는 시간 간격(초 단위)을 입력합니다. 기본 간격은 30초이며 유효 범위는 5~3600초입니다.
- 클라이언트 우회 프로토콜 활성화 - 이 옵션을 선택하면 보안 게이트웨이에서 (IPv6 트래픽만 예상할 때) IPv4 트래픽을 관리하는 방법 또는 (IPv4 트래픽만 예상할 때) IPv6 트래픽을 관리하는 방법을 구성할 수 있습니다.

  AnyConnect 클라이언트에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 “일반 텍스트” 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 컨피그레이션할 수 있습니다.

  예를 들어 보안 게이트웨이에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합시다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.
- **SSL** 키 재입력 - 클라이언트가 연결에 키를 재입력하여 암호화 키와 초기화 벡터를 재협상하고 연결 보안을 강화할 수 있습니다. 기본적으로 비활성화되어 있습니다. 활성화된 경우 지정된 간격으로 재협상이 발생하며 기존 터널에 키를 재입력하거나 다음 필드를 설정하여 새 터널을 생성합니다.
  - 방법 - SSL 키 재설정이 활성화되면 사용 가능합니다. 새 터널(기본값)을 생성하거나 기존 터널의 사양을 재협상합니다.
  - 간격 - SSL 키 재설정이 활성화되면 사용 가능합니다. 기본 범위는 4분이며 4-10080분(일주일) 범위 내에서 설정할 수 있습니다.
- 클라이언트 방화벽 규칙 - 클라이언트 방화벽 규칙을 사용하여 VPN 클라이언트 플랫폼에 대한 방화벽 설정을 구성합니다. 규칙은 소스 주소, 대상 주소 및 프로토콜 등의 기준을 기반으로 합니다. 확장 액세스 제어 목록 구성 요소 개체는 트래픽 필터 기준을 정의하는 데 사용됩니다. 이 그룹 정책에 대한 확장 ACL을 선택하거나 생성합니다. 프라이빗 네트워크의 데이터 플로우를 제어하는 프라이빗 네트워크 규칙과 설정된 VPN 터널 외부에 "있는 그대로" 데이터 플로우를 제어하는 공용 네트워크 규칙 또는 둘 다를 정의합니다.

참고 ACL이 TCP/UDP/ICMP/IP 포트를 포함하고 소스 네트워크가 any, any-ipv4 또는 any-ipv6을 포함하도록 확인합니다.

Microsoft Windows에서 실행되는 VPN 클라이언트만 이러한 방화벽 기능을 사용할 수 있습니다.

관련 항목

그룹 정책 개체 설정, 656 페이지

그룹 정책 고급 옵션

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**의 경우 **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다.을 클릭하고 고급 탭을 선택합니다.

트래픽 필터

- 액세스 목록 필터 - VPN 연결을 통해 수신되는 터널링된 데이터 패킷을 허용 또는 차단할지 여부를 결정하는 규칙으로 구성된 필터입니다. 규칙은 소스 주소, 대상 주소 및 프로토콜 등의 기준을 기반으로 합니다. 확장 액세스 제어 목록 구성 요소 개체는 트래픽 필터 기준을 정의하는 데 사용됩니다. 이 그룹 정책에 대한 새 확장 ACL을 선택하거나 생성합니다.
- **VPN**을 **VLAN**으로 제한 - "VLAN 매핑"이라고도 하는 이 파라미터는 이 그룹 정책이 적용되는 세션에 이그레스 VLAN 인터페이스를 지정합니다. ASA에서는 이 그룹의 모든 트래픽을 선택된 VLAN으로 전달합니다.

  이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 특성에 값을 할당하는 방법도 가능합니다. 기본값(Unrestricted(제한 없음)) 이외에는 이 ASA에 구성된 VLAN만 드롭다운 목록에 표시됩니다. 허용된 값의 범위는 1에서 4094까지입니다.

세션 설정 필드

- 액세스 시간 - 시간 범위 개체를 선택 또는 생성합니다. 이 개체는 이 그룹 정책이 원격 액세스 사용자에게 적용할 수 있는 시간 범위를 지정합니다. 자세한 내용은 시간 범위 개체, 578 페이지를 참조하십시오.
- 사용자당 동시 로그인 수 - 사용자에게 허용되는 최대 동시 로그인 수를 지정합니다. 기본값은 3입니다. 최소값은 0이며, 이 경우 로그인이 비활성화되고 사용자 액세스가 차단됩니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.
- 최대 연결 시간 / 알림 간격 - 최대 사용자 연결 시간을 분 단위로 설정합니다. 이 시간이 경과하면 시스템은 자동으로 연결을 종료합니다. 최소값은 1분입니다). 알림 간격은 최대 연결 시간에 도달하기 전 사용자에게 메시지를 표시하는 시간 간격입니다.

- 유휴 시간 제한 / 알림 간격 - 사용자의 유휴 시간 제한 기간을 분 단위로 지정합니다. 이 기간 동안 사용자 연결을 통한 통신 활동이 없는 경우 시스템은 연결을 종료합니다. 최소값은 1분입니다. 기본값은 30분입니다. 알림 간격은 유휴 시간 제한에 도달하기 전 사용자에게 메시지를 표시하는 시간 간격입니다.

관련 항목

그룹 정책 개체 설정, 656 페이지

FTD 파일 개체

파일 개체를 생성 및 편집하려면 파일 개체 추가 및 편집 대화 상자를 사용합니다. 파일 개체는 컨피그레이션(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect 클라이언트 프로파일, AnyConnect 클라이언트 이미지 파일을 포함할 수 있습니다.

프로파일은 또한 독립 프로파일 편집기를 사용하여 각 AnyConnect 모듈 및 AnyConnect Management VPN에 대해 생성되고 AnyConnect의 일부로 엔드포인트에서 관리자 정의 최종 사용자 요건 및 인증 정책에 구축되어 있으며 미리 설정된 네트워크 프로파일을 최종 사용자가 사용할 수 있게 설정되어 있습니다.

파일 개체를 생성하는 경우 Firepower Management Center은 저장소에서 파일의 복사본을 만듭니다. 이러한 파일은 데이터베이스 백업을 생성할 때마다 백업되고 데이터베이스를 복원하는 경우 복원됩니다. 파일 개체에 사용하기 위해 파일을 Firepower Management Center 플랫폼에 복사하는 경우, 파일 저장소를 파일 디렉토리에 복사하지 마십시오.

특정 파일 개체를 지정하는 설정을 구축하는 경우 관련 파일은 디바이스의 적절한 디렉터리에 다운로드됩니다.

각 파일에 대해 다음 옵션 중 하나를 클릭할 수 있습니다.

- **Download(**다운로드**)** - AnyConnect 파일을 다운로드하려면 클릭합니다.
- **Edit(**수정**)** - 파일 개체 세부 사항을 수정합니다.
- **Delete(**삭제**)** - AnyConnect 파일 개체를 삭제합니다. 파일 개체를 삭제하면 파일 저장소에서 관련 파일은 삭제되지 않고 개체만 삭제됩니다.

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File** > **Add AnyConnect File(AnyConnect** 파일 추가**)**.

필드

- **Name(**이름**)** - 파일 개체를 식별할 파일의 이름을 입력합니다. 최대 128자를 추가할 수 있습니다.
- **File Name(**파일 이름**)**—**Browse(**찾아보기**)**를 클릭하여 이미지 파일을 선택합니다. 파일을 선택하면 파일 이름과 파일의 전체 경로가 추가됩니다.
- **File Type(**파일 유형**)** - 선택한 파일에 해당하는 파일 유형을 선택합니다. 다음 파일 유형을 사용할 수 있습니다.

- **AnyConnect** 클라이언트 이미지 - Cisco Software Download Center에서 다운로드한 AnyConnect 클라이언트 이미지를 추가할 때 이 유형을 선택합니다.

  사용자는 새 AnyConnect 클라이언트 이미지 또는 추가 이미지를 VPN 정책에 연결할 수 있습니다. 또한 지원되지 않거나 단종되었으며 더 이상 필요하지 않은 클라이언트 패키지의 연결을 해제할 수 있습니다.

- **AnyConnect VPN** 프로파일 - AnyConnect VPN 프로파일 파일에 대해 이 유형을 선택합니다.

  프로파일 파일은 독립적인 설정 도구인 GUI 기반의 AnyConnect 프로파일 편집기를 사용하여 생성됩니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client Administrator Guide의 해당 릴리스의 *AnyConnect* 프로파일 편집기장을 참조하십시오.

- **AnyConnect** 관리 **VPN** 프로파일 - AnyConnect 관리 VPN 터널에 대한 프로파일 파일을 추가할 때 이 유형을 선택합니다.

  Cisco 소프트웨어 다운로드 센터에서 AnyConnect **VPN** 관리 터널 독립형 프로파일 편집기를 다운로드하지 않은 경우 다운로드하고 AnyConnect 관리 VPN 터널에 필요한 설정으로 프로파일을 생성합니다.

- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 이 프로파일과 함께 AMP Enabler가 FTD에서 엔드 포인트로 푸시됩니다.

- 피드백 프로파일 - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다.

- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다.

- **NAM** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다.

- 네트워크 가시성 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다.

- **Umbrella** 로밍 보안 프로파일 - 프로파일 편집기를 사용하여 생성한 .json 파일을 사용하여 Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다.

- 웹 보안 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다.

- 설명 - 필요한 설명을 추가합니다.

관련 항목

Cisco AnyConnect Secure Mobility Client 이미지, 1186 페이지
그룹 정책 AnyConnect 옵션, 659 페이지

FTD 인증서 맵 개체

인증서 맵 개체는 명명된 인증서 일치 규칙 집합입니다. 이런 개체는 수신된 인증서 및 원격 액세스 VPN 연결 프로파일 간 연결을 제공하는 데 사용됩니다. 연결 프로파일 및 인증서 맵 개체는 원격 액세스 VPN 정책의 일부입니다. 수신된 인증서가 인증서 맵에 포함된 규칙과 일치하는 경우 해당 연결은 "매핑되거나" 지정된 연결 프로파일에 연결됩니다. 규칙은 우선 순위에 따라 UI에 표시된 순서대로 적용됩니다. 인증서 맵 개체 내에서 첫 번째 규칙이 일치하는 경우 일치가 종료됩니다.

탐색

개체 > 개체 관리 > **VPN** > 인증서 맵

필드

- 이름 - 개체를 식별하여 원격 액세스 VPN 등 다른 설정에서 참조할 수 있도록 합니다.
- 매핑 기준-평가하기 위한 인증서의 내용을 지정합니다. 인증서가 이런 규칙을 만족시키는 경우 사용자는 이 개체를 포함하는 연결 프로파일에 매핑됩니다.
  - 구성 요소-일치시키는 규칙에 사용될 클라이언트 인증서의 구성 요소를 선택합니다.
  - 필드-클라이언트 인증서의 발급자 또는 제목에 따라 일치시키는 규칙에 대한 필드를 선택합니다.

    필드가 대체 제목 또는 확장 키 사용인 경우 구성 요소는 전체 필드여야 합니다.
  - 연산자-다음과 같은 일치 조건에 대한 연산자를 선택합니다.
    - 같음 - 인증서 구성 요소가 입력한 값과 일치해야 합니다. 정확하게 일치하지 않으면 연결이 거부됩니다.
    - 포함 - 인증서 구성 요소가 입력한 값을 포함해야 합니다. 구성 요소에 해당 값이 포함되지 않으면 연결이 거부됩니다.
    - 같지 않음 - 인증서 구성 요소가 입력한 값과 일치하면 안 됩니다. 예를 들어 인증서 요소 중 국가를 선택하고 입력한 값이 US인 경우, 클라이언트 국가 값이 US와 같다면 해당 연결이 거부됩니다.
    - 포함되어 있지 않음 - 인증서 구성 요소가 입력한 값을 포함하면 안 됩니다. 예를 들어 인증서 요소 중 국가를 선택하고 입력한 값이 US인 경우, 클라이언트 국가 값에 US를 포함하면 해당 연결이 거부됩니다.
- 값-일치 규칙의 값입니다. 입력한 값은 선택된 구성 요소 및 연산자와 연결됩니다.

관련 항목

인증서 맵 구성, 1189 페이지

주소 풀

클러스터링 또는 VPN 원격 액세스 프로파일을 사용해 진단 인터페이스로 사용할 수 있는 IPv4 및 IPv6에 대한 IP 주소 풀을 설정할 수 있습니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리 > 주소 풀 > **IPv4** 풀을 선택합니다.

단계 **2** **IPv4** 풀 추가를 클릭하고 다음 필드를 구성합니다.

- 이름 - 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
- 설명 - 필요한 경우 이 풀에 대한 설명을 추가합니다.
- **IP** 주소 - 풀에서 사용할 수 있는 주소 범위를 입력합니다. 예를 들어 10.10.147.100-10.10.147.177처럼 점으로 구분된 10진수 및 주소 앞뒤 및 사이에 대시를 사용합니다.
- 마스크 - 이 IP 주소 풀이 있는 서브넷을 식별합니다.
- 오버라이드 허용 - 개체 오버라이드를 활성화하려면 이 확인란을 선택합니다. 오버라이드 테이블을 표시하려면 확장 화살표를 클릭합니다. **Add(**추가**)**를 클릭하여 새 오버라이드를 추가할 수 있습니다. 자세한 내용은 개체 재정의, 568 페이지를 참조하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.

단계 **4** **IPv6** 풀 추가를 클릭하고 다음 필드를 구성합니다.

- 이름 - 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
- 설명 - 필요한 경우 이 풀에 대한 설명을 추가합니다.
- **IPv6** 주소 - 구성된 풀에서 사용한 첫 번째 IP 주소 및 접두어 길이를 비트로 입력합니다. 예를 들면 2001:DB8::1 / 64와 같습니다.
- 주소 수 - 시작 IP 주소에서 시작하여 풀에 있는 IPv6 주소 수를 식별합니다.
- 오버라이드 허용 - 개체 오버라이드를 활성화하려면 이 확인란을 선택합니다. 오버라이드 테이블을 표시하려면 확장 화살표를 클릭합니다. **Add(**추가**)**를 클릭하여 새 오버라이드를 추가할 수 있습니다. 자세한 내용은 개체 재정의, 568 페이지를 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

FlexConfig 개체

FTD 디바이스에서 사용할 수 없는 사용자 정의 설정 기능을 제공하려면 FlexConfig 정책에서 FlexConfig 정책 개체를 사용하거나 Firepower Management Center를 사용해 구성합니다. FlexConfig 정책에 대한 자세한 내용은 FlexConfig 정책 개요, 1269 페이지을 참조하십시오.

FlexConfig에 대한 다음과 같은 유형의 개체를 구성할 수 있습니다.

텍스트 개체

텍스트 개체는 FlexConfig 개체에서 변수로 사용하는 자유 형식의 텍스트 문자열을 정의합니다. 이러한 개체는 단일 값을 가질 수도 있고 여러 값의 목록일 수도 있습니다.

사전 정의된 FlexConfig 개체에서 사용되는 몇 가지 사전 정의된 텍스트 개체가 있습니다. 연결된 FlexConfig 개체를 사용하는 경우에 해당 디바이스에 FlexConfig 개체를 구성하는 방법을 사용자 정의하려면 텍스트 개체의 내용을 편집하면 됩니다. 사전 정의된 개체를 편집할 때 일반적으로 해당 개체의 기본값을 직접 변경하는 것보다 구성하는 각 디바이스에 디바이스 오버라이드를 생성하는 것이 더 낫습니다. 이렇게 하면 다른 사용자가 디바이스의 다른 집합에 동일한 FlexConfig 개체를 사용하려는 경우 예기치 않은 결과가 발생하는 것을 방지합니다.

텍스트 개체를 구성하는 방법에 대해서는 FlexConfig 텍스트 개체 설정, 1298 페이지을 참조하십시오.

FlexConfig 개체

FlexConfig 개체는 디바이스 설정 명령, 변수 및 스크립팅 언어 지침을 포함합니다. 설정을 구축하는 동안 대상 디바이스에 대해 특정 기능을 구성하기 위해 사용자 정의된 파라미터를 포함한 일련의 설정 명령어를 생성하기 위해 지침이 처리됩니다.

이러한 지침은 일반 Firepower Management Center 정책 및 설정에서 시스템 구성 기능이 정의되기 전(앞)에 구성되거나 후(뒤)에 구성됩니다. Firepower Management Center에 의존하는 모든 FlexConfig - 구성 구축에 구성된 개체(네트워크 개체 등)를 추가하지 않으면 FlexConfig가 개체 참조에 사용하기 전에 필요한 개체가 구성되지 않습니다.

FlexConfig 개체를 구성하는 방법에 대해서는 FlexConfig 개체 구성, 1293 페이지을 참조하십시오.

RADIUS 서버 그룹

RADIUS 서버 그룹 개체는 RADIUS 서버에 대한 하나 이상의 참조를 포함합니다. 이러한 서버는 원격 액세스 VPN 연결을 통해 로그인하는 사용자를 인증하는 데 사용됩니다.

이 개체는 FTD 디바이스와 함께 사용할 수 있습니다.

시작하기 전에

참고 RADIUS 서버 그룹 개체는 오버라이드할 수 없습니다.

프로시저

단계 **1** **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **RADIUS Server Group(RADIUS** 서버 그룹**)**을 선택합니다.

현재 구성된 모든 RADIUS 서버 그룹 개체가 나열됩니다. 필터를 사용하여 목록을 축소합니다.

단계 **2** 나열된 RADIUS 서버 그룹 개체를 선택하고 편집하거나 새로 추가합니다.

이 개체를 구성할 땐 RADIUS 서버 옵션, 669 페이지과 RADIUS 서버 그룹 옵션, 668 페이지를 참조하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.

RADIUS 서버 그룹 옵션

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **RADIUS Server Group(RADIUS** 서버 그룹**)**. 구성된 RADIUS 서버 그룹 개체를 선택하고 편집하거나 새로 추가합니다.

필드

- 이름 및 설명 - 이름을 입력하고 필요에 따라 RADIUS 서버 그룹 개체를 식별할 설명을 입력합니다.
- 그룹 계정 모드 - 그룹의 RADIUS 서버에 어카운팅 메시지를 전송하는 방법입니다. 단일을 선택하면 어카운팅 메시지가 그룹의 단일 서버에 전송됩니다. 기본 설정입니다. 동시를 선택하면 그룹 내 모든 서버에 동시에 어카운팅 메시지가 전송됩니다.
- 재시도 간격 - RADIUS 서버에 연결을 시도하는 간격입니다. 값의 범위는 1~10초입니다.
- 영역(선택 사항) - 이 RADIUS 서버 그룹이 연결될 Active Directory(AD) 영역을 지정 또는 선택합니다. 영역은 트래픽 플로우에 대한 VPN 인증 ID 소스를 결정하는 경우 연결된 RADIUS 서버 그룹에 액세스하기 위해 ID 정책에서 선택됩니다. 이 영역은 ID 정책에서 RADIUS 서버 그룹을 연결하는 브리지를 효과적으로 제공합니다. RADIUS 서버 그룹에 어떤 영역도 연결되지 않은 경우, ID 정책의 트래픽 플로우에 대한 VPN 인증 ID 소스를 결정할 때 RADIUS 서버 그룹을 연결할 수 없습니다.
- 권한 부여 전용 모드 활성화 - 이 RADIUS 서버 그룹이 인증에 사용되지 않지만 권한 부여 또는 계정 관리에 사용되는 경우 이 필드를 활성화하여 RADIUS 서버 그룹에 권한 부여 전용 모드를 활성화합니다.

  권한 부여 전용 모드는 Access-Request에서 RADIUS 서버 비밀번호를 포함해야 할 필요가 없습니다. 따라서 개별 RADIUS 서버에 대해 구성된 비밀번호는 무시됩니다.

- 중간 계정 업데이트 활성화 및 간격 - 새로 할당된 IP 주소의 RADIUS 서버를 알려주기 위해 RADIUS 중간 계정 관리 업데이트 메시지를 생성할 수 있습니다. 간격 필드의 주기적인 계정 관리 업데이트 간 시간 간격을 시간 단위로 설정합니다. 유효한 범위는 1에서 120이며 기본값은 24입니다.
- 동적 권한 부여 활성화 및 포트 - RADIUS 서버 그룹에 대한 RADIUS 동적 권한 부여 또는 CoA(Change of Authorization) 서비스를 활성화합니다. 포트 필드에서 RADIUS CoA 요청에 대한 수신 대기 포트를 지정합니다. 기본값은 1700이고, 범위는 1024~65535입니다. 일단 정의되면 해당 RADIUS 서버 그룹이 CoA 알림에 등록되고 ISE(Cisco Identity Services Engine)에서 보내는 CoA 정책 업데이트를 포트에서 수신합니다.
- **RADIUS** 서버 - RADIUS 서버 옵션, 669 페이지를 참조합니다.

관련 항목

RADIUS 서버 그룹, 667 페이지

RADIUS 서버 옵션

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **RADIUS Server Group(RADIUS** 서버 그룹**)**. 나열된 RADIUS 서버 그룹 개체를 선택하고 편집하거나 새로 추가합니다. 이후 RADIUS 서버 그룹 대화 상자에서 나열된 RADIUS 서버를 선택하고 수정하거나 새로 추가합니다.

필드

- **IP** 주소/호스트 이름 - 인증 요청이 전송되는 RADIUS 서버의 호스트 이름 또는 IP 주소를 식별하는 네트워크 개체입니다. RADIUS 서버 그룹 목록에 추가 RADIUS 서버 또는 추가 서버를 추가하려면 하나만 선택할 수 있습니다.

  참고 Firepower Threat Defense 이제 RADIUS 인증에 IPv6 IP 주소를 지원합니다.

- **Authentication Port(**인증 포트**)** - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- 키 및 키 확인 - 매니지드 디바이스(클라이언트) 및 RADIUS 서버 간 데이터를 암호화하는 데 사용되는 공유 암호입니다.

  키는 대소문자를 구분하며 최대 127자의 영숫자입니다. 특수 문자가 허용됩니다.

  이 필드에 정의된 키는 RADIUS 서버 키와 일치해야 합니다. 확인 필드에 키를 다시 입력합니다.
- 어카운팅 포트 - RADIUS 어카운팅을 수행하는 포트입니다. 기본값은 1,813입니다.
- 시간 초과 - 인증에 대한 세션 시간 초과입니다.

참고 RADIUS의 두 인증 요소에 대한 시간 초과 값은 60초 이상이어야 합니다. 기본 시간 제한 값은 10초입니다.

- 연결 사용 - 경로 조회 또는 특정 이터페이스를 사용해 Firepower Threat Defense에서 RADIUS 서버로의 연결성을 설정합니다. 라우팅 테이블을 사용하려면 라우팅을 선택합니다. 또는 특정 인터페이스를 선택하고 보안 영역/인터페이스 그룹 또는 진단 인터페이스(기본값)를 선택합니다.
- 재전송 **ACL** - 목록에서 재전송 ACL을 선택하거나 새 ACL을 추가합니다.

참고 재전송될 트래픽을 결정하는 Firepower Threat Defense에서 정의된 ACL의 이름입니다. 이 재전송 ACL 이름은 ISE 서버의 재전송 *ACL*과 동일해야 합니다. ACL 개체를 구성하는 경우 ISE 및 DNS 서버에 차단 작업을 선택하거나 나머지 서버에 허용 작업을 선택합니다.

관련 항목

RADIUS 서버 그룹, 667 페이지
RADIUS 서버 그룹 옵션, 668 페이지

SSO(Single Sign-On) 서버 추가

시작하기 전에

SAML ID 공급자에서 다음 정보를 가져옵니다.

- ID 제공자 엔티티 ID URL
- 로그인 URL
- 로그아웃 URL
- ID 제공자 인증서 및 FMC 웹 인터페이스를 사용하여 FTD에 인증서 등록(**Devices (**디바이스**)** > **Certificates (**인증서**)**)

자세한 내용은 SAML SSO(Single Sign-On) 인증 구성, 1207 페이지를 참고하십시오.

프로시저

단계 **1** **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **Single Sign-on Server(SSO(Single Sign-On)** 서버**)**를 선택합니다.

단계 **2** **Add Single Sign-on Server(SSO(Single Sign-On)** 서버 추가**)**를 클릭하고 다음 세부 정보를 제공합니다.

- **Name(**이름**)** - SAML SSO 서버 개체의 이름입니다.
- **Identity Provider Entity ID(ID** 공급자 엔터티 **ID)** - 서비스 공급자를 고유하게 식별하기 위해 SAML IdP에 정의된 URL입니다.

  SAML 발급자가 요청에 응답하는 방법을 설명하는 메타데이터 XML을 제공하는 페이지의 URL입니다.
- **Sign In URL(**로그인 **URL)** — ID 공급자 서버에 로그인하기 위한 URL입니다.
- **Sign Out URL(**로그아웃 **URL)** - ID 공급자 서버에서 로그아웃하기 위한 URL입니다.
- **Base URL(**기본 **URL)** - ID 공급자 인증이 완료되면 사용자를 FTD로 다시 리디렉션하는 URL입니다. FTD 원격 액세스 VPN용으로 설정된 액세스 인터페이스의 URL입니다.
- **Identity Provider Certificate(ID** 공급자 인증서**)** - IdP에서 서명한 메시지를 확인하기 위해 FTD에 등록된 IdP의 인증서입니다.
- **Service Provider Certificate(**서비스 공급자 인증서**)** - 요청에 서명하고 IdP와의 신뢰 관계를 구축하는 데 사용되는 FTD 인증서입니다.

  내부 FTD 인증서를 등록하지 않은 경우 +를 클릭하여 인증서를 추가하고 등록합니다. 자세한 내용은 FTDVPN 인증서 매핑, 677 페이지를 참고하십시오.
- **Request Signature(**요청 서명**)** - SAML SSO(Single Sign-On) 요청에 서명할 암호화 알고리즘을 선택합니다.

  서명은 SHA1, SHA256, SHA384, SHA512와 같이 가장 약한 항목부터 가장 강력한 항목까지 나열됩니다. 암호화를 비활성화하려면 None(없음)을 선택합니다.
- **Request Timeout(**요청 시간 초과**)** - 사용자가 단일 SSO 요청을 완료하는 데 사용할 SAML 어설션 유효 기간을 지정합니다. SAML IdP에는 *NotBefore* 및 *NotOnOrAfter*의 두 가지 시간 초과가 있습니다. 시간 초과를 IdP의 *NotOnOrAfter* 시간 초과보다 길게 설정하면 지정된 시간 초과가 무시되고 *NotOnOrAfter* 시간 초과가 선택됩니다. 지정된 시간 초과와 *NotBefore* 시간 초과의 합계가 *NotOnOrAfter* 시간보다 작으면 FTD 시간 초과가 시간 초과를 재정의합니다.

  시간 초과 범위는 1-7200초이며, 기본 시간 초과는 300초입니다.
- **Enable IdP only accessible on Internal Network(**내부 네트워크에서만 액세스 가능한 **IdP** 활성화**)** - SAML IdP가 내부 네트워크에 있는 경우 이 옵션을 선택합니다. FTD는 게이트웨이 역할을 하며 익명 webvpn 세션을 사용하여 사용자와 IdP 간의 통신을 설정합니다.
- **Request IdP re-authentication on Login(**로그인 시 **IdP** 재인증 요청**)** - 이전 IdP 세션이 유효한 경우에도 각 로그인 시 사용자를 인증하려면 이 옵션을 선택합니다.
- **Allow Overrides(**재정의 허용**)** - 이 SSO 서버 개체에 대한 재정의를 허용하려면 이 체크 박스를 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

관련 항목

Remote Access VPN에 대한 AAA 설정, 1177 페이지

재사용 가능 개체 히스토리

기능	버전	세부 사항
보안 인텔리전스 피드 옵션	6.7	사용자 지정 보안 인텔리전스 피드에 대한 새로운 업데이트 빈도 옵션(5분 및 15분) 업데이트 빈도가 30분 미만이면 피드가 변경되지 않은 경우, 불필요한 다운로드를 방지하기 위해 MD5 URL이 필요합니다. 신규/수정된 화면: **Security Intelligence(**보안 인텔리전스**) > Network Lists and Feeds(**네트워크 목록 및 피드**)**를 설정할 때 새로운 빈도 선택 지원되는 플랫폼: Firepower Management Center
쉼표로 구분 된 값(csv) 파일을 사용하는 개체의 벌크 업로드	6.7	쉼표로 구분된 값 파일에서 개체를 가져올 수 있습니다. 한 번에 최대 1,000개의 개체를 가져올 수 있습니다. 신규/수정된 화면: 다음 개체 유형의 **Add [Object Type]([**개체 유형**]** 추가**)** 드롭다운 목록에 새로운 **Import Object(**개체 가져오기**)** 옵션이 있습니다. • **Distinguished Name(**고유 이름**) > Individual Objects(**개별 개체**)** • 네트워크 개체 • **Port(**포트**)** • **URL** • **VLAN Tag** 지원되는 플랫폼: Firepower Management Center

기능	버전	세부 사항
인터페이스 개체가 사용되는 정책 확인	6.6	인터페이스 개체가 사용되는 정책을 확인합니다. 신규/수정된 화면: **Objects(**개체**) > Object Management(**개체 관리**)**의 **Interface(**인터페이스**)** 개체 페이지에 새 사용량 찾기( ) 버튼이 있습니다. 지원되는 플랫폼: Firepower Management Center
표준 시간대 개체 도입	6.6	FTD 디바이스에 시간대를 할당하여 시간 기반 정책을 적용할 수 있습니다. 신규/수정된 화면: **Objects(**개체**) > Object Management(**개체 관리**)**의 새 표준 시간대 개체 지원되는 플랫폼: Firepower Management Center
이제 시간 기반 개체를 액세스 제어 및 사전 필터 정책에서 사용할 수 있습니다.	6.6	액세스 제어 및 사전 필터 정책에서 시간 기반 규칙을 적용하려면 시간 범위 개체를 새 표준 시간대 개체와 함께 사용하십시오. 적용할 규칙에 대해 절대적이거나 반복되는 시간 또는 시간 범위를 지정할 수 있습니다. 규칙은 트래픽을 처리하는 디바이스의 표준 시간대에 따라 적용됩니다.
사전 필터 규칙 페이지의 개체 세부 사항 보기	6.6	도입된 기능: 사전 필터 규칙을 확인할 때 개체 또는 개체 그룹의 세부 사항을 볼 수 있는 옵션입니다. 신규 옵션: 사전 필터 규칙의 다음 열 중 하나에 있는 값을 클릭하면 소스 네트워크, 대상 네트워크, 소스 포트, 대상 포트, VLAN 태그 등 개체 세부 사항을 볼 수 있는 옵션이 제공됩니다. 지원되는 플랫폼: Firepower Management Center

23 장

Firepower Threat Defense 인증서 기반 인증

- FTD 인증서 기반 인증 요구 사항 및 사전 요건, 675 페이지
- Firepower Threat Defense VPN 인증서 가이드라인 및 제한 사항, 676 페이지
- FTDVPN 인증서 매핑, 677 페이지
- 자체 서명 등록을 사용한 인증서 설치 , 678 페이지
- SCEP 등록을 사용한 인증서 설치, 679 페이지
- 수동 등록을 사용한 인증서 설치, 680 페이지
- PKCS12 파일을 가져오는 방법으로 인증서 설치, 681 페이지
- FTD VPN 인증서 문제 해결, 681 페이지
- Firepower Threat Defense 인증서 기반 인증 히스토리, 682 페이지

FTD 인증서 기반 인증 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

Network Admin(네트워크 관리자)

Firepower Threat Defense VPN 인증서 가이드라인 및 제한 사항

- 인증서 등록 개체이 연결된 후 디바이스에 설치되면 인증서 등록 프로세스가 즉시 시작됩니다. 이 프로세스는 자체 서명 및 SCEP 등록 유형의 경우 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록 및 PKCS12 파일 가져오기의 경우 관리자의 추가 작업이 필요합니다.
- 인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.
- FTD 사용자 인터페이스에 선택 사항이 표시되지만 현재는 ECDSA가 아닌 RSA 키만 지원합니다.
- FTD VPN이 클러스터링된 환경에서 지원되지 않으므로 PKI도 클러스터링 환경에서 지원되지 않습니다.
- FTD 디바이스는 Microsoft CA 서비스, Cisco Adaptive Security Appliance 및 Cisco IOS Router에서 제공하는 CA 서비스를 사용한 인증서 등록을 지원합니다.
- FTD 디바이스는 CA(Certificate Authority)로 구성할 수 없습니다.

인증서 관리 도메인 및 디바이스에 대한 지침

- Firepower Threat Defense 디바이스는 Microsoft CA 서비스, Cisco Adaptive Security Appliance 및 Cisco IOS Router에서 제공하는 CA 서비스를 지원하고 이들을 사용해 인증합니다.
- 인증서 등록은 하위 또는 상위 도메인에서 수행할 수 있습니다.
- 상위 도메인에서 등록이 완료되면 동일한 도메인에 인증서 등록 개체가 포함되어야 합니다. 디바이스의 트러스트 포인트가 하위 도메인에 오버라이드된 경우, 오버라이드된 값이 디바이스에 구축됩니다.
- 리프 도메인의 디바이스에 인증서 등록이 완료되면 상위 도메인 및 다른 하위 도메인에서는 보이지 않습니다.
- 리프 도메인을 삭제하면 포함된 디바이스의 인증서 등록을 제거할 필요가 없습니다.
- 디바이스에 한 도메인의 인증서가 등록되면 다른 도메인에는 등록이 허용되지 않습니다. 하지만 다른 도메인에서 인증서를 볼 수 있습니다.
- 디바이스가 한 도메인에서 다른 도메인으로 이동하는 경우, 또는 도메인이 아닌 곳에서 도메인으로 이동하는 경우 해당 디바이스의 인증서 등록을 제거하고 새 도메인에 재구성되어야 합니다. 디바이스에서 등록을 제거하면 알림을 받게 됩니다.

FTDVPN 인증서 매핑

디지털 인증서의 소개는 PKI 인프라 및 디지털 인증서을 참조하십시오.

관리되는 디바이스에서 인증서를 가져오고 등록하는 데 사용되는 개체에 대한 설명은 인증서 등록 개체, 628 페이지을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Certificates(**인증서**)**을(를) 선택합니다.

이 화면에 나열된 각 디바이스에 대해 다음 열을 볼 수 있습니다.

- **Name(**이름**)** - 이미 관련된 트러스트 포인트가 있는 디바이스를 나열합니다. 연결된 트러스트 포인트 목록을 보려면 디바이스를 확장합니다.
- **Enrollment Type(**등록 유형**)** - 트러스트 포인트에 사용된 등록 유형을 표시합니다.
- **Status(**상태**)** - **CA** 인증서 및 **ID** 인증서의 상태를 제공합니다. 인증서 내용이 사용 가능일 때 돋보기를 클릭하여 볼 수 있습니다.

  CA 인증서 정보를 볼 때 CA 인증서를 발급한 모든 인증 기관의 계층 구조를 볼 수 있습니다.

  등록이 실패한 경우 오류 메시지를 보려면 상태를 클릭합니다.
- 추가 열은 **CA** 인증서 및 **ID** 인증서의 상태를 제공합니다. 인증서 내용의 각 열이 사용 가능일 때 돋보기를 클릭하여 볼 수 있습니다.

  이 열의 값은 등록 유형에 따라 다르며 등록 프로세스 동안 변경됩니다. CA 인증서는 사용 가능, 사용 불가, 해당 없음 상태가 될 수 있습니다. ID 인증서는 새로 고침 동안 사용 가능, 보류, 사용 가능 및 보류 상태가 될 수 있습니다.
- 추가 열에는 다음 작업을 수행하는 아이콘이 나열됩니다.
  - **Export Certificate(**인증서 내보내기**)** - 인증서의 복사본을 내보내고 다운로드하려면 클릭합니다. PKCS12(전체 인증서 체인) 또는 PEM(ID 인증서 전용) 형식을 내보내도록 선택할 수 있습니다.

    나중에 파일을 가져오려면 PKCS12 인증서 형식을 내보내려면 암호를 제공해야 합니다.
  - **Re-enroll certificate(**인증서 다시 등록**)** - 기존 인증서를 다시 등록합니다.
  - **Refresh certificate status(**인증서 상태 새로 고침**)** - 인증서를 새로 고쳐 Firepower Threat Defense 디바이스 인증서 상태를 Firepower Management Center와 동기화합니다.
  - **Delete certificate(**인증서 삭제**)** - 트러스트 포인트에 대한 모든 연결된 인증서를 삭제합니다.

단계 **2** **(+)** 선택 > 새 인증서 추가를 선택하여 디바이스에 등록 개체를 연결하고 설치합니다. 등록 유형에 따릅니다.

참고 인증서 등록 개체이 연결된 후 디바이스에 설치되면 인증서 등록 프로세스가 즉시 시작됩니다. 이 프로세스는 자체 서명 및 SCEP 등록 유형의 경우 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록 및 PKCS12 파일 가져오기의 경우 관리자의 추가 작업이 필요합니다.

관련 항목

자체 서명 등록을 사용한 인증서 설치 , 678 페이지
SCEP 등록을 사용한 인증서 설치, 679 페이지
수동 등록을 사용한 인증서 설치, 680 페이지
PKCS12 파일을 가져오는 방법으로 인증서 설치, 681 페이지

자체 서명 등록을 사용한 인증서 설치

프로시저

단계 **1** **Devices(**디바이스**) > Certificates(**인증서**)** 화면에서 **Add(**추가**) > Add New Certificate(**새 인증서 추가**)**를 선택하고 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 엽니다.

단계 **2** 드롭다운 목록에서 **Device(**디바이스**)**를 엽니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 개체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 적절한 유형의 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가, 630 페이지을 참조하십시오.

단계 **4** 설치를 누르면 자체 서명된 자동 등록 프로세스가 시작됩니다.

자체 서명된 등록 유형의 트러스트 포인트의 경우 관리되는 디바이스가 자체 CA로 작동하여 자체 ID를 생성하는 CA 인증서가 필요하지 않으므로 **CA** 인증서 상태는 항상 `NotApplicable` 상태입니다.

디바이스가 자체 서명된 ID 인증서를 생성하면 **ID** 인증서는 InProgress에서 Available 상태로 변경됩니다.

단계 **5** 이 장치에 대해 생성된 자체 서명된 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.

SCEP 등록을 사용한 인증서 설치

시작하기 전에

참고 SCEP 등록을 사용할 경우 매니지드 디바이스와 CA 서버 간에 직접 연결이 설정됩니다. 등록 프로세스를 시작하기 전에 디바이스가 CA 서버에 연결되었는지 확인하십시오.

프로시저

단계 **1** 설치를 누르면 자동 등록 프로세스가 시작됩니다.

단계 **2** **Devices(**디바이스**) > Certificates(**인증서**)** 화면에서 **Add(**추가**) > Add New Certificate(**새 인증서 추가**)**를 선택하고 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 엽니다.

단계 **3** 드롭다운 목록에서 **Device(**디바이스**)**를 엽니다.

단계 **4** 다음 방법 중 하나로 인증서 등록 개체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 적절한 유형의 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가, 630 페이지을 참조하십시오.

단계 **5** 설치를 누르면 자동 등록 프로세스가 시작됩니다.

SCEP 등록 유형 트러스트 포인트의 경우 CA 서버에서 CA 인증서를 가져와 디바이스에 설치하므로 **CA** 인증서 상태가 InProgress에서 Available로 전환됩니다.

ID 인증서는 디바이스가 특정 CA에서 SCEP를 사용해 ID 인증서를 가져오므로 `InProgress`에서 `Available` 상태로 변경됩니다.

참고 몇 가지 오류 메시지 때문에 SCEP 인증서 등록이 실패할 수 있습니다. 예를 들면 다음과 같습니다.

```
Error:
crypto ca authenticate scep1 nointeractive:[error]:ERROR:receiving Certificate
Authority certificate: status = FAIL, cert length = 0
Possible
```

이런 상황을 해결하기 위한 몇 가지 권장 사항입니다.

- FTD에서 SCEP 서버의 연결성을 확인하십시오 - SCEP 서버에 경로가 추가됩니다.
- SCEP 서버가 hostname/FQDN을 참조하면 FlexConfig 개체를 사용해 DNS 서버를 구성합니다.
- SCEP 서버와 FTD 디바이스가 동일한 NTP 서버 구성으로 실시간으로 동기화되도록 합니다.

단계 **6** 이 장치에 생성되고 설치된 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.

수동 등록을 사용한 인증서 설치

프로시저

단계 **1** 등록 프로세스를 시작 하려면 설치 를 누릅니다.

단계 **2** **Devices(**디바이스**) > Certificates(**인증서**)** 화면에서 **Add(**추가**) > Add New Certificate(**새 인증서 추가**)**를 선택하고 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 엽니다.

단계 **3** 드롭다운 목록에서 **Device(**디바이스**)**를 엽니다.

단계 **4** 다음 방법 중 하나로 인증서 등록 개체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 적절한 유형의 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가, 630 페이지을 참조하십시오.

단계 **5** 가져오기를 누르면 수동 등록 프로세스를 시작합니다.

Firepower Management Center가 (등록 개체가 제공한) CA 인증서를 관리되는 디바이스에 설치하고 CA 서버를 인증하며 관리되는 디바이스에 트러스트 포인트를 생성하므로 **CA** 인증서 상태는 `InProgress`에서 `Available` 상태로 전환됩니다.

ID 인증서 상태가 CSR 생성 및 ID 인증서 가져오기가 보류 중이라는 경고 메시지를 보여줄 수 있습니다.

단계 **6** ID 인증서를 가져오기 위해 PKI CA 서버에서 적절한 작업을 실행합니다.

a) CSR을 보고 복사하려면 **Identity Certificate(ID** 인증서**)** 경고를 클릭합니다.

b) CRS을 사용해 ID 인증서를 가져오기 위해 PKI CA 서버에서 적절한 작업을 실행합니다.

이러한 작업은 Firepower Management Center 또는 관리되는 디바이스와는 완전히 별개입니다. 완료되면 관리되는 디바이스에 대한 ID 인증서가 생성됩니다. 복사 또는 파일에 저장할 수 있습니다.

c) 수동 프로세스를 완료하려면 가져온 ID 인증서를 관리되는 디바이스에 설치합니다.

Firepower Management Center 대화 상자로 돌아가 ID 인증서를 필드에 붙여 넣습니다. 또는 검색을 선택하여 ID 인증서 파일을 선택합니다.

단계 **7** ID 인증서를 가져오려면 가져오기를 선택합니다.

가져오기가 완료되면 ID 인증서 상태는 Available이 됩니다.

단계 **8** 장치에 대한 **ID** 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.

PKCS12 파일을 가져오는 방법으로 인증서 설치

프로시저

단계 **1** 장치 > 인증서 화면에서 **PKCS12** 파일 가져오기 대화 상자를 열려면 + 추가 > **PKCS12** 파일 가져오기를 클릭합니다.

단계 **2** 디바이스 드롭다운 목록에서 사전 구성된 관리되는 디바이스를 선택합니다.

단계 **3** **PKCS12**인증서 등록 유형을 지정합니다.

단계 **4** PKCS#12 인증서 파일을 찾아서 선택하려면 검색을 선택합니다.

단계 **5** 암호 해독을 위해 암호 문구 값을 입력합니다.

단계 **6** 추가를 누릅니다.

파일 가져오기의 경우 CA 인증서 및 ID 인증서 상태는 PKCS12 파일이 디바이스에 설치됨에 따라 In Progress(진행 중)에서 Available(사용 가능)으로 전환됩니다.

단계 **7** 사용 가능 상태에서 장치에 대한 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

관리되는 디바이스의 인증서(트러스트 포인트)는 PKCS#12 파일과 동일합니다. VPN 인증 설정에서 이 인증서를 사용합니다.

FTD VPN 인증서 문제 해결

인증서 등록 환경의 차이로 인해 문제가 발생했는지 여부는 Firepower Threat Defense VPN 인증서 가이드라인 및 제한 사항, 676 페이지을 참조하십시오. 다음을 확인합니다.

- 디바이스에서 CA 서버에 대한 경로가 있는지 확인합니다.

  CA 서버의 호스트 이름이 등록 개체에 지정된 경우 Flex Config를 사용해 서버에 적절히 연결하는 DNS를 구성합니다. CA 서버의 IP 주소를 사용해도 됩니다.

- Microsoft 2012 CA 서버를 사용하는 경우 관리되는 디바이스에서 기본 IPsec 템플릿을 허용하지 않으므로 변경해야 합니다.

  작업 템플릿을 구성하려면 MS CA 설명서를 참조하여 다음 단계를 따르십시오.

  1. IPsec(오프라인 요청) 템플릿을 복제합니다.
  2. **Extensions(**확장**) > Application policies(**애플리케이션 정책**)**에서 *IP security IKE intermediate(IP* 보안 *IKE* 중급*)* 대신 *IP security end system(IP* 보안 최종 시스템*)*을 선택합니다.
  3. 권한 및 템플릿 이름을 설정합니다.
  4. 새 템플릿을 추가하고 새 템플릿 이름을 반영하기 위해 레지스트리 설정을 변경합니다.

Firepower Threat Defense 인증서 기반 인증 히스토리

기능	버전	세부 사항
수동 등록 기능 향상	6.7	이제 ID 인증서 없이 CA 인증서만 생성할 수 있습니다. CA 인증서 없이 CSR을 생성하고 CA에서 ID 인증서를 가져올 수도 있습니다.
PKCS CA 체인	6.7	인증서를 발급하는 인증 기관(CA)의 체인을 보고 관리할 수 있습니다. 인증서 복사본을 내보낼 수도 있습니다.

V 부

클래식 디바이스 구성 기본 사항

- 클래식 디바이스 관리 기본 사항, 685 페이지
- IPS 디바이스 구축 및 구성, 697 페이지

24 장

클래식 디바이스 관리 기본 사항

다음 주제는 Firepower System의 클래식 디바이스(7000 및 8000 시리즈 디바이스/ASA with FirePOWER Services/NGIPSv)를 관리하는 방법을 설명합니다.

- 클래식 디바이스 관리 요구 사항 및 사전 요건, 685 페이지
- 원격 관리 구성(클래식 디바이스), 685 페이지
- 인터페이스 설정, 688 페이지

클래식 디바이스 관리 요구 사항 및 사전 요건

모델 지원

절차에 나와 있는 클래식 모델

지원되는 도메인

Leaf 달리 명시되지 않은 경우

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)

원격 관리 구성(클래식 디바이스)

7000 및 **8000** 시리즈를 제외한 모든 디바이스

기본 라이선스를 사용하는 디바이스의 원격 관리를 구성하는 방법은 디바이스에 맞는 빠른 시작 가이드를 참조하십시오.

7000 및 **8000** 시리즈 디바이스

디바이스를 FMC에 등록하기 전 로컬 웹 인터페이스를 사용하여 7000 또는 8000 Series 디바이스의 원격 관리를 구성합니다.

Firepower 디바이스를 관리하기 전에 Firepower Management Center와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. 어플라이언스는 채널을 사용하여 구성 및 이벤트 정보를 공유합니다. 고가용성 피어도 채널을 사용하며, 기본 포트는 8305/tcp입니다.

두 어플라이언스 간 커뮤니케이션을 활성화하려면 어플라이언스가 서로 인식할 수 있는 다음과 같은 방법을 제공해야 합니다.

- 호스트 이름 또는 사용자가 커뮤니케이션을 설정하려는 어플라이언스의 IP 주소

  NAT 환경에서 다른 어플라이언스는 라우팅할 수 있는 주소가 없는 경우에도 원격 관리를 구성할 때 또는 관리 어플라이언스를 추가할 때 IP 주소 또는 호스트 이름을 제공해야 합니다.

- 연결을 식별하는 최대 37자의 자체 생성 영숫자 등록 키
- NAT 환경에서 이 커뮤니케이션을 설정하는 데 도움이 되는 선택적인 고유한 영숫자 NAT ID

  NAT ID는 반드시 관리되는 어플라이언스 등록에 사용되는 모든 NAT ID 중에서 고유한 것이어야 합니다.

매니지드 디바이스에서 원격 관리 구성

이 절차는 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 **1** 관리하려는 디바이스의 웹 인터페이스에서 **System(**시스템**)** > **Integration(**통합**)** > **Remote Management(**원격 관리**)**을 선택합니다.

단계 **2** 미리 표시되지 않은 경우 **Remote Management(**원격 관리**)**를 클릭합니다.

단계 **3** **Add Manager(**관리자 추가**)**를 클릭합니다.

단계 **4** 관리 호스트 필드에서 어플라이언스를 관리하는 데 사용할 Firepower Management Center에 대해 다음을 입력합니다.

- IP 주소
- FQDN(Fully Qualified Domain Name) 또는 로컬 DNS를 통해 확인한 이름(즉 호스트 이름)

주의 네트워크에서 DHCP를 사용하여 IP 주소를 할당하는 경우 IP 주소 대신 호스트 이름을 사용합니다.

NAT 환경에서 관리되는 어플라이언스를 추가할 때 IP 주소 또는 호스트 이름을 지정하려는 경우 여기에서 지정할 필요는 없습니다. 이 경우 Firepower System은 관리되는 어플라이언스의 웹 인터페이스에서 원격 관리자를 식별하기 위해 나중에 제공되는 NAT ID를 사용합니다.

단계 **5** **Registration Key(**등록 키**)** 필드에 어플라이언스 간 커뮤니케이션을 설정하는 데 사용할 등록 키를 입력합니다.

단계 **6** NAT 환경의 경우, **Unique NAT ID(**고유 **NAT ID)** 필드에 어플라이언스 간 커뮤니케이션을 설정하는 데 사용할 고유한 영숫자 NAT ID를 입력합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 어플라이언스가 서로 커뮤니케이션할 수 있는지 확인하면 Pending Registration(등록 보류) 상태가 표시됩니다.
- Firepower Management Center에 디바이스를 추가하려면 FMC에 디바이스 추가, 311 페이지를 참조하십시오.

매니지드 디바이스에서 원격 관리 수정

이 절차는 7000 및 8000 Series 디바이스에 적용됩니다.

원격 관리자를 편집할 때는 다음에 주의하십시오.

- 호스트 필드는 FQDN(Fully Qualified Domain Name) 또는 로컬 DNS를 통해 확인한 유효한 IP 주소(즉 호스트 이름)를 정의합니다.
- 이름 필드는 관리하는 어플라이언스의 표시 이름을 정의하며 이는 Firepower System의 컨텍스트 내에서만 사용됩니다. 다른 표시 이름을 입력해도 관리하는 디바이스의 호스트 이름은 변경되지 않습니다.

프로시저

단계 **1** 디바이스의 웹 인터페이스에서 **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

단계 **2** 미리 표시되지 않은 경우 **Remote Management(**원격 관리**)**를 클릭합니다.

단계 **3** 다음 작업을 수행할 수 있습니다.

- 원격 관리 비활성화 - 활성화를 하거나 비활성화하려면 관리자 옆의 슬라이더를 클릭합니다. 관리를 비활성화하면 Firepower Management Center와 디바이스 간 연결이 차단되지만 Firepower Management Center에서 디바이스가 삭제되지는 않습니다. 디바이스를 더 이상 관리하지 않으려면 FMC에서 디바이스 삭제, 315 페이지을 참조하십시오.
- 관리자 정보 편집 - 수정하려는 관리자 옆의 수정( )을 클릭하여 **Name(**이름**)** 및 **Host(**호스트**)** 필드를 수정하고 **Save(**저장**)**을 클릭합니다.

관리 포트 변경

어플라이언스는 기본적으로 포트 8305를 사용하는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

Cisco는 기본 설정을 유지할 것을 적극 권장하지만 관리 포트가 네트워크의 다른 통신과 충돌하는 경우 다른 포트를 선택할 수 있습니다. 일반적으로 관리 포트 변경은 설치 중에 수행합니다.

⚠

주의 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 어플라이언스의 설정을 변경해야 합니다.

전역 도메인에서 이 작업을 수행해야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** 관리 인터페이스를 클릭합니다.

단계 **3** 공유 설정 섹션의 원격 관리 포트 필드에 사용하려는 포트 번호를 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

어플라이언스와 통신해야 할 구축 시 모든 어플라이언스에 대해 이 절차를 반복합니다.

인터페이스 설정

어플라이언스 편집기의 인터페이스 페이지에 자세한 인터페이스 설정 정보가 표시됩니다. 페이지는 물리적 하드웨어 보기와 인터페이스 테이블 보기로 구성되며 설정 세부사항을 드릴다운할 수 있습니다. 이 페이지에서 인터페이스를 추가하고 편집할 수 있습니다.

물리적 하드웨어 보기

인터페이스 페이지 상단에는 7000 또는 8000 Series 디바이스에 대한 물리적 하드웨어 보기가 그림 형태로 표시됩니다.

물리적 하드웨어 보기를 사용하면 다음을 할 수 있습니다.

- 네트워크 모듈, 부품 번호 및 일련 번호 보기
- 인터페이스 테이블 보기에서 인터페이스 선택
- 인터페이스 편집기 열기
- 인터페이스의 이름, 인터페이스의 유형, 인터페이스의 링크 포함 여부, 인터페이스의 속도 설정, 인터페이스가 현재 우회 모드에 있는지 여부 보기
- 오류 또는 경고에 대한 세부 사항 보기

인터페이스 페이지

Interfaces(인터페이스) 페이지에는 디바이스에서 사용 가능한 모든 인터페이스가 나와 있습니다. 테이블에는 구성된 모든 인터페이스를 볼 때 사용할 수 있는 확장 가능한 탐색 트리가 포함되어 있습니다. 인터페이스 옆의 화살표 아이콘을 클릭하여 인터페이스를 확장하거나 축소하면 하위 구성 요소를 보거나 숨길 수 있습니다. 인터페이스 테이블 보기는 각 인터페이스에 대해 요약된 정보를 제공합니다.

필드	설명
이름	각 인터페이스 유형은 해당 유형 및 링크 상태(해당되는 경우)를 나타내는 고유한 아이콘으로 표시됩니다. 이름이나 아이콘 위에 포인터를 올려 놓으면 추가 정보를 제공하는 도구 설명이 표시됩니다. 인터페이스 아이콘에 대해서는 인터페이스 아이콘, 690 페이지에 설명되어 있습니다. 아이콘은 인터페이스의 다음 세 가지 상태 중 하나인 현재 링크 상태를 나타내기 위해 배지 표기 규칙을 사용합니다. • **Error** • **Fault(**결함**)** • 사용할 수 없음 논리적 인터페이스는 상위 물리적 인터페이스와 동일한 링크 상태를 가집니다. ASA FirePOWER 모듈은 링크 상태를 표시하지 않습니다. 비활성화된 인터페이스는 반투명 아이콘으로 표시됩니다. 아이콘 오른쪽에 나타나는 인터페이스 이름은 하이브리드 및 사용자가 정의한 ASA FirePOWER 인터페이스를 제외하면 자동으로 생성됩니다. ASA FirePOWER 인터페이스의 경우 시스템은 활성화되고 이름이 있으며 링크가 있는 인터페이스만 표시합니다. 물리적 인터페이스는 물리적 인터페이스의 이름을 표시합니다. 논리적 인터페이스는 물리적 인터페이스의 이름 및 할당된 VLAN 태그를 표시합니다. ASA FirePOWER 여러 보안 컨텍스트가 있는 경우 인터페이스는 보안 컨텍스트의 이름 및 인터페이스의 이름을 표시합니다. 보안 컨텍스트가 하나인 경우 시스템은 인터페이스의 이름만 표시합니다.
보안 영역	인터페이스가 할당된 보안 영역 보안 영역을 추가 또는 편집하려면 수정( )을 클릭합니다.
에서 사용(NGIPSv만 해당)	인터페이스가 할당된 인라인 집합, 가상 스위치 또는 가상 라우터
MAC Address(MAC 주소)	스위치 또는 라우팅 기능이 활성화되었을 때 인터페이스에 표시되는 MAC 주소 NGIPSv 디바이스의 경우 디바이스에 구성된 네트워크 어댑터를 인터페이스 페이지에 나타나는 인터페이스에 일치시킬 수 있는 MAC 주소가 표시됩니다.

필드	설명
IP 주소(7000/8000 시리즈만 해당)	인터페이스에 할당된 IP 주소 활성화 여부를 확인하려면 IP 주소 위로 포인터를 옮깁니다. 비활성 IP 주소는 회색으로 표시됩니다.

인터페이스 아이콘

표 ***65:*** 인터페이스 아이콘 유형 및 설명

아이콘	**Interface Type**	설명	확인
물리적	물리적	설정되지 않은 물리적 인터페이스	물리적 스위치 인터페이스 설정 또는 물리적 라우팅 인터페이스 설정
수동	수동	패시브 구축 시 트래픽을 분석하도록 설정된 센싱 인터페이스	패시브 인터페이스 구성, 699 페이지
인라인	인라인	인라인 구축 시 트래픽을 처리하도록 설정된 센싱 인터페이스	인라인 인터페이스 구성, 702 페이지
전환됨	전환됨	Layer 2 구축 시 트래픽을 전환하도록 설정된 인터페이스	스위치 인터페이스 구성
라우팅 모드	라우팅 모드	Layer 3 구축 시 트래픽을 라우팅하도록 설정된 인터페이스	라우팅 인터페이스
집계	집계	단일 논리적 링크로서 설정된 여러 물리적 인터페이스	집계 인터페이스 정보
집계 전환	집계 전환	Layer 2 구축 시 단일 논리적 링크로서 설정된 여러 물리적 인터페이스	집계 스위치 인터페이스 추가
집계 라우팅	집계 라우팅	Layer 3 구축 시 단일 논리적 링크로서 설정된 여러 물리적 인터페이스	집계 라우팅 인터페이스 추가
하이브리드	하이브리드	가상 라우터와 가상 스위치 간 트래픽을 연결하도록 설정된 논리적 인터페이스	논리적 하이브리드 인터페이스
ASA FirePOWER	ASA FirePOWER	ASA FirePOWER 모듈이 설치된 ASA 디바이스에 설정된 인터페이스	Cisco ASA FirePOWER 인터페이스 관리, 694 페이지

물리적 하드웨어 보기 사용

이 작업은 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 관리하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 다음 경우에 그래픽 인터페이스를 사용합니다.

- 선택 - 인터페이스를 선택하려면 인터페이스를 클릭합니다. 시스템은 인터페이스 테이블에서 관련된 항목을 강조 표시합니다.
- 편집 - 인터페이스 편집기를 열려는 경우 인터페이스를 두 번 클릭합니다.
- 오류 또는 경고 정보 보기 - 오류 또는 경고에 대한 세부 정보를 확인하려는 경우 네트워크 모듈에서 영향을 받은 포트 위에 마우스 커서를 이동합니다.
- 인터페이스 정보 보기 - 인터페이스 이름, 인터페이스 유형, 인터페이스의 링크 포함 여부, 인터페이스의 속도 설정, 인터페이스가 현재 우회 모드에 있는지 여부를 확인하려면 인터페이스 위에 커서를 올립니다.
- 네트워크 모듈 정보 보기 - 네트워크 모듈 유형, 부품 번호, 일련 번호를 보려면 네트워크 모듈 하단 왼쪽의 어두운 원 위에 커서를 올립니다.

센싱 인터페이스 설정

Firepower 구축에 따라 어플라이언스 편집기의 인터페이스 페이지에서 관리되는 디바이스의 센싱 인터페이스를 구성할 수 있습니다. 관리되는 디바이스에는 총 1024개의 인터페이스만 구성할 수 있습니다.

참고 ASA FirePOWER 디바이스를 SPAN 포트 모드에서 구축한 경우 Firepower Management Center에는 ASA 인터페이스가 표시되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 인터페이스를 구성하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 구성하려는 인터페이스 옆의 수정( )을 클릭합니다.

단계 **4** 인터페이스 편집기를 사용하여 다음과 같이 센싱 인터페이스를 구성합니다.

- HA 링크 - 7000/8000 시리즈 디바이스의 고가용성 쌍에서 각 멤버에 구성된 인터페이스가 이중 통신 채널 또는 고가용성 링크 인터페이스로 기능하도록 하는 경우 **HA** 링크를 클릭하고 HA 링크 인터페이스 설정, 692 페이지의 설명에 따라 진행합니다.
- 인라인 - 인터페이스가 인라인 구축에서 트래픽을 처리하도록 구성하려는 경우 인라인을 클릭하고 인라인 인터페이스 구성, 702 페이지의 설명에 따라 진행합니다.
- 패시브 - 인터페이스가 패시브 구축에서 트래픽을 분석하도록 구성하려는 경우 패시브를 클릭하고 패시브 인터페이스 구성, 699 페이지의 설명에 따라 진행합니다.
- 라우티드 - 인터페이스가 7000/8000 시리즈 Layer 3 구축 시 트래픽을 라우팅하도록 구성하려면 라우티드를 클릭하고 라우팅 인터페이스의 설명에 따라 진행합니다.
- 스위치드 - 인터페이스가 7000/8000 시리즈 Layer 2 구축 시 트래픽을 전환하도록 구성하려는 경우 스위치드를 클릭하고 스위치 인터페이스 구성의 설명에 따라 진행합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

HA 링크 인터페이스 설정

7000 또는 8000 Series 디바이스를 고가용성 쌍으로 설정한 후 물리적 인터페이스를 고가용성(HA) 링크 인터페이스로 구성해야 합니다. 이 링크는 페어링된 디바이스 간 상태 정보 공유를 위한 이중 통신 채널 역할을 합니다. 하나의 디바이스에서 HA 링크 인터페이스를 구성하면 두 번째 디바이스에서도 자동으로 인터페이스가 구성됩니다. 동일한 브로드캐스트 도메인에서는 HA 링크를 모두 구성해야 합니다.

동적 NAT는 다른 IP 주소 및 포트를 매핑할 때 동적 할당 IP 주소 및 포트에 의존합니다. HA 링크가 없는 경우 페일오버 시 매핑이 손실되어 현재 고가용성 쌍의 액티브 디바이스를 통해 라우팅된 모든 변환 연결에 실패하게 됩니다.

마찬가지로 고가용성 상태 공유 중인 7000 또는 8000 Series 디바이스, 동적 NAT 또는 VPN은 HA 링크 인터페이스를 요구합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** HA 링크 인터페이스를 설정하려는 피어 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** HA 링크 인터페이스로 설정하려는 인터페이스 옆의 수정( )을 클릭합니다.

단계 **4** **HA** 링크를 클릭합니다.

단계 **5** 활성화 확인란을 선택합니다.

체크 박스의 선택을 취소하는 경우 시스템은 이를 비활성화하고 관리를 위해 인터페이스를 종료합니다.

단계 **6** 모드 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 자동 협상을 선택하여 인터페이스의 자동 협상 속도 및 양방향 설정을 구성합니다.

단계 **7** **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다.

일반적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

단계 **8** **MTU** 필드에 최대 전송 단위 (MTU)를 입력합니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위, 695 페이지를 참조하십시오.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

인터페이스 비활성화

인터페이스 유형을 **None**으로 설정하여 인터페이스를 비활성화할 수 있습니다. 비활성화된 인터페이스는 인터페이스 목록에서 회색으로 표시됩니다.

이 절차는 NGIPSv 및 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인터페이스를 비활성화하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 비활성화하려는 인터페이스 옆의 수정( )을 클릭합니다.

단계 **4** **None**을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

Cisco ASA FirePOWER 인터페이스 관리

ASA FirePOWER 인터페이스를 수정할 때, Firepower Management Center에서 인터페이스의 보안 영역만 구성할 수 있습니다.

ASA 전용 소프트웨어 및 CLI를 사용하면 ASA FirePOWER 인터페이스를 완전히 구성할 수 있습니다. ASA FirePOWER을 편집하여 다중 컨텍스트 모드에서 단일 컨텍스트 모드(또는 그 반대로) 전환하면 ASA FirePOWER는 모든 인터페이스의 이름을 변경합니다. 업데이트된 ASA FirePOWER 인터페이스 이름을 사용하려면 모든 Firepower System 보안 영역, 상관관계 규칙 및 관련 설정을 재구성해야 합니다. ASA FirePOWER 인터페이스 설정에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

참고 ASA FirePOWER 인터페이스의 유형을 변경하거나 Firepower Management Center에서 인터페이스를 비활성화할 수 없습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 인터페이스를 비활성화하려는 디바이스 옆에 있는 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 미리 표시되지 않은 경우 인터페이스를 클릭합니다.

단계 **4** 편집하려는 인터페이스 옆에 있는 수정( )을 클릭합니다.

단계 **5** 보안 영역 드롭다운 목록에서 기존 보안 영역을 선택하거나 새 보안 영역을 추가하기 위해 새로 만들기를 선택합니다.

단계 **6** 저장을 클릭하여 보안 영역을 구성합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위

디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

참고 시스템은 구성된 MTU 값을 18바이트 크기로 줄입니다. IPv4 MTU를 594 이하로 설정하거나 IPv6 MTU를 1298 이하로 설정하지 마십시오.

플랫폼	**MTU** 범위
7000 및 8000 Series	576-9234(관리 인터페이스) 576 10172(인라인 집합, 패시브 인터페이스) 576-9922(기타 모두)
NGIPSv	576-9018(모든 인터페이스, 인라인 집합)

관련 항목

MTU 정보, 833 페이지

보안 영역 개체의 수정 버전 동기화

보안 영역 개체를 업데이트하면 시스템은 개체의 새 개정을 저장합니다. 따라서 인터페이스에 각기 다른 수정 버전의 보안 영역 개체가 구성되어 있는 매니지드 디바이스가 동일한 보안 영역에 있는 경우 중복 연결로 보이는 항목이 로깅될 수 있습니다.

이중 연결 보고가 발견되면 개체의 동일한 개정을 사용하도록 모든 매니지드 디바이스를 업데이트할 수 있습니다.

이 절차는 NGIPSv 및 7000 및 8000 Series 디바이스에 적용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 보안 영역 선택을 업데이트하려는 디바이스 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 중복 연결 이벤트를 로깅하는 각 인터페이스에 대해 **Security Zone(**보안 영역**)**을 다른 영역으로 변경하고, **Save(**저장**)**를 클릭한 다음 원하는 영역으로 다시 변경하고 **Save(**저장**)**를 다시 클릭합니다.

단계 **4** 이중 이벤트를 로깅하는 각 디바이스에 대해 2단계와 3단계를 반복합니다. 계속 진행하기 전에 모든 디바이스를 수정해야 합니다.

다음에 수행할 작업

- 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참고하십시오.

주의 동기화하려는 모든 디바이스에서 인터페이스에 대한 영역 설정을 수정하기 전에는 구성 변경 사항을 디바이스에 구축하지 마십시오. 모든 매니지드 디바이스에 동시에 구축해야 합니다.

25 장

IPS 디바이스 구축 및 구성

다음 주제는 IPS 구축에서 디바이스를 구성하는 방법을 설명합니다.

- IPS 디바이스 구축 및 구성 소개, 697 페이지
- IPS 디바이스 구축 라이선스 요구 사항, 697 페이지
- IPS 디바이스 구축 요구 사항 및 사전 요건, 697 페이지
- 수동 IPS 구축, 698 페이지
- 인라인 IPS 구축, 700 페이지

IPS 디바이스 구축 및 구성 소개

패시브 또는 인라인 IPS 구축에서 디바이스를 구성할 수 있습니다. 패시브 구축에서는 네트워크 트래픽 플로우 대역 외부에 시스템이 구축됩니다. 인라인 구축에서는 두 포트를 바인딩하여 네트워크 세그먼트에 투명하게 시스템을 구성합니다.

IPS 디바이스 구축 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

IPS 디바이스 구축 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

Leaf에 전달하는 고성능 고속 어플라이언스입니다.

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)

수동 IPS 구축

패시브 IPS 구축에서 Firepower System은 스위치 SPAN 또는 미러 포트를 사용해 네트워크에서 이동하는 트래픽을 모니터링합니다. SPAN을 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않는 경우에도 네트워크 내의 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 패시브 인터페이스는 로컬 SPAN 및 원격 SPAN(RSPAN) 트래픽을 모두 지원합니다.

참고 아웃바운드 트래픽은 플로우 제어 패킷을 포함합니다. 따라서 어플라이언스의 패시브 인터페이스는 아웃바운드 트래픽을 표시할 수 있으며 컨피그레이션에 따라 이벤트를 생성할 수 있는데, 이는 자연스러운 동작입니다.

Firepower System의 패시브 인터페이스

관리되는 디바이스에서 하나 이상의 물리적 포트를 수동 인터페이스로 구성할 수 있습니다.

트래픽을 모니터링하기 위해 패시브 인터페이스를 활성화하면 구리 인터페이스에서만 사용 가능한 모드 및 MDI/MDIX 설정을 지정합니다. 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

패시브 인터페이스를 비활성화하면 보안 때문에 사용자가 액세스할 수 없습니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

관련 항목

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위, 695 페이지
Snort® 재시작 시나리오, 505 페이지

패시브 인터페이스 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 패시브 인터페이스를 구성하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 패시브 인터페이스를 구성하려는 인터페이스 옆의 수정( )을 클릭합니다.

단계 **4** 패시브를 클릭합니다.

단계 **5** 보안 영역 내 패시브 인터페이스를 연결하려면 다음 중 하나를 수행합니다.

- 보안 영역 드롭다운 목록에서 기존 보안 영역을 선택합니다.
- 새 보안 영역을 추가하려면 새로 만들기를 선택합니다. 보안 영역 개체 생성, 578 페이지를 참조하십시오.

단계 **6** **Enable(**활성화**)** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

단계 **7** 7000 및 8000 Series 전용: 모드 드롭다운 목록에서 링크 모드를 지정하거나 자동 협상을 선택하여 인터페이스의 자동 협상 속도 및 양방향 설정을 지정합니다.

모드 설정은 구리 인터페이스에 대해서만 가능합니다.

8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

단계 **8** 7000 및 8000 Series 전용: **MDI/MDIX** 드롭다운 목록에서 인터페이스가 MDI(Medium Dependent Interface), MDIX(Medium Dependent Interface Crossover) 또는 Auto-MDIX로 구성될지 여부를 지정합니다.

MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

단계 **9** **MTU** 필드에 최대 전송 단위(MTU)를 입력합니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

인라인 IPS 구축

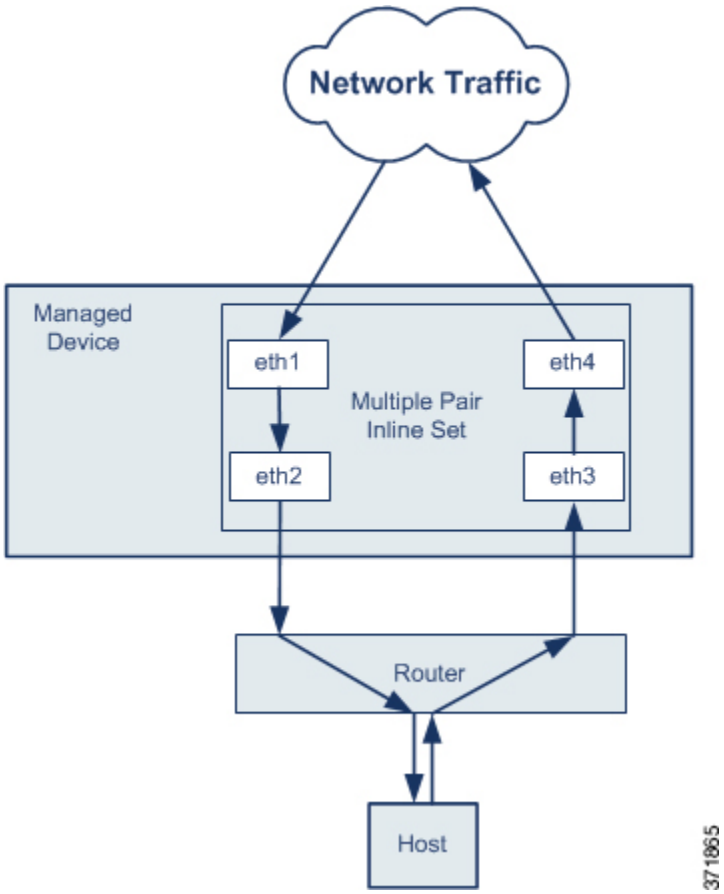
인라인 IPS 구축에서는 두 포트를 바인딩하여 네트워크 세그먼트에서 Firepower System을 투명하게 구성합니다. 이 기능을 사용하면 인접한 네트워크 디바이스의 구성 없이 네트워크 환경에 시스템을 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

참고 시스템이 트래픽에 영향을 미치려면 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 관련 구성을 매니지드 디바이스에 구축해야 합니다.

디바이스 트래픽이 인바운드인지 아웃바운드인지에 따라 서로 다른 인라인 인터페이스 쌍을 통해 네트워크의 호스트와 외부 호스트 간 트래픽을 라우팅하도록 관리되는 디바이스에서 인터페이스를 구성할 수 있습니다. 이는 비동기 라우팅 설정입니다. 비동기 라우팅을 구축하지만 인라인 집합에 인터페이스 쌍을 하나만 포함하려는 경우 트래픽이 절반만 표시되어 디바이스에서 네트워크 트래픽을 올바르게 분석하지 못할 수 있습니다.

동일한 인터페이스 집합에 여러 인라인 인터페이스 쌍을 추가하면 시스템은 동일한 트래픽 플로우의 일부로서 인바운드 및 아웃바운드 트래픽을 식별할 수 있습니다. 패시브 인터페이스에서는 인터페이스 쌍을 동일한 보안 영역에 포함해도 동일한 효과를 얻습니다.

시스템이 비동기 라우팅 컨피그레이션을 통과하는 트래픽에서 연결 이벤트를 생성하면, 해당 이벤트는 동일한 인터페이스 쌍에서 인그레스 및 이그레스 인터페이스를 식별할 수 있습니다. 예를 들어 다음 다이어그램의 설정은 **eth3**을 인그레스 인터페이스로, **eth2**를 이그레스 인터페이스로 식별하는 연결 이벤트를 생성합니다. 이 설정에서는 일반적인 동작입니다.



참고 여러 인터페이스 쌍을 단일 인라인 인터페이스 집합에 할당하여 중복 트래픽의 문제가 발생하는 경우 시스템이 패킷을 고유하게 식별하도록 다시 구성해야 합니다. 예를 들어 인라인 집합을 구별하도록 인터페이스 쌍을 다시 할당하거나 보안 영역을 수정할 수 있습니다.

인라인 집합이 있는 디바이스의 경우 디바이스를 다시 시작하면 소프트웨어 브리지가 패킷을 전송하도록 자동으로 다시 설정됩니다. 디바이스가 다시 시작 중이면 소프트웨어 브리지가 어디서도 실행되지 않습니다. 인라인 집합에서 우회 모드를 활성화하면 디바이스가 다시 시작되는 동안 하드웨어 우회로 들어갑니다. 이 경우 디바이스와의 링크 재협상 때문에, 시스템이 종료되었다가 다시 시작되면서 몇 초 분량의 패킷이 손실될 수 있습니다. 그러나 시스템은 Snort가 다시 시작되는 동안 트래픽을 전달합니다.

관련 항목

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위, 695 페이지
Snort® 재시작 시나리오, 505 페이지

Firepower System의 인라인 인터페이스

관리되는 디바이스에서 하나 이상의 물리적 포트를 인라인 인터페이스로 구성할 수 있습니다. 인라인 세트에 할당된 인라인 인터페이스 쌍에서만 인라인 구축의 트래픽을 처리할 수 있습니다.

참고:

- 시스템은 인라인 쌍의 인터페이스를 다른 속도로 설정하거나 인터페이스가 다른 속도로 협상하는 경우 경고를 표시합니다.
- 인터페이스를 인라인 인터페이스로 구성하는 경우 해당 NetMod의 인접 포트가 자동으로 인라인 인터페이스가 되어 쌍을 완성합니다.
- NGIPSv 디바이스에서 인라인 인터페이스를 구성하려면 인접 인터페이스를 사용하여 인라인 쌍을 생성해야 합니다.

인라인 인터페이스 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인터페이스를 구성하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 구성하려는 인터페이스 옆의 수정( )을 클릭합니다.

단계 **4** 인라인을 클릭 합니다.

단계 **5** 보안 영역이 있는 페시브 인터페이스를 연결하려면 다음 중 하나를 수행합니다.

- 보안 영역 드롭다운 목록에서 기존 보안 영역을 선택합니다.
- 새 보안 영역을 추가하려면 새로 만들기를 선택합니다. 보안 영역 개체 생성, 578 페이지를 참조하십시오.

단계 **6** 인라인 집합 드롭다운 목록에서 기존 인라인 집합을 선택하거나 새로 만들기로 새 인라인 집합을 추가합니다.

참고 새 인라인 집합을 추가하는 경우 인라인 인터페이스를 설정한 후 구성해야 합니다. 인라인 집합 추가, 705 페이지을 참조하십시오.

단계 **7** **Enable(**활성화**)** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

단계 **8** 7000 및 8000 Series 전용: 모드 드롭다운 목록에서 링크 모드를 지정하거나 자동 협상을 선택하여 인터페이스의 자동 협상 속도 및 양방향 설정을 지정합니다.

모드 설정은 구리 인터페이스에 대해서만 가능합니다.

8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

단계 **9** 7000 및 8000 Series 전용: **MDI/MDIX** 드롭다운 목록에서 인터페이스가 MDI(Medium Dependent Interface), MDIX(Medium Dependent Interface Crossover) 또는 Auto-MDIX로 구성될지 여부를 지정합니다.

MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

Firepower System의 인라인 집합

인라인 구축에서 인라인 인터페이스를 사용하려면 인라인 집합을 구성하고 여기에 인라인 인터페이스 쌍을 할당해야 합니다. 인라인 집합은 디바이스에 있는 하나 이상의 인라인 인터페이스 쌍을 그룹화한 것입니다. 한 인라인 인터페이스 쌍은 동시에 한 인라인 집합에만 속할 수 있습니다.

Device Management(디바이스 관리) 페이지의 **Inline Sets(**인라인 집합**)** 탭에는 디바이스에 구성한 모든 인라인 집합의 목록이 표시됩니다.

Device Management(디바이스 관리) 페이지의 **Inline Sets(**인라인 집합**)** 탭에서 인라인 집합을 추가하거나, 인라인 인터페이스를 구성할 때 인라인 집합을 추가할 수 있습니다.

인라인 인터페이스 쌍은 인라인 집합에만 할당할 수 있습니다. 매니지드 디바이스에서 인라인 인터페이스를 구성하기 전에 인라인 집합을 생성하려는 경우 빈 인라인 집합을 만들고 나중에 여기에 인터페이스를 추가할 수 있습니다. 인라인 집합의 이름을 입력할 때는 영숫자 및 공백을 사용할 수 있습니다.

참고 인라인 집합에서 인터페이스용 보안 영역을 추가하기 전에 인라인 집합을 생성합니다. 그렇지 않으면 보안 영역이 제거되므로 다시 추가해야 합니다.

이름

인라인 집합의 이름입니다.

Interfaces

인라인 집합에 할당된 모든 인라인 인터페이스 쌍의 목록입니다. Interfaces 탭에서 쌍의 두 인터페이스 중 하나를 비활성화하면 쌍을 사용할 수 없음

MTU

인라인 집합의 최대 전송 단위입니다. MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

Failsafe

트래픽이 탐지를 우회하고 디바이스를 계속 통과하도록 허용합니다. 매니지드 디바이스는 내부 트래픽 버퍼를 모니터링하고 버퍼가 꽉 차면 탐지를 우회합니다.

Bypass Mode(바이패스 모드**)**

Firepower 7000 또는 8000 Series에만 해당: 인라인 집합의 구성된 우회 모드입니다. 이 설정은 인터페이스에서 장애가 발생할 때 인라인 인터페이스의 릴레이가 어떻게 반응하는지를 결정합니다. 바이패스 모드에서는 트래픽이 인터페이스를 계속 통과할 수 있습니다. 바이패스 이외의 모드에서는 트래픽이 차단됩니다.

주의 우회 모드에서 어플라이언스를 재부팅하면 패킷이 약간 손실될 수 있습니다. 고가용성 쌍의 7000 또는 8000 Series 디바이스에 있는 인라인 집합, 8000 Series 디바이스에 있는 우회 이외의 NetMod 또는 Firepower 7115나 7125 디바이스의 SFP 모듈에 대해서는 우회 모드를 구성할 수 없습니다.

관련 항목

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위, 695 페이지
Snort® 재시작 시나리오, 505 페이지

인라인 집합 보기

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인라인 집합을 보려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

인라인 집합 추가

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인라인 집합을 추가하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **4** **Add Inline Set(**인라인 집합 추가**)**를 클릭합니다.

단계 **5** **Name(**이름**)**을 입력합니다.

단계 **6** 인터페이스 옆에서 하나 이상의 인라인 인터페이스 쌍을 선택한 다음 **Add Selected(**선택 항목 추가**)**를 클릭합니다. 인라인 집합에 모든 인터페이스 쌍을 추가하려면 **Add All(**모두 추가**)**을 클릭합니다.

팁 인라인 집합에서 인라인 인터페이스를 제거하려면 하나 이상의 인라인 인터페이스 쌍을 선택하고 **Remove Selected(**선택 항목 제거**)**를 클릭합니다. 인라인 집합에서 모든 인터페이스 쌍을 제거하려면 **Remove All(**모두 제거**)**을 클릭합니다. 인터페이스에서 인터페이스 쌍의 인터페이스 중 하나를 비활성화하면 인터페이스 쌍이 제거됩니다.

단계 **7** **MTU** 필드에 최대 전송 단위(MTU)를 입력합니다.

MTU 값의 범위는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

주의 디바이스의 모든 비관리 인터페이스에 대해 최고 MTU 값을 변경하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 비관리 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

단계 **8** 트래픽이 우회 탐지에서 허용되어 디바이스로 계속 진행하도록 하려는 경우 **Failsafe**를 선택합니다.

매니지드 디바이스는 내부 트래픽 버퍼를 모니터링하고 버퍼가 꽉 차면 탐지를 우회합니다.

단계 **9** (7000/8000 시리즈에만 해당) 우회 모드를 지정합니다.

- 트래픽이 인터페이스를 통과하도록 하려면 우회를 클릭합니다.
- 트래픽을 차단하려면 우회 안 함을 클릭합니다.

참고 고가용성 쌍의 7000 또는 8000 Series 디바이스에 있는 인라인 집합, NGIPSv 디바이스의 인라인 집합, 8000 Series 디바이스에 있는 우회 이외의 NetMod 또는 Firepower 7115나 7125 디바이스의 SFP 모듈에 대해서는 우회 모드를 구성할 수 없습니다.

단계 **10** 필요한 경우 고급 설정을 구성하려면 고급 인라인 설정 옵션, 706 페이지의 내용을 참조하십시오.

단계 **11** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

7000 및 8000 Series 디바이스 및 NGIPSv의 MTU 범위, 695 페이지
Snort® 재시작 시나리오, 505 페이지

고급 인라인 설정 옵션

인라인 집합을 구성할 때 고려해야 할 몇 가지 고급 옵션이 있습니다.

탭 모드

탭 모드는 7000 및 8000 Series 디바이스에서 인라인 또는 fail-open 인터페이스를 포함하는 인라인 집합을 생성할 때 사용 가능합니다.

탭 모드에서는 디바이스가 인라인으로 구축되지만, 패킷 플로우가 디바이스를 통과하는 대신 각 패킷의 복사본이 디바이스로 전송되며 네트워크 트래픽 플로우가 방해받지 않습니다. 패킷 자체가 아니라 패킷의 복사본으로 작업하므로 삭제하도록 설정한 규칙 및 교체 키워드를 사용하는 규칙은 패킷 흐름에 영향을 주지 않습니다. 그러나 트리거되면 이런 유형의 규칙은 침입 이벤트를 생성하며 침입 이벤트의 테이블 보기는 인라인 구축에서 트리거링 패킷이 삭제되었을 수도 있음을 표시합니다.

인라인으로 구축된 디바이스에서 탭 모드를 사용하는 데에는 몇 가지 이점이 있습니다. 예를 들어 디바이스가 인라인 상태인 것처럼 디바이스와 네트워크 간에 케이블링을 설정할 수 있으며 디바이스가 생성하는 침입 이벤트의 종류를 분석할 수 있습니다. 결과를 기반으로 침입 정책을 수정할 수 있으며, 효율성 저하 없이 네트워크를 가장 잘 보호하는 삭제 규칙을 추가할 수 있습니다. 디바이스를 인라인으로 구축할 준비가 되면, 디바이스와 네트워크 간 케이블링을 다시 구성하지 않고도 탭 모드를 비활성화하고 의심스러운 트래픽의 삭제를 시작할 수 있습니다.

동일한 인라인 집합에서 이 옵션 및 Strict TCP Enforcement를 활성화할 수 없습니다.

링크 상태 전파

참고 가상 디바이스에서는 링크 상태 전파가 지원되지 않습니다. 7000 및 8000 Series 디바이스만 링크 상태 전파를 지원합니다.

링크 상태 전파는 인라인 집합의 두 쌍이 상태를 추적하도록 우회 모드 및 비 우회 모드에서 구성되는 인라인 집합의 기능입니다. 링크 상태 전파는 구리 및 파이버 구성 가능 우회 인터페이스에서 모두 사용할 수 있습니다.

링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 중단될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다. 장애가 발생한 인터페이스가 복원되면 두 번째 인터페이스도 자동으로 활성화됩니다. 다시 말해, 한 인터페이스의 링크 상태가 변경되면 어플라이언스는 변경 사항을 감지하고 다른 인터페이스의 링크 상태가 일치하도록 업데이트합니다. 어플라이언스가 링크 상태 변경사항을 전파하려면 최대 4초가 걸립니다.

링크 상태 전파는 라우터가 장애 상태인 네트워크 디바이스를 우회해 트래픽을 자동으로 다시 라우팅하도록 구성된 탄력적인 네트워크 환경에서 특히 유용합니다.

고가용성 쌍 내 7000 및 8000 Series 디바이스에 구성된 인라인 집합에 대한 링크 상태 전파를 비활성화할 수 없습니다.

투명 인라인 모드

투명 인라인 모드 옵션은 디바이스가 "bump in the wire" 역할을 수행하도록 합니다. 즉 디바이스는 소스 및 대상과 관계없이 발견되는 모든 네트워크 트래픽을 전달합니다. 7000 및 8000 Series디바이스에서는 이 옵션을 비활성화할 수 없습니다.

엄격한 **TCP** 시행

참고 가상 디바이스에서는 엄격한 TCP 시행이 지원되지 않습니다. 7000 및 8000 Series 디바이스만 이 옵션을 지원합니다. 또한 동일한 인라인 집합에서 이 옵션 및 탭 모드를 활성화할 수 없습니다.

TCP 보안을 극대화하기 위해 엄격한 시행을 활성화할 수 있으며 3방향 핸드셰이크가 완료되지 않은 연결이 차단됩니다. 엄격한 시행은 다음 항목도 차단합니다.

- 3방향 핸드셰이크가 완료되지 않은 연결의 비 SYN TCP 패킷
- TCP 연결의 응답자가 SYN-ACK를 보내기 전에 이니시에이터가 보낸 비 SYN/RST 패킷
- TCP 연결에서 SYN 이후/세션이 설정되기 전에 응답자가 보낸 비 SYN-ACK/RST 패킷
- 설정된 TCP 연결에서 이니시에이터 또는 Responder가 보낸 SYN 패킷

고급 인라인 집합 옵션 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 인라인 집합을 편집하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **4** 편집하려는 인라인 집합 옆에 있는 수정( )을 클릭합니다.

단계 **5** **Advanced(**고급**)**를 클릭합니다.

단계 **6** 고급 인라인 설정 옵션, 706 페이지의 설명에 따라 옵션을 구성합니다.

참고 가상 디바이스에서는 링크 상태 전파 및 엄격한 TCP 시행이 지원되지 않습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

인라인 집합 삭제

인라인 집합을 삭제할 때 그 집합에 지정되었던 모든 인라인 인터페이스는 다른 집합에 포함될 수 있게 됩니다. 인터페이스가 삭제되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 인라인 집합을 삭제하려는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **4** 삭제하려는 인라인 집합 옆에 있는 삭제( )을 클릭합니다.

단계 **5** 확인 메시지가 표시되면 인라인 집합 삭제를 확인합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

VI 부

Firepower Threat Defense 시작하기

- Firepower Threat Defense에 대한 투명 또는 라우팅 방화벽 모드, 711 페이지
- 다음 위치의 Firepower Threat Defense에 대한 논리적 디바이스 Firepower 4100/9300, 725 페이지

26 장

Firepower Threat Defense에 대한 투명 또는 라우팅 방화벽 모드

이 장에서는 방화벽 모드를 라우팅 또는 투명 모드로 설정하는 방법 및 각 방화벽 모드에서 방화벽이 어떻게 작동하는지에 대해 설명합니다.

참고 방화벽 모드는 일반 방화벽 인터페이스에만 영향을 주고 인라인 집합이나 패시브 인터페이스 등 IPS 전용 인터페이스에는 영향을 주지 않습니다. 두 개의 방화벽 모드 모두에서 IPS 전용 인터페이스를 사용할 수 있습니다. IPS 전용 인터페이스에 대한 자세한 내용은 Firepower Threat Defense 인라인 집합 및 패시브 인터페이스, 847 페이지의 내용을 참조하십시오. 인라인 집합은 "투명 인라인 집합"으로 익숙할 수 있지만 인라인 인터페이스 유형은 이 장 및 방화벽 유형 인터페이스에서 설명한 투명 방화벽 모드와는 관련이 없습니다.

- 방화벽 모드 정보, 711 페이지
- 기본 설정, 720 페이지
- 방화벽 모드에 대한 지침, 721 페이지
- 방화벽 모드 설정, 722 페이지

방화벽 모드 정보

Firepower Threat Defense 디바이스에서는 일반 방화벽 인터페이스에 대해 두 가지 방화벽 모드(라우팅 방화벽 모드 및 투명 방화벽 모드)를 지원합니다.

라우팅 방화벽 모드 정보

라우팅 모드에서 Firepower Threat Defense 디바이스는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다.

통합 라우팅 및 브리징을 통해 네트워크에서 여러 인터페이스를 그룹화하는 "브리지 그룹"을 사용할 수 있으며, Firepower Threat Defense 디바이스에서는 브리징 기술을 사용하여 인터페이스 간에 트래픽을 통과시킵니다. 각 브리지 그룹에는 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)

가 있습니다. Firepower Threat Defense 디바이스에서는 BVI와 일반 라우팅 인터페이스 간을 라우팅합니다. 클러스터링, EtherChannel, 이중 멤버 인터페이스가 필요하지 않은 경우, 투명 모드 대신 라우팅 모드를 사용하는 것을 고려할 수 있습니다. 라우팅 모드에서는 투명 모드에서와 같이 하나 이상의 격리된 브리지 그룹을 가질 수 있지만, 혼합 구축을 위한 일반적인 라우팅 인터페이스도 가집니다.

투명 방화벽 모드 정보

일반적으로 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다. 그러나 다른 방화벽과 마찬가지로 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다.

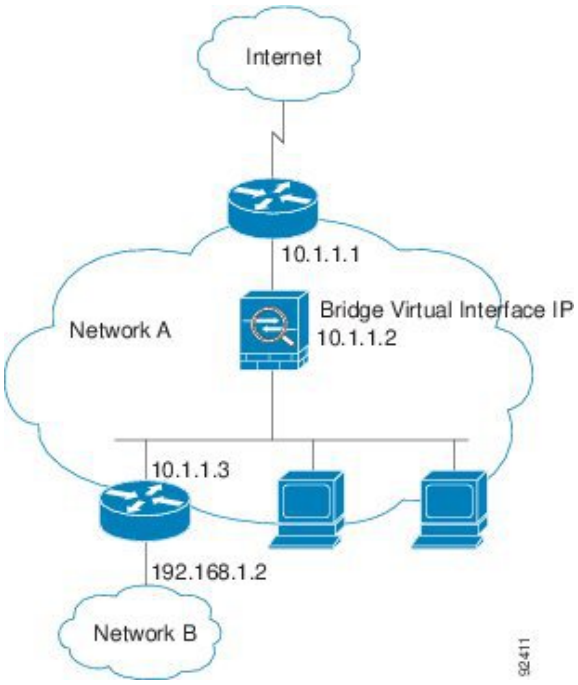
Layer 2 연결성은 네트워크의 내부 및 외부 인터페이스를 그룹화하는 "브리지 그룹"을 사용하여 획득할 수 있으며, Firepower Threat Defense 디바이스에서는 브리징 기술을 사용하여 인터페이스 간에 트래픽을 통과시킵니다. 각 브리지 그룹은 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)를 포함합니다. 여러 네트워크에 대해 여러 개의 브리지 그룹을 사용할 수 있습니다. 투명 모드에서 이러한 브리지 그룹은 서로 통신할 수 없습니다.

네트워크에서 투명 방화벽 사용

Firepower Threat Defense 디바이스에서는 인터페이스 간의 동일한 네트워크를 연결합니다. 방화벽은 라우팅 홉이 아니므로, 투명 모드를 기존 네트워크에서 쉽게 도입할 수 있습니다.

다음 그림에는 외부 디바이스가 내부 디바이스와 동일한 서브넷에 존재하는 일반적인 투명 방화벽 네트워크가 나와 잇습니다. 내부 라우터와 호스트는 외부 라우터에 직접 연결되어 있는 것으로 표시됩니다.

그림 7: 투명 방어벽 네트워크



진단 인터페이스

각 BVI(Bridge Virtual Interface) IP 주소 이외에도 브리지 그룹에 속하지 않은 별도의 진단 슬롯/포트 인터페이스를 추가할 수 있으며, 이렇게 하면 Firepower Threat Defense 디바이스에는 관리 트래픽만 허용됩니다.

라우팅 모드 기능의 트래픽 전달

투명 방화벽에서 직접 지원되지 않는 기능의 경우, 업스트림 및 다운스트림 라우터를 통해 트래픽이 전달되도록 허용하여 해당 기능을 지원할 수 있습니다. 예를 들어, 액세스 규칙을 사용하여 DHCP 트래픽(지원되지 않는 DHCP 릴레이 기능 대신) 또는 IP/TV에서 생성된 것과 같은 멀티캐스트 트래픽을 허용할 수 있습니다. 또한 투명 방화벽을 통해 라우팅 프로토콜 인접성을 설정할 수도 있습니다. 액세스 규칙을 기반으로 OSPF, RIP, EIGRP 또는 BGP 트래픽의 통과를 허용할 수 있습니다. 마찬가지로, HSRP 또는 VRRP와 같은 프로토콜이 Firepower Threat Defense 디바이스를 통과할 수 있습니다.

브리지 그룹 정보

브리지 그룹은 Firepower Threat Defense 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 브리지 그룹은 투명 방화벽 모드와 라우팅 방화벽 모드에서 지원됩니다. 다른 방화벽 인터페이스와 마찬가지로 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다.

BVI(Bridge Virtual Interface)

각 브리지 그룹에는 BVI(Bridge Virtual Interface)가 있습니다. Firepower Threat Defense 디바이스에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 BVI IP 주소를 사용합니다. BVI IP 주소는 브리지 그룹 멤버 인터페이스와 동일한 서브넷에 있어야 합니다. BVI는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

투명 모드에서는 브리지 그룹 멤버 인터페이스만 이름이 지정되고 인터페이스 기반 기능과 함께 사용될 수 있습니다.

라우팅 모드에서는 BVI가 브리지 그룹 및 기타 라우팅 인터페이스 간에 게이트웨이 역할을 합니다. 브리지 그룹/라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다. 일부 인터페이스 기반 기능에는 BVI 자체를 사용할 수 있습니다.

- DHCPv4 서버 — BVI에서만 DHCPv4 서버 구성을 지원합니다.
- 고정 경로 — BVI에 대한 고정 경로는 구성할 수 있지만, 멤버 인터페이스에 대한 고정 경로는 구성할 수 없습니다.
- Firepower Threat Defense 디바이스에서 시작되는 기타 트래픽 및 syslog 서버 — syslog 서버(또는 SNMP 서버나 Firepower Threat Defense 디바이스에서 트래픽이 시작되는 기타 서비스)를 지정하는 경우 BVI 또는 멤버 인터페이스를 지정할 수 있습니다.

라우팅 모드에서 BVI 이름을 지정하지 않는 경우 Firepower Threat Defense 디바이스에서는 브리지 그룹 트래픽을 라우팅하지 않습니다. 이 구성을 사용하면 브리지 그룹에 대한 투명 방화벽 모드가 복제됩니다. 클러스터링, EtherChannel, 이중 멤버 인터페이스가 필요하지 않은 경우, 라우팅 모드를 대신 사용하는 것을 고려할 수 있습니다. 라우팅 모드에서는 투명 모드에서와 같이 하나 이상의 격리된 브리지 그룹을 가질 수 있지만, 혼합 구축을 위한 일반적인 라우팅 인터페이스도 가집니다.

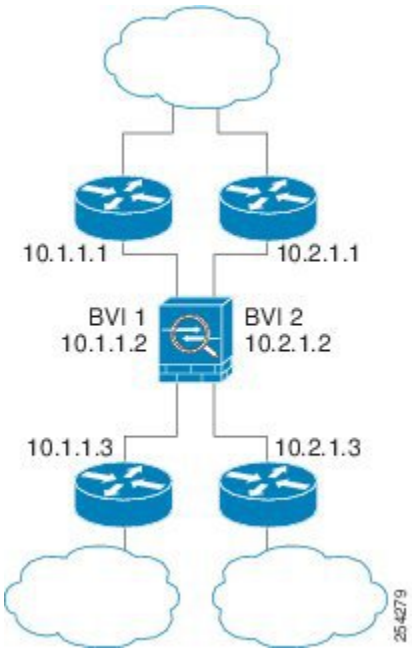
투명 방화벽 모드의 브리지 그룹

브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 트래픽은 Firepower Threat Defense 디바이스 내의 다른 브리지 그룹으로 라우팅되지 않으며, 트래픽은 외부 라우터에 의해 Firepower Threat Defense 디바이스의 다른 브리지 그룹으로 다시 라우팅되기 전에 Firepower Threat Defense 디바이스에서 나가야 합니다. 브리지 기능은 브리지 그룹마다 따로 있지만, 다른 여러 기능은 모든 브리지 그룹이 공유합니다. 예를 들어, 모든 브리지 그룹은 syslog 서버 또는 AAA 서버 컨피그레이션을 공유합니다.

브리지 그룹당 여러 인터페이스를 포함할 수 있습니다. 지원되는 브리지 그룹 및 인터페이스의 정확한 수는 방화벽 모드에 대한 지침, 721 페이지의 내용을 참조하십시오. 브리지 그룹당 3개 이상의 인터페이스를 사용하는 경우, 동일한 네트워크에 있는 여러 세그먼트 간의 통신은 제어할 수 있지만 내부 및 외부 간의 통신은 제어할 수 없습니다. 예를 들어, 서로 통신하는 것을 허용하지 않을 내부 세그먼트가 3개 있는 경우, 각 세그먼트를 개별 인터페이스에 두고 외부 인터페이스하고만 통신하도록 허용할 수 있습니다. 또는 원하는 만큼만 액세스하는 것을 허용하기 위해 인터페이스 간에 액세스 규칙을 맞춤화할 수 있습니다.

다음 그림에는 2개의 브리지 그룹이 있는 Firepower Threat Defense 디바이스에 연결된 2개의 네트워크가 나와 있습니다.

그림 8: 2개의 브리지 그룹이 있는 투명 방화벽 네트워크

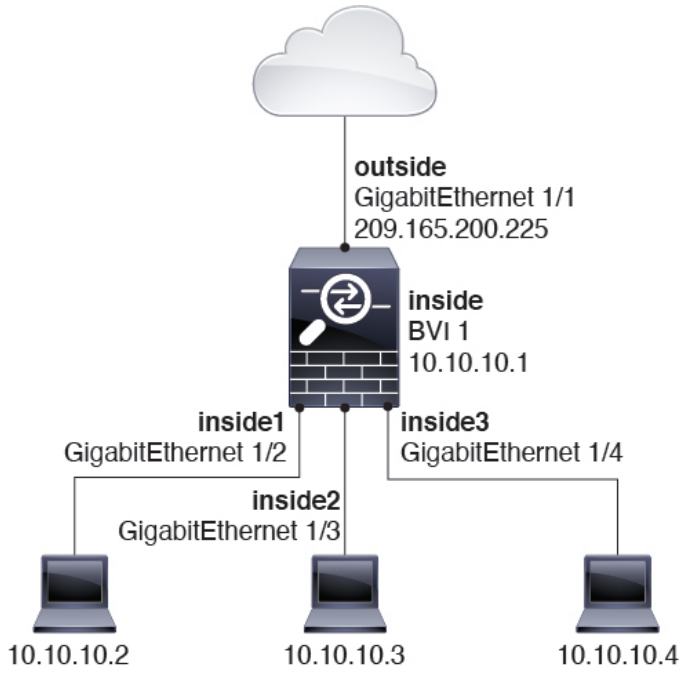


라우팅 방화벽 모드의 브리지 그룹

브리지 그룹 트래픽은 다른 브리지 그룹 또는 라우팅 인터페이스로 라우팅될 수 있습니다. 브리지 그룹의 BVI 인터페이스에 이름을 할당하지 않는 방법을 통해 브리지 그룹 트래픽을 격리하도록 선택할 수 있습니다. BVI에 이름을 지정하면 BVI에서는 다른 일반 인터페이스와 마찬가지로 라우팅에 참여합니다.

라우팅 모드에서 브리지 그룹을 사용하는 방식 중 하나는 외부 스위치 대신 FTD에서 추가 인터페이스를 사용하는 것입니다. 예를 들어 일부 디바이스에 대한 기본 구성에서는 외부 인터페이스를 일반 인터페이스로 포함한 다음, 내부 브리지 그룹에 할당된 기타 모든 인터페이스를 포함합니다. 이 브리지 그룹의 목적이 외부 스위치를 교체하는 것이므로 모든 브리지 그룹 인터페이스가 자유롭게 통신할 수 있도록 액세스 정책을 구성해야 합니다.

그림 9: 내부 브리지 그룹 및 외부 라우팅 인터페이스를 사용하는 라우팅 방화벽 네트워크



Layer 3 트래픽 허용

- 유니캐스트 IPv4 및 IPv6 트래픽을 사용하려면 액세스 규칙이 브리지 그룹을 통과하는 것이 허용되어야 합니다.
- ARP는 액세스 규칙 없이도 양방향에서 브리지 그룹을 통과할 수 있습니다. ARP 트래픽은 ARP 감시로 제어할 수 있습니다.
- IPv6 네이버 검색 및 라우터 요청 패킷은 액세스 규칙을 사용하여 전달될 수 있습니다.
- 액세스 규칙을 사용하여 브로드캐스트 및 멀티캐스트 트래픽을 전달할 수 있습니다.

허용되는 MAC 주소

액세스 정책에서 허용하는 경우 다음과 같은 대상 MAC 주소가 브리지 그룹을 통과할 수 있습니다 (Layer 3 트래픽 허용, 716 페이지 참조). 이 목록에 없는 모든 MAC 주소는 손실됩니다.

- FFFF.FFFF.FFFF와 같은 TRUE 브로드캐스트 목적지 MAC 주소
- 0100.5E00.0000에서 0100.5EFE.FFFF 사이의 IPv4 멀티캐스트 MAC 주소
- 3333.0000.0000에서 3333.FFFF.FFFF 사이의 IPv6 멀티캐스트 MAC 주소
- 0100.0CCC.CCCD와 같은 BPDU 멀티캐스트 주소

BPDU 처리

Spanning Tree Protocol을 사용하여 루프를 방지하기 위해 기본적으로 BPDU가 전달됩니다.

기본적으로 BPDU는 고급 검사에 포워딩되며 이런 유형의 패킷에 필수 사항은 아니지만 예를 들어 검사 재시작을 위해 차단될 경우 문제가 발생할 수도 있습니다. 고급 검사에서 BPDU를 항상 제외하는 것이 좋습니다. 이를 위해 FlexConfig를 사용하여 BPDU를 신뢰하고 각 구성원 인터페이스에 대한 고급 검사에서 이를 제외하는 EtherType ACL을 설정합니다. Firepower Threat Defense에 대한 FlexConfig 정책, 1269 페이지의 내용을 참조하십시오.

FlexConfig 개체는 다음 명령을 배포하여 <if-name>을 인터페이스 이름으로 교체합니다. 디바이스에서 각 브리지 그룹 멤버 인터페이스를 처리하기 위한 액세스 그룹 명령을 필요한 만큼 추가합니다. ACL에 다른 이름을 선택할 수도 있습니다.

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

MAC 주소 대 경로 조회 비교

브리지 그룹 내 트래픽의 경우 패킷의 발신 인터페이스는 경로 조회 대신 대상 MAC 주소 조회를 수행하여 확인할 수 있습니다.

그러나 다음과 같은 상황에는 경로 조회가 필요합니다.

- Firepower Threat Defense 디바이스에서 시작되는 트래픽 — 예를 들어, syslog 서버가 위치한 원격 네트워크로 향하는 트래픽을 위해 Firepower Threat Defense 디바이스에서 기본/고정 경로를 추가합니다.
- VoIP(Voice over IP) 및 TFTP 트래픽, 1홉 이상 떨어져 있는 엔드포인트 — 보조 연결에 성공하도록 원격 엔드포인트로 향하는 트래픽을 위해 Firepower Threat Defense 디바이스에서 고정 경로를 추가합니다. Firepower Threat Defense 디바이스에서는 보조 연결을 허용하기 위해 액세스 제어 정책에서 임시 "핀홀"을 생성합니다. 연결에서 기본 연결보다 다양한 IP 주소 집합을 사용할 수 있기 때문에, Firepower Threat Defense 디바이스에서는 올바른 인터페이스에서 핀홀을 설치하기 위해 경로 조회를 수행해야 합니다.

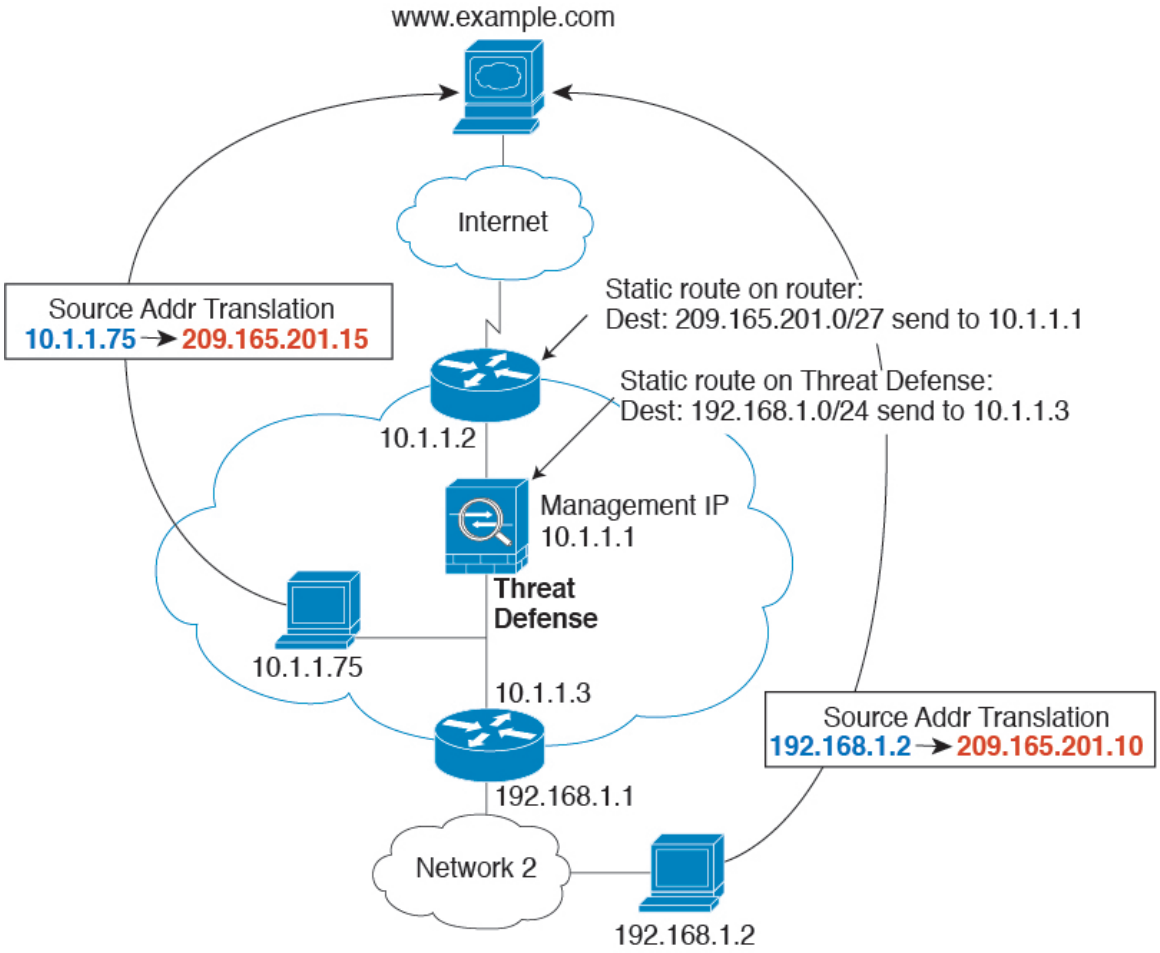
  영향을 받는 애플리케이션은 다음과 같습니다.

  - H.323
  - RTSP
  - SIP
  - Skinny(SCCP)
  - SQL*Net
  - SunRPC
  - TFTP

- Firepower Threat Defense 디바이스에서 NAT를 수행하는 1홉 이상 떨어져 있는 트래픽 — 원격 네트워크로 향하는 트래픽을 위해 Firepower Threat Defense 디바이스에서 고정 경로를 구성합니다. 또한 Firepower Threat Defense 디바이스로 전송될 매핑된 주소로 향하는 트래픽을 위해 업스트림 라우터에 고정 경로가 필요합니다.

  이 라우팅 요구 사항은 NAT가 활성화되어 있는 DNS 및 VoIP용 임베디드 IP 주소에도 마찬가지로 적용되며, 임베디드 IP 주소는 1홉 이상 떨어져 있습니다. Firepower Threat Defense 디바이스에서는 올바른 이그레스 인터페이스를 식별해야 변환을 수행할 수 있습니다.

그림 ***10: NAT*** 예: 브리지 그룹 내부의 ***NAT***



투명 모드의 브리지 그룹에 대해 지원되지 않는 기능

다음 표에는 투명 모드의 브리지 그룹에서 지원되지 않는 기능이 나와 있습니다.

표 ***66:*** 투명 모드에서 지원되지 않는 기능

기능	설명
동적 DNS	—

기능	설명
DHCP 릴레이	투명 방화벽에서는 DHCPv4 서버 역할을 수행할 수 있으나, DHCP 릴레이를 지원하지는 않습니다. 2개의 액세스 규칙을 사용하여 DHCP 트래픽이 통과되도록 할 수 있으므로 DHCP 릴레이가 필요하지 않습니다. 이러한 액세스 규칙 중 하나는 DHCP 요청이 내부 인터페이스에서 외부 인터페이스로 전달되도록 하고, 나머지 하나는 서버의 응답을 다른 방향으로 전달할 수 있도록 합니다.
동적 라우팅 프로토콜	그러나 브리지 그룹 멤버 인터페이스의 Firepower Threat Defense 디바이스에서 시작된 트래픽에 대한 고정 경로를 추가할 수 있습니다. 또한 액세스 규칙을 사용하여 동적 라우팅 프로토콜이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다.
멀티캐스트 IP 라우팅	액세스 규칙에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다.
QoS	—
통과 트래픽의 VPN 종료	투명 방화벽에서는 브리지 그룹 멤버 인터페이스에서만 관리 연결에 Site-to-Site VPN 터널을 지원합니다. 그러나 이로 인해 Firepower Threat Defense 디바이스를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 액세스 규칙을 사용하여 VPN 트래픽이 ASA를 통과하도록 할 수 있으나, 이로 인해 관리 이외 연결이 종료되지는 않습니다.

라우팅 모드의 브리지 그룹에 대해 지원되지 않는 기능

다음 표에는 라우팅 모드의 브리지 그룹에서 지원되지 않는 기능이 나와 있습니다.

표 ***67:*** 라우팅 모드에서 지원되지 않는 기능

기능	설명
EtherChannel 멤버 인터페이스	물리적 인터페이스, 이중 인터페이스 및 하위 인터페이스만 브리지 그룹 멤버 인터페이스로 지원됩니다. 진단 인터페이스도 지원되지 않습니다.
클러스터링	브리지 그룹은 클러스터링에서 지원되지 않습니다.

기능	설명
동적 DNS	—
DHCP 릴레이	라우팅 방화벽은 DHCPv4 서버로 작동할 수 있지만, BVI 또는 브리지 그룹 멤버 인터페이스에서 DHCP 릴레이를 지원하지는 않습니다.
동적 라우팅 프로토콜	그러나 BVI에 고정 경로를 추가할 수 있습니다. 또한 액세스 규칙을 사용하여 동적 라우팅 프로토콜이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다. 비 브리지 그룹 인터페이스에서는 동적 라우팅을 지원합니다.
멀티캐스트 IP 라우팅	액세스 규칙에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 Firepower Threat Defense 디바이스를 통과하도록 할 수 있습니다. 비 브리지 그룹 인터페이스에서는 멀티캐스트 라우팅을 지원합니다.
QoS	비 브리지 그룹 인터페이스에서는 QoS를 지원합니다.
통과 트래픽의 VPN 종료	BVI에서 VPN 연결을 종료할 수 없습니다. 비 브리지 그룹 인터페이스에서는 VPN을 지원합니다. 브리지 그룹 멤버 인터페이스에서는 관리 연결에만 Site-to-Site VPN 터널을 지원합니다. 그러나 이로 인해 Firepower Threat Defense 디바이스를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 액세스 규칙을 사용하여 VPN 트래픽이 브리지 그룹을 통과하도록 할 수 있으나, 이로 인해 관리 이외 연결이 종료되지는 않습니다.

기본 설정

브리지 그룹 기본값

기본적으로 모든 ARP 패킷은 브리지 그룹 내에서 전달됩니다.

방화벽 모드에 대한 지침

모델 지침

- 브리지 ixgbevf 인터페이스를 사용하는 VMware의 Firepower Threat Defense Virtual의 경우 브리지 그룹이 지원되지 않습니다.
- Firepower 2100 Series의 경우, 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.

브리지 그룹 지침(투명 모드 및 라우팅 모드)

- 브리지 그룹당 64개의 인터페이스가 있는 최대 250개의 브리지 그룹을 생성할 수 있습니다.
- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.
- Firepower Threat Defense 디바이스는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.
- IPv4에서는 관리 트래픽과 Firepower Threat Defense 디바이스를 거칠 트래픽 모두 브리지 그룹마다 BVI용 IP 주소가 필요합니다. IPv6 주소는 지원되지만 BVI에는 필요하지 않습니다.
- IPv6 주소만 수동으로 구성할 수 있습니다.
- BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다.
- 관리 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- Firepower 1010의 경우, 동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수 없습니다.
- Firepower 4100/9300의 경우, 데이터 공유 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- 투명 모드에서는 1개 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.
- 투명 모드에서는 BVI IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 Firepower Threat Defense 디바이스의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.
- 투명 모드에서는 관리 트래픽의 반환 경로를 제공하는 데 필요한 기본 경로가 하나의 브리지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브리지 그룹의 인터페이스 및 브리지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브리지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 일반 고정 경로를 지정해야 합니다.
- 투명 모드에서 PPPoE는 진단 인터페이스에 대해 지원되지 않습니다.
- 라우팅 모드에서 브리지 그룹 및 기타 라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다.

- 라우팅 모드에서 FTD 정의된 EtherChannel 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 브리지 그룹 멤버를 사용할 때 FTD를 통과하는 것이 허용되지 않습니다. BFD를 실행하는 FTD의 양쪽 측면에 두 개의 네이버가 있는 경우, FTD는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.

방화벽 모드 설정

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

CLI에서 초기 시스템 설정을 수행할 때 방화벽 모드를 설정할 수 있습니다. 방화벽 모드 변경은 설정을 삭제하므로 호환되지 않는 설정이 없도록 설정 중 방화벽 모드를 설정하는 것을 권장합니다. 나중에 방화벽 모드를 변경하려면 CLI에서 변경해야 합니다.

프로시저

단계 **1** FMC에서 FTD 디바이스를 등록 취소합니다.

디바이스를 등록 취소할 때까지 모드를 변경할 수 없습니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
b) 매니지드 디바이스 목록에서 디바이스를 선택합니다.
c) 디바이스를 삭제(휴지통 클릭)한 뒤 확인하고 시스템이 디바이스를 제거할 때까지 기다립니다.

단계 **2** FTD 디바이스 CLI에 액세스합니다. 콘솔 포트에서 액세스하는 것이 좋습니다.

진단 인터페이스에 SSH를 사용하면 모드를 변경할 때 인터페이스 설정을 삭제하며 연결이 끊어집니다. 그 경우 관리 인터페이스에 연결해야 합니다.

단계 **3** 방화벽 모드 변경

configure firewall[**routed** | **transparent**]

예제**:**

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

단계 **4** FMC로 다시 등록:

configure manager add {*hostname* | *ip_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *ip_address* | **DONTRESOLVE** }는 FMC의 완전히 검증된 호스트 명 또는 IP 주소를 지정합니다. FMC의 주소를 직접 지정할 수 없는 경우 **DONTRESOLVE**를 사용합니다.
- *reg_key*는 디바이스를 FMC에 등록하는 데 필요한 고유 영숫자 등록 키입니다.
- *nat_id*는 FMC와 장치 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 호스트 이름이 **DONTRESOLVE**로 설정된 경우 반드시 필요합니다.

27 장

다음 위치의 Firepower Threat Defense에 대한 논리적 디바이스 Firepower 4100/9300

Firepower 4100/9300은 하나 이상의 논리적 디바이스를 설치할 수 있는 유연한 보안 플랫폼입니다. FTD을 FMC에 추가하기 전에 섀시 인터페이스를 구성하고 논리적 디바이스를 추가하고 Firepower Chassis Manager 또는 FXOS CLI를 사용하는 Firepower 4100/9300 섀시의 디바이스에 인터페이스를 할당해야 합니다. 이 장에서는 기본 인터페이스 구성 및 Firepower Chassis Manager를 사용하여 독립형 디바이스 또는 고가용성 논리적 디바이스를 추가하는 방법을 설명합니다. 클러스터형 논리적 디바이스를 추가하려면 Firepower Threat Defense 클러스터링, 917 페이지의 내용을 참조하십시오. FXOS CLI를 사용하려면 FXOS CLI 구성 가이드를 참조하십시오. 고급 FXOS 절차 및 트러블슈팅에 대한 자세한 내용은 FXOS 구성 가이드를 참조하십시오.

- Firepower 인터페이스 정보, 725 페이지
- 논리적 디바이스 정보, 740 페이지
- 컨테이너 인스턴스용 라이선스, 748 페이지
- 논리적 디바이스의 요구 사항 및 사전 요구 사항, 749 페이지
- 논리적 디바이스 관련 지침 및 제한 사항, 753 페이지
- 인터페이스 구성, 756 페이지
- 논리적 디바이스 구성, 761 페이지
- History for Firepower Threat Defense Logical Devices, 773 페이지

Firepower 인터페이스 정보

Firepower 4100/9300 섀시에서는 물리적 인터페이스, 컨테이너 인스턴스용 VLAN 하위 인터페이스 및 EtherChannel(포트-채널) 인터페이스를 지원합니다. EtherChannel 인터페이스는 동일한 유형의 멤버 인터페이스를 최대 16개까지 포함할 수 있습니다.

섀시 관리 인터페이스

섀시 관리 인터페이스는 SSH 또는 Firepower Chassis Manager를 통한 FXOS 섀시 관리에 사용됩니다. 이 인터페이스는 **Interfaces(**인터페이스**)** 탭의 상단에 **MGMT**로 표시되며 **Interfaces(**인터페이스**)** 탭

에서 이 인터페이스를 활성화하거나 비활성화할 수만 있습니다. 이 인터페이스는 애플리케이션 관리용 논리적 디바이스에 할당하는 관리 유형 인터페이스와는 별개입니다.

이 인터페이스의 파라미터는 CLI에서 구성해야 합니다. FXOS CLI에서 이 인터페이스에 대한 정보를 확인하려면 로컬 관리에 연결한 다음 관리 포트를 표시합니다.

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

실제 케이블이나 SFP 모듈 연결을 해제하거나 **mgmt-port shut** 명령을 수행하더라도 섀시 관리 인터페이스는 계속 작동합니다.

참고 섀시 관리 인터페이스는 점보 프레임을 지원하지 않습니다.

인터페이스 유형

각 인터페이스는 다음 유형 중 하나일 수 있습니다.

- Data(데이터) - 일반 데이터에 사용합니다. 데이터 인터페이스는 논리적 디바이스 간에 공유할 수 없으며 논리적 디바이스는 백플레인을 통해 다른 논리적 디바이스와 통신할 수 없습니다. 데이터 인터페이스의 트래픽의 경우, 모든 트래픽은 하나의 인터페이스에서 섀시를 종료하고 다른 인터페이스로 돌아가서 다른 논리적 디바이스에 연결해야 합니다.
- Data-sharing(데이터 공유) - 일반 데이터에 사용합니다. 컨테이너 인스턴스에서만 지원되는 이러한 데이터 인터페이스는 하나 이상의 논리적 디바이스/컨테이너 인스턴스(FTD-using-FMC 전용)에서 공유할 수 있습니다. 각 컨테이너 인스턴스는 이 인터페이스를 공유하는 다른 모든 인스턴스와 백플레인을 통해 통신할 수 있습니다. 공유 인터페이스는 구축할 수 있는 컨테이너 인스턴스 수에 영향을 줄 수 있습니다. 브리지 그룹 멤버 인터페이스(투명 모드 또는 라우팅 모드), 인라인 집합, 패시브 인터페이스, 클러스터, 또는 페일오버 링크에 대해서는 공유 인터페이스가 지원되지 않습니다.
- Mgmt(관리) - 애플리케이션 인스턴스를 관리하는 데 사용합니다. 이러한 인터페이스는 외부 호스트에 액세스하기 위해 하나 이상의 논리적 디바이스에서 공유할 수 있습니다. 단, 논리적 디바이스에서는 인터페이스를 공유하는 다른 논리적 디바이스와 이 인터페이스를 통해 통신할 수 없습니다. 논리적 디바이스당 관리 인터페이스 1개만 할당할 수 있습니다. ASA, 의 경우: 나중에 데이터 인터페이스에서 관리를 활성화할 수 있습니다. 데이터 관리를 활성화한 후 사용하지 않으려는 경우에도 관리 인터페이스를 논리적 디바이스에 할당해야 합니다.개별 섀시 관리 인터페이스에 대한 내용은 섀시 관리 인터페이스, 725 페이지를 참조하십시오.
- Cluster(클러스터) - 클러스터형 논리적 디바이스용 클러스터 제어 링크로 사용합니다. 기본적으로, 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다. 이 클러스터 유형은 EtherChannel 인터페이스에서만 지원됩니다. 다중 인스턴스 클러스터링의 경우 디바이스 간에 클러스터 유형 인터페이스를 공유할 수 없습니다. VLAN 하위 인터페이스를 클러스터 EtherChannel에 추가하여 클러스터당 별도의 클러스터 제어 링크를 제공할 수 있습니다. 클러스터 인터페이스에 하위 인터페이스를 추가하면 네이티브 클러스터에서 해당 인터페이스를 사용할 수 없습니다. FDM은(는) 클러스터링을 지원하지 않습니다.

독립형 및 클러스터 구축에서 FTD 및 ASA 애플리케이션에 대한 인터페이스 유형 지원은 다음 표를 참조하십시오.

표 *68:* 인터페이스 유형 지원

애플리케이션		Data(데이터)	데이터: 하위 인터페이스	데이터 공유	데이터 공유: 하위 인터페이스	관리	Firepower Event	클러스터 (EtherChannel에만 해당)	클러스터: 하위 인터페이스
FTD	독립형 네이티브 인스턴스	예	—	—	—	예	예	—	—
	독립형 컨테이너 인스턴스	예	예	예	예	예	예	—	—
	클러스터 기본 인스턴스	예 (섀시 간 클러스터 전용 EtherChannel)	—	—	—	예	예	예	—
	클러스터 컨테이너 인스턴스	예 (섀시 간 클러스터 전용 EtherChannel)	—	—	—	예	예	예	예
ASA	독립형 네이티브 인스턴스	예	—	—	—	예	—	예	—
	클러스터 기본 인스턴스	예 (섀시 간 클러스터 전용 EtherChannel)	—	—	—	예	—	예	—

FXOS 인터페이스와 애플리케이션 인터페이스 비교

Firepower 4100/9300에서는 물리적 인터페이스, 컨테이너 인스턴스용 VLAN 하위 인터페이스 및 EtherChannel(포트-채널) 인터페이스의 기본 이더넷 설정을 관리합니다. 애플리케이션 내에서는 상위 레벨 설정을 구성합니다. 예를 들어 FXOS에서는 Etherchannel만 생성할 수 있습니다. 그러나 애플리케이션 내의 EtherChannel에 IP 주소를 할당할 수 있습니다.

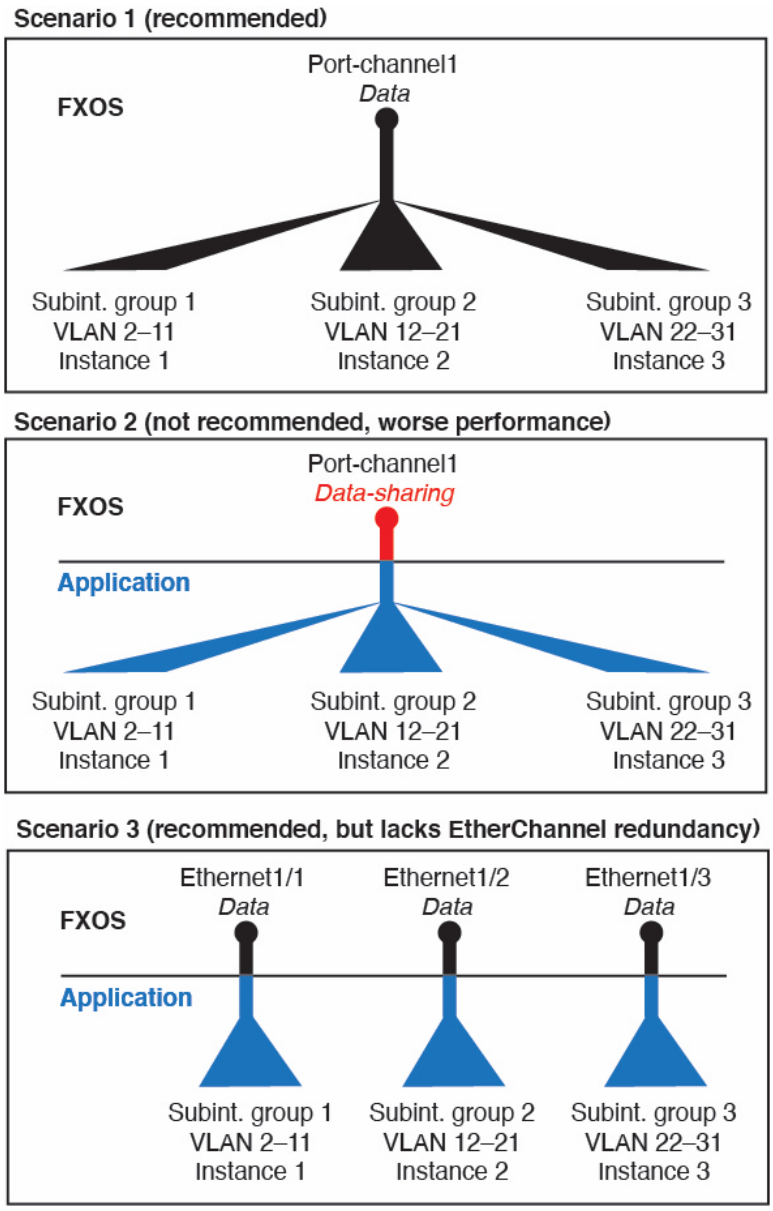
다음 섹션에서는 FXOS와 인터페이스에 대한 애플리케이션 간의 상호 작용에 대해 설명합니다.

VLAN 하위 인터페이스

논리적 디바이스의 경우에는 애플리케이션 내에서 VLAN 하위 인터페이스를 생성할 수 있습니다.

독립형 모드만의 컨테이너 인스턴스의 경우에는 또한 FXOS(FXOS 하위 인터페이스가 없는 인터페이스)에서 VLAN 하위 인터페이스를 생성할 수도 있습니다. 다중 인스턴스 클러스터는 클러스터 유형 인터페이스를 제외하고는 FXOS에서 하위 인터페이스를 지원하지 않습니다. 애플리케이션 정의 하위 인터페이스는 FXOS 제한에 영향을 받지 않습니다. 네트워크 구축 및 개인 기본 설정에 따라 하위 인터페이스를 생성할 운영 체제를 선택합니다. 예를 들어 하위 인터페이스를 공유하려면 FXOS에서 하위 인터페이스를 생성해야 합니다. FXOS 하위 인터페이스를 이용하는 또 다른 시나리오는 단일 인터페이스에서 하위 인터페이스 그룹을 여러 인스턴스로 할당하는 것입니다. 인스턴스 A에는 VLAN 2~11이, 인스턴스 B에는 VLAN 12~21, 인스턴스 C에는 VLAN 22~31이 있는 Port-channel1을 사용하려는 경우를 예로 들어 보겠습니다. 애플리케이션 내에서 이러한 하위 인터페이스를 생성하는 경우에는 FXOS에서 상위 인터페이스를 공유해야 하는데, 이러한 방식은 효율적이지 않을 수 있습니다. 다음 그림에서 이 시나리오를 수행할 수 있는 세 가지 방법을 참조하십시오.

그림 *11: FXOS*의 *VLAN* 및 컨테이너 인스턴스의 애플리케이션의 비교



섀시와 애플리케이션의 독립 인터페이스 상태

관리를 위해 섀시와 애플리케이션에서 인터페이스를 활성화하고 비활성화할 수 있습니다. 인터페이스는 두 운영 체제에서 모두 활성화해야 작동합니다. 인터페이스 상태는 독립적으로 제어되므로 섀시와 애플리케이션에서 상태가 일치하지 않을 수도 있습니다.

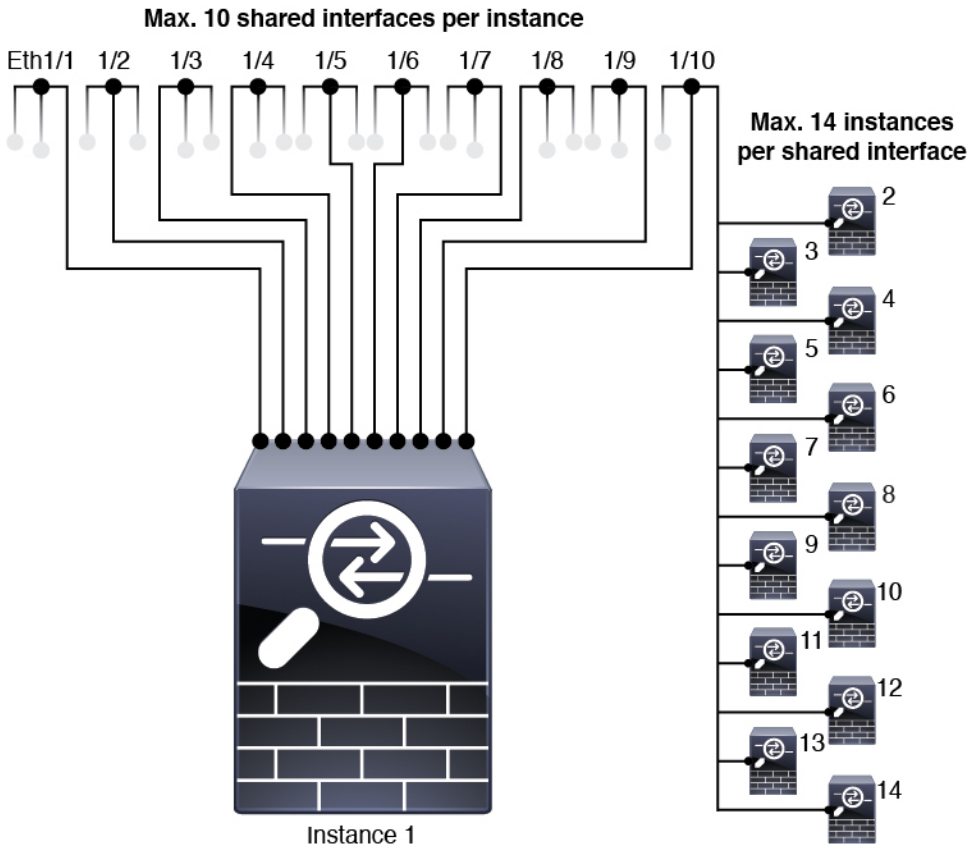
애플리케이션 내의 인터페이스 기본 상태는 인터페이스 유형에 따라 달라집니다. 예를 들어 물리적 인터페이스 또는 EtherChannel은 애플리케이션 내에서 기본적으로 비활성화되지만 하위 인터페이스는 기본적으로 활성화됩니다.

공유 인터페이스 확장성

컨테이너 인스턴스는 데이터 공유 유형 인터페이스를 공유할 수 있습니다. 이 기능을 통해 물리적 인터페이스 사용량을 절약하면서 유연한 네트워킹 구축도 지원할 수 있습니다. 인터페이스를 공유할 때 섀시는 고유한 MAC 주소를 사용하여 올바른 인스턴스로 트래픽을 포워딩합니다. 그러나 공유 인터페이스로 인해 섀시 내에 전체 메시 토폴로지가 필요해져서 포워딩 테이블이 커질 수 있습니다. 모든 인스턴스가 동일한 인터페이스를 공유하는 다른 모든 인스턴스와 통신할 수 있어야 하기 때문입니다. 따라서 공유할 수 있는 인터페이스 수에는 제한이 있습니다.

섀시는 포워딩 테이블 외에 VLAN 하위 인터페이스 포워딩용 VLAN 그룹 테이블도 유지합니다.최대 500개의 VLAN 하위 인터페이스를 생성할 수 있습니다.

공유 인터페이스 할당과 관련한 다음 제한을 참조하십시오.



공유 인터페이스 모범 사례

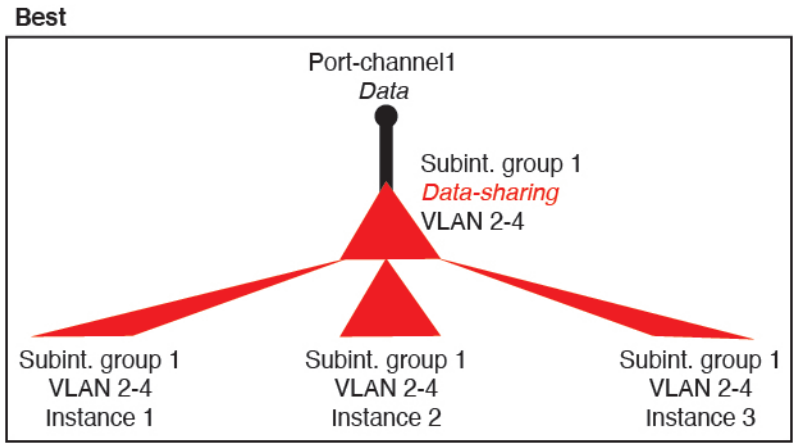
포워딩 테이블의 최적의 확장성을 위해 최대한 적은 수의 인터페이스를 공유합니다. 대신, 하나 이상의 물리적 인터페이스에서 최대 500개의 VLAN 하위 인터페이스를 생성하고 컨테이너 인스턴스 사이에 VLAN을 나눌 수 있습니다.

인터페이스 공유 시에는 다음 사례를 확장성이 높은 방식부터 차례로 따르십시오.

1. 최고 - 단일 상위 인터페이스에 속한 하위 인터페이스를 공유하고 동일한 인스턴스 그룹과 동일한 하위 인터페이스 집합을 사용합니다.

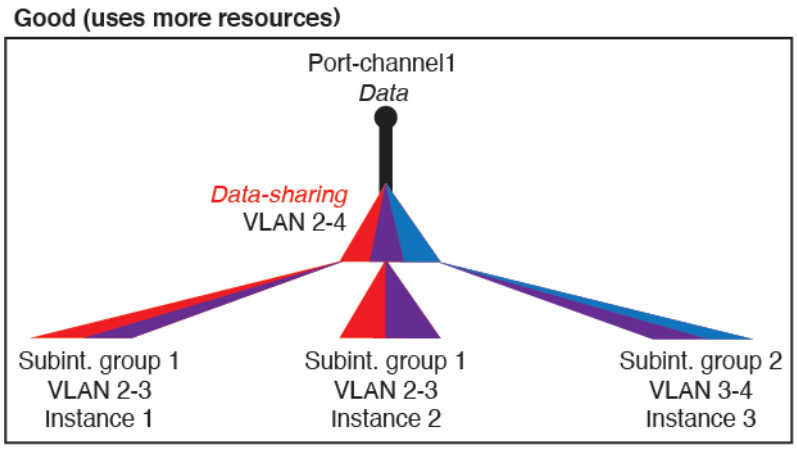
   예를 들어 대규모 EtherChannel 하나를 생성해 유사한 종류의 모든 인터페이스를 함께 번들로 묶은 다음 해당 EtherChannel의 하위 인터페이스를 공유합니다. 즉, Port-Channel2, Port-Channel3 및 Port-Channel4를 공유하는 대신 Port-Channel1.2, 3 및 4를 공유합니다. 단일 상위 인터페이스의 하위 인터페이스를 공유하면 상위 인터페이스 전체에서 하위 인터페이스를 공유하거나 물리적/EtherChannel 인터페이스를 공유할 때 VLAN 그룹 테이블이 전달 테이블보다 더 잘 확장됩니다.

   그림 ***12:*** 최고 **:** 하나의 상위에 있는 공유 하위 인터페이스 그룹



   인스턴스의 그룹과 동일한 하위 인터페이스 집합을 공유하지 않는 경우 구성으로 인해 더 많은 리소스 사용량(더 많은 VLAN 그룹)이 발생할 수 있습니다. Port-Channel1.3 및 4를 인스턴스 3(2개의 VLAN 그룹)과 공유하는 동안 Port-Channel1.2 및 3을 인스턴스 1 및 2와 공유하는 대신 Port-Channel1.2, 3 및 4를 인스턴스 1, 2 및 3(1개의 VLAN 그룹)과 공유하는 경우를 예로 들 수 있습니다.

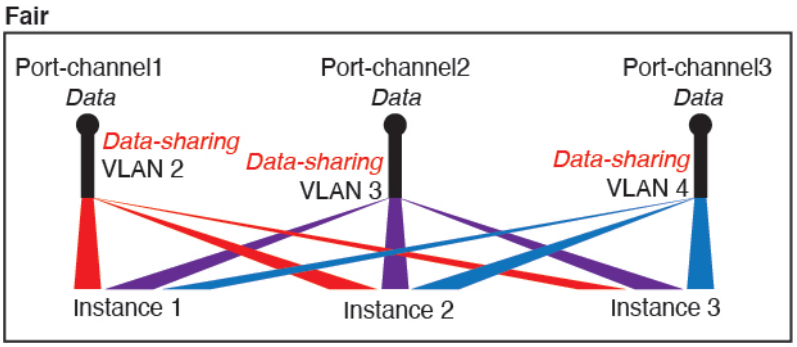
   그림 ***13:*** 좋음 **:** 하나의 상위에서 여러 하위 인터페이스 그룹 공유



2. 양호 - 여러 상위 인터페이스 간에 하위 인터페이스를 공유합니다.

예를 들어 Port-Channel2, Port-Channel4 및 Port-Channel4 대신 Port-Channel1.2, Port-Channel2.3 및 Port-Channel3.4를 공유합니다. 이러한 사용 방법은 동일한 상위 인터페이스에서 하위 인터페이스만 공유하는 것만큼 효율적이지는 않지만 여전히 VLAN 그룹의 장점을 활용합니다.

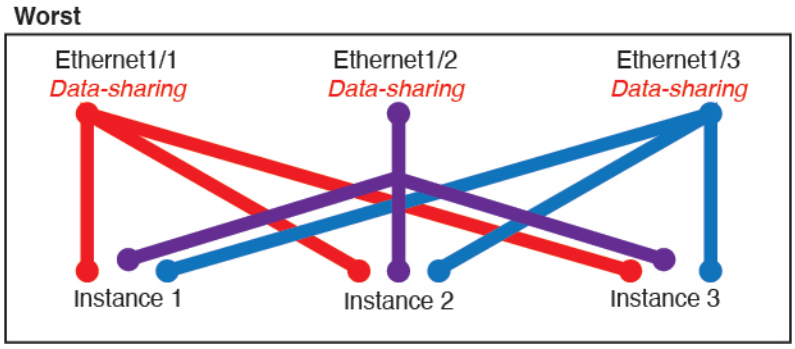
그림 *14:* 보통 *:* 개별 상위의 공유 하위 인터페이스



3. 최악 - 개별 상위 인터페이스(물리적 또는 EtherChannel)를 공유합니다.

   이 방법에서는 대부분의 전달 테이블 항목을 사용합니다.

그림 *15:* 최악 *:* 공유 상위 인터페이스



공유 인터페이스 사용 예시

인터페이스 공유 및 확장성에 대한 예시는 다음 표를 참조하십시오. 아래 시나리오는 모든 인스턴스 간에 공유되는 관리를 위해 하나의 물리적/EtherChannel 인터페이스를 사용하거나 고가용성에 사용하기 위해 전용 하위 인터페이스와 함께 다른 물리적 인터페이스 또는 EtherChannel 인터페이스를 사용하는 것으로 가정합니다.

- 표 69: Firepower 9300(SM-44 3개)의 물리적/EtherChannel 인터페이스 및 인스턴스, 733 페이지
- 표 70: Firepower 9300(SM-44 3개)에 있는 상위 인터페이스 하나의 하위 인터페이스 및 인스턴스, 735 페이지
- 표 71: Firepower 9300(SM-44 1개)의 물리적/EtherChannel 인터페이스 및 인스턴스, 736 페이지
- 표 72: Firepower 9300(SM-44 1개)에 있는 상위 인터페이스 하나의 하위 인터페이스 및 인스턴스, 738 페이지

Firepower 9300(SM-44 3개)

다음 표의 내용은 물리적 인터페이스 또는 EtherChannel만 사용하는 9300의 SM-44 보안 모듈 3개에 적용됩니다. 하위 인터페이스가 없으면 최대 인터페이스 수가 제한됩니다. 또한 여러 물리적 인터페이스를 공유하는 경우 여러 하위 인터페이스를 공유할 때보다 더 많은 전달 테이블 리소스를 사용합니다.

각 SM-44 모듈은 인스턴스를 14개까지 지원할 수 있습니다. 제한을 초과하지 않도록 하기 위해 필요에 따라 모듈 간에 인스턴스가 분할됩니다.

표 ***69: Firepower 9300(SM-44 3개)***의 물리적***/EtherChannel*** 인터페이스 및 인스턴스

전용 인터페이스	공유 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
32: • 8 • 8 • 8 • 8	**0**	**4:** • 인스턴스 1 • 인스턴스 2 • 인스턴스 3 • 인스턴스 4	16%
30: • 15 • 15	**0**	**2:** • 인스턴스 1 • 인스턴스 2	14%
14: • 14(각 1개)	**1**	**14:** • 인스턴스 1~인스턴스 14	46%
33: • 11(각 1개) • 11(각 1개) • 11(각 1개)	**3:** • 1 • 1 • 1	**33:** • 인스턴스 1~인스턴스 11 • 인스턴스 12~인스턴스 22 • 인스턴스 23~인스턴스 33	98%
33: • *11(각 1개)* • *11(각 1개)* • *12(각 1개)*	***3:*** • *1* • *1* • *1*	***34:*** • 인스턴스 *1*~인스턴스 *11* • 인스턴스 *12*~인스턴스 *22* • 인스턴스 *23*~인스턴스 *34*	*102%* 허용 안 됨
30: • 30(각 1개)	**1**	**6:** • 인스턴스 1~인스턴스 6	25%

전용 인터페이스	공유 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
30: • 10(각 5개) • 10(각 5개) • 10(각 5개)	**3:** • 1 • 1 • 1	**6:** • 인스턴스 1~인스턴스 2 • 인스턴스 2~인스턴스 4 • 인스턴스 5~인스턴스 6	23%
30: • 30(각 6개)	**2**	**5:** • 인스턴스 1~인스턴스 5	28%
30: • 12(각 6개) • 18(각 6개)	**4:** • 2 • 2	**5:** • 인스턴스 1~인스턴스 2 • 인스턴스 2~인스턴스 5	26%
24: • 6 • 6 • 6 • 6	**7**	**4:** • 인스턴스 1 • 인스턴스 2 • 인스턴스 3 • 인스턴스 4	44%
24: • 12(각 6개) • 12(각 6개)	**14:** • 7 • 7	**4:** • 인스턴스 1~인스턴스 2 • 인스턴스 2~인스턴스 4	41%

다음 표의 내용은 단일 상위 물리적 인터페이스에서 하위 인터페이스를 사용하는 9300의 SM-44 보안 모듈 3개에 적용됩니다. 예를 들어 대형 EtherChannel 하나를 생성해 유사한 종류의 모든 인터페이스를 함께 번들로 포함한 다음 해당 EtherChannel의 하위 인터페이스를 공유합니다. 여러 물리적 인터페이스를 공유하는 경우 여러 하위 인터페이스를 공유할 때보다 더 많은 전달 테이블 리소스를 사용합니다.

각 SM-44 모듈은 인스턴스를 14개까지 지원할 수 있습니다. 제한을 초과하지 않도록 하기 위해 필요에 따라 모듈 간에 인스턴스가 분할됩니다.

표 *70: Firepower 9300(SM-44 3*개*)*에 있는 상위 인터페이스 하나의 하위 인터페이스 및 인스턴스

전용 하위 인터페이스	공유 하위 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
168: • 168(각 4개)	**0**	**42:** • 인스턴스 1~인스턴스 42	33%
224: • 224(각 16개)	**0**	**14:** • 인스턴스 1~인스턴스 14	27%
14: • 14(각 1개)	**1**	**14:** • 인스턴스 1~인스턴스 14	46%
33: • 11(각 1개) • 11(각 1개) • 11(각 1개)	**3:** • 1 • 1 • 1	**33:** • 인스턴스 1~인스턴스 11 • 인스턴스 12~인스턴스 22 • 인스턴스 23~인스턴스 33	98%
70: • 70(각 5개)	**1**	**14:** • 인스턴스 1~인스턴스 14	46%
165: • 55(각 5개) • 55(각 5개) • 55(각 5개)	**3:** • 1 • 1 • 1	**33:** • 인스턴스 1~인스턴스 11 • 인스턴스 12~인스턴스 22 • 인스턴스 23~인스턴스 33	98%
70: • 70(각 5개)	**2**	**14:** • 인스턴스 1~인스턴스 14	46%
165: • 55(각 5개) • 55(각 5개) • 55(각 5개)	**6:** • 2 • 2 • 2	**33:** • 인스턴스 1~인스턴스 11 • 인스턴스 12~인스턴스 22 • 인스턴스 23~인스턴스 33	98%
70: • 70(각 5개)	**10**	**14:** • 인스턴스 1~인스턴스 14	46%

전용 하위 인터페이스	공유 하위 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
165: • *55(각 5개)* • *55(각 5개)* • *55(각 5개)*	***30:*** • *10* • *10* • *10*	***33:*** • 인스턴스 *1*~인스턴스 *11* • 인스턴스 *12*~인스턴스 *22* • 인스턴스 *23*~인스턴스 *33*	*102%* 허용 안 됨

Firepower 9300(SM-44 1개)

다음 표의 내용은 물리적 인터페이스 또는 EtherChannel만 사용하는 Firepower 9300(SM-44 1개)에 적용됩니다. 하위 인터페이스가 없으면 최대 인터페이스 수가 제한됩니다. 또한 여러 물리적 인터페이스를 공유하는 경우 여러 하위 인터페이스를 공유할 때보다 더 많은 전달 테이블 리소스를 사용합니다.

Firepower 9300(SM-44 1개)은 인스턴스를 14개까지 지원할 수 있습니다.

표 ***71: Firepower 9300(SM-44 1개)***의 물리적***/EtherChannel*** 인터페이스 및 인스턴스

전용 인터페이스	공유 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
32: • 8 • 8 • 8 • 8	**0**	**4:** • 인스턴스 1 • 인스턴스 2 • 인스턴스 3 • 인스턴스 4	16%
30: • 15 • 15	**0**	**2:** • 인스턴스 1 • 인스턴스 2	14%
14: • 14(각 1개)	**1**	**14:** • 인스턴스 1~인스턴스 14	46%
14: • 7(각 1개) • 7(각 1개)	**2:** • **1** • **1**	**14:** • 인스턴스 1~인스턴스 7 • 인스턴스 8~인스턴스 14	37%

전용 인터페이스	공유 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
32: • 8 • 8 • 8 • 8	**1**	**4:** • 인스턴스 1 • 인스턴스 2 • 인스턴스 3 • 인스턴스 4	21%
32: • 16(각 8개) • 16(각 8개)	**2**	**4:** • 인스턴스 1~인스턴스 2 • 인스턴스 3~인스턴스 4	20%
32: • 8 • 8 • 8 • 8	**2**	**4:** • 인스턴스 1 • 인스턴스 2 • 인스턴스 3 • 인스턴스 4	25%
32: • 16(각 8개) • 16(각 8개)	**4:** • 2 • 2	**4:** • 인스턴스 1~인스턴스 2 • 인스턴스 3~인스턴스 4	24%
24: • 8 • 8 • 8	**8**	**3:** • 인스턴스 1 • 인스턴스 2 • 인스턴스 3	37%
10: • 10(각 2개)	**10**	**5:** • 인스턴스 1~인스턴스 5	69%
10: • 6(각 2개) • 4(각 2개)	**20:** • 10 • 10	**5:** • 인스턴스 1~인스턴스 3 • 인스턴스 4~인스턴스 5	59%

전용 인터페이스	공유 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
14: • *12(각 2개)*	***10***	***7:*** • 인스턴스 *1*~인스턴스 *7*	*109%* 허용 안 됨

다음 표의 내용은 단일 상위 물리적 인터페이스에서 하위 인터페이스를 사용하는 Firepower 9300(SM-44 1개)에 적용됩니다. 예를 들어 대형 EtherChannel 하나를 생성해 유사한 종류의 모든 인터페이스를 함께 번들로 포함한 다음 해당 EtherChannel의 하위 인터페이스를 공유합니다. 여러 물리적 인터페이스를 공유하는 경우 여러 하위 인터페이스를 공유할 때보다 더 많은 전달 테이블 리소스를 사용합니다.

Firepower 9300(SM-44 1개)은 인스턴스를 14개까지 지원할 수 있습니다.

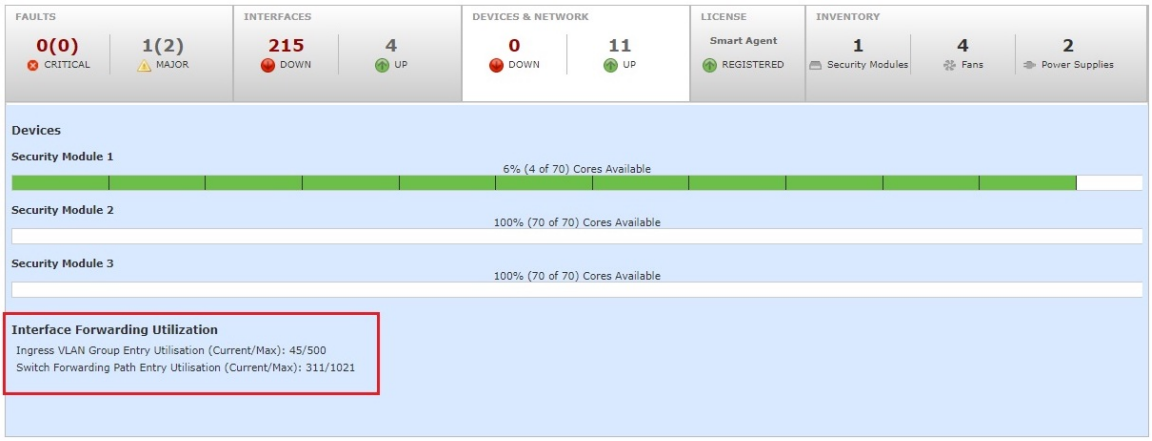
표 ***72: Firepower 9300(SM-44 1개)***에 있는 상위 인터페이스 하나의 하위 인터페이스 및 인스턴스

전용 하위 인터페이스	공유 하위 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
112: • 112(각 8개)	**0**	**14:** • 인스턴스 1~인스턴스 14	17%
224: • 224(각 16개)	**0**	**14:** • 인스턴스 1~인스턴스 14	17%
14: • 14(각 1개)	**1**	**14:** • 인스턴스 1~인스턴스 14	46%
14: • 7(각 1개) • 7(각 1개)	**2:** • 1 • 1	**14:** • 인스턴스 1~인스턴스 7 • 인스턴스 8~인스턴스 14	37%
112: • 112(각 8개)	**1**	**14:** • 인스턴스 1~인스턴스 14	46%
112: • 56(각 8개) • 56(각 8개)	**2:** • 1 • 1	**14:** • 인스턴스 1~인스턴스 7 • 인스턴스 8~인스턴스 14	37%
112: • 112(각 8개)	**2**	**14:** • 인스턴스 1~인스턴스 14	46%

전용 하위 인터페이스	공유 하위 인터페이스	인스턴스 수	사용되는 전달 테이블의 퍼센트
112: • 56(각 8개) • 56(각 8개)	**4:** • 2 • 2	**14:** • 인스턴스 1~인스턴스 7 • 인스턴스 8~인스턴스 14	37%
140: • 140(각 10개)	**10**	**14:** • 인스턴스 1~인스턴스 14	46%
140: • 70(각 10개) • 70(각 10개)	**20:** • 10 • 10	**14:** • 인스턴스 1~인스턴스 7 • 인스턴스 8~인스턴스 14	37%

공유 인터페이스 리소스 보기

포워딩 테이블 및 VLAN 그룹 사용량을 보려면 **Devices & Network(**디바이스 및 네트워크**) > Interface Forwarding Utilization(**인터페이스 포워딩 사용률**)** 영역을 확인하고 예를 들면 다음과 같습니다.



Firepower Threat Defense에 대한 인라인 집합 링크 상태 전파

비활성 엔드포인트(bump in the wire)처럼 작동하는 인라인 집합은 두 인터페이스를 함께 슬롯에 포함해 기존 네트워크에 바인딩합니다. 이 기능을 사용하면 인접한 네트워크 디바이스의 구성 없이 네트워크 환경에 시스템을 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

FTD 애플리케이션에서 인라인 집합을 구성하고 링크 상태 전파를 활성화하면 FTD에서 FXOS 섀시로 인라인 집합 멤버십을 전송합니다. 링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 중단될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다. 장애가 발생한 인터페이

스가 복원되면 두 번째 인터페이스도 자동으로 활성화됩니다. 다시 말해, 한 인터페이스의 링크 상태가 변경되면 섀시가 변경사항을 감지하고 다른 인터페이스의 링크 상태도 일치하도록 업데이트합니다. 섀시가 링크 상태 변경사항을 전파하려면 최대 4초가 걸립니다. 링크 상태 전파는 라우터가 장애 상태인 네트워크 디바이스를 우회해 트래픽을 자동으로 다시 라우팅하도록 구성된 탄력적인 네트워크 환경에서 특히 유용합니다.

논리적 디바이스 정보

논리적 디바이스를 사용하면 애플리케이션 인스턴스 하나(ASA 또는 Firepower Threat Defense)와 선택적 데코레이터 애플리케이션(Radware DefensePro)을 실행하여 서비스 체인을 만들 수 있습니다 .

논리적 디바이스를 추가할 때는 애플리케이션 인스턴스 유형 및 버전 정의, 인터페이스 할당, 애플리케이션 구성으로 푸시되는 부트스트랩 설정 작업도 수행합니다.

참고 Firepower 9300의 경우에는 섀시 내의 모든 모듈에 동일한 애플리케이션 인스턴스 유형(ASA 또는 FTD)을 설치해야 합니다. 다른 유형은 현재 지원되지 않습니다. 모듈은 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수 있습니다.

Firepower 9300의 경우 섀시 내의 개별 모듈에 서로 다른 애플리케이션 유형(ASA 및 FTD)을 설치할 수 있습니다. 개별 모듈에서 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수도 있습니다.

독립형 논리적 디바이스와 클러스터형 논리적 디바이스

다음의 논리적 디바이스 유형을 추가할 수 있습니다.

- 독립형 - 독립형 유닛으로 또는 고가용성 쌍의 유닛으로 작동하는 독립형 논리적 디바이스입니다.
- 클러스터 - 클러스터형 논리적 디바이스에서는 여러 유닛을 함께 그룹화할 수 있으므로 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. Firepower 9300과 같은 다중 모듈 디바이스는 인트라 섀시 클러스터링(intra-chassis clustering)을 지원합니다. Firepower 9300의 경우 세 개 모듈 모두가 네이티브와 컨테이너 인스턴스 모두에 대해 클러스터에 참여해야 합니다. FDM은(는) 클러스터를 지원하지 않습니다.

논리적 디바이스 애플리케이션 인스턴스: 컨테이너 및 기본

다음 구축 유형으로 애플리케이션 인스턴스가 실행됩니다.

- 기본 인스턴스 — 기본 인스턴스는 보안 모듈/엔진의 모든 리소스(CPU, RAM 및 디스크 공간)를 사용합니다. 따라서 하나의 기본 인스턴스만 설치할 수 있습니다.
- 컨테이너 인스턴스 — 컨테이너 인스턴스는 보안 모듈/엔진의 리소스 하위 집합을 사용합니다. 따라서 여러 개의 컨테이너 인스턴스를 설치할 수 있습니다. 다중 인스턴스 기능은 FMC를 사용

하는 Firepower Threat Defense에 대해서만 지원되며, ASA 또는 FDM 사용 FTD에 대해서는 지원되지 않습니다.

참고 다중 인스턴스 기능은 ASA 다중 컨텍스트 모드와 비슷하지만 구현은 서로 다릅니다. 다중 컨텍스트 모드에서는 단일 애플리케이션 인스턴스를 분할하는 반면 다중 인스턴스 기능 사용 시에는 독립적인 컨테이너 인스턴스를 사용할 수 있습니다. 컨테이너 인스턴스에서는 하드 리소스 분리, 별도의 구성 관리/다시 로드/소프트웨어 업데이트가 허용되며 전체 Firepower Threat Defense 기능이 지원됩니다. 다중 컨텍스트 모드에서는 리소스가 공유되므로 지정된 플랫폼에서 더 많은 컨텍스트가 지원됩니다. Firepower Threat Defense에서는 다중 컨텍스트 모드를 사용할 수 없습니다.

Firepower 9300의 경우 일부 모듈에서는 기본 인스턴스를, 다른 모듈에서는 컨테이너 인스턴스를 사용할 수 있습니다.

컨테이너 인스턴스 인터페이스

컨테이너 인스턴스에 대해 물리적 인터페이스를 유연하게 사용할 수 있도록 FXOS에서 VLAN 하위 인터페이스를 생성하는 동시에 여러 인스턴스 간에 인터페이스(VLAN 또는 물리적)를 공유할 수 있습니다. 기본 인스턴스는 VLAN 하위 인터페이스 또는 공유 인터페이스를 사용할 수 없습니다. 멀티 인스턴스 클러스터는 VLAN 하위 인터페이스 또는 공유된 인터페이스를 사용할 수 없습니다. 클러스터 EtherChannel의 하위 인터페이스를 사용할 수 있는 클러스터 제어 링크는 예외입니다. 공유 인터페이스 확장성, 730 페이지 및 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가, 760 페이지를 참조하십시오.

섀시가 패킷을 분류하는 방법

섀시에 들어오는 각 패킷은 분류되어야 합니다. 그러면 섀시에서 어떤 인스턴스에 패킷을 보낼지 판단할 수 있습니다.

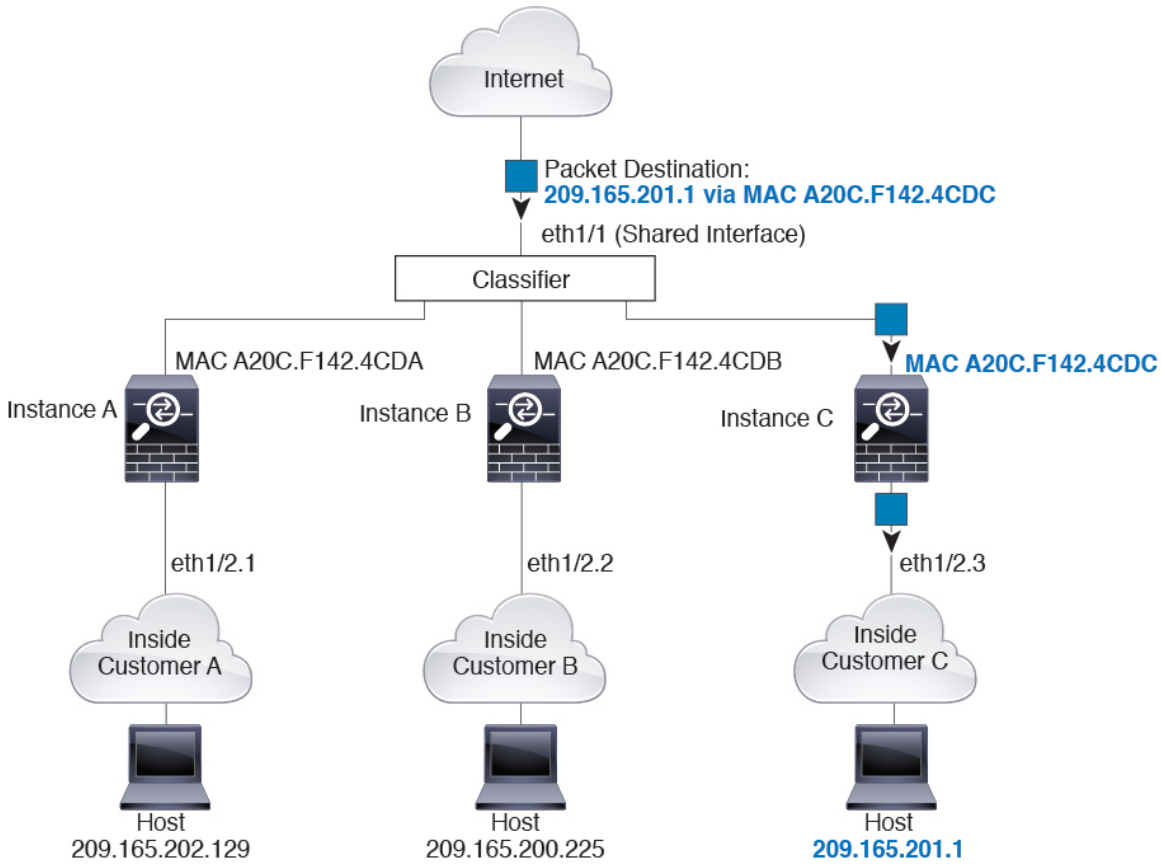
- 고유 인터페이스 - 단 하나의 인스턴스가 인그레스 인터페이스와 연결된 경우 섀시는 해당 패킷을 해당 인스턴스로 분류합니다. 투명 모드 또는 라우티드 모드의 브리지 그룹 멤버 인터페이스, 인라인 집합 또는 패시브 인터페이스의 경우에는 항상 이 방법을 사용하여 패킷을 분류합니다.
- 고유 MAC 주소 - 섀시가 공유 인터페이스를 포함한 모든 인터페이스에 대해 고유한 MAC 주소를 자동으로 생성합니다. 여러 인스턴스가 인터페이스 하나를 공유하는 경우 분류자는 각 인스턴스의 인터페이스에 할당된 고유 MAC 주소를 사용합니다. 업스트림 라우터는 고유 MAC 주소가 없으면 인스턴스로 직접 라우팅할 수 없습니다. 또한 애플리케이션 내에서 각 인터페이스를 구성할 때 수동으로 MAC 주소를 설정할 수도 있습니다.

참고 대상 MAC 주소가 멀티캐스트 또는 브로드캐스트 MAC 주소인 경우 패킷이 복제되어 각 인스턴스에 배포됩니다.

분류의 예

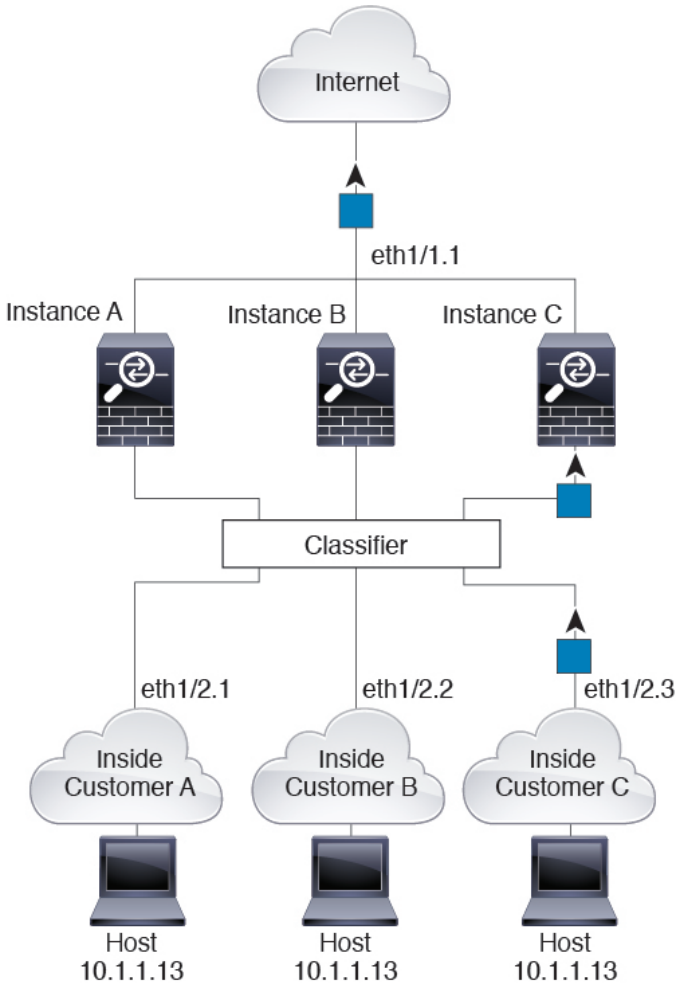
다음 그림은 외부 인터페이스를 공유하는 여러 인스턴스를 보여 줍니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 라우터에서 패킷을 보내는 MAC 주소가 인스턴스 C에 포함되어 있기 때문입니다.

그림 ***16: MAC*** 주소를 사용하는 공유 인터페이스를 통한 패킷 분류



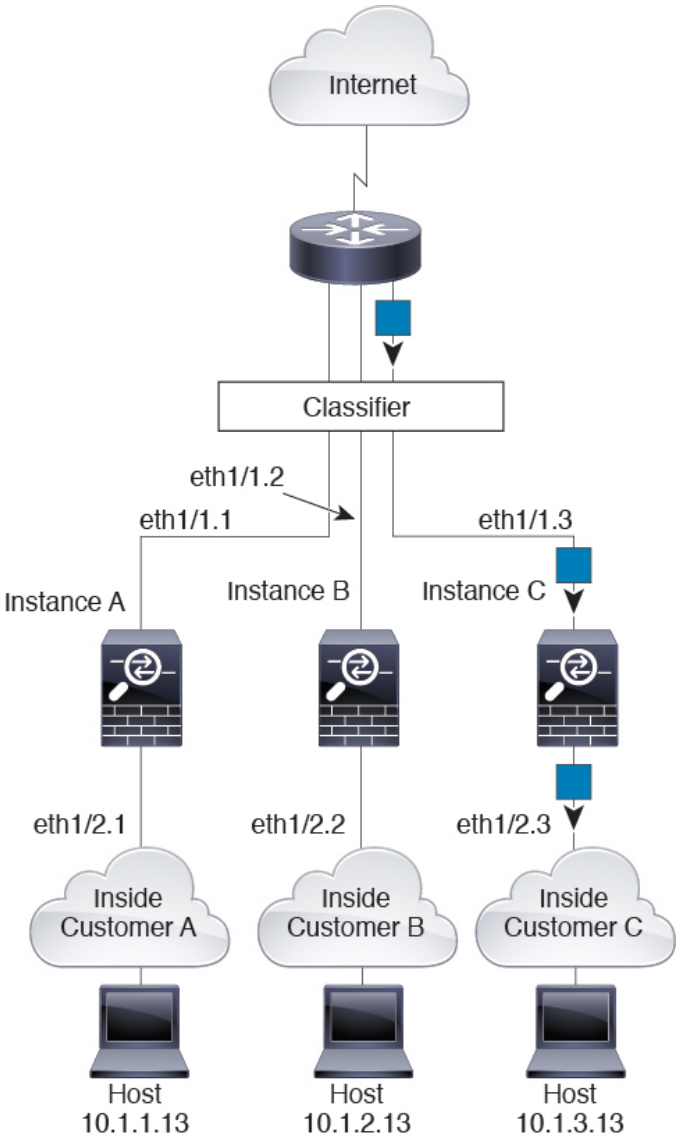
내부 네트워크에서 보낸 것을 비롯하여 모든 신규 수신 트래픽은 분류되어야 합니다. 다음 그림에는 인터넷에 액세스하는 네트워크 내의 인스턴스 C에 있는 호스트가 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 이더넷 1/2.3이기 때문입니다.

그림 *17:* 내부 네트워크로부터 수신하는 트래픽



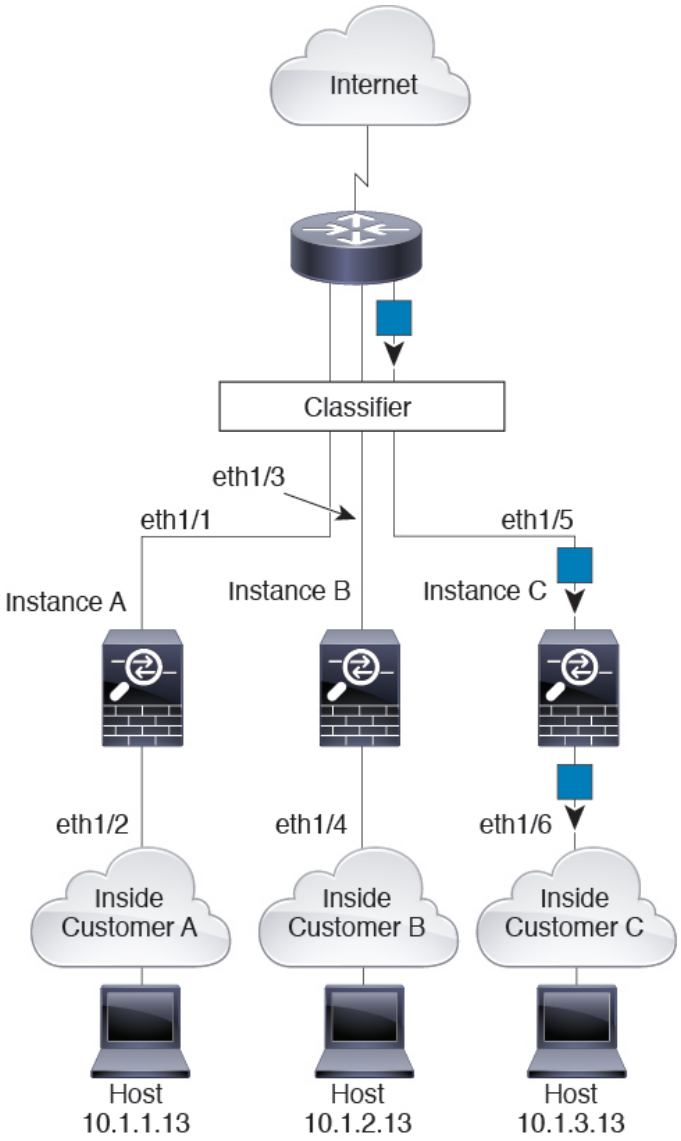
투명 방화벽의 경우 고유한 인터페이스를 사용해야 합니다. 다음 그림에는 인터넷의 네트워크 내 인스턴스 C에 있는 호스트로 전송되는 패킷이 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 이더넷 1/2.3이기 때문입니다.

그림 *18:* 투명한 방화벽 인스턴스



인라인 집합의 경우에는 고유 인터페이스를 사용해야 하며, 해당 인터페이스는 물리적 인터페이스 또는 EtherChannel이어야 합니다. 다음 그림에는 인터넷의 네트워크 내 인스턴스 C에 있는 호스트로 전송되는 패킷이 나와 있습니다. 분류자는 인스턴스 C에 패킷을 할당합니다. 인그레스 인터페이스가 인스턴스 C에 할당된 이더넷 1/5이기 때문입니다.

그림 ***19: FTD***용 인라인 집합

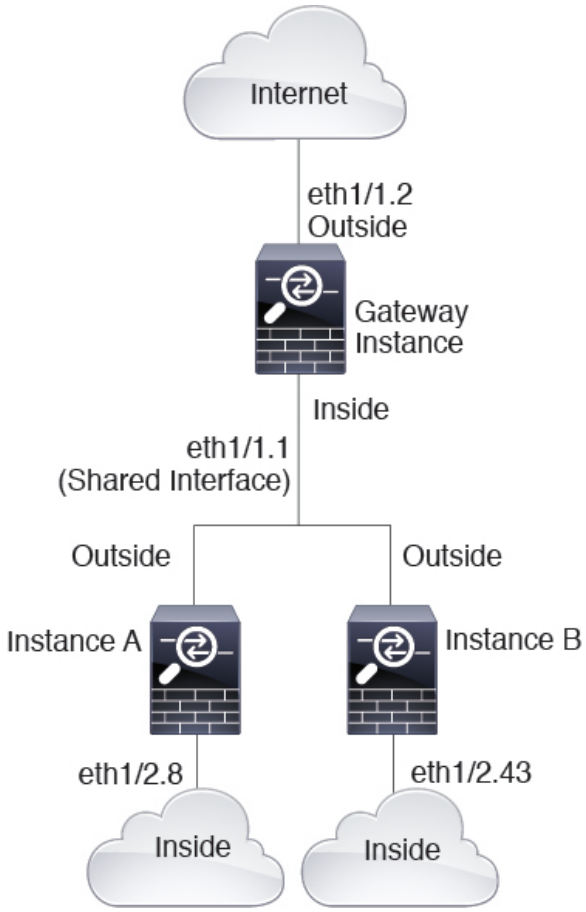


연속 컨테이너 인스턴스

다른 인스턴스 바로 앞에 컨테이너 인스턴스를 배치하는 것을 연속 컨테이너 인스턴스라고 합니다. 하나의 인스턴스의 외부 인터페이스는 다른 인스턴스의 내부 인터페이스와 동일한 인터페이스입니다. 최상위 인스턴스에서 공유 파라미터를 구성함으로써 일부 인스턴스의 구성을 간소화하고 싶다면 인스턴스 캐스케이딩이 유용할 수 있습니다.

다음 그림에는 게이트웨이 뒤에 인스턴스가 2개 있는 게이트웨이 인스턴스가 나와 있습니다.

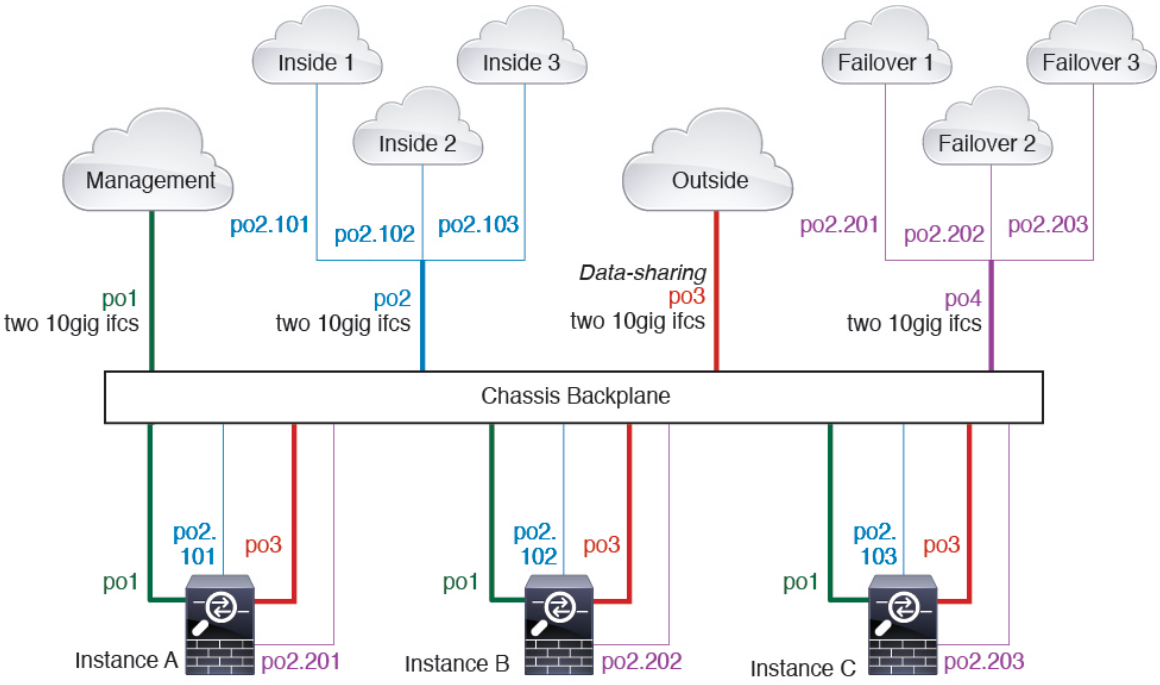
그림 *20:* 연속 컨테이너 인스턴스



일반적인 다중 인스턴스 구축

다음 예에는 라우팅된 방화벽 모드의 컨테이너 인스턴스 3개가 포함되어 있습니다. 이러한 컨테이너 인스턴스는 다음 인터페이스를 포함합니다.

- Management(관리) - 모든 인스턴스가 Port-Channel1 인터페이스(관리 유형)를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 애플리케이션 내에서 인터페이스는 동일한 관리 네트워크의 고유 IP 주소를 사용합니다.
- Inside(내부) - 각 인스턴스가 Port-Channel2(데이터 유형)의 하위 인터페이스를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 하위 인터페이스는 별도 네트워크에 있습니다.
- Outside(외부) - 모든 인스턴스가 Port-Channel3 인터페이스(데이터 공유 유형)를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 애플리케이션 내에서 인터페이스는 동일한 외부 네트워크의 고유 IP 주소를 사용합니다.
- Failover(페일오버) - 각 인스턴스가 Port-Channel4(데이터 유형)의 하위 인터페이스를 사용합니다. 이 EtherChannel에는 10기가비트 이더넷 인터페이스 2개가 포함됩니다. 각 하위 인터페이스는 별도 네트워크에 있습니다.



컨테이너 인스턴스 인터페이스용 자동 **MAC** 주소

FXOS 섀시는 컨테이너 인스턴스 인터페이스용 MAC 주소를 자동으로 생성하며 각 인스턴스의 공유 인터페이스가 고유한 MAC 주소를 사용하도록 보장합니다.

애플리케이션 내의 공유 인터페이스에 직접 MAC 주소를 할당하는 경우 직접 할당한 MAC 주소가 사용됩니다. 나중에 수동 MAC 주소를 삭제할 경우 자동 생성 주소가 사용됩니다. 드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 애플리케이션 내에서 인터페이스의 MAC 주소를 직접 설정하는 것이 좋습니다.

자동 생성 주소는 A2로 시작하기 때문에, 주소가 겹칠 위험이 있으므로 수동 MAC 주소를 A2로 시작해서는 안 됩니다.

FXOS 섀시는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2*xx.yyzz.zzzz*

여기서 *xx.yy*는 사용자 정의 접두사 또는 시스템 정의 접두사이고 *zz.zzzz*는 섀시에서 생성되는 내부 카운터입니다. 시스템 정의 접두사는 IDPROM에 프로그래밍되는 번인된 MAC 주소 풀의 첫 번째 MAC 주소의 하위 2바이트와 일치합니다. MAC 주소 풀을 확인하려면 **connect fxos**, **show module**을 차례로 사용합니다. 예를 들어 모듈 1에 대해 표시되는 MAC 주소 범위가 b0aa.772f.f0b0~b0aa.772f.f0bf이면 시스템 접두사는 f0b0입니다.

사용자 정의 접두사는 16진수로 변환되는 정수입니다. 사용자 정의 접두사가 어떻게 사용되는지 예를 들어 설명하자면, 접두사를 77로 설정하는 경우 섀시에서는 77을 16진수 값 004D(*yyxx*)로 변환합니다. 접두사가 MAC 주소에서 쓰일 때는 섀시 기본 형식에 부합하도록 역전됩니다(*xxyy*).

A2**4D.00***zz.zzzz*

접두사가 1009 (03F1)일 때 MAC 주소는 다음과 같습니다.

A2**F1.03***zz.zzzz*

컨테이너 인스턴스 리소스 관리

컨테이너 인스턴스당 리소스 사용량을 지정하려면 FXOS에서 리소스 프로파일을 하나 이상 생성합니다. 논리적 디바이스/애플리케이션 인스턴스를 구축할 때 사용할 리소스 프로필을 지정합니다. 리소스 프로파일은 CPU 코어 수를 설정합니다. RAM은 코어 수에 따라 동적으로 할당되며 디스크 공간은 인스턴스당 40GB로 설정됩니다. 모델당 사용 가능한 리소스를 확인하려면 컨테이너 인스턴스의 요구 사항 및 사전 요구 사항, 751 페이지 섹션을 참조하십시오. 리소스 프로파일을 추가하려면 컨테이너 인스턴스에 대한 리소스 프로파일 추가, 761 페이지 섹션을 참조하십시오.

다중 인스턴스 기능의 성능 확장 요인

플랫폼의 최대 처리량(연결, VPN 세션 및 TLS 프록시 세션)은 네이티브 인스턴스의 메모리 및 CPU 사용에 대해 계산됩니다. 이 값은 **show resource usage**에 표시됩니다. 다중 인스턴스를 사용하는 경우 처리량은 인스턴스에 할당하는 CPU 코어의 비율을 기준으로 계산해야 합니다. 예를 들어, 코어가 50%인 컨테이너 인스턴스를 사용하는 경우, 처음에는 처리량의 50%를 계산해야 합니다. 또한, 컨테이너 인스턴스에 사용 가능한 처리량은 기본 인스턴스에 사용 가능한 처리량보다 적을 수 있습니다(약 70%~80%). 네트워크에 따라 확장성이 향상되거나 더 나빠질 수 있습니다. 따라서 인스턴스가 50%인 경우, 예상 처리량을 약 40%(50%의 80%)로 줄여야 합니다.

컨테이너 인스턴스 및 고가용성

2개의 개별 섀시에서 컨테이너 인스턴스를 사용하여 고가용성을 사용할 수 있습니다. 예를 들어 각각 인스턴스가 10개인 섀시가 2개 있으면 고가용성 쌍 10개를 생성할 수 있습니다. FXOS에서 고가용성이 구성되지 않았으면 애플리케이션 관리자에서 각 고가용성 쌍을 구성합니다.

자세한 요구 사항은 고가용성 요구 사항 및 전제 조건, 752 페이지 및 고가용성 쌍 추가, 769 페이지의 내용을 참조하십시오.

컨테이너 인스턴스 및 클러스터링

보안 모듈/엔진당 하나의 컨테이너 인스턴스를 사용하여 컨테이너 인스턴스 클러스터를 생성할 수 있습니다. 자세한 요구 사항은 클러스터링의 요구 사항 및 사전 요구 사항, 923 페이지의 내용을 참조하십시오.

컨테이너 인스턴스용 라이선스

모든 라이선스는 (Firepower 4100의) 보안 엔진/섀시 또는 (Firepower 9300의) 보안 모듈에 대해 소비되지만 컨테이너 라이선스에 대해서는 소비되지 않습니다. 자세한 내용은 다음을 참조하십시오.

- 기본 라이선스는 보안 모듈/엔진당 하나씩 자동으로 할당됩니다.
- 기능 라이선스는 각 인스턴스에 대해 수동으로 할당되지만 사용자는 보안 모듈/엔진의 기능당 하나의 라이선스를 소비합니다. 예를 들어 3개의 보안 모듈이 있는 Firepower 9300에 대해서는 모듈당 하나의 URL 필터링 라이선스가 필요하므로 사용 중인 인스턴스 수와 관계없이 총 3개의 라이선스가 필요합니다.

- 고가용성은 고가용성 쌍의 FTD 디바이스에 대한 라이선스 요구 사항, 891 페이지을 참조하십시오.

예를 들면 다음과 같습니다.

표 *73: Firepower 9300*의 컨테이너 인스턴스에 대한 라이선스 사용

Firepower 9300	**Instance**	라이선스
보안 모듈 1	인스턴스 1	기본, URL 필터링, 악성코드
	인스턴스 2	기본, URL 필터링
	인스턴스 3	기본, URL 필터링
보안 모듈 2	인스턴스 4	기본, 위협
	인스턴스 5	기본, URL 필터링, 악성코드, 위협
보안 모듈 3	인스턴스 6	기본, 악성코드, 위협
	인스턴스 7	기본, 위협

표 *74:* 수총 라이선스 수

Base	**URL** 필터링	악성코드	위협
3	2	3	2

논리적 디바이스의 요구 사항 및 사전 요구 사항

요구 사항 및 사전 요구 사항에 대한 내용은 다음 섹션을 참조하십시오.

하드웨어 및 소프트웨어 조합에 대한 요건 및 사전 요구 사항

Firepower 4100/9300에서는 여러 모델, 보안 모듈, 애플리케이션 유형, 고가용성 및 확장성 기능을 지원합니다. 허용되는 조합에 대한 다음과 같은 요건을 참조하십시오.

Firepower 9300 요건

Firepower 9300에는 3개의 보안 모듈 슬롯 및 여러 유형의 보안 모듈이 포함되어 있습니다. 다음 요건을 참조하십시오.

- 보안 모듈 유형 - Firepower 9300에 다양한 유형의 모듈을 설치할 수 있습니다. 예를 들어, SM-36을 모듈 1로, SM-40을 모듈 2로, SM-44를 모듈 3으로 설치할 수 있습니다.

- 네이티브 인스턴스 클러스터링 - 클러스터의 모든 보안 모듈이 인트라 섀시(intra-chassis)든, 섀시 간(inter-chassis)이든 상관없이 동일한 유형이어야 합니다. 빈 슬롯을 포함하여 섀시에 있는 모든 모듈은 클러스터에 속해야 하지만 각 섀시에 설치된 보안 모듈의 수는 다를 수 있습니다. 예를 들어, 섀시 1에는 2개의 SM-36을 설치하고 섀시 2에는 3개의 SM-36을 설치할 수 있습니다. 동일한 섀시에 1개의 SM-24 및 2개의 SM-36을 설치하는 경우에는 클러스터링을 사용할 수 없습니다.
- 컨테이너 인스턴스 클러스터링 - 다양한 모델 유형에서 인스턴스를 사용하여 클러스터를 생성할 수 있습니다. 예를 들어 Firepower 9300 SM-56, SM-40, SM-36에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 그러나 동일한 클러스터에서 Firepower 9300과 Firepower 4100을 혼합할 수는 없습니다.

- 고가용성 - 고가용성은 Firepower 9300에서 동일한 유형의 모듈 간에만 지원됩니다. 그러나 두 섀시에는 혼합 모듈을 포함할 수 있습니다. 각 섀시에 SM-36, SM-40 및 SM-44가 있는 경우를 예로 들 수 있습니다. SM-36 모듈 간, SM-40 모듈 간, SM-44 모듈 간에 고가용성 쌍을 생성할 수 있습니다.
- ASA 및 FTD 애플리케이션 유형 - 섀시의 개별 모듈에 서로 다른 애플리케이션 유형을 설치할 수 있습니다. 예를 들어, 모듈 1 및 모듈 2에는 ASA를 설치하고 모듈 3에는 FTD를 설치할 수 있습니다.
- ASA 또는 FTD 버전 - 애플리케이션 인스턴스 유형의 서로 다른 버전을 별도의 모듈에서 실행하거나 동일한 모듈에서 별도의 컨테이너 인스턴스로 실행할 수 있습니다. 예를 들어, 모듈 1에는 FTD 6.3을, 모듈 2에는 FTD 6.4를 설치하고, 모듈 3에는 FTD 6.5를 설치할 수 있습니다.

Firepower 4100 요건

Firepower 4100은 여러 모델로 제공됩니다. 다음 요건을 참조하십시오.

- 기본 및 컨테이너 인스턴스 - Firepower 4100에 컨테이너 인스턴스를 설치하는 경우 해당 디바이스에서는 다른 컨테이너 인스턴스만 지원할 수 있습니다. 기본 인스턴스에서는 디바이스의 모든 리소스를 사용하므로 디바이스에는 하나의 기본 인스턴스만 설치할 수 있습니다.
- 네이티브 인스턴스 클러스터링 - 클러스터의 모든 섀시는 동일한 모델이어야 합니다.
- 컨테이너 인스턴스 클러스터링 - 다양한 모델 유형에서 인스턴스를 사용하여 클러스터를 생성할 수 있습니다. 예를 들어 Firepower 4140 및 4150에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 그러나 동일한 클러스터에서 Firepower 9300과 Firepower 4100을 혼합할 수는 없습니다.

- 고가용성 - 고가용성은 동일한 유형의 모듈 간에만 지원됩니다.
- ASA 및 FTD 애플리케이션 유형 - Firepower 4100에서는 하나의 애플리케이션 유형만 실행할 수 있습니다.
- FTD 컨테이너 인스턴스 버전 - 동일한 모듈에서 별도의 컨테이너 인스턴스로 서로 다른 버전의 FTD를 실행할 수 있습니다.

컨테이너 인스턴스의 요구 사항 및 사전 요구 사항

지원되는 애플리케이션 유형

- FMC를 사용하는 Firepower Threat Defense

모델당 최대 컨테이너 인스턴스 및 리소스

각 컨테이너 인스턴스에 대해 인스턴스에 할당할 CPU 코어의 수를 지정할 수 있습니다. 코어 수에 따라 RAM은 동적으로 할당되며 디스크 공간은 인스턴스당 40GB로 설정됩니다.

표 *75:* 모델당 최대 컨테이너 인스턴스 및 리소스

모델	최대 컨테이너 인스턴스 수	사용 가능한 **CPU** 코어	사용 가능한 **RAM**	사용 가능한 디스크 공간
Firepower 4110	3	22	53GB	125.6GB
Firepower 4112	3	22	78GB	308GB
Firepower 4115	7	46	162GB	308GB
Firepower 4120	3	46	101GB	125.6GB
Firepower 4125	10	62	162GB	644GB
Firepower 4140	7	70	222GB	311.8GB
Firepower 4145	14	86	344GB	608GB
Firepower 4150	7	86	222GB	311.8GB
Firepower 9300 SM-24 보안 모듈	7	46	226GB	656.4GB
Firepower 9300 SM-36 보안 모듈	11	70	222GB	640.4GB
Firepower 9300 SM-40 보안 모듈	13	78	334GB	1359GB
Firepower 9300 SM-44 보안 모듈	14	86	218GB	628.4GB
Firepower 9300 SM-48 보안 모듈	15	94	334GB	1341GB
Firepower 9300 SM-56 보안 모듈	18	110	334GB	1314GB

Firepower Management Center 요구 사항

Firepower 4100 섀시 또는 Firepower 9300 모듈의 모든 인스턴스에서는 라이선싱 구현으로 인해 동일한 Firepower Management Center(FMC)를 사용해야 합니다.

고가용성 요구 사항 및 전제 조건

- 고가용성 페일오버 설정에는 2개의 유닛이 필요합니다.
  - 별도의 섀시에 있어야 합니다. Firepower 9300용 섀시 내 고가용성은 지원되지 않습니다.
  - 같은 모델이어야 합니다.
  - 고가용성 논리 디바이스에는 동일한 인터페이스가 할당되어야 합니다.
  - 인터페이스 개수와 유형이 같아야 합니다. 고가용성을 활성화하기 전에 모든 인터페이스는 FXOS와 동일하게 사전 설정되어야 합니다.

- 고가용성은 Firepower 9300에서 동일한 유형의 모듈 간에만 지원되지만, 두 섀시는 혼합된 모듈을 포함할 수 있습니다. 각 섀시에 SM-36, SM-40 및 SM-44가 있는 경우를 예로 들 수 있습니다. SM-36 모듈 간, SM-40 모듈 간, SM-44 모듈 간에 고가용성 쌍을 생성할 수 있습니다.
- 컨테이너 인스턴스의 각 유닛은 동일한 리소스 프로파일 속성을 사용해야 합니다.
- 기타 고가용성을 위한 시스템 요구 사항은의 내용을 참조하십시오.

논리적 디바이스 관련 지침 및 제한 사항

지침 및 제한 사항은 다음 섹션을 참조하십시오.

Firepower 인터페이스에 대한 지침 및 제한 사항

VLAN 하위 인터페이스

- 하위 인터페이스(및 상위 인터페이스)는 컨테이너 인스턴스에만 할당할 수 있습니다.

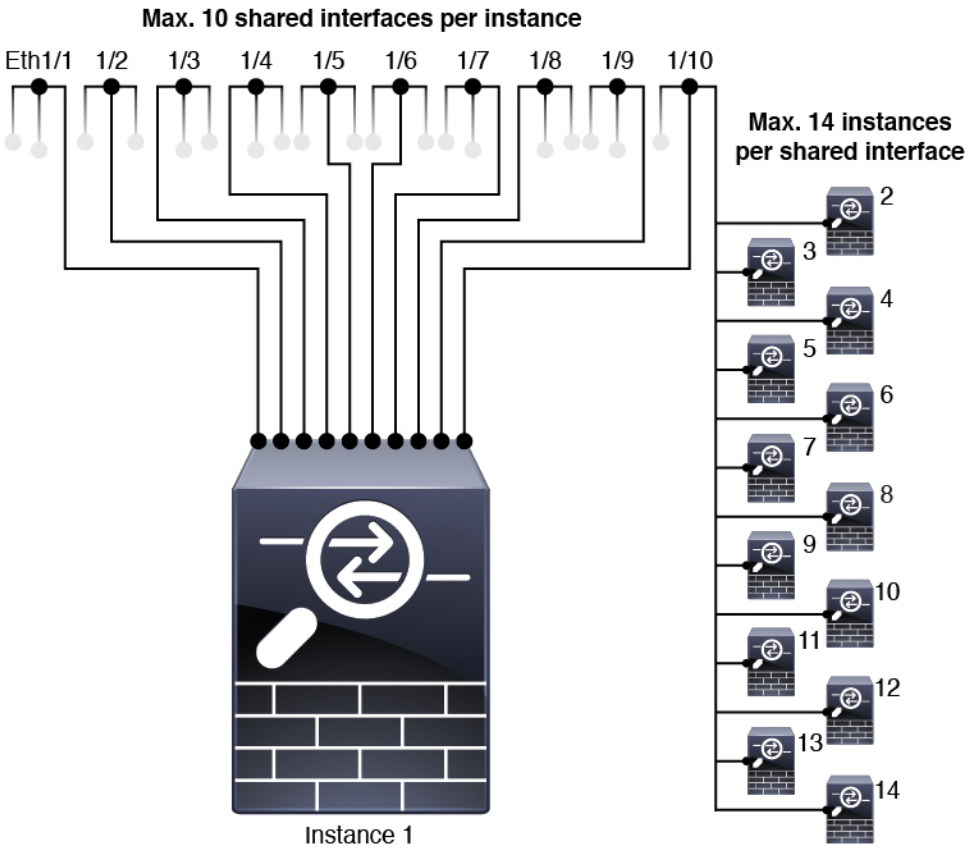
참고 컨테이너 인스턴스에 상위 인터페이스를 할당하는 경우에는 태그가 지정되지 않은(비 VLAN) 트래픽만 전달합니다. 태그가 지정되지 않은 트래픽을 전달하려는 경우가 아니라면 상위 인터페이스를 할당하지 마십시오. 클러스터 유형 인터페이스에는 상위 인터페이스를 사용할 수 없습니다.

- 하위 인터페이스는 데이터 또는 데이터 공유 유형 인터페이스와 클러스터 유형 인터페이스에서 지원됩니다. 클러스터 인터페이스에 하위 인터페이스를 추가하면 네이티브 클러스터에서 해당 인터페이스를 사용할 수 없습니다
- 다중 인스턴스 클러스터링의 경우 하위 인터페이스는 데이터 인터페이스에서 지원되지 않습니다. 그러나 하위 인터페이스는 클러스터 제어 링크에 대해 지원되므로 전용 EtherChannel 또는 EtherChannel의 하위 인터페이스를 클러스터 제어 링크에 사용할 수 있습니다.
- VLAN ID는 최대 500개까지 생성할 수 있습니다.
- 논리적 디바이스 애플리케이션 내에서 다음과 같은 제한 사항을 참조하십시오. 인터페이스 할당을 계획할 때 이러한 제한 사항을 염두에 두십시오.
  - 하위 인터페이스를 FTD 인라인 집합용으로 또는 패시브 인터페이스로 사용할 수는 없습니다.
  - 페일오버 링크용으로 하위 인터페이스를 사용하는 경우에는 해당 상위 인터페이스의 모든 하위 인터페이스와 상위 인터페이스 자체가 페일오버 링크로 사용되도록 제한됩니다. 페일오버 링크로 사용할 수 없는 하위 인터페이스도 있고, 일반 데이터 인터페이스로 사용할 수 없는 하위 인터페이스도 있습니다.

데이터 공유 인터페이스

- 데이터 공유 인터페이스는 기본 인터페이스와 함께 사용할 수 없습니다.
- 공유 인터페이스당 최대 인스턴스 수는 14개입니다. 예를 들어 Instance1~Instance14에 Ethernet1/1을 할당할 수 있습니다.

  인스턴스당 최대 공유 인터페이스 수는 10개입니다. 예를 들어 Instance1에 Ethernet1/1.1~Ethernet1/1.10을 할당할 수 있습니다.



- 데이터 공유 인터페이스는 클러스터에서 사용할 수 없습니다.
- 논리적 디바이스 애플리케이션 내에서 다음과 같은 제한 사항을 참조하십시오. 인터페이스 할당을 계획할 때 이러한 제한 사항을 염두에 두십시오.
  - 데이터 공유 인터페이스는 투명 방화벽 모드 디바이스에서 사용할 수 없습니다.
  - 데이터 공유 인터페이스는 FTD 인라인 집합 또는 패시브 인터페이스와 함께 사용할 수 없습니다.
  - 데이터 공유 인터페이스는 페일오버 링크용으로 사용할 수 없습니다.

하드웨어 바이패스

- FTD용으로 지원됩니다. ASA용 일반 인터페이스로 사용할 수 있습니다.

- FTD에서는 인라인 집합을 사용하는 하드웨어 바이패스만 지원합니다.
- Breakout 포트에 대해 하드웨어 바이패스 지원 인터페이스를 구성할 수 없습니다.
- 하드웨어 바이패스 인터페이스를 EtherChannel에 포함해 하드웨어 바이패스용으로 사용할 수는 없으며 EtherChannel에서 일반 인터페이스로 사용할 수는 있습니다.
- 하드웨어 바이패스 은(는) 고가용성 모드에서 지원되지 않습니다.

기본 **MAC** 주소

기본 인스턴스의 경우:

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- EtherChannel - EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트 채널 인터페이스는 풀의 고유 MAC 주소를 사용하며 인터페이스 멤버십은 MAC 주소에 영향을 주지 않습니다.

컨테이너 인스턴스의 경우:

- 모든 인터페이스의 MAC 주소를 MAC 주소 풀에서 가져옵니다. 하위 인터페이스의 경우에는 MAC 주소를 수동으로 구성할 때 적절한 분류를 위해 동일한 상위 인터페이스의 모든 하위 인터페이스에 대해 고유한 MAC 주소를 사용해야 합니다. 컨테이너 인스턴스 인터페이스용 자동 MAC 주소, 747 페이지의 내용을 참조하십시오.

일반 지침 및 제한 사항

방화벽 모드

FTD의 부트스트랩 구성에서 방화벽 모드를 라우팅 또는 투명으로 설정할 수 있습니다.

고가용성

- 애플리케이션 구성 내에서 고가용성을 구성합니다.
- 모든 데이터 인터페이스를 페일오버 및 상태 링크로 사용할 수 있습니다. 데이터 공유 인터페이스가 지원되지 않습니다.

다중 인스턴스 및 컨텍스트 모드

- 다중 상황 모드는 ASA에서만 지원됩니다.
- 컨테이너 인스턴스와의 다중 인스턴스 기능은 FTD FMC를 사용하는에서만 사용 가능합니다.

- FTD 컨테이너 인스턴스의 경우에는 단일 Firepower Management Center에서 보안 모듈/엔진의 모든 인스턴스를 관리해야 합니다.
- FTD 컨테이너 인스턴스의 경우에는 다음 기능이 지원되지 않습니다.
  - Radware DefensePro 링크 데코레이터
  - FMC UCAPL/CC 모드
  - 하드웨어로의 플로우 오프로드

인터페이스 구성

기본적으로 물리적 인터페이스는 비활성화되어 있습니다. 인터페이스 활성화, EtherChannels 추가, VLAN 하위 인터페이스 추가, 인터페이스 속성 수정 구성 작업을 수행할 수 있습니다.

인터페이스 활성화 또는 비활성화

각 인터페이스의 **Admin State(**관리 상태**)**를 활성화 또는 비활성화로 변경할 수 있습니다. 기본적으로 물리적 인터페이스는 비활성화되어 있습니다. VLAN 하위 인터페이스의 경우 관리 상태는 상위 인터페이스에서 상속됩니다.

프로시저

단계 **1** **Interfaces(**인터페이스**)**를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.

Interfaces(인터페이스) 페이지는 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.

단계 **2** 인터페이스를 활성화하려면 비활성화된 슬라이더 비활성화됨( )를 클릭하여 활성화된 슬라이더 활성화됨( )로 변경합니다.

Yes(예**)**를 클릭하여 변경을 확인합니다. 해당 인터페이스의 시각적 표시가 회색에서 녹색으로 변경됩니다.

단계 **3** 인터페이스를 비활성화하려면 활성화된 슬라이더 활성화됨( )를 클릭하여 비활성화된 슬라이더 비활성화됨( )로 변경합니다.

Yes(예**)**를 클릭하여 변경을 확인합니다. 해당 인터페이스의 시각적 표시가 녹색에서 회색으로 변경됩니다.

실제 인터페이스 구성

인터페이스를 물리적으로 활성화 및 비활성화할 뿐만 아니라 인터페이스 속도 및 듀플렉스를 설정할 수 있습니다. 인터페이스를 사용하려면 FXOS에서 인터페이스를 물리적으로 활성화하고 애플리케이션에서 논리적으로 활성화해야 합니다.

시작하기 전에

- 이미 EtherChannel의 멤버인 인터페이스는 개별적으로 수정할 수 없습니다. EtherChannel에 인터페이스를 추가하기 전에 설정을 구성하십시오.

프로시저

단계 **1** **Interfaces(**인터페이스**)**를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.

All Interfaces(모든 인터페이스**)** 페이지 상단에는 현재 설치되어 있는 인터페이스가 시각적으로 표시되며, 아래 표에는 설치되어 있는 인터페이스의 목록이 나와 있습니다.

단계 **2** 편집하려는 인터페이스 행에서 **Edit(**편집**)**를 클릭하여 **Edit Interface(**인터페이스 편집**)** 대화 상자를 엽니다.

단계 **3** 인터페이스를 활성화하려면 **Enable(**활성화**)** 확인란을 선택합니다. 인터페이스를 비활성화하려면 **Enable(**활성화**)** 확인란의 선택을 취소합니다.

단계 **4** 인터페이스 유형을 선택합니다.

인터페이스 유형 사용에 대한 자세한 내용은 인터페이스 유형, 726 페이지을(를) 참고하십시오.

- **Data(**데이터**)**
- 데이터 공유 - 컨테이너 인스턴스에만 해당됩니다.
- 관리
- **Firepower** - FTD에만 해당됩니다.
- 클러스터 - 클러스터 유형은 선택하지 마십시오. 기본적으로 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다.

단계 **5** (선택 사항) **Speed(**속도**)** 드롭다운 목록에서 인터페이스의 속도를 선택합니다.

단계 **6** (선택 사항) 인터페이스가 **Auto Negotiation(**자동 협상**)**을 지원하는 경우 **Yes(**예**)** 또는 **No(**아니요**)** 라디오 버튼을 클릭합니다.

단계 **7** (선택 사항) **Duplex(**듀플렉스**)** 드롭다운 목록에서 인터페이스의 듀플렉스를 선택합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

EtherChannel(포트 채널) 추가

EtherChannel(포트 채널로 알려짐)은 동일한 미디어 유형 및 용량의 멤버 인터페이스를 최대 16개까지 포함할 수 있으며 동일한 속도 및 듀플렉스로 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다. LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 데이터 또는 데이터 공유 인터페이스를 다음과 같이 구성할 수 있습니다.

- Active(활성화) — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- On(켜짐) — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

참고 On에서 활성화, 또는 활성화에서 On으로 모드를 변경하는 경우 EtherChannel가 작동하는 데 최대 3분이 걸립니다.

비 데이터 인터페이스는 액티브 모드만 지원합니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 구성이 확인되지 않습니다.

Firepower 4100/9300 섀시에서 EtherChannel을 생성하면 물리적 링크가 가동 중이더라도 EtherChannel은 논리적 디바이스에 할당될 때까지 Active LACP(액티브 LACP) 모드인 경우 **Suspended(**일시 중단**)** 상태로, On LACP(LACP 켜짐) 모드인 경우 **Down(**중단**)** 상태로 유지됩니다. 다음의 상황에서는 EtherChannel의 **Suspended(**일시 중단**)** 상태가 해제됩니다.

- EtherChannel이 독립형 논리적 디바이스에 대한 데이터 인터페이스 또는 관리 인터페이스로 추가됩니다.
- EtherChannel이 클러스터의 일부인 논리적 디바이스에 대한 관리 인터페이스 또는 클러스터 제어 링크로 추가됩니다.
- EtherChannel이 클러스터의 일부이며 유닛 하나 이상이 클러스터에 조인된 논리적 디바이스에 대한 데이터 인터페이스로 추가됩니다.

EtherChannel은 논리적 디바이스에 할당될 때까지 나타나지 않습니다. EtherChannel을 논리적 디바이스에서 제거하거나 논리적 디바이스가 삭제된 경우, EtherChannel은 **Suspended(**일시 중단**)** 또는 **Down(**중단**)** 상태로 전환됩니다.

프로시저

단계 1 **Interfaces(**인터페이스**)**를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.

All Interfaces(모든 인터페이스**)** 페이지 상단에는 현재 설치되어 있는 인터페이스가 시각적으로 표시되며, 아래 표에는 설치되어 있는 인터페이스의 목록이 나와 있습니다.

단계 2 인터페이스 테이블 위에 있는 **Add Port Channel(**포트 채널 추가**)**을 클릭하여 **Add Port Channel(**포트 채널 추가**)** 대화 상자를 엽니다.

단계 3 **Port Channel ID(**포트 채널 **ID)** 필드에 포트 채널의 ID를 입력합니다. 유효한 값은 1~47입니다.

Port-channel 48은 클러스터된 논리적 디바이스를 구축할 때 클러스터 제어 링크로 예약됩니다. 클러스터 제어 링크에 포트 채널 48을 사용하지 않으려면 포트 채널 48을 삭제한 다음 다른 ID로 클러스터 유형 EtherChannel을 구성하면 됩니다.여러 클러스터 유형 EtherChannel과 다중 인스턴스 클러스터링에 사용할 VLAN 하위 인터페이스를 추가할 수 있습니다. 인트라 섀시 클러스터링(intra-chassis clustering)의 경우, 클러스터 EtherChannel에 인터페이스를 할당하지 마십시오.

단계 4 포트 채널을 활성화하려면 **Enable(**활성화**)** 확인란을 선택합니다. 포트 채널을 비활성화하려면 **Enable(**활성화**)** 확인란의 선택을 취소합니다.

단계 5 인터페이스 유형을 선택합니다.

인터페이스 유형 사용에 대한 자세한 내용은 인터페이스 유형, 726 페이지을(를) 참고하십시오.

- **Data(**데이터**)**
- 데이터 공유 - 컨테이너 인스턴스에만 해당됩니다.
- 관리
- **Firepower** - FTD에만 해당됩니다.
- 클러스터

단계 6 드롭다운 목록에서 멤버 인터페이스의 필요한 **Admin Speed(**관리 속도**)**를 설정합니다.

지정된 속도가 아닌 멤버 인터페이스를 추가하면 포트 채널에 성공적으로 조인되지 않습니다.

단계 7 데이터 또는 데이터 공유 인터페이스의 경우 LACP 포트 채널 모드를 **Active(**액티브**)** 또는 **On(**켜짐**)** 중에서 선택합니다.

비 데이터 또는 비 데이터 공유 인터페이스의 경우 모드는 항상 액티브입니다.

단계 8 멤버 인터페이스에 대해 필요한 **Admin Duplex(**관리 듀플렉스**)**, **Full Duplex(**풀 듀플렉스**)** 또는 **Half Duplex(**하프 듀플렉스**)**를 설정합니다

지정된 듀플렉스로 설정된 멤버 인터페이스를 추가하면 포트 채널에 성공적으로 조인되지 않습니다.

단계 9 인터페이스를 포트 채널에 추가하려면 **Available Interface(**사용 가능한 인터페이스**)** 목록에서 인터페이스를 선택하고 **Add Interface(**인터페이스 추가**)**를 클릭하여 Member ID(멤버 ID) 목록으로 해당 인터페이스를 이동시킵니다.

미디어 유형과 용량이 동일한 멤버 인터페이스는 최대 16개까지 추가할 수 있습니다. 멤버 인터페이스는 동일한 속도 및 듀플렉스로 설정되어야 하며, 이 포트 채널에 대해 설정한 속도 및 듀플렉스와 일치해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다.

팁 한 번에 여러 인터페이스를 추가할 수 있습니다. 여러 개별 인터페이스를 선택하려면 **Ctrl** 키를 누른 상태에서 필요한 인터페이스를 클릭합니다. 인터페이스 범위를 선택하려면 범위에서 첫 번째 인터페이스를 선택한 다음 **Shift** 키를 누른 상태에서 범위에 있는 마지막 인터페이스를 선택합니다.

단계 **10** 포트 채널에서 인터페이스를 제거하려면 Member ID(멤버 ID) 목록의 인터페이스 오른쪽에 있는 **Delete(**삭제**)** 버튼을 클릭합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

컨테이너 인스턴스에 VLAN 하위 인터페이스 추가

네트워크 구축에 따라 섀시에 VLAN 하위 인터페이스 250~500개를 추가할 수 있습니다. 섀시에는 하위 인터페이스를 500 개까지 추가할 수 있습니다.

다중 인스턴스 클러스터링의 경우 클러스터 유형 인터페이스에 하위 인터페이스만 추가할 수 있습니다. 데이터 인터페이스의 하위 인터페이스는 지원되지 않습니다.

인터페이스당 VLAN ID는 고유해야 하며 컨테이너 인스턴스 내에서 VLAN ID는 모든 할당된 인터페이스에 대해 고유해야 합니다. VLAN ID가 다른 컨테이너 인스턴스에 할당되었다면 별도의 인터페이스에서 해당 VLAN ID를 재사용할 수 있습니다. 그러나 동일한 ID를 사용하더라도 계속해서 각 하위 인터페이스에는 이 제한이 적용됩니다.

또한 애플리케이션 내에 하위 인터페이스를 추가할 수 있습니다.FXOS 하위 인터페이스 및 애플리케이션 하위 인터페이스를 사용하는 시기에 대한 자세한 내용은 FXOS 인터페이스와 애플리케이션 인터페이스 비교, 727 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Interfaces(**인터페이스**)**를 선택하여 **All Interfaces(**모든 인터페이스**)** 탭을 엽니다.

All Interfaces(모든 인터페이스**)** 탭은 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.

단계 **2** **Add New(**새로 추가**)** > **Subinterface(**하위 인터페이스**)**를 클릭하여 **Add Subinterface(**하위 인터페이스 추가**)** 대화 상자를 엽니다.

단계 **3** 인터페이스 유형을 선택합니다.

인터페이스 유형 사용에 대한 자세한 내용은 인터페이스 유형, 726 페이지을(를) 참고하십시오.

- **Data(**데이터**)**

- 데이터 공유
- 클러스터 — 클러스터 인터페이스에 하위 인터페이스를 추가하면 네이티브 클러스터에서 해당 인터페이스를 사용할 수 없습니다.

데이터 및 데이터 공유 인터페이스: 유형은 상위 인터페이스 유형의 영향을 받지 않으므로 상위 인터페이스가 Data-sharing(데이터 공유) 유형이더라도 하위 인터페이스는 Data(데이터) 유형으로 설정할 수 있습니다.

단계 **4** 드롭다운 목록에서 상위 **Interface(**인터페이스**)**를 선택합니다.

논리적 디바이스에 현재 할당되어 있는 물리적 인터페이스에 하위 인터페이스를 추가할 수는 없습니다. 상위 인터페이스의 다른 하위 인터페이스가 할당되어 있는 경우 상위 인터페이스 자체가 할당되어 있지 않다면 새 하위 인터페이스를 추가할 수 있습니다.

단계 **5** 1~4294967295 사이의 **Subinterface ID(**하위 인터페이스 **ID)**를 입력합니다.

이 ID는 상위 인터페이스 ID에 *interface_id.subinterface_id*로 추가됩니다. 예를 들어 ID가 100인 Ethernet1/1에 하위 인터페이스를 추가하는 경우 하위 인터페이스 ID는 Ethernet1/1.100이 됩니다. 이 ID는 VLAN ID와는 다르지만 편의상 두 ID가 일치하도록 설정할 수 있습니다.

단계 **6** 1~4095 사이의 **VLAN ID**를 설정합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

상위 인터페이스를 확장하여 해당 인터페이스 아래의 모든 하위 인터페이스를 표시합니다.

논리적 디바이스 구성

Firepower 4100/9300 섀시에서 독립형 논리적 디바이스 또는 고가용성 쌍을 추가합니다.

클러스터링에 대해서는 Firepower Threat Defense 클러스터링, 917 페이지의 내용을 참조하십시오.

컨테이너 인스턴스에 대한 리소스 프로파일 추가

컨테이너 인스턴스당 리소스 사용량을 지정하려면 리소스 프로필을 하나 이상 생성합니다. 논리적 디바이스/애플리케이션 인스턴스를 구축할 때 사용할 리소스 프로필을 지정합니다. 리소스 프로파일은 CPU 코어 수를 설정합니다. RAM은 코어 수에 따라 동적으로 할당되며 디스크 공간은 인스턴스당 40GB로 설정됩니다.

- 최소 코어 수는 6입니다.

참고 코어 수가 적은 인스턴스는 코어 수가 더 많은 CPU 사용률보다 CPU 사용률이 상대적으로 높아질 수 있습니다. 코어 수가 적은 인스턴스는 트래픽 로드 변경에 더욱 민감합니다. 트래픽 삭제를 경험하는 경우 더 많은 코어를 할당해 보십시오.

- 코어는 최대값까지 짝수(6, 8, 10, 12, 14 등)로 할당할 수 있습니다.
- 사용 가능한 코어의 최대 수는 보안 모듈/섀시 모델에 따라 달라집니다. 컨테이너 인스턴스의 요구 사항 및 사전 요구 사항, 751 페이지 섹션을 참조하십시오.

섀시에는 최소 코어 수가 포함된 "Default-Small"이라는 기본 리소스 프로필이 있습니다. 이 프로필의 정의를 변경할 수 있으며 해당 프로필을 사용하지 않으면 삭제할 수도 있습니다. 이 프로필은 섀시를 다시 로드할 때 생성되며, 시스템에 다른 프로필은 없습니다.

리소스 프로파일이 현재 사용 중이라면 해당 설정을 변경할 수 없습니다. 해당 프로파일을 사용하는 인스턴스를 비활성화하고 리소스 프로파일을 변경한 후에 마지막으로 인스턴스를 다시 활성화해야 합니다. 설정된 고가용성 쌍 또는 클러스터에서 인스턴스 크기를 조정하는 경우에는 최대한 빠른 시간 내에 모든 멤버를 같은 크기로 설정해야 합니다.

FTD 인스턴스를 FMC에 추가한 후 리소스 프로파일 설정을 변경하는 경우 FMC **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **System(**시스템**)** > **Inventory(**인벤토리**)** 대화 상자에서 각 유닛의 인벤토리를 업데이트합니다.

프로시저

단계 **1** **Platform Settings(**플랫폼 설정**)** > **Resource Profiles(**리소스 프로필**)**를 선택한 다음 **Add(**추가**)**를 클릭합니다.

Add Resource Profile(리소스 프로필 추가**)** 대화 상자가 나타납니다.

단계 **2** 다음 파라미터를 설정합니다.

- **Name(**이름**)** - 1~64자 사이의 프로필 이름을 설정합니다. 프로필을 추가한 후에는 이 프로필 이름을 변경할 수 없습니다.
- **Description(**설명**)** - 프로필에 대한 설명(최대 510자)을 설정합니다.
- **Number of Cores(**코어 수**)** - 섀시에 따라 프로필의 코어 수를 6~최대값 사이의 짝수로 설정합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

용 독립형 Firepower Threat Defense 추가

독립형 논리적 디바이스는 단독으로 작동하거나 고가용성 쌍으로 작동합니다. 보안 모듈이 여러 개인 Firepower 9300에서는 클러스터 또는 독립형 디바이스를 구축할 수 있습니다. 클러스터는 모든 모듈을 사용해야 하므로 모듈이 2개인 클러스터와 단일 독립형 디바이스를 혼용하는 방식은 사용할 수 없습니다.

일부 모듈에서는 기본 인스턴스를, 다른 모듈에서는 컨테이너 인스턴스를 사용할 수 있습니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음 해당 이미지를 Firepower 4100/9300 섀시.

  참고 Firepower 9300의 경우에는 섀시 내의 모든 모듈에 동일한 애플리케이션 인스턴스 유형(ASA 또는 FTD)을 설치해야 합니다. 다른 유형은 현재 지원되지 않습니다. 모듈은 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수 있습니다.

  Firepower 9300의 경우 섀시 내의 개별 모듈에 서로 다른 애플리케이션 유형(ASA 및 FTD)을 설치할 수 있습니다. 개별 모듈에서 애플리케이션 인스턴스 유형의 서로 다른 버전을 실행할 수도 있습니다.

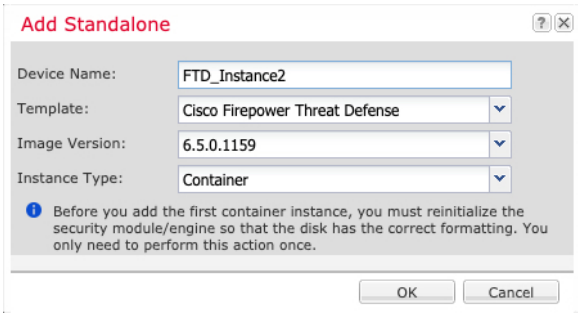
- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 섀시 관리용으로만 사용되는 섀시 관리 포트(**Interfaces(**인터페이스**)** 탭 상단에 **MGMT(**관리**)**로 표시됨)와는 다릅니다.
- 나중에 데이터 인터페이스에서 관리를 활성화할 수 있습니다. 데이터 관리를 활성화한 후 이를 사용하지 않으려는 경우에도 관리 인터페이스를 논리적 디바이스에 할당해야 합니다. 자세한 내용은 FTD 명령 참조의 **configure network management-data-interface** 명령을 참조하십시오.
- 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다. 또는 Firepower 이벤트 처리 인터페이스를 생성하여 모든 이벤트 트래픽을 전달할 수 있습니다(예: 웹 이벤트). 자세한 내용은 인터페이스 유형, 726 페이지를 참조하십시오.
- 컨테이너 인스턴스의 경우 기본 프로필을 사용하지 않으려면 컨테이너 인스턴스에 대한 리소스 프로파일 추가, 761 페이지에 따라 리소스 프로필을 추가합니다.
- 컨테이너 인스턴스의 경우 컨테이너 인스턴스를 처음으로 설치하기 전에 디스크가 올바른 형식을 갖도록 보안 모듈/엔진을 다시 초기화해야 합니다. **Security Modules(**보안 모듈**)** 또는 **Security Engine(**보안 엔진**)**을 선택하고 **Reinitialize(**초기화**)** 아이콘을 클릭합니다. 기존 논리적 디바이스가 삭제된 후에 새 디바이스로 재설치되며 로컬 애플리케이션 구성은 손실됩니다. 기본 인스턴스를 컨테이너 인스턴스로 교체할 때는 어떤 경우든 기본 인스턴스를 삭제해야 합니다. 기본 인스턴스를 컨테이너 인스턴스로 자동 마이그레이션할 수는 없습니다.
- 다음 정보를 수집합니다.
  - 이 디바이스의 인터페이스 ID

- 관리 인터페이스 IP 주소 및 네트워크 마스크
- Gateway IP address(게이트웨이 IP 주소)
- FMC 선택한 IP 주소 및/또는 NAT ID
- DNS 서버 IP 주소
- FTD 호스트 이름 및 도메인 이름

프로시저

단계 **1** **Logical Devices(**논리적 디바이스**)**를 선택합니다.

단계 **2** **Add(**추가**)** > **Standalone(**독립형**)**를 클릭하고 다음 파라미터를 설정합니다.



a) **Device Name(**디바이스 이름**)**을 입력합니다.

이 이름은 섀시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

b) **Template(**템플릿**)**에서 **Cisco Firepower Threat Defense**를 선택합니다.

c) **Image Version(**이미지 버전**)**을 선택합니다.

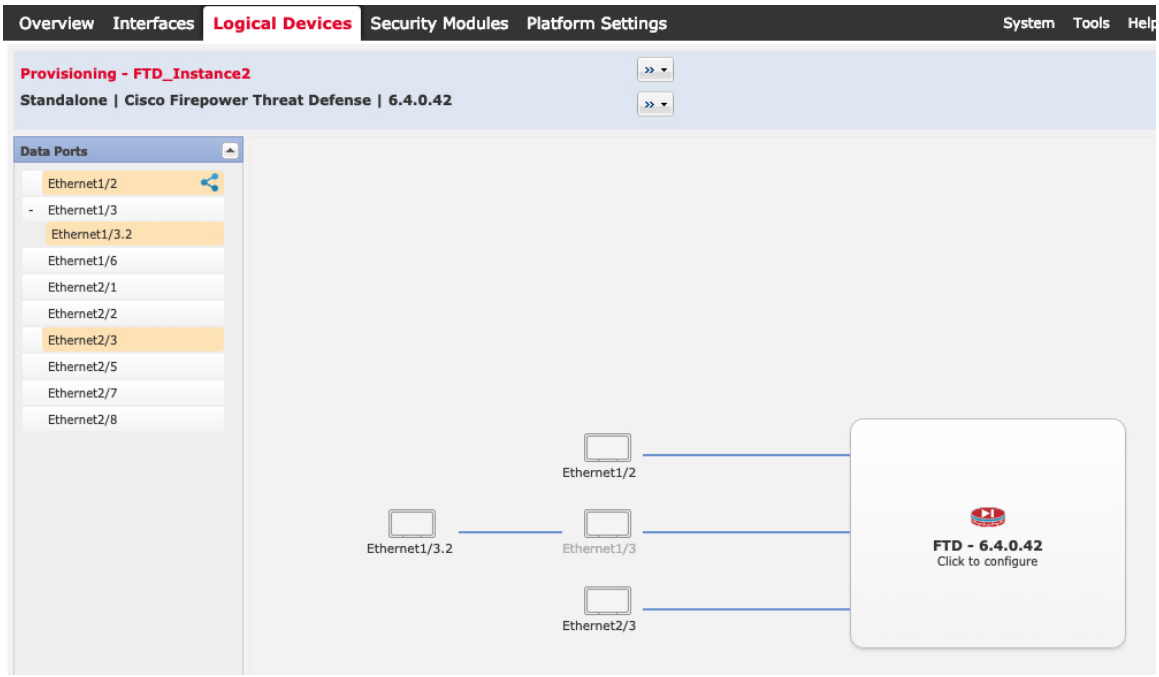
d) **Instance Type(**인스턴스 유형**)**을 **Container(**컨테이너**)** 또는 **Native(**기본**)** 중에서 선택합니다.

기본 인스턴스에서는 보안 모듈/엔진의 모든 리소스(CPU, RAM 및 디스크 공간)를 사용합니다. 따라서 하나의 기본 인스턴스만 설치할 수 있습니다. 컨테이너 인스턴스에서는 보안 모듈/엔진의 리소스 하위 집합을 사용합니다. 따라서 여러 개의 컨테이너 인스턴스를 설치할 수 있습니다.

e) **OK(**확인**)**를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 **3** **Data Ports(**데이터 포트**)** 영역을 확장하고 디바이스에 할당할 각 인터페이스를 클릭합니다.



이전에 **Interfaces(**인터페이스**)** 페이지에서 활성화한 데이터 및 데이터 공유 인터페이스만 할당할 수 있습니다. 나중에 IP 주소 설정을 비롯하여 FMC에서 이러한 인터페이스를 활성화하고 구성하게 됩니다.

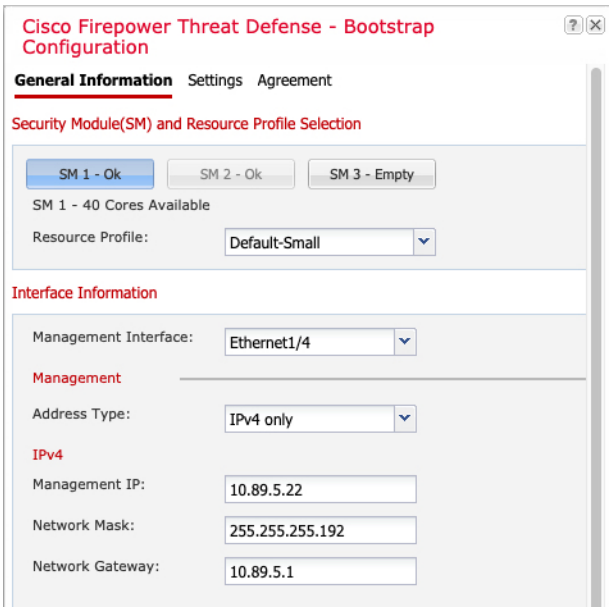
컨테이너 인스턴스에는 데이터 공유 인터페이스를 10개까지만 할당할 수 있습니다. 또한 각 데이터 공유 인터페이스는 최대 14개의 컨테이너 인스턴스에 할당할 수 있습니다. 데이터 공유 인터페이스는 공유 아이콘( )으로 표시됩니다.

하드웨어 바이패스 지원 포트가 아이콘( )과 함께 표시됩니다. 특정 인터페이스 모듈의 경우 인라인 집합 인터페이스에 대해서만 하드웨어 우회 기능을 활성화할 수 있습니다(FMC 구성 가이드 참조). Hardware Bypass는 정전 중에 트래픽이 인라인 인터페이스 쌍 사이에서 계속 흐르도록 합니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있습니다. 하드웨어 바이패스 쌍에서 두 인터페이스를 할당하지 않는 경우 그러한 할당이 의도적인지를 확인하는 경고 메시지가 표시됩니다. 하드웨어 바이패스 기능을 사용할 필요가 없으므로 원하는 경우 단일 인터페이스를 할당할 수 있습니다.

단계 **4** 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 **5** **General Information(**일반 정보**)** 페이지에서 다음 작업을 수행합니다.



a) (Firepower 9300의 경우) **Security Module Selection(**보안 모듈 선택**)** 아래에서 이 논리적 디바이스에 사용할 보안 모듈을 클릭합니다.

b) 컨테이너 인스턴스에 대해 **Resource Profile(**리소스 프로필**)**을 지정합니다.

나중에 다른 리소스 프로파일을 할당하는 경우 인스턴스가 다시 로드됩니다. 다시 로드는 5분 정도 걸릴 수 있습니다. 설정된 고가용성 쌍 또는 클러스터에 대해 크기가 다른 리소스 프로파일을 할당하는 경우에는 최대한 빠른 시간 내에 모든 멤버를 같은 크기로 설정해야 합니다.

c) **Management Interface(**관리 인터페이스**)**를 선택합니다.

이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 섀시 관리 포트와 별개입니다.

d) 관리 인터페이스 **Address Type(**주소 유형**)**을 **IPv4 only(IPv4** 전용**), IPv6 only(IPv6** 전용**)** 또는 **IPv4 and IPv6(IPv4** 및 **IPv6)** 중에서 선택합니다.

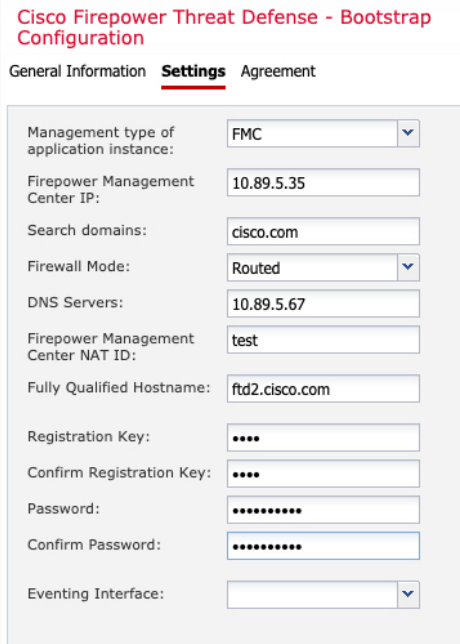
e) **Management IP(**관리 **IP)** 주소를 구성합니다.

이 인터페이스의 고유 IP 주소를 설정합니다.

f) **Network Mask(**네트워크 마스크**)** 또는 **Prefix Length(**접두사 길이**)**를 입력합니다.

g) **Network Gateway(**네트워크 게이트웨이**)** 주소를 입력합니다.

단계 **6** **Settings(**설정**)** 탭에서 다음 작업을 수행합니다.



a) 네이티브 인스턴스의 경우, **Management type of application instance(**애플리케이션 인스턴스의 관리 유형**)** 드롭다운 목록에서 **FMC**를 선택합니다.

네이티브 인스턴스에서는 FDM을 관리자로도 지원합니다. 논리적 디바이스를 구축한 후에는 관리자 유형을 변경할 수 없습니다.

b) FMC 관리에 사용할 **Firepower Management Center IP**를 입력합니다. FMC IP 주소를 알 수 없는 경우, 이 필드를 비워두고 **Firepower Management Center NAT ID** 필드에 암호를 입력합니다.

c) 컨테이너 인스턴스의 경우, **Permit Export mode from FTD SSH sessions(FTD SSH** 세션에서 전문가 모드 허용**)**에 대해 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다. 전문가 모드에서는 고급 트러블슈팅을 위한 FTD 셸 액세스 기능이 제공됩니다.

이 옵션에 대해 **Yes(**예**)**를 선택하는 경우 SSH 세션에서 컨테이너 인스턴스에 직접 액세스할 수 있는 사용자가 전문가 모드를 시작할 수 있습니다. **No(**아니요**)**를 선택하는 경우에는 FXOS CLI에서 컨테이너 인스턴스에 액세스할 수 있는 사용자만 전문가 모드를 시작할 수 있습니다. 각 인스턴스를 더욱 명확하게 격리할 수 있도록 **No(**아니요**)**를 선택하는 것이 좋습니다.

문서에 설명되어 있는 절차에 따라 Expert 모드가 필요하다고 알려주는 경우 또는 Cisco Technical Assistance Center에서 사용하도록 요청하는 경우에만 Expert 모드를 사용합니다. 이 모드를 설정하려면 FTD CLI에서 **expert** 명령을 사용합니다.

d) **Search Domains(**검색 도메인**)**를 쉼표로 구분된 목록으로 입력합니다.

e) **Firewall Mode(**방화벽 모드**)**를 **Transparent(**투명**)** 또는 **Routed(**라우팅**)** 중에서 선택합니다.

라우팅 모드에서 FTD는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

f) **DNS Servers(DNS** 서버**)**를 쉼표로 구분된 목록으로 입력합니다.

예를 들어, FMC의 호스트 이름을 지정하는 경우, FTD에서는 DNS를 사용합니다.

g) FTD의 **Fully Qualified Hostname(**정규화된 호스트 이름**)**을 입력합니다.

h) 등록 시 FMC와 디바이스 간에 공유할 **Registration Key(**등록 키**)**를 입력합니다.

이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.

i) FTD 관리 사용자가 CLI에 액세스할 때 사용할 **Password(**비밀번호**)**를 입력합니다.

j) Firepower 이벤트를 전송할 **Eventing Interface(**이벤트 인터페이스**)**를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.

이 인터페이스는 Firepower 이벤트 처리 인터페이스로 정의해야 합니다.

k) 컨테이너 인스턴스의 경우 **Hardware Crypto(**하드웨어 암호화**)**를 **Enabled(**활성화됨**)** 또는 **Disabled(**비활성화됨**)**로 설정합니다.

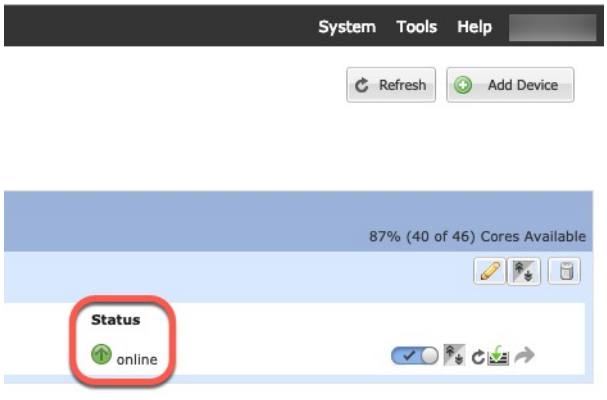
이 설정은 하드웨어에서 TLS 암호화 가속화를 활성화하고 특정 유형의 트래픽에 대한 성능을 개선합니다. 이 기능은 기본적으로 활성화되어 있습니다. 보안 모듈당 최대 16개의 인스턴스에 대해 TLS 암호화 가속화를 활성화할 수 있습니다. 이 기능은 네이티브 인스턴스에서 항상 사용할 수 있습니다. 이 인스턴스에 할당된 하드웨어 암호화 리소스의 백분율을 보려면 **show hw-crypto** 명령을 입력합니다.

단계 **7** **Agreement(**계약**)** 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 **8** **OK(**확인**)**를 클릭하여 구성 대화 상자를 닫습니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 애플리케이션 내에서 보안 정책 구성을 시작할 수 있습니다.



단계 **10** FTD를 매니지드 디바이스로 추가하고 보안 정책 구성을 시작하려면 FMC 구성 가이드를 참조합니다.

고가용성 쌍 추가

FTD 고가용성(장애 조치라고도 함)은 FXOS가 아닌 애플리케이션 내에 구성됩니다. 그러나 고가용성을 사용할 수 있도록 섀시를 준비하려는 경우 다음 단계를 참조하십시오.

시작하기 전에

의 내용을 참조하십시오.

프로시저

단계 **1** 각 논리적 디바이스에 동일한 인터페이스를 할당합니다.

단계 **2** 페일오버 및 상태 링크용으로 데이터 인터페이스 1~2개를 할당합니다.

이러한 인터페이스는 두 섀시 간의 고가용성 트래픽을 교환합니다. 페일오버 및 상태 링크를 함께 사용하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다. 사용 가능한 인터페이스가 있다면 페일오버 및 상태 링크를 각각 별도로 사용할 수 있습니다. 상태 링크에는 최대 대역폭이 필요합니다. 관리 유형 인터페이스는 페일오버 또는 상태 링크용으로 사용할 수 없습니다. 페일오버 인터페이스와 같은 네트워크 세그먼트에 다른 디바이스가 없는 상태로 섀시 간에 스위치를 사용하는 것이 좋습니다.

컨테이너 인스턴스의 경우 데이터 공유 인터페이스는 페일오버 링크용으로 지원되지 않습니다. 상위 인터페이스 또는 EtherChannel에서 하위 인터페이스를 생성한 다음 각 인스턴스에 대해 페일오버 링크로 사용할 하위 인터페이스를 할당하는 것이 좋습니다. 동일한 상위 인터페이스에 있는 모든 하위 인터페이스를 페일오버 링크로 사용해야 합니다. 하위 인터페이스 하나를 페일오버 링크로 사용하고 다른 하위 인터페이스(또는 상위 인터페이스)를 일반 데이터 인터페이스로 사용할 수는 없습니다.

단계 **3** 논리적 디바이스에서 고가용성을 활성화합니다.

단계 **4** 고가용성을 활성화한 후에 인터페이스를 변경해야 하는 경우에는 먼저 스탠바이 유닛에서 변경을 수행한 다음 액티브 유닛에서 변경을 수행합니다.

Firepower Threat Defense 논리적 디바이스의 인터페이스 변경

FTD 논리적 디바이스에서 인터페이스를 할당 또는 할당 해제하거나 관리 인터페이스를 교체할 수 있습니다. 그런 다음, 에서 인터페이스 구성을 동기화할 수 있습니다.

새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 FTD 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칩니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 FTD 구성의 여러 위치에서 인터페이스를 직접 참조

할 수 있습니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다. 논리적 디바이스에 영향을 주거나 에서 동기화할 필요 없이 할당된 EtherChannel의 멤버십을 수정할 수도 있습니다.

시작하기 전에

- 인터페이스를 구성하고 실제 인터페이스 구성, 757 페이지 및 EtherChannel(포트 채널) 추가, 758 페이지에 따라 EtherChannel을 추가합니다.
- 모든 인터페이스가 기본적으로 클러스터에 할당된 경우와 같이 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우에는 먼저 논리적 디바이스에서 인터페이스 할당을 해제한 다음 EtherChannel에 인터페이스를 추가해야 합니다. 새 EtherChannel의 경우 이렇게 한 후에 디바이스에 EtherChannel을 할당할 수 있습니다.
- 관리 또는 Firepower 이벤트 인터페이스를 관리 EtherChannel로 교체하려는 경우에는 미할당 데이터 멤버 인터페이스가 하나 이상 포함된 EtherChannel을 생성한 다음 현재 관리 인터페이스를 EtherChannel로 교체해야 합니다. FTD가 리부팅되고(관리 인터페이스를 변경하면 리부팅됨) 에서 구성을 동기화한 후에는 이제 할당 해제된 관리 인터페이스를 EtherChannel에 추가할 수도 있습니다.
- 클러스터링 또는 고가용성의 경우에는 에서 구성을 동기화하기 전에 모든 유닛에서 인터페이스를 추가하거나 제거해야 합니다. 인터페이스는 먼저 데이터/스탠바이 유닛에서 변경한 후에 제어/액티브 유닛에서 변경하는 것이 좋습니다. 새 인터페이스는 관리를 위해 다운된 상태로 추가되므로 인터페이스 모니터링에는 영향을 주지 않습니다.

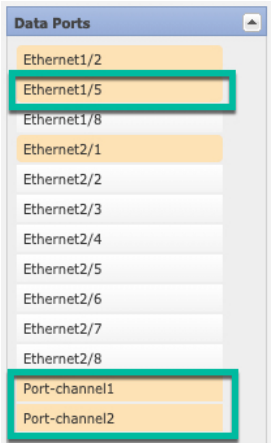
프로시저

단계 **1** Firepower Chassis Manager에서 **Logical Devices(**논리적 디바이스**)**를 선택합니다.

단계 **2** 오른쪽 상단의 **Edit(**수정**)** 아이콘을 클릭하여 논리적 디바이스를 수정합니다.

단계 **3** **Data Ports(**데이터 포트**)** 영역에서 인터페이스를 선택하여 새 데이터 인터페이스를 할당합니다.

아직 인터페이스를 삭제하지 마십시오.



단계 **4** 관리 또는 이벤트 처리 인터페이스를 교체합니다.

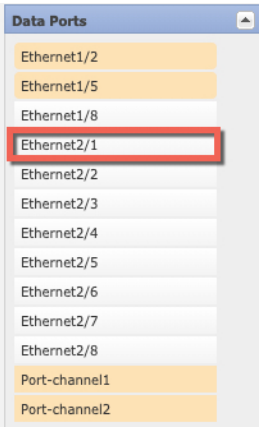
이러한 인터페이스 유형의 경우 변경 사항을 저장하고 나면 디바이스가 리부팅됩니다.

a) 페이지 중앙의 디바이스 아이콘을 클릭합니다.
b) **General(**일반**)** 또는 **Cluster Information(**클러스터 정보**)** 탭의 드롭다운 목록에서 새 **Management Interface(**관리 인터페이스**)**를 선택합니다.
c) **Settings(**설정**)** 탭의 드롭다운 목록에서 새 **Eventing Interface(**이벤트 인터페이스**)**를 선택합니다.
d) **OK(**확인**)**를 클릭합니다.

관리 인터페이스의 IP 주소를 변경하는 경우에는 Firepower Management Center에서 디바이스의 IP 주소도 변경해야 합니다. 이렇게 하려면 **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device/Cluster(**디바이스/클러스터**)**로 이동합니다. **Management(**관리**)** 영역에서 부트스트랩 구성 주소와 일치하도록 IP 주소를 설정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** Firepower Chassis Manager의 **Data Ports(**데이터 포트**)** 영역에서 인터페이스를 선택 취소하여 데이터 인터페이스를 할당 해제합니다.



단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 에서 인터페이스를 다시 동기화합니다.

애플리케이션 콘솔에 연결

다음 절차를 수행하여 애플리케이션의 콘솔에 연결합니다.

프로시저

단계 **1** 콘솔 연결 또는 텔넷 연결을 사용하여 모듈 CLI에 연결합니다.

connect module *slot_number* {**console** | **telnet**}

여러 보안 모듈을 지원하지 않는 디바이스의 보안 엔진에 연결하려면 항상 **1**을 *slot_number*로 사용합니다.

텔넷 연결 사용 시에는 동시에 여러 세션을 모듈에 연결할 수 있으며 연결 속도가 더 빠르다는 이점이 있습니다.

예제:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

단계 **2** 애플리케이션 콘솔에 연결합니다.

connect ftd *name*

인스턴스 이름을 확인하려면 이름 없이 명령을 입력합니다.

예제:

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

단계 **3** 애플리케이션 콘솔을 FXOS 모듈 CLI로 종료합니다.

- FTD - **exit**를 입력합니다.

단계 **4** FXOS CLI의 Supervisor(관리자) 수준으로 돌아갑니다.

콘솔을 종료합니다**.**

a) **~**를 입력합니다.

텔넷 애플리케이션을 종료합니다.

b) 텔넷 애플리케이션을 종료하려면 다음을 입력합니다.

telnet>**quit**

텔넷 세션을 종료합니다**.**

a) **Ctrl-], .**를 입력합니다.

History for Firepower Threat Defense Logical Devices

기능	버전	세부 사항
FTD 작동 링크 상태와 물리적 링크 상태 간 동기화	6.7	이제 섀시가 FTD 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. FTD 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 FTD에서 동기화하지 않으면 FTD 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 FTD 종료를 시작한 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 인라인 집합의 경우 FTD에서 트래픽을 처리하기 전에 외부 라우터가 FTD로 트래픽 전송을 시작할 수 있으므로 이러한 상태 불일치로 인해 패킷이 삭제될 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다. 참고 이 기능은 클러스터링, 컨테이너 인스턴스 또는 Radware vDP 데코레이터가 포함된 FTD에는 지원되지 않습니다. ASA에서도 지원되지 않습니다. 신규/수정된 Firepower Chassis Manager 화면: **Logical Devices(**논리적 디바이스**) > Enable Link State(**링크 상태 활성화**)** 신규/수정된 FXOS 명령: **set link-state-sync enabled**, **show interface expand detail**
컨테이너 인스턴스에 FMC를 사용하여 FTD 구성 백업 및 복원	6.7	이제 FTD 컨테이너 인스턴스에서 FMC 백업/복원 도구를 사용할 수 있습니다. 신규/수정된 FMC 화면: **System(**시스템**) > Tools(**도구**) > Backup/Restore(**백업/복원**) > Managed Device Backup(**매니지드 디바이스 백업**)** 신규/수정된 FTD CLI 명령: **restore** 지원되는 플랫폼: Firepower 4100/9300 참고 FXOS 2.9가 필요합니다.

기능	버전	세부 사항
클러스터 유형 인터페이스의 VLAN 하위 인터페이스 지원(다중 인스턴스 전용)	6.6	다중 인스턴스 클러스터에 사용하기 위해 클러스터 유형 인터페이스에서 VLAN 하위 인터페이스를 생성할 수 있습니다. 각 클러스터에는 고유한 클러스터 제어 링크가 필요하므로 VLAN 하위 인터페이스는 이 요구 사항을 충족하는 간단한 방법을 제공합니다. 아니면 클러스터마다 전용 EtherChannel을 할당해도 됩니다. 이제 여러 클러스터 인터페이스가 허용됩니다. 신규/수정된 Firepower Chassis Manager 화면: **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Add New(**새로 추가**)** 드롭다운 메뉴 **> Subinterface(**하위 인터페이스**)** > **Type(**유형**)** 필드 신규/수정된 FXOS 명령: **set port-type** 클러스터 참고 FXOS 2.8.1이 필요합니다.
FTD Firepower 4112	6.6	Firepower 4112가 도입되었습니다. 참고 FXOS 2.8.1이 필요합니다.
여러 컨테이너 인스턴스에 대한 TLS 암호화 가속	6.5	TLS 암호화 가속은 이제 Firepower 4100/9300 섀시의 여러 컨테이너 인스턴스(최대 16 개)에서 지원됩니다. 이전에는 모듈/보안 엔진 당 하나의 컨테이너 인스턴스에 대해서만 TLS 암호화 가속을 활성화 할 수 있었습니다. 새 인스턴스에는 기본적으로 이 기능이 활성화되어 있습니다. 그러나 업그레이드는 기존 인스턴스에서 가속화를 활성화하지 않습니다. 대신 **enter hw-crypto** 및 **set admin-state enabled** FXOS 명령을 사용합니다. 신규/수정된 Firepower Chassis Manager 화면: **Logical Devices(**논리 디바이스**)** > **Add Device(**디바이스 추가**)** > **Settings(**설정**)** > **Hardware Crypto(**하드웨어 암호화**)** 드롭 다운 메뉴 참고 FXOS 2.7.1이 필요합니다.
FTD Firepower 4115, 4125, 4145	6.4	Firepower 4115, 4125, 및 4145를 도입했습니다. 참고 FXOS 2.6.1.157이 필요합니다.
Firepower 9300 SM-40, SM-48 및 SM-56지원	6.4	다음 세 가지 보안 모듈을 도입했습니다: SM-40, SM-48, SM-56 참고 FXOS 2.6.1.157이 필요합니다.

기능	버전	세부 사항
동일한 Firepower 9300의 별도의 모듈에서 ASA 및 FTD에 대한 지원	6.4	이제 동일한 Firepower 9300에서 ASA 및 FTD 논리적 디바이스를 구축할 수 있습니다. 참고 FXOS 2.6.1.157이 필요합니다.
모듈/보안 엔진에서 하나의 FTD 컨테이너 인스턴스에 대한 SSL 하드웨어 가속 지원	6.4	이제 모듈/보안 엔진에서 하나의 컨테이너 인스턴스에 대해 SSL 하드웨어 가속을 활성화할 수 있습니다. SSL 하드웨어 가속은 다른 컨테이너 인스턴스에 대해서는 비활성화되어 있지만 기본 인스턴스에 대해서는 활성화되어 있습니다. 신규/수정된 FXOS 명령: **config hwCrypto enable** 수정된 화면이 없습니다. 참고 FXOS 2.6.1.157이 필요합니다.

기능	버전	세부 사항
Firepower 4100/9300에 대한 Firepower Threat Defense의 다중 인스턴스 기능	6.3	

기능	버전	세부 사항
		이제 단일 보안 엔진/모듈에서 각 Firepower Threat Defense 컨테이너 인스턴스로 여러 논리적 디바이스를 구축할 수 있습니다. 이전에는 단일 기본 애플리케이션 인스턴스만 구축할 수 있었습니다. 물리적 인터페이스를 유연하게 사용할 수 있도록 FXOS에서 VLAN 하위 인터페이스를 생성하는 동시에 여러 인스턴스 간에 인터페이스를 공유할 수 있습니다. 리소스 관리를 사용하면 각 인스턴스에 대한 성능 기능을 맞춤화할 수 있습니다. 2개의 개별 섀시에서 컨테이너 인스턴스를 활용한 고가용성을 사용할 수 있습니다. 클러스터링은 지원되지 않습니다. 참고 다중 인스턴스 기능은 ASA 다중 컨텍스트 모드와 비슷하지만 구현은 서로 다릅니다. Firepower Threat Defense에서는 다중 컨텍스트 모드를 사용할 수 없습니다. 신규/수정된 Firepower Management Center 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**수정**)** 아이콘 **>** **Interfaces(**인터페이스**)** 탭 신규/수정된 Firepower Chassis Manager 화면: • **Overview(**개요**)** > **Devices(**디바이스**)** • **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Add New(**새로 추가**)** 드롭다운 메뉴 **>** **Subinterface(**하위 인터페이스**)** • **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Type(**유형**)** • **Logical Devices(**논리적 디바이스**)** > **Add Device(**디바이스 추가**)** • **Platform Settings(**플랫폼 설정**)** > **MAC Pool(MAC** 풀**)** • **Platform Settings(**플랫폼 설정**)** > **Resource Profiles(**리소스 프로파일**)** 신규/수정된 FXOS 명령: **connect ftd** *name*, **connect module telnet, createbootstrap-key PERMIT_EXPERT_MODE, create resource-profile, create subinterface, scope auto-macpool, set cpu-core-count, set deploy-type, set port-type data-sharing, set prefix, set resource-profile-name, setvlan, scope app-instance ftd** *name***, show cgroups container, show interface, show mac-address, show subinterface, show tech-support module app-instance, show version**

기능	버전	세부 사항
		지원되는 플랫폼: Firepower 4100/9300
Firepower 4100/9300에 대한 클러스터 제어 링크의 맞춤화 가능한 IP 주소	6.3	기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 이제 FXOS에서 클러스터를 구축하는 경우 네트워크를 설정할 수 있습니다. 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id*.*slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 따라서 이제 FXOS에서 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외하고 클러스터 제어 링크의 맞춤형 /16 서브넷을 설정할 수 있습니다. 신규/수정된 Firepower Chassis Manager 화면: • **Logical Devices(**논리적 디바이스**)** > **Add Device(**디바이스 추가**)** > **Cluster Information(**클러스터 정보**)** > **CCL Subnet IP(CCL** 서브넷 **IP)** 필드 신규/수정된 FXOS 명령: **set cluster-control-link network** 지원되는 플랫폼: Firepower 4100/9300
On(켜기) 모드에서 데이터 EtherChannel 지원	6.3	이제 데이터 및 데이터 공유 EtherChannel을 Active LACP(액티브 LACP) 모드 또는 On(켜기) 모드로 설정할 수 있습니다. 다른 유형의 Etherchannel은 Active(액티브) 모드만 지원합니다. 신규/수정된 Firepower Chassis Manager 화면: • **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Edit Port Channel(**포트 채널 수정**)** > **Mode(**모드**)** 신규/수정된 FXOS 명령: **set port-channel-mode** 지원되는 플랫폼: Firepower 4100/9300
FTD 인라인 집합에서 EtherChannel 지원	6.2	이제 FTD 인라인 집합에서 EtherChannel을 사용할 수 있습니다. 지원되는 플랫폼: Firepower 4100/9300
FTD 모듈 6개를 위한 섀시 간 클러스터링	6.2	이제 FTD를 위한 섀시 간 클러스터링을 활성화할 수 있습니다. 최대 6개의 섀시에 최대 6개의 모듈을 포함할 수 있습니다. 신규/수정된 Firepower Chassis Manager 화면: • 논리적 디바이스 > 구성 지원되는 플랫폼: Firepower 4100/9300

기능	버전	세부 사항
지원되는 네트워크 모듈용 Firepower 4100/9300에 대한 하드웨어 우회 지원	6.1	Hardware Bypass는 정전 중에 트래픽이 인라인 인터페이스 쌍 사이에서 계속 흐르도록 합니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** 지원되는 플랫폼: Firepower 4100/9300
인라인 집합 링크 상태 전파 지원 FTD	6.1	FTD 애플리케이션에서 인라인 집합을 구성하고 링크 상태 전파를 활성화하면 FTD에서 FXOS 섀시로 인라인 집합 멤버십을 전송합니다. 링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 중단될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다. 신규/수정된 FXOS 명령: **show fault |grep link-down**, **show interface detail** 지원되는 플랫폼: Firepower 4100/9300
Firepower 9300의 FTD에서 인트라 섀시 클러스터링(intra-chassis clustering) 지원	6.0.1	Firepower 9300은 FTD 애플리케이션이 있는 인트라 섀시 클러스터링(intra-chassis clustering)을 지원합니다. 신규/수정된 Firepower Chassis Manager 화면: • 논리적 디바이스 > 설정 신규/수정된 FXOS 명령: **enter mgmt-bootstrap ftd, enter bootstrap-key FIREPOWER_MANAGER_IP, enter bootstrap-key FIREWALL_MODE, enter bootstrap-key-secret REGISTRATION_KEY, enter bootstrap-key-secret PASSWORD, enter bootstrap-key FQDN, enter bootstrap-key DNS_SERVERS, enter bootstrap-key SEARCH_DOMAINS, enter ipv4 firepower, enter ipv6 firepower, set value, set gateway, set ip, accept-license-agreement** 지원되는 플랫폼: Firepower 4100/9300

VII 부

Firepower Threat Defense 인터페이스 및 디바이스 설정

- Firepower Threat Defense 인터페이스 개요, 783 페이지
- Firepower Threat Defense 일반 방화벽 인터페이스, 793 페이지
- Firepower Threat Defense 인라인 집합 및 패시브 인터페이스, 847 페이지
- Threat Defense용 DHCP 및 DDNS 서비스, 859 페이지
- Firepower 1000/2100 용 SNMP, 873 페이지
- QoS(Quality of Service) Firepower Threat Defense, 879 페이지

28 장

Firepower Threat Defense 인터페이스 개요

FTD 디바이스에는 여러 모드를 설정할 수 있는 데이터 인터페이스와 관리/진단 인터페이스가 포함됩니다.

- 관리/진단 인터페이스, 783 페이지
- 인터페이스 모드 및 유형, 784 페이지
- 보안 영역 및 인터페이스 그룹, 785 페이지
- Auto-MDI/MDIX 기능, 786 페이지
- 인터페이스의 기본 설정, 786 페이지
- 물리적 인터페이스 활성화 및 이더넷 설정, 787 페이지
- Firepower Management Center를 사용한 동기화 인터페이스 변경, 788 페이지

관리/진단 인터페이스

물리적 관리 인터페이스는 논리적 진단 인터페이스와 논리적 관리 인터페이스 간에 공유됩니다.

관리 인터페이스

관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 Firepower Management Center에 설치하고 등록하는 데 사용됩니다. 고유 IP 주소 및 정적 라우팅을 사용합니다. **configure network** 명령을 사용해 CLI에서 설정을 구성할 수 있습니다. Firepower Management Center에 IP 주소를 추가한 뒤 CLI에서 IP 주소를 변경하는 경우, **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Devices(**디바이스**)** > **Management(**관리**)** 영역의 Firepower Management Center에서 IP 주소를 일치시킬 수 있습니다.

관리 인터페이스 대신 데이터 인터페이스를 사용하여 FTD를 관리할 수도 있습니다.

진단 인터페이스

논리적 진단 인터페이스는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** 화면에서 나머지 데이터 인터페이스와 함께 설정할 수 있습니다. 진단 인터페이스 사용은 선택 사항입니다(라우팅 및 투명 모드 구축 시나리오 참조). 진단 인터페이스는 관리 트래픽만 허용

하며 통과 트래픽은 허용하지 않습니다. SSH를 지원하지 않습니다. 데이터 인터페이스 또는 관리 인터페이스 사용 시에만 SSH를 사용할 수 있습니다. 진단 인터페이스는 SNMP 또는 시스템 로그 모니터링에 유용합니다.

인터페이스 모드 및 유형

일반 방화벽 모드와 IPS 전용 모드에서 FTD 인터페이스를 구축할 수 있습니다. 동일한 디바이스에 방화벽 및 IPS 전용 인터페이스를 포함시킬 수 있습니다.

일반 방화벽 모드

방화벽 모드 인터페이스는 IP 및 TCP 레이어, IP 조각 모음, TCP 표준화에서 플로우 유지, 플로우 상태 추적 등의 방화벽 기능에 트래픽을 적용합니다. 필요한 경우 보안 정책에 따라 해당 트래픽에 대한 IPS 기능을 구성할 수도 있습니다.

구성할 수 있는 방화벽 인터페이스의 유형은 디바이스의 방화벽 모드 집합이 라우팅인지 투명 모드인지에 따라 달라집니다. 자세한 내용은 Firepower Threat Defense에 대한 투명 또는 라우팅 방화벽 모드, 711 페이지를 참조하십시오.

- 라우팅 모드 인터페이스(라우팅된 방화벽 모드 전용) - 서로 라우팅하려는 각 인터페이스가 다른 서브넷에 있습니다.
- 브리지 그룹 인터페이스(라우팅 및 투명 방화벽 모드 - 네트워크의 여러 인터페이스를 그룹화할 수 있고 Firepower Threat Defense 디바이스는 브리지 기술을 사용해 인터페이스 간 트래픽을 전달합니다. 각 브리지 그룹은 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)를 포함합니다. 라우팅 모드에서 Firepower Threat Defense 디바이스는 BVI 및 일반 라우팅 인터페이스를 라우팅합니다. 투명 모드에서 의 각 브리지 그룹은 구분되며 서로 통신할 수 없습니다.

IPS 전용 모드

IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 이런 인터페이스를 보호하는 개별 방화벽이 있고 방화벽 기능의 오버헤드를 원하지 않는 경우 IPS 전용 인터페이스를 구현합니다.

참고 방화벽 모드는 일반 방화벽 인터페이스에만 영향을 주고 인라인 집합이나 패시브 인터페이스 등 IPS 전용 인터페이스에는 영향을 주지 않습니다. 두 개의 방화벽 모드 모두에서 IPS 전용 인터페이스를 사용할 수 있습니다.

IPS 전용 인터페이스는 다음과 같은 유형으로 구축할 수 있습니다.

- 필요에 따라 탭 모드가 가능한 인라인 집합 - 인라인 집합은 비활성 엔드포인트(bump in the wire)처럼 작동하며 두 인터페이스를 슬롯에 포함해 기존 네트워크에 바인딩합니다. 이 기능을 사용하면 인접한 네트워크 디바이스의 설정 없이 네트워크 환경에 FTD를 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

탭 모드에서는 FTD가 인라인으로 구축되지만, 네트워크 트래픽 플로우는 방해받지 않습니다. 대신 FTD는 패킷을 분석할 수 있도록 각 패킷의 복사본을 만듭니다. 트리거되면 이런 유형의 규칙은 침입 이벤트를 생성하며, 침입 이벤트의 테이블 보기는 인라인 구축에서 트리거링 패킷이 삭제되었을 수도 있음을 표시합니다. 인라인으로 구축된 FTD에서 탭 모드를 사용하는 데는 몇 가지 이점이 있습니다. 예를 들어, 디바이스가 인라인 상태인 것처럼 FTD와 네트워크 간에 케이블링을 설정할 수 있으며 FTD가 생성하는 침입 이벤트의 종류를 분석할 수 있습니다. 결과를 기반으로 침입 정책을 수정할 수 있으며, 효율성 저하 없이 네트워크를 가장 잘 보호하는 삭제 규칙을 추가할 수 있습니다. FTD를 인라인으로 구축할 준비가 되면 FTD와 네트워크 간 케이블링을 다시 설정하지 않고도 탭 모드를 비활성화하고 의심스러운 트래픽을 삭제할 수 있습니다.

참고 탭 모드는 트래픽에 따라 FTD 성능에 상당한 영향을 줍니다.

참고 인라인 집합은 "투명 인라인 집합"으로 익숙할 수 있지만 인라인 인터페이스 유형은 투명 방화벽 모드 또는 방화벽 유형 인터페이스와는 관련이 없습니다.

- 패시브 또는 ERSPAN 패시브 - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용해 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 패시브 구축으로 FTD를 설정한 경우, FTD에서 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며, 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 캡슐화된 원격 스위치 포트 분석기(ERSPAN) 인터페이스는 여러 스위치를 통해 배포되는 소스 포트의 트래픽을 모니터링하고 GRE를 사용해 트래픽을 캡슐화합니다. ERSPAN 인터페이스는 FTD가 라우팅된 방화벽 모드에 있을 때만 허용됩니다.

보안 영역 및 인터페이스 그룹

각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당될 수 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어, "내부" 인터페이스는 "내부" 영역에, "외부" 인터페이스는 "외부" 영역에 할당할 수 있습니다. 예를 들어, 트래픽이 내부에서 외부로는 이동하되 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 인터페이스 또는 영역 이름 자체는 보안 정책과 관련하여 기본 동작을 제공하지 않습니다. 향후 설정에서 실수를 방지하려면 자체 설명 이름을 사용하는 것이 좋습니다. 올바른 이름은 논리적 세그먼트 또는 트래픽 사양을 나타냅니다. 예를 들면 다음과 같습니다.

- 내부 인터페이스의 이름 - InsideV110, InsideV160, InsideV195
- DMZ 인터페이스의 이름 - DMZV11, DMZV12, DMZV-TEST
- 외부 인터페이스의 이름 - Outside-ASN78, Outside-ASN91

일부 정책은 보안 영역만 지원하고 일부 정책은 영역 및 그룹을 지원합니다. 자세한 내용은 보안 영역, 577 페이지를 참조하십시오. 개체 페이지에서 보안 영역 및 인터페이스 그룹을 생성할 수 있습니다. 인터페이스를 구성하는 경우 영역을 추가할 수 있습니다. 패시브, 인라인, 라우팅, 스위치 영역 유형 등 인터페이스의 올바른 영역 유형에만 인터페이스를 추가할 수 있습니다.

참고 모든 영역(전역 정책)에 적용되는 정책은 영역의 인터페이스 및 영역에 할당되지 않은 인터페이스에도 적용됩니다.

진단/관리 인터페이스는 영역 또는 인터페이스 그룹에 속하지 않습니다.

Auto-MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 사용 해제하면 Auto-MDI/MDIX도 사용 해제됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

인터페이스의 기본 설정

이 섹션에서는 인터페이스에 대한 기본 설정이 나열됩니다.

인터페이스의 기본 상태

인터페이스의 기본 상태는 유형에 따라 다릅니다.

- 물리적 인터페이스 - 비활성화됨. 초기 설정에 대해 활성화된 진단 인터페이스는 예외입니다.
- 이중 인터페이스 — 활성화되어 있습니다. 그러나 트래픽이 이중 인터페이스를 통과하려면 물리적 인터페이스 멤버도 활성화되어야 합니다.
- VLAN 하위 인터페이스 - 활성화됨, 그러나 트래픽이 하위 인터페이스를 통과하려면 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 - 채널 인터페이스 (ASA 모델) - 활성화되어 있습니다. 그러나 EtherChannel을 통해 트래픽을 전달하려면 채널 그룹 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 - 채널 인터페이스(Firepower 모델) - 비활성화되어 있습니다.

기본 속도와 양방향

기본적으로 구리(RJ-45) 인터페이스의 속도와 양방향은 자동 협상이 이루어지도록 설정됩니다.

물리적 인터페이스 활성화 및 이더넷 설정

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 물리적 인터페이스 활성화 기본적으로 물리적 인터페이스는 비활성화됩니다(진단 인터페이스의 경우는 제외).
- 특성 속도 및 양방향 설정 기본적으로 속도 및 양방향은 자동으로 설정되어 있습니다.

이 절차에서는 인터페이스 설정의 작은 하위 집합에 대해서만 설명합니다. 이 시점에서 다른 파라미터 설정은 하지 않는 것이 좋습니다. 예를 들면 EtherChannel 또는 이중 인터페이스의 일부로 사용하려는 인터페이스의 이름을 지정할 수 없습니다.

참고 Firepower 4100/9300의 경우 기본 인터페이스 설정을 FXOS로 구성합니다. 자세한 내용은 실제 인터페이스 구성, 757 페이지를 참조하십시오.

참고 Firepower 1010 스위치 포트에 대해서는 Firepower 1010 스위치 포트 구성, 794 페이지의 내용을 참조하십시오.

시작하기 전에

FMC에 추가한 후 디바이스의 물리적 인터페이스를 변경한 경우, **Interfaces(**인터페이스**)**의 왼쪽 상단에 있는 **Sync Interfaces from device(**디바이스의 인터페이스 동기화**)**를 클릭하여 인터페이스 목록을 새로 고쳐야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

단계 **3** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **4** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **5** (선택 사항) **Hardware Configuration(**하드웨어 설정**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.

- **Duplex(**듀플렉스**) - Auto(**자동**)**를 선택하여 인터페이스가 듀플렉스를 협상하도록 하거나(Auto(자동)는 RJ-45 인터페이스에서만 사용 가능) 특정 **Half(**하프**)**, **Full(**풀**)** 듀플렉스를 선택합니다.
- **Speed(**속도**)** — **Auto(**자동**)**를 선택하여 인터페이스가 속도를 협상하도록 하거나(Auto(자동)는 RJ-45 인터페이스에서만 사용 가능), **10**, **100**, **1000**, **10000**Mbps 중에서 특정 속도를 선택합니다. SFP 인터페이스의 경우, 하드웨어에 따라 **No Negotiate(**협상 없음**)**를 선택하여 속도를 1000으로 설정하고 링크 협상을 비활성화할 수 있습니다.

단계 **6** 모드 드롭다운 목록에서 다음을 선택합니다.

- 없음 - 일반 방화벽 인터페이스 및 인라인 집합을 설정하려면 이 옵션을 선택합니다. 추가 설정에 따라 라우팅, 스위치, 인라인 모드로 자동 변경됩니다.
- 패시브 - 패시브 IPS 전용 인터페이스의 경우 이 설정을 선택합니다.
- **Erspan** - ERSPAN 패시브 IPS 전용 인터페이스의 경우 이 설정을 선택합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**) > Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Firepower Management Center를 사용한 동기화 인터페이스 변경

디바이스의 인터페이스 설정 변경은 FMC과 디바이스의 동기화 오류를 발생시킬 수 있습니다. FMC은 다음 방법 중 하나로 인터페이스 변경을 탐지할 수 있습니다.

- 디바이스에서 전송된 이벤트
- 에서 구축할 때 동기화 FMC

  FMC이 구축을 시도하지만 실패하는 경우 인터페이스 변경 사항을 탐지합니다. 먼저 인터페이스 변경 사항을 적용해야 합니다.

- 수동 동기화

FMC 외부에서 수행되는 두 가지 유형의 인터페이스 변경은 동기화되어야 합니다.

- 물리적 인터페이스 추가 또는 삭제 - 새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 FTD 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칩니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 FTD 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 인터페이스를 삭제하면 해

당 인터페이스와 연결된 모든 구성이 삭제됩니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다. 논리적 디바이스에 영향을 주거나 FMC에서 동기화할 필요 없이 할당된 EtherChannel의 멤버십을 수정할 수도 있습니다.

FMC가 변경 사항을 탐지하는 경우 인터페이스 페이지는 각 인터페이스 왼쪽에 상태(제거, 변경, 추가)를 표시합니다.

- FMC 액세스 인터페이스 변경 - **configure network management-data-interface** 명령을 사용하여 FMC 관리용 데이터 인터페이스를 구성하는 경우 FMC에서 일치하는 구성 변경을 수동으로 수행한 다음 변경을 승인해야 합니다. 이러한 인터페이스 변경은 자동으로 수행할 수 없습니다.

이 절차는 필요한 경우 디바이스 변경 사항을 수동으로 동기화하는 방법과 탐지된 변경 사항을 인식하는 방법을 설명합니다. 디바이스가 임시로 변경되는 경우 FMC에 변경 사항을 저장하지 말고 디바이스가 안정될 때까지 기다린 뒤 다시 동기화해야 합니다.

시작하기 전에

- 모델 지원—FTD
- 사용자 역할:
  - 관리자
  - 액세스 관리자
  - Network Admin(네트워크 관리자)

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 필요한 경우 인터페이스 왼쪽 상단의 디바이스 동기화를 클릭합니다.

단계 **3** 변경 사항이 탐지되면 다음 단계를 참조하십시오.

물리적 인터페이스 추가 또는 삭제

a) **Interfaces(**인터페이스**)**에 인터페이스 구성이 변경되었음을 나타내는 빨간색 배너가 표시됩니다. 인터페이스 변경 사항을 보려면 클릭하여 더 보기 링크를 클릭합니다.

b) 인터페이스 변경 이후에도 정책이 계속 작동할 수 있도록 변경 사항 유효성 확인을 클릭합니다.

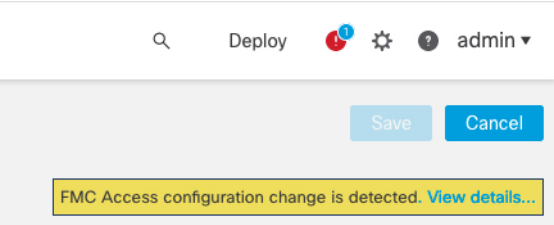
오류가 발생하는 경우 정책을 변경하고 유효성 검사를 다시 실행해야 합니다.

c) **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다.

FMC 액세스 인터페이스 변경

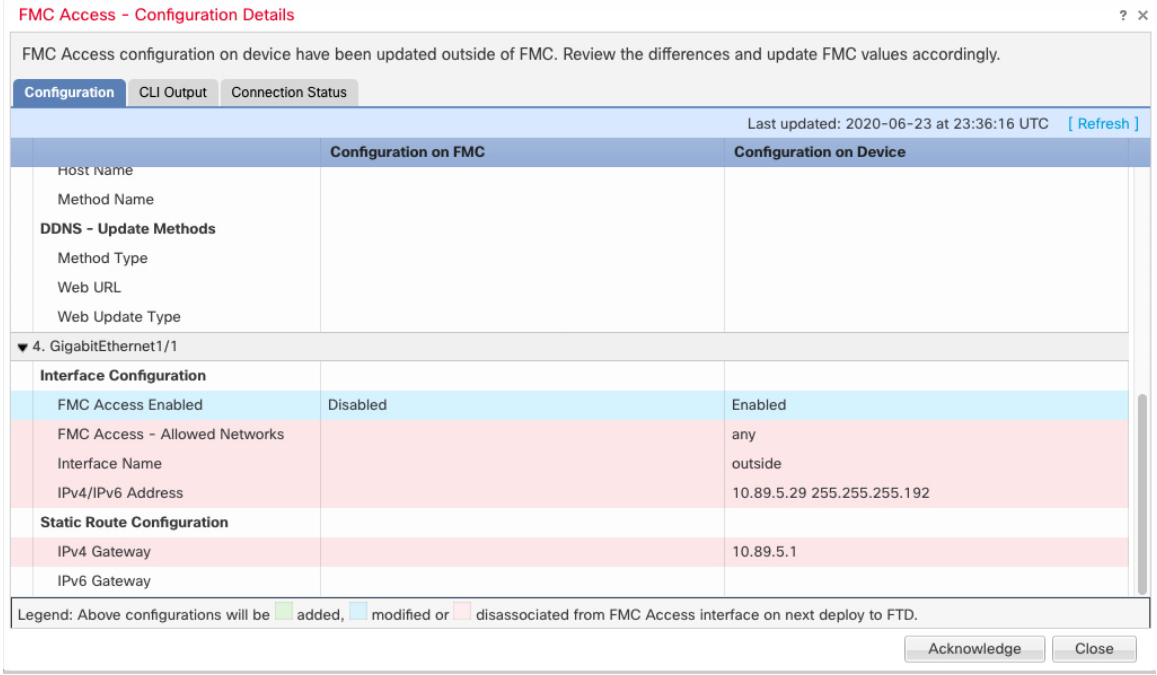
a) **Device(**디바이스**)** 페이지의 오른쪽 상단에 FMC 액세스 구성이 변경되었음을 나타내는 노란색 배너가 표시됩니다. 인터페이스 변경 사항을 보려면 세부 정보 보기 링크를 클릭합니다.



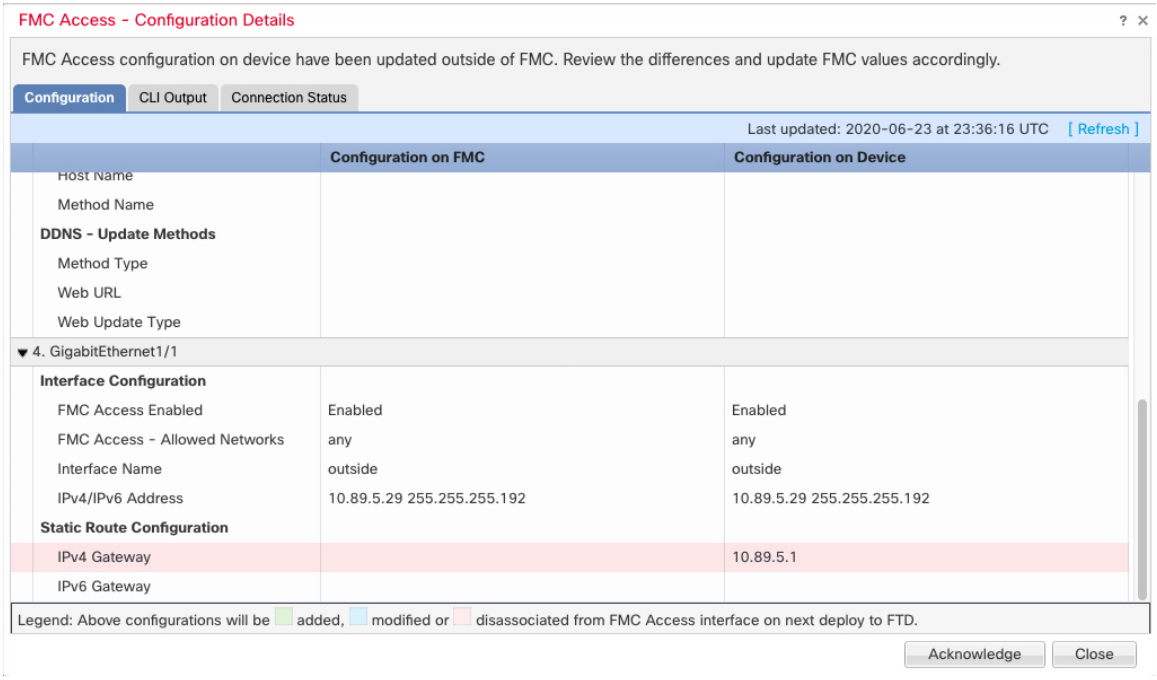
FMC Access - Configuration Details(FMC 액세스 - 구성 세부 정보**)** 대화 상자가 열립니다.

b) 강조 표시된 모든 구성, 특히 빨간색으로 강조 표시된 구성을 확인합니다. FMC에서 수동으로 값을 구성하여 FTD의 값을 일치시켜야 합니다.

예를 들어 아래의 분홍색 강조 표시는 FTD에는 있지만 아직 FMC에는 없는 구성을 보여줍니다.



다음 예는 FMC에서 인터페이스를 구성한 후의 이 페이지를 보여줍니다. 인터페이스 설정이 일치하고 분홍색 강조 표시가 제거되었습니다.



c) **Acknowledge(**승인**)**를 클릭합니다.

FMC 구성을 완료하고 구축 준비가 완료될 때까지 **Acknowledge(**승인**)**를 클릭하지 않는 것이 좋습니다. **Acknowledge(**승인**)**를 클릭하면 구축시 차단이 제거됩니다. 다음에 구축할 때 FMC 컨피그레이션은 FTD의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 FMC에서 컨피그레이션을 수동으로 수정하는 것은 사용자의 책임입니다.

d) 이제 **Deploy(**구축**) > Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다.

29 장

Firepower Threat Defense 일반 방화벽 인터페이스

이 장에는 EtherChannel, VLAN 하위 인터페이스, IP 주소 등 일반 방화벽 FTD 인터페이스 설정을 포함합니다.

참고 Firepower 4100/9300의 초기 인터페이스 설정에 대해서는 인터페이스 구성, 756 페이지를 참조합니다.

- 정규 방화벽 인터페이스 요구 사항 및 사전 요건, 793 페이지
- Firepower 1010 스위치 포트 구성, 794 페이지
- EtherChannel 및 이중 인터페이스 구성, 804 페이지
- VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성, 812 페이지
- 라우팅 및 투명 모드 인터페이스 구성, 814 페이지
- 고급 인터페이스 설정 구성, 832 페이지
- Firepower Threat Defense 일반 방화벽 인터페이스 기록, 843 페이지

정규 방화벽 인터페이스 요구 사항 및 사전 요건

모델 지원

FTD

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

Firepower 1010 스위치 포트 구성

각 Firepower 1010 인터페이스가 일반 방화벽 인터페이스 또는 레이어 2 하드웨어 스위치 포트로 실행되도록 구성할 수 있습니다. 이 섹션에는 스위치 모드의 활성화 또는 비활성화, VLAN 인터페이스 생성 및 스위치 포트에 할당하는 작업 등을 비롯한, 스위치 포트의 구성을 시작하기 위한 작업이 포함되어 있습니다. 이 섹션에서는 지원되는 인터페이스에서 PoE(Power over Ethernet)를 맞춤화하는 방법에 대해서도 설명합니다.

Firepower 1010 스위치 포트 관련 정보

이 섹션에서는 Firepower 1010의 스위치 포트를 설명합니다.

Firepower 1010 포트 및 인터페이스 이해

포트 및 인터페이스

각 물리적 Firepower 1010 인터페이스의 경우, 해당 작업을 방화벽 인터페이스 또는 스위치 포트로 설정할 수 있습니다. 물리적 인터페이스, 포트 유형 및 스위치 포트를 할당할 논리적 VLAN 인터페이스에 대한 다음과 같은 정보를 참조하십시오.

- 물리적 방화벽 인터페이스 - 라우팅 모드에서 이러한 인터페이스는 구성된 보안 정책을 사용해 방화벽과 VPN 서비스를 적용하여 레이어 3에서 네트워크 간에 트래픽을 전달합니다. 투명 모드에서 이러한 인터페이스는 구성된 보안 정책을 사용해 방화벽 서비스를 적용하여 레이어 2에서 동일한 네트워크에 있는 인터페이스 간에 트래픽을 전달하는 브리지 그룹 멤버입니다. 라우팅 모드에서는 일부 인터페이스와의 통합 라우팅 및 브리징을 브리지 그룹 멤버로 사용하고 기타 인터페이스를 레이어 3 인터페이스로 사용할 수도 있습니다. 기본적으로 Ethernet 1/1 인터페이스는 방화벽 인터페이스로 구성됩니다.이러한 인터페이스를 IPS 전용(인라인 집합 및 패시브 인터페이스)으로 구성할 수도 있습니다.

- 물리적 스위치 포트 - 스위치 포트에서는 하드웨어에서 스위칭 기능을 사용하여 레이어 2에서 트래픽을 전달합니다. 동일한 VLAN의 스위치 포트는 하드웨어 스위칭을 사용하여 서로 통신할 수 있으며 트래픽에는 FTD 보안 정책이 적용되지 않습니다. 액세스 포트의 경우 태그 없는 트래픽만 허용되며 이러한 포트는 단일 VLAN에 할당할 수 있습니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용되며 둘 이상의 VLAN에 속할 수 있습니다. 기본적으로, Ethernet 1/2~1/8은 VLAN 1에서 액세스 스위치 포트로 설정됩니다. 진단 인터페이스는 스위치 포트로 구성할 수 없습니다.

- 논리적 VLAN 인터페이스 - 이러한 인터페이스는 물리적 방화벽 인터페이스와 동일하게 작동합니다. 단, 하위 인터페이스, 이중 인터페이스, IPS 전용 인터페이스(인라인 집합 및 패시브 인터페이스) 또는 EtherChannel 인터페이스는 생성할 수 없습니다. 스위치 포트가 다른 네트워크와 통신해야 하는 경우, FTD에서 VLAN 인터페이스에 보안 정책을 적용하고 다른 논리적 VLAN 인터페이스 또는 방화벽 인터페이스로 라우팅됩니다. VLAN 인터페이스와의 통합 라우팅 및 브리징을 브리지 그룹 멤버로 사용할 수도 있습니다. 동일한 VLAN의 스위치 포트 간 트래픽에는 FTD 보안 정책이 적용되지 않지만, 브리지 그룹에 있는 VLAN 간의 트래픽에는 보안 정책이 적

용됩니다. 따라서 특정 세그먼트 간에 보안 정책을 적용하려면 레이어 브리지 그룹 및 스위치 포트를 계층화하도록 선택할 수 있습니다.

PoE(Power over Ethernet)

Ethernet 1/7 및 Ethernet 1/8에서는 PoE+(Power over Ethernet+)를 지원합니다.

Auto-MDI/MDIX 기능

Firepower 1010 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 사용 해제하면 Auto-MDI/MDIX도 사용 해제됩니다. 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

Firepower 1010 스위치 포트에 대한 지침 및 제한 사항

고가용성

- 고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 및 스탠바이 유닛에서 계속 트래픽을 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하기 위해 고안되었지만 스위치 포트로 확장되지는 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다. 이론적으로는 VLAN에 단일 스위치 포트를 배치하고 고가용성을 정상적으로 사용할 수 있지만, 물리적 방화벽 인터페이스를 대신 사용하면 더 간단하게 설정할 수 있습니다.
- 방화벽 인터페이스만 장애 조치 링크로 사용할 수 있습니다.

논리적 **VLAN** 인터페이스

- 최대 60개의 VLAN 인터페이스를 생성할 수 있습니다.
- 방화벽 인터페이스에서 VLAN 하위 인터페이스도 사용하는 경우에는 논리적 VLAN 인터페이스에 동일한 VLAN ID를 사용할 수 없습니다.
- MAC 주소:
  - 라우팅 방화벽 모드 - 모든 VLAN 인터페이스에서는 MAC 주소를 공유합니다. 연결된 스위치가 이 시나리오에 도움이 될 수 있을지 확인하십시오. 연결된 스위치에 고유한 MAC 주소가 필요한 경우, MAC 주소를 수동으로 할당할 수 있습니다. MAC 주소 구성, 838 페이지의 내용을 참조하십시오.

- 투명 방화벽 모드 - 각 VLAN 인터페이스에는 고유한 MAC 주소가 있습니다. 원하는 경우 MAC 주소를 수동으로 할당하여 생성된 MAC 주소를 재정의할 수 있습니다. MAC 주소 구성, 838 페이지의 내용을 참조하십시오.

브리지 그룹

동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수는 없습니다.

VLAN 인터페이스 및 스위치 포트에서 지원되지 않는 기능

VLAN 인터페이스 및 스위치 포트에서는 다음을 지원하지 않습니다.

- 동적 라우팅
- 멀티캐스트 라우팅
- ECMP(Equal-Cost Multi-Path) 라우팅
- 인라인 집합 또는 패시브 인터페이스
- EtherChannel
- 이중 인터페이스(Firepower 1010에서는 모든 인터페이스 유형에 대해 이중 인터페이스를 지원하지 않음)
- 장애 조치 및 상태 링크
- SGT(Security Group Tagging)

기타 지침 및 제한 사항

- Firepower 1010에서 명명된 인터페이스를 최대 60개 구성할 수 있습니다.
- 진단 인터페이스는 스위치 포트로 구성할 수 없습니다.

기본 설정

- Ethernet 1/1은 방화벽 인터페이스입니다.
- Ethernet 1/2~Ethernet 1/8은 VLAN 1에 할당된 스위치 포트입니다.
- 기본 속도 및 듀플렉스 - 기본적으로 속도 및 듀플렉스는 자동 협상으로 설정됩니다.

스위치 포트 및 PoE(Power over Ethernet) 구성

스위치 포트 및 PoE를 구성하려면 다음 작업을 완료합니다.

스위치 포트 모드 활성화 또는 비활성화

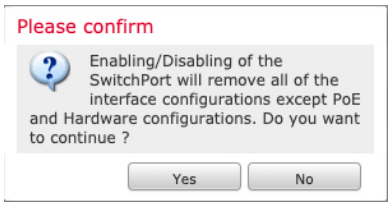
각 인터페이스를 방화벽 인터페이스나 스위치 포트 중 하나에 독립적으로 설정할 수 있습니다. 기본적으로 이더넷 1/1은 방화벽 인터페이스이며, 남은 이더넷 인터페이스는 스위치 포트로 구성됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** **SwitchPort** 열에서 슬라이더를 클릭해서 스위치 포트 모드를 설정해서 슬라이더 활성화됨( ) 또는 슬라이더 비활성화됨( )으로 표시되도록 합니다.

기본적으로 스위치 포트는 VLAN 1에서 액세스 모드로 설정됩니다. 논리적 VLAN 1 인터페이스(또는 이러한 스위치 포트에 설정한 모든 VLAN)를 수동으로 추가해 트래픽이 라우팅되고 FTD 보안 정책에 참여하게 합니다(자세한 내용은 VLAN 인터페이스 구성, 797 페이지의 내용을 참조하십시오). 진단 인터페이스는 스위치 포트 모드로 설정할 수 없습니다. 스위치 포트 모드를 변경하면 지원되지 않는 구성은 모두 제거됩니다.



VLAN 인터페이스 구성

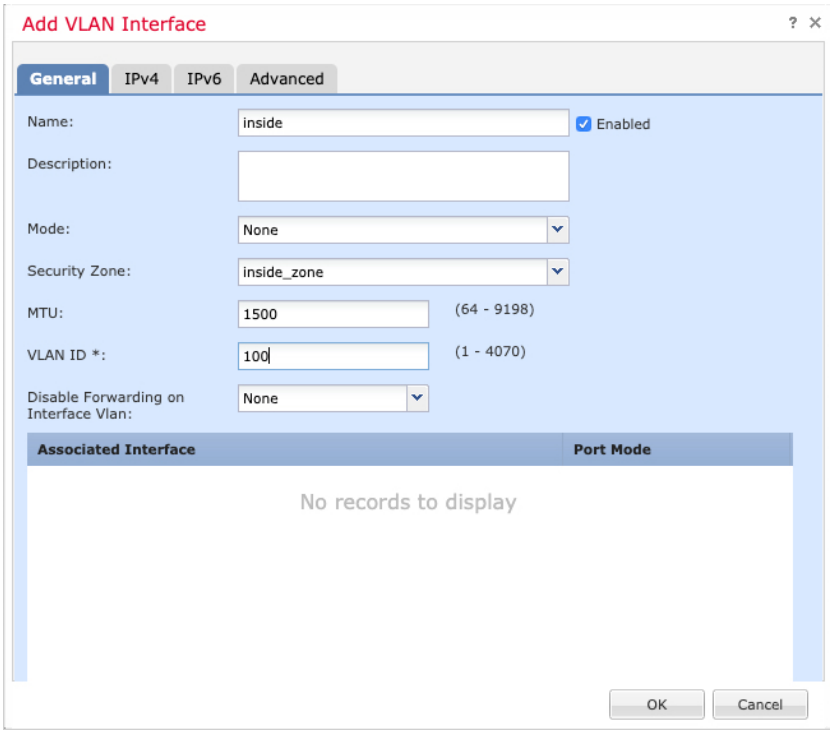
이 섹션에서는 연결된 스위치 포트에 사용할 VLAN 인터페이스를 구성하는 방법에 대해 설명합니다. 기본적으로 스위치 포트는 VLAN1에 할당됩니다. 하지만 논리적 VLAN1 인터페이스(또는 이러한 스위치 포트에 설정한 모든 VLAN)를 수동으로 추가해 트래픽이 라우팅되고 FTD 보안 정책에 참여하게 해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** **Add Interfaces(**인터페이스 추가**)** > **VLAN Interface(VLAN** 인터페이스**)**를 클릭합니다.

단계 **3** **General(**일반**)**에서 다음 VLAN 전용 매개변수를 설정합니다.



기존 VLAN 인터페이스를 편집한다면, **Associated Interface(**연결된 인터페이스**)** 테이블에는 이 VLAN의 스위치 포트가 표시됩니다.

a) 내부 사용을 위해 예약된 3968~4047 범위의 ID를 제외하고 1~4070의 **VLAN ID**를 설정합니다.

인터페이스를 저장한 후에는 VLAN ID를 변경할 수 없습니다. VLAN ID는 사용된 VLAN 태그이자 구성의 인터페이스 ID입니다.

b) (선택 사항) **Disable Forwarding on Interface VLAN(Interface VLAN**에서의 포워딩 비활성화**)**의 VLAN ID를 클릭해 다른 VLAN에 대한 포워딩을 비활성화합니다.

예를 들어, 인터넷 액세스를 위해 외부에 VLAN 1개를, 내부 비즈니스용 네트워크에 또 다른 VLAN 1개를 그리고 홈 네트워크에 3번째 VLAN을 할당합니다. 홈 네트워크에서는 비즈니스 네트워크에 액세스할 필요가 없으므로 홈 VLAN에서 포워딩을 비활성화할 수 있습니다. 비즈니스 네트워크에서는 홈 네트워크에 액세스할 수 있지만 홈 네트워크에서는 비즈니스 네트워크에 액세스할 수 없습니다.

단계 **4** 인터페이스 구성을 완료하려면 다음 절차 중 하나를 참조하십시오.

- 라우팅 모드 인터페이스 구성, 817 페이지
- 일반 브리지 그룹 멤버 인터페이스 파라미터 구성, 821 페이지

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(구축)** > **Deployment(구축)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

스위치 포트를 액세스 포트로 구성

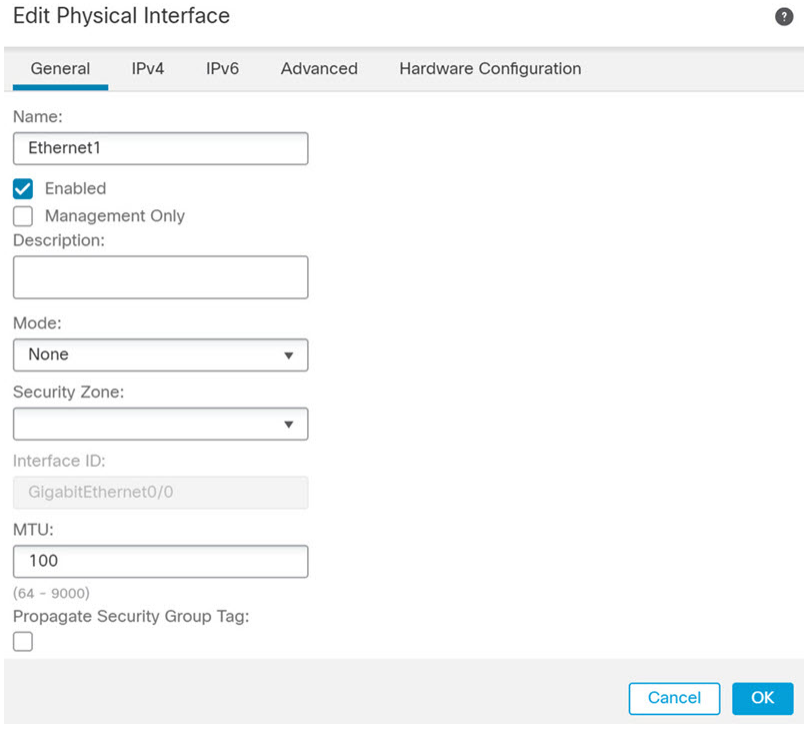
단일 VLAN에 스위치 포트를 할당하려면 해당 포트를 액세스 포트로 구성합니다. 액세스 포트에서는 태그 없는 트래픽만 허용됩니다. 기본적으로 이더넷 1/2~이더넷 1/8 스위치 포트는 VLAN 1에 할당됩니다.

참고 Firepower 1010에서는 네트워크에서의 루프 탐지를 위해 Spanning Tree Protocol을 지원하지 않습니다. 따라서 FTD와의 연결이 네트워크 루프에서 종료되지 않도록 해야 합니다.

프로시저

단계 **1** **Devices(디바이스)** > **Device Management(디바이스 관리)**를 선택하고 FTD 디바이스에 대한 수정(✎)를 클릭합니다. 기본적으로는 **Interfaces(인터페이스)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정(✎)을 클릭합니다.



단계 **3** **Enabled(활성화됨)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **4** (선택 사항) **Description(설명)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **5** **Port Mode(**포트 모드**)**를 **Access(**액세스**)**로 설정합니다.

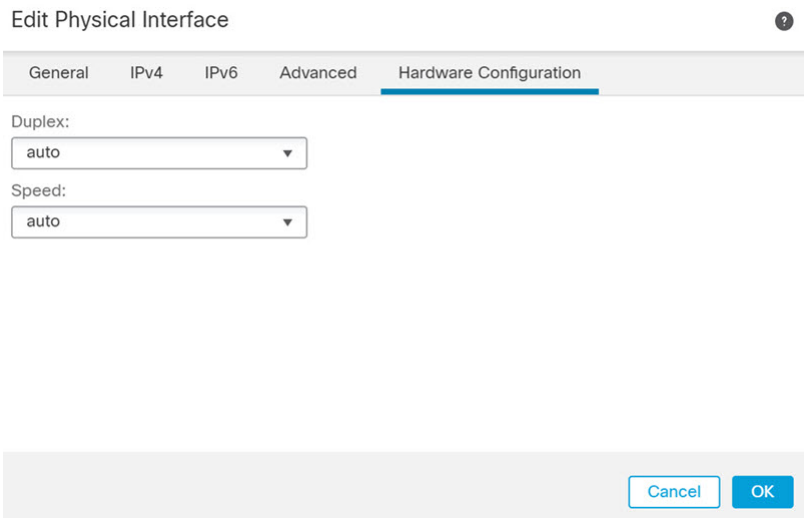
단계 **6** **VLAN ID** 필드에서 이 스위치 포트의 VLAN을 1~4070으로 설정합니다.

기본 VLAN ID는 1입니다.

단계 **7** (선택 사항) **Protected(**보호됨**)** 확인란을 선택하여 이 스위치 포트를 보호된 상태로 설정합니다. 그러면 스위치 포트가 동일한 VLAN에서 보호되는 다른 스위치 포트와 통신하는 것을 방지할 수 있습니다.

스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되어 VLAN 간 액세스를 허용할 필요가 없으며 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하려는 경우 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우, 각 스위치 포트에 **Protected(**보호됨**)**을 활성화하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.

단계 **8** (선택 사항) **Hardware Configuration(**하드웨어 설정**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.



Auto-negotiation(자동 협상**)** 확인란(기본값)을 선택해 속도와 듀플렉스를 자동으로 탐지합니다. 이 확인란 선택 취소하면 속도와 듀플렉스를 수동으로 설정할 수 있습니다.

- **Duplex(**듀플렉스**)** - **Full(**풀**)** 또는 **Half(**하프**)**를 선택합니다.
- **Speed(**속도**)** - **10mbps**, **100mbps** 또는 **1gbps**를 선택합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

스위치 포트를 트렁크 포트로 구성

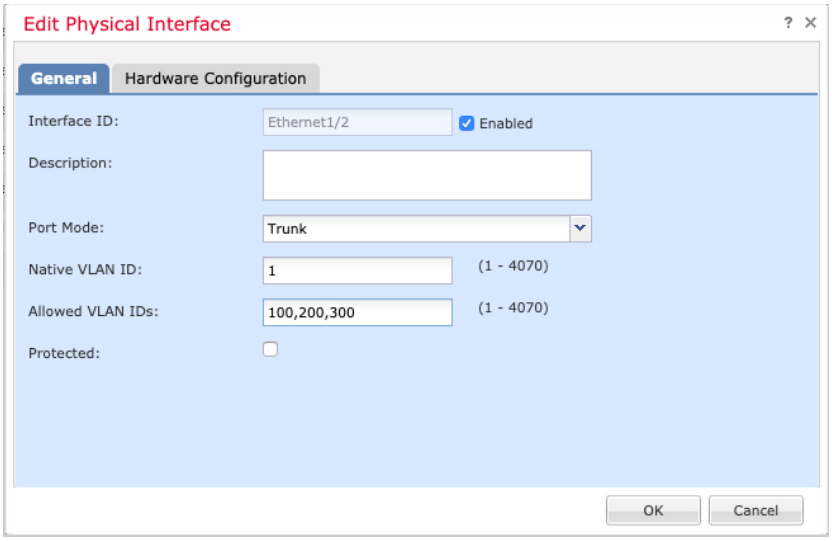
이 절차에서는 802.1Q 태깅을 사용하여 여러 VLAN을 전송할 수 있는 트렁크 포트를 생성하는 방법에 대해 설명합니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용됩니다. 허용된 VLAN의 트래픽에서는 트렁크 포트가 변경되지 않은 상태로 전달됩니다.

트렁크에서는 태그 없는 트래픽을 수신하는 경우 ASA에서 해당 트래픽을 올바른 스위치 포트로 전달하거나 다른 방화벽 인터페이스로 라우팅할 수 있도록 해당 트래픽을 네이티브 VLAN ID에 대해 태그 지정합니다. ASA에서는 트렁크 포트 외부로 네이티브 VLAN ID 트래픽을 전송하는 경우 VLAN 태그를 제거합니다. 태그 없는 트래픽이 동일한 VLAN에 대해 태그 지정될 수 있도록 다른 스위치의 트렁크 포트에서 동일한 네이티브 VLAN을 설정해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.



단계 **3** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **4** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **5** **Port Mode(**포트 모드**)**를 **Trunk(**트렁크**)**로 설정합니다.

단계 **6** **Native VLAN ID(**네이티브 **VLAN ID)** 필드에 이 스위치 포트의 네이티브 VLAN을 1~4070으로 설정합니다.

기본 네이티브 VLAN ID는 1입니다.

각 포트에는 하나의 네이티브 VLAN만 있을 수 있지만, 모든 포트의 네이티브 VLAN은 같거나 다를 수 있습니다.

단계 **7** **Allowed VLAN IDs(**허용되는 **VLAN ID)** 필드에 이 트렁크 포트의 VLAN을 1~4070으로 입력합니다.

다음 방법 중 하나를 통해 최대 20개의 ID를 식별할 수 있습니다.

- 단일 번호(n)
- 범위(n-x)
- 쉼표로 구분된 번호와 범위는 다음 예와 같습니다.

  5,7-10,13,45-100

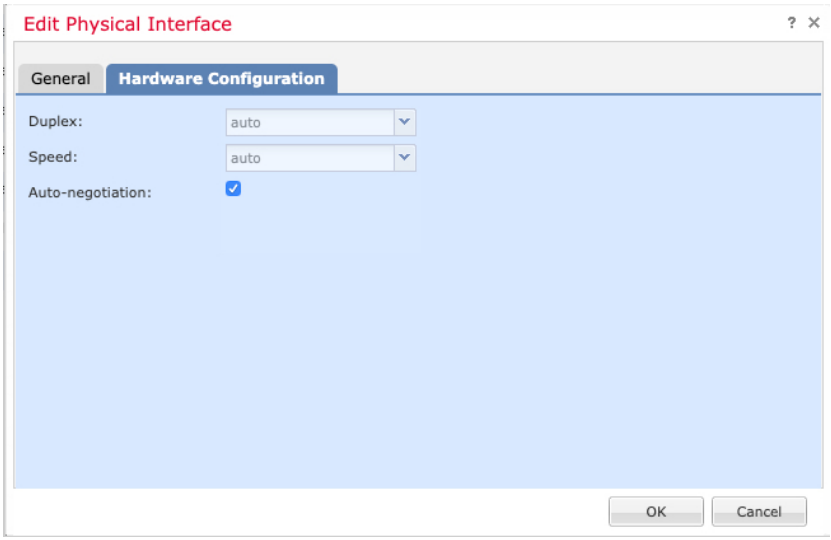
  쉼표 대신 공백을 입력해도 됩니다.

이 필드에 네이티브 VLAN을 포함하는 경우 해당 VLAN은 무시됩니다. 트렁크 포트에서는 포트 외부로 네이티브 VLAN 트래픽을 전송할 때 항상 VLAN 태깅을 제거합니다. 뿐만 아니라, 이렇게 한 후에도 네이티브 VLAN 태깅이 있는 트래픽은 수신하지 않습니다.

단계 **8** (선택 사항) **Protected(**보호됨**)** 확인란을 선택하여 이 스위치 포트를 보호된 상태로 설정합니다. 그러면 스위치 포트가 동일한 VLAN에서 보호되는 다른 스위치 포트와 통신하는 것을 방지할 수 있습니다.

스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되어 VLAN 간 액세스를 허용할 필요가 없으며 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하려는 경우 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우, 각 스위치 포트에 **Protected(**보호됨**)**을 활성화하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.

단계 **9** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.



Auto-negotiation(자동 협상**)** 확인란(기본값)을 선택해 속도와 듀플렉스를 자동으로 탐지합니다. 이 확인란 선택 취소하면 속도와 듀플렉스를 수동으로 설정할 수 있습니다.

- **Duplex(**듀플렉스**) - Full(**풀**)** 또는 **Half(**하프**)**를 선택합니다.

- **Speed(속도) - 10mbps**, **100mbps** 또는 **1gbps**를 선택합니다.

단계 **10** **OK(확인)**를 클릭합니다.

단계 **11** **Save(저장)**를 클릭합니다.

이제 **Deploy(구축)** > **Deployment(구축)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

PoE(Power over Ethernet) 구성

이더넷 1/7 및 이더넷 1/8에서는 IP 전화기 또는 무선 액세스 포인트와 같은 디바이스에 대해 PoE(Power over Ethernet)를 지원합니다. Firepower 1010에서는 IEEE 802.3af(PoE) 및 802.3at(PoE+)을 모두 지원합니다. PoE+에서는 LLDP(Link Layer Discovery Protocol)를 사용하여 전력 레벨을 협상합니다. PoE+에서는 전력 디바이스에 최대 30와트를 제공할 수 있습니다. 전원은 필요한 경우에만 제공됩니다.

스위치 포트를 종료하거나 포트를 방화벽 인터페이스로 구성한다면, 디바이스의 전원을 비활성화해야 합니다.

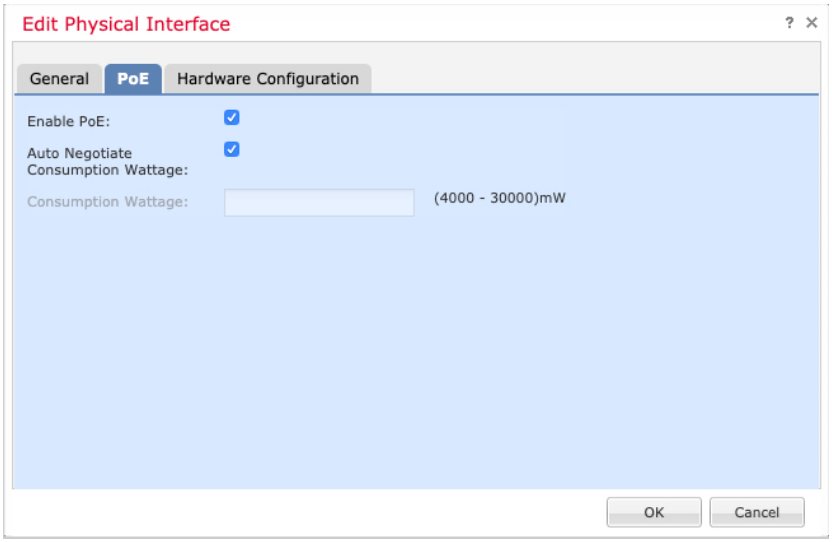
PoE는 이더넷 1/7 및 이더넷 1/8에서 기본적으로 활성화되어 있습니다. 이 절차에서는 PoE를 비활성화하는 방법과 활성화하는 방법, 파라미터(선택 사항)를 설정하는 방법을 설명합니다.

프로시저

단계 **1** **Devices(디바이스)** > **Device Management(디바이스 관리)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(인터페이스)** 페이지가 선택됩니다.

단계 **2** Ethernet1/7 또는 1/8에 대해 수정( )을(를) 클릭합니다.

단계 **3** **PoE**를 클릭합니다.



단계 **4** **Enable PoE(PoE 활성화)** 확인란을 선택합니다.

PoE는 기본적으로 활성화되어 있습니다.

단계 **5** (선택 사항) 필요한 전력량을 정확하게 알고 있다면 **Auto Negotiate Consumption Wattage(**소비 전력량 자동 협상**)** 확인란을 선택 해제하고 **Consumption Wattage(**소비 전력량**)**를 입력합니다.

기본적으로 PoE에서는 전력 디바이스의 클래스에 적절한 전력량을 사용하여 전력 디바이스에 전원을 자동으로 제공합니다. Firepower 1010에서는 LLDP를 사용하여 정확한 전력량을 추가로 협상합니다. 특정 전력량을 알고 있으며 LLDP 협상을 비활성화하려는 경우 4,000~30,000 밀리와트의 값을 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

EtherChannel 및 이중 인터페이스 구성

이 섹션에서는 EtherChannel 및 이중 인터페이스를 구성하는 방법을 알려줍니다.

참고 Firepower 4100/9300의 경우 FXOS에 EtherChannel을 구성합니다. 자세한 내용은 EtherChannel(포트 채널) 추가, 758 페이지를 참조하십시오.

참고 ASA 5500-X 모델만 이중 인터페이스를 지원합니다. Firepower 모델은 지원하지 않습니다.

EtherChannel 및 이중 인터페이스 정보

이 섹션에서는 EtherChannel 및 이중 인터페이스를 설명합니다.

이중 인터페이스 관련 정보(ASA 플랫폼 전용)

논리적 이중 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중 인터페이스를 구성하여 Firepower Threat Defense 디바이스의 안정성을 높일 수 있습니다.

최대 8개의 이중 인터페이스 쌍을 구성할 수 있습니다.

이중 인터페이스 MAC 주소

이중 인터페이스는 추가한 첫 번째 물리적 인터페이스의 MAC 주소를 사용합니다. 구성에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 변경됩니다. 또는 멤버 인터페이스 MAC 주소에 관계없이 사용되는 이중 인터페이스에 수동 MAC 주소를 할당할 수 있습니다. 액티브 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 때 같은 MAC 주소가 유지되므로 트래픽이 중단되지 않습니다.

EtherChannel 정보

802.3ad EtherChannel은 개별 이더넷 링크(채널 그룹)의 번들로 구성된 논리적 인터페이스(일명 포트 채널 인터페이스)이므로, 단일 네트워크의 대역폭을 늘리게 됩니다. 포트 채널 인터페이스는 인터페이스 관련 기능을 구성할 경우 물리적 인터페이스와 동일한 방식으로 사용됩니다.

모델에서 지원하는 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.

채널 그룹 인터페이스

채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.

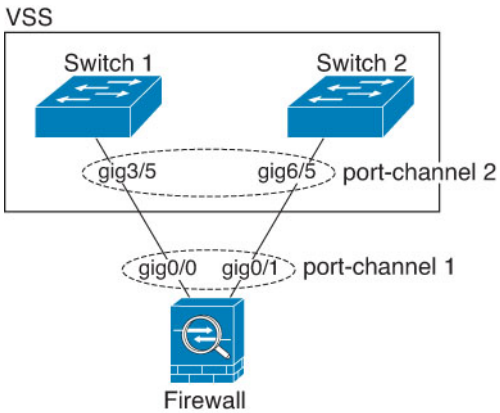
EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 소스 또는 목적지 MAC 주소, IP 주소, TCP 및 UDP 포트 번호, VLAN 번호를 기준으로 전용 해시 알고리즘을 사용하여 인터페이스를 선택합니다.

다른 디바이스에서 EtherChannel에 연결

FTD EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어 Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.

스위치가 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel)의 일부인 경우, 동일한 EtherChannel 내에서 FTD 인터페이스를 연결하여 VSS/vPC에서 스위치를 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다.

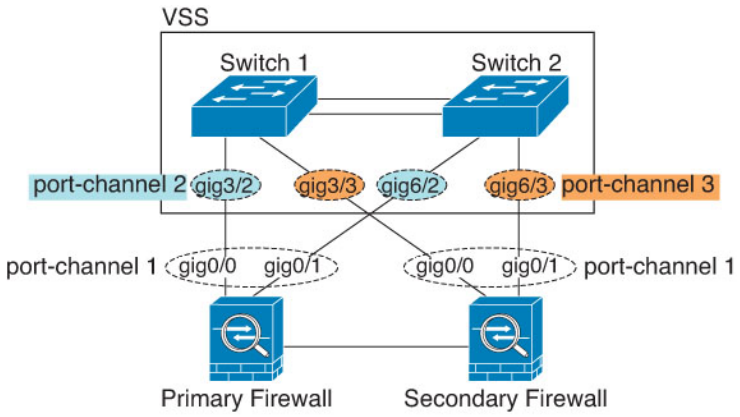
그림 ***21: VSS/vPC*에 연결**



참고 FTD의 모드가 투명 방화벽 모드이고, 두 VSS/vPC 스위치 세트 사이에 FTD의 배치가 이루어지는 경우, EtherChannel을 사용하여 FTD에 연결된 모든 스위치 포트에서 UDLD(Unidirectional Link Detection)를 비활성화해야 합니다. UDLD를 활성화하면 스위치 포트가 다른 VSS/vPC 쌍의 두 스위치에서 제공되는 UDLD 패킷을 수신할 수 있습니다. 수신 스위치는 "UDLD 인접한 라우터 불일치"라는 이유와 함께 수신 인터페이스를 중단 상태로 설정합니다.

활성/대기 장애 조치 구축 시 FTD를 사용할 경우 VSS/vPC의 스위치에 각 FTD에 별도의 EtherChannel을 생성해야 합니다. 각 FTD에서 하나의 EtherChannel이 두 스위치 모두에 연결됩니다. 모든 스위치 인터페이스를 FTD에 연결된 단일 EtherChannel으로 그룹화하는 것은 가능하지만(이 경우 별도의 FTD 시스템 ID로 인해 EtherChannel이 설정되지 않음), 스탠바이 FTD로 트래픽이 전송되는 것은 바람직하지 않으므로 단일 EtherChannel은 권장되지 않습니다.

그림 ***22:*** 액티브/스탠바이 장애 조치 및 ***VSS/vPC***



LACP(Link Aggregation Control Protocol)

LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 인터페이스를 다음과 같이 구성할 수 있습니다.

- Active(활성화) — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- 패시브 — LACP 업데이트를 받습니다. 패시브 EtherChannel은 오로지 액티브 EtherChannel과 연결을 설정할 수 있습니다. Firepower 하드웨어 모델에서는 지원되지 않습니다.
- On(켜짐) — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는

지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

부하 균형

FTD에서는 패킷의 소스 및 대상 IP 주소를 해싱하여 EtherChannel의 인터페이스에 패킷을 분산시킵니다(이 조건은 구성 가능함). 결과의 나머지 부분에 따라 흐름을 보유하는 인터페이스가 결정되는 모듈로 작업의 액티브 링크 수를 기준으로 결과 해시가 분할됩니다. *hash_value* **mod** *active_links*의 결과가 0인 모든 패킷은 EtherChannel의 첫 번째 인터페이스로 이동하고, 결과가 1인 패킷은 두 번째 인터페이스, 결과가 2인 패킷은 세 번째 인터페이스로 이동하는 방식이 이어집니다. 예를 들어 액티브 링크가 15개 있는 경우 모듈로 작업에서는 0에서 14까지의 값을 제공합니다. 액티브 링크가 6개인 경우 해당 값은 0 ~ 5가 되며, 이런 식으로 계속 적용할 수 있습니다.

액티브 인터페이스가 중단되고 스탠바이 인터페이스로 대체되지 않을 경우, 나머지 링크 간의 트래픽이 다시 밸런싱됩니다. 오류는 Layer 2의 스패닝 트리와 Layer 3의 라우팅 테이블에서 모두 마스킹되므로, 전환 작업은 다른 네트워크 디바이스에 투명하게 이루어집니다.

EtherChannel MAC 주소

채널 그룹의 일부인 모든 인터페이스에서는 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다.

포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

EtherChannel 및 이중 인터페이스에 대한 지침

브리지 그룹

라우팅 모드에서 FMC 정의 EtherChannel은 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.

모델 지원

- 이중 인터페이스는 ASA 5500-X 플랫폼에서만 지원됩니다. Firepower 1000, Firepower 2100, Firepower 4100/9300 및 FTDv에서는 사용할 수 없습니다.
- EtherChannel에서는 Firepower 1010 스위치 포트 또는 VLAN 인터페이스를 사용할 수 없습니다.

이중 인터페이스 일반 지침

- 최대 8개의 이중 인터페이스 쌍을 구성할 수 있습니다.
- 모든 FTD 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 이중 인터페이스를 참조합니다.

- 이중 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중 인터페이스 일부로 사용할 수 없습니다. 이중 인터페이스 및 EtherChannel 인터페이스에서 동일한 물리적 인터페이스를 사용할 수 없습니다. 그러나 이러한 인터페이스에서 동일한 물리적 인터페이스를 사용하지 않을 경우 FTD에서 두 가지 유형을 구성할 수 있습니다.
- 액티브 인터페이스를 종료할 경우 스탠바이 인터페이스가 액티브 상태로 됩니다.
- 이중 인터페이스는 진단 슬롯/포트 인스턴스를 멤버로 지원하지 않습니다. 그러나, 비진단 인터페이스로 구성된 이중 인터페이스를 관리 전용으로 설정할 수 있습니다.

EtherChannel 일반 지침

- 모델에서 사용할 수 있는 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.
-
- 채널 그룹의 모든 인터페이스는 미디어 유형 및 용량이 동일해야 하며 속도 및 듀플렉스를 동일하게 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다.
- FTD EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다.
- FTD에서는 VLAN 태그 처리된 LACPDU를 지원하지 않습니다. Cisco IOS **vlan dot1Q tag native** 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태깅을 활성화할 경우, FTD에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태깅을 비활성화해야 합니다.
- ASA 5500-X 모델, Firepower 1000 및 Firepower 2100은 LACP 속도, fast(빠르게)를 지원하지 않습니다. LACP는 항상 정상 속도를 사용합니다. 이 설정은 구성 가능하지 않습니다. FXOS에서 EtherChannel을 구성하는 Firepower 4100/9300의 LACP 속도는 기본적으로 fast(빠르게)로 설정되어 있습니다. 이러한 플랫폼에서는 속도를 구성할 수 있습니다.
- 15.1(1)S2 이전 Cisco IOS 소프트웨어 버전에서는 FTD가 EtherChannel과 스위치 스택 간의 연결을 지원하지 않았습니다. 기본 스위치 설정으로 FTD EtherChannel이 교차 스택에 연결되어 있는 상태에서 기본 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.
- 모든 FTD 컨피그레이션에서는 멤버 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.
- 이중 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중 인터페이스 일부로 사용할 수 없습니다. 이중 인터페이스 및 EtherChannel 인터페이스에서 동일한 물리적 인터페이스를 사용할 수 없습니다. 그러나 이러한 인터페이스에서 동일한 물리적 인터페이스를 사용하지 않을 경우 FTD에서 두 가지 유형을 구성할 수 있습니다.

이중화 인터페이스 구성(ASA 플랫폼만 해당)

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

논리적 이중 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중 인터페이스를 구성하여 FTD의 안정성을 높일 수 있습니다. 기본적으로 이중 인터페이스는 활성화되어 있습니다.

- 최대 8개의 이중 인터페이스 쌍을 구성할 수 있습니다.
- 두 멤버 인터페이스 모두 물리적 유형이 같아야 합니다. 이를테면 모두 GigabitEthernet이어야 합니다.

참고 이중 인터페이스는 Firepower 플랫폼에서 지원되지 않습니다. ASA 5500-X 모델 만 이중 인터페이스를 지원합니다.

시작하기 전에

- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 이중 인터페이스에 추가할 수 없습니다. 먼저 이름을 제거해야 합니다.

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 물리적 인터페이스 활성화 및 이더넷 설정, 787 페이지에 따라 멤버 인터페이스를 활성화합니다.

단계 **3** 인터페이스 추가 > 이중 인터페이스를 클릭합니다.

단계 **4** 일반 탭에서 다음 파라미터를 설정합니다.

a) 이중 **ID** - 1에서 8사이의 정수를 설정합니다.

b) 기본 인터페이스 - 드롭다운 목록에서 인터페이스를 선택합니다. 인터페이스를 추가하면 해당 인터페이스의 모든 컨피그레이션(예: IP 주소)이 제거됩니다.

c) 보조 인터페이스 - 두 번째 인터페이스는 첫 번째 인터페이스와 물리적 유형이 동일해야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 **7** (선택 사항) VLAN 하위 인터페이스 추가 하위 인터페이스 추가, 813 페이지의 내용을 참조하십시오.

단계 **8** 라우팅 및 투명 모드 인터페이스 파라미터 구성 라우팅 모드 인터페이스 구성, 817 페이지 또는 브리지 그룹 인터페이스 구성, 821 페이지를 참조하십시오.

EtherChannel 구성

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고, EtherChannel에 인터페이스를 할당하며, EtherChannel을 맞춤화하는 방법에 대해 알아봅니다.

지침

- 모델용 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 16개의 액티브 인터페이스를 포함할 수 있습니다. 단, 8개의 액티브 인터페이스를 지원하는 Firepower 1000 또는 2100은 제외됩니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다.
- 채널 그룹의 모든 인터페이스는 유형, 속도, 양방향이 동일해야 합니다. 반이중은 지원되지 않습니다.

참고 Firepower 4100/9300의 경우 FXOS에 EtherChannel을 구성합니다. 자세한 내용은 EtherChannel(포트 채널) 추가, 758 페이지를 참조하십시오.

시작하기 전에

- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 채널 그룹에 추가할 수 없습니다. 먼저 이름을 제거해야 합니다.

참고 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 물리적 인터페이스 활성화 및 이더넷 설정, 787 페이지에 따라 멤버 인터페이스를 활성화합니다.

단계 3 인터페이스 추가 > **EtherChannel** 인터페이스를 클릭합니다.

단계 4 **General(**일반**)** 탭에서 **Ether Channel ID**를 1에서 48까지의 숫자로(Firepower 1010에서는 1에서 8까지의 숫자로) 설정합니다.

단계 5 사용 가능한 인터페이스 영역에서 인터페이스를 클릭하고 추가를 클릭하여 선택된 인터페이스 영역으로 이동합니다. 멤버로 추가하려면 모든 인터페이스에 대해 반복합니다.

모든 인터페이스의 유형과 속도가 같은지 확인합니다. 첫 번째로 추가된 인터페이스가 EtherChannel의 유형과 속도를 결정합니다. 추가되었으나 일치하지 않는 인터페이스는 보류 상태가 됩니다. FMC은 일치하지 않는 인터페이스 추가를 막을 수 없습니다.

단계 6 (선택 사항) EtherChannel을 사용자 정의하려면 고급 탭을 클릭합니다. 정보 하위 탭에서 다음 파라미터를 설정합니다.

- (ASA 5500-X 모델에만 해당) 로드 밸런싱 - 그룹 채널 인터페이스 전반에서 패킷 로드 밸런싱에 사용되는 기준을 선택합니다. 기본적으로 FTD 디바이스는 패킷의 소스 및 대상 IP 주소에 따라 인터페이스에서 패킷 로드 밸런싱을 수행합니다. 패킷이 분류되는 속성을 변경하려면 다른 기준 집합을 선택합니다. 예를 들어 동일한 소스와 목적지 IP 주소에 트래픽이 심하게 편중된 경우 EtherChannel의 인터페이스에 트래픽 할당이 불균형해질 수 있습니다. 다른 알고리즘으로 변경할 경우 트래픽이 보다 고르게 분산될 수 있습니다. 로드 밸런싱에 대한 자세한 내용은 부하 균형, 807 페이지을 참조하십시오.
- **LACP** 모드 - 액티브, 패시브, 켜기를 선택합니다. 액티브 모드(기본값)를 사용하는 것이 좋습니다.
- (ASA 5500-X 모델에만 해당) 액티브 물리적 인터페이스**:** 범위 - 왼쪽의 드롭다운 목록에서 EtherChannel 시 액티브 상태여야 할 액티브 인터페이스의 최소 개수를 1~16 사이에서 선택합니다. 기본값은 1입니다. 오른쪽의 드롭다운 목록에서 EtherChannel에 허용되는 액티브 인터페이스의 최대 개수를 1~16 사이에서 선택합니다. 기본값은 16입니다. 스위치에서 16개의 액티브 인터페이스를 지원하지 않을 경우, 이 명령을 8 이하로 설정합니다.
- 액티브 **Mac** 주소 - 필요한 경우 수동 MAC 주소를 설정합니다. mac_address는 H.H.H 형식이며, 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력됩니다.

단계 **7** (선택 사항) 하드웨어 구성 탭을 클릭하고 모든 멤버 인터페이스에 이런 설정을 오버라이드하기 위한 듀플렉스 및 속도를 설정합니다. 이러한 매개변수는 채널 그룹의 모든 인터페이스와 일치해야 하므로, 이 방법을 사용하면 이러한 매개변수를 빠르게 설정할 수 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 **10** (선택 사항) VLAN 하위 인터페이스 추가 하위 인터페이스 추가, 813 페이지의 내용을 참조하십시오.

단계 **11** 라우팅 및 투명 모드 인터페이스 파라미터 구성 라우팅 모드 인터페이스 구성, 817 페이지 또는 브리지 그룹 인터페이스 구성, 821 페이지를 참조하십시오.

VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성

VLAN 하위 인터페이스를 사용하면 물리적, 이중 또는 EtherChannel 인터페이스를 다른 VLAN ID가 태그 처리된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 주어진 물리적 인터페이스에서 트래픽을 분리할 수 있으므로 추가로 물리적 인터페이스 또는 디바이스를 추가하지 않고도 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

VLAN 하위 인터페이스에 대한 가이드라인 및 제한 사항

모델 지원

- Firepower 1010 - VLAN 하위 인터페이스는 스위치 포트 또는 VLAN 인터페이스에서 지원되지 않습니다.

고가용성

페일오버 또는 상태 링크용 하위 인터페이스를 사용할 수 없습니다. 컨테이너 인스턴스용으로 Firepower 4100/9300 섀시에 정의된 하위 인터페이스는 제외됩니다.

추가 지침

- 물리적 인터페이스의 태그 지정되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 지정되지 않은 패킷을 전달하기 때문입니다. 이러한 속성은 이중 인터페이스 쌍의 물리적 인터페이스 및 EtherChannel 링크에서도 마찬가지입니다. 하위 인터페이스에서 트래픽을 전달하려면 물리적, 이중화 또는 EtherChannel 인터페이스를 활성화해야 하므로, 인터페이스 이름을 설정하지 않음으로써 물리적, 이중화 또는 EtherChannel 인터페이스가 트래픽을 전달하지 않도록 합니다. 물리적, 이중화 또는 EtherChannel 인터페이스에서 태그되지 않은 패킷을 전달하려면 평소와 같이 이름을 구성합니다.

- 진단 인터페이스에서는 하위 인터페이스를 설정할 수 없습니다.
- FTD에서는 DTP(Dynamic Trunking Protocol)를 지원하지 않으므로 조건 없이 트렁킹을 수행할 연결된 스위치 포트를 구성해야 합니다.
- FTD에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 FTD의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

디바이스 모델별 VLAN 하위 인터페이스의 최대 수

디바이스 모델은 구성할 수 있는 VLAN 하위 인터페이스의 최대 수를 제한합니다. 하위 인터페이스는 데이터 인터페이스에서만 구성할 수 있으며 관리 인터페이스에서는 구성할 수 없습니다.

다음 표에서는 각 디바이스 모델의 제한 사항에 대해 설명합니다.

모델	VLAN 하위 인터페이스의 최대 수
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Firepower 2100	1024
ASA 5508-X	50
ASA 5516-X	100

하위 인터페이스 추가

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

물리적, 이중 또는 포트 채널 인터페이스에 하나 이상의 하위 인터페이스를 추가합니다.

Firepower 4100/9300의 경우 컨테이너 인스턴스와 함께 사용하기 위해 FXOS에서 하위 인터페이스를 구성할 수 있습니다. 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가, 760 페이지를 참조하십시오. 이러한 하위 인터페이스는 FMC 인터페이스 목록에 표시됩니다. FMC에 하위 인터페이스를 추가할 수도 있습니다. 그러나 FXOS에서 정의된 하위 인터페이스가 아직 없는 상위 인터페이스에서만 가능합니다.

참고 상위 물리적 인터페이스는 태그가 지정되지 않은 패킷을 전달합니다. 태그가 지정되지 않은 패킷을 전달하고 싶지 않은 경우 보안 정책에 상위 인터페이스를 포함하지 않아야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 물리적 인터페이스 활성화 및 이더넷 설정, 787 페이지에 따라 상위 인터페이스를 활성화합니다.

단계 **3** 인터페이스 추가 > 하위 인터페이스를 클릭합니다.

단계 **4** 일반에서 다음 파라미터를 설정합니다.

a) 인터페이스 - 하위 인터페이스에 추가할 물리적, 이중화 또는 포트 채널 인터페이스를 선택합니다.

b) 하위 인터페이스 **ID** - 하위 인터페이스 ID를 1~4294967295 사이의 정수로 입력합니다. 허용되는 하위 인터페이스의 개수는 플랫폼에 따라 다릅니다. 다음을 설정한 후에는 ID를 변경할 수 없습니다.

c) **VLAN ID** - 이 하위 인터페이스에서 패킷에 태그를 지정하는 데 사용할 1~4094 사이의 VLAN ID를 입력합니다.

이 VLAN ID에는 상위 인터페이스에 대해 고유한 에서는 이 VLAN을 재사용할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 **7** 라우팅 및 투명 모드 인터페이스 파라미터 구성 라우팅 모드 인터페이스 구성, 817 페이지 또는 브리지 그룹 인터페이스 구성, 821 페이지를 참조하십시오.

라우팅 및 투명 모드 인터페이스 구성

이 섹션은 라우팅 또는 투명 방화벽 모드에서 모든 모델의 일반 인터페이스 구성을 완료하는 작업이 포함되어 있습니다.

라우팅 및 투명 모드 인터페이스 정보

방화벽 모드 인터페이스는 IP 및 TCP 레이어, IP 조각 모음, TCP 표준화에서 플로우 유지, 플로우 상태 추적 등의 방화벽 기능에 트래픽을 적용합니다. 필요한 경우 보안 정책에 따라 해당 트래픽에 대한 IPS 기능을 구성할 수도 있습니다.

구성할 수 있는 방화벽 인터페이스의 유형은 디바이스의 방화벽 모드 집합이 라우팅인지 투명 모드인지에 따라 달라집니다. 자세한 내용은 Firepower Threat Defense에 대한 투명 또는 라우팅 방화벽 모드, 711 페이지를 참조하십시오.

- 라우팅 모드 인터페이스(라우팅된 방화벽 모드 전용) - 서로 라우팅하려는 각 인터페이스가 다른 서브넷에 있습니다.
- 브리지 그룹 인터페이스(라우팅 및 투명 방화벽 모드 - 네트워크의 여러 인터페이스를 그룹화할 수 있고 Firepower Threat Defense 디바이스는 브리지 기술을 사용해 인터페이스 간 트래픽을 전달합니다. 각 브리지 그룹은 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)를 포함합니다. 라우팅 모드에서 Firepower Threat Defense 디바이스는 BVI 및 일반 라우팅 인터페이스를 라우팅합니다. 투명 모드에서 의 각 브리지 그룹은 구분되며 서로 통신할 수 없습니다.

이중 IP 스택(IPv4 및 IPv6)

Firepower Threat Defense 디바이스은 하나의 인터페이스에서 IPv6 및 IPv4 주소를 모두 지원합니다. IPv4 및 IPv6 모두에 대한 기본 경로를 구성해야 합니다.

라우팅 모드 및 투명 모드 인터페이스에 대한 지침 및 제한 사항

고가용성

- 이 장의 절차를 사용하여 장애 조치 링크를 구성해서는 안 됩니다. 자세한 내용은 고가용성 장을 참조하십시오.
- 고가용성를 사용하는 경우 데이터 인터페이스에 대해 IP 주소 및 스탠바이 주소를 수동으로 설정해야 하며, DHCP 및 PPPoE는 지원되지 않습니다. 모니터링되는 인터페이스 영역의 디바이스 > 디바이스 관리 > 고가용성 탭에서 스탠바이 IP 주소를 설정합니다. 자세한 내용은 고가용성 장을 참조하십시오.

IPv6

- 모든 인터페이스에서 IPv6가 지원됩니다.
- 투명 모드에서 IPv6 주소만 수동으로 구성할 수 있습니다.
- Firepower Threat Defense 디바이스는 IPv6 애니캐스트 주소를 지원하지 않습니다.

모델 지침

- 브리지 ixgbevf 인터페이스를 사용하는 VMware의 Firepower Threat Defense Virtual의 경우 브리지 그룹이 지원되지 않습니다.
- Firepower 2100 Series의 경우, 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.

투명 모드 및 브리지 그룹 지침

- 브리지 그룹당 64개의 인터페이스가 있는 최대 250개의 브리지 그룹을 생성할 수 있습니다.

- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.
- Firepower Threat Defense 디바이스는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.
- IPv4에서는 관리 트래픽과 Firepower Threat Defense 디바이스를 거칠 트래픽 모두 브리지 그룹마다 BVI용 IP 주소가 필요합니다. IPv6 주소는 지원되지만 BVI에는 필요하지 않습니다.
- IPv6 주소만 수동으로 구성할 수 있습니다.
- BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다.
- 관리 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- Firepower 1010의 경우, 동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수 없습니다.
- Firepower 4100/9300의 경우, 데이터 공유 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- 투명 모드에서는 1개 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.
- 투명 모드에서는 BVI IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 Firepower Threat Defense 디바이스의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.
- 투명 모드에서는 관리 트래픽의 반환 경로를 제공하는 데 필요한 기본 경로가 하나의 브리지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브리지 그룹의 인터페이스 및 브리지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브리지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 일반 고정 경로를 지정해야 합니다.
- 투명 모드에서 PPPoE는 진단 인터페이스에 대해 지원되지 않습니다.
- 라우팅 모드에서 브리지 그룹 및 기타 라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다.
- 라우팅 모드에서 FTD 정의된 EtherChannel 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 브리지 그룹 멤버를 사용할 때 FTD를 통과하는 것이 허용되지 않습니다. BFD를 실행하는 FTD의 양쪽 측면에 두 개의 네이버가 있는 경우, FTD는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.

추가 지침 및 요건

- FTD는 패킷에서 하나의 802.1Q 헤더만 지원하며 방화벽 인터페이스에 대해 여러 헤더(Q-in-Q 지원이라고 하는)를 지원하지 않습니다.참고: 인라인 집합 및 패시브 인터페이스의 경우 FTD는

하나의 802.1Q 헤더만 지원하는 Firepower 4100/9300을 제외하고 패킷에서 최대 2개의 802.1Q 헤더를 지원합니다.

라우팅 모드 인터페이스 구성

이 절차에서는 이름, 보안 영역, IPv4 주소를 설정하는 방법에 대해 설명합니다.

시작하기 전에

- **Firepower 4100/9300**
  1. 실제 인터페이스 구성, 757 페이지
  2. (선택 사항) 특수 인터페이스를 구성합니다.
     - EtherChannel(포트 채널) 추가, 758 페이지
     - 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가, 760 페이지 FXOS에서
     - 하위 인터페이스 추가, 813 페이지 in FMC
- (선택 사항) 기타 모든 모델:
  - 이중화 인터페이스 구성(ASA 플랫폼만 해당), 809 페이지
  - EtherChannel 구성, 810 페이지
  - 하위 인터페이스 추가, 813 페이지
  - Firepower 1010: VLAN 인터페이스 구성, 797 페이지

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 수정할 인터페이스의 수정( )을 클릭합니다.

단계 3 **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

단계 4 **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 5 (선택 사항) 관리 트래픽으로 트래픽을 제한하려면 이 인터페이스를 관리 전용으로 설정합니다. through-the-box 트래픽은 허용되지 않습니다.

단계 6 (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 7 **Mode(**모드**)** 드롭다운 목록에서 **None(**없음**)**을 선택합니다.

일반 방화벽 인터페이스는 None(없음) 모드로 설정됩니다. 다른 모드는 IPS 전용 인터페이스 유형입니다.

단계 **8** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

라우팅된 인터페이스는 라우팅 유형 인터페이스이며 라우팅 유형 영역에만 속할 수 있습니다.

단계 **9** **MTU**에 대한 자세한 내용은 MTU 구성, 837 페이지를 참조하십시오.

단계 **10** **IPv4** 탭을 클릭합니다. IP 주소를 설정하려면 **IP** 유형 드롭다운 목록에서 다음 중 하나를 사용합니다.

고가용성 및 클러스터링 인터페이스는 고정 IP 주소 설정만 지원합니다. DHCP 및 PPPoE는 지원되지 않습니다.

- 고정 **IP** 사용 - IP 주소 및 서브넷 마스크를 입력합니다. 고가용성의 경우 고정 IP 주소만 사용할 수 있습니다. 모니터링되는 인터페이스 영역의 디바이스 > 디바이스 관리 > 고가용성 탭에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **DHCP** 사용 - 다음 선택 파라미터를 구성합니다.
  - **DHCP**에서 기본 경로 가져오기 - DHCP 서버에서 기본 경로를 가져옵니다.
  - **DHCP** 경로 메트릭 - 파악된 경로에 대해 1과 255 사이의 관리 거리를 할당합니다. 파악된 경로의 기본 관리 거리는 1입니다.
- **PPPoE** 사용 - 인터페이스가 DSL, 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하며 ISP가 PPPoE를 사용해 IP 주소를 제공하는 경우 다음 파라미터를 구성합니다.
  - **VPDN** 그룹 이름 - 이 연결을 대표하는 그룹 이름을 원하는 대로 지정합니다.
  - **PPPoE** 사용자 이름 - ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE** 암호/암호 확인 - ISP에서 제공한 비밀번호를 지정하고 확인합니다.
  - **PPP Authentication(PPP** 인증**)** - **PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

    PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
  - **PPPoE** 경로 메트릭 - 파악된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - 경로 설정 사용 - PPPoE IP 주소를 수동으로 구성하려면 이 체크 박스를 선택하고 **IP** 주소를 입력합니다.

    Enable Route Settings(경로 설정 활성화**)** 확인란을 선택하고 **IP Address(IP** 주소**)**를 입력하지 않으면, 이 예시에서처럼 **ip address pppoe setroute** 명령이 적용됩니다.

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- 플래시에 사용자 이름 및 비밀번호 저장 - 플래시 메모리에 사용자 이름 및 비밀번호를 저장합니다.

  FTD에서는 NVRAM의 특수 위치에 사용자 이름 및 비밀번호를 저장합니다.

단계 **11** (선택 사항) **IPv6** 탭에서 IPv6 주소 지정을 구성하려면 IPv6 주소 지정 구성, 826 페이지를 참조하십시오.

단계 **12** (선택 사항) 고급 탭에서 MAC 주소를 수동으로 구성하려면 MAC 주소 구성, 838 페이지를 참조하십시오.

단계 **13** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)** 탭을 클릭하여 듀플렉스 및 속도를 설정합니다.

- **Duplex(**듀플렉스**) - Full(**풀 듀플렉스**), Half(**하프 듀플렉스**)** 또는 **Auto(**자동**)**를 선택합니다. 인터페이스가 지원하는 경우 자동이 기본값입니다. 예를 들어 Firepower 2100 시리즈의 SFP 인터페이스에 대에서는 자동을 선택할 수 없습니다.
- **Speed(**속도**) - 10**, **100**, **1000** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다. 인터페이스 유형에 따라 선택할 수 있는 옵션이 제한됩니다. 예를 들어 Firepower 2100 시리즈 디바이스의 GigabitEthernet 포트에 10, 100, 1000(1Gbps)를, SFP 포트에 1000 또는 10000(10Gpbs)를 선택할 수 있습니다. Firepower 2100 시리즈 디바이스의 SFP 인터페이스는 자동을 지원하지 않습니다.

단계 **14** (선택 사항) **FMC** 액세스 페이지의 데이터 인터페이스에서 FMC 관리 액세스를 활성화합니다.

FTD를 처음 설정할 때 데이터 인터페이스에서 FMC 액세스를 활성화할 수 있습니다. FMC에 FTD를 추가한 후 FMC 액세스를 활성화하거나 비활성화하려면 다음을 참조하십시오.

- FMC 액세스를 활성화합니다. 관리에서 데이터로 FMC 액세스 인터페이스 변경, 318 페이지

  참고 관리에서 데이터 인터페이스로의 관리 인터페이스 마이그레이션을 먼저 시작하지 않으면 FMC 액세스를 활성화할 수 없습니다. 마이그레이션을 시작한 후 **FMC** 액세스 페이지에서 FMC 액세스를 활성화하고 구성을 성공적으로 저장할 수 있습니다.

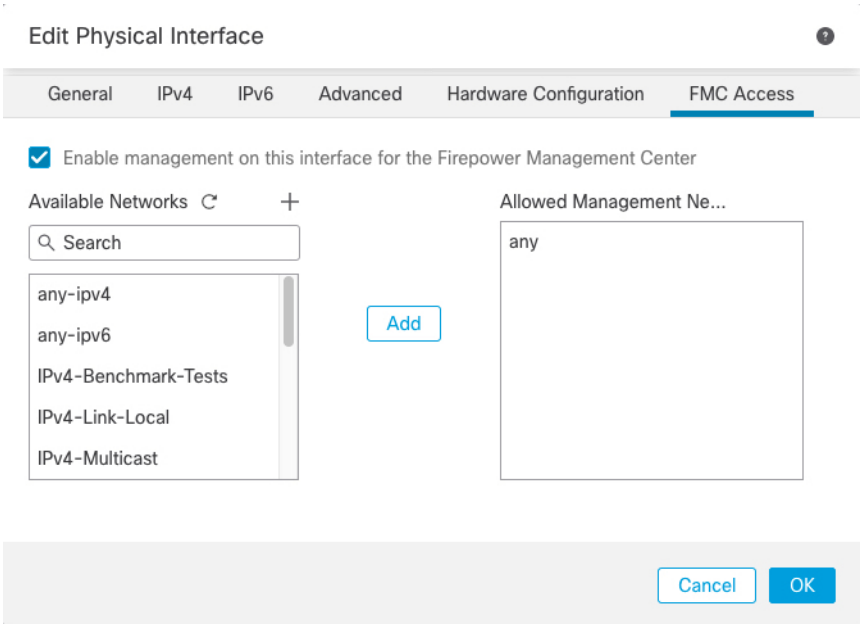
- FMC 액세스를 비활성화합니다. 데이터에서 관리로 FMC 액세스 인터페이스 변경, 321 페이지

FMC 액세스 인터페이스를 한 데이터 인터페이스에서 다른 데이터 인터페이스로 변경하려면 원래 데이터 인터페이스에서 FMC 액세스를 비활성화해야 하지만 인터페이스 자체는 아직 비활성화하지 않아야 합니다. 원본 데이터 인터페이스를 사용하여 구축을 수행해야 합니다. 새 FMC 액세스 인터페이스에서 동일한 IP 주소를 사용하려는 경우 원래 인터페이스에서 IP 구성을 삭제하거나 변경할 수 있습니다. 이 변경 사항은 구축에 영향을 미치지 않습니다. 새 인터페이스에 다른 IP 주소를 사용하는 경우 FMC에 표시된 디바이스 IP 주소도 변경합니다. FMC에서 호스트 이름 또는 IP 주소 업데이트 ,

317 페이지의 내용을 참조하십시오. 정적 경로, DDNS 및 DNS 설정과 같은 새 인터페이스를 사용하려면 관련 구성도 업데이트해야 합니다.

데이터 인터페이스에서의 FMC 액세스에는 다음과 같은 제한이 있습니다.

- 하나의 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 FMC를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.



- Firepower Management Center가 전용 관리 인터페이스 대신 이 데이터 인터페이스를 관리용으로 사용하려면 **Enable interface on this interface for this interface(**이 인터페이스에서 관리 활성화**)**를 선택합니다.
- (선택 사항) **Allowed Management Networks(**허용되는 관리 네트워크**)** 상자에 FMC 액세스를 허용할 네트워크를 추가합니다. 기본적으로 모든 네트워크가 허용됩니다.

단계 **15** **OK(**확인**)**를 클릭합니다.

단계 **16** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

브리지 그룹 인터페이스 구성

브리지 그룹은 Firepower Threat Defense 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 브리지 그룹은 투명 방화벽 모드와 라우팅 방화벽 모드에서 지원됩니다. 브릿지 그룹에 대한 자세한 내용은 브리지 그룹 정보, 713 페이지를 참조하십시오.

브리지 그룹 및 연결된 인터페이스를 구성하려면, 다음 단계를 수행하십시오.

일반 브리지 그룹 멤버 인터페이스 파라미터 구성

이 절차에서는 각 브리지 그룹 멤버 인터페이스의 이름 및 보안 영역을 설정하는 방법을 설명합니다. 동일한 브리지 그룹은 다양한 유형의 인터페이스를 포함할 수 있습니다. 예를 들어, 물리적 인터페이스, VLAN 하위 인터페이스, Firepower 1010 VLAN 인터페이스, EtherChannel 및 이중 인터페이스가 있습니다. 진단 인터페이스는 지원되지 않습니다. 라우팅된 모드에서 Etherchannel은 지원되지 않습니다. Firepower 4100/9300의 경우 데이터 공유 유형 인터페이스는 지원되지 않습니다.

시작하기 전에

- **Firepower 4100/9300**
  1. 실제 인터페이스 구성, 757 페이지
  2. (선택 사항) 특수 인터페이스를 구성합니다.
     - EtherChannel(포트 채널) 추가, 758 페이지
     - 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가, 760 페이지 FXOS에서
     - 하위 인터페이스 추가, 813 페이지 in FMC
- (선택 사항) 기타 모든 모델**:**
  - 이중화 인터페이스 구성(ASA 플랫폼만 해당), 809 페이지
  - EtherChannel 구성, 810 페이지
  - 하위 인터페이스 추가, 813 페이지
  - Firepower 1010: VLAN 인터페이스 구성, 797 페이지

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 수정할 인터페이스의 수정( )을 클릭합니다.

단계 3 **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

단계 4 **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 5 (선택 사항) 관리 트래픽으로 트래픽을 제한하려면 이 인터페이스를 관리 전용으로 설정합니다. through-the-box 트래픽은 허용되지 않습니다.

단계 6 (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 7 **Mode(**모드**)** 드롭다운 목록에서 **None(**없음**)**을 선택합니다.

일반 방화벽 인터페이스는 None(없음) 모드로 설정됩니다. 다른 모드는 IPS 전용 인터페이스 유형입니다. 이 인터페이스를 브리지 그룹으로 할당하면 모드는 스위치라고 표시됩니다.

단계 8 **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

브리지 그룹 멤버 인터페이스는 스위치 유형 인터페이스이며 스위치 유형 영역에만 속할 수 있습니다. 이 인터페이스에는 IP 주소 설정을 구성하지 마십시오. 브리지 가상 인터페이스(BVI)에만 IP 주소를 구성할 수 있습니다. BVI는 영역에 속하지 않으므로 BVI에 액세스 제어 정책을 적용할 수 없습니다.

단계 9 **MTU**에 대한 자세한 내용은 MTU 구성, 837 페이지를 참조하십시오.

단계 10 (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)** 탭을 클릭하여 듀플렉스 및 속도를 설정합니다.

- **Duplex(**듀플렉스**)** - **Full(**풀 듀플렉스**)**, **Half(**하프 듀플렉스**)** 또는 **Auto(**자동**)**를 선택합니다. 인터페이스가 지원하는 경우 자동이 기본값입니다. 예를 들어 Firepower 2100 시리즈의 SFP 인터페이스에 대에서는 자동을 선택할 수 없습니다.
- **Speed(**속도**)** - **10**, **100**, **1000** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다. 인터페이스 유형에 따라 선택할 수 있는 옵션이 제한됩니다. 예를 들어 Firepower 2100 시리즈 디바이스의 GigabitEthernet 포트에 10, 100, 1000(1Gbps)를, SFP 포트에 1000 또는 10000(10Gpbs)를 선택할 수 있습니다. Firepower 2100 시리즈 디바이스의 SFP 인터페이스는 자동을 지원하지 않습니다.

단계 11 (선택 사항) **IPv6** 탭에서 IPv6 주소 지정을 구성하려면 IPv6 주소 지정 구성, 826 페이지를 참조하십시오.

단계 12 (선택 사항) 고급 탭에서 MAC 주소를 수동으로 구성하려면 MAC 주소 구성, 838 페이지를 참조하십시오.

단계 13 **OK(**확인**)**를 클릭합니다.

단계 14 **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

BVI(Bridge Virtual Interface) 구성

각 브리지 그룹에는 IP 주소를 구성하는 BVI가 필요합니다. FTD에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. IPv4 트래픽의 경우 트래픽을 전달하려면 BVI IP 주소가 필요합니다. IPv6 트래픽에서는 적어도 트래픽을 전달하기 위해서는 링크-로컬 주소를 구성해야 합니다. 그러나 원격 관리, 기타 관리 작업을 포함한 전체 기능에 하나의 전역 관리 주소를 사용하는 것이 좋습니다.

라우팅 모드에서 BVI의 이름을 제공하는 경우 BVI는 라우팅에 참여합니다. 이름이 없는 경우 브리지 그룹은 투명 방화벽 모드에서와 같이 격리된 상태로 남아 있습니다.

참고 별도의 진단 인터페이스의 경우 구성 불가한 브리지 그룹(ID 301)이 자동으로 설정에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.

시작하기 전에

BVI를 보안 영역에 추가할 수 없습니다. 따라서 BVI에 액세스 제어 정책을 적용할 수 없습니다. 영역에 따라 브리지 그룹 멤버 인터페이스에 정책을 적용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 인터페이스 추가 > 브리지 그룹 인터페이스를 선택합니다.

단계 **3** (라우팅 모드 이름 필드에서 최대 48자의 이름을 입력합니다.

브리지 그룹 외부 멤버에게 트래픽을 라우팅하려는 경우 BVI의 이름을 지정해야 합니다. 예를 들어, 외부 인터페이스 또는 기타 브리지 그룹의 멤버에게 트래픽을 라우팅하는 경우입니다. 이름은 대소문자를 구분하지 않습니다.

단계 **4** 브리지 그룹 **ID** 필드에는 1~250 범위로 브리지 그룹 ID를 입력합니다.

단계 **5** 설명 필드에는 브리지 그룹에 대한 설명을 입력합니다.

단계 **6** 인터페이스 탭에서 인터페이스를 클릭하고 추가를 클릭하여 선택된 인터페이스 영역으로 이동합니다. 멤버로 추가하려면 모든 인터페이스에 대해 반복합니다.

단계 **7** (투명 모드) **IPv4** 탭을 클릭합니다. **IP** 주소 필드에 IPv4 주소 및 서브넷 마스크를 입력합니다.

BVI에 호스트 주소(/32 또는 255.255.255.255)를 할당하지 마십시오. 또한 /30 서브넷(255.255.255.252)과 같이 3개 미만의 호스트 주소(업스트림 라우터, 다운스트림 라우터, 투명 방화벽 각각 하나씩)를 포함한 다른 서브넷은 사용하지 마십시오. FTD 디바이스는 서브넷의 첫 주소 및 마지막 주소와 주고

받는 모든 ARP 패킷을 삭제합니다. 만약 /30 서브넷을 사용하고 그 서브넷에서 업스트림 라우터에 예약된 주소를 지정할 경우 FTD 디바이스는 다운스트림 라우터에서 업스트림 라우터로 ARP 요청을 폐기합니다.

고가용성을 위해서는 모니터링되는 인터페이스 영역의 디바이스 > 디바이스 관리 > 고가용성 탭에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

단계 **8** (라우팅 모드) **IPv4** 탭을 클릭합니다. IP 주소를 설정하려면 **IP** 유형 드롭다운 목록에서 다음 중 하나를 사용합니다.

고가용성 및 클러스터링 인터페이스는 고정 IP 주소 설정만 지원합니다. DHCP는 지원되지 않습니다.

- 고정 **IP** 사용 - IP 주소 및 서브넷 마스크를 입력합니다. 고가용성의 경우 고정 IP 주소만 사용할 수 있습니다. 모니터링되는 인터페이스 영역의 디바이스 > 디바이스 관리 > 고가용성 탭에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **DHCP** 사용 - 다음 선택 파라미터를 구성합니다.
  - **DHCP**에서 기본 경로 가져오기 - DHCP 서버에서 기본 경로를 가져옵니다.
  - **DHCP** 경로 메트릭 - 파악된 경로에 대해 1과 255 사이의 관리 거리를 할당합니다. 파악된 경로의 기본 관리 거리는 1입니다.

단계 **9** (선택 사항) IPv6 주소를 설정하려면 IPv6 주소 지정 구성, 826 페이지을 참조하십시오.

단계 **10** (선택 사항) (투명 모드에 한해) **ARP**와 **MAC** 설정을 구성하려면 고정 ARP 항목 추가, 839 페이지및 고정 MAC 주소를 추가하고 브리지 그룹에 대한 MAC 학습을 비활성화합니다., 840 페이지를 참조하십시오.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

투명 모드의 진단(관리) 인터페이스 구성

투명 방화벽 모드에서는 모든 인터페이스가 브리지 그룹에 속해야 합니다. 유일한 예외는 진단 슬롯/포트 인터페이스입니다. Firepower 4100/9300 섀시의 경우 진단 인터페이스 ID는 FTD 논리 디바이스에 할당된 mgmt 유형 인터페이스에 따라 달라집니다. 다른 인터페이스 형식은 진단 인터페이스로 사용할 수 없습니다. 하나의 진단 인터페이스만 구성할 수 있습니다.

시작하기 전에

이 인터페이스는 브리지 그룹에 할당하지 마십시오. 구성 불가한 브리지 그룹(ID 301)이 자동으로 구성에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 진단 인터페이스에 대해 수정( )를 클릭합니다.

단계 3 **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

단계 4 **IPv4** 탭을 클릭합니다. IP 주소를 설정하려면 **IP** 유형 드롭다운 목록에서 다음 중 하나를 사용합니다.

- 고정 **IP** 사용 - IP 주소 및 서브넷 마스크를 입력합니다.
- **DHCP** 사용 - 다음 선택 파라미터를 구성합니다.
  - **DHCP**에서 기본 경로 가져오기 - DHCP 서버에서 기본 경로를 가져옵니다.
  - **DHCP** 경로 메트릭 - 파악된 경로에 대해 1과 255 사이의 관리 거리를 할당합니다. 파악된 경로의 기본 관리 거리는 1입니다.
- **PPPoE** 사용 - 다음 매개 변수를 구성합니다.
  - **VPDN** 그룹 이름 - 그룹 이름을 지정합니다.
  - **PPPoE** 사용자 이름 - ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE** 암호/암호 확인 - ISP에서 제공한 비밀번호를 지정하고 확인합니다.
  - **PPP Authentication(PPP** 인증**)** - **PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

    PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
  - **PPPoE** 경로 메트릭 - 파악된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - 경로 설정 사용 - PPPoE IP 주소를 수동으로 구성하려면 이 체크 박스를 선택하고 **IP** 주소를 입력합니다.
  - 플래시에 사용자 이름 및 비밀번호 저장 - 플래시 메모리에 사용자 이름 및 비밀번호를 저장합니다.

    FTD에서는 NVRAM의 특수 위치에 사용자 이름 및 비밀번호를 저장합니다.

단계 5 (선택 사항) **IPv6** 주소를 설정하려면 IPv6 주소 지정 구성, 826 페이지를 참조하십시오.

단계 6 (선택 사항) 고급 탭에서 기타 설정을 구성합니다.

- MAC 주소 구성, 838 페이지의 내용을 참조하십시오.
- 고정 ARP 항목 추가, 839 페이지의 내용을 참조하십시오.

- 보안 구성 파라미터 설정, 841 페이지의 내용을 참조하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

IPv6 주소 지정 구성

이 섹션에서는 라우팅 및 투명 모드에서 IPv6 주소 지정을 구성하는 방법에 대해 설명합니다.

IPv6 정보

이 섹션에서는 IPv6에 대한 정보를 다룹니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- 전역—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 브리지 그룹의 경우 이 주소는 멤버 인터페이스가 아닌 BVI에 대해 구성되어야 합니다. 투명 모드에서는 관리 인터페이스에 대해 전역 IPv6 주소를 구성할 수도 있습니다.
- 링크-로컬—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 주소 구성 또는 주소 확인과 같은 네이버 검색 기능에 사용할 수 있습니다. 브리지 그룹에서 멤버 인터페이스에만 링크 로컬 주소가 있습니다. BVI에는 링크 로컬 주소가 없습니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 링크-로컬 주소가 인터페이스에서 자동으로 구성되므로 링크-로컬 주소를 특별히 구성하지 않아도 됩니다. 브리지 그룹 멤버 인터페이스에서 BVI에 전역 주소를 구성하는 경우, Firepower Threat Defense 디바이스에서는 멤버 인터페이스에 대한 링크 로컬 주소를 자동으로 생성합니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

수정된 EUI-64 인터페이스 ID

RFC 3513: IPv6(Internet Protocol Version 6) Addressing Architecture에 따르면, 모든 유니캐스트 IPv6 주소(이진 값 000으로 시작하는 것 제외)의 인터페이스 식별자 부분은 길이가 64비트이고 Modified EUI-64 형식이어야 합니다. Firepower Threat Defense 디바이스는 로컬 링크에 연결된 호스트에 이 요구 사항을 적용할 수 있습니다.

이 기능이 인터페이스에서 활성화된 경우, 그 인터페이스에서 수신한 IPv6 패킷의 소스 주소를 소스 MAC 주소와 비교하여 검증함으로써 인터페이스 식별자가 Modified EUI-64 형식을 사용하는지 확인합니다. IPv6 패킷에서 인터페이스 식별자에 Modified EUI-64 형식을 사용하지 않을 경우 패킷은 폐기되고 다음 시스템 로그 메시지가 생성됩니다.

```
325003: EUI-64 source address check failed.
```

주소 형식 검증은 흐름이 생성되는 경우에만 수행됩니다. 기존 흐름의 패킷은 검사하지 않습니다. 또한 이 주소 검증은 로컬 링크의 호스트에 대해서만 수행할 수 있습니다.

전역 IPv6 주소 구성

모든 라우팅 모드 인터페이스와 투명 또는 라우팅 모드 BVI에 전역 IPv6 주소를 구성하려면, 다음 단계를 수행하십시오.

참고 전역 주소를 자동으로 구성하면 링크-로컬 주소가 구성됩니다. 즉 따로 구성할 필요 없습니다. 브리지 그룹에서 BVI에 전역 주소를 구성하면 모든 멤버 인터페이스에서 링크 로컬 주소가 자동으로 구성됩니다.

FTD에서 정의된 하위 인터페이스는 상위 인터페이스에 동일하게 번인된 MAC 주소를 사용하기 때문에 MAC 주소의 수동 설정을 권장합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 FTD의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다. MAC 주소 구성, 838 페이지의 내용을 참조하십시오.

시작하기 전에

브리지 그룹에 대한 IPv6 네이버 검색의 경우, 양방향 액세스 규칙을 사용하여 FTD 브리지 그룹 멤버 인터페이스를 통해 네이버 요청(ICMPv6 유형 135) 및 네이버 알림(ICMPv6 유형 136) 패킷을 명시적으로 허용해야 합니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 수정할 인터페이스의 수정( )을 클릭합니다.

단계 3 **IPv6** 페이지를 클릭합니다.

라우팅 모드에서는 기본적으로 **Basic(**기본**)** 페이지가 선택되어 있습니다. 투명 모드에서는 기본적으로 **Address(**주소**)** 페이지가 선택되어 있습니다.

단계 4 **Basic(**기본**)** 페이지에서 **Enable IPv6(IPv6** 활성화**)**를 선택합니다.

단계 5 다음 방법 중 하나를 사용하여 전역 IPv6 주소를 구성합니다.

- (라우팅 인터페이스) 상태 비저장 자동 구성 - 자동 구성 확인란을 선택합니다.

  인터페이스에서 스테이트리스 자동 컨피그레이션을 활성화하면 라우터 광고 메시지에서 수신된 접두사를 기반으로 IPv6 주소가 구성됩니다. 스테이트리스 자동 컨피그레이션이 활성화될 경

우, Modified EUI-64 인터페이스 ID를 기반으로 하는 Link-Local 주소가 인터페이스에 대해 자동으로 생성됩니다.

RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 FTD 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지가 표시되지 않도록 하려면 **IPv6** > 설정 > **RA** 활성화 체크 박스의 선택을 취소합니다.

- 수동 컨피그레이션 — 전역 IPv6 주소를 수동으로 컨피그레이션하려면

  1. **Address(**주소**)** 페이지를 클릭하고 **Add Address(**주소 추가**)**를 클릭합니다.

     주소 추가 대화 상자가 나타납니다.

  2. 주소 필드에 인터페이스 ID를 포함한 전체 전역 IPv6 주소를 입력하거나 IPv6 접두사 길이를 포함한 IPv6 접두사를 입력합니다. (라우팅 모드) 접두사만 입력하려면 **EUI 64** 강제 체크 박스를 선택하여 수정된 EUI-64 형식을 사용한 인터페이스 ID를 생성해야 합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48(전체 주소) 또는 2001:0DB8::/48(접두사, EUI 64 선택됨) 같은 형태입니다.

     (**EUI 64** 강제를 선택하지 않은 경우) 고가용성의 경우, **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **High Availability(**고가용성**)** 페이지의 **Monitored Interfaces(**모니터링되는 인터페이스**)**에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

단계 **6** 라우팅 인터페이스의 경우, **Basic(**기본**)** 페이지에서 필요에 따라 다음 값을 설정할 수 있습니다.

- 로컬 링크의 IPv6 주소에서 수정된 EUI-64 형식 인터페이스 식별자 사용을 강제하려면 **EUI-64** 체크 상자를 확인하십시오.
- 링크-로컬 주소를 수동으로 설정하려면 링크-로컬 주소 필드에 주소를 입력합니다.

  링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). 전역 주소를 구성하지 않고 링크-로컬 주소만 구성해야 할 경우, 링크-로컬 주소를 수동으로 정의하는 옵션을 선택할 수 있습니다. Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.
- 주소 구성에 **DHCP** 사용 체크 상자를 선택하면 IPv6 라우터 알림 패킷에서 기타 주소 구성 플래그를 설정합니다.

  IPv6 라우터 알림의 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 파생된 스테이트리스 자동 컨피그레이션 주소 이외의 주소도 얻도록 안내합니다.
- 주소 외 구성에 **DHCP** 사용 체크 상자를 선택하면 IPv6 라우터 알림 패킷에서 기타 주소 구성 플래그를 설정합니다.

  IPv6 라우터 알림의 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.

단계 **7** 라우팅 인터페이스의 **Prefixes(**접두사**)** 및 **Settings(**설정**)** 페이지에서 설정을 구성하려면 IPv6 네이버 검색 구성, 829 페이지의 내용을 참조하십시오. BVI 인터페이스의 경우, **Settings(**설정**)** 페이지에 있는 다음의 매개변수를 확인하십시오.

- **DAD** 시도 - 최대 DAD 시도 수로 1에서 600사이의 값을 지정합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다. 이 설정은 IPv6 주소에 대한 DAD를 수행하는 동안 인터페이스에서 전송되는 연속 네이버 요청 메시지의 개수를 구성합니다. 기본값은 1입니다.
- **NS** 간격 - 인터페이스에서 IPv6 네이버 요청 재전송 간격이며 1000~3600000밀리초 사이의 범위입니다. 기본값은 1000밀리초입니다.
- 연결 가능 확인 - 연결 가능 확인 이벤트가 일어나고 원격 IPv6 노드가 연결 가능한 것으로 간주되는 시간이며 0~3600000밀리초 사이의 범위입니다. 기본값은 0밀리초입니다. 값이 0이면 연결 가능 시간은 undetermined로 전송됩니다. 연결 가능 시간의 값을 설정하고 추적하는 일은 수신 디바이스에서 담당합니다. 네이버 연결 가능 시간으로 사용 불가 네이버를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 네이버를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

IPv6 네이버 검색 구성

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

IPv6 네이버 검색 프로세스는 ICMPv6 메시지와 solicited-node 멀티캐스트 주소를 사용하여 동일 네트워크(로컬 링크)에 있는 네이버의 링크 계층 주소를 확인하고 네이버의 가독성을 확인하며 주변 라우터를 추적합니다.

노드(호스트)는 네이버 검색을 사용하여 연결된 링크에 상주하는 것으로 알려진 네이버에 대한 링크 계층 주소를 확인하고 무효화되는 충돌 값을 빠르게 삭제합니다. 호스트는 또한 네이버 검색을 사용하여 대신 패킷을 전달할 의사가 있는 주변 라우터를 찾기도 합니다. 또한 노드는 프로토콜을 이용하여 네이버의 연결 가능 여부를 능동적으로 추적하고 변경된 링크 계층 주소를 감지합니다. 라우터 또는 라우터 경로가 실패할 경우 호스트가 정상 작동하는 대안을 능동적으로 검색합니다.

시작하기 전에

라우팅 모드에서만 지원됩니다. 투명 모드에서 지원되는 IPv6 네이버 설정에 대해서는 전역 IPv6 주소 구성, 827 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

단계 **3** **IPv6**를 클릭한 다음 접두사를 클릭합니다.

단계 **4** (선택 사항) IPv6 라우터 알림에 어떤 IPv6 접두사를 포함할지 구성하려면 다음 단계를 수행합니다.

a) **Add Prefix(**접두사 추가**)**를 클릭합니다.

b) 주소 필드에 접두사 길이를 포함한 IPv6 주소를 입력하거나 기본 접두사를 사용하려면 기본 확인란을 선택합니다.

c) (선택 사항) 알림의 체크 박스의 선택을 해제하면 IPv6 접두사가 알려지지 않음을 나타냅니다.

d) 오프 링크 체크 박스를 선택하면 지정된 접두사가 링크에 할당됨을 나타냅니다. 지정된 접두사를 포함한 주소로 트래픽을 보내는 노드는 링크에서 목적지와의 로컬 연결이 가능한 것으로 간주합니다. 이 접두사는 온 링크 결정에 사용할 수 없습니다.

e) 자동 설정에 지정된 접두사를 사용하려는 경우 자동 설정 확인란을 선택합니다.

f) 접두사 수명을 선택하려면 기간 또는 만료 날짜를 클릭합니다.

- 기간 - 접두사에 대한 선호 수명을 초 단위로 입력합니다. 이 설정은 지정된 IPv6 접두사가 유효 수명으로 광고되는 기간입니다. 최대값은 무한대를 나타냅니다. 유효한 값은 0~4294967295입니다. 기본값은 2592000(30일)입니다. 접두사에 대한 유효 수명을 초 단위로 입력합니다. 이 설정은 지정된 IPv6 접두사가 기본 수명으로 광고되는 기간입니다. 최대값은 무한대를 나타냅니다. 유효한 값은 0 ~ 4294967295입니다. 기본 설정은 604800(7일)입니다. 무제한 기간을 설정하려면 무한 체크 상자를 선택합니다.
- 만료 날짜 - 유효하고 선호되는 날짜 및 시간을 선택합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **5** 설정을 클릭합니다.

단계 **6** (선택 사항) 1~600 사이로 **DAD** 시도 최대 수를 설정합니다. 기본값은 1입니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.

이 설정은 IPv6 주소에 대한 DAD를 수행하는 동안 인터페이스에서 전송되는 연속 네이버 요청 메시지의 개수를 구성합니다.

스테이트리스 자동 컨피그레이션 프로세스에서 DAD(Duplicate Address Detection)는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다.

중복 주소가 확인되면 주소 상태가 DUPLICATE로 설정되고 주소가 사용되지 않으며 다음 오류 메시지가 생성됩니다.

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다.

단계 **7** (선택 사항) **NS** 간격 필드에서 1000~3600000밀리초 사이로 IPv6 네이버 요청 재전송 간격을 설정합니다.

기본값은 1000밀리초입니다.

네이버 요청 메시지(ICMPv6 Type 135)는 로컬 링크에 있는 다른 노드의 링크 계층 주소를 발견하려는 노드가 로컬 링크에서 전송합니다. 네이버 요청 메시지를 수신한 후 목적지 노드는 로컬 링크에서 네이버 광고 메시지(ICPMv6 Type 136)를 전송함으로써 응답합니다.

소스 노드가 네이버 광고를 수신한 후 소스 노드와 목적지 노드가 통신할 수 있습니다. 네이버 요청 메시지는 네이버의 링크 계층 주소를 식별한 후 네이버의 연결 가능성을 확인하는 데 사용됩니다. 노드가 네이버의 연결 가능성을 확인하고자 하는 경우 네이버 요청 메시지의 목적지 주소는 네이버의 유니캐스트 주소입니다.

네이버 광고 메시지는 로컬 링크에 있는 노드의 링크 계층 주소가 변경될 경우에도 전송됩니다.

단계 **8** (선택 사항) 연결 가능 확인 이벤트가 일어나고 원격 IPv6 노드가 연결 가능한 것으로 간주되는 시간을 연결 가능 확인 필드에 0~3600000밀리초 사이의 범위로 입력합니다.

기본값은 0밀리초입니다. 값이 0이면 연결 가능 시간은 undetermined로 전송됩니다. 연결 가능 시간의 값을 설정하고 추적하는 일은 수신 디바이스에서 담당합니다.

네이버 연결 가능 시간으로 사용 불가 네이버를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 네이버를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.

단계 **9** (선택 사항) 라우터 알림 전송을 원하지 않을 경우 **RA** 활성화 체크 박스의 선택을 취소합니다. 라우터 알림 전송을 활성화하는 경우 RA 수명 및 간격을 설정할 수 있습니다.

라우터 알림 메시지(ICMPv6 Type 134)는 라우터 요청 메시지(ICMPv6 Type 133)에 대한 응답으로 자동 전송됩니다. 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

Firepower Threat Defense 디바이스가 IPv6 접두사를 전송하길 원치 않는 인터페이스에서 이 메시지를 비활성화할 수 있습니다(예: 인터페이스 외부).

- **RA** 수명 - 0~9000초 사이로 IPv6 라우터 알림에서 라우터 수명 값을 구성합니다.

  기본값은 1800초입니다.

- **RA** 간격 - 3~1800초 사이로 IPv6 라우터 알림 전송 간격을 구성합니다.

  기본값은 200초입니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

고급 인터페이스 설정 구성

이 섹션에서는 일반 방화벽 모드 인터페이스에 대한 MAC 주소를 구성하는 방법, 최대 전송 단위(MTU)를 설정하는 방법, 기타 고급 파라미터를 설정하는 방법을 설명합니다.

고급 인터페이스 구성 정보

이 섹션에서는 고급 인터페이스 설정을 설명합니다.

MAC 주소 정보

MAC 주소를 수동으로 할당하여 기본값을 재정의할 수 있습니다. . 컨테이너 인스턴스의 경우 FXOS 섀시는 모든 인터페이스에 대해 고유 MAC 주소를 자동으로 생성합니다.

참고 FTD에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 FTD의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

참고 컨테이너 인스턴스의 경우에는 하위 인터페이스를 공유하지 않더라도 MAC 주소를 수동으로 구성하는 경우에는 패킷이 적절하게 분류되도록 같은 상위 인터페이스의 모든 하위 인터페이스에 대해 고유 MAC 주소를 사용해야 합니다.

기본 MAC 주소

기본 인스턴스의 경우**:**

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- VLAN 인터페이스(Firepower 1010) - 라우팅된 방화벽 모드: 모든 VLAN 인터페이스에서 MAC 주소를 공유합니다. 연결된 스위치가 이 시나리오에 도움이 될 수 있을지 확인하십시오. 연결된 스위치에 고유한 MAC 주소가 필요한 경우, MAC 주소를 수동으로 할당할 수 있습니다. MAC 주소 구성, 838 페이지를 참조하십시오.

투명 방화벽 모드: 각 VLAN 인터페이스에는 고유한 MAC 주소가 있습니다. 원하는 경우 MAC 주소를 수동으로 할당하여 생성된 MAC 주소를 재정의할 수 있습니다. MAC 주소 구성, 838 페이지의 내용을 참조하십시오.

- 이중 인터페이스 - 이중 인터페이스에서는 추가하는 첫 물리적 인터페이스의 MAC 주소를 사용합니다. 구성에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 이중 인터페이스에 MAC 주소를 할당하면 멤버 인터페이스 MAC 주소와 상관없이 이 주소가 사용됩니다.
- 하위 인터페이스(FTD에서 정의) - 물리적 인터페이스의 모든 하위 인터페이스에서도 동일한 번인된(burned-in) MAC 주소를 사용합니다. 하위 인터페이스에 고유한 MAC 주소를 할당할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 FTD의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

컨테이너 인스턴스의 경우:

- 모든 인터페이스의 MAC 주소를 MAC 주소 풀에서 가져옵니다. 하위 인터페이스의 경우에는 MAC 주소를 수동으로 구성할 때 적절한 분류를 위해 동일한 상위 인터페이스의 모든 하위 인터페이스에 대해 고유한 MAC 주소를 사용해야 합니다. 컨테이너 인스턴스 인터페이스용 자동 MAC 주소, 747 페이지의 내용을 참조하십시오.

MTU 정보

MTU에서는 Firepower Threat Defense 디바이스가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 없는 프레임 크기입니다. 예를 들어, MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더 포함 시 1518바이트이고 VLAN 사용 시에는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오.

경로 MTU 검색

Firepower Threat Defense 디바이스에서는 경로 MTU 검색을 지원하며(RFC 1191에 규정), 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

기본 MTU

Firepower Threat Defense 디바이스의 기본 MTU는 1500바이트입니다. 이 값에는 18~22바이트의 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 포함되지 않습니다.

MTU 및 단편화

IPv4의 경우 지정된 MTU보다 큰 발신 IP 패킷은 2개 이상의 프레임으로 단편화됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. IPv6의 경우에는 일반적으로 패킷의 단편화가 전혀 허용되지 않습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

TCP 패킷의 경우 엔드포인트는 일반적으로 해당 MTU를 사용해 TCP 최대 세그먼트 크기(예: MTU - 40)를 결정합니다. 중간에 사이트 대 사이트 VPN 터널 등에 사용하기 위해 TCP 헤더가 더 추가된 경우에는 터널링 엔티티를 통해 TCP MSS를 하향 조정해야 할 수 있습니다. TCP MSS 정보, 834 페이지를 참조하십시오.

UDP 또는 ICMP의 경우 애플리케이션은 단편화 방지를 위해 MTU를 고려해야 합니다.

참고 Firepower Threat Defense 디바이스에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다.

MTU와 점보 프레임

큰 MTU를 사용하는 경우 더 큰 패킷을 전송할 수 있습니다. 큰 패킷은 네트워크에서 더욱 효율적으로 사용할 수 있습니다. 다음 지침을 참조하십시오.

- 트래픽 경로의 MTU 일치 — 모든 FTD 인터페이스 및 기타 디바이스 인터페이스의 MTU를 트래픽 경로와 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.

TCP MSS 정보

TCP MSS(최대 세그먼트 크기)는 TCP 및 IP 헤더가 추가되기 전의 TCP 페이로드 크기입니다. UDP 패킷은 영향을 받지 않습니다. 연결을 설정할 경우 클라이언트와 서버에서는 3방향 핸드셰이크 동안 TCP MSS 값을 교환합니다.

Firepower Threat Defense 디바이스에서 통과 트래픽에 대해 FlexConfig의 Sysopt_Basic 개체를 사용하여(참조) TCP MSS를 설정할 수 있습니다(Firepower Threat Defense에 대한 FlexConfig 정책, 1269 페이지 참조). 기본적으로 최대 TCP MSS는 1380바이트로 설정됩니다. 이 설정은 Firepower Threat Defense 디바이스에서 IPsec VPN 캡슐화를 할 때 패킷 크기를 추가해야 하는 경우 유용합니다. 그러나 IPsec 이외의 엔드포인트에 대해서는 Firepower Threat Defense 디바이스에서 최대 TCP MSS를 비활성화해야 합니다.

최대 TCP MSS를 설정하는 경우, 연결의 엔드포인트에서 Firepower Threat Defense 디바이스에 설정된 값보다 큰 TCP MSS를 요청하면 Firepower Threat Defense 디바이스에서는 요청 패킷의 TCP MSS를 Firepower Threat Defense 디바이스 최대값으로 덮어씁니다. 호스트 또는 서버에서 TCP MSS를 요청하지 않을 경우, Firepower Threat Defense 디바이스에서는 RFC 793 기본값을 536바이트(IPv4) 또는 1220바이트(IPv6)로 가정하며 패킷을 수정하지 않습니다. 기본 MTU를 1500바이트로 유지하는 경우를 예로 들어보겠습니다. 이 경우 호스트는 1500바이트에서 TCP 및 IP 헤더 길이를 뺀 MSS를 요청하므로 MSS는 1460으로 설정됩니다. Firepower Threat Defense 디바이스 최대 TCP MSS가 1380(기본값)이면 Firepower Threat Defense 디바이스에서는 TCP 요청 패킷의 MSS 값을 1380으로 변경합니다. 그러면 서버에서는 1380바이트 페이로드가 포함된 패킷을 전송합니다. 이 경우 Firepower Threat Defense 디바이스이(가) 최대 120바이트의 헤더를 패킷에 추가해도 MTU 크기인 1500을 맞출 수 있습니다.

또한 최소 TCP MSS를 구성할 수 있습니다. 호스트 또는 서버에서 요청한 TCP MSS가 매우 작을 경우, Firepower Threat Defense 디바이스에서는 값을 조정하여 올릴 수 있습니다. 기본적으로 최소 TCP MSS는 활성화되어 있지 않습니다.

SSL VPN 연결 트래픽을 포함한 to-the-box 트래픽에는 이 설정이 적용되지 않습니다. 이 경우 Firepower Threat Defense 디바이스에서는 MTU를 사용하여 TCP MSS: MTU - 40(IPv4) 또는 MTU - 60(IPv6)을 파생합니다.

기본 TCP MSS

기본적으로 Firepower Threat Defense 디바이스의 최대 TCP MSS는 1380바이트입니다. 이 기본값을 사용하면 헤더가 120바이트와 동일한 값까지 가능한 경우 IPv4 IPsec VPN 연결을 수용하는 것이 가능합니다. 이 값은 기본값이 1500바이트인 MTU에 적합합니다.

최대 TCP MSS 설정 제안

기본 TCP MSS는 Firepower Threat Defense 디바이스가 IPv4 IPsec VPN 엔드포인트 역할을 수행하고 1500바이트의 MTU를 갖는다고 가정합니다. Firepower Threat Defense 디바이스가 IPv4 IPsec VPN 엔드포인트 역할을 수행하는 경우, TCP 및 IP 헤더용으로 최대 120바이트까지 수용해야 합니다.

MTU 값을 변경하고 IPv6를 사용하거나 Firepower Threat Defense 디바이스를 IPsec VPN 엔드포인트로 사용하지 않는 경우, FlexConfig에서 Sysopt_Basic 개체를 사용하여 TCP MSS 설정을 변경해야 합니다. Firepower Threat Defense에 대한 FlexConfig 정책, 1269 페이지의 내용을 참조하십시오. 다음 지침을 참조하십시오.

- 정상 트래픽 — TCP MSS 제한을 비활성화하고 연결 엔드포인트 간에 설정한 값을 허용합니다. 연결 엔드포인트의 경우 대개 MTU에서 TCP MSS가 파생되므로 비 IPsec 패킷은 일반적으로 이러한 TCP MSS에 적합합니다.
- IPv4 IPsec 엔드포인트 트래픽 — MTU에 대한 최대 TCP MSS를 120으로 설정합니다. 예를 들어, 점보 프레임을 사용하고 MTU를 9000으로 설정할 경우 새로운 MTU를 활용하기 위해 TCP MSS를 8880으로 설정해야 합니다.
- IPv6 IPsec 엔드포인트 트래픽 — MTU에 대한 최대 TCP MSS를 140으로 설정합니다.

브리지 그룹 트래픽에 대한 ARP 검사

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 간에 허용됩니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다.

ARP 감시 기능은 악의적인 사용자가 다른 호스트 또는 라우터로 위장(ARP 스푸핑이라고도 함)하는 것을 방지합니다. ARP 스푸핑은 "끼어들기" 공격을 활성화할 수 있습니다. 예를 들어, 호스트에서 ARP 요청을 게이트웨이 라우터에 전송할 경우 해당 게이트웨이 라우터는 게이트웨이 라우터 MAC 주소에 응답합니다. 그러나 공격자는 라우터 MAC 주소가 아닌 공격자 MAC 주소가 포함된 다른 ARP 응답을 호스트에 전송합니다. 이제 공격자는 라우터에 트래픽이 전달되기 전에 모든 호스트 트래픽을 가로챌 수 있게 됩니다.

ARP 감시 기능은 고정 ARP 테이블에 올바른 MAC 주소와 관련 IP 주소를 입력하기만 하면 공격자가 공격자 MAC 주소가 포함된 ARP 응답을 보낼 수 없도록 합니다.

ARP 감시를 활성화할 경우 Firepower Threat Defense 디바이스에서는 MAC 주소, IP 주소, 모든 ARP 패킷의 소스 인터페이스를 ARP 테이블의 고정 항목과 비교하고 다음과 같은 조치를 취합니다.

- IP 주소, MAC 주소, 소스 인터페이스가 ARP 항목과 일치하면 패킷이 통과됩니다.

- MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 Firepower Threat Defense 디바이스에서는 패킷을 누락시킵니다.
- ARP 패킷이 고정 ARP 테이블의 어느 항목과도 일치하지 않으면 Firepower Threat Defense 디바이스를 설정하여 패킷을 모든 인터페이스로 전달(플러딩)하거나 패킷이 누락되도록 합니다.

참고 전용 진단 인터페이스는 이 파라미터가 플러딩을 실행하도록 설정된 경우에도 패킷을 플러딩하지 않습니다.

MAC 주소 테이블

브리지 그룹을 사용할 때 FTD에서는 일반적인 브리지 또는 스위치와 유사한 방식으로 MAC 주소 테이블을 학습하고 구축합니다. 디바이스에서 브리지 그룹을 통해 패킷을 전송하면 FTD에서는 MAC 주소를 해당 테이블에 추가합니다. 테이블에서는 MAC 주소와 소스 인터페이스를 연결하므로 FTD에서는 디바이스에 대해 주소가 지정된 모든 패킷을 올바른 인터페이스로 전송할 수 있다는 사실을 파악합니다. 브리지 그룹 멤버는 FTD 보안 정책의 적용을 받으므로, 패킷의 목적지 MAC 주소가 테이블에 없다면 일반적인 브리지에서는 원래 패킷을 모든 인터페이스에 플러딩하지만 FTD의 경우에는 이러한 작업을 수행하지 않습니다. 그 대신 ASA에서는 직접 연결된 디바이스 또는 원격 디바이스에 다음 패킷을 생성합니다.

- 직접 연결된 디바이스에 대한 패킷 - FTD에서 대상 IP 주소에 대한 ARP 요청을 생성하므로 어떤 인터페이스에서 ARP 응답을 수신하는지 알 수 있습니다.
- 원격 디바이스에 대한 패킷 — FTD에서 대상 IP 주소에 대한 Ping을 생성하므로 어떤 인터페이스에서 Ping 응답을 수신하는지 알 수 있습니다.

원래 패킷은 손실됩니다.

기본 설정

- ARP 감시를 활성화할 경우 기본 설정은 불일치 패킷을 플러딩하는 것입니다.
- 동적 MAC 주소 테이블 항목의 기본 시간 초과 값은 5분입니다.
- 기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, Firepower Threat Defense 디바이스에서는 해당 항목을 MAC 주소 테이블에 추가합니다.

참고 Firepower Threat Defense 디바이스 상태 기반 검사 엔진에 의해 거부된 연결을 재설정하기 위한 재설정 패킷을 생성합니다. 여기서 패킷의 대상 MAC 주소는 ARP 테이블 조회를 기반으로 결정되지 않지만 거부되는 패킷(연결)에서 직접 가져옵니다.

ARP 검사 및 MAC 주소 테이블에 대한 지침

- ARP 검사는 브리지 그룹에만 지원됩니다.
- MAC 주소 테이블 구성은 브리지 그룹에만 지원됩니다.

MTU 구성

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

점보 프레임을 허용하려면 인터페이스에서 MTU를 사용자 정의해야 합니다.

⚠

주의 데이터 인터페이스에 대해 디바이스의 최고 MTU 값을 변경하면 구성 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 데이터 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 이 주의 사항은 진단 인터페이스 또는 관리 전용 인터페이스에는 적용되지 않습니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

시작하기 전에

- MTU를 1500바이트 이상으로 변경하면 점보 프레임이 자동으로 활성화됩니다. ASA 모델의 경우 점보 프레임을 사용하려면 시스템을 다시 로드해야 합니다.
- 인라인 집합의 인터페이스를 사용하는 경우 MTU 설정이 사용되지 않습니다. 그러나 점보 프레임 설정은 인라인 집합과 관련이 있으며 점보 프레임은 최대 9000바이트까지 패킷을 수신하도록 인라인 인터페이스를 활성화합니다. 점보 프레임을 활성화하려면 모든 인터페이스의 MTU를 1500바이트 이상으로 설정해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정(✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정(✎)을 클릭합니다.

단계 **3** 일반 탭에서 64~9198바이트 사이의 **MTU**를 설정하십시오. Firepower Threat Defense Virtual의 경우 9000이고 Firepower 4100/9300 섀시의 FTD의 경우 9184입니다.

기본값은 1500바이트입니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 **6** ASA 모델의 경우 MTU를 1500바이트 이상으로 설정하면 점보 프레임을 활성화하기 위해 시스템을 다시 로드해야 합니다.

MAC 주소 구성

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

MAC 주소를 수동으로 할당해야 할 수 있습니다. 또한 디바이스 > 기기 관리 > 고가용성 탭에서 액티브 및 스탠바이 MAC 주소를 설정할 수 있습니다. 두 화면의 인터페이스에 대한 MAC 주소를 설정하는 경우 인터페이스 > 고급 탭의 주소가 우선 적용됩니다.

참고 컨테이너 인스턴스의 경우에는 하위 인터페이스를 공유하지 않더라도 MAC 주소를 수동으로 구성하는 경우에는 패킷이 적절하게 분류되도록 같은 상위 인터페이스의 모든 하위 인터페이스에 대해 고유 MAC 주소를 사용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

단계 **3** **Advanced(**고급**)** 탭을 클릭합니다.
정보 탭을 선택합니다.

단계 **4** 액티브 **MAC** 주소 필드에 H.H.H. 형식으로 MAC 주소를 입력하고, 여기서 H는 16비트 16진수입니다.

예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력됩니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다. 즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없습니다.

단계 **5** 스탠바이 **MAC** 주소에 고가용성에 사용할 MAC 주소를 입력합니다.

액티브 유닛이 페일오버되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

단계 6 **OK(**확인**)**를 클릭합니다.

단계 7 **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

고정 ARP 항목 추가

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 간에 허용됩니다. ARP 검사를 활성화하여 ARP 패킷 플로우를 제어할 수 있습니다.(ARP 검사 설정, 1423 페이지 참조) ARP 검사에서는 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교합니다.

라우팅 인터페이스의 경우 고정 ARP 항목을 입력할 수 있지만 일반적으로 동적 항목이면 충분합니다. 라우팅 인터페이스의 경우 직접 연결된 호스트에 패킷을 전달하는 데 ARP 테이블이 사용됩니다. 발신자가 IP 주소로 패킷 대상을 식별하긴 하지만, 이더넷에서 패킷이 실제 전달되는 것은 이더넷 MAC 주소에 달려 있습니다. 라우터 또는 호스트에서 패킷을 직접 연결된 디바이스에 전달하려는 경우, IP 주소와 연관된 MAC 주소를 묻는 ARP 요청이 전송되며 그 후 ARP 응답에 따라 패킷이 MAC 주소로 전달됩니다. 호스트 또는 라우터에서는 ARP 테이블을 보관하므로, 모든 패킷을 전달할 때마다 ARP 요청을 보내지 않아도 됩니다. ARP 테이블은 ARP 응답이 네트워크로 전송될 때마다 동적으로 업데이트되며, 일정 기간 동안 사용되지 않는 항목이 있으면 해당 항목은 시간 초과로 만료됩니다. 항목이 잘못된 경우(예: 제공된 IP 주소의 MAC 주소가 변경된 경우), 해당 항목은 새 정보로 업데이트되기 전에 시간 제한에 도달해야 합니다.

투명 모드의 경우 FTD은 관리 트래픽 등 FTD 디바이스와 주고받는 ARP 테이블의 다이내믹 ARP 항목만 사용합니다.

시작하기 전에

이 화면은 명명된 인터페이스에서만 사용 가능합니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 수정할 인터페이스의 수정( )을 클릭합니다.

단계 3 고급 탭을 클릭하고 **ARP** 탭(투명 모드의 경우 **ARP** 및 **MAC**)을 클릭합니다.

단계 4 **ARP** 설정 추가를 클릭합니다.

ARP 설정 추가 대화 상자가 나타납니다.

단계 **5** **IP** 주소 필드에 호스트의 IP 주소를 입력합니다.

단계 **6** **MAC** 주소 필드에 호스트의 MAC 주소를 00e0.1e4e.3d8b과 같은 형식으로 입력합니다.

단계 **7** 이 주소에 대해 프록시 ARP를 수행하려면 별칭 활성화 체크 상자를 선택합니다.

지정된 IP 주소의 ARP 요청이 FTD 디바이스에 수신되면 ASA에서는 지정된 MAC 주소에 응답합니다.

단계 **8** **OK**를 클릭하고 고급 설정에서 나가려면 다시 **OK**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

고정 MAC 주소를 추가하고 브리지 그룹에 대한 MAC 학습을 비활성화합니다.

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

일반적으로 MAC 주소는 특정 MAC 주소의 트래픽이 인터페이스에 들어올 때 MAC 주소 테이블에 동적으로 추가됩니다. MAC 주소 학습을 비활성화할 수 있으나, 테이블에 MAC 주소를 고정으로 추가하지 않으면 트래픽이 FTD를 통과하여 전달될 수 없습니다. 고정 MAC 주소를 MAC 주소 테이블에 추가할 수 있습니다. 고정 항목을 추가함으로써 얻을 수 있는 한 가지 혜택은 MAC 스푸핑을 차단할 수 있다는 점입니다. 동일한 MAC 주소를 고정 항목으로 보유한 클라이언트에서 고정 항목이 일치하지 않는 인터페이스에 트래픽을 전송하려고 시도할 경우, FTD 디바이스에서는 해당 트래픽을 누락하며 시스템 메시지가 생성됩니다. 고정 ARP 항목을 추가할 경우(고정 ARP 항목 추가, 839 페이지 참조), 고정 MAC 주소가 MAC 주소 테이블에 자동으로 추가됩니다.

시작하기 전에

이 화면은 명명된 인터페이스에서만 사용 가능합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

단계 **3** 고급 탭을 클릭하고 **ARP** 및 **MAC** 탭을 클릭합니다.

단계 **4** (선택 사항) **MAC** 학습 활성화 체크 박스 선택을 취소하여 MAC 학습을 비활성화합니다.

단계 **5** 고정 MAC 주소를 추가하려면 **MAC** 구성 추가를 클릭합니다.
MAC 설정 추가 대화 상자가 나타납니다.

단계 **6** **MAC** 주소 필드에 호스트의 MAC 주소를 00e0.1e4e.3d8b과 같은 형식으로 입력합니다. **OK(**확인**)**를 클릭합니다.

단계 **7** 고급 설정에서 나가려면 **OK**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

보안 구성 파라미터 설정

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD	Any(모든)	관리자 액세스 관리자 네트워크 관리자

이 섹션에서는 IP 스푸핑을 방지하여 전체 프래그먼트 리어셈블리를 허용하고 플랫폼 설정의 디바이스 수준에서 기본 프래그먼트 설정 집합을 오버라이드하는 방법을 설명합니다.

스푸핑 차단

이 섹션에서는 인터페이스의 유니캐스트 역방향 경로 전달을 활성화합니다. 유니캐스트 RPF는 모든 패킷이 라우팅 테이블에 따라 올바른 소스 인터페이스와 일치하는 소스 IP 주소를 갖도록 보장함으로써 IP 스푸핑(실제 소스를 알아볼 수 없도록 패킷이 잘못된 소스 IP 주소를 사용함)을 방지합니다.

일반적으로 FTD 디바이스는 패킷을 어디로 전달할지를 결정할 때 수신 주소만 확인합니다. 유니캐스트 RPF는 디바이스에 소스 주소도 확인하도록 지시합니다. 따라서 이것을 RPF(Reverse Path Forwarding)라고 부릅니다. FTD 디바이스의 통과를 허용할 모든 트래픽에 대해 디바이스 라우팅 테이블은 소스 주소로 돌아가는 경로를 포함해야 합니다. 자세한 내용은 RFC 2267을 참조하십시오.

예를 들어 외부 트래픽의 경우 FTD 디바이스는 유니캐스트 RPF 보호를 충족하기 위해 기본 경로를 사용할 수 있습니다. 트래픽이 외부 인터페이스에서 들어오고 소스 주소가 라우팅 테이블에 알려지지 않은 경우, 디바이스는 기본 경로를 사용하여 외부 인터페이스를 소스 인터페이스로서 정확히 식별합니다.

트래픽이 라우팅 테이블에 알려진 주소에서 외부 인터페이스로 이동하는 경우 FTD 디바이스는 패킷을 삭제합니다. 마찬가지로, 트래픽이 알려지지 않은 소스 주소로부터 내부 인터페이스로 이동하는 경우 일치하는 경로(기본 경로)가 외부 인터페이스임을 나타내기 때문에 디바이스는 패킷을 삭제합니다.

유니캐스트 RPF는 다음과 같이 구현됩니다.

- ICMP 패킷에는 세션이 없으므로 각 패킷이 점검됩니다.

- UDP 및 TCP에는 세션이 있으므로 초기 패킷에서 역방향 경로 조회를 요구합니다. 세션 중에 도착하는 후속 패킷은 세션의 일부로서 유지 관리되는 기존 상태를 사용하여 점검됩니다. 초기 패킷 이외의 패킷에서는 초기 패킷에 사용된 것과 동일한 인터페이스에 도착했는지를 확인합니다.

패킷당 프래그먼트

기본적으로 FTD 디바이스는 IP 패킷당 최대 24 프래그먼트를 허용하고 리어셈블리 대기열에 최대 200개의 프래그먼트를 허용합니다. UDP를 통한 NFS와 같이 일상적으로 패킷을 프래그먼트하는 애플리케이션이 있는 경우 네트워크에 프래그먼트가 필요할 수도 있습니다. 그러나 트래픽을 프래그먼트하는 애플리케이션이 없으면 FTD 디바이스로 프래그먼트를 허용하지 않는 것이 좋습니다. 프래그먼트 패킷은 종종 서비스 거부(DoS) 공격으로 사용됩니다.

프래그먼트 리어셈블리

FTD 디바이스는 다음 프래그먼트 리어셈블리 프로세스를 수행합니다.

- IP 프래그먼트는 프래그먼트 집합이 구성되거나 시간 초과 간격이 경과할 때까지 수집됩니다.
- 어떤 프래그먼트 집합이 구성되면 그 집합에 대해 무결성 검사가 실시됩니다. 이 검사에서는 중복, 테일 오버플로우, 체인 오버플로우가 없는지도 검사합니다.
- FTD 디바이스에서 종료하는 IP 프래그먼트는 항상 완전히 재결합됩니다.
- 전체 프래그먼트 리어셈블리가 비활성화된 경우(기본), 프래그먼트 집합은 추가 처리를 위해 전송 레이어에 전달됩니다.
- 전체 프래그먼트 리어셈블리를 활성화하는 경우 프래그먼트 집합은 단일 IP 패킷에 먼저 결합됩니다. 이 단일 IP 패킷이 추가 처리를 위해 전송 계층으로 전달됩니다.

시작하기 전에

이 화면은 명명된 인터페이스에서만 사용 가능합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

단계 **3** 고급 탭을 클릭하고 보안 설정 탭을 클릭합니다.

단계 **4** 유니캐스트 역방향 경로 전송을 활성화하려면 스푸핑 차단 확인란을 선택합니다.

단계 **5** 전체 프래그먼트 리어셈블리를 활성화 하려면 전체 프래그먼트 리어셈블리 확인란을 선택합니다.

단계 **6** 패킷당 허용되는 프래그먼트의 수를 변경하려면 기본 프래그먼트 설정 오버라이드 체크 박스를 선택하고 다음 값을 설정합니다.

- 크기 - 리어셈블리를 위해 대기하는 IP 리어셈블리 데이터베이스에 포함될 수 있는 최대 패킷 수를 설정합니다. 기본값은 200입니다. 비활성화 프래그먼트는 1로 설정합니다.
- 체인 - 프래그먼트가 가능한 전체 IP 패킷의 최대 패킷 수입니다. 기본값은 24패킷입니다.

- 시간 초과 - 프래그먼트된 전체 패킷이 도착할 때까지 대기하는 최대 시간(초)입니다. 패킷의 첫 번째 프래그먼트가 도착하면 타이머가 시작됩니다. 패킷의 모든 프래그먼트가 지정된 시간(초)에 도착하지 않을 경우 이미 수신된 패킷의 프래그먼트는 모두 폐기됩니다. 기본값은 5일입니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Firepower Threat Defense 일반 방화벽 인터페이스 기록

기능	버전	세부 사항
FTD 작동 링크 상태와 Firepower 4100/9300의 물리적 링크 상태 간 동기화	6.7	이제 Firepower 4100/9300 섀시는 FTD 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. FTD 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 FTD에서 동기화하지 않으면 FTD 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 FTD 종료를 시작한 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 인라인 집합의 경우 FTD에서 트래픽을 처리하기 전에 외부 라우터가 FTD로 트래픽 전송을 시작할 수 있으므로 이러한 상태 불일치로 인해 패킷이 삭제될 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다. 참고 이 기능은 클러스터링, 컨테이너 인스턴스 또는 Radware vDP 데코레이터가 포함된 FTD에는 지원되지 않습니다. ASA에서도 지원되지 않습니다. 신규/수정된 Firepower Chassis Manager 화면: **Logical Devices(**논리적 디바이스**) > Enable Link State(**링크 상태 활성화**)** 신규/수정된 FXOS 명령: **set link-state-sync enabled**, **show interface expand detail** 지원되는 플랫폼: Firepower 4100/9300

기능	버전	세부 사항
Firepower 1010 하드웨어 스위치 지원	6.5	Firepower 1010에서는 각 이더넷 인터페이스를 스위치 포트 또는 방화벽 인터페이스로 설정하는 것을 지원합니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Add VLAN Interface(VLAN** 인터페이스 추가**)**
이더넷 1/7 및 이더넷 1/8에서의 Firepower 1010 PoE+ 지원	6.5	Firepower 1010에서는 스위치 포트로 구성된 이더넷 1/7 및 이더넷 1/8의 PoE+(Power over Ethernet+)를 지원합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** > **PoE**
컨테이너 인스턴스에 사용할 VLAN 하위 인터페이스	6.3.0	물리적 인터페이스를 유연하게 사용할 수 있도록 FXOS에서 VLAN 하위 인터페이스를 생성하는 동시에 여러 인스턴스 간에 인터페이스를 공유할 수 있습니다. 신규/수정된 Firepower Management Center 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**수정**)** 아이콘 > **Interfaces(**인터페이스**)** 탭 신규/수정된 Firepower Chassis Manager 화면: **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Add New(**새로 추가**)** 드롭다운 메뉴 > **Subinterface(**하위 인터페이스**)** 신규/수정된 명령: **create subinterface, set vlan, show interface,show subinterface** 지원되는 플랫폼: Firepower 4100/9300
컨테이너 인스턴스용 데이터 공유 인터페이스	6.3.0	물리적 인터페이스를 유연하게 사용할 수 있도록 여러 인스턴스 간에 인터페이스를 공유할 수 있습니다. 신규/수정된 Firepower Chassis Manager화면. **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Type(**유형**)** 신규/수정된 명령: **set port-type data-sharing, show interface** 지원되는 플랫폼: Firepower 4100/9300

기능	버전	세부 사항
통합 라우팅 및 브리징	6.2.0	통합 라우팅 및 브리징은 브리지 그룹과 라우팅 인터페이스 간을 라우팅하는 기능을 제공합니다. 브리지 그룹은 FTD에서 경로 대신 브리징하는 인터페이스 그룹입니다. FTD는 실제 브리지가 아닙니다. FTD는 계속해서 방화벽으로 작동하며, 이를 통해 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다. 이전에는 브리지 그룹 간에 라우팅할 수 없는 투명 방화벽 모드에서만 브리지 그룹을 구성할 수 있었습니다. 이 기능을 사용하면 라우팅 방화벽 모드에서 브리지 그룹을 구성하고 브리지 그룹 간, 그리고 브리지 그룹과 라우팅 인터페이스 간을 라우팅할 수 있습니다. 브리지 그룹은 BVI(브리지 가상 인터페이스)를 사용하여 라우팅에 참여함으로써 브리지 그룹의 게이트웨이로 작동합니다. 브리지 그룹에 할당할 추가 인터페이스가 FTD에 있는 경우에는 외부 Layer 2 스위치를 사용하는 대신 통합형 라우팅 및 브리징을 사용할 수 있습니다. 라우팅 모드에서 BVI는 명명된 인터페이스가 될 수 있으며 액세스 규칙 및 DHCP 서버 같은 일부 기능에서 멤버 인터페이스와 별도로 참여할 수 있습니다. 투명 모드에서 지원되는 클러스터링은 라우팅 모드에서는 지원되지 않습니다. 다음 기능은 BVI에서도 지원되지 않습니다. 동적 라우팅 및 멀티캐스트 라우팅. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** • 디바이스 > 디바이스 관리 > 인터페이스 > 인터페이스 추가 > 브리지 그룹 인터페이스 지원되는 플랫폼: Firepower 2100 및 Firepower Threat Defense Virtual을 제외한 모든 플랫폼

30 장

Firepower Threat Defense 인라인 집합 및 패시브 인터페이스

IPS 전용 패시브 인터페이스, 패시브 ERSPAN 인터페이스 및 인라인 집합을 구성할 수 있습니다. IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 이런 인터페이스를 보호하는 개별 방화벽이 있고 방화벽 기능의 오버헤드를 원하지 않는 경우 IPS 전용 인터페이스를 구현합니다.

- IPS 인터페이스, 847 페이지
- 인라인 집합의 요구 사항 및 사전 요건, 850 페이지
- 인라인 집합 및 패시브 인터페이스 가이드라인, 851 페이지
- 패시브 인터페이스 구성, 852 페이지
- 인라인 집합 구성, 853 페이지
- Firepower Threat Defense 인라인 집합 및 패시브 인터페이스 기록, 857 페이지

IPS 인터페이스

이 섹션에서는 IPS 인터페이스에 대해 설명합니다.

IPS 인터페이스 유형

IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 이런 인터페이스를 보호하는 개별 방화벽이 있고 방화벽 기능의 오버헤드를 원하지 않는 경우 IPS 전용 인터페이스를 구현합니다.

참고 방화벽 모드는 일반 방화벽 인터페이스에만 영향을 주고 인라인 집합이나 패시브 인터페이스 등 IPS 전용 인터페이스에는 영향을 주지 않습니다. 두 개의 방화벽 모드 모두에서 IPS 전용 인터페이스를 사용할 수 있습니다.

IPS 전용 인터페이스는 다음과 같은 유형으로 구축할 수 있습니다.

- 필요에 따라 탭 모드가 가능한 인라인 집합 - 인라인 집합은 비활성 엔드포인트(bump in the wire)처럼 작동하며 두 인터페이스를 슬롯에 포함해 기존 네트워크에 바인딩합니다. 이 기능을 사용하면 인접한 네트워크 디바이스의 설정 없이 네트워크 환경에 FTD를 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

  탭 모드에서는 FTD가 인라인으로 구축되지만, 네트워크 트래픽 플로우는 방해받지 않습니다. 대신 FTD는 패킷을 분석할 수 있도록 각 패킷의 복사본을 만듭니다. 트리거되면 이런 유형의 규칙은 침입 이벤트를 생성하며, 침입 이벤트의 테이블 보기는 인라인 구축에서 트리거링 패킷이 삭제되었을 수도 있음을 표시합니다. 인라인으로 구축된 FTD에서 탭 모드를 사용하는 데는 몇 가지 이점이 있습니다. 예를 들어, 디바이스가 인라인 상태인 것처럼 FTD와 네트워크 간에 케이블링을 설정할 수 있으며 FTD가 생성하는 침입 이벤트의 종류를 분석할 수 있습니다. 결과를 기반으로 침입 정책을 수정할 수 있으며, 효율성 저하 없이 네트워크를 가장 잘 보호하는 삭제 규칙을 추가할 수 있습니다. FTD를 인라인으로 구축할 준비가 되면 FTD와 네트워크 간 케이블링을 다시 설정하지 않고도 탭 모드를 비활성화하고 의심스러운 트래픽을 삭제할 수 있습니다.

  참고 탭 모드는 트래픽에 따라 FTD 성능에 상당한 영향을 줍니다.

  참고 인라인 집합은 "투명 인라인 집합"으로 익숙할 수 있지만 인라인 인터페이스 유형은 투명 방화벽 모드 또는 방화벽 유형 인터페이스와는 관련이 없습니다.

- 패시브 또는 ERSPAN 패시브 - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용해 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 패시브 구축으로 FTD를 설정한 경우, FTD에서 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며, 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 캡슐화된 원격 스위치 포트 분석기(ERSPAN) 인터페이스는 여러 스위치를 통해 배포되는 소스 포트의 트래픽을 모니터링하고 GRE를 사용해 트래픽을 캡슐화합니다. ERSPAN 인터페이스는 FTD가 라우팅된 방화벽 모드에 있을 때만 허용됩니다.

인라인 집합용 하드웨어 바이패스 정보

Firepower 9300, 4100, 2100 시리즈(인라인 집합의 요구 사항 및 사전 요건, 850 페이지 참조)의 특정 인터페이스에서 하드웨어 바이패스 기능을 활성화할 수 있습니다. 하드웨어 바이패스는 트래픽이 정전 중에 1개의 인라인 인터페이스 쌍 사이에서 이동하도록 해 줍니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있습니다.

하드웨어 바이패스 트리거

하드웨어 바이패스 다음 시나리오에서 트리거될 수 있습니다.

- FTD 애플리케이션 충돌
- FTD 애플리케이션 재부팅
- 보안 모듈 재부팅
- 화력 섀시 충돌
- Firepower 섀시의 재부팅 또는 업그레이드
- 수동 트리거
- Firepower 섀시 전력 손실
- 보안 모듈 전력 손실

참고 하드웨어 우회는 계획되지 않은/예기치 않은 장애 시나리오를 위한 것이며, 계획된 소프트웨어 업그레이드 중에 자동으로 트리거되지 않습니다. 하드웨어 우회는 FTD 애플리케이션이 재부팅될 때 계획된 업그레이드 프로세스가 끝날 때만 사용됩니다.

하드웨어 우회 전환

정상 작동 상태에서 하드웨어 우회로 전환하거나 그 반대로 전환하는 경우에는 몇 초 동안 트래픽 전송이 중단될 수 있습니다. 구리 포트 자동 협상이나 파트너가 링크 결함 및 디바운스 타이밍을 처리하는 방식 등 광학 링크 파트너의 활동, STP(Spanning Tree Protocol) 컨버전스, 동적 라우팅 프로토콜 컨버전스 등 여러 가지 요인이 이 중단 시간에 영향을 줄 수 있습니다. 이 시간 동안에는 연결이 끊길 수 있습니다.

일반 작업으로 돌아온 이후 연결 미드스트림을 분석할 때 애플리케이션 식별 오류 때문에 연결 중단이 발생할 수도 있습니다.

Snort Fail Open vs.하드웨어 바이패스

탭 모드의 인라인 집합이 아닌 경우 Snort 프로세스가 바쁘거나 중단된 경우 검사 없이 트래픽을 삭제하거나 허용하려고 할 때 Snort Fail Open 옵션을 사용할 수 있습니다. Snort Fail Open는 하드웨어 바이패스을 지원하는 인터페이스만이 아니라 탭 모드가 아닌 모든 인라인 집합에서 지원합니다.

하드웨어 바이패스 기능을 사용하면 전원 완전 차단을 포함한 하드웨어 오류와 일부 한정 소프트웨어 오류가 발생한 경우에도 트래픽이 전송됩니다. Snort Fail Open을 트리거하는 소프트웨어 오류는 하드웨어 바이패스을 트리거하지 않습니다.

하드웨어 바이패스 **Status(**상태**)**

시스템에 전원이 있는 경우 우회 LED는 하드웨어 바이패스 상태를 나타냅니다. LED 설명에 대해서는 Firepower 섀시 하드웨어 설치 가이드를 참조하십시오.

인라인 집합의 요구 사항 및 사전 요건

모델 지원

FTD

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

하드웨어 바이패스 지원

FTD는 다음 모델에서 특정 네트워크 모듈의 인터페이스 쌍에 대해 하드웨어 바이패스를 지원합니다.

- Firepower 9300
- Firepower 4100 Series
- Firepower 2100 Series

이러한 모델에 대해 지원되는 하드웨어 바이패스 네트워크 모듈은 다음과 같습니다.

- Firepower 6 포트 1G SX FTW Network Module single-wide(FPR-NM-6X1SX-F)
- Firepower 6 포트 10G SR FTW Network Module single-wide(FPR-NM-6X10SR-F)
- Firepower 6 포트 10G LR FTW Network Module single-wide(FPR-NM-6X10LR-F)
- Firepower 2 포트 40G SR FTW Network Module single-wide(FPR-NM-2X40G-F)
- Firepower 8 포트 1G Copper FTW Network Module single-wide(FPR-NM-8X1G-F)

하드웨어 바이패스는 다음 포트 쌍만 사용할 수 있습니다.

- 1 및 2
- 3 및 4
- 5 및 6
- 7 및 8

인라인 집합 및 패시브 인터페이스 가이드라인

방화벽 모드

- ERSPAN 인터페이스는 디바이스가 라우팅된 방화벽 모드에 있을 때만 허용됩니다.

일반 지침

- 인라인 집합 및 패시브 인터페이스는 물리적 인터페이스 및 EtherChannel만 지원하며 이중 인터페이스, VLAN 등을 사용할 수 없습니다. Firepower 4100/9300 하위 인터페이스는 또한 IPS 전용 인터페이스를 지원하지 않습니다.
- 인라인 집합 및 패시브 인터페이스는 섀시 내 및 섀시 간 클러스터링에서 지원됩니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 인라인 집합을 사용할 때 FTD을 통과할 수 없습니다. BFD를 실행하는 FTD의 양쪽 측면에 두 개의 네이버가 있는 경우, FTD는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.
- 인라인 집합 및 패시브 인터페이스의 경우, FTD는 패킷에서 최대 2개의 802.1Q 헤더(Q-in-Q 지원이라고도 함)를 지원합니다. 단, 하나의 802.1Q 헤더만 지원하는 Firepower 4100/9300은 예외입니다. 참고**:** 방화벽 유형 인터페이스는 Q-in-Q를 지원하지 않으며, 802.1Q 헤더를 하나만 지원합니다.

하드웨어 바이패스 지침

- 하드웨어 바이패스 포트는 인라인 집합에만 지원됩니다.
- 하드웨어 바이패스 포트는 EtherChannel의 일부가 될 수 없습니다.
- 섀시 내 클러스터링에 지원됩니다. 포트는 섀시의 마지막 유닛에 오류가 발생하는 경우 하드웨어 바이패스 모드에 배치됩니다. 섀시 간 클러스터링은 지원 되지 않습니다.
- 클러스터의 모든 유닛에 오류가 발생하는 경우 하드웨어 바이패스은 최종 유닛에서 트리거되고 트래픽은 계속 전달됩니다. 유닛이 복구되면 하드웨어 바이패스은 스탠바이 모드로 돌아갑니다. 그러나 애플리케이션 트래픽과 일치하는 규칙을 사용하면 이 연결이 삭제되어 다시 설정해야 할 수 있습니다. 클러스터 유닛에 상태 정보가 보존되지 않으므로 연결이 삭제되고 유닛은 허용된 애플리케이션에 속한 트래픽을 식별하지 못합니다. 트래픽 삭제를 방지하려면 애플리케이션 기반 규칙 대신 구축에 적합한 경우 포트 기반 규칙을 사용합니다.
- 하드웨어 바이패스 는 고가용성 모드에서 지원되지 않습니다.

IPS 인터페이스에서 지원되지 않는 방화벽 기능

- DHCP 서버
- DHCP 릴레이

- DHCP 클라이언트
- TCP 인터셉트
- 라우팅
- NAT
- VPN
- 애플리케이션 검사
- QoS
- NetFlow
- VXLAN

패시브 인터페이스 구성

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 인터페이스를 활성화합니다. 기본적으로 인터페이스는 비활성화되어 있습니다.
- 인터페이스 모드를 패시브 또는 ERSPAN으로 설정합니다. ERSPAN 인터페이스의 경우 ERSPAN 파라미터와 IP 주소를 설정할 수 있습니다.
- MTU를 변경합니다. 기본적으로 MTU는 1500 바이트로 설정됩니다. MTU에 대한 자세한 내용은 MTU 정보, 833 페이지을 참조하십시오.
- 특정 속도 및 양방향 설정(제공되는 경우) 기본적으로 속도 및 양방향은 자동으로 설정되어 있습니다.

참고 FXOS 섀시의 Firepower Threat Defense의 경우 Firepower 4100/9300 섀시에서 기본 인터페이스 설정을 구성합니다. 자세한 내용은 실제 인터페이스 구성, 757 페이지를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

단계 **3** 모드 드롭다운 목록에서 패시브 또는 **ERSPAN**을 선택합니다.

단계 **4** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **5** **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

단계 **6** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

단계 **7** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **8** (선택 사항) 일반에서 64와 9198바이트 사이의 **MTU**를 설정하십시오. Firepower Threat Defense Virtual과 FXOS 섀시의 Firepower Threat Defense의 경우 9000바이트가 최대입니다.

기본값은 1500바이트입니다.

단계 **9** ERSPAN 인터페이스에 대한 다음 파라미터를 설정합니다.

- 플로우 **ID** - ERSPAN 트래픽을 식별하기 위해 소스 및 대상 세션에서 사용하는 ID를 구성하며 그 값은 1에서 1023 사이입니다. 이 ID 값은 ERSPAN 대상 세션에도 입력해야 합니다.
- 소스 **IP** - ERSPAN 트래픽 소스로 사용되는 IP 주소를 구성합니다.

단계 **10** ERSPAN 인터페이스의 경우 **IPv4**에서 IPv4 주소 및 마스크를 설정합니다.

단계 **11** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.

정확한 속도 및 듀플렉스 옵션은 하드웨어에 따라 달라집니다.

- **Duplex(**듀플렉스**)** - **Full(**풀 듀플렉스**)**, **Half(**하프 듀플렉스**)** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.
- **Speed(**속도**)** - **10**, **100**, **1000** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.

단계 **12** **OK(**확인**)**를 클릭합니다.

단계 **13** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

인라인 집합 구성

이 섹션에서는 인라인 집합에 추가할 수 있는 물리적 인터페이스 2개를 활성화하고 이름을 지정합니다. 원하는 경우 지원되는 인터페이스 쌍에 대해 하드웨어 바이패스를 활성화할 수도 있습니다.

참고 FXOS 섀시의 Firepower Threat Defense의 경우 Firepower 4100/9300 섀시에서 기본 인터페이스 설정을 구성합니다. 자세한 내용은 실제 인터페이스 구성, 757 페이지를 참조하십시오.

시작하기 전에

- Firepower Threat Defense 인라인 쌍 인터페이스에 연결하는 STP 활성화 스위치에 대해 STP PortFast를 구성하는 것이 좋습니다. 이 설정은 하드웨어 바이패스 구성에 특히 유용하며, 우회 시간을 줄일 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스에 대한 수정( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 수정( )을 클릭합니다.

단계 **3** **Mode(**모드**)** 드롭다운 목록에서 **None(**없음**)**을 선택합니다.

인라인 집합에 이 인터페이스를 추가하고 나면 이 필드에 모드로 Inline(인라인)이 표시됩니다.

단계 **4** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **5** **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

보안 구역은 아직 설정하지 마십시오. 이 절차 후반에서 인라인 모음을 생성한 다음에 설정해야 합니다.

단계 **6** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **7** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.

정확한 속도 및 듀플렉스 옵션은 하드웨어에 따라 달라집니다.

- **Duplex(**듀플렉스**)** - **Full(**풀 듀플렉스**)**, **Half(**하프 듀플렉스**)** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.
- **Speed(**속도**)** - **10**, **100**, **1000** 또는 **Auto(**자동**)**를 선택합니다. 기본값은 Auto(자동)입니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

이 인터페이스에 대한 다른 설정은 지정하지 마십시오.

단계 **9** 인라인 집합에 추가할 두 번째 인터페이스에 대해 수정( )을 클릭합니다.

단계 **10** 첫 번째 인터페이스에 대한 설정을 구성합니다.

단계 **11** **Inline Sets(**인라인 집합**)**를 클릭합니다.

단계 **12** **Add Inline Set(**인라인 집합 추가**)**를 클릭합니다.
General(일반**)**이 선택된 상태로 **Add Inline Set(**인라인 집합 추가**)** 대화 상자가 나타납니다.

단계 **13** **Name(**이름**)** 필드에 집합의 이름을 입력합니다.

단계 **14** (선택 사항) 점보 프레임을 활성화하려면 **MTU**를 변경합니다.

인라인 집합의 경우, MTU 설정이 사용되지 않습니다. 그러나 점보 프레임 설정은 인라인 집합과 관련이 있으며 점보 프레임은 최대 9000바이트까지 패킷을 수신하도록 인라인 인터페이스를 활성화합니다. 점보 프레임을 활성화하려면 1500바이트 이상인 디바이스에서 모든 인터페이스의 MTU를 설정해야 합니다.

단계 **15** (선택 사항) **Bypass(**바이패스**)** 모드의 경우 다음 옵션 중 하나를 선택합니다.

- **Disabled(**비활성화됨**)** - 하드웨어 바이패스가 지원되는 인터페이스에 대해 하드웨어 바이패스를 비활성화하거나, 하드웨어 바이패스가 지원되지 않는 인터페이스를 사용합니다.
- **Standby(**스탠바이**)** - 지원되는 인터페이스에서 하드웨어 바이패스를 스탠바이 상태로 설정합니다. 하드웨어 바이패스 인터페이스 쌍만 표시됩니다. 스탠바이 상태에서 인터페이스는 트리거 이벤트가 발생할 때까지 정상 작동 상태로 유지됩니다.
- **Bypass-Force(**바이패스-강제**)** - 인터페이스 쌍이 바이패스 상태가 되도록 수동으로 강제 지정합니다. **Inline Sets(**인라인 집합**)**에서 Bypass-Force(바이패스-강제) 모드인 모든 인터페이스 쌍에 대해 **Yes(**예**)**가 표시됩니다.

단계 **16** **Available Interfaces Pairs(**사용 가능한 인터페이스 쌍**)** 영역에서 쌍을 클릭한 다음 **Add(**추가**)**를 클릭하여 해당 쌍을 **Selected Interface Pair(**선택한 인터페이스 쌍**)** 영역으로 이동합니다.

모드가 None(없음)으로 설정된 명명된 인터페이스와 활성화된 인터페이스 간에 가능한 모든 쌍이 이 영역에 표시됩니다.

단계 **17** (선택 사항) **Advanced(**고급**)**를 클릭하여 다음의 선택적 파라미터를 설정합니다.

- **Tap Mode(**탭 모드**)** - 인라인 탭 모드로 설정합니다.

  동일한 인라인 집합에서 이 옵션 및 Strict TCP Enforcement를 활성화할 수 없습니다.

  참고 탭 모드는 트래픽에 따라 FTD 성능에 상당한 영향을 줍니다.

- **Propagate Link State(**링크 상태 전파**)** - 링크 상태 전파를 구성합니다.

  링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 중단될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다. 장애가 발생한 인터페이스가 복원되면 두 번째 인터페이스도 자동으로 활성화됩니다. 다시 말해, 한 인터페이스의 링크 상태가 변경되면 디바이스가 변경사항을 감지하고 다른 인터페이스의 링크 상태도 일치하도록 업데이트합니다. 디바이스가 링크 상태 변경사항을 전파하려면 최대 4초가 걸립니다. 링크 상태 전파는 라우터가 장애 상태인 네트워크 디바이스를 우회해 트래픽을 자동으로 다시 라우팅하도록 구성된 탄력적인 네트워크 환경에서 특히 유용합니다.

- **Strict TCP Enforcement(**엄격한 **TCP** 시행**)** - TCP 보안을 극대화하기 위해 엄격한 시행을 활성화할 수 있습니다. 그러면 3방향 핸드셰이크가 완료되지 않은 연결이 차단됩니다.

  엄격한 시행은 다음 항목도 차단합니다.

  - 3방향 핸드셰이크가 완료되지 않은 연결의 비 SYN TCP 패킷
  - TCP 연결의 Responder가 SYN-ACK를 보내기 전에 이니시에이터가 보낸 비 SYN/RST 패킷
  - TCP 연결에서 SYN 이후/세션이 설정되기 전에 Responder가 보낸 비 SYN-ACK/RST 패킷

- 설정된 TCP 연결에서 이니시에이터 또는 Responder가 보낸 SYN 패킷

- **Snort Fail-Open** - Snort 프로세스가 사용 중이거나 중단될 때 새 트래픽과 기존 트래픽을 검사 없이 통과할지(활성화됨) 아니면 삭제할지(비활성화됨)에 따라 **Busy(**사용 중**)** 및 **Down(**중단**)** 옵션 중 하나 또는 둘 다를 활성화하거나 비활성화합니다.

  기본적으로 Snort 프로세스가 중단되면 트래픽이 검사 없이 통과되고, Snort 프로세스가 사용 중이면 트래픽이 삭제됩니다.

  Snort 프로세스의 상태별 속성은 다음과 같습니다.

  - Busy(사용 중) - 디바이스가 처리할 수 있는 양보다 트래픽이 더 많아서 트래픽 버퍼가 꽉 차거나 다른 소프트웨어 리소스 문제가 있어서 Snort 프로세스가 트래픽을 충분히 빠르게 처리할 수 없습니다.
  - Down(중단) - Snort 프로세스를 재시작해야 하는 컨피그레이션을 구축했으므로 프로세스가 재시작됩니다. 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지의 내용을 참조하십시오.

    Snort 프로세스는 중단되었다가 다시 작동할 때 새 연결을 검사합니다. 오탐(False Positive) 및 미탐(False Negative)을 방지하기 위해 Snort 프로세스는 인라인, 라우팅 또는 Transparent 인터페이스의 기존 연결을 검사하지 않습니다. 프로세스가 중단된 동안 초기 세션 정보가 손실되었을 수 있기 때문입니다.

참고 Snort가 열리지 않으면 Snort 프로세스를 사용하는 기능이 작동하지 않습니다. 이러한 기능에는 애플리케이션 제어 및 심층 검사가 포함됩니다. 시스템은 단순하며 쉽게 확인 가능한 전송 및 네트워크 계층 특성을 사용하여 기본적인 액세스 제어만 수행합니다.

단계 **18** **Interfaces(**인터페이스**)**를 클릭합니다.

단계 **19** 구성원 인터페이스 중 하나에 대한 아이콘(수정( ))을 클릭합니다.

단계 **20** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

인라인 집합에 인터페이스를 추가한 후에만 영역을 설정할 수 있습니다. 인라인 집합에 영역을 추가하면 모드가 Inline(인라인)으로 구성되며, 인라인 유형 보안 영역을 선택할 수 있습니다.

단계 **21** **OK(**확인**)**를 클릭합니다.

단계 **22** 두 번째 인터페이스의 보안 영역을 설정합니다.

단계 **23** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Firepower Threat Defense 인라인 집합 및 패시브 인터페이스 기록

기능	버전	세부 사항
FTD 작동 링크 상태와 Firepower 4100/9300의 물리적 링크 상태 간 동기화	6.7	이제 Firepower 4100/9300 섀시는 FTD 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. FTD 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 FTD에서 동기화하지 않으면 FTD 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 FTD 종료를 시작한 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 인라인 집합의 경우 FTD에서 트래픽을 처리하기 전에 외부 라우터가 FTD로 트래픽 전송을 시작할 수 있으므로 이러한 상태 불일치로 인해 패킷이 삭제될 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다. 참고 이 기능은 클러스터링, 컨테이너 인스턴스 또는 Radware vDP 데코레이터가 포함된 FTD에는 지원되지 않습니다. ASA에서도 지원되지 않습니다. 신규/수정된 Firepower Chassis Manager 화면: **Logical Devices(**논리적 디바이스**) > Enable Link State(**링크 상태 활성화**)** 신규/수정된 FXOS 명령: **set link-state-sync enabled**, **show interface expand detail** 지원되는 플랫폼: Firepower 4100/9300

기능	버전	세부 사항
지원되는 네트워크 모듈용 Firepower 2100에 대한 하드웨어 우회 지원	6.3.0	Firepower 2100은 이제 하드웨어 우회 네트워크를 사용할 때 하드웨어 우회 기능을 지원합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** 지원되는 플랫폼: Firepower 2100
FTD 인라인 집합에서 EtherChannel 지원	6.2.0	이제 FTD 인라인 집합에서 EtherChannel을 사용할 수 있습니다. 지원되는 플랫폼: Firepower 4100/9300, Firepower 2100(6.2.1 이상)
지원되는 네트워크 모듈용 Firepower 4100/9300에 대한 하드웨어 우회 지원	6.1.0	Hardware Bypass는 정전 중에 트래픽이 인라인 인터페이스 쌍 사이에서 계속 흐르도록 합니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** 지원되는 플랫폼: Firepower 4100/9300
인라인 집합 링크 상태 전파 지원 FTD	6.1.0	FTD 애플리케이션에서 인라인 집합을 구성하고 링크 상태 전파를 활성화하면 FTD에서 FXOS 섀시로 인라인 집합 멤버십을 전송합니다. 링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 중단될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다. 신규/수정된 FXOS 명령: **show fault |grep link-down**, **show interface detail** 지원되는 플랫폼: Firepower 4100/9300, Firepower 2100(6.2.1 이상)

31 장

Threat Defense용 DHCP 및 DDNS 서비스

다음 주제는 DHCP 및 DDNS 서비스와 Threat Defense 디바이스에서 구성하는 방법을 설명합니다.

- DHCP 및 DDNS 서비스 정보, 859 페이지
- DHCP 및 DDNS 요구 사항 및 사전 요건, 860 페이지
- DHCP 및 DDNS 서비스에 대한 지침, 861 페이지
- DHCP 서버 구성, 862 페이지
- DHCP 릴레이 에이전트 구성, 864 페이지
- 동적 DNS 구성, 865 페이지

DHCP 및 DDNS 서비스 정보

다음 주제는 DHCP 서버, DHCP 릴레이 에이전트 및 DDNS 업데이트를 설명합니다.

DHCPv4 서버 정보

DHCP는 IP 주소와 같은 네트워크 컨피그레이션 매개변수를 DHCP 클라이언트에 제공합니다. Firepower Threat Defense 디바이스은 Firepower Threat Defense 디바이스 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버를 제공할 수 있습니다. DHCP 서버는 DHCP 클라이언트에 직접 네트워크 컨피그레이션 매개변수를 제공합니다.

IPv4 DHCP 클라이언트는 서버와 연결하는 데 멀티캐스트 주소가 아닌 브로드캐스트를 사용합니다. DHCP 클라이언트는 UDP 포트 68에서 메시지를 수신합니다. DHCP 서버는 UDP 포트 67에서 메시지를 수신합니다.

하지만 Ipv6의 DHCP 서버는 지원되지 않습니다. 그러나 IPv6 트래픽에 대한 DHCP 릴레이를 활성화할 수 있습니다.

DHCP 옵션

DHCP는 TCP/IP 네트워크에서 호스트할 구성 정보를 전달하기 위한 프레임워크를 제공합니다. 구성 파라미터는 DHCP 메시지의 Options(옵션) 필드에 저장된 태깅 항목으로 전달되며, 데이터는 옵션이라고도 합니다. 벤더 정보는 Options(옵션)에도 저장되어 있으며 모든 벤더 정보는 확장하여 DHCP 옵션으로 사용될 수 있습니다.

Cisco IP Phone은 TFTP 서버에서 구성을 다운로드합니다. Cisco IP Phone이 시작할 때 IP 주소 및 TFTP 서버 IP 주소 모두 미리 구성되지 않았다면 이 정보를 얻고자 DHCP 서버에 옵션 150 또는 66으로 요청을 보냅니다.

- DHCP 옵션 150은 일련의 TFTP 서버의 IP 주소를 제공합니다.
- DHCP 옵션 66은 단일 TFTP 서버의 IP 주소 또는 호스트 이름을 제공합니다.
- DHCP 옵션 3은 기본 경로를 설정합니다.

하나의 요청에서 옵션 150과 66을 모두 포함할 수 있습니다. 이 경우, 두 옵션의 값이 이미 ASA에 구성되어 있다면 ASA DHCP 서버에서는 두 옵션을 모두 포함하여 응답합니다.

DHCP 클라이언트에 DNS, WINS 및 도메인 이름 파라미터를 제공하기 위해 고급 DHCP 옵션을 사용할 수 있습니다. DHCP 옵션 15는 DNS 도메인 접미사에 사용됩니다. 이러한 값을 얻거나 수동으로 정의하기 위해 DHCP 자동 구성 설정을 사용할 수도 있습니다. 이 정보를 정의하는 데 둘 이상의 방법을 사용할 경우 다음 순서로 DHCP 클라이언트에 전달됩니다.

1. 직접 구성한 설정
2. 고급 DHCP 옵션 설정
3. DHCP 자동 컨피그레이션 설정

이를테면 DHCP 클라이언트에서 수신할 도메인 이름을 직접 정의한 다음 DHCP 자동 컨피그레이션을 활성화할 수 있습니다. DHCP 자동 컨피그레이션에서 DNS 및 WINS 서버와 함께 도메인을 검색하더라도, 수동으로 정의된 도메인 이름이 검색된 DNS 및 WINS 서버 이름과 함께 DHCP 클라이언트에 전달됩니다. DHCP 자동 컨피그레이션 프로세스에 의해 검색된 도메인 이름보다 수동 정의된 도메인 이름이 우선하기 때문입니다.

DHCP 릴레이 에이전트 소개

인터페이스에서 수신한 DHCP 요청을 하나 이상의 DHCP 서버에 전달하도록 DHCP 릴레이 에이전트를 구성할 수 있습니다. DHCP 클라이언트는 최초 DHCPDISCOVER 메시지를 보내는 데 UDP 브로드캐스트를 사용합니다. 연결된 네트워크에 대한 정보가 없기 때문입니다. 클라이언트가 연결된 세그먼트에 서버가 없을 경우, Firepower Threat Defense 디바이스는 (브로드캐스트 트래픽을 전달하지 않으므로) 대개는 UDP 브로드캐스트를 전달하지 않습니다. DHCP 릴레이 에이전트를 사용하면 DHCP 요청을 다른 인터페이스의 DHCP 서버로 전송하는 브로드캐스트를 수신하는 Firepower Threat Defense 디바이스의 인터페이스를 구성할 수 있습니다.

DHCP 및 DDNS 요구 사항 및 사전 요건

모델 지원

FTD

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

DHCP 및 DDNS 서비스에 대한 지침

이 섹션에는 DHCP 및 DDNS 서비스를 구성하기 전에 확인해야 하는 제한사항 및 지침이 포함되어 있습니다.

방화벽 모드

- DHCP 릴레이는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 지원되지 않습니다.
- DHCP 서버는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드에서 지원됩니다. 라우팅 모드에서 DHCP 서버는 브리지 그룹 멤버 인터페이스가 아닌 BVI 인터페이스에서 지원됩니다. DHCP 서버가 작동하려면 BVI에 이름이 있어야 합니다.
- DDNS는 BVI 또는 브리지 그룹 멤버 인터페이스의 투명 방화벽 모드 또는 라우팅 모드에서 지원되지 않습니다.

IPv6

DHCP 서버에 대해 IPv6 DHCP 릴레이에 대한 IPv6가 지원됩니다.

DHCPv4 서버

- 최대 가용 DHCP 풀은 주소 256개입니다.
- 각 인터페이스에서 DHCP 서버를 1개만 구성할 수 있습니다. 각 인터페이스는 자체 주소 풀을 두고 사용할 수 있습니다. 그러나 DNS 서버, 도메인 이름, 옵션, ping 시간 초과, WINS 서버와 같은 나머지 DHCP 설정은 전역으로 구성되며 모든 인터페이스에서 DHCP 서버에 의해 사용됩니다.
- 해당 인터페이스에서 DHCP 서버도 활성화된 경우, 인터페이스를 DHCP 클라이언트로 설정할 수 없습니다. 고정 IP 주소를 사용해야 합니다.
- 서로 다른 인터페이스에서 활성화하려 하더라도 동일한 디바이스에서 DHCP 서버와 DHCP 릴레이를 모두 설정할 수 없습니다. 단 하나의 서비스 유형만 구성 가능합니다.
- Firepower Threat Defense 디바이스 는 QIP DHCP 서버를 DHCP 프록시 서비스와 함께 사용하는 것을 지원하지 않습니다.
- DHCP 서버는 BOOTP 요청을 지원하지 않습니다.

DHCP 릴레이

- 전역 서버와 인터페이스 특정 서버를 포함하여 최대 10개의 DHCPv4 릴레이 서버를 구성할 수 있으며, 각 인터페이스에는 최대 4개의 서버가 가능합니다.
- 단일 모드 및 각 상황를 구성할 수 있습니다. IPv6 인터페이스 특정 서버는 지원되지 않습니다.
- 서로 다른 인터페이스에서 활성화하려 하더라도 동일한 디바이스에서 DHCP 서버와 DHCP 릴레이를 모두 설정할 수 없습니다. 단 하나의 서비스 유형만 구성 가능합니다.
- DHCP 릴레이 서비스는 BVI 또는 브리지 그룹 멤버 인터페이스 또는 라우팅 모드에서 사용할 수 없습니다. 그러나 액세스 목록을 사용하는 방법으로 DHCP 트래픽을 허용할 수 있습니다. DHCP 요청과 응답이 Firepower Threat Defense 디바이스를 지날 수 있게 하려면 2개의 액세스 규칙을 구성해야 합니다. 하나는 내부 인터페이스에서 외부(UDP 대상 포트 67)로 보내는 DHCP 요청을 허용하는 것이고 다른 하나는 반대 방향(UDP 대상 포트 68)으로 서버의 응답을 허용하는 것입니다.
- IPv4에서는 클라이언트가 Firepower Threat Defense 디바이스에 직접 연결되어야 하며, 다른 릴레이 에이전트 또는 라우터를 통해 요청을 보낼 수 없습니다. IPv6에서는 Firepower Threat Defense 디바이스가 다른 릴레이 서버에서 보낸 패킷을 지원합니다.
- DHCP 클라이언트는 Firepower Threat Defense 디바이스에서 요청을 릴레이하는 DHCP 서버와 다른 인터페이스에 있어야 합니다.
- 트래픽 영역의 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.
- DHCP 릴레이는 VTI(Virtual Tunnel Interface)에서 지원되지 않습니다.

DHCP 서버 구성

DHCP 서버를 설정하려면 다음 단계를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **DHCP** > **DHCP** 서버를 선택합니다.

단계 **3** 다음 DHCP 서버 옵션을 구성합니다.

- **Ping** 시간 초과 - DHCP Ping 시도 시 시간 초과까지 Firepower Threat Defense 디바이스가 대기하는 시간의 양으로 밀리초 단위입니다. 유효한 값의 범위는 10밀리초 ~ 10000밀리초입니다. 기본값은 50밀리초입니다.

  주소 충돌을 방지하고자 Firepower Threat Defense 디바이스는 DHCP 클라이언트에 주소를 지정하기 전에 주소에 2개의 ICMP ping 패킷을 보냅니다.

- 임대 길이 - 클라이언트가 할당받은 IP 주소를 임대 만료 전까지 사용할 수 있는 시간으로 초 단위입니다. 유효한 값은 300초 ~ 9000초입니다. 기본값은 3600초(1시간)입니다.

- (라우팅된 모드) 자동 설정 - Firepower Threat Defense 디바이스에서 DHCP 자동 설정을 활성화합니다. 자동 컨피그레이션은 DHCP 서버가 지정된 인터페이스에서 실행 중인 어떤 DHCP 클라이언트로부터 얻은 DNS 서버, 도메인 이름, WINS 서버 정보를 DHCP 클라이언트에 제공할 수 있게 합니다. 그렇지 않은 경우 자동 설정을 비활성화하고 4단계에서 사용자가 직접 값을 추가할 수 있습니다.
- (라우팅된 모드) 인터페이스 - 자동 설정에 사용할 인터페이스를 지정합니다. 가상 라우팅 기능이 있는 디바이스의 경우, 이 인터페이스는 전역 가상 라우터 인터페이스만 될 수 있습니다.

단계 **4** 자동 구성된 설정을 오버라이드하려면 다음을 수행합니다.

- 인터페이스의 도메인 이름을 입력합니다. 장치가 Your_Company 도메인 내에 있을 수 있습니다.
- 드롭다운 목록에서 인터페이스에 구성된 DNS 서버(기본, 보조)를 선택합니다. 새 DNS 서버를 추가하려면 네트워크 개체 생성, 571 페이지의 내용을 참조하십시오.
- 드롭다운 목록에서 인터페이스에 구성된 WINS 서버(기본, 보조)를 선택합니다. 새 WINS 서버를 추가 하려면 네트워크 개체 생성, 571 페이지의 내용을 참조하십시오.

단계 **5** **Server(**서버**)**를 선택하고 **Add(**추가**)**를 클릭하여 탭에서 다음 옵션을 구성합니다.

- 인터페이스 - 드롭다운 목록에서 인터페이스를 선택합니다. 투명 모드에서 명명된 브리지 그룹 멤버 인터페이스를 지정합니다. 라우팅 모드에서 명명된 라우팅 인터페이스 또는 명명된 BVI를 지정합니다. 브리지 그룹 멤버 인터페이스는 지정하지 마십시오. 각 BVI의 브리지 그룹 구성원 인터페이스가 DHCP 서버에서 작동하려면 이름이 있어야 합니다.
- 주소 풀 - DHCP 서버에서 사용되는 최소 및 최대 IP 주소 범위입니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소는 포함할 수 없습니다.
- **DHCP** 서버 활성화 - 선택한 인터페이스에서 DHCP 서버를 활성화합니다.

단계 **6** **OK**를 클릭하여 DHCP 서버 설정을 저장합니다.

단계 **7** (선택 사항) **Advanced(**고급**)**를 선택하고 **Add(**추가**)**를 클릭하여 옵션이 DHCP 클라이언트에 반환하려는 정보 유형을 지정하십시오.

- 옵션 코드 - Firepower Threat Defense 디바이스는 정보 전송을 위해 RFC 2132, RFC 2563, RFC 5510의 DHCP 옵션을 지원합니다. 1, 12, 50–54, 58–59, 61, 67, 82를 제외하고 모든 DHCP 옵션(1 ~ 255)이 지원됩니다. DHCP 옵션 코드에 대한 자세한 내용은 DHCPv4 서버 정보, 859 페이지을 참조하십시오.

  참고 Firepower Threat Defense 디바이스는 사용자가 제공하는 옵션의 유형 및 값이 RFC 2132에 정의된 옵션 코드의 예상 유형 및 값과 일치하는지 확인하지 않습니다. 옵션 코드와 그 유형 및 예상 값에 대한 자세한 내용은 RFC 2132를 참조하십시오.

- 유형 - DHCP 옵션 유형입니다. 사용 가능한 옵션에는 **IP**, **ASCII**및 **16** 진수가 있습니다. IP를 선택한 경우에 IP 주소 필드에 IP 주소를 추가해야 합니다. ASCII를 선택한 경우에 ASCII 필드에 ASCII 값을 추가해야 합니다. 16 진수를 선택한 경우 HEX 필드에 16 진수 값을 추가해야 합니다.

- **IP** 주소 **1** 및 **IP** 주소 **2** - 이 옵션 코드로 반환될 IP 주소입니다. 새 IP 주소를 추가하려면 네트워크 개체 생성, 571 페이지의 내용을 참조하십시오.
- **ASCII** - DHCP 클라이언트에 반환될 ASCII 값입니다. 이 문자열은 공백을 포함할 수 없습니다.
- **16** 진수 - DHCP 클라이언트에 반환될 16 진수 값입니다. 문자열은 짝수여야 하며 공백이 없어야 합니다. 0x 접두사를 사용할 필요 없습니다.

단계 **8** **OK**를 클릭하여 옵션 코드 설정을 저장합니다.

단계 **9** 변경 사항을 저장하려면 DHCP 페이지에서 저장을 클릭합니다.

DHCP 릴레이 에이전트 구성

인터페이스에서 수신한 DHCP 요청을 하나 이상의 DHCP 서버에 전달하도록 DHCP 릴레이 에이전트를 구성할 수 있습니다. DHCP 클라이언트는 최초 DHCPDISCOVER 메시지를 보내는 데 UDP 브로드캐스트를 사용합니다. 연결된 네트워크에 대한 정보가 없기 때문입니다. 클라이언트가 연결된 세그먼트에 서버가 없을 경우, Firepower Threat Defense 디바이스는 (브로드캐스트 트래픽을 전달하지 않으므로) 대개는 UDP 브로드캐스트를 전달하지 않습니다.

브로드캐스트를 수신하는 Firepower Threat Defense 디바이스의 인터페이스를 구성하여 DHCP 요청을 다른 인터페이스의 DHCP 서버에 전달하게 함으로써 이러한 문제를 해결할 수 있습니다.

참고 투명 방화벽 모드에서에서는 DHCP 릴레이가 지원되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **DHCP** > **DHCP** 릴레이를 선택합니다.

단계 **3** 시간 초과 필드에 Firepower Threat Defense 디바이스가 DHCP 릴레이 에이전트가 시간 초과될 때까지 대기하는 시간을 초 단위로 입력합니다. 유효한 값의 범위는 1초 ~ 3600초입니다. 기본값은 60초입니다.

시간 초과는 로컬 DHCP 릴레이 에이전트를 통한 주소 협상에 필요합니다.

단계 **4** **DHCP Relay Agent(DHCP** 릴레이 에이전트**)**에서 **Add(**추가**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

- 인터페이스 - DHCP 클라이언트에 연결된 인터페이스입니다.
- **IPv4** 릴레이 활성화 - 이 인터페이스에서 IPv4 DHCP 릴레이를 활성화합니다.
- 경로 설정 - (IPv4의 경우) 서버에서 전송한 DHCP 메시지 내의 기본 게이트웨이 주소를 초기 DHCP 요청을 릴레이한 DHCP 클라이언트와 가장 가까운 Firepower Threat Defense 디바이스 인

터페이스의 주소로 변경합니다. 이 작업을 수행하면 클라이언트는 DHCP 서버가 다른 라우터를 지정하더라도 Firepower Threat Defense 디바이스를 가리키는 기본 경로를 설정할 수 있습니다. 패킷에 기본 라우터 옵션이 없는 경우 Firepower Threat Defense 디바이스는 인터페이스 주소를 포함하는 것을 추가합니다.

- **IPv6** 릴레이 활성화 - 이 인터페이스에서 IPv6 DHCP 릴레이를 활성화합니다.

단계 **5** DHCP 릴레이 에이전트 변경 사항을 저장하려면 **OK**를 클릭합니다.

단계 **6** **DHCP Servers(DHCP** 서버**)**에서 **Add(**추가**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

동일한 서버에 속해 있는 경우에도 IPv4 및 IPv6 서버 주소를 개별 항목으로 추가합니다.

- 서버 - DHCP 서버의 IP 주소입니다. 드롭다운 목록에서 IP 주소를 선택합니다. 새로 추가하려는 경우 를 참조하십시오. 네트워크 개체 생성, 571 페이지
- 인터페이스 - 드롭다운 목록에서 지정된 DHCP 서버가 연결된 인터페이스입니다. DHCP 릴레이 에이전트 및 DHCP 서버는 동일한 인터페이스에 구성될 수 없습니다.

단계 **7** DHCP 서버 변경 사항을 저장하려면 **OK**를 클릭합니다.

단계 **8** 변경 사항을 저장하려면 DHCP 페이지에서 저장을 클릭합니다.

동적 DNS 구성

인터페이스에서 DHCP IP 주소 지정을 사용하는 경우, DHCP 리스가 갱신될 때 할당된 IP 주소가 변경될 수 있습니다. FQDN(Fully Qualified Domain Name)을 사용하여 인터페이스에 연결해야 하는 경우, IP 주소를 변경하면 DNS 서버 리소스 레코드(RR)가 오래 될 수 있습니다. DDNS(Dynamic DNS)는 IP 주소 또는 호스트네임이 변경될 때마다 DNS RR을 업데이트하는 메커니즘을 제공합니다. 고정 또는 PPPoE IP 주소 지정에 DDNS를 사용할 수도 있습니다.

DDNS는 DNS 서버에서 다음 RR을 업데이트합니다. A RR은 이름-IP 주소 매핑을 포함하고 PTR RR은 주소를 이름에 매핑합니다.

FTD는 다음 DDNS 업데이트 방법을 지원합니다.

- 표준 DDNS - 표준 DDNS 업데이트 방법은 RFC 2136에 의해 정의됩니다.

  이 방법을 사용하는 경우, FTD 및 DHCP 서버는 DNS 요청을 사용하여 DNS RR을 업데이트합니다. FTD 또는 DHCP 서버는 호스트네임에 대한 정보를 얻기 위해 DNS 요청을 로컬 DNS 서버로 전송하고, 응답에 따라 RR을 소유한 기본 DNS 서버를 결정합니다. 그런 다음 FTD 또는 DHCP 서버는 기본 DNS 서버로 직접 업데이트 요청을 보냅니다. 다음과 같은 일반적인 시나리오를 참조하십시오.

  - FTD가 A RR을 업데이트하고, DHCP 서버가 PTR RR을 업데이트합니다.

    일반적으로 FTD는 A RR을 "소유"하고 DHCP 서버는 PTR RR을 "소유"하므로 두 엔티티 모두 업데이트를 별도로 요청해야 합니다. IP 주소 또는 호스트네임이 변경되면 FTD는 DHCP

요청(FQDN 옵션 포함)을 DHCP 서버에 전송하여 PTR RR 업데이트를 요청해야 함을 알립니다.

- DHCP 서버가 A RR과 PTR RR을 모두 업데이트합니다.

  FTD에 A RR을 업데이트 할 권한이 없는 경우, 이 시나리오를 사용합니다. IP 주소 또는 호스트네임이 변경되면 FTD는 DHCP 요청(FQDN 옵션 포함)을 DHCP 서버에 전송하여 A RR 및 PTR RR 업데이트를 요청해야 함을 알립니다.

보안 요구 사항과 기본 DNS 서버의 요구 사항에 따라 다른 소유권을 설정할 수 있습니다. 예를 들어, 고정 주소의 경우, FTD는 두 레코드의 업데이트를 모두 소유해야 합니다.

- 웹 - 웹 업데이트 방법은 DynDNS 원격 API 사양(https://help.dyn.com/remote-access-api/)을 활용합니다.

  이 방법을 사용하면 IP 주소 또는 호스트네임이 변경될 때 FTD에서 계정이 있는 DNS 제공자에게 직접 HTTP 요청을 보냅니다.

DDNS 페이지는 DDNS와 관련된 DHCP 서버 설정도 지원합니다.

참고 DDNS는 브리지 그룹 멤버 인터페이스 또는 BVI에서 지원되지 않습니다.

시작하기 전에

- **Objects(**개체**)** > **Object Management(**개체 관리**)** > **DNS Server Group(DNS** 서버 그룹**)**에서 DNS 서버 그룹을 설정한 다음 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **DNS**에서 인터페이스에 대해 그룹을 활성화합니다. DNS 구성, 1425 페이지의 내용을 참조하십시오.
- 디바이스 호스트네임을 설정합니다. FTD 초기 설정을 수행할 때 또는 **configure network hostname** 명령을 사용하여 호스트네임을 설정할 수 있습니다. 인터페이스당 호스트네임을 지정하지 않으면 디바이스 호스트네임이 사용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **DHCP** > **DDNS**를 선택합니다.

단계 **3** 표준 DDNS 방법: FTD에서 DNS 요청을 활성화하도록 DDNS 업데이트 방법을 설정합니다.

DHCP 서버가 모든 요청을 수행할 경우, DDNS 업데이트 방법을 설정할 필요가 없습니다.

a) **DDNS Update Methods(DDNS** 업데이트 방법**)**에서 **Add(**추가**)**를 클릭합니다.
b) 방법 이름을 설정합니다.
c) **DDNS**를 클릭합니다.

d) (선택 사항) DNS 요청 간 업데이트 간격을 설정합니다. 기본적으로 모든 값이 0으로 설정된 경우, IP 주소 또는 호스트네임이 변경될 때마다 업데이트 요청이 전송됩니다. 요청을 정기적으로 보내려면 일(0~364), 시간, 분 및 초를 설정합니다.

e) FTD에서 업데이트할 업데이트 레코드를 설정합니다.

이 설정은 FTD에서 직접 업데이트하려는 레코드에만 적용됩니다. DHCP 서버가 업데이트할 레코드를 결정하려면 인터페이스당 또는 전역적으로 DHCP 클라이언트 설정을 구성합니다. 단계 5, 867 페이지단계를 참조하십시오.

- **Not Defined(**정의되지 않음**)** - FTD에서 DNS 업데이트를 비활성화합니다.
- **Both A and PTR Records(A** 및 **PTR** 레코드 모두**)** - A RR 및 PTR RR을 모두 업데이트하도록 FTD를 설정합니다. 고정 또는 PPPoE IP 주소 지정에 이 옵션을 사용합니다.
- **A Records(A** 레코드**)** - A RR만 업데이트하도록 FTD를 설정합니다. DHCP 서버가 PTR RR을 업데이트하도록 하려면 이 옵션을 사용합니다.

f) **OK(**확인**)**를 클릭합니다.

g) 이 방법을 단계 5, 867 페이지단계의 인터페이스에 할당합니다.

단계 **4** 웹 방법: FTD에서 HTTP 업데이트 요청을 활성화하도록 DDNS 업데이트 방법을 설정합니다.

a) **DDNS Update Methods(DDNS** 업데이트 방법**)**에서 **Add(**추가**)**를 클릭합니다.

b) 방법 이름을 설정합니다.

c) **Web(**웹**)**을 클릭합니다.

d) IPv4, IPv6 또는 두 주소 유형을 모두 업데이트하도록 웹 업데이트 유형을 설정합니다.

e) 웹 **URL**을 설정합니다. 업데이트 URL을 지정합니다. 필요한 URL은 DNS 제공자에 확인하십시오.

다음 구문을 사용합니다.

https://*username***:***password***@***provider-domain/path***?hostname=<h>&myip=<a>**

예제**:**

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) (선택 사항) DNS 요청 간 업데이트 간격을 설정합니다. 기본적으로 모든 값이 0으로 설정된 경우, IP 주소 또는 호스트네임이 변경될 때마다 업데이트 요청이 전송됩니다. 요청을 정기적으로 보내려면 일(0~364), 시간, 분 및 초를 설정합니다.

g) **OK(**확인**)**를 클릭합니다.

h) 이 방법을 단계 5, 867 페이지단계의 인터페이스에 할당합니다.

i) DDNS용 웹 유형 방법에서는 또한 DDNS 서버 루트 CA를 식별하여 HTTPS 연결을 위해 DDNS 서버 인증서를 검증해야 합니다. 단계 9, 869 페이지단계를 참조하십시오.

단계 **5** 업데이트 방법 설정, DHCP 클라이언트 설정, 해당 인터페이스의 호스트네임 등 DDNS에 대한 인터페이스 설정을 구성합니다.

a) **DDNS Interface Settings(DDNS** 인터페이스 설정**)**에서 **Add(**추가**)**를 클릭합니다.

b) 드롭다운 목록에서 **Interface(**인터페이스**)**를 선택합니다.

c) **DDNS Update Methods(DDNS** 업데이트 방법**)** 페이지에서 생성한 방법 이름을 선택합니다.

(표준 DDNS 방법) DHCP 서버가 모든 업데이트를 수행하도록 하려면 방법을 할당할 필요가 없습니다.

d) 이 인터페이스의 호스트네임을 설정합니다.

호스트네임을 설정하지 않으면 디바이스 호스트네임이 사용됩니다. FQDN을 지정하지 않으면 DNS 서버 그룹의 기본 도메인이 추가되거나(고정 또는 PPPoE IP 주소 지정) DHCP 서버의 도메인 이름이 추가됩니다(DHCP IP 주소 지정용).

e) 표준 DDNS 방법: DHCP 서버가 업데이트할 레코드를 결정하기 위해 **DHCP Client requests DHCP server to update requests(**요청을 업데이트하도록 **DHCP** 클라이언트 요청 **DHCP** 서버**)**를 설정합니다.

FTD는 DHCP 서버에 DHCP 클라이언트 요청을 전송합니다. DDNS를 지원하도록 DHCP 서버도 설정해야 합니다. 클라이언트 요청을 준수하도록 서버를 설정하거나 클라이언트를 재정의할 수 있습니다(이 경우, 클라이언트가 서버에 수행 중인 업데이트를 수행하지 않도록 클라이언트에 응답함).

고정 또는 PPPoE IP 주소 지정의 경우, 이러한 설정은 무시됩니다.

참고 **DDNS** 페이지의 모든 인터페이스에 대해 이러한 값을 전역적으로 설정할 수도 있습니다. 인터페이스별 설정이 전역 설정보다 우선합니다.

- **Not Selected(**선택하지 않음**)** - DHCP 서버에 대한 DDNS 요청을 비활성화합니다. 클라이언트가 DDNS 업데이트를 요청하지 않더라도 DHCP 서버가 업데이트를 보내도록 설정할 수 있습니다.
- **No Update(**업데이트 없음**)** - 업데이트를 수행하지 않도록 DHCP 서버에 요청합니다. 이 설정은 **A** 및 **PTR** 레코드 모두가 활성화된 DDNS 업데이트 방법과 함께 작동합니다.
- **Only PTR(PTR** 만**)** - DHCP 서버가 PTR RR 업데이트를 수행하도록 요청합니다. 이 설정은 **A** 레코드가 활성화된 DDNS 업데이트 방법과 함께 작동합니다.
- **Both A and PTR Records(A** 및 **PTR** 레코드 모두**)** - DHCP 서버가 A 및 PTR RR 업데이트를 모두 수행하도록 요청합니다. 이 설정에서는 DDNS 업데이트 방법을 인터페이스와 연결할 필요가 없습니다.

f) **OK(**확인**)**를 클릭합니다.

참고 **Dynamic DNS Update(**동적 **DNS** 업데이트**)** 설정은 FTD에서 DHCP 서버를 활성화할 때 DHCP 서버 설정과 관련이 있습니다. 자세한 내용은 단계 6, 868 페이지단계를 참조하십시오.

단계 **6** FTD에서 DHCP 서버를 활성화하는 경우, DDNS에 대한 DHCP 서버 설정을 구성할 수 있습니다.

DHCP 서버를 활성화하려면 DHCP 서버 구성, 862 페이지의 내용을 참조하십시오. DHCP 클라이언트가 표준 DDNS 업데이트 방법을 사용할 때 서버 동작을 설정할 수 있습니다. 서버가 업데이트를 수행하는 경우, 클라이언트 리스가 만료되고 갱신되지 않으면 서버는 DNS 서버가 담당했던 RR을 제거하도록 요청합니다.

a) 전역적으로 또는 인터페이스별로 서버 설정을 구성할 수 있습니다. 전역 설정은 기본 **DDNS** 페이지를 참조하십시오. 인터페이스별 설정은 **DDNS Interface Settings(DDNS** 인터페이스 설정**)** 페이지를 참조하십시오. 인터페이스 설정이 전역 설정보다 우선합니다.

b) DHCP 서버가 **Dynamic DNS Update(**동적 **DNS** 업데이트**)**에서 업데이트할 DNS RR을 설정합니다.

- **Not Selected(**선택하지 않음**)** - 클라이언트가 요청하는 경우에도 DDNS 업데이트가 비활성화됩니다.
- **Only PTR(PTR**만**)** - DDNS 업데이트를 활성화합니다. **Override DHCP Client Requests(DHCP** 클라이언트 요청 재정의**)** 설정을 활성화하면 서버가 PTR RR만 업데이트합니다. 활성화하지 않으면 서버는 클라이언트가 요청하는 RR을 업데이트합니다. 클라이언트가 FQDN 옵션과 함께 업데이트 요청을 보내지 않으면 서버는 DHCP 옵션 12에서 검색된 호스트네임을 사용하여 A 및 PTR RR 모두에 대한 업데이트를 요청합니다.
- **Both A and PTR Records(A** 및 **PTR** 레코드 모두**)** - DDNS 업데이트를 활성화합니다. **Override DHCP Client Requests(DHCP** 클라이언트 요청 재정의**)** 설정을 활성화하면 서버가 A 및 PTR RR을 모두 업데이트합니다. 활성화하지 않으면 서버는 클라이언트가 요청하는 RR을 업데이트합니다. 클라이언트가 FQDN 옵션과 함께 업데이트 요청을 보내지 않으면 서버는 DHCP 옵션 12에서 검색된 호스트네임을 사용하여 A 및 PTR RR 모두에 대한 업데이트를 요청합니다.

c) DHCP 클라이언트에서 요청한 업데이트 작업을 재정의하려면 **Override DHCP Client Requests(DHCP** 클라이언트 요청 재정의**)**를 선택합니다.

서버는 요청이 재정의되었다고 클라이언트에 응답하므로, 클라이언트는 서버가 수행 중인 업데이트도 수행하지 않습니다.

단계 **7** (선택 사항) 일반 DHCP 클라이언트 설정을 구성합니다. 이러한 설정은 DDNS와 관련이 없지만, DHCP 클라이언트의 동작 방식과 관련이 있습니다.

a) **DDNS** 페이지에서 **Enable DHCP Client Broadcast(DHCP** 클라이언트 브로드캐스트 활성화**)**를 선택하여 DHCP 서버가 DHCP 응답을 브로드캐스트하도록 요청합니다(DHCP 옵션 1).

b) **DDNS** > **DHCP Client ID Interface(DHCP** 클라이언트 **ID** 인터페이스**)**에서 MAC 주소가 내부에서 생성된 기본 문자열 대신 옵션 61에 대한 DHCP 요청 패킷 내부에 저장되도록 하려면 **Available Interfaces(**사용 가능한 인터페이스**)** 목록에서 인터페이스를 선택한 다음 **Add(**추가**)**를 클릭하여 **Selected Interfaces(**선택한 인터페이스**)** 목록으로 이동합니다.

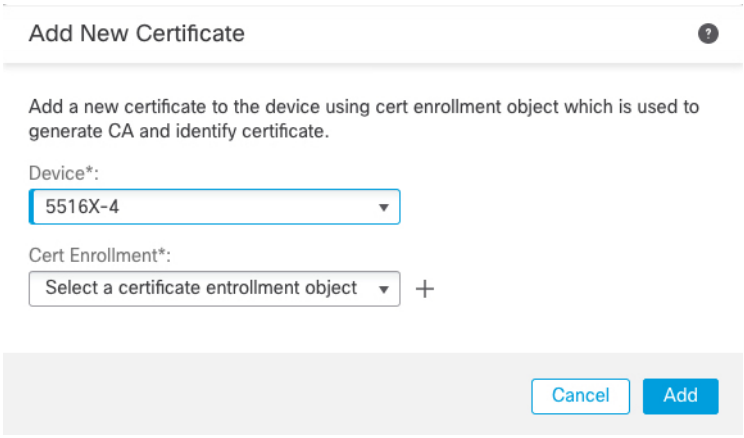
일부 ISP의 경우 옵션 61이 인터페이스 MAC 주소가 됩니다. MAC 주소가 DHCP 요청 패킷에 포함되지 않은 경우 IP 주소는 지정되지 않습니다. 이 설정은 DDNS와 직접 관련이 없지만, 일반적인 DHCP 클라이언트 설정입니다.

단계 **8** 변경 사항을 저장하려면 Device(디바이스) 페이지에서 **Save(**저장**)**를 클릭합니다.

단계 **9** DDNS용 웹 방법에서는 또한 DDNS 서버 루트 CA를 식별하여 HTTPS 연결을 위한 DDNS 서버 인증서를 검증해야 합니다.

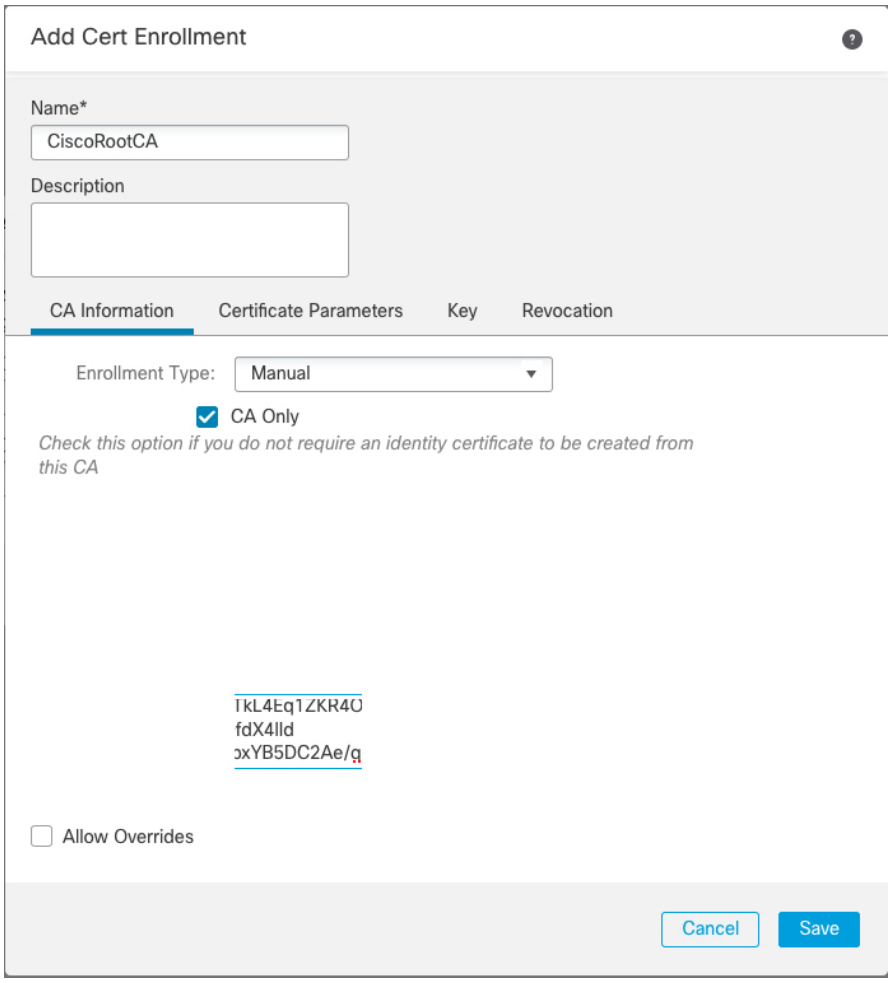
다음 예에서는 DDNS 서버의 CA를 신뢰 지점으로 추가하는 방법을 보여줍니다.

a) DDNS 서버 CA 인증서를 가져옵니다. 이 절차에서는 PEM 형식을 사용하는 수동 가져오기를 보여주지만, PKCS12를 사용할 수도 있습니다.
b) FMC에서 **Devices(**디바이스**)** > **Certficates(**인증서**)**를 선택하고 **Add(**추가**)**를 클릭합니다.
c) **Device(**디바이스**)**를 선택하고 추가(+)을(를) 클릭합니다.



Add Cert Enrollment(인증서 등록 추가**)** 대화 상자가 나타납니다.

d) 다음 필드에 입력하고 **Save(**저장**)**를 클릭합니다.



- **Name(**이름**)**을 입력합니다.
- **Enrollment Type(**등록 유형**)** > **Manual(**수동**)**을 선택합니다.
- **CA Only(CA** 전용**)**를 클릭합니다.
- 9.a, 870 페이지단계의 CA 텍스트에 붙여 넣습니다.

e) **Save(**저장**)**를 클릭합니다.

32 장

Firepower 1000/2100 용 SNMP

이 장에서는 Firepower 1000/2100용 SNMP를 구성하는 방법을 설명합니다.

- Firepower 1000/2100 시리즈용 SNMP 정보, 873 페이지
- Firepower 1000/2100용 SNMP 활성화 및 SNMP 속성 구성, 873 페이지
- Firepower 1000 /2100용 SNMP 트랩 생성, 875 페이지
- Firepower 1000/2100에 대한 SNMP 사용자 생성, 876 페이지

Firepower 1000/2100 시리즈용 SNMP 정보

SNMP(Simple Network Management Protocol)는 SNMP 관리자 및 에이전트 간 통신에 메시지 형식을 제공하는 애플리케이션 레이어 프로토콜입니다. SNMP는 네트워크에 있는 디바이스의 모니터링 및 관리에 사용되는 표준화된 프레임워크 및 공통 언어를 제공합니다.

SNMP 프레임워크는 다음 3가지 항목으로 구성됩니다.

- SNMP 관리자 — SNMP를 사용하는 네트워크 디바이스의 활동을 제어하고 모니터링하는 데 쓰이는 시스템.
- SNMP 에이전트 - Firepower 섀시의 데이터를 유지 관리하고 필요 시 데이터를 SNMP 관리자에 보고하는 Firepower 1000/2100 섀시에 포함된 소프트웨어 구성 요소입니다. Firepower 섀시는 MIB 컬렉션 및 에이전트를 포함합니다. SNMP 에이전트를 활성화하고 관리자와 에이전트 간의 관계를 생성하려면 Firepower Management Center에서 SNMP를 활성화하고 구성합니다.
- MIB(managed information base) - SNMP 에이전트에 있는 관리되는 개체의 모음.

Firepower 1000 /2100 섀시는 SNMPv1, SNMPv2c, SNMPv3를 지원합니다. SNMPv1 및 SNMPv2c는 모두 보안 커뮤니티 기반 양식을 사용합니다.

Firepower 1000/2100용 SNMP 활성화 및 SNMP 속성 구성

참고 이 절차는 Firepower 2100 및 Firepower 1000 시리즈 디바이스에만 적용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** **SNMP**를 클릭합니다.

단계 **3** 다음 필드를 입력합니다.

이름	설명
Admin State(관리 상태**)** 체크 박스	SNMP 활성화 또는 비활성화 여부. 시스템에 SNMP 서버와의 통합이 포함된 경우에만 이 서비스를 활성화합니다.
Port(포트**)** 필드	Firepower 섀시가 SNMP 호스트와 통신할 때 사용하는 포트입니다. 기본 포트를 변경할 수 없습니다.
Community(커뮤니티**)** 필드	Firepower 섀시가 SNMP 호스트에 전송하는 모든 트랩 메시지에 포함되는 기본 SNMP v1 또는 v2 커뮤니티 이름 또는 SNMP v3 사용자 이름입니다. 영숫자 문자열은 1자~32자로 입력합니다. @(at 기호), \(백슬래시), "(큰 따옴표), ? (물음표) 또는 공백을 사용하지 마십시오. 기본값은 **`public`**입니다. **Community(**커뮤니티**)** 필드가 이미 설정된 경우 빈 필드 오른쪽의 텍스트에 **Set: Yes(**설정**:** 예**)**가 표시됩니다. **Community(**커뮤니티**)** 필드에 아직 값이 채워지지 않은 경우 빈 필드 오른쪽의 텍스트에 **Set: No(**설정**:** 아니요**)**가 표시됩니다.
System Administrator Name(시스템 관리자 이름**)** 필드	SNMP 구현을 책임지는 담당자입니다. 이메일 주소, 이름, 전화 번호 등 최대 255자의 문자열로 입력합니다.
Location(위치**)** 필드	SNMP 에이전트(서버)가 실행되는 호스트의 위치입니다. 최대 510자의 영숫자 문자열을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

SNMP 트랩 및 사용자를 생성합니다.

Firepower 1000 /2100용 SNMP 트랩 생성

참고 이 절차는 Firepower 2100 및 Firepower 1000 시리즈 디바이스에만 적용됩니다

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** **SNMP**를 클릭합니다.

단계 **3** **SNMP Traps(SNMP** 트랩**)** 영역에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **SNMP Trap Configuration(SNMP** 트랩 설정**)** 대화 상자에서 다음 필드를 입력합니다.

이름	설명
Host Name(호스트 이름**)** 필드	Firepower 새시가 트랩을 전송해야 하는 SNMP 호스트의 호스트 이름 또는 IP 주소입니다.
Community(커뮤니티**)** 필드	Firepower 새시가 SNMP 호스트에 트랩을 전송할 때 포함하는 SNMP v1 또는 v2 커뮤니티 이름 또는 SNMP v3 사용자 이름입니다. 이것은 SNMP 서비스를 위해 구성된 커뮤니티 또는 사용자 이름과 동일해야 합니다. 영숫자 문자열은 1자~32자로 입력합니다. @(at 기호), \(백슬래시), "(큰 따옴표), ? (물음표) 또는 공백을 사용하지 마십시오.
Port(포트**)** 필드	Firepower 새시가 트랩을 위해 SNMP 호스트와 통신하는 포트입니다. 1 ~ 65535 범위의 정수를 입력합니다.
Version(버전**)** 필드	트랩에 사용되는 SNMP 버전 및 모델입니다. 다음 중 하나일 수 있습니다. • **V1** • **V2** • **V3**
Type(유형**)** 필드	버전을 **V2** 또는 **V3**로 선택한 경우 트랩 유형이 전송됩니다. 다음 중 하나일 수 있습니다. • 트랩 • **Informs**

이름	설명
Privilege(권한**)** 필드	버전을 **V3**로 선택한 경우 권한이 트랩과 연결되어 있습니다. 다음 중 하나일 수 있습니다. • **Auth** — 인증하지만 암호화 없음 • **Noauth** — 인증 또는 암호화 없음 • **Priv** — 인증 및 암호화

단계 **5** **OK(**확인**)**를 클릭하여 **SNMP Trap Configuration(SNMP** 트랩 구성**)** 대화 상자를 닫습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

Firepower 1000/2100에 대한 SNMP 사용자 생성

참고 이 절차는 Firepower 2100 및 Firepower 1000 시리즈 디바이스에만 적용됩니다

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** **SNMP**를 클릭합니다.

단계 **3** **SNMP Users Configuration(SNMP** 사용자 설정**)** 영역에서 **Add(**추가**)**를 선택합니다.

단계 **4** **SNMP User Configuration(SNMP** 사용자 설정**)** 대화 상자에서 다음 필드를 입력합니다.

이름	설명
사용자 이름 필드	SNMP 사용자에게 할당된 사용자 이름입니다. 최대 32개의 문자 또는 숫자를 입력합니다. 이름은 문자로 시작해야 하며 _(밑줄), . (마침표), @(at 기호) 및 -(하이픈)을 지정할 수 있습니다.
Auth Algorithm Type(인증 알고리즘 유형**)** 필드	권한 부여 유형: **SHA**.

이름	설명
USe AES-128(AES-128 사용**)** 체크상자	이 확인란을 선택한 경우, 해당 사용자는 AES-128 암호화를 사용합니다. 참고 SNMPv3는 DES를 지원하지 않습니다. AES-128 상자를 선택하지 않은 상태로 두면 프라이버시 암호화가 수행되지 않으며, 설정된 프라이버시 비밀번호가 적용되지 않습니다.
Authentication Password(인증 비밀번호**)** 필드	사용자의 비밀번호입니다.
Confirm(확인**)** 필드	확인을 위해 다시 한 번 입력하는 비밀번호입니다.
Encryption Password(암호화된 비밀번호**)** 필드	사용자의 비공개 비밀번호입니다.
Confirm(확인**)** 필드	확인을 위해 다시 한 번 입력하는 프라이버시 비밀번호입니다.

단계 **5** **OK(**확인**)**를 클릭하여 **SNMP User Configuration(SNMP** 사용자 구성**)** 대화 상자를 닫습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

33 장

QoS(Quality of Service) Firepower Threat Defense

다음 주제에서는 Firepower Threat Defense 디바이스의 QoS(Quality of Service)를 사용하여 네트워크 트래픽을 폴리싱하는 방법을 설명합니다.

- QoS 소개, 879 페이지
- QoS 정책 정보, 879 페이지
- QoS 요구 사항 및 사전 요건, 880 페이지
- QoS 정책을 사용한 속도 제한, 881 페이지

QoS 소개

액세스 제어에서 허용되거나 신뢰하는 서비스 품질 또는 QoS, 속도 제한(정책) 네트워크 트래픽 시스템은 빠른 경로가 지정된 트래픽의 속도를 제한하지 않습니다.

QoS는 Firepower Threat Defense 디바이스의 라우팅된 인터페이스만 지원합니다.

속도 제한된 연결 로깅

QoS에 대한 로깅 구성이 없습니다. 연결은 로깅 없이 속도 제한을 받을 수 있으며 속도 제한을 이유로 연결을 로깅할 수 없습니다. 연결 이벤트에서 QoS 정보를 보려면 적절한 연결의 종료를 Firepower Management Center 데이터베이스에 개별적으로 기록해야 합니다. 로깅할 수 있는 기타 연결, 2861 페이지를 참조하십시오.

속도 제한된 연결에 대한 연결 이벤트는 삭제된 트래픽의 양과 트래픽이 제한된 QoS 설정에 대한 정보를 포함합니다. 이 정보는 이벤트 보기(워크플로), 대시보드, 보고서에서 볼 수 있습니다.

QoS 정책 정보

매니지드 디바이스의 속도 제한을 제어하기 위해 구축된 QoS 정책 각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

QoS 정책에서는 최대 32개의 QoS 규칙이 네트워크 트래픽을 처리합니다. 시스템은 사용자가 지정하는 순서대로 트래픽이 QoS 규칙과 일치하는지 확인합니다. 시스템은 모든 규칙 조건이 트래픽과 일치하는 첫 번째 규칙에 따라 트래픽의 속도를 제한합니다. 모든 규칙 조건과 일치하지 않는 트래픽의 속도는 제한되지 않습니다.

소스 또는 대상(라우팅) 인터페이스에서 QoS 규칙을 제한해야 합니다. 시스템은 각 인터페이스에서 개별적으로 속도를 제한합니다. 인터페이스 집합에 대해 합계 속도 제한을 지정할 수 없습니다.

QoS 규칙은 애플리케이션, URL, 사용자 ID, 사용자 정의 보안 그룹 태그(SGT)와 같은 상황 정보 및 다른 네트워크 특징으로도 트래픽 속도를 제한할 수 있습니다.

다운로드 트래픽과 업로드 트래픽의 속도를 개별적으로 제한할 수 있습니다. 시스템은 연결 이니시에이터에 따라 다운로드 및 업로드 규칙을 결정합니다.

참고 QoS는 메인 액세스 제어 설정에 속하지 않으며 독립적으로 구성됩니다. 그러나 동일한 디바이스의 공유 ID 설정에 구축된 액세스 제어 및 QoS 정책은 액세스 제어에 다른 정책 연결, 1641 페이지을 참조하십시오.

QoS 정책 및 멀티 테넌시

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인의 관리자는 다른 하위 도메인의 디바이스에 동일한 QoS 정책을 구축할 수 있습니다. 이 하위 도메인의 관리자는 상위에서 구축한 QoS 정책을 읽기 전용으로 사용하거나 로컬 정책으로 대체할 수 있습니다.

QoS 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

QoS 정책을 사용한 속도 제한

정책 기반 속도 제한을 수행하려면 매니지드 디바이스에 QoS 정책을 구성 및 구축합니다. 각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장한 변경사항이 유지됩니다. 편의상 시스템에는 현재 각 정책을 수정하고 있는 사용자(있는 경우)에 대한 정보가 표시됩니다. 세션의 개인 정보를 보호하기 위해 정책 편집기에서 30분 동안 아무런 작업을 하지 않으면 경고가 표시됩니다. 60분이 지나면 시스템에서 변경사항을 삭제합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **QoS**을(를) 선택합니다.

단계 **2** **New Policy(**새 정책**)**를 클릭해 새 QoS 정책을 생성하고, 원한다면 대상 디바이스를 할당합니다. 자세한 내용은 QoS 정책 생성, 882 페이지의 내용을 참조하십시오.

기존 정책을 복사 ( )하거나 수정( )할 수도 있습니다.

단계 **3** QoS 규칙 구성은 QoS 규칙 구성, 883 페이지과 규칙 관리: 일반 특성, 523 페이지를 참조하십시오.

QoS 정책 편집기의 규칙은 평가 순서대로 규칙을 나열하고 규칙 조건 및 속도 제한 설정 요약을 표시합니다. 마우스 오른쪽 버튼 클릭 메뉴는 이동, 활성화 및 비활성화를 포함한 규칙 관리 옵션을 제공합니다.

디바이스별 필터를 사용하여 특정 디바이스 또는 디바이스 그룹에만 영향을 주는 규칙을 표시할 수 있어 대규모 구축에 유용합니다. 규칙에 대해 또는 규칙 내에서 검색할 수 있습니다. 시스템은 검색 조건 필드에 입력한 텍스트를 개체 및 개체 그룹을 포함해 규칙 이름, 조건 값과 일치시킵니다.

참고 규칙을 올바르게 생성하고 순서를 지정하는 것은 복잡한 작업이지만, 효과적인 구축에 필수적입니다. 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이선스를 요구하거나, 잘못된 구성을 포함할 수 있습니다. 아이콘은 설명, 경고 및 오류를 나타냅니다. 문제가 있을 경우 경고 표시를 클릭하면 목록이 표시됩니다. 자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지의 내용을 참고하십시오.

단계 **4** 정책 할당을 클릭하여 정책의 대상이 되는 매니지드 디바이스를 식별합니다. QoS 정책에 대한 대상 디바이스 설정, 882 페이지를 참조하십시오.

정책을 생성하는 중에 대상 디바이스를 식별한 경우 선택 사항을 확인합니다.

단계 **5** QoS 정책을 저장합니다.

단계 **6** 이 기능은 일부 패킷의 통과를 허용해야 하므로 해당 패킷을 검사하도록 시스템을 설정해야 합니다. 트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례, 2202 페이지 및 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정, 2203 페이지를 참조하십시오.

단계 **7** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

QoS 정책 생성

규칙이 없는 새 QoS 정책은 속도 제한을 수행하지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **QoS**을(를) 선택합니다.

단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** **Name(**이름**)**을 입력하고, 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **4** 필요에 따라 정책을 구축할 사용 가능한 디바이스를 선택하고 정책에 추가 또는 드래그 앤 드롭을 클릭하여 선택한 디바이스를 추가합니다. 표시되는 디바이스의 범위를 좁히려면 검색 필드에 검색 문자열을 입력합니다.

정책을 구축하기 전에 디바이스를 할당해야 합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- QoS 정책을 구축하고 구성하려면 QoS 정책을 사용한 속도 제한, 881 페이지을 참조하십시오.

QoS 정책에 대한 대상 디바이스 설정

각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

프로시저

단계 **1** QoS 정책 편집기에서 정책 할당을 클릭합니다.

단계 **2** 대상 목록 작성:

- 추가 - 하나 이상의 사용 가능한 디바이스를 선택한 다음 정책에 추가를 클릭하거나 선택한 디바이스 목록으로 드래그 앤 드롭합니다.
- 삭제 - 단일 디바이스 옆에 있는 삭제( )을 클릭하거나 여러 디바이스를 선택하고 오른쪽 클릭한 다음 **Delete Selected(**선택 항목 삭제**)**를 선택합니다.
- 검색 - 검색 필드에 검색 문자열을 입력합니다. 지우기( )을 클릭하여 검색 내용을 삭제합니다.

단계 **3** **OK**를 클릭하여 정책 할당을 저장합니다.

단계 4 **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

QoS 규칙 구성

규칙을 생성하거나 편집할 때 규칙 편집기의 상단을 사용해 일반 규칙 속성을 설정할 수 있습니다. 규칙 편집기 하단을 사용하여 규칙 조건 및 설명을 설정합니다.

프로시저

단계 1 QoS 정책 편집기의 규칙에는 다음이 있습니다.

- 규칙 추가 - **Add Rule(**규칙 추가**)**를 클릭합니다.
- Edit Rule(규칙 편집) - 수정( )을 클릭합니다.

단계 2 **Name(**이름**)**을 입력합니다.

단계 3 규칙 구성 요소를 구성합니다.

- Enabled(활성화) — 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.
- QoS 적용 켜기 - 대상 인터페이스 개체의 인터페이스 또는 소스 인터페이스 개체의 인터페이스 중 속도를 제한하려는 인터페이스를 선택합니다. 이때 선택은 생성된 인터페이스 제약**(Any(**모든**)**이 아닌)에 일치해야 합니다.
- 인터페이스별 트래픽 제한 - Mbit/초 단위로 다운로드 제한 용량 및 업로드 제한 용량을 입력합니다. **Unlimited(**무제한**)**의 기본값은 해당 방향의 일치하는 트래픽의 속도 제한을 방지합니다.
- 조건 - 추가할 조건을 클릭합니다. **Apply QoS On(QoS** 적용**)**에 대한 선택에 해당하는 소스 또는 대상 인터페이스 조건을 설정해야 합니다.
- 설명 - **Comment(**설명**)**를 클릭합니다. 설명을 추가하려면 **New Comment(**새 설명**)**을 클릭해 설명을 입력하고 **OK(**확인**)**을 클릭합니다. 규칙을 저장할 때까지 이 코멘트를 수정하거나 삭제할 수 있습니다.

규칙 구성 요소에 대한 자세한 내용은 QoS 규칙 구성 요소, 884 페이지을 참조하십시오.

단계 4 규칙을 저장합니다.

단계 5 정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

QoS 규칙 구성 요소

상태(활성화/비활성화)

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하지 않으며, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

인터페이스(QoS 적용됨)

모든 트래픽의 속도를 제한하는 QoS 규칙은 저장할 수 없습니다. 각 QoS 규칙에 대해 다음의 경우 QoS를 적용해야 합니다.

- 소스 인터페이스 개체의 인터페이스 - 규칙의 소스 인터페이스를 통해 트래픽 속도를 제한합니다. 이 옵션을 선택하는 경우 하나 이상의 소스 인터페이스 제약 조건(**any** 불가)을 추가해야 합니다.
- 대상 인터페이스 개체의 인터페이스 - 규칙의 대상 인터페이스를 통해 트래픽 속도를 제한합니다. 이 옵션을 선택하는 경우 하나 이상의 대상 인터페이스 제약 조건 (**any** 불가)를 추가해야 합니다.

인터페이스별 트래픽 제한

QoS 규칙은 옵션에서 QoS 적용을 지정한 각 인터페이스에 개별적으로 속도를 제한합니다. 인터페이스 집합에 대해 통합적인 속도 제한을 지정할 수 없습니다.

초당 Mbits로 트래픽을 제한할 수 있습니다. **Unlimited**(무제한)의 기본값은 일치하는 트래픽의 속도 제한을 방지합니다.

다운로드 트래픽과 업로드 트래픽의 속도를 개별적으로 제한할 수 있습니다. 시스템은 연결 이니시에이터에 따라 다운로드 및 업로드 규칙을 결정합니다.

인터페이스의 최대 처리량보다 큰 한계를 지정하는 경우 시스템은 일치하는 트래픽의 속도 제한을 하지 않습니다. 최대 처리량은 각 디바이스의 속성에서 지정한 인터페이스의 하드웨어 설정에 영향을 받을 수 있습니다.(**Devices**(디바이스) > **Device Management**(디바이스 관리))

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 규칙마다 여러 조건을 구성할 수 있습니다. 트래픽은 규칙과 일치하는 모든 조건과 일치해야 합니다. 각 조건 유형은 규칙 편집기에 고유한 탭이 있습니다. 다음을 사용하여 트래픽 속도를 제한할 수 있습니다.

- 인터페이스 조건 (라우팅 전용, 필수)
- 네트워크 조건, 530 페이지
- 포트 및 ICMP 코드 조건, 532 페이지
- 애플리케이션 조건(애플리케이션 컨트롤), 535 페이지
- URL 필터링, 1665 페이지
- 사용자, 영역 및 ISE 속성 조건(사용자 제어), 545 페이지
- 맞춤형 SGT 조건

코멘트

규칙에 대한 변경 사항을 저장할 때마다 코멘트를 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다.

시스템 정책 편집기에서 시스템은 규칙에 포함될 코멘트 수를 표시합니다. 규칙 편집기에서 Comments(코멘트) 탭을 사용하여 기존 코멘트를 확인하고 새 코멘트를 추가합니다.

VIII 부

Firepower Threat Defense 고가용성 및 확장성

- Firepower Threat Defense의 고가용성, 889 페이지
- Firepower Threat Defense 클러스터링, 917 페이지

34 장

Firepower Threat Defense의 고가용성

다음 주제에서는 Cisco Firepower Threat Defense의 고가용성을 달성하기 위해 액티브/스탠바이 장애 조치를 구성하는 방법을 설명합니다.

- Firepower Threat Defense 고가용성 정보, 889 페이지
- 고가용성 요구 사항 및 전제 조건, 904 페이지
- 고가용성 지침, 905 페이지
- Firepower Threat Defense 고가용성 쌍 추가, 906 페이지
- 선택적 고가용성 파라미터 구성, 908 페이지
- Manage(관리) 고가용성, 910 페이지
- 모니터링 고가용성, 915 페이지

Firepower Threat Defense 고가용성 정보

고가용성 또는 장애 조치를 구성하려면 두 개의 동일한 Firepower Threat Defense디바이스가 장애 조치 전용 링크 또는 경우에 따라 상태 링크와 각각 연결되어야 합니다. Firepower Threat Defense는 한 개의 유닛이 액티브 유닛으로 트래픽을 통과하는 Active/Standby(액티브/스탠바이) 장애 조치를 지원합니다. 스탠바이 유닛은 능동적으로 트래픽을 전달하지 않지만, 액티브 유닛에서 컨피그레이션 및 기타 상태 정보를 동기화합니다. 장애 조치가 일어나면 액티브 유닛은 스탠바이 유닛으로 장애 조치를 시작하며, 이때 스탠바이 유닛이 액티브 유닛이 됩니다.

액티브 유닛의 상태(하드웨어, 인터페이스, 소프트웨어 및 환경 상태)를 모니터링하여 특정 페일오버 조건이 충족되는지 확인합니다. 이러한 조건이 충족되면 장애 조치가 이루어집니다.

참고 고가용성은 퍼블릭 클라우드에서 실행되는 Firepower Threat Defense Virtual에서 지원되지 않습니다.

고가용성 시스템 요구 사항

이 섹션에서는 고가용성 구성에서 ASA의 하드웨어, 소프트웨어 및 라이선스 요구 사항에 대해 설명합니다.

하드웨어 요구 사항

고가용성 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 모델이어야 합니다. 또한 컨테이너 인스턴스에 동일한 리소스 프로파일 속성을 사용해야 합니다.

  Firepower 9300의 경우 고가용성은 동일한 유형의 모듈 간에만 지원되지만, 두 섀시는 혼합된 모듈을 포함할 수 있습니다. 각 섀시에 SM-36 및 SM-44가 있는 경우를 예로 들 수 있습니다. SM-36 모듈 간 SM-44 모듈 간에 고가용성 쌍을 생성할 수 있습니다.

  고가용성 쌍을 FMC에 추가한 후 리소스 프로파일을 변경하는 경우 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **System(**시스템**)** > **Inventory(**인벤토리**)** 대화 상자에서 각 유닛의 인벤토리를 업데이트합니다.

- 인터페이스 개수와 유형이 같아야 합니다.

  의 Firepower 4100/9300 섀시의 경우, 고가용성 기능을 활성화하기 전에 FXOS에서 동일하게 모든 인터페이스를 사전에 구성해야 합니다. 고가용성 기능을 활성화한 후에 인터페이스를 변경하는 경우, 스탠바이 유닛의 FXOS에서 인터페이스를 변경하고 나서 활성 유닛에서 동일하게 변경을 수행합니다.

- 같은 모듈을 설치해야 합니다(있을 경우).

- 같은 RAM을 설치해야 합니다.

고가용성 구성에서 플래시 메모리 크기가 다른 유닛을 사용 중인 경우, 플래시 메모리 용량이 작은 유닛에 소프트웨어 이미지 파일 및 구성 파일을 수용할 수 있는 충분한 공간이 있는지 확인해야 합니다. 그렇지 않을 경우 플래시 메모리 용량이 큰 유닛에서 플래시 메모리 용량이 작은 유닛으로 컨피그레이션을 동기화할 수 없습니다.

소프트웨어 요구 사항

고가용성 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 상황 모드에 있어야 합니다(단일 또는 다중).

- 같은 방화벽 모드에 있어야 합니다(라우팅 또는 투명).

- 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 같아야 합니다. 그러나 업그레이드 과정에서 일시적으로 여러 소프트웨어 버전을 사용할 수 있습니다. 예를 들어, 버전 8.3(1)에서 버전 8.3(2)으로 업그레이드하고 장애 조치를 활성 상태로 유지할 수 있습니다. 장기적으로 호환성을 보장하려면 두 유닛을 모두 같은 버전으로 업그레이드하는 것이 좋습니다.

- 같은 AnyConnect 이미지가 있어야 합니다. 무중단 업그레이드를 수행할 때 장애 조치 쌍에 불일치하는 이미지가 있을 경우, 업그레이드 프로세스의 마지막 재부팅 단계에서 클라이언트리스 SSL VPN 연결이 종료되고 데이터베이스에 Orphan 세션이 표시되며 IP 풀에는 클라이언트에 할당된 IP 주소가 "사용 중"인 것으로 표시됩니다.

- (Firepower 4100/9300) 같은 플로우 오프로드 모드가 있으며, 둘 다 활성화하거나 비활성화해야 합니다.

고가용성 쌍의 FTD 디바이스에 대한 라이선스 요구 사항

Firepower Threat Defense 고가용성이 설정된 디바이스에는 동일한 라이선스가 있어야 합니다.

고가용성 컨피그레이션에서는 디바이스 쌍의 각 디바이스에 대해 하나씩, 두 개의 Smart License 자격이 필요합니다.

고가용성을 설정하기 전에는 보조/스탠바이 디바이스에 어떤 라이선스가 할당되든 상관이 없습니다. 고가용성 설정 중에 Firepower Management Center은 스탠바이 디바이스에 할당된 불필요한 라이선스를 해제하고 기본/액티브 디바이스에 할당된 것과 동일한 라이선스로 교체합니다. 예를 들어 액티브 디바이스에 Base 라이선스와 Threat 라이선스가 있고 스탠바이 디바이스에는 Base 라이선스만 있는 경우, Firepower Management Center은 Cisco Smart Software Manager와 통신하여 스탠바이 디바이스의 계정에서 사용 가능한 Threat 라이선스를 가져옵니다. Smart License에 포함되어 있는 구매한 엔타이틀먼트가 충분하지 않으면 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태가 됩니다.

가상 고 가용성 구성에서 등록 할 각 FTD에는 추가 Firepower MCv 디바이스 라이선스가 필요합니다.Firepower Management Center

페일오버 및 스테이트풀 페일오버 링크

장애 조치 링크 및 스테이트풀 장애 조치 링크(선택 사항)는 2개 유닛 간의 전용 연결입니다. Cisco에서는 페일오버 링크 또는 스테이트 풀 페일오버 링크의 두 디바이스 간에 같은 인터페이스 사용을 권장합니다. 예를 들어 페일오버 링크에서 device 1에 eth0를 사용한다면, device 2에서도 같은 인터페이스(eth0)를 사용해야 합니다.

주의 IPsec 터널이나 장애 조치 키로 통신 보안을 설정하지 않는 한 장애 조치 및 상태 링크를 통해 전송되는 모든 정보는 일반 텍스트로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(사전 공유 키)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 IPsec 터널이나 장애 조치 키로 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

페일오버 링크

장애 조치 쌍의 유닛 2개에서는 장애 조치 링크를 통해 지속적으로 통신을 수행하여 각 유닛의 작동 상태를 확인합니다.

장애 조치 링크 데이터

다음 정보는 페일오버 링크를 통해 전달됩니다.

- 유닛 상태(액티브 또는 스탠바이)
- Hello 메시지(keep-alives)
- 네트워크 링크 상태

- MAC 주소 교환
- 컨피그레이션 복제 및 동기화

장애 조치 링크에 대한 인터페이스

사용되지 않는 데이터 인터페이스(물리적, 이중화 또는 EtherChannel)는 모두 장애 조치 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다. Firepower 4100/9300 섀시에 정의되어 있는 하위 인터페이스를 제외하고 하위 인터페이스를 사용할 수 없습니다 장애 조치 링크 인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 상태 링크용으로도 사용 가능).

FTD에서는 사용자 데이터와 장애 조치 링크 간에 인터페이스 공유를 지원하지 않습니다.또한 데이터와 장애 조치 링크에 대해 동일한 상위에서 별도의 하위 인터페이스를 사용할 수 없습니다(Firepower 4100/9300 섀시 하위 인터페이스만 해당). 장애 조치 링크용으로 Firepower 4100/9300 하위 인터페이스를 사용하는 경우에는 해당 상위 인터페이스의 모든 하위 인터페이스와 상위 인터페이스 자체가 장애 조치 링크로 사용되도록 제한됩니다.

참고 EtherChannel 또는 이중 인터페이스를 장애 조치 또는 상태 링크로 사용하는 경우, 고가용성을 설정하기 전에 동일한 멤버 인터페이스를 사용하는 동일한 EtherChannel 또는 이중 인터페이스가 두 디바이스에 있는지 확인해야 합니다.

장애 조치 링크에 대한 다음 지침을 참조하십시오.

- Firepower 4100/9300 - 페일오버 및 상태 링크를 통합하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다.
- 기타 모델 — 1GB 인터페이스는 통합된 장애 조치 및 상태 링크에 충분한 크기입니다.

장애 조치 링크로 사용된 이중 인터페이스의 경우, 추가된 이중성에 대한 다음 이점을 참조하십시오.

- 장애 조치 유닛이 부팅될 때, 활성 유닛을 검색하기 위해 멤버 인터페이스 간에 교체를 수행합니다.
- 장애 조치 유닛이 멤버 인터페이스 중 하나에서 피어로부터 keepalive 메시지 수신을 중지하는 경우, 다른 멤버 인터페이스로 전환합니다.

장애 조치 링크로 사용된 EtherChannel의 경우, EtherChannel의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

장애 조치 링크 연결

다음 2가지 방법 중 하나를 사용하여 장애 조치 링크를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 의 장애 조치 인터페이스로 사용합니다.

- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 유닛을 직접 연결합니다.

유닛 간에 스위치를 사용하지 않으려는 경우 인터페이스에 오류가 발생하면 두 피어에서 링크가 중단됩니다. 이 경우 인터페이스에 오류가 발생하고 링크가 중단된 결과를 초래한 유닛이 어떤 것인지 쉽게 확인할 수 없으므로 문제 해결에 방해될 수 있습니다.

ASA에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through 케이블을 사용할 수 있습니다. 다이렉트 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

스테이트풀 페일오버 링크

스테이트풀 장애 조치를 사용하려면 연결 상태 정보를 전달할 스테이트풀 장애 조치 링크(상태 링크라고도 함)를 구성해야 합니다.

장애 조치 링크 공유

장애 조치 링크를 공유하는 방법은 인터페이스를 보호하는 가장 좋은 방법입니다. 그러나 컨피그레이션 규모가 크고 네트워크의 트래픽이 많은 경우에는 상태 링크와 페일오버 링크에 대해 전용 인터페이스를 사용하는 것을 고려해야 합니다.

전용 인터페이스

상태 링크에 전용 데이터 인터페이스(물리적, 이중 또는 EtherChannel)를 사용할 수 있습니다. 전용 상태 링크의 요구 사항은 장애 조치 링크에 대한 인터페이스, 892 페이지의 내용, 그리고 상태 링크 연결에 대한 정보는 장애 조치 링크 연결, 892 페이지의 내용을 참조하십시오.

장거리 페일오버를 사용할 경우 최적의 성능을 보장하려면 페일오버 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 페일오버 메시지의 재전송으로 인해 성능이 다소 저하됩니다.

페일오버 및 데이터 링크 중단 방지

페일오버 링크 및 데이터 인터페이스가 다른 경로를 통해 이동하도록 설정하여 모든 인터페이스에 동시 다발적으로 오류가 발생하는 가능성을 줄이는 것이 좋습니다. 페일오버 링크가 중단될 경우 Firepower Threat Defense 디바이스는 데이터 인터페이스를 사용하여 페일오버가 필요한지 여부를 확인할 수 있습니다. 그런 다음 페일오버 링크 상태가 복원될 때까지는 페일오버 작업이 보류됩니다.

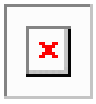
복원력이 뛰어난 페일오버 네트워크를 설계하려면 다음 연결 시나리오를 참조하십시오.

시나리오 **1** — 권장하지 않음

단일 스위치 또는 스위치 집합을 사용하여 두 Firepower Threat Defense 디바이스 간의 페일오버 및 데이터 인터페이스를 모두 연결한 상태에서 스위치 또는 스위치 간 링크가 중단될 경우 두 Firepower Threat Defense 디바이스 모두 액티브 상태가 됩니다. 따라서 아래의 그림에 있는 다음 2가지 연결 방법은 권장하지 않습니다.

그림 *23:* 단일 스위치로 연결 - 권장하지 않음

그림 *24:* 이중 스위치로 연결 - 권장하지 않음



시나리오 2 - 권장함

페일오버 링크에서는 데이터 인터페이스와 같은 스위치를 사용하지 않는 것이 좋습니다. 대신 다음 그림에 나와 있는 것처럼 다른 스위치를 사용하거나 다이렉트 케이블을 사용하여 페일오버 링크에 연결합니다.

그림 *25:* 다른 스위치로 연결

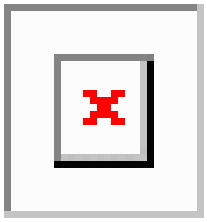
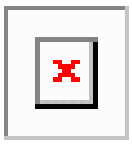


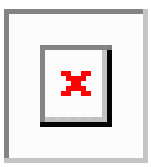
그림 *26:* 케이블로 연결



시나리오 3 — 권장

Firepower Threat Defense 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 페일오버 링크는 이러한 스위치 중 하나에 연결될 수 있으며 다음 그림에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 *27:* 보안 스위치로 연결



시나리오 4 — 권장

가장 안정적인 페일오버 컨피그레이션에서는 다음 그림에 나와 있는 것처럼 페일오버 링크에서 이중 인터페이스를 사용합니다.

그림 *28:* 이중 인터페이스로 연결

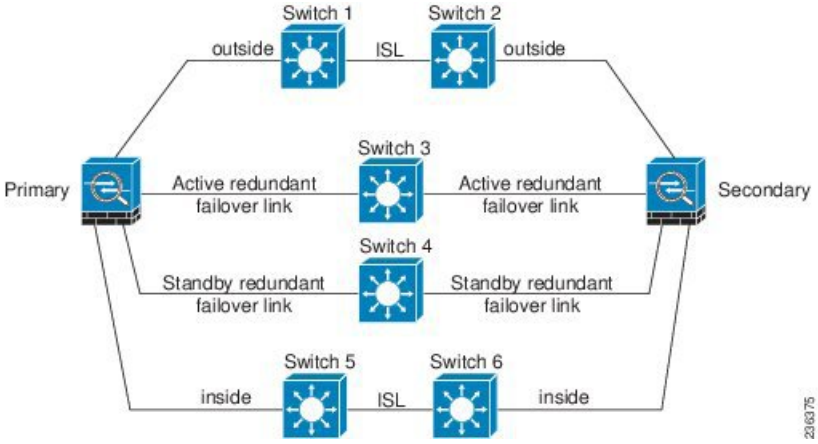
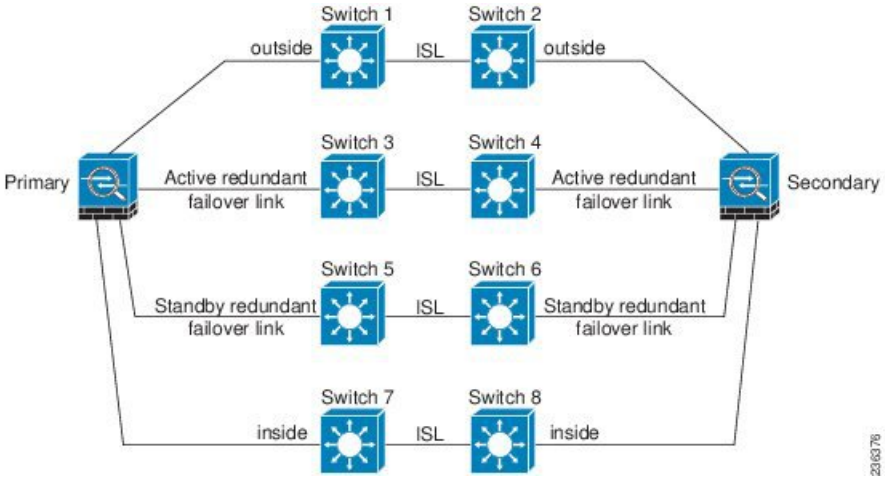


그림 *29:* 스위치 간 링크로 연결



MAC 주소와 IP 주소 - 고가용성

인터페이스를 구성할 때는 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정할 수 있습니다. 일반적으로 페일오버가 발생할 때는 활성 IP 주소와 MAC 주소가 새 액티브 유닛에 승계됩니다. 네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

참고 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다. 관리 목적으로 해당 인터페이스에서 스탠바이 유닛에 연결할 수도 없습니다.

상태 링크의 IP 주소와 MAC 주소는 장애 조치 시 변경되지 않습니다.

액티브/스탠바이 **IP** 주소와 **MAC** 주소

액티브/스탠바이 고가용성의 경우 페일오버 이벤트가 발생하는 동안의 IP 주소 및 MAC 주소 사용법은 다음 설명을 참조하십시오.

1. 액티브 유닛은 항상 기본 유닛의 IP 주소와 MAC 주소를 사용합니다.
2. 액티브 유닛에서 장애 조치가 수행될 때 스탠바이 유닛에서는 장애 발생 유닛의 IP 주소와 MAC 주소를 사용해 트래픽 전달을 시작합니다.
3. 장애 발생 유닛은 다시 온라인으로 설정되면 스탠바이 상태가 되며 스탠바이 IP 주소와 MAC 주소를 승계합니다.

하지만 기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 기본 유닛이 사용 가능해지면 보조(액티브) 유닛이 MAC 주소를 기본 유닛의 주소로 변경하므로 네트워크 트래픽이 중단될 수 있습니다. 마찬가지로, 기본 유닛을 새 하드웨어로 교체하면 새 MAC 주소가 사용됩니다.

시작 시 보조 유닛에 액티브 MAC 주소가 알려지므로 가상 MAC 주소에서는 이러한 중단을 방지하며, 새 기본 유닛 하드웨어가 사용될 경우에도 가상 MAC 주소는 그대로 유지됩니다. 가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다. MAC 주소가 변경될 경우 Firepower Threat Defense 디바이스에서는 고정 NAT 주소에 불필요한 ARP를 전송하지 않으므로, 연결된 라우터에서는 이러한 주소의 MAC 주소 변경을 알지 못합니다.

가상 **MAC** 주소

Firepower Threat Defense 디바이스에서는 여러 가지 방법으로 가상 MAC 주소를 구성할 수 있습니다. 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

다중 인스턴스 기능의 경우 FXOS 섀시에서는 모든 인터페이스에 대해 기본 MAC 주소만 자동 생성합니다. 생성된 MAC 주소를 기본 및 보조 MAC 주소가 모두 포함된 가상 MAC 주소로 덮어쓸 수 있습니다. 보조 MAC 주소를 반드시 사전 정의해야 하는 것은 아니지만, 보조 MAC 주소를 설정하면 새 보조 유닛 하드웨어 사용 시 to-the-box 관리 트래픽이 중단되지 않도록 보장할 수 있습니다.

스테이트풀 페일오버

스테이트풀 장애 조치를 스테이트풀 장애 조치 동안액티브 유닛에서는 연결당 상태 정보를 스탠바이 유닛으로 전달하거나 액티브/액티브 장애 조치에서 액티브 및 스탠바이 장애 조치 그룹 간에 지속적으로 전달합니다. 장애 조치가 일어난 후에는 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다. 지원되는 최종 사용자 애플리케이션이 없어도 다시 연결하여 동일한 통신 세션을 그대로 유지할 수 있습니다.

지원 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 Firepower Threat Defense 디바이스로 전달됩니다.

- NAT 변환 테이블.

- TCP 및 UDP 연결과 상태(HTTP 연결 상태 포함). 다른 유형의 IP 프로토콜과 ICMP는 새 패킷이 도착하면 새 액티브 유닛에서 설정되므로 액티브 유닛에서 구문 분석되지 않습니다.
- SCTP 연결 상태. 그러나 SCTP 검사 스테이트풀 페일오버가 최상의 결과입니다. 페일오버 중에 SACK 패킷이 손실되면 새 액티브 유닛은 누락된 패킷이 수신될 때까지 대기열에서 문제가 있는 기타 모든 패킷을 삭제합니다.
- Snort 연결 상태, 검사 결과 및 핀홀 정보(엄격한 TCP 적용 포함).
- ARP 테이블
- 레이어 2 브리지 테이블(브리지 그룹용)
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 시그널링 세션 및 핀홀.
- 정적 및 동적 라우팅 테이블 - 스테이트풀 페일오버는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 확인한 경로는 스탠바이 유닛의 RIB(Routing Information Base) 테이블에 유지됩니다. 페일오버 이벤트 발생 시 액티브 보조 유닛에서는 초기 규칙에 따라 기본 유닛을 미러링하므로 트래픽 중단을 최소화면서도 패킷이 정상적으로 이동됩니다. 페일오버가 끝난 직후에는 새 액티브 유닛에서 재통합 타이머가 시작됩니다. 그러면 RIB 테이블의 시간대 숫자가 늘어납니다. 재통합을 수행하는 동안 OSPF 및 EIGRP 경로는 새 시간대 숫자로 업데이트됩니다. 타이머가 만료되면 오래된 경로 항목(시간대 숫자에 의해 결정됨)이 테이블에서 제거됩니다. 그런 다음 RIB에 새 액티브 유닛에 대한 최신 라우팅 프로토콜 전달 정보가 포함됩니다.

  참고 경로는 액티브 유닛의 링크 작동 또는 링크 중단 이벤트가 있을 경우에만 동기화됩니다. 스탠바이 유닛에서 링크가 작동하거나 중단될 경우, 액티브 유닛에서 전송된 동적 경로가 손실될 수 있습니다. 이는 일반적이고 정상적인 동작입니다.

- DHCP 서버 - DHCP 주소 임대는 복제되지 않습니다. 그러나 인터페이스에 구성된 DHCP 서버는 ping을 전송하여 특정 주소가 사용 중이지 않음을 확인한 후에 DHCP 클라이언트에 해당 주소를 부여하므로 서비스에는 영향이 없습니다. 상태 정보는 DHCP 릴레이 또는 DDNS와 관련이 없습니다.
- 액세스 제어 정책 결정 - 트래픽 일치(URL, URL 카테고리, 지리위치 등), 침입 탐지, 악성코드 및 파일 유형과 관련된 결정은 페일오버 중에 그대로 유지됩니다. 그러나 페일오버 시점에서 평가 중인 연결의 경우 다음 경고가 적용됩니다.
  - AVC - 앱-ID 판정은 복제되지만 탐지 상태는 복제되지 않습니다. 페일오버가 수행되기 전에 앱-ID 판정이 완료 및 동기화되면 적절한 동기화가 수행됩니다.
  - 침입 탐지 상태 - 페일오버 시 중간 플로우 픽업이 발생하면 새 검사는 완료되지만 이전 상태는 손실됩니다.

- 파일 악성코드 차단 - 페일오버 전에 파일 상태를 확인할 수 있어야 합니다.
- 파일 유형 탐지 및 차단 - 페일오버 전에 파일 유형이 식별되어야 합니다. 원래 액티브 디바이스가 파일을 식별하는 중에 페일오버가 수행되면 파일 유형이 동기화되지 않습니다. 따라서 파일 정책에서 해당 파일 유형을 차단하더라도 새 액티브 디바이스는 파일을 다운로드합니다.

- 보안 인텔리전스 결정. 그러나 페일오버 시점에서 처리 중인 DNS 기반 결정은 완료되지 않습니다.
- RA VPN - 원격 액세스 VPN 최종 사용자는 페일오버 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 페일오버 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.

지원되지 않는 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 Firepower Threat Defense 디바이스로 전달되지 않습니다.

- GRE 또는 IP-in-IP와 같은 일반 텍스트 터널 내의 세션. 터널 내의 세션은 복제되지 않으며, 새 액티브 노드는 기존 검사 판정을 재사용하여 정확한 정책 규칙 일치 여부를 확인할 수 없습니다.
- 암호 해독된 TLS/SSL 연결 - 암호 해독 상태가 동기화되지 않고 만약 액티브 유닛에 장애가 발생하면 암호 해독된 연결이 재설정됩니다. 새 활성 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.
- TCP 상태 우회 연결
- 멀티캐스트 라우팅.

고가용성에 대한 브리지 그룹 요구 사항

브리지 그룹 사용 시 고가용성에 대해 특별히 고려해야 할 사항이 있습니다.

액티브 유닛이 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 스위치 포트가 토폴로지 변경을 인지하는 경우 30초~50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 브리지 그룹 멤버 인터페이스에서 트래픽 손실을 방지하려면 다음 해결 방법 중 하나를 구성할 수 있습니다.

- 스위치 포트는 액세스 모드입니다 - 스위치에서 STP PortFast 기능을 활성화합니다.

```
interface interface_id
  spanning-tree portfast
```

PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 스위치 포트가 트렁크 모드 상태이거나 STP PortFast를 활성화할 수 없는 경우 페일오버 기능 또는 STP 안정성에 영향을 줄 수 있는 다음 해결 방법을 선택할 수 있습니다.
  - 브리지 그룹 및 멤버 인터페이스에 인터페이스 모니터링을 비활성화합니다.
  - 페일오버 기준에서 인터페이스 대기 시간을 큰 값으로 늘려 유닛 페일오버 전 STP를 통합시킵니다.
  - 스위치가 STP를 인터페이스 대기 시간보다 빠르게 통합하도록 STP 타이머를 감소시킵니다.

장애 조치 상태 모니터링

ASA에서는 각 유닛의 전체 상태 및 인터페이스 상태를 모니터링합니다. 이 섹션에는 ASA에서 각 유닛의 상태를 확인하기 위해 테스트를 수행하는 방법에 대한 정보가 포함되어 있습니다.

유닛 상태 모니터링

ASA에서는 hello 메시지가 있는 장애 조치 링크를 모니터링하여 다른 유닛의 상태를 확인합니다. 장애 조치 링크에서 hello 메시지가 유닛에 3번 연속으로 수신되지 않는 경우, 유닛에서는 장애 조치 링크를 비롯한 각 데이터 인터페이스에 LANTEST 메시지를 전송하여 피어의 응답 여부를 확인합니다. ASA에서 취하는 조치는 다른 유닛의 응답에 따라 달라집니다. 아래의 가능한 조치를 참조하십시오.

- ASA에서 장애 조치 링크에 대한 응답을 수신하지 못할 경우 장애 조치가 이루어지지 않습니다.
- ASA에서 장애 조치 링크에 대한 응답은 수신하지 못했으나 데이터 인터페이스에 대한 응답은 수신한 경우, 유닛에서 장애 조치를 수행하지 않습니다. 페일오버 링크가 실패한 것으로 표시됩니다. 페일오버 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버할 수 없으므로 최대한 빨리 페일오버 링크를 복원해야 합니다.
- ASA에서 인터페이스에 대한 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 실패한 것으로 분류합니다.

인터페이스 모니터링

최대 1025개의 인터페이스를 모니터링할 수 있습니다(다중 상황 모드에서 해당되며 모든 상황 간에 분할됨). 중요한 인터페이스를 모니터링해야 합니다. 예를 들어 다중 상황 모드에서 하나의 공유 인터페이스를 모니터링하기 위해 단일 상황을 구성할 수 있습니다. 인터페이스가 공유되므로, 모든 상황은 모니터링을 활용합니다.

15초(기본값) 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 인터페이스 테스트가 실행됩니다. (기간을 변경하려면 **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **Failover(**페일오버**)** > **Criteria(**기준**)** > **Failover Poll Times(**페일오버 폴링 시간**)**를 참조하십시오.) 인터페이스에 대한 단일 인터페이스 테스트가 실패하였으나 다른 유닛에 있는 이 동일한 인터페이스에서는 지속적으로 트래픽을 전달할 수 있다면, 해당 인터페이스는 오류가 발생한 것으로 간주되며 ASA는 테스트를 중단합니다.

오류가 발생한 인터페이스 수에 정의한 임계값이 충족된다면를 참조하십시오. 액티브 유닛이 대기 유닛보다 오류가 발생한 인터페이스가 많으면 페일오버가 발생합니다. 두 유닛의 인터페이스가 모두 실패하면, 두 인터페이스 모두 'Unknown(알 수 없음)' 상태가 되며 페일오버 인터페이스 정책에서 정의하는 페일오버 한도에 합산되지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 장애 임계값이 더 이상 충족되지 않을 경우 장애가 발생한 ASA는 스탠바이 모드로 돌아갑니다.

ASA FirePOWER 모듈이 있다면, ASA에서는 백플레인 인터페이스에서 모듈의 상태를 모니터링합니다. 모듈의 오류를 유닛 오류로 간주하고 장애 조치를 시작합니다. 이 설정은 구성 가능합니다.

인터페이스에 구성된 IPv4 및 IPv6 주소가 없는 경우 ASA에서는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다. 인터페이스에 IPv6 주소만 구성되어 있으면 ASA에서는 ARP 대신 IPv6 네이버 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 ping 테스트의 경우 ASA에서는 IPv6 모든 노드 주소를 사용합니다(FE02::1).

참고 오류가 발생한 유닛에서 복구가 이루어지지 않고 오류가 발생해서는 안 되는 유닛일 경우 **failover reset** 명령을 입력하여 상태를 재설정할 수 있습니다. 그러나 장애 조치 상태가 지속되면 유닛에 다시 오류가 발생합니다.

인터페이스 테스트

ASA에서는 다음과 같은 인터페이스 테스트를 사용합니다. 각 테스트 시간은 기본적으로 1.5초이며, 페일오버 인터페이스 대기 시간의 경우에는 1/16초입니다(**Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **Failover(**페일오버**)** > **Criteria(**기준**)** > **Failover Poll Times(**페일오버 폴링 시간**)**참조).

1. 링크 작동/중단 테스트 - 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 중단되었는지 여부를 나타내며, ASA에서는 이 상태를 실패로 간주하고 테스트를 중단합니다. 작동 상태일 경우 ASA에서는 네트워크 활동 테스트를 수행합니다.
2. 네트워크 활동 테스트 - 수신된 네트워크 활동 테스트입니다. 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 유닛에서 테스트 도중 적합한 패킷을 수신하는 즉시, 인터페이스는 작동 중으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛에서도 트래픽을 수신하지 못하면, ASA에서는 ARP 테스트를 시작합니다.
3. ARP 테스트 - 성공적인 ARP 응답에 대한 테스트입니다. 각 유닛은 ARP 테이블의 가장 최근 항목에 있는 IP 주소에 대한 단일 ARP 요청을 전송합니다. 유닛이 테스트 중에 ARP 응답이나 기타 네트워크 트래픽을 수신한다면, 인터페이스는 작동하는 것으로 간주됩니다. 유닛이 ARP 회신을 수신하지 못한다면, ASA는 ARP 테이블의 다음 항목에 있는 IP 주소에 대한 단일 ARP 요청을 전송합니다. 유닛이 테스트 중에 ARP 응답이나 기타 네트워크 트래픽을 수신한다면, 인터페이스는 작동하는 것으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛에서도 트래픽을 수신하지 못하면, ASA에서는 Broadcast Ping(브로드캐스트 핑) 테스트를 시작합니다.

4. Broadcast Ping(브로드캐스트 핑) 테스트 - 성공적인 핑 회신에 대한 테스트입니다. 각 유닛은 브로드캐스트 핑을 보낸 다음 수신된 모든 패킷을 계산합니다. 유닛이 테스트 도중 패킷을 수신하면, 인터페이스는 작동 중으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛도 트래픽을 수신하지 않으면, 테스트는 ARP 테스트와 함께 다시 시작됩니다. 두 유닛 모두 ARP 및 Broadcast Ping(브로드캐스트 핑) 테스트에서 트래픽을 계속 수신하지 못하면, 테스트는 영구적으로 계속 실행됩니다.

인터페이스 상태

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- Normal - 인터페이스를 트래픽을 받는 중입니다.
- Testing - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- Link Down - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- No Link - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- Failed - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

장애 조치 시간

다음 이벤트는 Firepower 고가용성 쌍에서 페일오버를 트리거합니다.

- 활성 유닛의 Snort 인스턴스 중 50 % 이상이 다운되었습니다.
- 활성 유닛의 디스크 공간이 90 % 이상 찼습니다.
- **no failover active(**활성 페일오버 없음**)** 명령이 활성 유닛에서 실행되거나 **failover active(**활성 페일오버**)** 명령이 대기 유닛에서 실행됩니다.
- 대기 유닛보다 활성 유닛에 더 많은 실패 인스턴스가 있습니다.
- 활성 디바이스의 인터페이스 오류가 구성된 임계 값을 초과합니다.

  기본적으로 하나의 인터페이스에 오류가 발생하면 페일오버가 실행됩니다. 인터페이스 수에 대한 임계값 또는 페일오버가 발생하기 위해 실패해야 하는 모니터링되는 인터페이스의 백분율을 구성하여 기본값을 변경할 수 있습니다. 활성 디바이스에서 임계값이 위반되면 페일오버가 발생합니다. 대기 디바이스에서 임계값 위반이 발생하면 유닛은 **Fail(**실패**)** 상태로 전환됩니다.

  기본 페일오버 기준을 변경하려면 전역 구성 모드에서 다음 명령을 입력합니다.

표 *76:*

명령어	목적
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	기본 페일오버 기준을 변경합니다. 인터페이스의 특정 개수를 지정할 경우, *num* 인수의 지원되는 범위는 1에서 250까지입니다. 인터페이스의 백분율을 지정할 경우 *num* 인수의 지원되는 범위는 1에서 100까지입니다.

표 *77: ASA*

장애 조치 조건	최소	기본	최대
활성 유닛의 전원이 끊기거나, 하드웨어가 다운되거나, 소프트웨어가 다시 로드되거나 충돌합니다. 이러한 상황이 발생하면 모니터링되는 인터페이스 또는 페일오버 링크에서 hello 메시지를 수신하지 않습니다.	800밀리초	15초	45초
액티브 유닛 메인 보드 인터페이스 의 연결이 해제됩니다.	500밀리초	5초	15초
액티브 유닛 4GE 모듈 인터페이스 링크가 중단됩니다.	2초	5초	15초
액티브 유닛 FirePOWER 모듈에 장애가 발생합니다.	2초	2초	2초
액티브 유닛 인터페이스가 작동하지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

액티브/스탠바이 페일오버 정보

액티브/스탠바이 페일오버에서는 스탠바이 Firepower Threat Defense 디바이스를 사용해 장애가 발생한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛에 장애가 발생하는 경우 스탠바이 유닛이 액티브 유닛이 됩니다.

기본/보조 역할 및 액티브/스탠바이 상태

페일오버 쌍의 두 유닛의 주된 차이점은 어느 유닛이 액티브 유닛이고 어느 유닛이 스탠바이 유닛인지와 관련 있습니다. 즉, 어떤 IP 주소를 사용하고 어떤 유닛이 트래픽을 능동적으로 전달하는지에 달려 있습니다.

그러나 유닛 간의 몇몇 차이점은 어느 유닛이 기본(컨피그레이션에 지정된 사항에 따라) 유닛이고 어느 유닛이 보조 유닛인지에 따라서도 결정됩니다.

- 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.
- 기본 유닛의 MAC 주소는 액티브 IP 주소와 항상 연계됩니다. 보조 유닛이 액티브 유닛이 되고 페일오버 링크를 통해 기본 유닛의 MAC 주소를 획득할 수 없는 경우에는 이러한 규칙에 예외가 발생합니다. 이 경우 보조 유닛의 MAC 주소가 사용됩니다.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 스탠바이 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 스탠바이 유닛이 됩니다.

페일오버 이벤트

액티브/스탠바이 페일오버 시 페일오버는 유닛을 기준으로 실행됩니다.

다음 표에서는 각 페일오버 이벤트에 대한 페일오버 작업을 보여줍니다. 이 표에는 각 페일오버 이벤트에 적용되는 페일오버 정책(페일오버 실행 또는 페일오버 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 페일오버 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 ***78:*** 페일오버 이벤트

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 페일오버 링크에 대한 hello 메시지가 수신되지 않음
이전 액티브 유닛 복구	페일오버 없음	스탠바이 상태가 됨	작업 없음	없음

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
스탠바이 유닛 오류(전력 또는 하드웨어)	페일오버 없음	스탠바이가 실패한 것으로 표시됨	해당 없음	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
작동 중 페일오버 링크에 오류 발생	페일오버 없음	페일오버 링크가 실패한 것으로 표시됨	페일오버 링크가 실패한 것으로 표시됨	페일오버가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버를 시작하지 못하므로 최대한 빨리 페일오버 링크를 복구해야 합니다.
시작 시 페일오버 링크에 오류 발생	페일오버 없음	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	시작 시 페일오버 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	페일오버 없음	작업 없음	작업 없음	페일오버가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	페일오버	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	페일오버 없음	작업 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

고가용성 요구 사항 및 전제 조건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

Network Admin(네트워크 관리자)

고가용성 지침

모델 지원

- Firepower 1010:
  - 고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 및 스탠바이 유닛에서 계속 트래픽을 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하기 위해 고안되었지만 스위치 포트로 확장되지는 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다. 이론적으로는 VLAN에 단일 스위치 포트를 배치하고 고가용성을 정상적으로 사용할 수 있지만, 물리적 방화벽 인터페이스를 대신 사용하면 더 간단하게 설정할 수 있습니다.
  - 방화벽 인터페이스만 장애 조치 링크로 사용할 수 있습니다.

  참고 버전 6.5 이상이 Firepower Management Center 버전 6.5 이상에서 새로 설치하고 관리하는 Firepower 1010 디바이스에서 기본 인터페이스는 스위치 포트 유형이 됩니다. 스위치 포트 기능은 페일오버에 지원되지 않으므로 해당 인터페이스에서 스위치 포트를 끄고 구축을 수행한 다음 페일오버를 생성합니다. 6.5 이전 버전에서 업그레이드된 Firepower 1010 시스템의 경우, 기본 인터페이스는 이전 버전과 동일합니다.

- Microsoft Azure 및 Amazon Web Services와 같은 퍼블릭 클라우드 네트워크에 있는 Firepower Threat Defense Virtual에서는 Layer 2 연결이 필요하기 때문에 고가용성를 통해 지원되지 않습니다.

추가 지침

- 액티브 유닛에서 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30초 ~ 50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하기 위해 스위치에서 STP PortFast 기능을 활성화할 수 있습니다.

interface *interface_id* **spanning-tree portfast**

이 해결 방법은 라우팅 모드 및 브리지 그룹 인터페이스에 모두 연결된 스위치에 적용됩니다. PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 로컬 CA 서버가 구성된 경우 장애 조치를 활성화할 수 없습니다. **no crypto ca server** 명령을 사용하여 CA 구성을 제거합니다.
- Firepower Threat Defense 장애 조치 쌍에 연결된 스위치에서 포트 보안을 구성할 경우 장애 조치 이벤트가 발생할 때 통신에 문제가 생길 수 있습니다. 이러한 문제는 한 보안 포트에서 구성하거나 확보한 보안 MAC 주소가 다른 보안 포트로 이동될 경우 발생하며, 스위치 포트 보안 기능에 의해 위반 여부가 플래그로 표시됩니다.
- 액티브/스탠바이 고가용성 및 VPN IPsec 터널의 경우, VPN 터널을 통해 SNMP를 사용하여 액티브 유닛과 스탠바이 유닛을 모두 모니터링할 수는 없습니다. 스탠바이 유닛에는 활성 VPN 터널이 없으며 NMS로 전송되는 트래픽은 삭제됩니다. 암호화 기능이 있는 SNMPv3을 대신 사용하면 IPsec 터널을 사용하지 않아도 됩니다.

Firepower Threat Defense 고가용성 쌍 추가

액티브/스탠 바이 고가용성 쌍을 설정하는 경우 하나를 기본 디바이스로 지정하고 다른 하나를 보조 디바이스로 지정합니다. 시스템은 페어링된 디바이스에 병합된 설정을 적용합니다. 충돌이 있는 경우 기본으로 지정한 디바이스의 설정이 적용됩니다.

다중 도메인 구축의 고가용성 쌍의 디바이스는 동일한 도메인에 속해야 합니다.

참고 스테이트풀 페일오버 링크는 피어 간 애플리케이션 콘텐츠 동기화에 사용되며 시스템은 페일오버 링크로 구성을 동기화합니다. 페일오버 링크와 스테이트풀 페일오버 링크는 사설 IP 공간에 있으며 고가용성 쌍의 피어 간 통신에만 사용됩니다. 고가용성이 설정되면 선택된 인터페이스 링크와 암호화 설정은 고가용성 쌍을 해제하고 재구성하기 전까지 수정할 수 없습니다.

주의 Firepower Threat Defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

시작하기 전에

두 디바이스에 대해 다음을 확인합니다.

- 같은 모델이어야 합니다.
- 인터페이스의 개수와 유형이 동일해야 합니다.
- 동일한 도메인 및 그룹에 포함되어야 합니다.
- 정상 상태이고 동일한 소프트웨어를 실행해야 합니다.
- 라우팅 또는 투명 모드가 필요합니다.
- NTP 구성이 같아야 합니다. Threat Defense를 위한 NTP 시간 동기화 구성, 1463 페이지의 내용을 참조하십시오.
- 커밋되지 않은 변경 사항 없이 완전히 구축되어야 합니다.
- DHCP 또는 PPPoE가 인터페이스에 구성되어 있지 않아야 합니다.

참고 원격 액세스 VPN에 고가용성 기능을 설정할 때 주 디바이스가 CertEnrollment 개체를 사용해 등록한 ID 인증서로 RAVPN 설정을 한 경우 보조 디바이스의 ID 인증서는 동일한 CertEnrollment 개체를 사용해 등록해야 합니다. CertEnrollment 개체는 디바이스별 오버라이드로 인해 주 디바이스 및 보조 디바이스에 다른 값을 가질 수 있습니다. HA를 형성하기 전 두 개의 디바이스에 대해 동일한 CertEnrollment 개체를 보유해야 한다는 제약이 있습니다.

프로시저

단계 **1** FMC에 디바이스 추가, 311 페이지에 따라 Firepower Management Center에 두 디바이스를 추가합니다.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **3** **Add(**추가**)** 드롭다운 메뉴에서 **High Availability(**고가용성**)**을 선택합니다.

단계 **4** 고가용성 쌍에 대한 표시 이름을 입력합니다.

단계 **5** 장치 유형에서 **Firepower Threat Defense**를 선택합니다.

단계 **6** 고가용성 쌍에 기본 피어 디바이스를 선택합니다.

단계 **7** 고가용성 쌍에 보조 피어 디바이스를 선택합니다.

단계 **8** **Continue(**계속**)**를 클릭합니다.

단계 **9** LAN 페일오버 링크에서 페일오버 통신이 충분히 가능한 대역폭이 있는 인터페이스를 선택합니다.

참고 논리적 이름을 갖지 않고 보안 영역에 속하지 않은 인터페이스만 고가용성 쌍 추가 대화상자의 인터페이스 드롭다운 메뉴에 표시됩니다.

단계 **10** 식별된 논리적 이름을 입력합니다.

단계 **11** 액티브 유닛에서 페일오버 링크에 대한 기본 **IP** 주소를 입력합니다. 이 주소는 사용되지 않는 서브넷에 있어야 합니다.

참고 169.254.0.0/16 및 fd00:0:0:*::/64는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.

단계 **12** 필요에 따라 **IPv6** 주소 사용을선택합니다.

단계 **13** 스탠바이 유닛에서 페일오버 링크에 대한 보조 **IP** 주소를 입력합니다. 이 IP 주소는 기본 IP 주소와 동일한 서브넷에 있어야 합니다.

단계 **14** IPv4 주소를 사용하는 경우 기본 및 보조 IP 주소에 적용되는 서브넷 마스크 를 입력합니다.

단계 **15** 필요에 따라 스테이트풀 페일오버 링크에서 동일한 인터페이스를 선택하거나 다른 인터페이스를 선택하고 고가용성 설정 정보를 입력합니다.

참고 169.254.0.0/16 및 fd00:0:0:*::/64는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.

단계 **16** 필요에 따라 활성화를 선택하고 페일오버 링크 간 IPsec 암호화 용 키 생성 방법을 선택합니다.

단계 **17** **OK(**확인**)**를 클릭합니다. 이때 시스템에서 데이터를 동기화하는 데 몇 분 정도 걸립니다.

다음에 수행할 작업

디바이스를 백업하는지 확인합니다. 백업을 이용하면 장애가 발생한 디바이스를 빠르게 교체하고, Firepower Management Center와의 연결을 해제하지 않고도 고가용성 서비스를 복원할 수 있습니다. 자세한 내용은 백업 및 복원, 203 페이지를 참고하십시오.

선택적 고가용성 파라미터 구성

Firepower Management Center에서 초기 고가용성 설정을 볼 수 있습니다. 고가용성 쌍을 해제하고 다시 설정하지 않으면 이러한 설정을 편집할 수 없습니다.

페일오버 결과를 개선하기 위해 페일오버 트리거 기준을 편집할 수 있습니다. 인터페이스 모니터링은 페일오버에 가장 적합한 인터페이스를 결정하도록 합니다.

스탠바이 **IP** 주소 및 인터페이스 모니터링 구성

각 인터페이스에 대한 스탠바이 IP 주소를 설정합니다. 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다.

기본적으로 모니터링은 모든 물리적 인터페이스에서 활성화되며, Firepower 1010에서는 논리적 이름이 구성된 모든 VLAN 인터페이스에서 활성화됩니다. 중요도가 낮은 네트워크에 연결된 인터페이스를 제외하여 페일오버 정책에 영향을 미치지 않도록 하고자 할 수 있습니다. Firepower 1010 스위치 포트는 인터페이스 모니터링에 적용되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **High Availability(**고가용성**)** 탭을 클릭합니다.

단계 **4** 모니터링되는 인터페이스 영역에서 편집하려는 인터페이스 옆의 수정( )를 클릭합니다.

단계 **5** 오류에 대해 이 인터페이스 모니터링 확인란을 선택합니다.

단계 **6** **IPv4** 탭에서 스탠바이 **IP** 주소를 입력합니다.

이 주소는 액티브 IP 주소와 같은 네트워크에 있는 여유 주소여야 합니다.

단계 **7** **IPv6** 탭에서 수동으로 IPv6 주소를 구성하는 경우 액티브 IP 주소 옆의 수정( )를 클릭하고 스탠바이 **IP** 주소를 입력한 뒤 **OK**를 클릭합니다.

이 주소는 액티브 IP 주소와 같은 네트워크에 있는 여유 주소여야 합니다. 자동으로 생성되거나 **EUI 64** 강제 적용된 주소의 경우 스탠바이 주소가 자동으로 생성됩니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

고가용성 페일오버 기준 수정

네트워크 구축에 따라 페일오버 기준을 사용자 정의할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** **Failover Trigger Criteria(**페일오버 트리거 기준**)** 옆의 수정( )을(를) 클릭합니다.

단계 **5** **Interface Failure Threshold(**인터페이스 페일오버 임계값**)**에서 디바이스 페일오버 이전에 오류가 발생해야 하는 인터페이스의 수 또는 비율을 선택합니다.

단계 **6** **Hello** 패킷 간격**(Hello** 패킷 간격**)**에서 페일오버 링크에 보낼 Hello 패킷 수를 선택합니다.

참고 Firepower 2100에서 원격 액세스 VPN을 사용한다면, 기본 Hello 패킷 간격을 사용합니다. 그렇지 않으면 높은 CPU 사용량 때문에 페일오버가 발생할 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

가상 MAC 주소 구성

Firepower Management Center의 두 위치에서 페일오버에 대해 액티브 및 스탠바이 MAC 주소를 구성할 수 있습니다.

- 인터페이스 구성 중 인터페이스 편집 내 고급 탭에 대한 설명은 MAC 주소 구성, 838 페이지의 내용을 참조하십시오.
- 고가용성 페이지에서 액세스한 인터페이스 MAC 주소 추가는 참조합니다.

액티브 및 스탠바이 MAC 주소가 두 위치에 구성되면 페일오버 시 인터페이스 구성 중 설정한 주소가 우선됩니다.

물리적 인터페이스에 액티브 및 스탠바이 MAC 주소를 지정하여 페일오버 중 트래픽 손실을 최소화할 수 있습니다. 이 기능은 페일오버에 대한 IP 주소 매핑의 이중화를 제공합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 인터페이스 MAC 주소 옆의 추가( )을 선택합니다.

단계 **5** 물리적 인터페이스를 선택합니다.

단계 **6** 액티브 인터페이스 **MAC** 주소를 입력합니다.

단계 **7** 스탠바이 인터페이스 **MAC** 주소를 입력합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Manage(관리) 고가용성

이 섹션에서는 고가용성를 활성화한 다음, 고가용성 유닛을 관리하는 방법을 설명합니다. 고가용성 설정을 변경하고 한 유닛에서 다른 유닛으로의 장애 조치를 강제로 수행하는 방법도 알아봅니다.

Firepower Threat Defense 고가용성 쌍의 활성 피어 전환

Firepower Threat Defense 고가용성 쌍을 설정하면 액티브 및 스탠바이 유닛을 수동으로 전환할 수 있으며 현재 액티브 유닛의 영구 오류 또는 상태 이벤트 시 페일오버를 효과적으로 강제할 수 있습니다. 이 절차를 완료하기 전 두 유닛이 모두 완전히 구축되어야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 액티브 피어를 변경할 고가용성 쌍 옆에 있는 **Switch Active Peer(**액티브 피어 전환**)**를 클릭합니다.

단계 **3** 다음 작업을 수행할 수 있습니다.

- **Yes(**예**)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.
- 취소하고 디바이스 관리 페이지로 돌아가려면 아니오를 클릭합니다.

고가용성 일시 중단 또는 재개

고가용성 쌍의 유닛을 일시 중단할 수 있습니다. 이렇게 하면 다음과 같은 경우에 유용합니다.

- 두 유닛이 모두 액티브-액티브인 상태에서 페일오버 링크의 통신을 수정해도 문제가 해결되지 않는 경우.
- 액티브 또는 스탠바이 유닛을 트러블슈팅하고 트러블슈팅 중에는 유닛을 페일오버하지 않으려는 경우.

고가용성을 일시 중단하면 디바이스 쌍이 더 이상 페일오버 유닛으로 동작하지 않게 됩니다. 현재 액티브 디바이스는 액티브 상태로 유지되어 모든 사용자 연결을 처리합니다. 그러나 페일오버 기준은 더 이상 모니터링되지 않으며 시스템은 현재 의사 스탠바이 디바이스로 페일오버되지 않습니다. 스탠바이 디바이스의 컨피그레이션은 보존되지만 해당 디바이스는 비활성 상태로 유지됩니다.

HA 일시 중단과 해제의 주요 차이점은 일시 중단된 HA 디바이스에서는 고가용성 컨피그레이션이 보존된다는 것입니다. 반면 HA를 해제하면 컨피그레이션이 지워집니다. 따라서 일시 중단된 시스템에서 HA를 다시 시작하는 옵션이 제공됩니다. 그러면 기존 컨피그레이션이 활성화되며 두 디바이스가 다시 페일오버 쌍으로 작동합니다.

HA를 일시 중단하려면 **configure high-availability suspend** 명령을 사용합니다.

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

액티브 유닛에서 고가용성을 일시 중단하면 액티브 유닛과 스탠바이 유닛 둘 다에서 컨피그레이션이 일시 중단됩니다. 스탠바이 유닛에서 고가용성을 일시 중단하는 경우에는 스탠바이 유닛에서만 고가용성이 일시 중단되며 액티브 유닛은 일시 중단된 유닛으로의 페일오버를 시도하지 않습니다.

페일오버를 재시작하려면 **configure high-availability resume** 명령을 사용합니다.

```
> configure high-availability resume
```

```
Successfully resumed high-availablity.
```

Suspended(일시 중단됨) 상태인 유닛만 다시 시작할 수 있습니다. 이 유닛은 피어 유닛과 액티브/스탠바이 상태를 협상합니다.

참고 고가용성 일시 중단은 임시 상태입니다. 유닛을 다시 불러오면 고가용성 구성을 자동으로 재시작하고 피어와 액티브/스탠바이 상태 협상을 시작합니다.

FTD 고가용성 쌍의 유닛 교체

백업 파일을 사용하여 Firepower Threat Defense 고가용성 쌍에서 장애가 발생한 유닛을 교체하려면 Firepower 어플라이언스 복구, 218 페이지의 내용을 참조하십시오.

장애가 발생한 디바이스의 백업이 없는 경우 고가용성을 해제해야 합니다. 그런 다음 Firepower Management Center에 교체 디바이스를 등록하고 고가용성을 다시 설정합니다. 이 프로세스는 디바이스가 기본 디바이스인지 보조 디바이스인지에 따라 달라집니다.

- 기본 FTD HA 유닛을 백업 없이 교체, 912 페이지
- 보조 FTD HA 유닛을 백업 없이 교체, 913 페이지

기본 FTD HA 유닛을 백업 없이 교체

Firepower Threat Defense 고가용성 쌍에서 장애가 발생한 기본 유닛을 교체하려면 다음 단계를 수행합니다. 다음 단계를 수행하지 않으면 기존 고가용성 설정을 오버라이트할 수 있습니다.

주의 Firepower Threat Defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

프로시저

단계 **1** 고가용성 쌍을 분리하기 위해 강제 해제를 선택합니다. 고가용성 쌍의 유닛 분리, 914 페이지를 참조하십시오.

참고 중단 작업은 Firepower Threat Defense 및 Firepower Management Center에서 HA와 관련된 모든 구성을 제거하며, 나중에 수동으로 다시 생성해야 합니다. 동일한 HA 쌍을 설정하려면 HA 중단 작업을 실행하기 전에 모든 인터페이스/하위 인터페이스의 IP, MAC 주소, 모니터링 설정을 저장해야 합니다.

단계 2 Firepower Management Center에서 오류가 발생한 기본 Firepower Threat Defense 유닛의 등록을 해제하려면 FMC에서 디바이스 삭제, 315 페이지을 참조하십시오.

단계 3 Firepower Management Center에 Firepower Threat Defense을 교체 등록하려는 경우 FMC에 디바이스 추가, 311 페이지을 참조하십시오.

단계 4 등록 시 기존 보조/액티브 유닛을 기본 디바이스로 사용하고 교체 디바이스를 보조/스탠바이 디바이스로 하여 고가용성을 구성하려면 Firepower Threat Defense 고가용성 쌍 추가, 906 페이지을 참조하십시오.

보조 FTD HA 유닛을 백업 없이 교체

Firepower Threat Defense 고가용성 쌍에서 장애가 발생한 보조 유닛을 교체하려면 다음 단계를 수행합니다.

주의 Firepower Threat Defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

프로시저

단계 1 고가용성 쌍을 분리하기 위해 강제 해제를 선택합니다. 고가용성 쌍의 유닛 분리, 914 페이지를 참조하십시오.

참고 중단 작업은 Firepower Threat Defense 및 Firepower Management Center에서 HA와 관련된 모든 구성을 제거하며, 나중에 수동으로 다시 생성해야 합니다. 동일한 HA 쌍을 설정하려면 HA 중단 작업을 실행하기 전에 모든 인터페이스/하위 인터페이스의 IP, MAC 주소, 모니터링 설정을 저장해야 합니다.

단계 2 Firepower Management Center에서 Firepower Threat Defense 보조 디바이스의 등록을 해제합니다. FMC에서 디바이스 삭제, 315 페이지을 참조하십시오.

단계 3 Firepower Management Center에 Firepower Threat Defense의 교체 디바이스를 등록합니다. FMC에 디바이스 추가, 311 페이지을 참조하십시오.

단계 4 등록 시 기존 기본/액티브 유닛을 기본 디바이스로 사용하고 교체 디바이스를 보조/스탠바이 디바이스로 하여 고가용성을 구성하려면 Firepower Threat Defense 고가용성 쌍 추가, 906 페이지을 참조하십시오.

고가용성 쌍의 유닛 분리

고가용성 쌍을 해제하는 경우 액티브 디바이스는 전체 구축된 기능을 유지합니다. 스탠바이 디바이스는 페일오버 및 인터페이스 구성을 잃고 독립형 디바이스가 됩니다. Firepower Management Center는 고가용성 라이선스를 내보내고 독립형 디바이스의 개별 라이선스로 교체합니다. 고가용성 쌍을 해제하기 전 해제 작업 이전에 액티브 디바이스에 구축된 정책은 해제 작업이 완료되면 자동으로 구축됩니다.

팁 FlexConfig 정책은 예외입니다. 액티브 디바이스에 구축된 FlexConfig 정책은 HA 해제 작업 완료 후 구축 실패를 표시할 수 있습니다. FlexConfig 정책을 변경하고 액티브 디바이스에 다시 구축해야 합니다.

참고 Firepower Management Center을 사용해 고가용성 쌍에 연결할 수 없는 경우 **configure high-availability disable** CLI 명령을 사용하여 두 디바이스에서 페일오버 설정을 제거해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 해제하려는 고가용성 쌍 옆의 **Break HA(HA** 해제**)**를 클릭합니다.

단계 **3** 스탠바이 피어가 응답하지 않고 필요한 경우 강제 해제 확인란을 선택합니다.

단계 **4** **Yes(**예**)**를 클릭합니다. 디바이스 고가용성 쌍이 분리됩니다.

해제 작업은 액티브 및 스탠바이 디바이스에서 페일오버 설정을 제거합니다.

다음에 수행할 작업

(선택 사항) 액티브 디바이스에서 flex-config 정책을 사용하는 경우 구축 오류를 제거하기 위해 flex-config 정책을 변경하고 다시 구축합니다.

고가용성 쌍 등록 해제

Firepower Management Center에서 쌍을 삭제하고 CLI를 사용해 각 유닛에서 고가용성을 비활성화할 수 있습니다.

시작하기 전에

이 절차에서는 CLI 액세스가 필요합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 등록을 취소하려는 고가용성 쌍 옆의 삭제( )을 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭합니다. 디바이스 고가용성 쌍이 삭제됩니다.

단계 **4** 각 유닛에서 Firepower Threat Defense CLI에 액세스하고 다음 명령을 입력합니다.

configure high-availability disable

이 명령을 입력하지 않으면 유닛을 다시 등록하고 새로운 HA 쌍을 형성할 수 없습니다.

참고 방화벽 모드를 변경하기 전에 이 명령을 입력하십시오. 모드를 변경하면 유닛은 **configure high-availability disable** 명령의 입력을 거부할 것이며 Firepower Management Center은 이 명령을 사용하지 않으면 HA 쌍으로 재구성되지 않습니다.

모니터링 고가용성

이 섹션에서는 고가용성 상태를 모니터링할 수 있습니다.

페일오버 기록 보기

두 개의 고가용성 디바이스의 페일오버를 단일 보기에서 볼 수 있습니다. 시간 순으로 표시되며 페일오버의 이유를 표시합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 요약을 선택합니다.

단계 **4** General(일반)에서 보기 ( )을 클릭합니다.

스테이트풀 페일오버 통계 보기

고가용성 쌍의 기본 및 보조 디바이스에 대한 스테이트풀 고가용성 링크 통계를 볼 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** Stateful Failover Link(스테이트풀 페일오버 링크)에서 보기 ( )를 클릭합니다.

단계 **5** 통계를 보려는 디바이스를 선택합니다.

35 장

Firepower Threat Defense 클러스터링

클러스터링을 사용하면 여러 개의 FTD를 하나의 논리적 디바이스로 그룹화할 수 있습니다. FTD 디바이스의 클러스터링은 Firepower 9300과 Firepower 4100 Series에서 지원합니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

참고 클러스터링을 사용할 경우 일부 기능이 지원되지 않습니다. 클러스터링으로 지원되지 않는 기능, 959 페이지의 내용을 참조하십시오.

- Firepower 4100/9300 섀시 클러스터링 정보, 917 페이지
- 클러스터링용 라이선스, 922 페이지
- 클러스터링의 요구 사항 및 사전 요구 사항, 923 페이지
- 클러스터링 지침 및 제한 사항, 926 페이지
- 클러스터링 설정, 930 페이지
- FXOS: 클러스터 유닛 제거, 950 페이지
- FMC: 클러스터 멤버 관리, 952 페이지
- FMC: 클러스터 모니터링, 958 페이지
- 클러스터링에 대한 참조, 959 페이지
- 클러스터링 기록, 970 페이지

Firepower 4100/9300 섀시 클러스터링 정보

클러스터는 단일 논리적 유닛으로 작동하는 여러 개의 디바이스로 구성됩니다. Firepower 4100/9300 섀시에서 클러스터를 구축할 때는 다음 작업이 수행됩니다.

- 네이티브 인스턴스 클러스터링의 경우: 유닛 간 통신에 사용되는 클러스터 제어 링크(기본값: port-channel 48)를 생성합니다.

  다중 인스턴스 클러스터링의 경우에는 하나 이상의 클러스터 유형 Etherchannel에서 하위 인터페이스를 사전 구성해야 합니다. 각 인스턴스에는 자체 클러스터 제어 링크가 필요 합니다.

섀시 내 클러스터링(Firepower 9300 전용)의 경우, 이 링크는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다.

섀시 간 클러스터링의 경우, 섀시 간의 통신을 위해 물리적 인터페이스를 이 EtherChannel에 수동으로 할당해야 합니다.

- 애플리케이션 내부에 클러스터 부트스트랩 구성을 생성합니다.

  클러스터를 구축할 때, 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다.

- 데이터 인터페이스를 *Spanned* 인터페이스로 클러스터에 할당합니다.

  섀시 내 클러스터링의 경우, 스팬 인터페이스는 섀시 간 클러스터링과 마찬가지로 EtherChannel에 국한되지 않습니다. Firepower 9300 수퍼바이저는 EtherChannel 기술을 내부에 사용하여 트래픽을 공유 인터페이스의 다중 모듈에 로드 밸런싱하므로 모든 데이터 인터페이스 유형이 Spanned(스팬) 모드에서 작동합니다. 섀시 간 클러스터링의 경우, 모든 데이터 인터페이스에 Spanned EtherChannel을 사용해야 합니다.

  참고 개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

- 관리 인터페이스를 클러스터의 모든 유닛에 할당합니다.

다음 섹션에서는 클러스터링 개념 및 구현에 대한 자세한 정보를 제공합니다. 클러스터링에 대한 참조, 959 페이지 섹션도 참조하십시오.

부트스트랩 컨피그레이션

클러스터를 구축할 때, Firepower 4100/9300 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다.

클러스터 멤버

클러스터 멤버는 보안 정책 및 트래픽 흐름을 공유하기 위해 서로 연동됩니다.

클러스터의 멤버 중 하나는 제어 유닛입니다. 제어 유닛은 자동으로 결정됩니다. 다른 모든 멤버는 데이터 유닛입니다.

모든 설정은 제어 유닛에서만 수행되어야 하며, 이후 설정이 데이터 유닛에 복제됩니다.

일부 기능은 클러스터로 확장되지 않으며, 제어 유닛에서 이러한 기능에 대한 모든 트래픽을 처리합니다. 의 내용을 참조하십시오.클러스터링을 위한 중앙 집중식 기능, 960 페이지의 내용을 참조하십시오.

Cluster Control Link

네이티브 인스턴스 클러스터링의 경우: 클러스터 제어 링크는 Port-channel 48 인터페이스를 사용하여 자동으로 생성됩니다.

다중 인스턴스 클러스터링의 경우에는 하나 이상의 클러스터 유형 Etherchannel에서 하위 인터페이스를 사전 구성해야 합니다. 각 인스턴스에는 자체 클러스터 제어 링크가 필요 합니다.

섀시 내 클러스터링의 경우, 이 인터페이스에는 멤버 인터페이스가 없습니다. 이 클러스터 유형 EtherChannel은 인트라 섀시 클러스터링(intra-chassis clustering)을 위한 클러스터 통신에 Firepower 9300 백플레인을 활용합니다. 섀시 간 클러스터링의 경우에는 EtherChannel에 인터페이스를 하나 이상 추가해야 합니다.

2-멤버 섀시 간 클러스터의 경우 클러스터 제어 링크를 한 섀시에서 다른 섀시로 직접 연결하지 마십시오. 인터페이스에 직접 연결할 경우, 유닛 하나에 오류가 발생하면 클러스터 제어 링크에도 오류가 발생하므로 나머지 정상 유닛에도 오류가 발생합니다. 스위치를 통해 클러스터 제어 링크를 연결할 경우 클러스터 제어 링크는 가동 상태를 유지하여 정상 유닛을 지원합니다.

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

섀시 간 클러스터링을 위한 클러스터 제어 링크 크기 조정

가능한 경우, 각 섀시의 예상 처리량에 맞게 클러스터 제어 링크의 크기를 조정하여 클러스터 제어 링크가 최악의 시나리오를 처리할 수 있게 해야 합니다.

클러스터 제어 링크 트래픽은 주로 상태 업데이트 및 전달된 패킷으로 구성되어 있습니다. 클러스터 제어 링크의 트래픽 양은 언제든지 달라질 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예를 들면 다음과 같습니다.

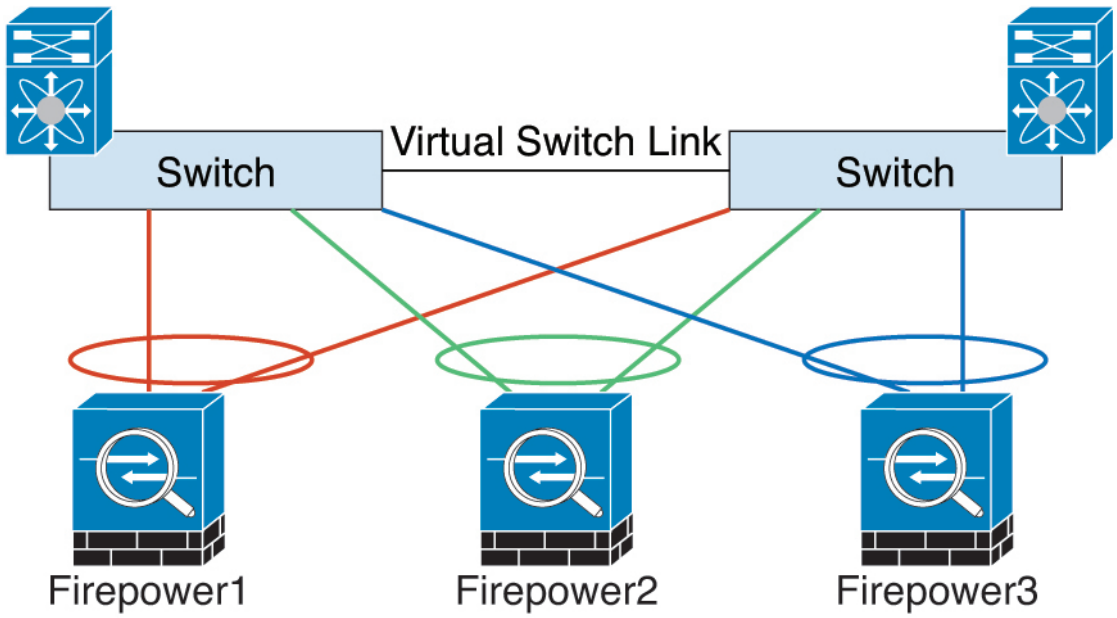
- NAT의 경우 연결의 로드 밸런싱이 저하되며, 모든 반환 트래픽을 올바른 유닛으로 다시 밸런싱해야 합니다.
- 멤버가 변경된 경우, 클러스터에서는 다량의 연결을 다시 밸런싱해야 하므로 일시적으로 많은 양의 클러스터 제어 링크 대역폭을 사용합니다.

대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.

참고 클러스터에 비대칭(다시 밸런싱된) 트래픽이 많은 경우 클러스터 제어 링크 크기를 늘려야 합니다.

섀시 간 클러스터링을 위한 클러스터 제어 링크 이중화

다음 다이어그램에는 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel) 환경에서 EtherChannel을 클러스터 제어 링크로 사용하는 방법이 나와 있습니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 VSS 또는 vPC의 일부일 경우 동일한 EtherChannel 내에 있는 Firepower 9300 섀시 인터페이스를 연결하여 VSS 또는 vPC의 스위치를 별도로 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 스팬 EtherChannel입니다.



섀시 간 클러스터링을 위한 클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(round-trip time)가 20ms 이하여야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선하는 역할을 합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축의 경우 전용 링크를 사용해야 합니다.

클러스터 제어 링크 네트워크

Firepower 4100/9300 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id*.*slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 일반적으로 같은 EtherChannel의 다른 VLAN 하위 인터페이스를 사용하는 다중 인스턴스 클러스터의 경우 VLAN 분리로 인해 서로 다른 클러스터에 같은 IP 주소를 사용할 수 있습니다. 클러스터 제어 링크 네트워크는 유닛 간에 라우터를 포함할 수 없으며 레이어 2 스위칭만 허용됩니다.

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결할 것을 권장합니다. 이 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

관리 인터페이스

클러스터에 관리 유형 인터페이스를 할당해야 합니다. 이 인터페이스는 Spanned 인터페이스와는 다른 특수 개별 인터페이스입니다. 관리 인터페이스를 사용하면 각 유닛에 직접 연결할 수 있습니다. 논리적 관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스

는 디바이스를 Firepower Management Center에 설치하고 등록하는 데 사용됩니다. 또한 하고 자체 로컬 인증, IP 주소 및 정적 라우팅을 사용합니다. 각 클러스터 멤버는 부트스트랩 설정의 일부로 설정하는 관리 네트워크에 별도 IP 주소를 사용합니다.

관리 인터페이스는 논리적 관리 인터페이스와 논리적 진단 인터페이스 간에 공유됩니다. 논리적 진단 인터페이스는 선택 사항이며 부트스트랩 설정의 일부로 구성되어 있지 않습니다. 진단 인터페이스는 다른 데이터 인터페이스와 함께 구성할 수 있습니다. 진단 인터페이스를 설정하기로 선택하면 기본 클러스터 IP 주소를 현재 제어 유닛에 항상 속해 있는 클러스터의 고정 주소로 설정할 수 있습니다. 주소의 범위를 설정하여 현재 제어 유닛을 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소는 하나의 주소에 지속적인 진단 액세스를 제공합니다. 제어 유닛이 변경되면 기본 클러스터 IP 주소는 새 제어 유닛으로 이동하므로 클러스터에 지속적으로 원활하게 액세스할 수 있습니다. TFTP 또는 시스템 로그 같은 아웃바운드 관리 트래픽의 경우, 제어 유닛을 비롯한 각 유닛에서는 로컬 IP 주소를 사용하여 서버에 연결합니다.

클러스터 인터페이스

인트라 섀시 클러스터링의 경우, 클러스터에 물리적 인터페이스 또는 Etherchannel(포트 채널)을 할당할 수 있습니다. 클러스터에 할당된 인터페이스는 클러스터의 모든 멤버에 대해 트래픽의 로드 밸런싱을 수행하는 Spanned 인터페이스입니다.

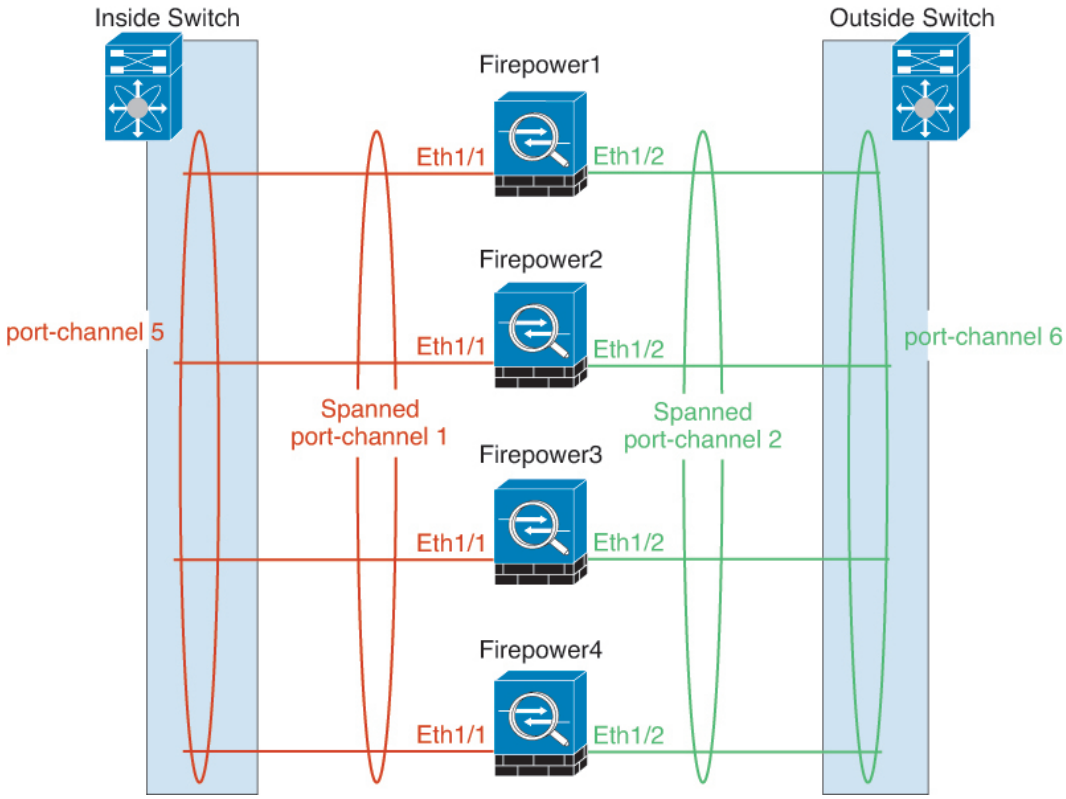
섀시 간 클러스터링의 경우 클러스터에 데이터 Etherchannel만 할당할 수 있습니다. Spanned EtherChannel은 각 섀시에 동일한 멤버 인터페이스를 포함합니다. 업스트림 스위치에서 모든 인터페이스는 단일 EtherChannel에 포함되므로 스위치는 인터페이스가 여러 디바이스와 연결되었는지 알지 못합니다.

개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

Spanned EtherChannels

섀시당 하나 이상의 인터페이스를 클러스터 내의 모든 섀시를 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 스팬 EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 브리지 그룹 멤버 인터페이스가 아닌 BVI에 IP 주소가 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.

다중 인스턴스 클러스터의 경우 각 클러스터에 전용 데이터 EtherChannel이 필요하며 공유 인터페이스 또는 VLAN 하위 인터페이스를 사용할 수 없습니다.



VSS 또는 vPC에 연결

인터페이스에 이중화를 제공하기 위해 Etherchannel을 VSS 또는 vPC에 연결하는 것이 좋습니다.

구성 복제

클러스터의 모든 유닛에서는 단일 구성을 공유합니다. 기본 유닛에서는 컨피그레이션만 변경할 수 있으며 변경 사항은 클러스터의 모든 다른 유닛에 자동으로 동기화됩니다.

클러스터링용 라이선스

FTD은 스마트 라이선싱을 사용합니다. 개별 유닛이 아니라 전체 클러스터에 라이선스를 할당합니다. 그러나 클러스터의 각 유닛은 각 기능에 대한 별도 라이선스를 사용합니다. 클러스터링 기능 자체에는 라이선스가 필요하지 않습니다.

FMC에 클러스터 멤버를 추가하는 경우 클러스터에 사용하려는 기능 라이선스를 지정할 수 있습니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** > **License(**라이선스**)** 영역에서 클러스터에 대한 라이선스를 수정할 수 있습니다.

참고 FMC이 라이선스 되기 전에 (평가 모드에서 실행 되기 전에) 클러스터를 추가하는 경우, FMC를 라이선스하면 클러스터에 정책 변경을 구축할 때 트래픽 중단이 발생할 수 있습니다. 라이선스 모드를 변경하면 모든 데이터 유닛이 클러스터를 벗어났다가 다시 참가합니다.

클러스터링의 요구 사항 및 사전 요구 사항

클러스터 모델 지원

FTD은 다음 모델에서 클러스터링을 지원합니다.

- Firepower 9300 - 클러스터는 유닛을 6개까지 포함할 수 있습니다. 예를 들어 섀시 6개에 모듈 1개, 섀시 3개에 모듈 2개, 또는 모듈을 6개까지 제공하는 어떤 조합도 사용할 수 있습니다. 섀시 내 및 섀시 간 클러스터링 지원
- Firepower 4100 Series- 섀시 간 클러스터링에 최대 유닛 6개 사용 지원

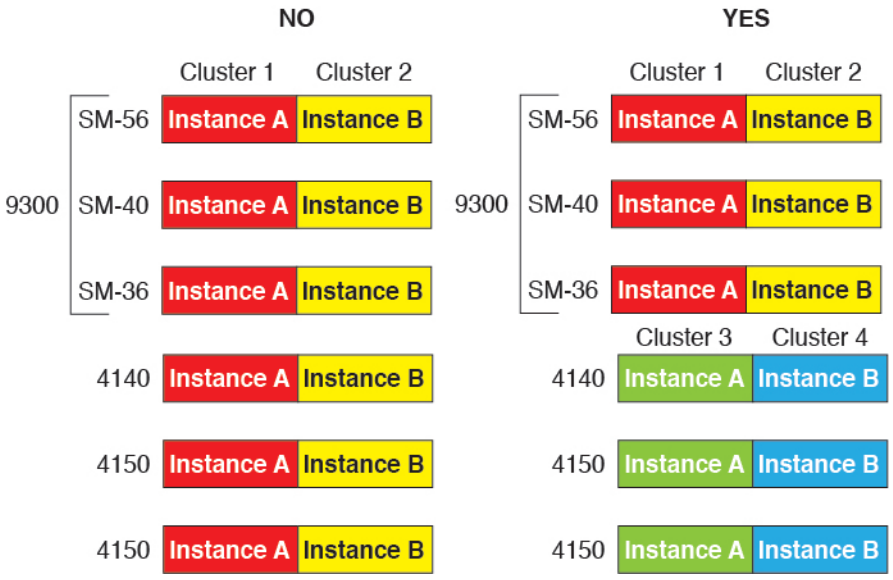
사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

섀시 간 클러스터링 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 섀시:

- 네이티브 인스턴스 클러스터링 - Firepower 4100 시리즈의 경우 모든 섀시가 동일한 모델이어야 합니다. Firepower 9300의 경우: 모든 보안 모듈이 동일한 유형이어야 합니다. 예를 들어 클러스터링을 사용하는 경우 Firepower 9300의 모든 모듈은 SM-40이어야 합니다. 빈 슬롯을 포함하여 섀시에 있는 모든 모듈은 클러스터에 속해야 하지만 각 섀시에 설치된 보안 모듈의 수는 다를 수 있습니다.
- 컨테이너 인스턴스 클러스터링 - 각 클러스터 인스턴스에 동일한 보안 모듈 또는 섀시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 예를 들어 Firepower 9300 SM-56, SM-40, SM-36에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 또는 Firepower 4140 및 4150에서 클러스터를 생성할 수 있습니다.

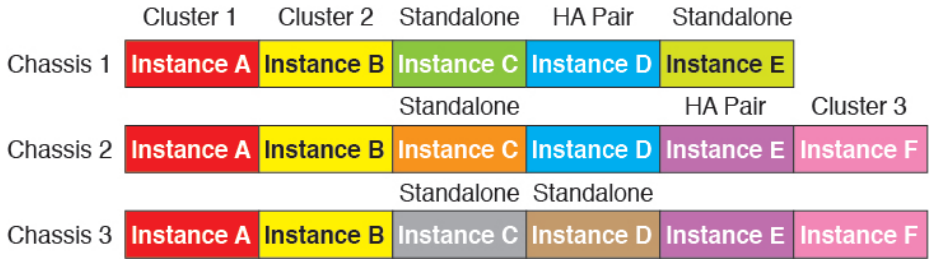


- 이미지 업그레이드 시 동일한 FXOS 소프트웨어 예외를 실행해야 합니다.
- 클러스터에 할당하는 인터페이스에 대한 것과 동일한 인터페이스 구성을 포함해야 합니다(예: EtherChannel, 활성 인터페이스, 속도 및 이중 등). 동일한 인터페이스 ID에 대해 용량이 일치하고 동일한 Spanned EtherChannel에서 성공적인 인터넷 번들링이 가능한 한 섀시에서 서로 다른 네트워크 모듈 유형을 사용할 수 있습니다. 모든 데이터 인터페이스는 섀시 간 클러스터링에서 EtherChannel이어야 합니다. 인터페이스 모듈을 추가 또는 제거하거나 EtherChannel을 설정하는 등의 방법을 통해 클러스터링을 활성화한 후 FXOS에서 인터페이스를 변경하는 경우에는 각 섀시에서 데이터 유닛부터 시작하여 마지막으로 제어 유닛까지 같은 변경을 수행합니다.
- 동일한 NTP 서버를 사용해야 합니다. Firepower Threat Defense의 경우 Firepower Management Center도 동일한 NTP 서버를 사용해야 합니다. 시간을 수동으로 설정해서는 안 됩니다.

멀티 인스턴스 클러스터링 요구 사항

- 모든 내부 보안 모듈/엔진 클러스터링 안 함 - 지정된 클러스터에 대해 보안 모듈/엔진당 단일 컨테이너 인스턴스만 사용할 수 있습니다. 동일한 모듈에서 실행 중인 경우에는 두 컨테이너 인스턴스를 동일한 클러스터에 추가할 수 없습니다.

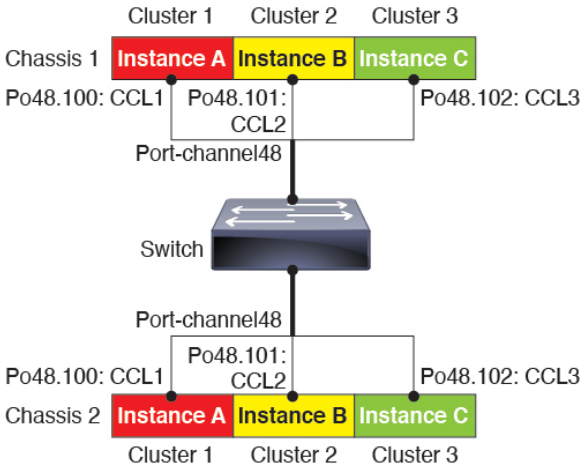
- 클러스터 및 독립형 인스턴스를 혼용 - 보안 모듈/엔진의 모든 컨테이너 인스턴스가 하나의 클러스터에 속할 필요가 없습니다. 일부 인스턴스는 독립형이나 고가용성 유닛으로 사용할 수 있습니다. 동일한 보안 모듈/엔진에서 별도의 인스턴스를 사용해 여러 클러스터를 생성할 수도 있습니다.



- Firepower 9300의 모든 모듈 세 가지는 해당 클러스터에 속해야 합니다 - Firepower 9300의 경우 클러스터에는 모든 3개의 모듈에서 단일 컨테이너 인스턴스가 필요합니다. 모듈 1 및 2의 인스턴스를 사용하여 클러스터를 생성한 다음 모듈 3 또는 예제에서 네이티브 인스턴스를 사용할 수 없습니다.

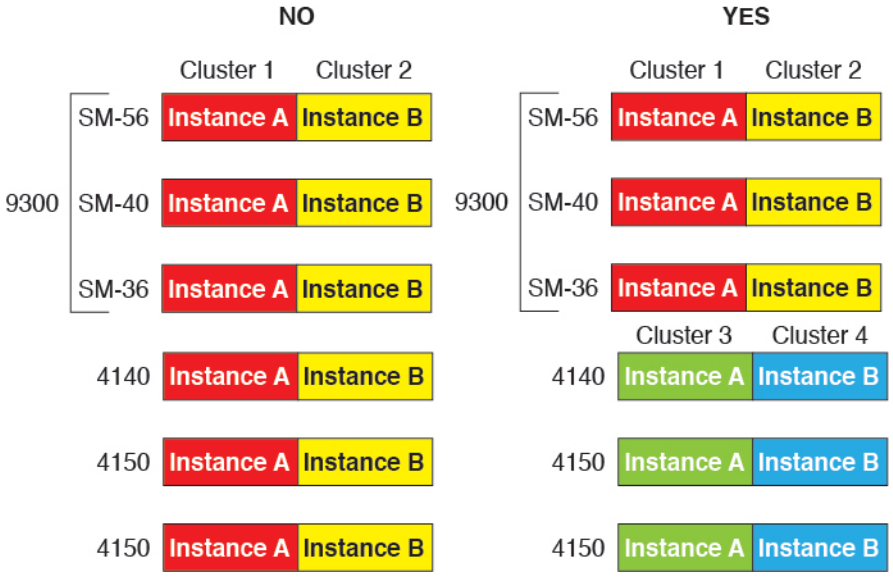
- 리소스 프로파일 일치 - 클러스터의 각 유닛이 동일한 리소스 프로파일 특성을 사용하는 것이 좋습니다. 그러나 클러스터 유닛을 다른 리소스 프로파일로 변경하거나 다른 모델을 사용하는 경우 일치하지 않는 리소스가 허용됩니다.

- 전용 클러스터 제어 링크 - 섀시 간 클러스터링의 경우 각 클러스터에 전용 클러스터 제어 링크가 필요합니다. 예를 들어 각 클러스터는 동일한 클러스터 유형 EtherChannel에서 별도의 하위 인터페이스를 사용하거나 별도의 EtherChannel을 사용할 수 있습니다.



- 공유 인터페이스 없음 - 클러스터링에서 공유 유형 인터페이스를 지원하지 않습니다. 그러나 동일한 관리 및 이벤트 인터페이스는 여러 클러스터에서 사용할 수 있습니다.

- 하위 인터페이스 없음 - 다중 인스턴스 클러스터는 FXOS 정의 VLAN 하위 인터페이스를 사용할 수 없습니다. 클러스터 EtherChannel의 하위 인터페이스를 사용할 수 있는 클러스터 제어 링크는 예외입니다.
- 섀시 모델 혼합 - 각 클러스터 인스턴스에 동일한 보안 모듈 또는 섀시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 예를 들어 Firepower 9300 SM-56, SM-40, SM-36에서 인스턴스를 사용해 하나의 클러스터를 생성할 수 있습니다. 또는 Firepower 4140 및 4150에서 클러스터를 생성할 수 있습니다.



- 최대 6개 유닛 - 하나의 클러스터에서 최대 6개의 컨테이너 인스턴스를 사용할 수 있습니다.

섀시 간 클러스터링을 위한 스위치 요구 사항

- Firepower 4100/9300 섀시에서 클러스터링을 구성하기 전에 스위치 구성을 완료하고 섀시의 모든 EtherChannel을 스위치에 성공적으로 연결하십시오.
- 지원되는 스위치 특성은 Cisco FXOS 호환성을 참고하십시오.

클러스터링 지침 및 제한 사항

섀시 간 클러스터링을 위한 스위치

- 연결된 스위치가 클러스터 데이터 인터페이스 및 클러스터 제어 링크 인터페이스 모두의 MTU와 일치해야 합니다. 클러스터 제어 링크 인터페이스 MTU를 데이터 인터페이스 MTU보다 100바이트 이상 높게 설정해야 하므로 스위치를 연결하는 클러스터 제어 링크를 적절하게 설정해야 합니다. 클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드를 모두 수용해야 합니다.

- Cisco IOS XR 시스템의 경우 기본이 아닌 MTU를 설정하려면 IOS 인터페이스 MTU를 클러스터 디바이스 MTU보다 14바이트 높게 설정합니다. 그렇지 않으면, **mtu-ignore** 옵션을 사용하지 않는 경우 OSPF 인접 피어링 시도에 실패할 수 있습니다. 클러스터 디바이스 MTU는 IOS *IPv4* MTU와 일치해야 합니다. Cisco Catalyst 및 Cisco Nexus 스위치에는 이 조정이 필요하지 않습니다.
- 클러스터 제어 링크 인터페이스용 스위치의 경우, 클러스터 유닛에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 디바이스에 트래픽이 균일하지 않게 분산될 수 있습니다.
- 스위치에서 EtherChannel의 로드 밸런싱 알고리즘을 변경할 경우, 스위치의 EtherChannel 인터페이스에서 트래픽 전달이 일시적으로 중단되며 Spanning Tree Protocol이 재시작됩니다. 트래픽에서 흐름을 다시 시작하기 전까지 지연이 발생하게 됩니다.
- 일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 동적 포트 우선순위를 비활성화하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다.
- 클러스터 제어 링크 경로의 스위치에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다.
- 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다.
- Supervisor 2T EtherChannel에서 기본 해시 분산 알고리즘은 적응형입니다. VSS 설계에서 비대칭 트래픽을 방지하려면 클러스터 디바이스에 연결된 포트 채널의 해시 알고리즘을 다음과 같이 변경하여 수정합니다.

  router(config) # **port-channel** *id* **hash-distribution fixed**

  VSS 피어 링크의 적응형 알고리즘을 활용할 때가 있을 수 있으므로 알고리즘을 전역으로 변경하지 마십시오.

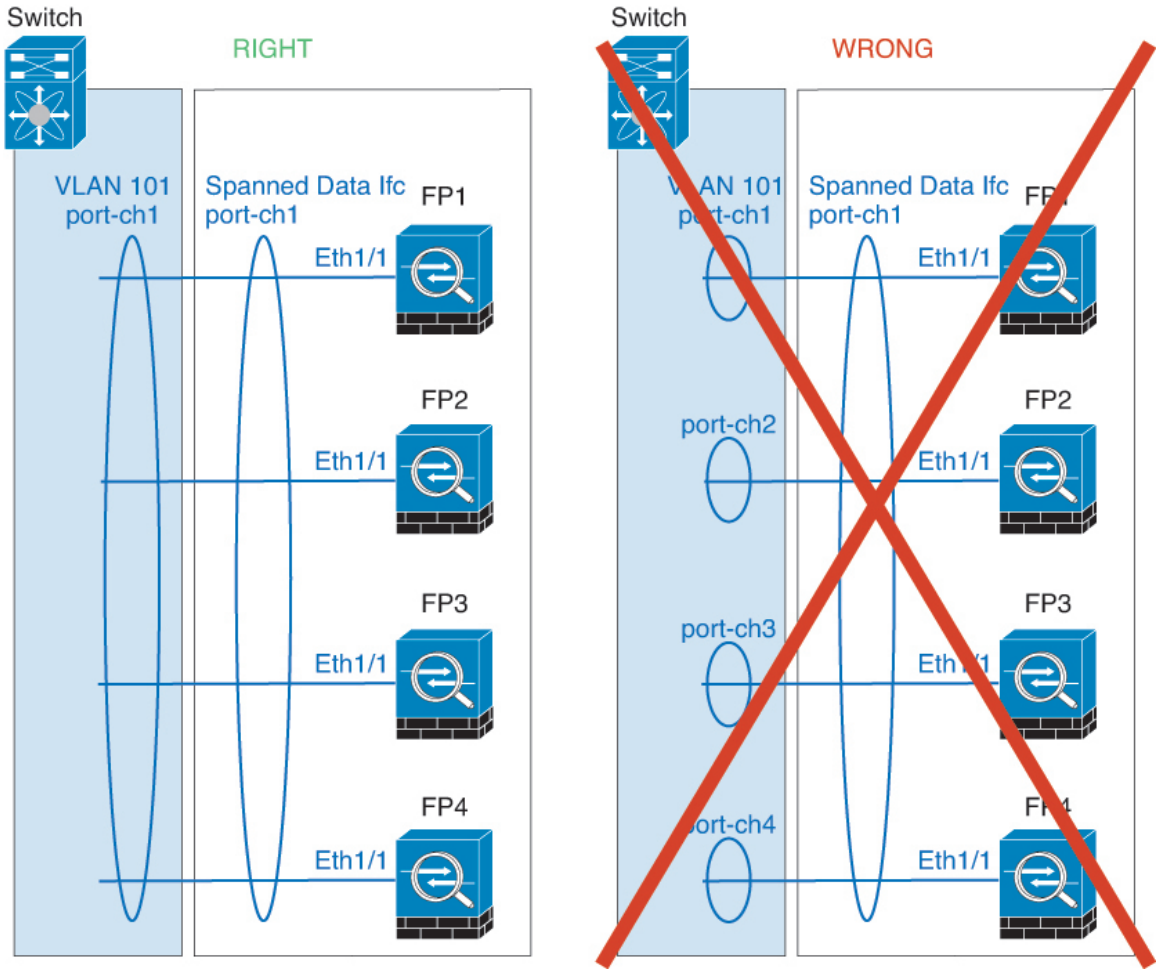
- Firepower 4100/9300 클러스터는 LACP 단계적 통합을 지원합니다. 따라서 연결된 Cisco Nexus 스위치에서 LACP 단계적 통합을 활성화된 상태로 둘 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다. FXOS EtherChannel에서는 기본적으로 LACP 속도가 fast(고속)로 설정됩니다. Nexus Series와 같은 일부 스위치는 ISSU(In-Service Software Upgrade) 수행 시 고속 LACP를 지원하지 않으므로 클러스터링에서는 ISSU를 사용하지 않는 것이 좋습니다.

새시 간 클러스터링을 위한 **EtherChannel**

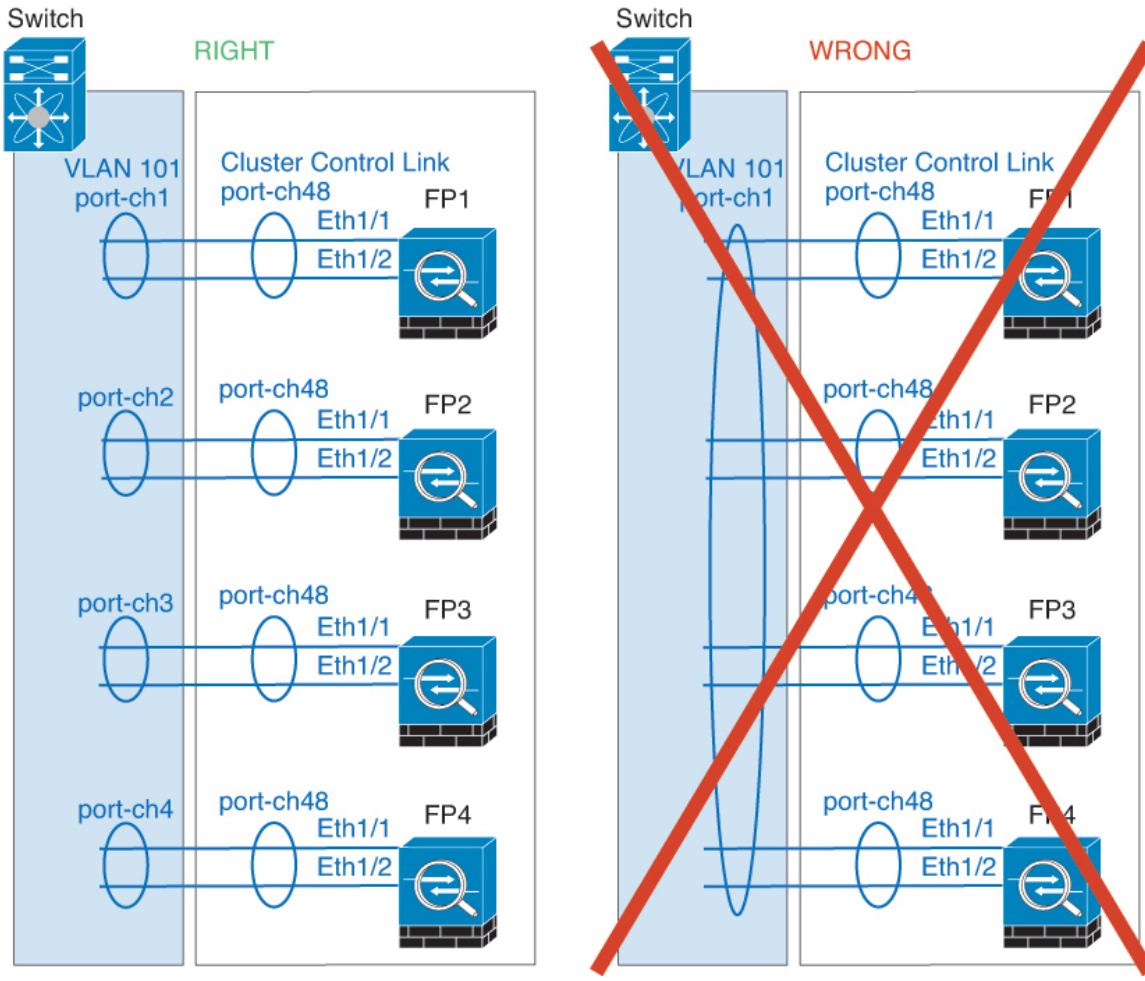
- 15.1(1)S2 이전 Catalyst 3750-X Cisco IOS 소프트웨어 버전에서는 클러스터 유닛에서 EtherChannel과 스위치 스택 간 연결을 지원하지 않았습니다. 기본 스위치 설정으로 클러스터 유닛 EtherChannel

이 교차 스택에 연결되어 있는 상태에서 제어 유닛 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.

- Spanned EtherChannel 구성과 디바이스-로컬 EtherChannel 구성 — Spanned EtherChannel과 디바이스-로컬 EtherChannel에서 각각 알맞게 스위치를 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 클러스터 유닛 *Spanned* EtherChannels의 경우, 인터페이스가 스위치의 단일 EtherChannel에 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



  - 디바이스-로컬 EtherChannel - 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 클러스터 유닛 디바이스-로컬 EtherChannel의 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 클러스터 유닛 EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



추가 지침

- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.
- Spanned EtherChannel 인터페이스에 연결된 Windows 2003 서버를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않아 대량의 ICMP 메시지가 클러스터에 다시 전송됩니다. 이러한 메시지로 인해 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능에 영향을 미칠 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.
- 이중화를 위해 EtherChannel을 VSS 또는 vPC에 연결하는 것이 좋습니다.
- 섀시 내에서 일부 보안 모듈을 클러스터하여 독립형 모드에서 다른 보안 모듈을 실행할 수 없습니다. 클러스터에 모든 보안 모듈을 포함해야 합니다.

- 암호 해독된 TLS/SSL 연결의 경우, 암호 해독 상태가 동기화되지 않습니다. 연결 소유자 장애가 발생하는 경우, 암호 해독된 연결이 재설정됩니다. 새 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.

기본값

- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 실패한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도하도록 설정됩니다.
- 실패한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도하도록 설정됩니다.
- 5초 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

클러스터링 설정

Firepower 4100/9300 섀시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다. FMC에 유닛을 추가하고 클러스터로 그룹화할 수 있습니다.

FXOS: Firepower Threat Defense 클러스터 추가

네이티브 모드에서 단일 Firepower 9300 섀시를 섀시 내 클러스터로 추가하거나 .

다중 인스턴스 모드에서 단일 Firepower 9300 섀시에 하나 이상의 클러스터를 섀시 내 클러스터로 추가하거나(각 모듈에 인스턴스를 포함해야 함) 섀시 간 클러스터링용으로 여러 섀시에 하나 이상의 클러스터를 추가할 수 있습니다.

섀시 간 클러스터링의 경우 각 섀시를 개별적으로 구성해야 합니다. 섀시 하나에 클러스터를 추가한 다음 쉽게 구축하기 위해 첫 번째 섀시의 부트스트랩 구성을 다음 섀시에 복사합니다.

Firepower Threat Defense 클러스터 생성

Firepower 4100/9300 섀시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다.

섀시 간 클러스터링의 경우 각 섀시를 개별적으로 구성해야 합니다. 섀시 하나에 클러스터를 구축한 다음 쉽게 구축하기 위해 첫 번째 섀시의 부트스트랩 컨피그레이션을 다음 섀시에 복사합니다.

모듈을 설치하지 않은 경우에도 Firepower 9300 섀시의 3개 모듈 슬롯 모두 또는 컨테이너 인스턴스, 각 슬롯의 컨테이너 인스턴스에 대해 클러스터링을 활성화해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음, 해당 이미지를 Firepower 4100/9300 섀시에 업로드합니다.
- 컨테이너 인스턴스의 경우 기본 프로필을 사용하지 않으려면 컨테이너 인스턴스에 대한 리소스 프로파일 추가, 761 페이지에 따라 리소스 프로필을 추가합니다.
- 컨테이너 인스턴스의 경우 컨테이너 인스턴스를 처음으로 설치하기 전에 디스크가 올바른 형식을 갖도록 보안 모듈/엔진을 다시 초기화해야 합니다. **Security Modules(**보안 모듈**)** 또는 **Security Engine(**보안 엔진**)**을 선택하고 다시 초기화 아이콘(↻)을 클릭합니다. 기존 논리적 디바이스가 삭제된 후에 새 디바이스로 재설치되며 로컬 애플리케이션 구성은 손실됩니다. 기본 인스턴스를 컨테이너 인스턴스로 교체할 때는 어떤 경우든 기본 인스턴스를 삭제해야 합니다. 기본 인스턴스를 컨테이너 인스턴스로 자동 마이그레이션할 수는 없습니다.
- 다음 정보를 수집합니다.
  - 관리 인터페이스 ID, IP 주소, 네트워크 마스크
  - Gateway IP address(게이트웨이 IP 주소)
  - FMC 선택한 IP 주소 및/또는 NAT ID
  - DNS 서버 IP 주소
  - FTD 호스트 이름 및 도메인 이름

프로시저

단계 **1** 인터페이스를 구성합니다.

a) 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(port-channel이라고도 함)을 최소 1개 추가합니다. EtherChannel(포트 채널) 추가, 758 페이지 또는 실제 인터페이스 구성, 757 페이지를 참조하십시오.

섀시 간 클러스터링의 경우, 모든 데이터 인터페이스는 멤버 인터페이스가 최소 1개 있는 Spanned EtherChannel이어야 합니다. 각 섀시에 동일한 EtherChannel을 추가합니다. 스위치의 단일 EtherChannel에 모든 클러스터 유닛의 멤버 인터페이스를 결합합니다. 섀시 간 클러스터링을 위한 EtherChannel에 대한 자세한 내용은 클러스터링 지침 및 제한 사항, 926 페이지을 참조하십시오.

다중 인스턴스 클러스터링의 경우 클러스터의 FXOS 정의 VLAN 하위 인터페이스 또는 데이터 공유 인터페이스를 사용할 수 없습니다. 애플리케이션 정의 하위 인터페이스만 지원됩니다. 자세한 내용은 FXOS 인터페이스와 애플리케이션 인터페이스 비교, 727 페이지를 참조하십시오.

b) 관리 유형 인터페이스 또는 EtherChannel을 추가합니다. EtherChannel(포트 채널) 추가, 758 페이지 또는 실제 인터페이스 구성, 757 페이지를 참조하십시오.

관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 섀시 관리용으로만 사용되는 섀시 관리 인터페이스(FXOS에서 MGMT, management0 또는 기타 유사한 이름으로 표시되는 섀시 관리 인터페이스 확인 가능)와는 다릅니다.

섀시 간 클러스터링의 경우 각 섀시에 동일한 Management(관리) 인터페이스를 추가합니다.

멀티 인스턴스 클러스터링의 경우 동일한 섀시의 여러 클러스터 또는 독립형 인스턴스에서 동일한 관리 인터페이스를 공유할 수 있습니다.

c) 섀시간 클러스터링의 경우, 멤버 인터페이스를 클러스터 제어 링크 EtherChannel에 추가합니다(기본: 포트 채널 48). EtherChannel(포트 채널) 추가, 758 페이지의 내용을 참조하십시오.

인트라 섀시 클러스터링(intra-chassis clustering)용으로 멤버 인터페이스를 추가하지 마십시오. 멤버를 추가하면 섀시에서는 이 클러스터를 섀시 간 클러스터로 가정하며, 예를 들어 Spanned EtherChannel만 사용하도록 허용합니다.

멤버 인터페이스가 포함되지 않은 경우, **Interfaces(**인터페이스**)** 탭에서 port-channel 48 클러스터 유형 인터페이스에 **Operation State(**운영 상태**)**가 **failed(**실패**)**로 표시됩니다. 인트라 섀시 클러스터링(intra-chassis clustering)의 경우 이 EtherChannel에는 멤버 인터페이스가 필요하지 않으므로 이 Operation State(운영 상태)를 무시할 수 있습니다.

각 섀시에 동일한 멤버 인터페이스를 추가합니다. 클러스터 제어 링크는 각 섀시의 디바이스-로컬 EtherChannel입니다. 디바이스별 스위치에서 별도의 EtherChannel을 사용합니다. 섀시 간 클러스터링을 위한 EtherChannel에 대한 자세한 내용은 클러스터링 지침 및 제한 사항, 926 페이지을 참조하십시오.

다중 인스턴스 클러스터링의 경우 추가 클러스터 유형 Etherchannel를 생성할 수 있습니다. 관리 인터페이스와 달리 클러스터 제어 링크는 여러 디바이스에서 공유할 수 없으므로 각 클러스터에 대한 클러스터 인터페이스가 필요합니다. 그러나 여러 Etherchannel 대신 VLAN 하위 인터페이스를 사용하는 것이 좋습니다. 클러스터 인터페이스에 VLAN 하위 인터페이스를 추가하려면 다음 단계를 참조하십시오.

d) 다중 인스턴스 클러스터링의 경우 각 클러스터에 별도의 클러스터 제어 링크를 사용할 수 있도록 VLAN 하위 인터페이스를 클러스터 EtherChannel에 추가합니다. 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가, 760 페이지의 내용을 참조하십시오.

클러스터 인터페이스에 하위 인터페이스를 추가하면 네이티브 클러스터에서 해당 인터페이스를 사용할 수 없습니다.

e) (선택 사항) Firepower 이벤트 처리 인터페이스를 추가합니다. EtherChannel(포트 채널) 추가, 758 페이지 또는 실제 인터페이스 구성, 757 페이지를 참조하십시오.

이 인터페이스는 FTD 디바이스의 보조 관리 인터페이스입니다. 이 인터페이스를 사용하려면 FTD CLI에서 해당 IP 주소 및 기타 매개변수를 구성해야 합니다. 예를 들면 관리 트래픽을 이벤트(예: 웹 이벤트)에서 분리할 수 있습니다. Firepower Threat Defense 명령 참조에서 **configure network** 명령을 참조하십시오.

섀시 간 클러스터링의 경우 각 섀시에 동일한 Eventing 인터페이스를 추가합니다.

단계 **2** **Logical Devices(**논리적 디바이스**)**를 선택합니다.

단계 **3** 를 클릭하고 다음 파라미터를 설정합니다.

그림 *30:* 네이티브 클러스터

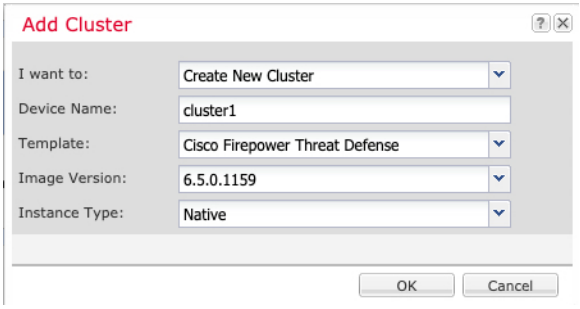
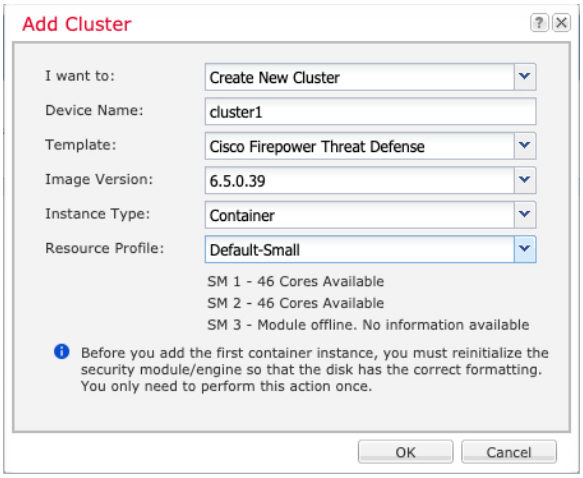


그림 *31:* 다중 인스턴스 클러스터



a) **I want to:(**수행할 작업**:)** > **Create New Cluster(**새 클러스터 생성**)**를 선택합니다.
b) **Device Name(**디바이스 이름**)**을 입력합니다.

   이 이름은 내부적으로 섀시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

c) **Template(**템플릿**)**에서 **Cisco Firepower Threat Defense**를 선택합니다.
d) **Image Version(**이미지 버전**)**을 선택합니다.
e) **Instance Type(**인스턴스 유형**)**의 경우 **Native(**네이티브**)** 또는 **Container(**컨테이너**)**를 선택합니다.

   네이티브 인스턴스는 보안 모듈/엔진의 모든 리소스(CPU, RAM 및 디스크 공간)를 사용합니다. 따라서 하나의 기본 인스턴스만 설치할 수 있습니다. 컨테이너 인스턴스는 보안 모듈/엔진의 리소스 하위 집합을 사용합니다. 따라서 여러 개의 컨테이너 인스턴스를 설치할 수 있습니다.

f) (컨테이너 인스턴스만 해당) **Resource Type(**리소스 유형**)**의 드롭다운 목록에서 리소스 프로파일 중 하나를 선택합니다.

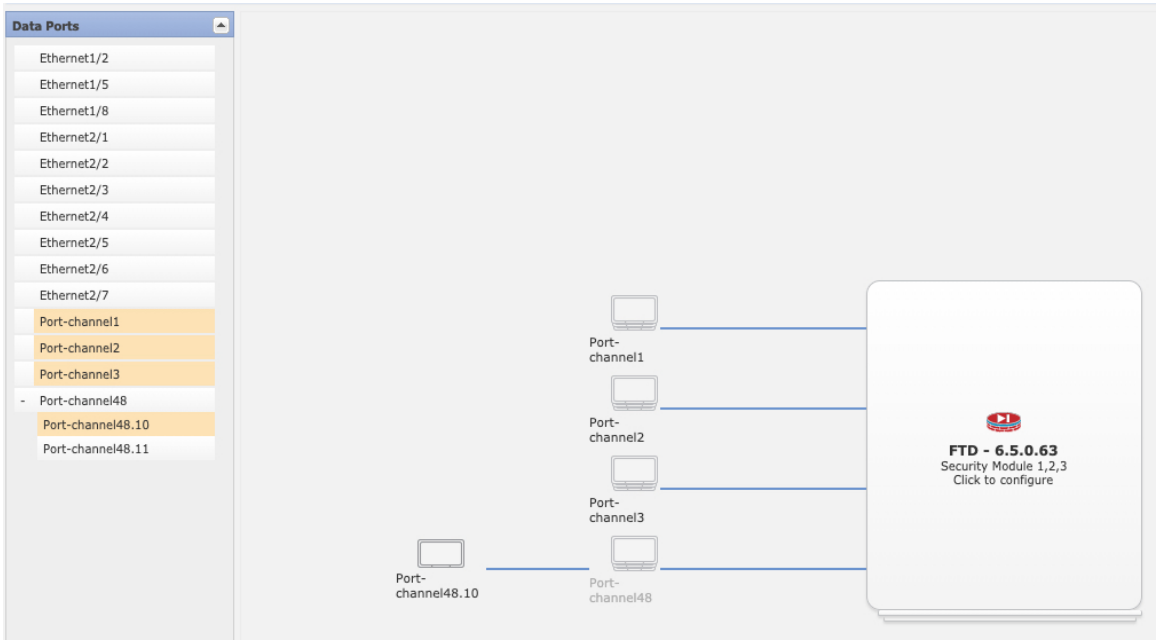
   Firepower 9300의 경우 이 프로파일은 보안 모듈의 각 인스턴스에 적용됩니다. 이 절차에서 나중에 보안 모듈별로 서로 다른 프로파일을 설정할 수 있습니다. 예를 들어 다른 보안 모듈 유형을 사용하면서 더 성능이 낮은 모델에서 더 많은 CPU를 사용할 수도 있습니다. 클러스터를 생성하기 전에 올바른 프로파일을 선택하는 것이 좋습니다. 새 프로파일을 생성해야 하는 경우 클러스터

생성을 취소하고 컨테이너 인스턴스에 대한 리소스 프로파일 추가, 761 페이지을 사용해 하나를 추가합니다.

g) **OK(**확인**)**를 클릭합니다.

Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 **4** 이 클러스터에 할당할 인터페이스를 선택합니다.



네이티브 모드 클러스터링의 경우: 유효한 모든 인터페이스가 기본적으로 할당되어 있습니다. 여러 클러스터 유형의 인터페이스를 지정했다면 하나를 제외하고 모두 선택 해제합니다.

다중 인스턴스 클러스터링의 경우: 클러스터에 할당할 각 데이터 인터페이스를 선택하고 클러스터 유형 포트 채널 또는 포트 채널 하위 인터페이스도 선택합니다.

단계 **5** 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 **6** **Cluster Information(**클러스터 정보**)** 페이지에서 다음 작업을 수행합니다.

그림 *32:* 네이티브 클러스터

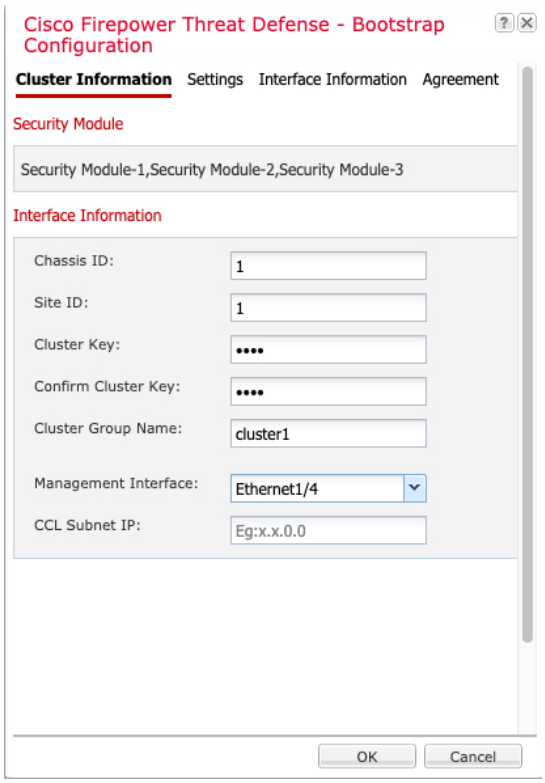
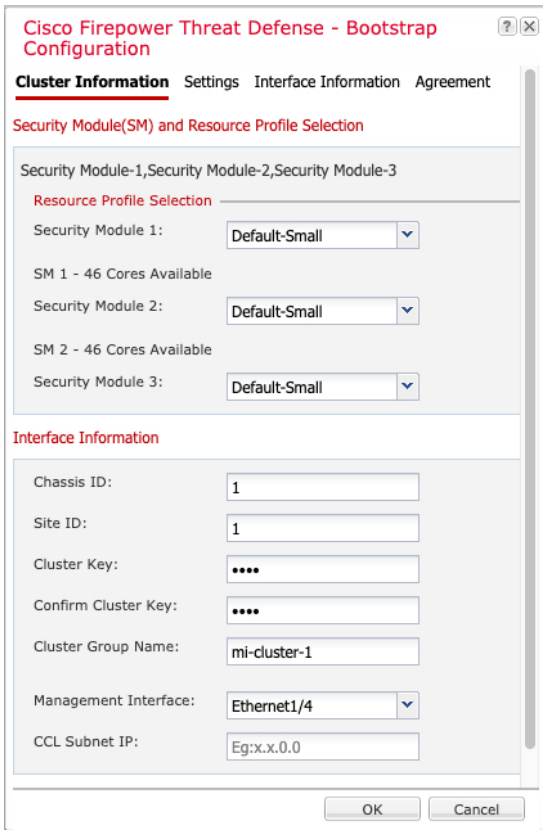


그림 *33:* 다중 인스턴스 클러스터



a) (Firepower 9300 컨테이너 인스턴스만 해당) 보안 모듈**(SM)** 및 리소스 프로파일 선택 영역에서 모듈별로 다른 리소스 프로파일을 설정할 수 있습니다. 예를 들어 다른 보안 모듈 유형을 사용하면서 더 성능이 낮은 모델에서 더 많은 CPU를 사용할 수도 있습니다.

b) 섀시 간 클러스터링의 경우, **Chassis ID(**섀시 **ID)** 필드에 섀시 ID를 입력합니다. 클러스터의 각 섀시는 고유 ID를 사용해야 합니다.

이 필드는 클러스터 제어 링크 Port-Channel 48에 멤버 인터페이스를 추가한 경우에만 나타납니다.

c) 사이트 간 클러스터링의 경우 이 섀시에 대해 **Site ID(**사이트 **ID)** 필드에 1~8의 사이트 ID를 입력합니다. FlexConfig 기능. 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 Firepower Management Center FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.

d) **Cluster Key(**클러스터 키**)** 필드에서 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 구성합니다.

공유 비밀은 1자 ~ 63자로 된 ASCII 문자열입니다. 공유 비밀은 키를 생성하는 데 사용됩니다. 이 옵션은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

e) **Cluster Group Name(**클러스터 그룹 이름**)**(논리적 디바이스 구성의 클러스터 그룹 이름)을 설정합니다.

이름은 1자 ~ 38자로 된 ASCII 문자열이어야 합니다.

f) **Management Interface(**관리 인터페이스**)**를 선택합니다.

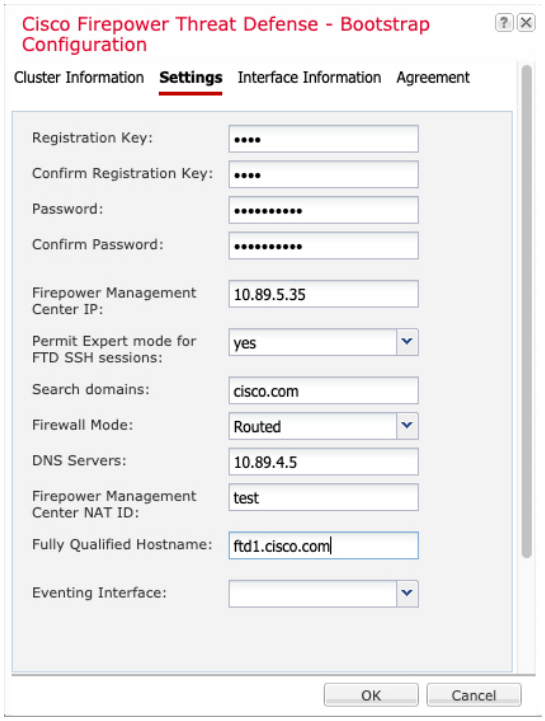
이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 섀시 관리 포트와 별개입니다.

g) (선택 사항) **CCL Subnet IP(CCL** 서브넷 **IP)**를 *a.b***.0.0**으로 설정합니다.

기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 이 경우 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외한 모든 /16 네트워크 주소를 클러스터용 고유 네트워크에 지정합니다. 값을 0.0.0.0으로 설정하는 경우 기본 네트워크가 사용됩니다.

섀시에서는 섀시 ID 및 슬롯 ID *a.b.chassis_id.slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다.

단계 **7** **Settings(**설정**)** 페이지에서 다음 작업을 완료합니다.



a) **Registration Key(**등록 키**)** 필드에 등록하는 동안 Firepower Management Center와 클러스터 멤버 간에 공유할 키를 입력합니다.

이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.

b) FTD 관리 사용자가 CLI에 액세스할 때 사용할 **Password(**비밀번호**)**를 입력합니다.

c) **Firepower Management Center IP** 필드에 Firepower Management Center를 관리하기 위한 IP 주소를 입력합니다. FMC IP 주소를 알 수 없는 경우, 이 필드를 비워두고 **Firepower Management Center NAT ID** 필드에 암호를 입력합니다.

d) (선택 사항) 컨테이너 인스턴스의 경우, **Permit Export mode from FTD SSH sessions(FTD SSH** 세션에서 전문가 모드 허용**)**에 대해 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다. 전문가 모드에서는 고급 트러블슈팅을 위한 FTD 셸 액세스 기능이 제공됩니다.

이 옵션에 대해 **Yes(**예**)**를 선택하는 경우 SSH 세션에서 컨테이너 인스턴스에 직접 액세스할 수 있는 사용자가 전문가 모드를 시작할 수 있습니다. **No(**아니요**)**를 선택하는 경우에는 FXOS CLI에서 컨테이너 인스턴스에 액세스할 수 있는 사용자만 전문가 모드를 시작할 수 있습니다. 각 인스턴스를 더욱 명확하게 격리할 수 있도록 **No(**아니요**)**를 선택하는 것이 좋습니다.

문서에 설명되어 있는 절차에 따라 Expert 모드가 필요하다고 알려주는 경우 또는 Cisco Technical Assistance Center에서 사용하도록 요청하는 경우에만 Expert 모드를 사용합니다. 이 모드를 설정하려면 FTD CLI에서 **expert** 명령을 사용합니다.

e) (선택 사항) **Search Domains(**검색 도메인**)** 필드에 관리 네트워크의 쉼표로 구분된 검색 도메인 목록을 입력합니다.

f) (선택 사항) **Firewall Mode(**방화벽 모드**)** 드롭다운 목록에서 **Transparent(**투명**)** 또는 **Routed(**라우팅됨**)**를 선택합니다.

라우팅 모드에서 FTD는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

g) (선택 사항) **DNS Servers(DNS** 서버**)** 필드에 쉼표로 구분된 DNS 서버 목록을 입력합니다.

예를 들어, FMC의 호스트 이름을 지정하는 경우, FTD에서는 DNS를 사용합니다.

h) (선택 사항) 새 디바이스로 클러스터를 추가할 때 FMC에도 입력할 암호를 **Firepower Management Center NAT ID** 필드에 입력합니다.

일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. 1~37자의 임의의 텍스트 문자열을 NAT ID로 지정할 수 있습니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

i) (선택 사항) **Fully Qualified Hostname(**정규화된 호스트 이름**)** 필드에 FTD 디바이스의 정규화된 이름을 입력합니다.

유효한 문자는 a부터 z까지의 문자, 0과 9 사이의 숫자, 점(.) 및 하이픈(-)입니다. 최대 문자 수는 253자입니다.

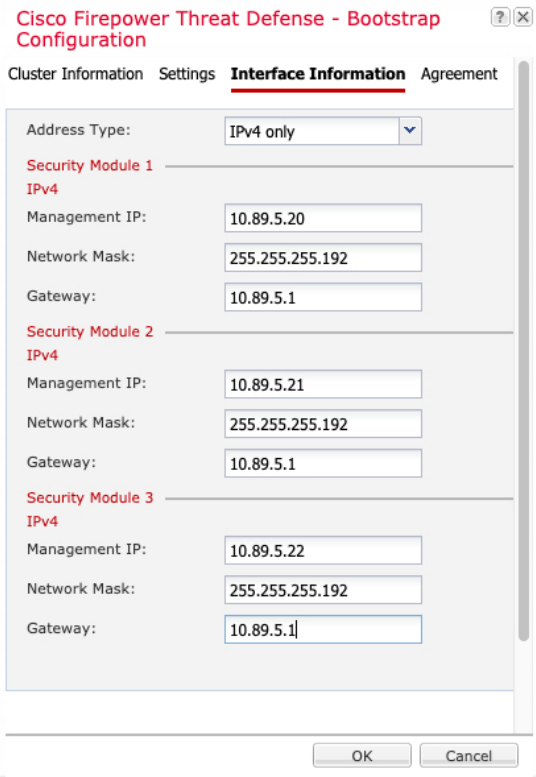
j) (선택 사항) **Eventing Interface(Eventing** 인터페이스**)** 드롭다운 목록에서 Firepower 이벤트가 전송되어야 할 인터페이스를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.

Firepower 이벤트에 사용할 별도의 인터페이스를 지정하려면 인터페이스를 *Firepower* 이벤트 처리 인터페이스로 구성해야 합니다. 하드웨어 바이패스 지원 인터페이스를 Eventing(이벤트)

인터페이스로 할당하는 경우 그러한 할당이 의도적인지를 확인하는 경고 메시지가 표시됩니다.

단계 **8** **Interface Information(**인터페이스 정보**)** 페이지에서 클러스터의 각 보안 모듈의 관리 IP 주소를 구성합니다. **Address Type(**주소 유형**)** 드롭다운 목록에서 주소 유형을 선택한 다음 각 보안 모듈에 대해 다음 작업을 수행합니다.

참고 모듈을 설치하지 않은 경우에도 섀시의 3개 모듈 슬롯 모두에 대해 IP 주소를 설정해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.



a) **Management IP(**관리 **IP)** 필드에서 IP 주소를 구성합니다.

각 모듈에 대해 동일한 네트워크에서 고유한 IP 주소를 지정합니다.

b) **Network Mask(**네트워크 마스크**)** 또는 **Prefix Length(**접두사 길이**)**를 입력합니다.

c) **Network Gateway(**네트워크 게이트웨이**)** 주소를 입력합니다.

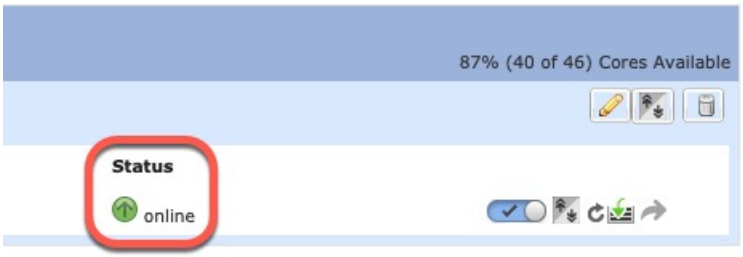
단계 **9** **Agreement(**계약**)** 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 **10** **OK(**확인**)**를 클릭하여 구성 대화 상자를 닫습니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 상태가 **online(**온라인**)**으로 표시되면 수도 있고, 섀시 내 클러스터링의 경우 애플리케이션 내에서 클러스터 구성을 시작할 수

도 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 **12** 섀시 간 클러스터링의 경우, 다음 섀시를 클러스터에 추가합니다.

a) 첫 번째 섀시 Firepower Chassis Manager에서 오른쪽 상단에 있는 **Show Configuration(**컨피그레이션 표시**)** 아이콘을 클릭하여 표시된 클러스터 컨피그레이션을 복사합니다.

b) 다음 섀시에 있는 Firepower Chassis Manager에 연결하고 이 절차에 따라 논리적 디바이스를 추가합니다.

c) **I want to:(**수행할 작업**:) > Join an Existing Cluster(**기존 클러스터에 조인**)**를 선택합니다.

d) **OK(**확인**)**를 클릭합니다.

e) **Copy Cluster Details(**클러스터 세부사항 복사**)** 상자에서 첫 번째 섀시의 클러스터 구성에 붙여 넣고 **OK(**확인**)**를 클릭합니다.

f) 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

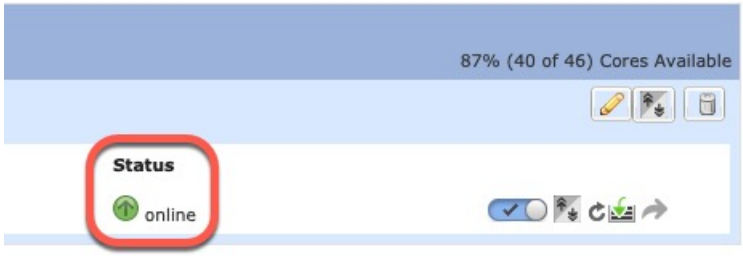
- **Chassis ID(**섀시 **ID)** - 고유한 섀시 ID를 입력합니다.
- **Site ID(**사이트 **ID)** - 사이트 간 클러스터링의 경우 이 섀시에 대해 1~8 사이의 사이트 ID를 입력합니다. 디렉터 현지화, 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 추가적인 사이트 간 클러스터 맞춤화는 Firepower Management Center FlexConfig 기능을 사용하는 경우에만 구성 가능합니다.
- **Cluster Key(**클러스터 키**)** - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.
- **Management IP(**관리 **IP)** - 각 모듈의 관리 주소를 다른 클러스터 멤버와 동일한 네트워크에 있는 고유 IP 주소로 변경합니다.

OK(확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤

버의 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 **13** 관리 IP 주소를 사용하여 제어 유닛을 Firepower Management Center에 추가합니다.

Firepower Management Center에 추가하기 전에 모든 클러스터 유닛이 FXOS에서 성공적으로 형성된 클러스터에 있어야 합니다.

그러면 Firepower Management Center에서 데이터 유닛을 자동으로 탐지합니다.

클러스터 유닛 추가

기존 클러스터에서 FTD 클러스터 유닛을 추가하거나 교체합니다.

참고 이 절차의 FXOS 단계는 새 섀시 추가 시에만 적용됩니다. 클러스터링이 이미 활성화된 Firepower 9300에 새 모듈을 추가하는 경우에는 모듈이 자동으로 추가됩니다. 그래도 Firepower Management Center에는 새 모듈을 추가해야 합니다. Firepower Management Center 단계로 건너뜁니다.

시작하기 전에

- 교체 시 기존 클러스터 유닛을 Firepower Management Center에서 삭제해야 합니다. 새 유닛으로 교체할 경우, 해당 유닛은 Firepower Management Center에서 새 디바이스로 간주됩니다.
- 인터페이스 구성은 새 섀시에서 동일해야 합니다. FXOS 섀시 구성 내보내기와 가져오기를 통해 이 프로세스를 더 쉽게 수행할 수 있습니다.

프로시저

단계 **1** 기존 클러스터 섀시 Firepower Chassis Manager에서 **Logical Devices(**논리적 디바이스**)**를 선택하여 **Logical Devices(**논리적 디바이스**)** 페이지를 엽니다.

단계 **2** 오른쪽 상단에 있는 설정 표시 아이콘을 클릭하여 표시된 클러스터 설정을 복사합니다.

단계 **3** 새 섀시에서 Firepower Chassis Manager에 연결한 다음 **Add(**추가**)** > **Cluster(**클러스터**)**를 클릭합니다.

단계 **4** **Device Name(**디바이스 이름**)**에 논리적 디바이스의 이름을 입력합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Copy Cluster Details(**클러스터 세부사항 복사**)** 상자에서 첫 번째 섀시의 클러스터 구성에 붙여 넣고 **OK(**확인**)**를 클릭합니다.

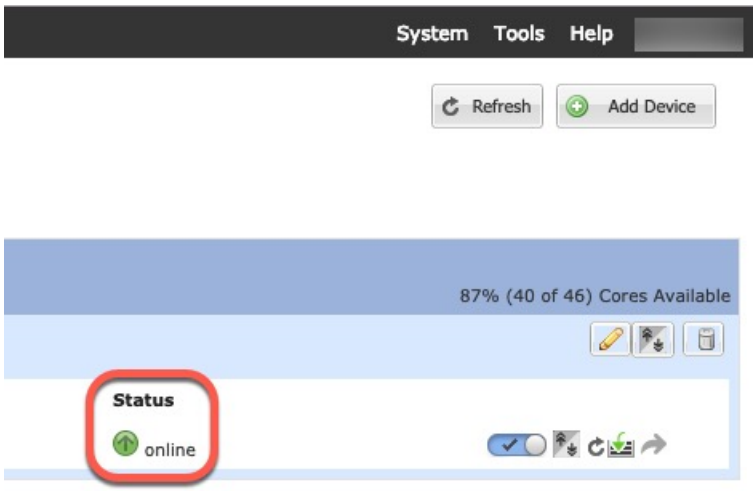
단계 **7** 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID(**섀시 **ID)** - 고유한 섀시 ID를 입력합니다.
- **Site ID(**사이트 **ID)** - 사이트 간 클러스터링의 경우 이 섀시에 대해 1~8 사이의 사이트 ID를 입력합니다. Firepower Management Center FlexConfig 기능을 통해서만 이 기능을 구성할 수 있습니다.
- **Cluster Key(**클러스터 키**)** - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.
- **Management IP(**관리 **IP)** - 각 모듈의 관리 주소를 다른 클러스터 멤버와 동일한 네트워크에 있는 고유 IP 주소로 변경합니다.

OK(확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



FMC: 클러스터 추가

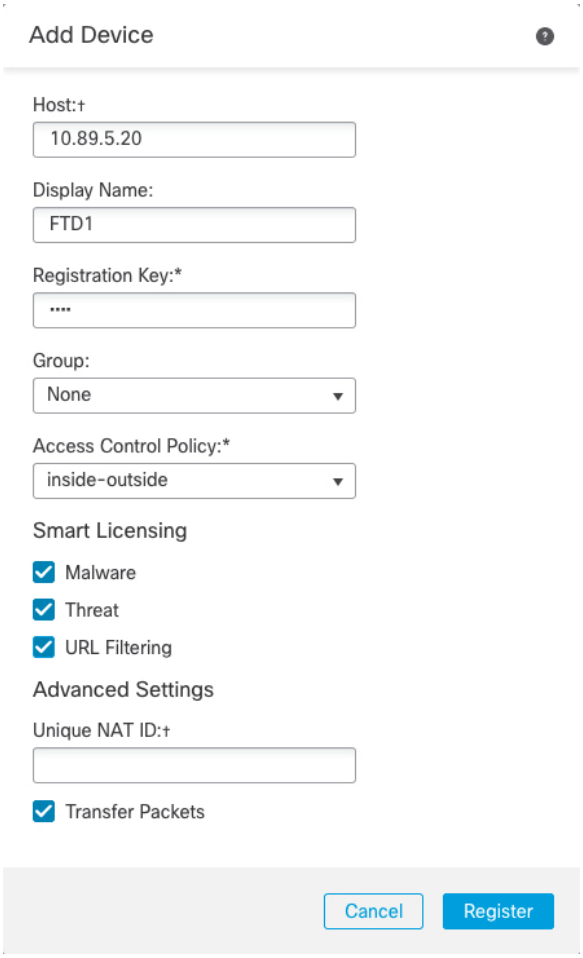
Firepower Management Center에 클러스터 유닛 중 하나를 새 장치로 추가합니다. FMC는 다른 클러스터 멤버를 자동으로 감지합니다.

시작하기 전에

- 클러스터를 추가하기 위한 이 방법은 Firepower Threat Defense 버전 6.2 이상이 필요합니다. 이전 버전 디바이스를 관리해야 하는 경우 해당 버전의 Firepower Management Center 환경 설정 가이드를 참조합니다.
- 클러스터를 관리 센터에 추가하기 전에 모든 클러스터 단위가 FXOS에서 성공적으로 구성된 클러스터에 있어야 합니다. 제어 유닛을 확인하십시오. Firepower 섀시 관리자의 논리적 디바이스 화면을 참조하거나 Firepower Threat Defense **show cluster info** 명령어를 사용하십시오.

프로시저

단계 **1** FMC에서 디바이스 > 디바이스 관리을 선택하고 클러스터 구축 시 할당한 유닛의 관리 IP 주소를 사용해 제어 유닛을 추가하기 위해 추가 > 디바이스 추가를 선택합니다.



a) **Host(**호스트**)** 필드에 제어 유닛의 IP 주소나 호스트 이름을 입력합니다.

최적의 성능을 위해서는 제어 유닛을 추가하는 것이 좋습니다 하지만 모든 클러스터 유닛을 추가할 수 있습니다.

디바이스 설정 중에 NAT ID를 사용한 경우 이 필드를 입력하지 않아도 됩니다.자세한 내용은 NAT 환경, 302 페이지를 참조하십시오.

b) FMC에 표시할 제어 유닛의 이름을 표시 이름 필드에 입력합니다.

이 표시 이름은 클러스터용이 아닙니다. 추가하려는 제어 유닛에만 해당됩니다. 나중에 다른 클러스터 멤버의 이름과 클러스터 표시 이름을 변경할 수 있습니다.

c) FXOS에 클러스터를 구축할 때 사용한 것과 동일한 등록 키를 등록 키 필드에 입력합니다. 등록 키는 일회용 공유 암호입니다.

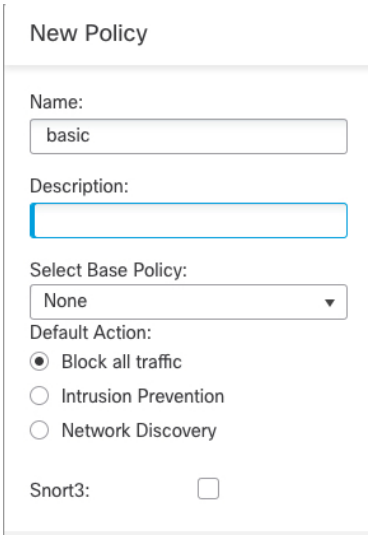
d) 다중 도메인 구축에서는 현재 도메인과 상관없이 디바이스를 리프 도메인으로 할당합니다.

현재 도메인이 리프 도메인인 경우 디바이스는 자동으로 현재 도메인에 추가됩니다. 현재 도메인이 리프 도메인이 아닌 경우나 이후 재등록을 한 경우라면 리프 도메인으로 전환하여 디바이스를 구성합니다.

e) (선택 사항) 디바이스 그룹에 디바이스를 추가합니다.

f) 등록 시 디바이스를 구축하기 위해 초기 액세스 제어 정책을 선택하거나 새 정책을 생성합니다.

새 정책을 생성하는 경우 기본 정책만 생성합니다. 나중에 필요에 따라 정책을 사용자 정의할 수 있습니다.



g) 디바이스에 적용할 라이선스를 선택합니다.

h) 디바이스 설정 중 NAT ID를 사용하는 경우 고급 섹션을 확장하고 고유 **NAT ID** 필드에 동일한 NAT ID를 입력합니다.

i) 패킷 전송 체크 박스를 선택하여 디바이스가 FMC에 패킷을 전송하도록 합니다.

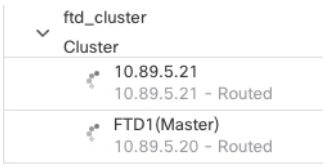
이 옵션은 기본적으로 활성화되어 있습니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 FMC에 전송합니다. 이벤트를 비활성화하면 이벤트 정보는 FMC에 전송되지만 패킷 데이터는 전송되지 않습니다.

j) **Register(**등록**)**를 클릭합니다.

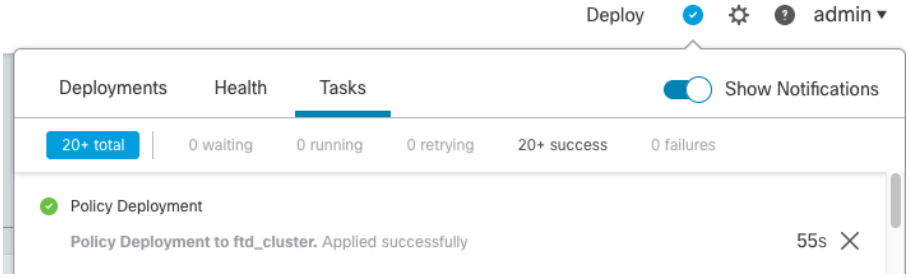
FMC은 제어 유닛을 식별해 등록하고 모든 데이터 유닛을 등록합니다. 제어 유닛이 성공적으로 등록되지 않는 경우 클러스터가 추가되지 않습니다. 클러스터가 섀시에 없거나 다른 연결 문제로 등록이 실패할 수 있습니다. 이 경우 클러스터 유닛 추가를 다시 시도하시기를 권장합니다.

디바이스 > 디바이스 관리 페이지에 클러스터 이름이 표시됩니다. 클러스터 유닛을 보려면 클러스터를 확장합니다.

현재 등록되는 유닛에는 로딩 아이콘이 표시됩니다.



알림 아이콘을 클릭하고 작업을 선택하여 클러스터 유닛 등록을 모니터링할 수 있습니다. FMC은 각 유닛이 등록될 때마다 클러스터 등록 작업을 업데이트합니다. 유닛 등록에 실패하는 경우 클러스터 멤버 조정, 957 페이지의 내용을 참조하십시오.



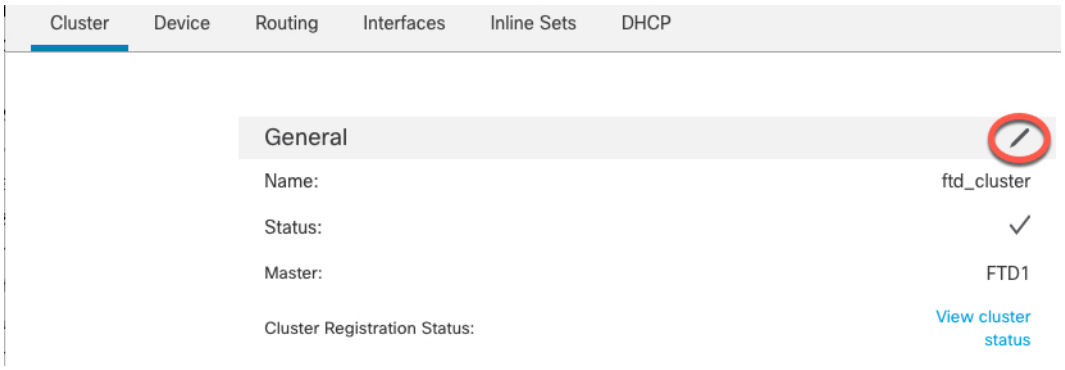
단계 **2** 클러스터에 대해 수정( )을 클릭하여 디바이스별 설정을 구성합니다.

대부분의 구성은 클러스터의 멤버 유닛이 아닌 클러스터 전체에 적용할 수 있습니다. 예를 들어 유닛당 표시 이름을 변경할 수 있지만 전체 클러스터에 대해서만 인터페이스를 설정할 수 있습니다.

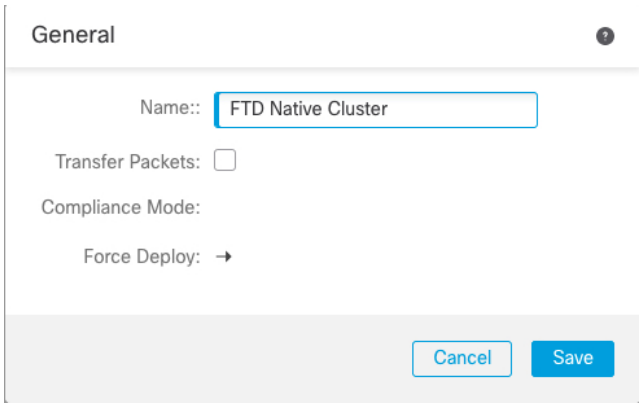
단계 **3** 디바이스 > 디바이스 관리 > 클러스터 화면에서 일반, 라이선스, 시스템및 상태 설정을 표시합니다.

다음 클러스터별 항목을 참조하십시오.

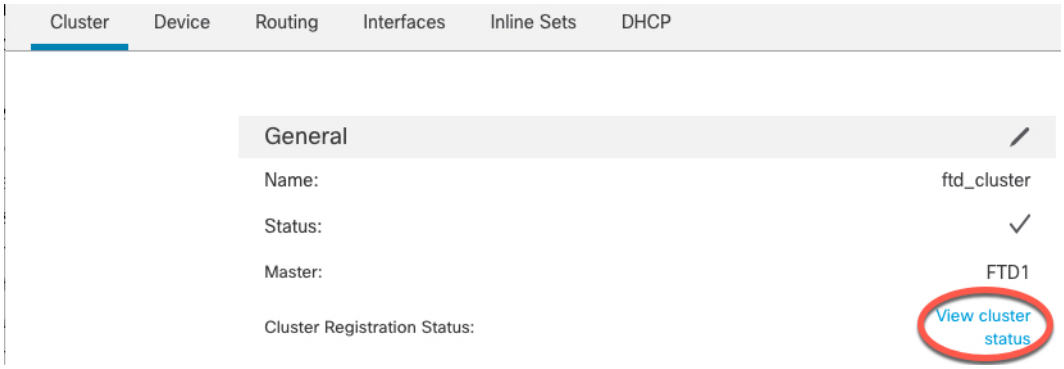
- **General (일반)> Name (이름)** - 수정( )를 클릭하여 클러스터 표시 이름을 변경합니다.



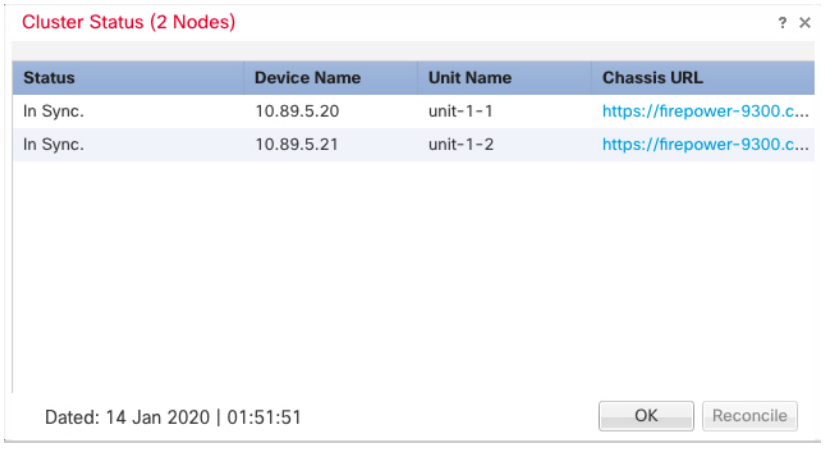
그런 다음 **Name(이름)** 필드를 설정합니다.



- **General(일반) > View cluster status(클러스터 상태 보기)**—**View cluster status(클러스터 상태 보기)** 링크를 클릭하여 **Cluster Status(클러스터 상태)** 대화 상자를 엽니다.



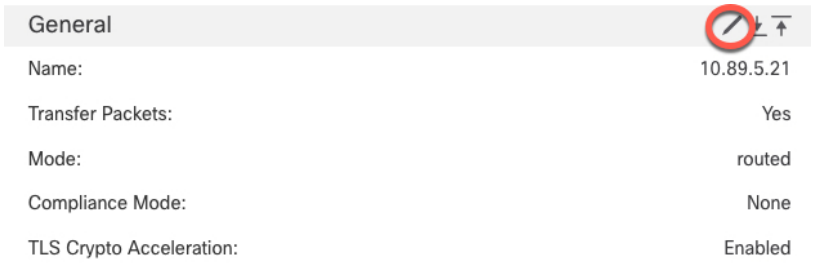
Cluster Status(클러스터 상태) 대화 상자에서 **Reconcile(조정)**을 클릭하면 데이터 유닛 등록을 다시 시도할 수도 있습니다.



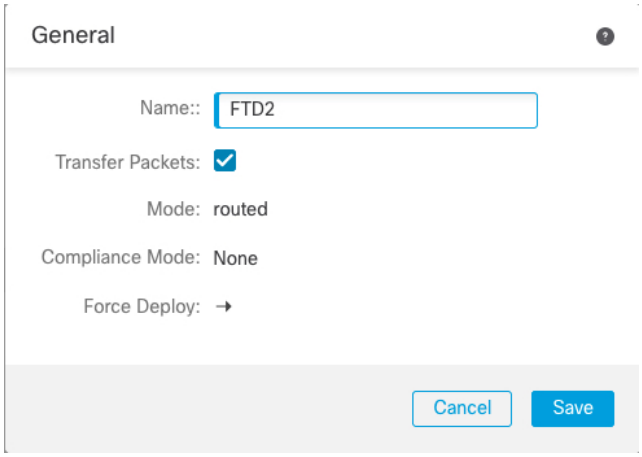
- **License(라이선스)** - 수정( )을 클릭하여 라이선스 등록을 설정할 수 있습니다.

단계 **4** **Devices(디바이스) > Device Management(디바이스 관리) >** 디바이스**(디바이스)**의 오른쪽 상단 드롭다운 메뉴에서 클러스터의 각 멤버를 선택하고 다음 설정을 구성할 수 있습니다.

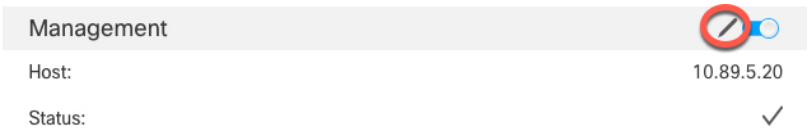
- **General(일반) > Name (이름)** - 수정( )을 클릭하여 클러스터 멤버 표시 이름을 변경합니다.



그런 다음 **Name(이름)** 필드를 설정합니다.



- **Management(관리) > Host(호스트)**—디바이스 설정에서 관리 IP 주소를 변경하는 경우 새 주소를 FMC에 일치시켜야 네트워크의 디바이스와 연결할 수 있습니다. **Management(관리)** 영역에서 **Host(호스트)** 주소를 편집합니다.



FMC: 클러스터, 데이터, 진단 인터페이스 구성

이 절차에서는 FXOS에서 클러스터를 구축할 때 클러스터에 할당한 각 데이터 인터페이스의 기본 파라미터를 구성합니다. 섀시 간 클러스터링의 경우, 데이터 인터페이스는 항상 Spanned EtherChannel 인터페이스입니다. 섀시 간 클러스터링을 위한 클러스터 제어 링크 인터페이스의 경우 MTU를 기본값에서 늘려야 합니다. 개별 인터페이스로 실행할 수 있는 유일한 인터페이스인 진단 인터페이스를 구성할 수도 있습니다.

참고 섀시 간 클러스터링을 위해 Spanned EtherChannel을 사용할 경우, 클러스터링이 완전히 활성화될 때까지 포트 채널 인터페이스가 나타나지 않습니다. 이러한 요구 사항으로 인해 클러스터의 활성 유닛이 아닌 유닛에는 트래픽이 전달되지 않습니다.

프로시저

단계 **1** 디바이스 > 디바이스 관리를 선택하고 클러스터 옆의 수정( )를 클릭합니다.

단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

단계 **3** 클러스터 제어 링크 구성

섀시 간 클러스터링의 경우, 클러스터 제어 링크 MTU를 데이터 인터페이스의 최고 MTU보다 최소 100바이트 이상 높게 설정합니다. 클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드를 모두 수용해야 합니다. MTU를 최댓값인 9184바이트로 설정하는 것이 좋습니다. 최솟값은 1400바이트입니다. 예를 들어 최대 MTU가 9184바이트이므로 가장 높은 데이터 인터페이스 MTU는 9084이 될 수 있는 반면, 클러스터 제어 링크는 9184로 설정할 수 있습니다.

기본 클러스터의 경우: 클러스터 제어 링크 인터페이스는 기본적으로 Port-Channel48입니다.

a) 클러스터 제어 링크 인터페이스에 대한 수정( )를 클릭합니다.
b) **General(**일반**)** 페이지의 **MTU** 필드에 1400에서 9184 사이의 값을 입력합니다. 최대값인 9184를 사용하는 것이 좋습니다.
c) **OK(**확인**)**를 클릭합니다.

단계 **4** 데이터 인터페이스 구성

a) (선택 사항) 데이터 인터페이스에 VLAN 하위 인터페이스를 구성합니다. 이 절차의 나머지는 하위 인터페이스에 적용됩니다. 하위 인터페이스 추가, 813 페이지를 참조하십시오.
b) 데이터 인터페이스를 위해 수정( )을 클릭합니다.
c) 라우팅 모드 인터페이스 구성, 817 페이지 또는 에 따라 이름, IP 주소 및 기타 파라미터 브리지 그룹 인터페이스 구성, 821 페이지를 구성하십시오.

참고 클러스터 제어 링크 인터페이스 MTU가 데이터 인터페이스 MTU보다 최소 100바이트 이상 높지 않으면 데이터 인터페이스의 MTU를 줄여야 한다는 오류가 표시됩니다. 클러스터 제어 링크 MTU를 늘리려면 단계 단계 3, 949 페이지의 내용을 참조하십시오. 그 후에는 계속해서 데이터 인터페이스를 구성할 수 있습니다.

d) 섀시 간 클러스터의 경우 EtherChannel의 수동 전역 MAC 주소를 설정합니다. **Advanced(**고급**)**를 클릭해서 액티브 **MAC** 주소 필드에 H.H.H. 형식으로 MAC 주소를 입력합니다. 여기서 H는 16비트 16진수입니다.

예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력됩니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다. 즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없습니다.

스탠바이 **MAC** 주소는 무시되므로 설정하지 마십시오.

잠재적인 네트워크 연결 문제를 방지하기 위해 Spanned EtherChannel에 대한 MAC 주소를 구성해야 합니다. 수동 구성된 MAC 주소를 사용할 경우, 해당 MAC 주소가 현재 제어 유닛에 유지됩니다. MAC 주소를 구성하지 않은 상태에서 제어 유닛을 변경하는 경우 새 제어 유닛에서는 인터페이스의 새 MAC 주소를 사용하며, 이로 인해 네트워크가 잠시 중단될 수 있습니다.

e) **OK(**확인**)**를 클릭합니다. 다른 데이터 인터페이스에 대해 위 단계를 반복합니다.

단계 **5** (선택 사항) 진단 인터페이스 구성

진단 인터페이스는 개별 인터페이스 모드에서 실행할 수 있는 유일한 인터페이스입니다. 예를 들어 시스템 로그 메시지 또는 SNMP에 이 인터페이스를 사용할 수 있습니다.

a) IPv4 및/또는 IPv6 주소 풀을 추가하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Address Pools(**주소 풀**)**을 선택합니다. 주소 풀, 666 페이지를 참조하십시오.

최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. 가상 IP 주소가 이 풀의 일부가 아니어도 동일한 네트워크에 있어야 합니다. 사전에 각 장치에 할당된 정확한 로컬 주소를 확인할 수 없습니다.

b) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**에서 진단 인터페이스에 대한 수정( )를 클릭합니다.

c) **IPv4**에서 **IP** 주소 및 마스크를 입력합니다. IP 주소는 현재 제어 유닛에 항상 속해 있는 클러스터의 고정 주소입니다.

d) **IPv4** 주소 풀 드롭다운 목록에서 생성한 주소 풀을 선택합니다.

e) **IPv6 >** 기본 탭의 **IPv6** 주소 풀 드롭다운 목록에서 생성한 주소 풀을 선택합니다.

f) 다른 인터페이스 설정은 기본으로 구성합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

FXOS: 클러스터 유닛 제거

다음 섹션에서는 클러스터에서 유닛을 일시적으로 또는 영구적으로 제거하는 방법을 설명합니다.

임시 제거

하드웨어나 네트워크 장애 등의 이유 때문에 클러스터 유닛이 클러스터에서 자동으로 제거됩니다. 이 제거는 조건을 수정할 때까지 임시로 적용되며, 클러스터에 다시 참여할 수 있습니다. 클러스터링을 수동으로 비활성화할 수도 있습니다.

디바이스가 현재 클러스터에 있는지 확인하려면, 애플리케이션에서 **show cluster info** 명령을 사용해 Firepower Chassis Manager **Logical Devices(**논리적 디바이스**)** 디바이스

FMC을(를) 사용하는 FTD의 경우에는 FMC 디바이스 목록에 디바이스를 남겨 두어야 클러스터링 재활성화 후 전체 기능을 다시 사용할 수 있습니다.

- 애플리케이션에서 클러스터링 비활성화 - 애플리케이션 CLI를 사용하여 클러스터링을 비활성화할 수 있습니다. **cluster remove unit** *name* 명령을 입력해 로그인한 유닛 외의 모든 유닛을 제거합니다. 부트스트랩 설정과 제어 유닛에서 동기화한 마지막 설정도 그대로 유지되므로 나중에 설정이 유실되는 일 없이 유닛을 다시 추가할 수 있습니다. 이 명령을 데이터 유닛에 입력해서 제어 유닛을 제거하면 새로운 제어 유닛이 선택됩니다.

  디바이스가 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 재개하려면 클러스터링을 다시 활성화합니다. 관리 인터페이스에서는 부트스트랩 구성에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우에는 관리 인터페이스가 비활성화됩니다.

  클러스터링을 다시 활성화하려면 FTD에 **cluster enable**을(를) 입력합니다.

- 애플리케이션 인스턴스 비활성화 - **Logical Devices(**논리적 디바이스**)** 페이지의 Firepower Chassis Manager에서 슬라이더 활성화됨( )을(를) 클릭합니다. 나중에 슬라이더 비활성화됨( )을(를) 사용하여 다시 활성화할 수 있습니다.

- 보안 모듈/엔진 종료 - **Security Module/Engine(**보안 모듈/엔진**)** 페이지의 Firepower Chassis Manager에서 전원 끄기 아이콘을 클릭합니다.

- 섀시 종료 - **Overview(**개요**)** 페이지의 Firepower Chassis Manager에서 종료 아이콘을 클릭합니다.

영구 제거

다음 방법을 사용하면 클러스터 멤버를 영구적으로 제거할 수 있습니다.

FMC을(를) 사용하는 FTD의 경우, 섀시에서 클러스터링을 비활성화하면 유닛을 FMC 디바이스 목록에서 제거해야 합니다.

- 논리적 디바이스 삭제 - **Logical Devices(**논리적 디바이스**)** 페이지의 Firepower Chassis Manager에서 삭제( )을(를) 클릭합니다. 이제 독립형 논리적 디바이스, 새 클러스터를 구축하거나 동일한 클러스터에 새 논리적 디바이스를 추가할 수 있습니다.

- 서비스에서 섀시 또는 보안 모듈 제거- 서비스에서 디바이스를 제거하면, 교체 하드웨어를 클러스터의 새 멤버로 추가할 수 있습니다.

FMC: 클러스터 멤버 관리

클러스터를 배치한 후에는 컨피그레이션을 변경하고 클러스터 멤버를 관리할 수 있습니다.

새 클러스터 멤버 추가

FXOS에서 새 클러스터 멤버를 추가할 때 Firepower Management Center에서는 멤버를 자동으로 추가합니다.

시작하기 전에

- 인터페이스 구성은 다른 섀시의 교체 유닛과 동일해야 합니다.

프로시저

단계 **1** FXOS에서 클러스터에 새 장치를 추가합니다. FXOS 설정 가이드를 참조하십시오.

새 유닛이 클러스터에 추가될 때까지 기다립니다. 클러스터 상태를 보려면 Firepower 섀시 관리자의 논리적 디바이스 화면을 참조하거나 Firepower Threat Defense **show cluster info** 명령어를 사용하십시오.

단계 **2** 새 클러스터 멤버는 자동으로 추가됩니다. 교체 유닛 등록을 모니터링하려면 다음을 확인합니다.

- **Cluster Status(**클러스터 상태**)** 대화 상자(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) 아이콘 또는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 탭 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크)—섀시의 클러스터에 등록 중인 장치는 "클러스터 등록 중"이 표시됩니다. 클러스터에 참가한 후 FMC이 등록을 시도하며 상태가 "등록 사용 가능"으로 변경됩니다. 등록이 완료되면 상태가 "동기화 중"으로 변경됩니다. 등록에 실패하는 경우 유닛은 "등록 사용 가능" 상태가 유지됩니다. 이 경우 조정을 클릭하여 강제로 다시 등록합니다.
- 시스템 상태 아이콘 > **Task(**작업**)** - FMC는 모든 등록 이벤트 및 오류를 표시합니다.
- 디바이스 > 디바이스 관리 - 디바이스 목록 페이지에서 클러스터를 확장하면 유닛이 등록될 때 왼쪽에 로딩 아이콘이 표시되는 것을 볼 수 있습니다.

클러스터 멤버 교체

기존 클러스터에서 클러스터 멤버를 추가하거나 교체합니다. FMC은 교체 유닛을 자동으로 감지합니다. 하지만 FMC의 기존 클러스터 멤버를 수동으로 삭제해야 합니다. 이 절차는 다시 초기화하는 유닛에도 적용됩니다. 이 경우 하드웨어는 동일하지만 새로운 멤버로 표시됩니다.

시작하기 전에

- 인터페이스 구성은 다른 섀시의 교체 유닛과 동일해야 합니다.

프로시저

단계 **1** 가능한 경우, 새로운 섀시에 FXOS의 이전 섀시에 대한 설정을 백업하고 복원합니다.

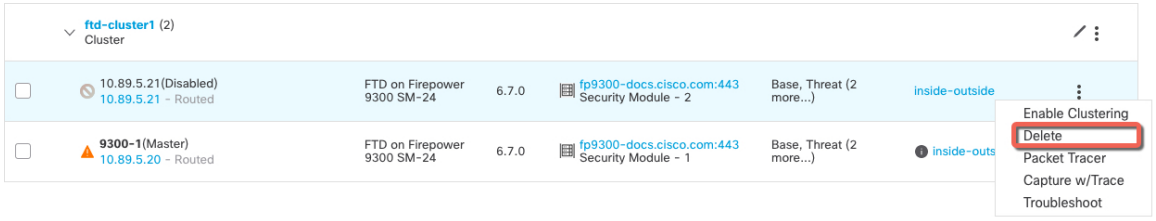
Firepower 9300에서 모듈을 교체하는 경우 이 단계를 수행할 필요가 없습니다.

기존 섀시에 백업 FXOS 컨피그레이션이 없는 경우 새 클러스터 멤버 추가, 952 페이지의 단계를 먼저 수행합니다.

아래 단계에 대한 자세한 정보는 FXOS 환경 설정 가이드를 참조하십시오.

a) Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정이 포함된 XML 파일을 내보내려면 구성 내보내기 기능을 사용합니다.
b) 교체 섀시에 설정 파일을 가져옵니다.
c) 라이선스 계약에 동의합니다.
d) 필요한 경우 클러스터의 나머지와 일치하도록 논리적 디바이스 애플리케이션의 인스턴스 버전을 업그레이드합니다.

단계 **2** 이전 유닛의 FMC에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) > **Delete(**삭제**)**을 클릭합니다.



단계 **3** 유닛을 삭제하려면 확인합니다.

유닛이 클러스터 및 FMC 디바이스 리스트에서 삭제됩니다.

단계 **4** 신규 또는 새로 초기화된 클러스터 멤버는 자동으로 추가됩니다. 교체 유닛 등록을 모니터링하려면 다음을 확인합니다.

- **Cluster Status(**클러스터 상태**)** 대화 상자(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) 아이콘 또는 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크)—섀시

의 클러스터에 등록 중인 장치는 "클러스터 등록 중"이 표시됩니다. 클러스터에 참가한 후 FMC이 등록을 시도하며 상태가 "등록 사용 가능"으로 변경됩니다. 등록이 완료되면 상태가 "동기화 중"으로 변경됩니다. 등록에 실패하는 경우 유닛은 "등록 사용 가능" 상태가 유지됩니다. 이 경우 **Reconcile(조정) All(전부)**을 클릭하여 강제로 다시 등록합니다.

- 시스템 ( ) > **Tasks(작업)** - FMC는 모든 등록 이벤트 및 오류를 표시합니다.
- 디바이스 > 디바이스 관리 - 디바이스 목록 페이지에서 클러스터를 확장하면 유닛이 등록될 때 왼쪽에 로딩 아이콘이 표시되는 것을 볼 수 있습니다.

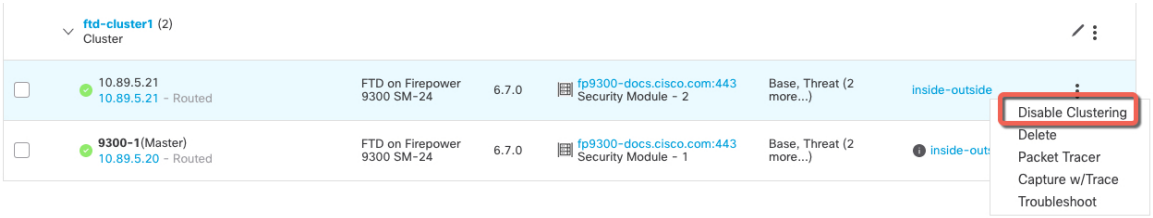
멤버 비활성화

유닛 삭제를 준비하거나 유지 보수를 위해 일시적으로 멤버를 비활성화할 수 있습니다. 이 절차는 멤버를 일시적으로 비활성화하기 위함이며, FMC 디바이스 목록에 유닛을 유지해야 합니다.

참고 유닛이 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 재개하려면 클러스터링을 다시 활성화합니다. 관리 인터페이스에서는 부트스트랩 구성에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 유닛이 클러스터에서 여전히 비활성 상태인 경우 관리 인터페이스가 비활성화됩니다. 추가 구성을 하려면 콘솔을 사용해야 합니다.

프로시저

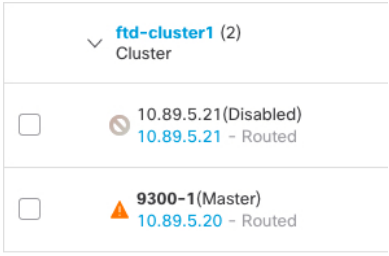
단계 **1** 비활성화하려는 유닛에 대해 **Devices(디바이스) > Device Management(디바이스 관리)** 추가 ( ) **Disable Clustering(클러스터링 비활성화)**을 선택합니다.



Cluster Status(클러스터 상태) 대화 상자(**Devices(디바이스) > Device Management(디바이스 관리) >** 추가 ( ) **> Cluster Live Status(클러스터 라이브 상태)**)에서 유닛을 비활성화할 수도 있습니다.

단계 **2** 유닛에서 클러스터링을 비활성화하고자 함을 확인합니다.

유닛이 **Devices(디바이스) > Device Management(디바이스 관리)** 목록에서 그 이름 옆에 **(Disabled(비활성화 됨))**로 표시됩니다.



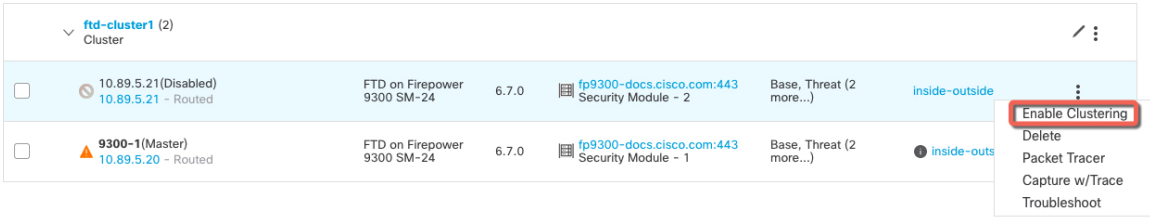
단계 **3** 클러스터링을 다시 활성화하려면 클러스터 재참가, 955 페이지의 내용을 참조하십시오.

클러스터 재참가

예를 들어 인터페이스 오류 등으로 유닛이 클러스터에서 제거되거나 수동으로 클러스터링을 비활성화한 경우 유닛 CLI에 액세스하여 클러스터 다시 조인을 시도하기 전에 오류가 해결되었는지 확인하십시오. 유닛이 클러스터에서 제거되는 이유에 대한 자세한 내용은 클러스터 다시 참가, 966 페이지을 참조하십시오.

프로시저

단계 **1** 다시 활성화하려는 유닛에 대해 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 추가 (⋮) **Enable Clustering(**클러스터링 다시 활성화**)**을 선택합니다.



Cluster Status(클러스터 상태**)** 대화 상자(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) > **Cluster Live Status(**클러스터 라이브 상태**)**)에서 유닛을 다시 활성화할 수도 있습니다.

단계 **2** 유닛에서 클러스터링을 활성화할지 확인합니다.

데이터 유닛 삭제

클러스터 멤버를 영구적으로 제거해야 한다면(예를 들어 Firepower 9300에서 모듈, 섀시를 제거하는 경우) FMC에서 삭제해야 합니다.

클러스터의 정상 부분에 해당하거나, 멤버를 임시로 비활성화하고 싶다면 멤버를 삭제해선 안 됩니다. FXOS의 클러스터에서 영구적으로 삭제하는 방법은 FXOS: 클러스터 유닛 제거, 950 페이지의 내

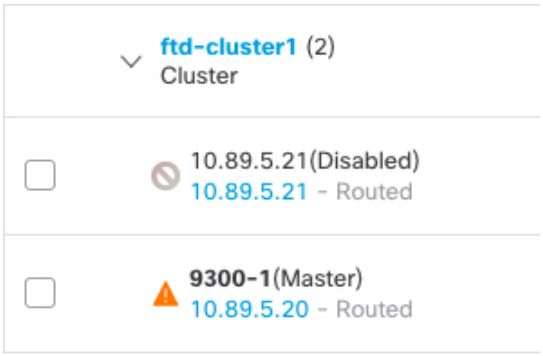
용을 참조하십시오. FMC에서 제거했지만 여전히 클러스터에 속한다면 트래픽을 계속 전달하며, FMC에서는 관리할 수 없는 제어 유닛이 될 수도 있습니다.

시작하기 전에

수동으로 유닛을 비활성화하려면 멤버 비활성화, 954 페이지의 내용을 참조하십시오. 유닛을 삭제하기 전에 수동으로 또는 상태 장애로 인해 유닛이 비활성 상태여야 합니다.

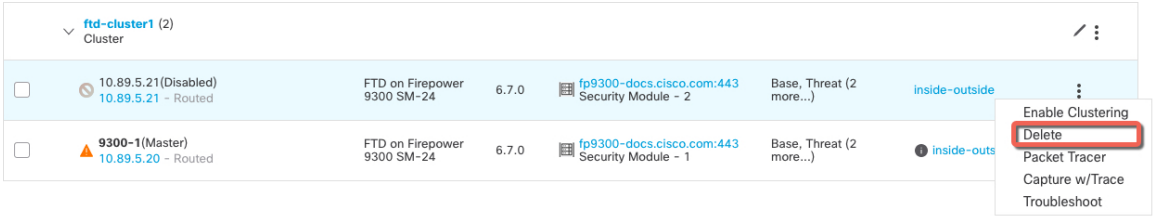
프로시저

단계 **1** FMC에서 유닛이 삭제될 수 있는지 확인합니다.**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**에서 유닛에 **(Disabled (**비활성화됨**))**가 표시되는지 확인합니다.



추가 (⋮)의 **Cluster Status(**클러스터 상태**)** 대화 상자에서 각 유닛의 상태를 확인할 수도 있습니다. 상태가 변하지 않는 경우 **Cluster Status(**클러스터 상태**)** 대화 상자에서 **Reconcile All(**모두 조정**)**을 클릭하여 강제로 업데이트합니다.

단계 **2** 데이터 유닛의 FMC에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮) > **Delete(**삭제**)**을 클릭합니다.



단계 **3** 유닛을 삭제하려면 확인합니다.

유닛이 클러스터 및 FMC 디바이스 리스트에서 삭제됩니다.

제어 유닛 변경

주의 제어 유닛을 변경하는 가장 좋은 방법은 제어 유닛의 클러스터링을 비활성화한 후 새 제어가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 제어 유닛이 될 정확한 유닛을 지정해야 할 경우, 이 섹션의 절차를 참조하십시오. 그러나 중앙 집중식 기능의 경우, 이 절차를 통해 제어 유닛을 강제로 변경하면 모든 연결이 끊어지며 새 제어 유닛에서 연결을 다시 설정해야 합니다.

제어 유닛을 변경하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > 추가 (⋮)> **Cluster Live Status(**클러스터 라이브 상태**)**를 선택하여 **Cluster Status(**클러스터 상태**)** 대화 상자를 엽니다.

Devices(디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크에서 **Cluster Status(**클러스터 상태**)** 대화 상자에 액세스할 수도 있습니다.

단계 **2** 제어 유닛이 될 유닛에 대해 추가 (⋮) **Change Role to Control(**역할을 제어로 변경**)**을 선택합니다.

단계 **3** 역할 변경을 확인하라는 메시지가 표시됩니다. 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

클러스터 멤버 조정

클러스터 멤버 등록에 실패하면 섀시에서 Firepower Management Center에 대해 클러스터 멤버십을 다시 조정합니다. 예를 들어, FMC이 특정 프로세스 중이거나 네트워크에 문제가 있는 경우, 데이터 유닛 등록에 실패할 수 있습니다.

프로시저

단계 **1** 클러스터에 대해 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 추가 (⋮)를 선택한 다음 **Cluster Live Status(**클러스터 라이브 상태**)**를 선택하여 **Cluster Status(**클러스터 상태**)** 대화 상자를 엽니다.

Devices(디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크에서 **Cluster Status(**클러스터 상태**)** 대화 상자를 열 수도 있습니다.

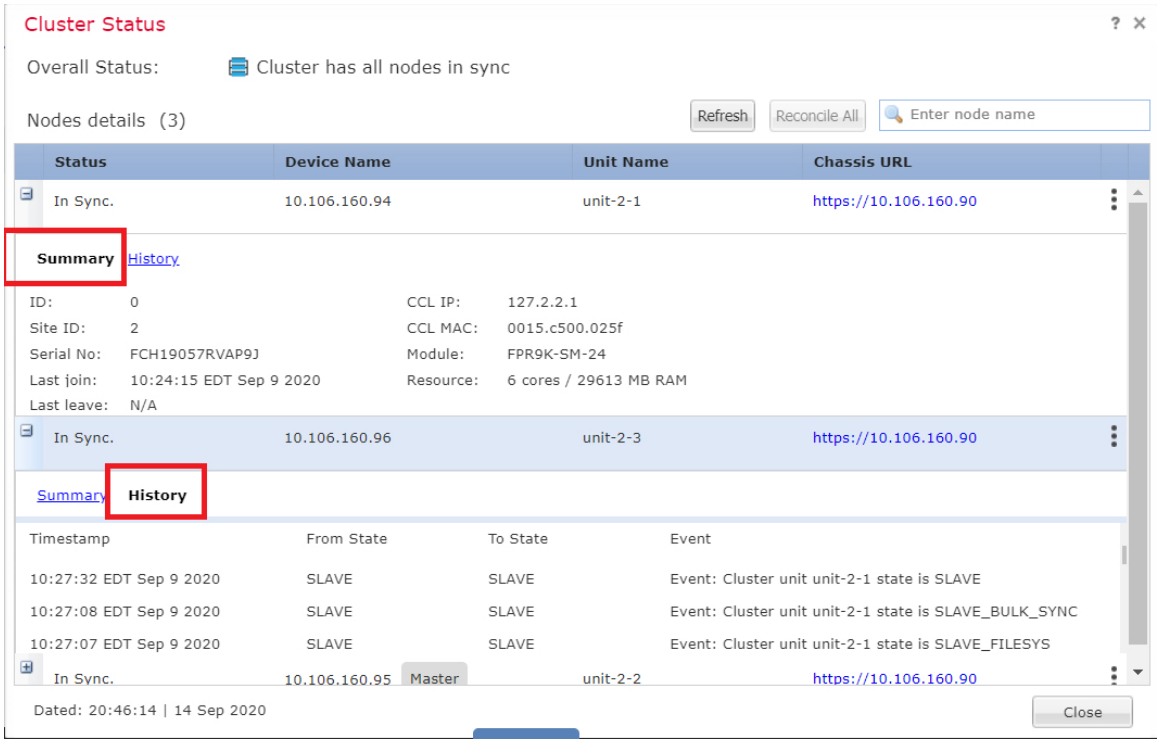
단계 **2** **Reconcile(**조정**)All(**모두**)**을 클릭합니다.

클러스터 상대에 대한 자세한 내용은 FMC: 클러스터 모니터링, 958 페이지을 참고하십시오.

FMC: 클러스터 모니터링

Firepower Management Center과 FTD CLI에서 클러스터를 모니터링할 수 있습니다.

- **Cluster Status(**클러스터 상태**)** 대화 상자는 **Devices(**디바이스**) > Device Management** > 추가 (⋮) 아이콘 또는 **Devices(**디바이스**) > Device Management(**디바이스 관리**) > Cluster(**클러스터**)** 페이지 > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)**에서 제공됩니다.



제어 유닛에는 역할을 식별하는 그래픽 표시기가 있습니다.

클러스터 멤버 상태에는 다음 상태가 포함됩니다.

- 동기화 중 - 유닛이 FMC에 등록되었습니다.
- 등록 보류 중 - 유닛이 클러스터의 일부이지만 아직 FMC에 등록되지 않았습니다. 유닛 등록에 실패하는 경우, **Reconcile(**조정**)All(**모두**)**을 클릭하여 등록을 다시 시도할 수 있습니다.
- 클러스터링이 비활성화됨 - 유닛이 FMC에 등록되었지만, 클러스터의 비활성 멤버입니다. 클러스터링 설정은 나중에 다시 활성화하려는 경우에도 그대로 유지됩니다. 또는 클러스터에서 유닛을 삭제할 수 있습니다.
- 클러스터 참가 중... - 유닛이 새시의 클러스터에 참가 중이지만 아직 참가가 완료되지 않았습니다. 참가가 끝나면 FMC로 등록합니다.

각 유닛에 대해 요약 또는 기록을 볼 수 있습니다.

추가 (⋮) 메뉴의 각 유닛에 대해 다음 상태 변경을 수행할 수 있습니다.

- 클러스터링 비활성화
- 클러스터링 활성화
- 역할을 제어로 변경

- 시스템 (⚙) > **Tasks(**작업**)** 페이지로 이동합니다.

  Tasks(작업**)** 페이지는 각 유닛 등록에 대한 클러스터 등록 작업의 업데이트를 보여줍니다.

- 디바이스 > 디바이스 관리 > *cluster_name*입니다.

  디바이스 목록 페이지에서 클러스터를 확장하는 경우, IP 주소 옆에 해당 역할과 함께 표시되는 제어 유닛을 포함하여 모든 멤버 유닛을 볼 수 있습니다. 아직 등록 중인 유닛은 로딩 아이콘이 표시됩니다.

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  전체 클러스터에 대한 집계된 데이터 또는 다른 정보를 보려면 **show cluster** 명령을 사용합니다.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  클러스터 정보를 보려면 **show cluster info** 명령을 사용합니다.

클러스터링에 대한 참조

이 섹션에는 클러스터링이 작동하는 방식에 대한 자세한 정보가 포함되어 있습니다.

Firepower Threat Defense 기능 및 클러스터링

일부 FTD 기능은 클러스터링이 지원되지 않으며, 일부 기능은 기본 유닛에서만 지원됩니다. 기타 기능의 경우 올바르게 사용하는 데 필요한 주의 사항이 있을 수 있습니다.

클러스터링으로 지원되지 않는 기능

이러한 기능은 클러스터링을 사용하도록 설정한 경우 구성할 수 없으며 명령이 거부됩니다.

참고 클러스터링으로도 지원되지 않는 FlexConfig 기능(예: WCCP 검사)을 보려면 ASA 일반 운영 설정 가이드를 참조하십시오. FlexConfig를 사용하면 FMC GUI에 없는 여러 ASA 기능을 설정할 수 있습니다. Firepower Threat Defense에 대한 FlexConfig 정책, 1269 페이지를 참조하십시오.

- Site-Site VPN
- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)

- DHCP 클라이언트, 서버, 프록시 DHCP 릴레이가 지원됩니다.
- 고가용성
- 통합 라우팅 및 브리징
- FMC UCAPL/CC 모드

클러스터링을 위한 중앙 집중식 기능

다음 기능은 제어 유닛에서만 지원되며 클러스터에 확장되지 않습니다.

참고 중앙 집중식 기능의 트래픽은 클러스터 제어 링크를 통해 멤버 유닛에서 제어 유닛으로 전달됩니다.

리밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 제어 유닛으로 리밸런싱될 수 있습니다. 이렇게 되면 해당 트래픽은 제어 유닛으로 다시 전송됩니다.

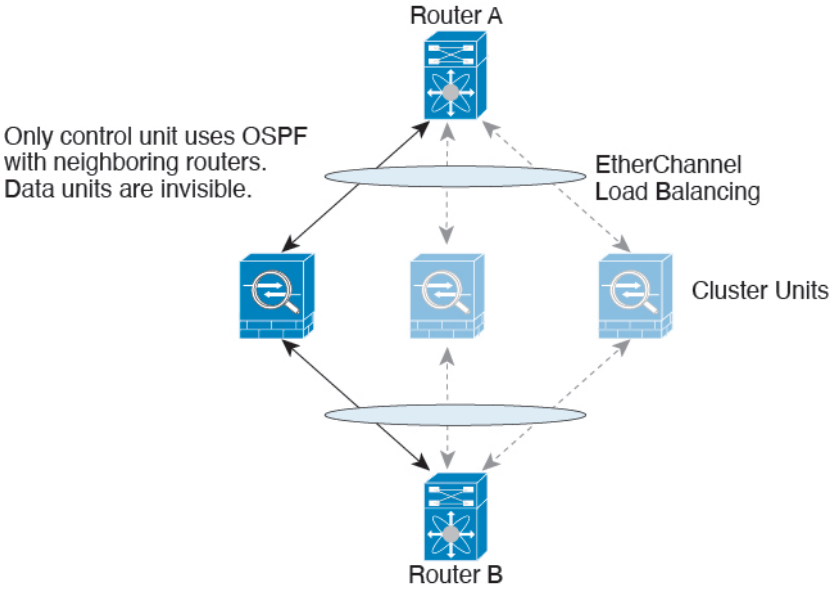
중앙 집중식 기능의 경우 제어 유닛에 오류가 발생하면 모든 연결이 취소되며 새 제어 유닛에서 연결을 다시 설정해야 합니다.

- 다음과 같은 애플리케이션 감시:
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- 동적 라우팅
- 고정 경로 모니터링

동적 라우팅 및 클러스터링

라우팅 프로세스는 제어 유닛에서만 실행되며, 경로는 제어 유닛을 통해 파악되고 보조 유닛에 복제됩니다. 라우팅 패킷이 데이터 유닛에 전송되면 해당 패킷은 제어 유닛에 리디렉션됩니다.

그림 *34:* 동적 라우팅



데이터 유닛이 제어 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 제어 유닛에서 데이터 유닛으로 동기화되지 않습니다. 제어 유닛 전환이 있을 경우, 네이버 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

연결 설정

연결 제한은 클러스터 전체에서 시행됩니다. 각 유닛에는 브로드캐스트 메시지를 기반으로 한 클러스터 전체의 카운터 값이 표시됩니다. 효율성을 고려하여 클러스터 전체에 구성된 연결 제한이 제한 수에 정확하게 적용되지 않을 수 있습니다. 각 유닛은 언제든지 클러스터 전체 카운터 값을 과대 평가하거나 과소 평가할 수 있습니다. 그러나 로드 밸런싱된 클러스터에서는 시간이 지남에 따라 정보가 업데이트됩니다.

FTP 및 클러스터링

- 다른 클러스터 멤버가 FTP 데이터 채널 및 제어 채널의 흐름을 소유한 경우, 데이터 채널 소유자 유닛에서는 유휴 시간 제한 업데이트를 제어 채널 소유자에게 주기적으로 전송하고 유휴 시간 제한 값을 업데이트합니다. 그러나 제어 흐름 소유자가 다시 로드되고 제어 흐름이 다시 호스팅된 경우, 부모/자식 흐름 관계가 더 이상 유지되지 않으며 제어 흐름 유휴 시간 제한도 업데이트되지 않습니다.

NAT 및 클러스터링

NAT는 클러스터의 전체 처리량에 영향을 미칠 수 있습니다. 로드 밸런싱 알고리즘은 IP 주소와 포트를 기반으로 할 뿐만 아니라 NAT로 인해 인바운드 및 아웃바운드 패킷의 IP 주소 및/또는 포트가 서로 달라질 수 있으므로, 인바운드 및 아웃바운드 NAT 패킷을 클러스터의 다른 FTD에 전송할 수 있습니다. 패킷이 NAT 소유자가 아닌 FTD에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다. 보안 및 정책 확인 결과에 따라 NAT 소유자가 패킷에 대해 연결을 생성하지 않을 수도 있으므로 수신 유닛은 소유자에 대한 전달 플로우를 생성하지 않습니다.

클러스터링에 NAT를 계속 사용하려면 다음 지침을 숙지하십시오.

- 포트 블록 할당이 있는 PAT - 이 기능에 대한 다음 지침을 참조하십시오.
  - 호스트당 최대 제한은 클러스터 전체 제한이 아니며 각 유닛에서 개별적으로 적용됩니다. 호스트당 최대 제한이 1로 구성된 3-노드 클러스터에서, 호스트의 트래픽이 3개 유닛 모두에 부하 분산되는 경우 각 유닛에 하나씩 3개의 블록이 할당될 수 있습니다.
  - 백업 풀의 백업 유닛에서 생성된 포트 블록은 호스트당 최대 제한을 적용할 때 고려되지 않습니다.
  - 완전히 새로운 IP 범위로 PAT 풀을 수정하는 즉석 PAT 규칙 수정을 수행할 경우, 새 풀이 작동하게 되는 동안 여전히 전환 중이던 xlate 백업 요청에 대해 xlate 백업 생성이 실패하게 됩니다. 이러한 동작은 포트 블록 할당 기능과 관련이 없으며, 풀이 분산되고 트래픽이 클러스터 유닛 전체에서 부하 분산되는 클러스터 구축 과정에서만 발생하는 일시적인 PAT 풀 문제입니다.
  - 클러스터에서 작업할 때는 단순히 블록 할당 크기를 변경할 수 없습니다. 새 크기는 클러스터에서 각 디바이스를 다시 로드한 후에만 적용됩니다. 각 디바이스를 다시 로드하지 않으려면 모든 블록 할당 규칙을 삭제하고 해당 규칙과 관련된 모든 xlate를 지우는 것이 좋습니다. 그런 다음 블록 크기를 변경하고 블록 할당 규칙을 다시 생성할 수 있습니다.
- 동적 PAT에 대한 NAT 풀 주소 분산 - PAT 풀을 구성하면 클러스터는 풀의 각 IP 주소를 포트 블록으로 나눕니다. 기본적으로 각 블록은 512포트이지만 포트 블록 할당 규칙을 구성하는 경우에는 블록 설정이 대신 사용됩니다. 이러한 블록은 클러스터의 유닛 간에 균등하게 분산되므로 각 유닛에는 PAT 풀의 각 IP 주소에 대해 하나 이상의 블록이 있습니다. 따라서 예상되는 PAT 처리된 연결 수에 충분한 경우 클러스터의 PAT 풀에 IP 주소를 하나만 포함할 수 있습니다. PAT 풀 NAT 규칙에 예약된 포트 1~1023을 포함하도록 옵션을 구성하지 않는 한 포트 블록은 1024~65535 포트 범위를 포함합니다.
- 여러 규칙에서 PAT 풀 재사용 - 여러 규칙에서 동일한 PAT 풀을 사용하려면 규칙에서 인터페이스 선택에 주의해야 합니다. 모든 규칙에서 특정 인터페이스를 사용하거나 또는 모든 규칙에서 "any(임의의)"를 사용해야 합니다. 규칙 전체에서 특정 인터페이스와 "any(임의의)"를 혼합할 수 없거나, 시스템에서 클러스터의 오른쪽 노드에 대한 반환 트래픽을 일치시키지 못할 수 있습니다. 규칙 당 고유한 PAT 풀을 사용하는 것은 가장 신뢰할 수 있는 옵션입니다.
- 라운드 로빈 없음 — 클러스터링에서는 PAT 풀을 위한 라운드 로빈을 지원하지 않습니다.
- 확장 PAT 없음 - 클러스터링에서 확장 PAT가 지원되지 않습니다.

- 제어 유닛에 의해 관리되는 동적 NAT xlate — 제어 유닛에서는 xlate 테이블을 유지하고 이를 데이터 유닛에 복제합니다. 동적 NAT가 필요한 연결이 데이터 유닛에 전달되고 xlate가 테이블에 없을 경우, 데이터 유닛에서는 제어 유닛에서 xlate를 요청합니다. 데이터 유닛에서는 이 연결을 소유합니다.
- 오래된 xlates - 연결 소유자의 xlate 유휴 시간이 업데이트되지 않습니다. 따라서 유휴 시간이 유휴 시간 제한을 초과할 수 있습니다. refcnt가 0인 구성된 시간 초과 값보다 큰 유휴 타이머 값은 오래된 xlate를 나타냅니다.
- 다음을 검사할 수 있는 고정 PAT 없음
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

SIP 검사 및 클러스터링

로드 밸런싱으로 인해 모든 디바이스에서 제어 흐름을 만들 수 있지만 자식 데이터 흐름은 동일한 디바이스에 상주해야 합니다.

SNMP 및 클러스터링

SNMP 에이전트에서는 진단 인터페이스 로컬 IP 주소로 각각의 개별 FTD를 폴링합니다. 클러스터의 통합 데이터는 폴링할 수 없습니다.

SNMP 폴링에는 기본 클러스터 IP 주소가 아닌 로컬 주소를 항상 사용해야 합니다. SNMP 에이전트에서 기본 클러스터 IP 주소를 폴링하면서 새 제어 유닛이 선택된 경우, 새 제어 유닛에 대한 폴링이 이루어지지 않습니다.

Syslog 및 클러스터링

- 클러스터의 각 유닛에서는 고유한 syslog 메시지를 생성합니다. 각 유닛에서 syslog 메시지 헤더 필드에 동일하거나 다른 디바이스 ID를 사용하도록 로깅을 구성할 수 있습니다. 예를 들어, 호스트 이름 구성은 클러스터의 모든 유닛에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 유닛에서는 단일 유닛에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 구성에 할당된 로컬-유닛 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, syslog 메시지는 다른 유닛에서 생성된 것처럼 보입니다.

TLS/SSL 연결 및 클러스터링

TLS/SSL 연결의 암호 해독된 상태는 동기화되지 않습니다. 연결 소유자 장애가 발생하는 경우, 암호 해독된 연결이 재설정됩니다. 새 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.

Cisco TrustSec 및 클러스터링

제어 유닛에서만 SGT(보안 그룹 태그) 정보를 파악합니다. 그런 다음 제어 유닛에서는 SGT를 데이터 유닛에 제공하며, 데이터 유닛에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

성능 확장 요소

클러스터에 여러 유닛을 결합할 경우 총 클러스터 성능을 대략 다음과 같이 예측할 수 있습니다.

- 통합 TCP 또는 CPS 처리량의 80%
- 통합 UDP 처리량의 90%
- 트래픽 조합에 따라 통합된 EMIX(이더넷 MIX) 처리량의 60%

예를 들어 TCP 처리량의 경우 3개의 SM-44 모듈이 있는 Firepower 9300은 단독으로 실행하면 실제 방화벽 트래픽 중 약 135Gbps를 처리할 수 있습니다. 2개의 섀시의 경우 최대 통합 처리량은 270Gbps(2개 섀시 x 135Gbps)의 약 80%인 216Gbps입니다.

제어 유닛 선택

클러스터의 멤버는 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 제어 '유닛을 선택합니다.

1. 클러스터를 구축할 때 각 유닛은 3초마다 선택 요청을 브로드캐스트합니다.
2. 다른 유닛의 우선순위가 더 높을 경우 해당 유닛이 선택 요청에 응답하게 됩니다. 우선순위는 클러스터를 구축할 때 설정되며 구성 불가능합니다.
3. 45초 후에 우선순위가 더 높은 다른 유닛에서 응답을 받지 못한 유닛은 제어 유닛이 됩니다.

참고 가장 우선순위가 높은 유닛이 공동으로 여러 개인 경우, 클러스터 유닛 이름과 일련 번호를 사용하여 제어 유닛을 결정합니다.

4. 유닛이 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 유닛이 자동으로 제어 유닛이 되는 것은 아닙니다. 기존 제어 유닛은 응답이 중지되지 않는 한 항상 제어 유닛으로 유지되며 응답이 중지될 때에 새 제어 유닛이 선택됩니다.
5. 제어 유닛이 일시적으로 여러 개 있는 "스플릿 브레인" 시나리오에서는 우선 순위가 가장 높은 유닛이 역할을 유지하는 반면 다른 유닛은 데이터 유닛 역할로 돌아갑니다.

참고 유닛을 수동으로 강제 변경하여 제어 유닛이 되도록 할 수 있습니다. 중앙 집중식 기능의 경우 제어 유닛을 강제로 변경하면 모든 연결이 취소되며 새 제어 유닛에서 연결을 다시 설정해야 합니다.

클러스터 내의 고가용성

클러스터링에서는 섀시, 유닛 및 인터페이스의 상태를 모니터링하고 유닛 간의 연결 상태를 복제하여 고가용성을 제공합니다.

섀시 애플리케이션 모니터링

섀시 애플리케이션 상태 모니터링은 항상 활성화되어 있습니다. Firepower 4100/9300 섀시 수퍼바이저는 Firepower Threat Defense 애플리케이션을 주기적으로(1초마다) 검사합니다. Firepower Threat Defense 디바이스가 작동 중인데 Firepower 4100/9300 섀시 수퍼바이저와 3초 동안 통신할 수 없는 경우, Firepower Threat Defense 디바이스에서는 syslog 메시지를 생성하고 클러스터를 떠납니다.

Firepower 4100/9300 섀시 수퍼바이저가 45초 후에 애플리케이션과 통신할 수 없는 경우, Firepower Threat Defense 디바이스를 다시 로드합니다. Firepower Threat Defense 디바이스가 수퍼바이저와 통신할 수 없는 경우, 클러스터에서 자신을 제거합니다.

유닛 상태 모니터링

각 유닛은 클러스터 제어 링크를 통해 브로드 캐스트 keepalive keepalive 패킷을 주기적으로 전송합니다. 제어 유닛이 시간 초과 기간 내에 데이터 유닛에서 keepalive keepalive 패킷 또는 기타 패킷을 수신하지 않는 경우, 제어 유닛은 클러스터에서 데이터 유닛을 제거합니다. 데이터 유닛이 제어 유닛에서 패킷을 수신하지 않으면 나머지 제어 멤버에서 새 제어 유닛이 선택됩니다.

네트워크 장애로 인해 유닛이 실제로 장애가 발생한 것이 아니라 클러스터 제어 링크를 통해 유닛이 서로 연결할 수 없는 경우, 클러스터는 격리된 데이터 유닛이 자체 제어 유닛을 선택하는 "스플릿 브레인" 시나리오로 전환될 수 있습니다. 예를 들어 두 클러스터 위치 간에 라우터가 실패하면 위치 1의 원래 제어 유닛이 클러스터에서 위치 2 데이터 유닛을 제거합니다. 한편, 위치 2의 유닛은 자체 제어 유닛을 선택하고 자체 클러스터를 구성합니다. 이 시나리오에서는 비대칭 트래픽이 실패할 수 있습니다. 클러스터 제어 링크가 복원되면 우선 순위가 더 높은 제어 장치가 제어 장치의 역할을 유지합니다. 자세한 내용은 제어 유닛 선택, 964 페이지를 참조하십시오.

인터페이스 모니터링

각 유닛에서는 사용 중인 모든 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 제어 유닛에 보고합니다. 섀시 간 클러스터링의 경우 Spanned EtherChannel은 클러스터 cLACP(Link Aggregation Control Protocol)를 사용합니다. 각 섀시에서는 링크 상태 및 cLACP 프로토콜 메시지를 모니터링하여 EtherChannel에서 포트가 아직 활성화된 상태인지 확인하고 인터페이스가 작동 중단 상태인지 Firepower Threat Defense 애플리케이션에 정보를 제공합니다. 물리적 인터페이스가 모니터링됩니다(EtherChannel 인터페이스에 대한 기본 EtherChannel 포함). 작동 상태인 명명된 인터페이스만 모니터링 대상이 될 수 있습니다. 예를 들어, EtherChannel의 모든 멤버 포트는 명명된 EtherChannel이 클러스터에서 제거되기 전에 장애가 발생해야 합니다.

특정 유닛의 모니터링된 인터페이스에 장애가 발생하였으나 다른 유닛에서는 액티브 상태인 경우, 클러스터에서 해당 유닛이 제거됩니다. Firepower Threat Defense 디바이스에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다. Firepower Threat Defense 디바이스에서는 유닛이 클러스터에 참가하는 처음 90초 동안에는 인터페이스를 모니터링하지 않습니다. 이 시간 동안에는 인터페이스 상태가 변경되어도 Firepower Threat Defense 디바이스가 클러스터에서 제거되지 않습니다. 구성된 멤버의 경우 유닛은 500밀리초 후에 제거됩니다.

섀시 간 클러스터링의 경우 클러스터에서 EtherChannel을 추가 또는 삭제하는 경우 인터페이스 상태 모니터링은 각 섀시의 변경을 확인할 수 있도록 95초간 일시 중단됩니다.

데코레이터 애플리케이션 모니터링

인터페이스에서 Radware DefensePro 애플리케이션과 같은 데코레이터 애플리케이션을 설치하는 경우, Firepower Threat Defense 디바이스 및 데코레이터 애플리케이션 둘 다 클러스터에서 계속 작동해야 합니다. 유닛은 두 애플리케이션이 모두 작동할 때까지 클러스터에 참가하지 않습니다. 클러스터에 참가한 이후에 유닛은 3초마다 데코레이터 애플리케이션의 상태를 모니터링합니다. 데코레이터 애플리케이션이 작동하지 않으면 유닛이 클러스터에서 제거됩니다.

실패 이후 상태

클러스터의 유닛에 오류가 발생할 경우, 해당 유닛에서 호스팅하는 연결이 다른 유닛으로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 유닛의 클러스터 제어 링크를 통해 공유됩니다.

제어 유닛에 장애가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 제어 유닛이 됩니다.

FTD는 실패 이벤트에 따라 클러스터에 다시 참가하려고 시도합니다.

참고 FTD가 비활성화되고 클러스터에 자동으로 다시 조인하지 못할 경우, 모든 데이터 인터페이스가 종료되며 관리/진단 인터페이스에서만 트래픽을 주고받을 수 있습니다.

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 최초 가입 시 오류가 발생한 클러스터 제어—클러스터 제어 링크의 문제를 해결한 다음 클러스터링을 다시 활성화하여 수동으로 클러스터를 다시 가입시켜야 합니다.
- 클러스터 가입 후 클러스터 제어 링크 장애 — FTD에서는 자동으로 5분마다 무기한으로 다시 가입하려고 시도합니다.
- 데이터 인터페이스 오류 — FTD에서는 5분에 다시 참가를 시도하며 그다음에는 10분, 마지막으로 20분에 참가를 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 FTD에서는 클러스터링을 비활성화합니다. 데이터 인터페이스의 문제를 해결한 다음 수동으로 클러스터링을 활성화해야 합니다.

- 유닛 오류 — 유닛 상태 검사 오류로 인해 클러스터에서 유닛이 제거된 경우, 클러스터에 다시 참가할 수 있을지 여부는 오류의 원인에 따라 결정됩니다. 예를 들어, 일시적인 정전이 발생한 경우 클러스터 제어 링크가 작동 상태이면 전원을 다시 가동할 때 유닛이 클러스터에 다시 참가할 수 있습니다. FTD 애플리케이션은 5초마다 클러스터에 다시 참가하려고 시도합니다.
- 섀시 애플리케이션 통신 장애 — FTD 애플리케이션에서 섀시 애플리케이션 상태가 복구되었는지 탐지할 경우, 클러스터에 자동으로 다시 참가하려고 시도합니다.
- 내부 오류 — 내부 장애 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등이 있습니다. 문제를 해결한 후 클러스터링을 다시 사용하도록 설정하여 클러스터에 수동으로 다시 참가해야 합니다.
- 실패한 구성 구축-FMC에서 새 구성을 구축하는 경우 일부 클러스터 멤버에서는 구축이 실패하지만 다른 클러스터 멤버에서는 성공할 경우 실패한 유닛은 클러스터에서 제거됩니다. 문제를 해결한 후 클러스터링을 다시 사용하도록 설정하여 클러스터에 수동으로 다시 참가해야 합니다. 제어 유닛에서 구축이 실패하면 구축이 롤백되고 멤버가 제거되지 않습니다. 모든 데이터 유닛에서 구축이 실패하면 구축이 롤백되고 멤버가 제거되지 않습니다.

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 장애 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다. 백업 소유자는 일반적으로 관리자이기도 합니다.

일부 트래픽의 경우 TCP 또는 UDP 레이어 상위에 대한 상태 정보가 필요합니다. 클러스터링 지원에 대해 알아보거나 이러한 종류의 트래픽에 대한 지원이 부족한 경우 다음 표를 참조하십시오.

표 ***79:*** 클러스터 전반에 걸쳐 복제된 기능

트래픽	상태 지원	**Notes(**참고**)**
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	—
MAC 주소 테이블	예	—
사용자 ID	Yes(예)	—
IPv6 네이버 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—
중앙 집중식 VPN(사이트 대 사이트)	아니요	제어 유닛에 오류가 발생할 경우 VPN 세션의 연결이 끊어집니다.

클러스터에서 연결을 관리하는 방법

클러스터의 여러 멤버에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다.

연결 역할

각 연결에 대해 정의된 다음 역할을 참조하십시오.

- 소유자 - 일반적으로 연결을 가장 처음 수신하는 유닛입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다. 원래 소유자가 실패하고 새 유닛이 연결에서 패킷을 수신하면, 관리자는 해당 유닛으로부터 새 소유자를 선택합니다.
- 백업 소유자 - 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있도록 소유자로부터 수신한 TCP/UDP 상태 정보를 저장하는 유닛입니다. 백업 소유자는 장애 발생 시 연결을 승계할 수 없습니다. 소유자를 사용할 수 없을 경우, 연결에서 패킷을 받을(로드 밸런싱을 기준으로) 첫 번째 유닛이 백업 소유자에 관련 상태 정보를 문의하면 해당 백업 소유자가 새로운 소유자가 될 수 있습니다.

  관리자(아래 설명 참조)는 소유자와 같은 유닛이 아니라면 백업 소유자로도 사용됩니다. 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  Firepower 9300의 섀시 간 클러스터링(섀시 하나에 클러스터 유닛이 3개까지 포함될 수 있음)에서 백업 소유자가 소유자와 같은 섀시에 있으면 섀시 장애로부터 플로우를 보호하기 위해 다른 섀시에서 추가 백업 소유자가 선택됩니다.
- 관리자 - 전달자의 소유자 조회 요청을 처리하는 유닛입니다. 소유자가 새 연결을 수신할 경우, 소유자 유닛에서는 소스/대상 IP 주소와 포트의 해시를 기준으로 관리자 유닛을 선택하며 관리자 유닛에 메시지를 전송하여 새 연결을 등록합니다. 패킷이 소유자 유닛이 아닌 다른 유닛에 전달될 경우, 해당 유닛에서는 관리자 유닛에 어떤 유닛이 소유자인지 조회하여 패킷이 전달될 수 있도록 합니다. 연결이 하나인 경우 관리자 유닛도 1개뿐입니다. 관리자가 실패하면 소유자는 새 관리자를 선택합니다.

  관리자는 소유자와 같은 유닛이 아니라면 백업 소유자로도 사용됩니다(위의 설명 참조). 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.
- 전달자 — 패킷을 소유자 유닛에 전달하는 유닛입니다. 소유하지 않은 연결 패킷이 전달자 유닛에 수신될 경우, 전달자 유닛에서는 소유자 유닛의 관리자를 조회한 다음 이러한 연결을 수신하는 기타 모든 패킷의 소유자에 대한 흐름을 설정합니다. 관리자 유닛은 전달자가 될 수도 있습니다. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 시퀀스 임의 설정을 비활성화한 경우 SYN 쿠키는 사용되지 않으며, 책임자에게 쿼리해야 합니다.) DNS 및 ICMP 같이 짧은 흐름의 경우 쿼리 대신 전달자가 책임자에게 패킷을 즉시 전송하고 책임자가 소유자에게 전송합니다. 하나의 연결에 여러 개의 전달자 유닛이 있을 수 있습니다. 가장 효율적인 처리량 목표를 실현하려면 전달자가 없고 연결의 모든 패킷이 소유자 유닛에 전송되는 우수한 로드 밸런싱 방법을 사용합니다.

참고 클러스터링을 사용할 때는 TCP 시퀀스 임의 설정을 비활성화하지 않는 것이 좋습니다. SYN/ACK 패킷이 삭제될 수 있으므로 일부 TCP 세션이 설정되지 않을 가능성이 적습니다.

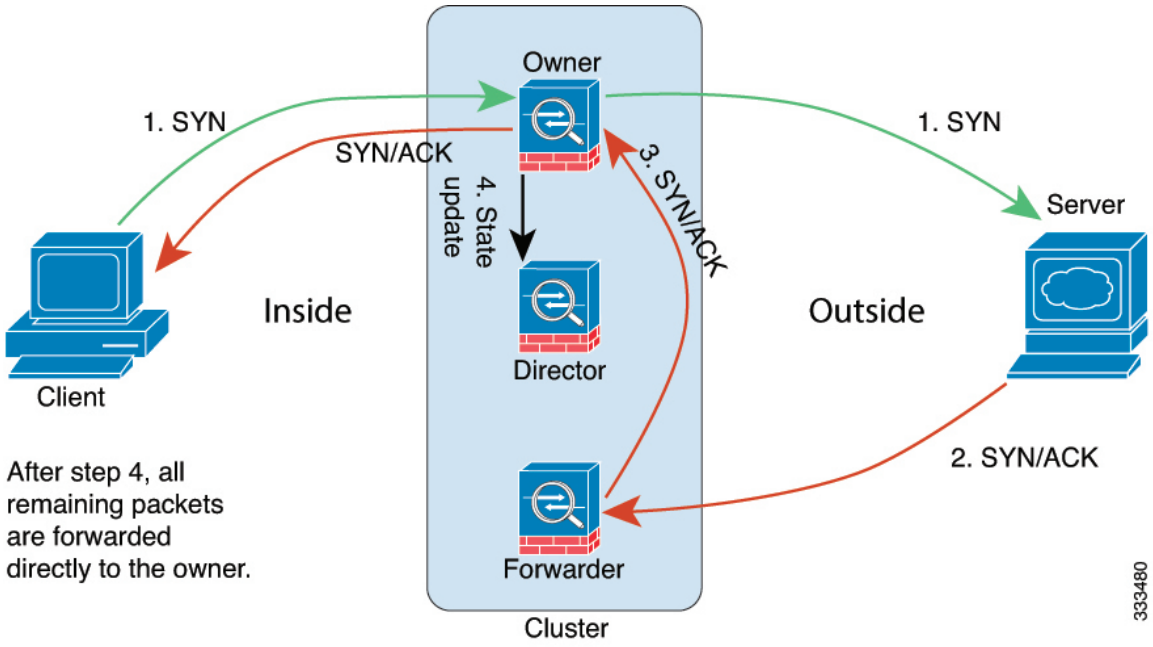
- 프래그먼트 소유자 - 프래그먼트화된 패킷의 경우 프래그먼트를 수신하는 클러스터 유닛이 프래그먼트 소스 IP 주소, 대상 IP 주소 및 패킷 ID의 해시를 사용하여 프래그먼트 소유자를 결정합니다. 그런 다음 모든 프래그먼트가 클러스터 제어 링크를 통해 프래그먼트 소유자에게 전달됩니다. 첫 번째 프래그먼트만 스위치 로드 밸런싱 해시에 사용되는 5 튜플을 포함하기 때문에 프래그먼트는 다른 클러스터 유닛으로 로드 밸런싱될 수 있습니다. 다른 프래그먼트는 소스 및 대상 포트를 포함하지 않으며 다른 클러스터 유닛에 로드 밸런싱될 수 있습니다. 프래그먼트 소유자는 패킷을 일시적으로 리어셈블하므로 소스/대상 IP 주소 및 포트의 해시를 기반으로 디렉터를 확인할 수 있습니다. 새 연결인 경우 프래그먼트 소유자가 연결 소유자로 등록됩니다. 기존 연결인 경우 프래그먼트 소유자는 클러스터 제어 링크를 통해 모든 프래그먼트를 제공된 연결 소유자에게 전달합니다. 그러면 연결 소유자가 모든 프래그먼트를 리어셈블합니다.

새 연결 소유권

로드 밸런싱을 통해 클러스터의 멤버에 새 연결이 전송될 경우, 해당 유닛에서는 연결의 양방향을 모두 소유합니다. 다른 유닛에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 유닛에 전달됩니다. 다른 유닛에 반대 방향의 흐름이 전송될 경우, 이는 원래 유닛으로 다시 리디렉션됩니다.

샘플 데이터 흐름

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.



1. SYN 패킷은 클라이언트에서 시작되고 FTD에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 흐름을 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 FTD에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 FTD는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 흐름을 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 소유자 유닛에서는 관리자 유닛에 상태 업데이트를 보내고, SYN-ACK를 클라이언트에 전달합니다.
5. 관리자 유닛에서는 소유자 유닛을 통해 상태 업데이트를 수신하고, 소유자에 대한 흐름을 생성하며, TCP 상태 정보는 물론 소유자를 기록합니다. 관리자 유닛은 연결의 백업 소유자 역할을 수행합니다.
6. 전달자 유닛에 전달된 모든 후속 패킷은 소유자 유닛에 전달됩니다.
7. 패킷이 추가 유닛에 전달된 경우, 소유자 유닛에 관리자를 쿼리하고 흐름을 설정합니다.
8. 흐름 결과의 상태가 변경되면 소유자 유닛과 관리자 유닛의 상태도 업데이트됩니다.

클러스터링 기록

기능	버전	세부 사항
클러스터 구축이 더 빨리 완료되고 이벤트가있을경우 더 빨리 실패합니다.	6.7	이제 클러스터 구축이 더 빠르게 완료됩니다. 또한 클러스터에 FMC 구축 실패를 초래하는 이벤트가 있을 경우 이제 장애가 더 빠르게 발생합니다. 신규/수정된 화면: 없음

기능	버전	세부 사항
FMC의 개선된 클러스터 관리	6.7	FMC에서는 이전에 CLI를 사용해야만 수행할 수 있었던 다음과 같은 클러스터 관리 기능을 개선했습니다. • 클러스터 유닛 활성화 및 비활성화 • 디바이스 관리 페이지에서 유닛별 히스토리 및 요약을 포함하여 클러스터 상태를 표시합니다. • 제어 유닛에 대한 역할 변경 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **More(**더 보기**)** 메뉴 • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** > **General(**일반**)** 영역 > **Cluster Live Status(**클러스터 라이브 상태**)** 링크 **Cluster Status(**클러스터 상태**)** 지원되는 플랫폼: Firepower 4100/9300
다중 인스턴스 클러스터링	6.6	이제 컨테이너 인스턴스로 클러스터를 생성할 수 있습니다. Firepower 9300에서 클러스터의 각 모듈에 하나의 컨테이너 인스턴스를 포함해야 합니다. 보안 엔진/모듈마다 하나 이상의 컨테이너 인스턴스를 추가할 수 없습니다. 각 클러스터 인스턴스에 동일한 보안 모듈 또는 섀시 모델을 사용하는 것이 좋습니다. 그러나 Firepower 9300 보안 모듈 유형이나 Firepower 4100 모델에서는 필요한 경우 동일한 클러스터에서 다른 컨테이너 인스턴스를 혼용해 사용할 수 있습니다. 동일한 클러스터에서 Firepower 9300 및 4100 인스턴스를 혼용할 수 없습니다. 신규/수정된 FXOS 명령: **set port-type cluster** 신규/수정된 Firepower Chassis Manager 화면: • 논리적 디바이스 > 클러스터 추가 • **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Add New(**새로 추가**)** 드롭다운 메뉴 > **Subinterface(**하위 인터페이스**)** > **Type(**유형**)** 필드 지원되는 플랫폼: Firepower 4100/9300의 Firepower Threat Defense
병렬로 데이터 유닛에 구성 동기화	6.6	제어 유닛은 이제 기본적으로 구성 변경 사항을 데이터 유닛과 동시에 동기화합니다. 이전에는 동기화가 순차적으로 발생했습니다. 신규/수정된 화면: 없음

기능	버전	세부 사항
클러스터 가입 실패 또는 제거에 대한 메시지가 추가됨 **show cluster history**	6.6	클러스터 유닛이 클러스터에 조인하지 못하거나 클러스터를 떠나는 경우를 위한 새 메시지가 **show cluster history** 명령에 추가되었습니다. 신규/수정된 명령: **show cluster history** 신규/수정된 화면: 없음
DCD(Dead Connection Detection)의 이니시에이터 및 응답자 정보와, 클러스터에서의 DCD 지원입니다.	6.5	DCD(Dead Connection Detection)를 활성화하면, **show conn detail** 명령을 이용해 이니시에이터 및 응답자 정보를 얻을 수 있습니다. DCD(Dead Connection Detection)를 이용하면 비활성 연결을 유지할 수 있으며, **show conn** 출력은 엔드포인트를 얼마나 자주 조사했는지 알려줍니다. 또한 이제 DCD는 클러스터에서도 지원됩니다. 신규/수정된 명령: **show conn** (출력 전용) 지원되는 플랫폼: Firepower 4100/9300의 Firepower Threat Defense
Firepower Management Center에 향상된 Firepower Threat Defense 클러스터 추가	6.3	이제는 Firepower Management Center에 클러스터 유닛을 추가할 수 있으며 다른 클러스터 유닛은 자동으로 탐지됩니다. 이전에는 각 클러스터 유닛을 별도 디바이스로 추가한 뒤 관리 센터에서 클러스터로 그룹화해야 했습니다. 이제 클러스터 유닛 추가는 자동으로 진행됩니다. 유닛은 수동으로 삭제해야 합니다. 신규/수정된 화면: 디바이스 > 디바이스 관리> 추가 드롭다운 메뉴 > 디바이스 > 디바이스 추가 대화 상자 디바이스 > 디바이스 관리> 클러스터 탭 > 일반 영역 > 클러스터 등록 상태 > 현재 클러스터 요약 링크 > 클러스터 상태 대화 상자 지원되는 플랫폼: Firepower 4100/9300의 Firepower Threat Defense

기능	버전	세부 사항
Firepower 4100은 6개 모듈을 위한 섀시 간 클러스터링을 지원합니다.	6.2	FXOS 2.1.1의 경우 이제 Firepower 9300 및 4100에서 섀시 간 클러스터링을 활성화할 수 있습니다. Firepower 9300의 경우에는 모듈을 6 개까지 포함할 수 있습니다. 예를 들어 섀시 6개에 모듈 1개, 섀시 3개에 모듈 2개, 또는 모듈을 6개까지 제공하는 어떤 조합도 사용할 수 있습니다. Firepower 4100의 경우에는 섀시를 6 개까지 포함할 수 있습니다. 참고 사이트 간 클러스터링은 지원되지 않습니다. 사이트별 MAC 및 IP 주소, 디렉터 현지화 , 사이트 이중화, 클러스터 플로우 이동성 같은 이중화 및 안정성을 개선하기 위한 맞춤화는 FlexConfig 기능을 사용하는 경우에만 구성 가능합니다. 수정된 화면이 없습니다. 지원되는 플랫폼: Firepower 4100/9300의 Firepower Threat Defense
Firepower 9300을 위한 섀시 내 클러스터링	6.0.1	Firepower 9300 섀시 내에서 최대 3개의 보안 모듈을 클러스터링할 수 있습니다. 섀시의 모든 모듈은 클러스터에 속해야 합니다. 신규/수정된 화면: 디바이스 > 디바이스 관리 > 추가 > 클러스터 추가 디바이스 > 디바이스 관리 > 클러스터 지원되는 플랫폼: Firepower 9300의 Firepower Threat Defense

IX 부

Firepower Threat Defense 라우팅

- Firepower Threat Defense 라우팅 개요, 977 페이지
- Firepower Threat Defense에 대한 가상 라우팅, 987 페이지
- Firepower Threat Defense 정적 및 기본 경로, 1035 페이지
- Firepower Threat Defense OSPF, 1041 페이지
- Firepower Threat Defense BGP, 1073 페이지
- Firepower Threat Defense RIP, 1091 페이지
- Firepower Threat Defense 멀티캐스트 라우팅, 1099 페이지

36 장

Firepower Threat Defense 라우팅 개요

이 장에서는 Firepower Threat Defense 내 라우팅 동작 및 지원되는 라우팅 프로토콜의 중요 개념을 설명합니다.

- 경로 결정, 977 페이지
- 지원되는 경로 유형, 978 페이지
- 라우팅을 위한 지원되는 인터넷 프로토콜, 979 페이지
- 라우팅 테이블, 980 페이지
- 관리 트래픽용 라우팅 테이블, 984 페이지
- ECMP(Equal-Cost Multi-Path) 라우팅, 984 페이지
- 경로 맵 정보, 984 페이지

경로 결정

라우팅 프로토콜은 메트릭을 사용하여 패킷이 이동할 최적의 경로를 평가합니다. 메트릭은 경로 대역폭과 같은 측정 기준이며, 목적지에 대한 최적 경로를 결정하는 라우팅 알고리즘에 사용됩니다. 라우팅 알고리즘은 경로 결정을 돕기 위해 경로 정보를 포함하는 라우팅 테이블을 초기화하고 유지합니다. 경로 정보는 사용된 경로 알고리즘에 따라 달라집니다.

라우팅 알고리즘은 다양한 정보로 라우팅 테이블을 채웁니다. 목적지 또는 다음 홉 연결은 최종 목적지로 향하는 과정에서 다음 홉에 해당하는 라우터에 패킷을 전달하는 것이 목적지에 도달하는 최적의 방식임을 라우터에 알립니다. 라우터가 수신 패킷을 수신하면 목적지 주소를 확인하고 이 주소를 다음 홉과 연결하려고 시도합니다.

라우팅 테이블은 또한 경로의 선호도와 같은 다른 정보도 포함합니다. 라우터는 메트릭을 비교하여 최적의 경로를 결정하고 이러한 메트릭은 사용된 라우팅 알고리즘의 설계에 따라 달라집니다.

라우터는 서로 통신하며 다양한 메시지의 전송을 통해 라우팅 테이블을 유지합니다. 라우팅 업데이트 메시지는 일반적으로 라우팅 테이블 전체 또는 일부로 구성되는 메시지입니다. 라우터는 다른 모든 라우터의 라우팅 업데이트를 분석함으로써 네트워크 토폴로지에 대한 자세한 그림을 그릴 수 있습니다. 라우터 간에 전송되는 메시지의 또 다른 예인 링크-상태 알림은 다른 라우터에 발신자 링크의 상태를 알려줍니다. 연결 정보는 라우터가 네트워크 목적지로의 최적의 경로를 결정할 수 있도록 네트워크 토폴로지의 완전한 그림을 그리는 데에도 사용됩니다.

지원되는 경로 유형

라우터는 몇 가지 경로 유형을 사용할 수 있습니다. Firepower Threat Defense 디바이스는 다음 경로 유형을 사용합니다.

- 고정 대 동적
- 단일 경로 대 다중 경로
- 평면 대 계층형
- 연결 상태 대 거리 벡터

고정 대 동적

고정 라우팅 알고리즘은 실제로 네트워크 관리자가 설정한 테이블 매핑입니다. 이러한 매핑은 네트워크 관리자가 변경하지 않는 한 변경되지 않습니다. 고정 경로를 사용하는 알고리즘은 설계하기가 쉽고 네트워크 트래픽을 상대적으로 예측하기 쉬운 환경과 네트워크 설계가 상대적으로 단순한 환경에서 효과적입니다.

고정 라우팅 시스템은 네트워크 변화에 대응할 수 없기 때문에 꾸준히 변화하는 대규모 네트워크에는 일반적으로 적합하지 않습니다. 대부분의 주요 라우팅 알고리즘은 수신 라우팅 업데이트 메시지를 분석함으로써 네트워크 상황의 변화에 대응하는 동적 라우팅 알고리즘입니다. 메시지가 네트워크 변경 사실을 알리면 라우팅 소프트웨어가 경로를 다시 계산하고 새로운 라우팅 업데이트 메시지를 보냅니다. 이 메시지는 네트워크를 통과하며 라우터가 알고리즘을 다시 실행하고 라우팅 테이블을 그에 따라 변경하게 합니다.

동적 라우팅 알고리즘은 고정 경로로 적절히 보완할 수 있습니다. 예를 들어 최후의 수단으로 사용하는 라우터(모든 라우팅 불가 패킷이 전송되는 라우터의 기본 경로)는 모든 라우팅 불가 패킷에 대한 저장소 역할을 하도록 지정되어 모든 메시지가 어떻게든 처리되도록 할 수 있습니다.

단일 경로 대 다중 경로

일부 고급 라우팅 프로토콜은 동일 목적지에 대한 다중 경로를 지원합니다. 단일 경로 알고리즘과 달리 이러한 다중 경로 알고리즘은 여러 회선에 걸친 트래픽 멀티플렉싱을 허용합니다. 다중 경로 알고리즘의 이점은 보통 로드 공유라고 부르는 훨씬 뛰어난 처리량과 신뢰성입니다.

평면 대 계층형

일부 라우팅 알고리즘은 평면 공간에서 작동하고 또 다른 일부는 라우팅 계층을 사용합니다. 평면 라우팅 시스템에서 라우터는 다른 모든 라우터의 피어입니다. 계층형 라우팅 시스템에서는 일부 라우터가 모여 라우팅 백본을 형성합니다. 비 백본 라우터의 패킷은 백본 라우터로 이동하고 여기서 백본을 통해 목적지의 일반 영역에 전달됩니다. 이 지점에 이르면 마지막 백본 라우터에서 하나 이상의 비 백본 라우터를 거쳐 최종 목적지로 이동합니다.

대개 라우팅 시스템은 도메인, 자율 시스템 또는 영역이라고 하는 논리적인 노드 그룹을 지정합니다. 계층형 시스템에서는 다른 도메인의 라우터와 통신할 수 있는 라우터도 있고 같은 도메인의 라우터하고만 통신할 수 있는 라우터도 있습니다. 대규모 네트워크에서는 추가적인 계층 수준이 있을 수 있고 가장 높은 계층 수준의 라우터가 라우팅 백본을 형성합니다.

계층형 라우팅의 가장 큰 장점은 기업 대부분의 조직 구조와 비슷하기 때문에 조직의 트래픽 패턴도 잘 지원한다는 점입니다. 대부분의 네트워크 통신은 소규모 기업 그룹(도메인) 내에서 발생합니다. 인트라도메인 라우터는 도메인 내의 다른 라우터에 대해서만 알면 되므로 라우팅 알고리즘을 간소화할 수 있고 사용되는 라우팅 알고리즘에 따라 라우팅 업데이트 트래픽을 줄일 수 있습니다.

연결 상태 대 거리 벡터

링크 상태 알고리즘 (최단 경로 우선 알고리즘)은 인터네트워크의 모든 노드로 라우팅 정보를 전달합니다. 하지만 각 라우터는 자신의 링크 상태를 설명하는 라우팅 테이블의 일부만 전송합니다. 링크 상태 알고리즘에서는 각 라우터가 라우팅 테이블에서 전체 네트워크의 상태를 그립니다. 거리 벡터 알고리즘(Bellman-Ford 알고리즘이라고도 함)은 각 라우터를 호출하여 라우팅 테이블의 전체 또는 일부를 네이버에 한해 전송하도록 합니다. 기본적으로 링크 상태 알고리즘은 모든 곳으로 소규모 업데이트를 전송하는 반면 거리 벡터 알고리즘은 대규모 업데이트를 인접 디바이스로만 보냅니다. 거리 벡터 알고리즘은 네이버에 대해서만 알고 있습니다. 일반적으로 링크 상태 알고리즘은 OSPF 라우팅 프로토콜과 함께 사용됩니다.

라우팅을 위한 지원되는 인터넷 프로토콜

Firepower Threat Defense 디바이스는 라우팅을 위해 몇 가지 인터넷 프로토콜을 지원합니다. 이 섹션에서는 각 프로토콜에 대해 간단하게 설명합니다.

- EIGRP(Enhanced Interior Gateway Routing Protocol)

  EIGRP는 IGRP 라우터와의 호환성 및 원활한 상호 작용을 제공하는 Cisco 고유의 프로토콜입니다. 자동 재배포 메커니즘이 IGRP 경로를 Enhanced IGRP로 또한 그 반대로 가져올 수 있게 합니다. 따라서 Enhanced IGRP를 기존 IGRP 네트워크에 점진적으로 추가할 수 있습니다.

- OSPF(Open Shortest Path First)

  OSPF는 IETF(Internet Engineering Task Force)의 IGP(interior gateway protocol) 작업 그룹에서 IP(Internet Protocol) 네트워크를 위해 개발한 라우팅 프로토콜입니다. OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터는 동일한 링크 상태 데이터베이스를 갖고 있는데, 이는 각 라우터에서 사용 가능한 인터페이스 및 연결 가능한 네이버의 목록입니다.

- RIP(Routing Information Protocol)

  RIP는 홉 카운트를 메트릭으로 사용하는 거리 벡터 프로토콜입니다. RIP는 글로벌 인터넷에서 라우팅 트래픽을 위해 널리 사용되며 내부 게이트웨이 프로토콜(IGP)이기 때문에 단일 자율 시스템 내에서 라우팅을 수행합니다.

- BGP(Border Gateway Protocol)

BGP는 자율 시스템 간 라우팅 프로토콜입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. AS(autonomous system) 사이에서 BGP가 사용될 때 이 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때의 프로토콜은 IBGP(Interior BGP)라고 합니다.

- IS-IS(Intermediate System to Intermediate System)

  IS-IS는 링크 상태 IGP(Interior Gateway Protocol)입니다. 링크 상태 프로토콜은 각 참여 라우터에서 전체 네트워크 연결 맵을 구성하는 데 필요한 정보를 전파하는 것이 특징입니다. 해당 맵은 대상으로의 최단 경로 계산에 사용됩니다.

라우팅 테이블

FTD에서는 (디바이스를 통한) 데이터 트래픽과 (디바이스에서의) 관리 트래픽에 별도의 라우팅 테이블을 사용합니다. 이 섹션에서는 라우팅 테이블을 작동 방식을 설명합니다.관리 라우팅 트래픽에 관한 내용은 관리 트래픽용 라우팅 테이블, 984 페이지의 내용을 참조하십시오.

라우팅 테이블을 채우는 방법

FTD 라우팅 테이블은 정적으로 정의된 경로, 직접 연결된 경로, 그리고 동적 라우팅 프로토콜에서 검색한 경로로 채울 수 있습니다. FTD는 라우팅 테이블에 고정 경로와 연결 경로를 가지는 것 외에도 여러 라우팅 프로토콜을 실행할 수 있기 때문에 같은 경로가 하나 이상의 방법으로 다시 발견되거나 입력될 수 있습니다. 같은 목적지로의 두 경로를 라우팅 테이블에 넣으면 라우팅 테이블에 유지되는 항목은 다음과 같이 결정됩니다.

- 두 경로의 네트워크 접두사 길이(네트워크 마스크)가 다르면 두 경로 모두 고유한 것으로 간주되어 라우팅 테이블에 입력됩니다. 그런 다음 패킷 전달 로직에서 둘 중 어느 것을 사용할지 결정합니다.

  예를 들어 RIP 및 OSPF 프로세스에서 다음 경로를 검색한 경우

  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19

  비록 OSPF 경로의 관리 영역이 더 낮지만, 접두사 길이(서브넷 마스크)가 다르기 때문에 두 경로 모두 라우팅 테이블에 설치됩니다. 이들은 다른 목적지로 간주되며 패킷 전달 로직에서 사용할 경로를 결정합니다.

- FTD가 RIP와 같이 단일 라우팅 프로토콜에서 같은 대상으로의 여러 경로를 학습하는 경우 메트릭이 더 나은 경로(라우팅 프로토콜이 결정)가 라우팅 테이블에 입력됩니다.

  메트릭은 특정 경로와 연결되는 값이며, 선호도가 가장 높은 것부터 순위를 지정합니다. 메트릭을 결정하는 데 사용되는 매개변수는 라우팅 프로토콜에 따라 다릅니다. 가장 낮은 메트릭을 갖는 경로가 최적의 경로로 선택되고 라우팅 테이블에 설치됩니다. 동일한 목적지의 다중 경로가 메트릭 값이 같을 경우 이 동일 비용 경로에 대한 로드 밸런싱이 수행됩니다.

- FTD가 두 개 이상이 라우팅 프로토콜로부터 대상에 대해 학습하는 경우 경로의 관리 거리를 비교하고 관리 거리가 짧은 경로가 라우팅 테이블에 입력됩니다.

경로의 관리 거리

라우팅 프로토콜에서 검색 또는 재배포되는 경로에 대한 관리 영역을 변경할 수 있습니다. 서로 다른 두 라우팅 프로토콜의 두 경로가 관리 영역이 같을 경우 기본 관리 영역이 낮은 경로가 라우팅 테이블에 입력됩니다. EIGRP 및 OSPF 경로의 경우 EIGRP 경로와 OSPF 경로가 관리 영역이 같으면 기본적으로 EIGRP 경로가 선택됩니다.

관리 영역은 서로 다른 두 라우팅 프로토콜로부터 동일한 목적지의 서로 다른 경로가 2개 이상 나올 경우 최적의 경로를 선택하기 위해 Firepower Threat Defense 디바이스에서 사용하는 경로 매개변수입니다. 라우팅 프로토콜은 다른 프로토콜과 구별되는 알고리즘을 기반으로 한 메트릭을 갖기 때문에 서로 다른 라우팅 프로토콜에서 생성된 동일 목적지의 경로 2개 중에서 최적의 경로를 결정하는 것이 가능하지 않을 수도 있습니다.

각 라우팅 프로토콜은 관리 영역 값을 사용하여 우선순위가 지정됩니다. 다음 표에는 Firepower Threat Defense 디바이스에서 지원하는 라우팅 프로토콜의 기본 관리 거리 값이 정리되어 있습니다.

표 ***80:*** 지원되는 라우팅 프로토콜의 기본 관리 영역

경로 소스	기본 관리 영역
연결된 인터페이스	0
고정 경로	1
EIGRP 요약 경로	5
외부 BGP	20
내부 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 외부 경로	170
내부 및 로컬 BGP	200
알 수 없음	255

관리 영역의 값이 작을수록 프로토콜 우선순위가 높습니다. 예를 들어, Firepower Threat Defense 디바이스가 OSPF 라우팅 프로세스(기본 관리 거리 - 110)와 RIP 라우팅 프로세스(기본 관리 거리 - 120)로부터 모두 특정 네트워크로의 경로를 수신할 경우 Firepower Threat Defense 디바이스는 우선순위가 더 높은 OSPF 경로를 선택합니다. 이러한 경우 라우터가 라우팅 테이블에 경로의 OSPF 버전을 추가합니다.

이 예제에서, OSPF 파생 경로의 소스가 손실된 경우(예: 전원 꺼짐) Firepower Threat Defense 디바이스는 OSPF 파생 경로가 다시 나타날 때까지 RIP 파생 경로를 사용합니다.

관리 영역은 로컬 설정입니다. 예를 들어 OSPF를 통해 얻은 경로의 관리 거리를 변경하면 이 변경 사항은 이 명령을 입력한 Firepower Threat Defense 디바이스의 라우팅 테이블에만 영향을 미칩니다. 관리 영역은 라우팅 업데이트에서 광고되지 않습니다.

관리 영역은 라우팅 프로세스에 영향을 주지 않습니다. 라우팅 프로세스에서는 라우팅 프로세스를 통해 검색되었거나 라우팅 프로세스로 재배포된 경로만 알립니다. 예를 들어 RIP 라우팅 프로세스는 OSPF 라우팅 프로세스를 통해 발견된 경로가 라우팅 테이블에 사용되더라도 RIP 경로를 광고합니다.

동적 및 부동 정적 경로 백업

다른 경로가 설치되었기 때문에 라우팅 테이블에 경로를 설치하려는 첫 번째 시도가 실패하면 백업 경로가 등록됩니다. 라우팅 테이블에 설치된 경로가 실패할 경우 라우팅 테이블 유지 관리 프로세스는 백업 경로를 등록한 각 라우팅 프로토콜 프로세스를 호출하고 해당 경로를 라우팅 테이블에 다시 설치하도록 요청합니다. 실패한 경로에 대해 백업이 등록된 프로토콜이 여럿인 경우 관리 영역을 기준으로 우선 경로가 선택됩니다.

이 프로세스 때문에 동적 라우팅 프로토콜을 통해 발견된 경로가 실패할 때 라우팅 테이블에 설치된 유동 고정 경로를 생성할 수 있습니다. 유동 고정 경로는 단순히 Firepower Threat Defense 디바이스에서 실행되는 동적 라우팅 프로토콜보다 큰 관리 영역으로 설정된 고정 경로입니다. 동적 라우팅 프로세스에서 발견한 경로가 실패하면 라우팅 테이블에 고정 경로가 설치됩니다.

포워딩 결정 방법

포워딩 결정은 다음과 같이 이루어집니다.

- 목적지가 라우팅 테이블 내의 항목과 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 포워딩됩니다. 기본 경로가 구성되지 않은 경우 패킷이 폐기됩니다.
- 목적지가 라우팅 테이블의 단일 항목과 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 포워딩됩니다.
- 목적지가 라우팅 테이블에 있는 두 개 이상의 항목과 일치하면 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다.

예를 들어 목적지가 192.168.32.1인 패킷은 라우팅 테이블의 다음 경로를 통해 인터페이스에 도착합니다.

- 192.168.32.0/24 게이트웨이 10.1.1.2
- 192.168.32.0/19 게이트웨이 10.1.1.3

이 경우 192.168.32.1이 192.168.32.0/24 네트워크 범위에 해당되기 때문에 목적지가 192.168.32.1인 패킷은 10.1.1.2로 전달됩니다. 이 주소는 라우팅 테이블 내 다른 경로에도 포함되지만, 라우팅 테이블의 다른 경로 접두사는 19비트인 데 비해 192.168.32.0/24의 접두사는 24비트이므로 이 경로의 접두사가 가장 깁니다. 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.

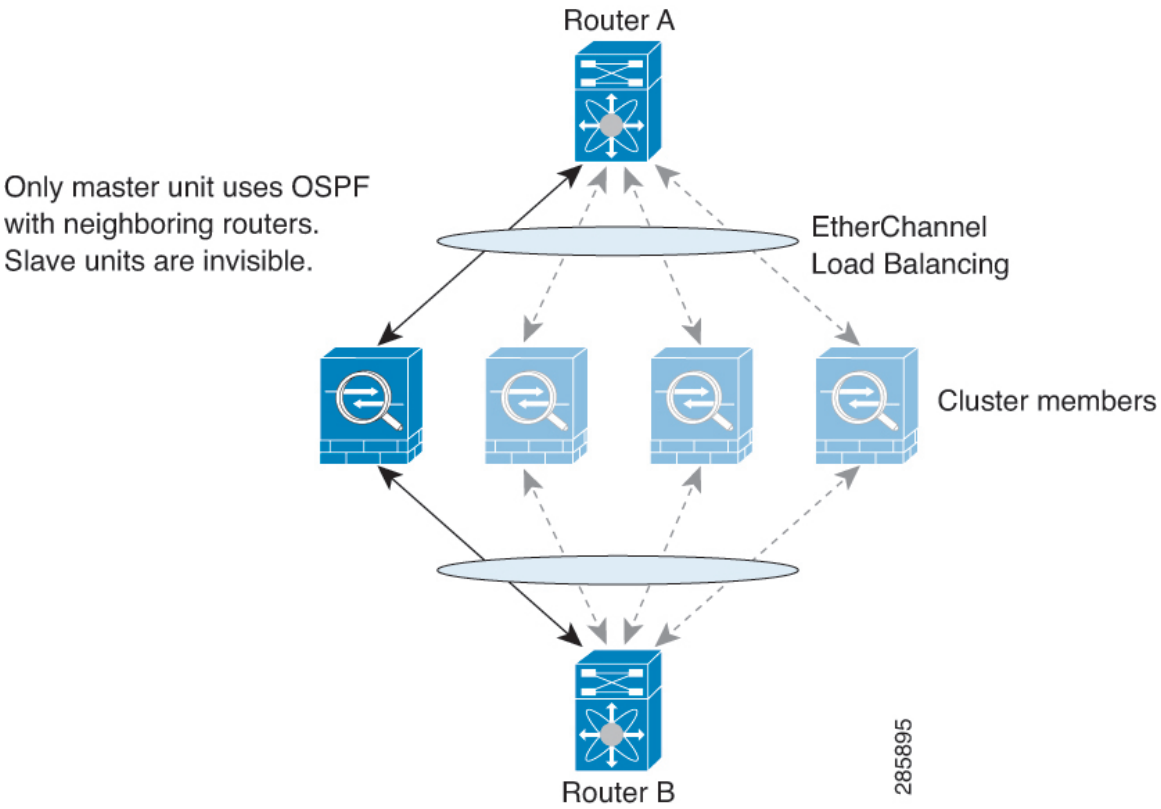
참고 새로운 유사한 연결이 경로 변경으로 인해 다른 동작을 유발하는 경우에도 기존의 연결은 계속해서 설정된 인터페이스를 사용합니다.

클러스터링의 동적 라우팅

참고 IS-IS는 Spanned EtherChannel 모드에서 지원되지 않습니다.

라우팅 프로세스는 제어 유닛에서만 실행되며, 제어 유닛을 통해 경로가 파악되고 데이터 유닛에 복제됩니다. 라우팅 패킷이 데이터 유닛에 전송되면 해당 패킷은 제어 유닛에 리디렉션됩니다.

그림 ***35:*** 클러스터링의 동적 라우팅



데이터 유닛이 제어 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 제어 유닛에서 데이터 유닛으로 동기화되지 않습니다. 제어 유닛 전환이 있을 경우, 네이버 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면

클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

관리 트래픽용 라우팅 테이블

ECMP(Equal-Cost Multi-Path) 라우팅

Firepower Threat Defense 디바이스에서는 ECMP(Equal-Cost Multi-Path) 라우팅을 지원합니다.

인터페이스당 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 외부 인터페이스에서 서로 다른 게이트웨이를 지정하는 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

여기서는 외부 인터페이스에서 0.1.1.2, 10.1.1.3, 10.1.1.4끼리 트래픽 로드 밸런싱을 수행합니다. 트래픽은 소스와 대상 IP 주소, 수신 인터페이스, 프로토콜, 소스 및 대상 포트를 해싱하는 알고리즘에 따라 지정된 게이트웨이 사이에서 분배됩니다.

트래픽 영역을 사용하는 여러 인터페이스의 **ECMP**

참고 FlexConfig를 사용하여 **zone** 및 **zone-member** 명령을 통해 트래픽 영역을 설정합니다.

인터페이스 그룹을 포함하도록 트래픽 영역을 구성할 경우, 하나의 영역 내에서 최대 8개의 인터페이스에 걸쳐 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 다음과 같이 영역 내 인터페이스 3개의 전 범위에 걸쳐 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

또한 동적 라우팅 프로토콜은 동일 비용 경로를 자동으로 구성할 수 있습니다. Firepower Threat Defense 디바이스에서는 더 강력한 로드 밸런싱 메커니즘을 통해 인터페이스 간의 트래픽을 로드 밸런싱합니다.

어떤 경로가 사라지면 디바이스에서는 다른 경로로 원활하게 플로우를 이동합니다.

경로 맵 정보

경로 맵은 경로를 OSPF, RIP, EIGRP 또는 BGP 라우팅 프로세스로 재배포할 때 사용됩니다. 또한 OSPF 라우팅 프로세스로 기본 경로를 생성할 때도 사용됩니다. 경로 맵은 지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 정의합니다.

경로 맵은 널리 알려진 ACL과 여러 기능을 공유합니다. 다음은 두 가지에서 모두 일반적인 특성입니다.

- 이들은 순서가 정해진 개별 구문이며 각각 허용 또는 거부라는 결과를 갖습니다. ACL 또는 경로 맵의 평가는 사전 정의된 순서에 따른 목록 스캔과 그에 일치하는 각 구문의 기준에 대한 평가로 구성됩니다. 목록 스캔은 첫 번째 구문 일치가 발견되고 해당 구문 일치와 연결된 작업이 수행되면 중단됩니다.
- 이들은 일반 메커니즘입니다. 기준 일치와 일치 해석은 적용되는 방식과 이를 사용하는 기능에 따라 정해집니다. 같은 경로 맵이라도 다른 기능에 적용되면 다르게 해석될 수 있습니다.

다음은 경로 맵과 ACL의 차이점입니다.

- 경로 맵은 ACL보다 유연하며 ACL이 확인할 수 없는 기준으로 경로를 확인할 수 있습니다. 예를 들어 경로 맵은 경로 유형이 내부인지 확인할 수 있습니다.
- 각 ACL은 설계 관행에 따라 암시적 거부 문구로 종료됩니다. 일치 시도 중에 경로 맵의 끝에 도달하는 경우 결과는 경로 맵의 애플리케이션이 무엇인지에 따라 달라집니다. 재배포에 적용되는 경로 맵은 ACL과 동일하게 작동합니다. 경로가 경로 맵의 조항과 일치하지 않으면 마치 경로 맵이 끝에 거부 구문을 포함한 것처럼 경로 재배포가 거부됩니다.

허용 및 거부 절

경로 맵은 허용 및 거부 절을 가질 수 있습니다. 거부 절은 재배포에서 경로 일치를 거부합니다. 경로 맵의 일치 기준으로 ACL을 사용할 수 있습니다. ACL에도 허용 및 거부 절이 있으므로 패킷이 ACL과 일치하는 경우 다음 규칙이 적용됩니다.

- ACL 허용 + 경로 맵 허용: 경로가 재배포됩니다.
- ACL 허용 + 경로 맵 거부: 경로가 재배포되지 않습니다.
- ACL 거부 + 경로 맵 허용 또는 거부: 경로 맵 절이 일치하지 않으며 다음 경로 맵 절이 평가됩니다.

절의 일치 및 설정 값

각 경로 맵 절은 두 가지 값을 갖습니다.

- 일치 값은 이 절을 적용할 경로를 선택합니다.
- 설정 값은 대상 프로토콜로 재배포될 정보를 수정합니다.

재배포되는 각 경로에 대해 라우터는 먼저 경로 맵에 있는 절의 일치 기준을 평가합니다. 일치 기준이 성공하면 허용 또는 거부 절에 따라 경로가 재배포되거나 거부되고 set 명령에서 설정된 값으로 일부 속성이 수정될 수 있습니다. 일치 기준이 실패하면 이 절은 경로에 적용되지 않고 소프트웨어가 경로 맵의 다음 절에 대해 경로를 평가합니다. 절이 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 스캔이 계속됩니다.

다음 조건 중 하나가 존재할 경우 각 절의 일치 또는 설정 값은 누락되거나 여러 번 반복될 수 있습니다.

- 절에 여러 match 항목이 존재하는 경우 주어진 경로에 대해 모두 성공해야 경로가 절에 일치할 수 있습니다(논리 AND 알고리즘이 여러 일치 명령에 적용됨).
- match 항목이 하나의 항목에서 여러 개체를 참조하는 경우 둘 중 하나가 일치해야 합니다(논리 OR 알고리즘 적용).
- match 항목이 존재하지 않으면 모든 경로가 절과 일치합니다.
- set 항목이 경로 맵 허용 절에 없는 경우 현재 속성의 수정 없이 경로가 재배포됩니다.

참고 경로 맵의 set 항목이 절을 거부하도록 구성하지 마십시오. 거부 절은 경로 재배포를 금지하므로 수정할 정보가 없기 때문입니다.

match 또는 set 항목이 없는 경로 맵 절이 작업을 수행합니다. 빈 허용 절은 수정 없이 남은 경로의 재배포를 허용합니다. 빈 거부 절은 다른 경로의 재배포를 허용하지 않습니다(경로 맵을 완전히 스캔했으나 정확한 match 항목을 찾지 못한 경우 이것이 기본 작업).

37 장

Firepower Threat Defense에 대한 가상 라우팅

이 장에서는 Firepower Threat Defense 내 가상 라우터 그리고 가상 라우터 동작 방법의 기본 개념을 설명합니다.

- 가상 라우터 및 VRF(가상 라우팅 및 포워딩) 정보, 987 페이지
- 디바이스 모델별 최대 가상 라우터 수, 992 페이지
- 가상 라우터를 위한 요구 사항 및 사전 요건, 993 페이지
- 가상 라우터 대한 지침 및 제한 사항, 993 페이지
- FMC 웹 인터페이스 라우팅 페이지에 대한 수정 사항, 995 페이지
- 가상 라우터 관리 페이지, 996 페이지
- 가상 라우터 생성, 996 페이지
- 가상 라우터의 구성 예시, 1000 페이지
- Firepower Threat Defense의 가상 라우터 기록, 1033 페이지

가상 라우터 및 VRF(가상 라우팅 및 포워딩) 정보

여러 가상 라우터를 생성하여 인터페이스 그룹에 대해 별도의 라우팅 테이블을 유지 관리할 수 있습니다. 각 가상 라우터에는 자체 라우팅 테이블이 있으므로 디바이스를 통과하는 트래픽에서 명확하게 분리하는 기능을 제공할 수 있습니다.

따라서 공통 네트워킹 장비 집합을 통해 둘 이상의 개별 고객을 지원할 수 있습니다. 또한 가상 라우터를 사용하여 자체 네트워크의 요소를 더 쉽게 분리할 수 있습니다. 일반 목적의 기업 네트워크에서 개발 네트워크를 격리하는 경우를 예로 들 수 있습니다.

가상 라우터에서는 가상 라우팅 및 포워딩의 "light" 버전, 즉 VRF-Lite를 구현합니다. 이는 BGP용 멀티프로토콜 확장(MBGP)을 지원하지 않습니다.

가상 라우터를 생성하는 경우 라우터에 인터페이스를 할당합니다. 특정 인터페이스는 하나의 가상 라우터에만 할당할 수 있습니다. 그런 다음 고정 경로를 정의하고 각 가상 라우터에 대해 OSPF 또는 BGP와 같은 라우팅 프로토콜을 구성합니다. 또한 모든 참여 디바이스의 라우팅 테이블이 동일한 가상 라우터 라우팅 프로세스 및 테이블을 사용하도록 전체 네트워크에 대해 별도의 라우팅 프로세스를 구성합니다. 가상 라우터를 사용하면 동일한 물리적 네트워크를 통해 논리적으로 구분된 네트워크를 생성하여 각 가상 라우터를 통해 실행되는 트래픽의 프라이버시를 확보할 수 있습니다.

라우팅 테이블은 분리되어 있으므로 가상 라우터 전체에서 동일하거나 중복되는 어드레스 스페이스를 사용할 수 있습니다. 예를 들어, 2개의 개별 물리적 인터페이스에서 지원되는 2개의 개별 가상 라우터에 대해 192.168.1.0/24 어드레스 스페이스를 사용할 수 있습니다.

가상 라우터별로 별도의 관리 및 데이터 라우팅 테이블이 있습니다. 예를 들어, 가상 라우터에 관리 전용 인터페이스를 할당하는 경우 해당 인터페이스에 대한 라우팅 테이블은 가상 라우터에 할당된 데이터 인터페이스와는 별개입니다.

가상 라우터의 애플리케이션

가상 라우터를 사용하여 공유 리소스에서 네트워크를 격리하거나 공통 보안 정책으로 네트워크를 격리할 수 있습니다. 따라서 가상 라우터를 사용하면 다음을 달성할 수 있습니다.

- 각 고객 또는 다른 부서의 전용 라우팅 테이블을 통해 고객을 위한 트래픽 분리
- 여러 부서 또는 네트워크에 대한 공통 보안 정책 관리
- 다른 부서 또는 네트워크에 대한 공유 인터넷 액세스

전역 및 사용자 정의 가상 라우터

전역 가상 라우터

가상 라우팅 기능이 있는 디바이스의 경우 시스템은 기본적으로 전역 가상 라우터를 생성합니다. 시스템은 네트워크의 모든 인터페이스를 글로벌 가상 라우터에 할당합니다. 라우팅 인터페이스는 사용자 정의 가상 라우터 또는 전역 가상 라우터에 속할 수 있습니다. FTD 디바이스를 가상 라우터 기능이 있는 버전으로 업그레이드할 경우 기존의 모든 라우팅 구성이 전역 가상 라우터의 일부가 됩니다.

사용자 정의 가상 라우터

사용자 정의 가상 라우터는 사용자가 정의한 가상 라우터입니다. 디바이스에서 둘 이상의 가상 라우터를 생성할 수 있습니다. 그러나 언제든 하나의 사용자 정의 가상 라우터에만 인터페이스를 할당할 수 있습니다. 일부 디바이스 기능은 사용자 정의 가상 라우터에서 지원되지만 일부 기능은 전역 가상 라우터에서만 지원됩니다.

지원되는 기능 및 모니터링 정책

글로벌 가상 라우터에서만 다음 기능을 구성할 수 있습니다.

- OSPFv3
- RIP
- EIGRP
- IS-IS
- BGPv6

- 멀티캐스트 라우팅
- Policy Based Routing (PBR)
- VPN

EIGRP, ISIS 및 PBR은 FMC의 Flex 구성을 통해 지원됩니다(사전 정의된 FlexConfig 개체, 1281 페이지 참조). 이러한 기능을 위해 전역 가상 라우터의 인터페이스만 구성합니다.

DHCP 서버 자동 구성에서는 인터페이스에서 학습된 WINS/DNS 서버를 사용합니다. 이 인터페이스는 전역 가상 라우터 인터페이스만 될 수 있습니다.

각 사용자 정의 가상 라우터에 대해 다음 기능을 개별적으로 구성할 수 있습니다.

- 고정 경로 및 해당 SLA 모니터
- OSPFv2
- BGPv4
- 통합 라우팅 및 브리징(IRB)

다음 기능은 원격 시스템을 통해 쿼리하거나 통신할 때 시스템에서 사용됩니다(from-the-box 트래픽). 이러한 기능에서는 글로벌 가상 라우터의 인터페이스만 사용합니다. 즉, 이 기능을 위해 인터페이스를 구성하는 경우 해당 인터페이스는 글로벌 가상 라우터에 속해야 합니다. 일반적으로 시스템에서는 자체 관리 목적으로 외부 서버에 연결하기 위해 경로를 조회해야 할 때마다 글로벌 가상 라우터에서 경로 조회를 수행합니다.

- 액세스 제어 규칙 또는 **ping** 명령의 이름을 확인할 때 사용되는 정규화된 이름을 확인하는 데 사용되는 DNS 서버입니다. DNS 서버에 대한 인터페이스로 **any**를 지정하면 시스템에서는 글로벌 가상 라우터의 인터페이스만 고려합니다.
- VPN과 함께 사용하는 경우 ID 영역 또는 AAA 서버입니다. 글로벌 가상 라우터의 인터페이스에서만 VPN을 구성할 수 있습니다. VPN에 사용되는 외부 AAA 서버(예: Active Directory)는 글로벌 가상 라우터의 인터페이스를 통해 연결할 수 있어야 합니다.
- Syslog 서버.
- SNMP.

가상 라우터 인식 정책 구성

가상 라우터를 생성하면 해당 가상 라우터에 대한 라우팅 테이블이 전역 가상 라우터 또는 다른 모든 가상 라우터와 자동으로 분리됩니다. 그러나 보안 정책에서는 자동으로 가상 라우터를 인식하지 않습니다.

예를 들어 "any" 소스 또는 대상 보안 영역에 적용되는 액세스 제어 규칙을 작성하는 경우, 규칙은 모든 가상 라우터의 모든 인터페이스에 적용됩니다. 이는 실제로 원하는 것과 정확히 같을 수 있습니다. 예를 들어 모든 고객이 유해한 URL 카테고리의 동일한 목록에 대한 액세스를 차단하고자 할 수 있습니다.

그러나 가상 라우터 중 하나에만 정책을 적용해야 하는 경우에는 해당 단일 가상 라우터의 인터페이스만 포함하는 보안 영역을 생성해야 합니다. 그런 다음, 보안 정책의 소스 및 대상 기준에서 가상 라우터 제한 보안 영역을 사용합니다.

해당 멤버십이 단일 가상 라우터에 할당된 인터페이스로 제한되는 보안 영역을 사용하여 다음 정책에서 가상 라우터 인식 규칙을 작성할 수 있습니다.

- 액세스 제어 정책
- 침입 및 파일 정책
- SSL 암호 해독 정책
- ID 정책 및 사용자-IP 주소 매핑 가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 각 가상 라우터에 대해 별도의 영역을 생성하고 ID 정책 규칙에서 올바르게 적용해야 합니다.

가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 보안 영역을 사용하여 적절한 정책이 적용되도록 해야 합니다. 예를 들어, 두 개의 개별 가상 라우터에서 192.168.1.0/24 어드레스 스페이스를 사용하는 경우, 두 가상 라우터의 트래픽에 192.168.1.0/24 네트워크가 적용되도록 지정하는 액세스 제어 규칙이 적용됩니다. 원하는 결과가 아닌 경우, 가상 라우터 중 하나에 대해서만 소스/대상 보안 영역을 지정하여 규칙의 적용을 제한할 수 있습니다.

인터커넥트 가상 라우터

가상 라우터 간의 트래픽을 라우팅하는 정적 경로를 구성할 수 있습니다.

예를 들어 전역 가상 라우터에 외부 인터페이스가 있는 경우, 각각의 다른 가상 라우터에서 정적 기본 경로를 설정하여 외부 인터페이스로 트래픽을 전송할 수 있습니다. 그런 다음, 지정된 가상 라우터 내에서 라우팅할 수 없는 모든 트래픽은 후속 라우팅을 위해 전역 라우터로 전송됩니다.

다른 가상 라우터로의 트래픽을 유출하고 있으므로 가상 라우터 간의 정적 경로를 경로 유출이라고 합니다. VR1 경로에서 VR2로 경로를 유출하는 경우 VR2에서 VR1로만 연결을 시작할 수 있습니다. VR1에서 VR2로의 트래픽을 전송하려면 역방향 경로를 구성해야 합니다. 다른 가상 라우터의 인터페이스에 대한 정적 경로를 생성할 경우 게이트웨이 주소를 지정하지 않아도 됩니다. 대상 인터페이스만 선택하면 됩니다.

가상 라우터 간 경로의 경우, 시스템에서는 소스 가상 라우터에서 대상 인터페이스를 조회합니다. 그런 다음, 대상 가상 라우터에서 다음 홉의 MAC 주소를 조회합니다. 따라서 대상 가상 라우터에는 대상 주소에 대해 선택된 인터페이스의 동적(학습한) 또는 정적 경로가 있어야 합니다.

서로 다른 가상 라우터에서 소스 및 대상 인터페이스를 사용하는 NAT 규칙을 구성하면 가상 라우터 간의 트래픽이 라우팅될 수도 있습니다. NAT에 대해 경로 조회를 수행하는 옵션을 선택하지 않을 경우, 대상 변환이 발생할 때마다 규칙에 따라 NAT 적용 주소가 있는 대상 인터페이스로 트래픽이 전송됩니다. 그러나 대상 가상 라우터에는 변환된 대상 IP 주소에 대한 경로가 있어야 next-hop 조회가 성공할 수 있습니다.

NAT 규칙에서 한 가상 라우터에서 다른 가상 라우터로 트래픽을 유출하여 올바른 라우팅이 보장되는 경우, 변환된 트래픽에 대해 이러한 가상 라우터 간에 정적 경로 유출을 구성하는 것을 권장합니다. 경로 유출이 없는 경우, 일치할 것으로 예상되는 트래픽과 규칙이 일치하지 않을 수도 있으며 변환이 적용되지 않을 수 있습니다.

가상 라우팅은 경로 유출의 연속 또는 체인을 지원하지 않습니다. 예를 들어 FTD에 VR1, VR2 및 VR3 가상 라우터가 있다고 가정합니다. VR3는 네트워크 - 10.1.1.0/24에 직접 연결됩니다. 이제 VR2 및 VR2에서 인터페이스를 통한 네트워크 10.1.1.0/24의 VR1에서의 경로 유출을 구성하고 VR3를 통한 10.1.1.0/24에 대한 경로 유출을 정의한다고 가정합니다. 이 경로 유출 체인은 VR1에서 VR2로의 홉에 대한 트래픽을 허용하지 않으며 VR3에서 나갈 수 없습니다. 경로 유출이 발생하는 경우, 경로 조회는 먼저 입력 가상 라우터의 라우팅 테이블에서 이그레스 인터페이스를 확인한 후, 다음 홉 조회에 대한 가상 라우터의 라우팅 테이블 출력을 확인합니다. 두 조회 모두에서 이그레스 인터페이스가 일치해야 합니다. 이 예에서는, 이그레스 인터페이스가 동일하지 않으므로 트래픽이 통과하지 않습니다.

중복된 IP 주소

가상 라우터는 독립적인 라우팅 테이블의 여러 인스턴스를 생성하므로 동일하거나 중복되는 IP 주소를 충돌 없이 사용할 수 있습니다. FTD를 사용하면 동일한 네트워크를 둘 이상의 가상 라우터에 포함할 수 있습니다. 여기에는 인터페이스 또는 가상 라우터 레벨에서 적용할 여러 정책이 포함됩니다.

몇 가지 예외를 제외하면 라우팅 기능과 대부분의 NGFW 및 IPS 기능은 중복되는 IP 주소의 영향을 받지 않습니다. 다음 섹션에서는 IP 주소 중복과 관련된 제한 사항 및 이를 해결하기 위한 제안 또는 권장 사항에 대해 설명합니다.

중복 IP 주소의 제한 사항

여러 가상 라우터에서 중복 IP 주소를 사용하는 경우 정책을 적절하게 적용하려면 일부 기능에 대해 정책 또는 규칙을 수정해야 합니다. 이러한 기능을 사용하려면 기존 보안 영역을 분할하거나 필요에 따라 새 인터페이스 그룹을 사용하여 더 구체적인 인터페이스를 사용해야 합니다.

다음 기능은 IP 주소가 겹치는 올바른 기능을 위해 수정이 필요합니다.

- 네트워크 맵 - 일부 중복 IP 세그먼트를 제외하도록 네트워크 검색 정책을 수정하여 매핑되는 중복 IP 주소가 없는지 확인합니다.
- ID 정책 - ID 피드 소스는 가상 라우터를 구분할 수 없습니다. 이 제한 사항을 극복하기 위해 중복 주소 공간 또는 가상 라우터를 서로 다른 영역에 매핑합니다.

다음 기능의 경우, 중복 IP 세그먼트에 서로 다른 정책이 적용되도록 특정 인터페이스에 규칙을 적용해야 합니다.

- 액세스 정책
- 사전 필터 정책
- QoS/속도 제한
- SSL 정책

중복 IP 주소로 지원되지 않는 기능

- AC 정책의 ISE SGT 기반 규칙 - Cisco ISE(Identity Services Engine)에서 다운로드한 IP 주소 매핑에 대한 고정 SGT(보안 그룹 태그)에서 가상 라우터를 인식하지 않습니다. 가상 라우터마다 서로 다른 SGT 매핑을 생성해야 하는 경우 가상 라우터마다 별도의 ISE 시스템을 설정합니다. 각

가상 라우터에서 동일한 SGT 번호에 동일한 IP 주소를 매핑하려는 경우에는 이 작업이 필요하지 않습니다.

- 가상 라우터에서는 중복 DHCP 서버 풀이 지원되지 않습니다.
- 이벤트 및 분석 - 대부분의 FMC 분석은 네트워크 맵 및 ID 매핑에 따라 달라지며, 동일한 IP 주소가 두 개의 서로 다른 엔드 호스트에 속하는 경우 이를 구분할 수 없습니다. 따라서 이러한 분석은 동일한 디바이스에 있지만 서로 다른 가상 라우터에 중복 IP 세그먼트가 있는 경우에는 정확하지 않습니다.

디바이스 모델별 최대 가상 라우터 수

생성할 수 있는 최대 가상 라우터 수는 디바이스 모델에 따라 다릅니다. 다음 표에는 최대 한도가 나와 있습니다. 글로벌 가상 라우터를 포함하지 않는 해당 플랫폼에 대해 최대 사용자 정의 가상 라우터 수를 표시하는 **show vrf counters** 명령을 입력하여 시스템을 두 번 확인할 수 있습니다. 아래 표의 숫자에는 사용자 및 글로벌 라우터가 포함되어 있습니다. Firepower 4100/9300의 경우 이러한 숫자는 네이티브 모드에 적용됩니다.

Firepower 4100/9300 등의 다중 인스턴스 기능을 지원하는 플랫폼의 경우 최대 가상 라우터를 디바이스의 코어 수만큼 분할한 다음 가장 근접한 정수로 내림하여 인스턴스에 할당된 코어 수를 곱하여 컨테이너 인스턴스 당 최대 가상 라우터 수를 결정합니다. 예를 들어 플랫폼에서 최대 100개의 가상 라우터를 지원하고 70 코어를 보유한 경우, 각 코어는 최대 1.43개의 가상 라우터(내림됨)를 지원합니다. 따라서 6개의 코어에 할당된 인스턴스는 8.58 가상 라우터를 지원하며, 이 라우터는 8개로 내림되며, 10개의 코어가 할당된 인스턴스는 14.3 가상 라우터(내림함, 14)를 지원합니다.

디바이스 모델	최대 가상 라우터 수
ASA 5508-X	10
ASA 5516-X	10
Firepower 1010	가상 라우터는 이 모델에서 지원되지 않습니다.
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Firepower 4110	60
Firepower 4112	60

디바이스 모델	최대 가상 라우터 수
Firepower 4115	80
Firepower 4120	80
Firepower 4125	100
Firepower 4140	100
Firepower 4145	100
Firepower 4150	100
Firepower 9300 Appliance, 모든 모델	100
Firepower Threat Defense Virtual, 모든 플랫폼	30
ISA 3000	가상 라우터는 이 모델에서 지원되지 않습니다.

관련 항목

컨테이너 인스턴스의 요구 사항 및 사전 요구 사항, 751 페이지

가상 라우터를 위한 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

Network Admin(네트워크 관리자)

보안 승인자

가상 라우터 대한 지침 및 제한 사항

방화벽 모드 지침

가상 라우터는 라우팅 방화벽 모드에서만 지원됩니다.

디바이스 지침

- 가상 라우터는 라우팅된 Firepower Threat Defense 디바이스 버전 6.6 이상에서만 지원됩니다. Firepower Management Center 릴리스 6.6은 6.6 이전의 FTD 버전을 지원하지만, 이러한 디바이스에서는 가상 라우터를 활성화할 수 없습니다.
- Snort3 지원 디바이스는 가상 라우터 기능을 지원하지 않습니다. 따라서 사용자 정의 가상 라우터로 활성화된 Snort2 디바이스를 Snort3 엔진으로 전환하기 전에 가상 라우터에서 디바이스를 제거합니다.

인터페이스 지침

- 인터페이스를 하나의 가상 라우터에만 할당할 수 있습니다.
- 가상 라우터에 할당되는 인터페이스 수에는 제한이 없습니다.
- 논리적 이름의 라우팅 인터페이스만 사용자 정의 가상 라우터에 할당할 수 있습니다.
- 명명된 BVI는 사용자 정의 라우터에 할당할 수 있으며, 가상 라우팅의 IRB에서 지원됩니다.
- 진단 및 관리 전용 인터페이스를 사용자 정의 가상 라우터에 할당할 수도 있습니다.
- 가상 라우터 인터페이스를 비 라우팅 모드로 변경하려면 가상 라우터에서 인터페이스를 제거한 다음 해당 모드를 변경합니다.
- 전역 가상 라우터 또는 다른 사용자 정의 가상 라우터에서 가상 라우터에 인터페이스를 할당할 수 있습니다.
- 이동 중인 인터페이스 또는 가상 라우터를 삭제하는 경로가 소스 또는 대상 가상 라우터 테이블에 있는 경우, 인터페이스 이동 또는 가상 라우터 삭제 전에 경로를 제거합니다.
- 각 가상 라우터에 대해 별도의 라우팅 테이블이 유지되므로, 인터페이스가 하나의 가상 라우터에서 다른 가상 라우터로 이동하면(전역 또는 사용자 정의) 시스템은 인터페이스에 설정된 IP 주소를 일시적으로 제거합니다. 인터페이스의 모든 기존 연결이 종료됩니다. 그러므로 가상 라우터 간에 인터페이스를 이동하면 네트워크 트래픽에 막대한 영향을 미치게 됩니다. 따라서 인터페이스를 이동하기 전에 예방 조치를 취해야 합니다.

전역 가상 라우터 지침

- 이름이 지정되고 다른 가상 라우터의 일부가 아닌 인터페이스는 전역 가상 라우터의 일부입니다.
- 전역 가상 라우터에서 라우팅 인터페이스를 제거할 수 없습니다.
- 전역 가상 라우터는 수정할 수 없습니다.
- 일반적으로 인터페이스를 설정한 후 등록을 취소하고 동일하거나 다른 FMC에 다시 등록하면 디바이스에서 인터페이스 설정을 다시 가져옵니다. 가상 라우터를 지원할 경우, 제한 사항이 있습니다. 전역 가상 라우터 인터페이스의 IP 주소만 유지됩니다.

추가 지침

- 보안 인텔리전스 정책 - 보안 인텔리전스 정책에서는 가상 라우터를 인식하지 않습니다. IP 주소, URL 또는 DNS 이름을 차단 목록에 추가하면 해당 항목이 모든 가상 라우터에 대해 차단됩니다. 이 제한 사항은 보안 영역이 있는 인터페이스에 적용됩니다.
- NAT 규칙 - NAT 규칙에서 인터페이스를 혼합하지 마십시오. 가상 라우팅에서 지정된 소스 및 대상 인터페이스 개체(인터페이스 그룹 또는 보안 영역)에 서로 다른 가상 라우터에 속하는 인터페이스가 있는 경우, NAT 규칙에서는 다른 가상 라우터를 통해 하나의 가상 라우터에서 트래픽을 전환합니다. NAT는 인바운드 인터페이스에 대해서만 가상 라우터 테이블에서 경로 조회를 수행합니다. 필요한 경우 소스 가상 라우터에서 대상 인터페이스에 대한 고정 경로를 정의합니다. 인터페이스를 **any**로 둘 경우, 가상 라우터 멤버십에 관계없이 규칙이 모든 인터페이스에 적용됩니다.
- DHCP 릴레이 - DHCP 릴레이에 대한 가상 라우터 상호 연결은 지원되지 않습니다. 예를 들어, DHCP 클라이언트가 VR1 인터페이스에서 활성화되고 DHCP 릴레이 서버가 VR2 인터페이스에서 활성화된 경우, VR1 및 VR2를 상호 연결하면 가상 라우터 내에서 DHCP 전송이 이루어집니다.

FMC 웹 인터페이스 라우팅 페이지에 대한 수정 사항

FTD 6.6 이전 디바이스 및 소수의 디바이스 모델은 가상 라우팅 기능을 지원하지 않습니다. FMC 웹 인터페이스는 이러한 비 지원 디바이스에 대해 FMC 6.5 또는 이전 버전과 동일한 라우팅 페이지를 표시합니다. 가상 라우팅이 지원되는 디바이스 및 플랫폼을 확인하려면 디바이스 모델별 최대 가상 라우터 수을 참조하십시오.

지원되는 디바이스의 라우팅 페이지에서 가상 라우터를 구성할 수 있습니다.

1. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**로 이동하여 가상 라우터 인식 디바이스를 편집합니다.
2. **Routing(**라우팅**)**을 클릭하여 가상 라우터 페이지에 입장합니다.

가상 라우팅을 사용하는 디바이스의 경우 Routing(라우팅) 페이지의 왼쪽 창에는 다음이 표시됩니다.

- **Manage Virtual Routers(**가상 라우터 관리**)**-가상 라우터를 생성하고 관리할 수 있습니다.
- List of virtual routing protocols(가상 라우팅 프로토콜 목록)-가상 라우터에 대해 구성할 수있는 라우팅 프로토콜을 나열합니다.
- **Settings(**설정**)** - 모든 가상 라우터에 적용 가능한 BGP 일반 설정을 구성할 수 있습니다. 다른 BGP 설정을 정의하려면 **Enable BGP(BGP** 활성화**)** 확인란을 선택합니다. 가상 라우터에 대한 다른 BGP 설정을 구성하려면 가상 라우팅 프로토콜에서 **BGP**로 이동합니다.

가상 라우터 관리 페이지

Virtual Routers(가상 라우터) 창에서 **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭하면 Manage Virtual Routers(가상 라우터 관리) 페이지가 나타납니다. 이 페이지에는 디바이스 및 연결된 인터페이스의 기존 가상 라우터가 표시됩니다. 이 페이지에서 디바이스에 가상 라우터 추가 ( )할 수 있습니다. 사용자 정의 가상 라우터를 수정( )하거나 삭제( )할 수도 있습니다. 전역 가상 라우터는 편집하거나 제거할 수 없습니다. 전역 가상 라우터의 세부 사항만 보기 ( ) 수 있습니다.

가상 라우터 생성

프로시저

단계 **1** **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭합니다.

단계 **4** 가상 라우터 추가 ( ) 버튼을 클릭합니다.

단계 **5** Add Virtual Router(가상 라우터 추가) 상자에 가상 라우터의 이름과 설명을 입력합니다.

단계 **6** **Ok(**확인**)**를 클릭합니다.

Routing(라우팅) 페이지가 나타나고 새로 생성된 가상 라우터 페이지가 표시됩니다.

다음에 수행할 작업

- 가상 라우터 구성.

가상 라우터 구성

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	해당 없음	FTD 및 FTDv	Any(모든)	관리자/네트워크 관리자/보안 승인자

사용자 정의 가상 라우터에 인터페이스를 할당하고 디바이스에 대한 라우팅 정책을 설정할 수 있습니다. 글로벌 가상 라우터의 인터페이스를 수동으로 추가하거나 제거할 수는 없지만, 디바이스 인터페이스에 대한 라우팅 정책을 설정할 수 있습니다.

시작하기 전에

- 사용자 정의 가상 라우터에 대한 라우팅 정책을 구성하려면 라우터를 추가합니다. 가상 라우터 생성, 996 페이지의 내용을 참조하십시오.
- 비 VRF 가능 디바이스의 모든 라우팅 구성 설정은 글로벌 가상 라우터에도 사용할 수 있습니다. 설정에 대한 자세한 내용은 Firepower Threat Defense 라우팅 개요을 참조하십시오.
- 사용자 정의 가상 라우터에는 제한된 라우팅 프로토콜만 지원됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 가상 라우터 지원 디바이스를 편집합니다. **Routing(**라우팅**)**으로 이동합니다. 라우팅 페이지 수정에 대해서는 FMC 웹 인터페이스 라우팅 페이지에 대한 수정 사항, 995 페이지의 내용을 참조하십시오.

단계 **2** 드롭다운 목록에서 원하는 가상 라우터를 선택합니다.

단계 **3** **Virtual Router Properties(**가상 라우터 속성**)** 페이지에서 설명을 수정할 수 있습니다.

단계 **4** 인터페이스를 추가하려면 **Available Interface(**사용 가능한 인터페이스**)** 상자에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭합니다.

다음 사항에 유의하십시오.

- **Available Interface(**사용 가능한 인터페이스**)** 상자 아래에는 논리적 이름이 있는 인터페이스만 나열됩니다. **Interface(**인터페이스**)**에서 논리적 이름을 제공하고 인터페이스를 편집할 수 있습니다. 설정이 적용되려면 변경 사항을 저장해야 합니다.
- 전역 가상 라우터의 인터페이스만 할당에 사용할 수 있습니다. 즉, **Available Interfaces(**사용 가능한 인터페이스**)** 상자에는 다른 사용자 정의 가상 라우터에 할당되지 않은 인터페이스만 나열됩니다.

단계 **5** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

단계 **6** 가상 라우터에 대한 라우팅 정책을 설정하려면 각 이름을 클릭하여 해당하는 설정 페이지를 엽니다.

- **OSPF** - 사용자 정의 가상 라우터에서는 OSPFv2만 지원됩니다. OSPFv2에 대한 다른 모든 설정은 비 가상 라우터 인식 인터페이스에 적용됩니다. 단, **Interface(**인터페이스**)**에서는 설정한 가상 라우터의 인터페이스만 선택할 수 있습니다. 전역 가상 라우터에 대해 OSPFv3 및 OSPFv2 라우팅 정책을 정의할 수 있습니다. OSPF 설정에 대한 자세한 내용은 Firepower Threat Defense OSPF, 1041 페이지의 내용을 참조하십시오.
- **RIP** - 전역 가상 라우터에 대해서만 RIP 라우팅 정책을 설정할 수 있습니다. RIP 설정에 대한 자세한 내용은 Firepower Threat Defense RIP, 1091 페이지의 내용을 참조하십시오.
- **BGP** - 이 페이지는 **Settings(**설정**)**에서 구성한 BGP 일반 설정을 표시합니다.
  - 이 페이지에서는 라우터 ID 설정을 제외한 일반 설정을 수정할 수 없습니다. 이 페이지에서 **Settings(**설정**)** 페이지에 정의된 라우터 ID 설정을 수정하여 재정의할 수 있습니다.

- 다른 BGP IPv4 또는 IPv6 설정을 구성하려면 **BGP** 페이지의 **General Settings(**일반 설정**)**에서 BGP 옵션을 활성화해야 합니다.
- 사용자 정의 가상 라우터에는 IPv4 주소군이 있는 BGP 구성만 지원됩니다.

BGP 설정 구성에 대한 자세한 내용은 Firepower Threat Defense BGP, 1073 페이지의 내용을 참조하십시오.

- 정적 경로 - 이 설정을 사용하여 특정 대상 네트워크에 대해 트래픽을 보낼 위치를 정의합니다. 이 설정을 통해 가상 라우터 간 정적 경로를 생성할 수도 있습니다. 사용자 정의 또는 글로벌 가상 라우터의 인터페이스를 사용하여 연결된 경로 또는 정적 경로 유출을 생성할 수 있습니다. **FMC**는 인터페이스가 다른 가상 라우터에 속해 있음을 나타내기 위해 인터페이스에 접두사를 지정하여 경로 유출에 사용할 수 있습니다. 경로 유출이 성공하려면 다음 홉 게이트웨이를 지정하지 마십시오.

  정적 경로 테이블은 **Leaked from Virtual Router(**가상 라우터에서 유출된 경로**)** 열에서 경로 유출에 사용되는 인터페이스가 있는 가상 라우터를 표시합니다. 경로 유출이 아닌 경우, 열이 N/A(해당 없음)로 표시됩니다.

  정적 경로가 속한 가상 라우터에 관계없이 Null0 인터페이스는 정적 경로가 속한 동일한 가상 라우터의 인터페이스와 함께 나열됩니다.

  정적 경로 설정에 대한 자세한 내용은 Firepower Threat Defense 정적 및 기본 경로, 1035 페이지의 내용을 참조하십시오.

- 멀티캐스트 - 전역 가상 라우터에 대해서만 멀티캐스트 라우팅 정책을 설정할 수 있습니다. 멀티캐스트 설정에 대한 자세한 내용은 Firepower Threat Defense 멀티캐스트 라우팅, 1099 페이지의 내용을 참조하십시오.

단계 **7** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 가상 라우터 수정
- 가상 라우터 제거

가상 라우터 수정

가상 라우터의 설명 및 기타 라우팅 정책을 수정할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭합니다.

가상 라우터 페이지에 할당된 인터페이스와 함께 모든 가상 라우터가 표시됩니다.

단계 **4** 가상 라우터를 수정하려면 원하는 가상 라우터에 해당하는 수정( )을 클릭합니다.

참고 글로벌 가상 라우터의 일반 설정은 수정할 수 없습니다. 따라서 글로벌 라우터에서는 편집을 사용할 수 없습니다. 대신 설정을 볼 수 있는 보기 ( )이 제공됩니다.

단계 **5** 변경 사항을 저장하려면 **Save(**저장**)**을 클릭합니다.

다음에 수행할 작업

- 가상 라우터 제거

가상 라우터 제거

시작하기 전에

- 글로벌 가상 라우터는 삭제할 수 없습니다. 따라서 글로벌 가상 라우터에서는 삭제 옵션을 사용할 수 없습니다.
- 한 번에 여러 가상 라우터를 제거할 수 있습니다.
- 삭제된 가상 라우터의 모든 라우팅 정책도 삭제됩니다.
- 삭제된 가상 라우터의 모든 인터페이스는 글로벌 가상 라우터로 이동합니다.
- IP 이동, 경로 충돌 등 인터페이스 이동에 제한이 있는 경우, 충돌을 해결한 후에만 라우터를 제거할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭합니다.

매핑된 인터페이스와 함께 모든 가상 라우터가 가상 라우터 페이지에 표시됩니다.

단계 **4** 가상 라우터를 제거하려면 원하는 가상 라우터에 해당하는 삭제( )을 클릭합니다.

단계 **5** 여러 라우터를 제거하려면 CTRL 키를 누른 상태에서 삭제할 가상 라우터를 클릭합니다. 마우스 오른쪽 버튼을 클릭하고 **Delete(**삭제**)**를 클릭합니다.

단계 **6** 변경 사항을 저장하려면 **Save(**저장**)**을 클릭합니다.

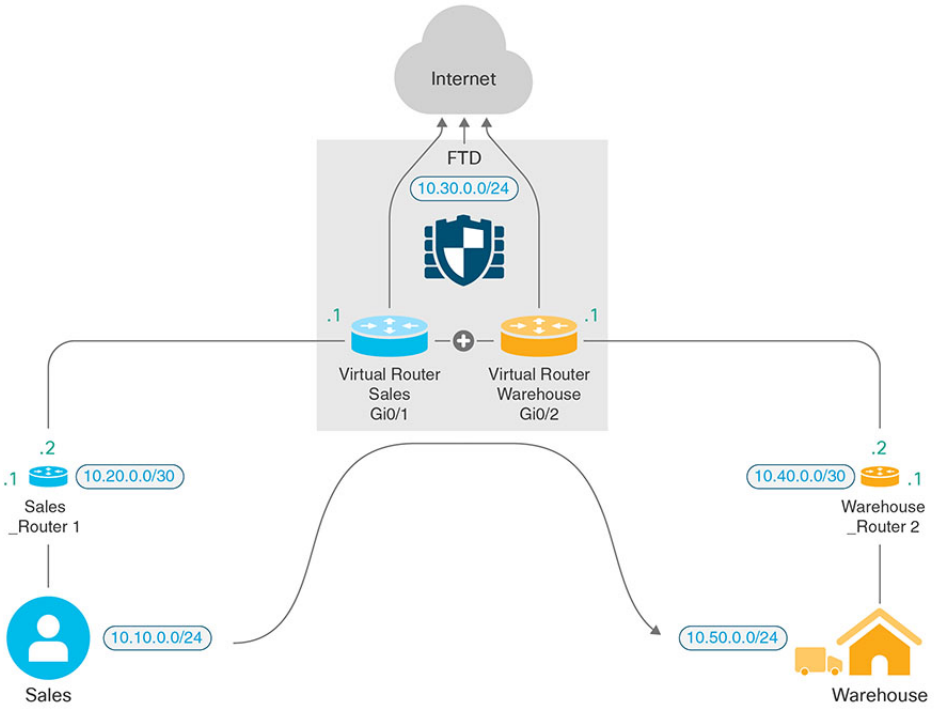
가상 라우터의 구성 예시

가상 라우터를 통해 원거리 서버로 라우팅하는 방법

가상 라우팅에서 여러 가상 라우터를 생성하여 인터페이스 그룹에 대해 별도의 라우팅 테이블을 유지 관리할 수 있으므로 네트워크 분리를 달성할 수 있습니다. 일부 시나리오에서는 별도의 가상 라우터를 통해서만 연결할 수 있는 서버에 액세스해야 할 수 있습니다. 이 예에서는 여러 홉이 있는 호스트에 연결하기 위해 가상 라우터를 상호 연결하는 절차를 제공합니다.

의류 회사 영업 부서 직원이 공장 유닛의 창고 관리 부서에서 보관 중인 재고를 조회하려는 경우를 예로 들어 보겠습니다. 가상 라우팅 환경에서는 영업 부서에서 대상(창고 관리 부서)까지 가상 라우터 간에 멀티 홉의 경로 유출을 사용해야 합니다. 이 경로 유출은 멀티 홉 경로 유출을 추가하여 수행됩니다. 이 경우 영업 가상 라우터(소스)에 있는 정적 경로에서 창고 가상 라우터의 인터페이스(대상)까지의 정적 경로를 구성합니다. 대상 네트워크가 떨어져 있으므로(멀티 홉), 창고 가상 라우터를 또한 대상 네트워크(일명 10.50.0.0/24)까지의 경로를 통해 구성해야 합니다.

그림 ***36: 2***개의 가상 라우터 인터커넥트 **-** 예



시작하기 전에

이 예에서는 10.20.0.1/30 인터페이스에서 10.50.0.5/24로의 트래픽을 라우팅하기 위해 이미 Sales_Router1를 구성한 것으로 가정합니다.

프로시저

단계 **1** 영업 가상 라우터에 할당할 디바이스의 내부 인터페이스(Gi0/1)를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) Gi0/1 인터페이스를 수정합니다:

- 이름 - 이 예의 경우 VR-Sales입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 10.30.0.1/24를 입력합니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** 창고 가상 라우터에 할당할 디바이스의 내부 인터페이스(Gi0/2)를 구성합니다:

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) Gi0/2 인터페이스를 수정합니다:

- 이름 - 이 예의 경우 VR-Warehouse입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 공백으로 둡니다. 아직 사용자 정의 가상 라우터를 생성하지 않았으므로 동일한 IP 주소(10.30.0.1/24)의 인터페이스를 구성할 수 없습니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **3** 영업 및 창고 가상 라우터를 생성하고 해당 인터페이스를 할당합니다:

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다.

c) **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 Sales(영업)를 생성합니다.

d) **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 Warehouse(창고)를 생성합니다.

e) **Virtual Router Properties(**가상 라우터 속성**)**의 가상 라우터 드롭다운에서 Sales(영업)를 선택하고 VR-Sales를 **Selected Interface(**선택된 인터페이스**)**로 추가하고 저장합니다.

f) **Virtual Router Properties(**가상 라우터 속성**)**의 가상 라우터 드롭다운에서 Warehouse(창고)를 선택하고 VR-Warehouse를 **Selected Interface(**선택된 인터페이스**)**로 추가하고 저장합니다.

단계 **4** VR-Warehouse 인터페이스 컨피그레이션을 다시 확인합니다:

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VR-Warehouse 인터페이스에 대해 **Edit(**편집**)**를 클릭합니다. IP 주소를 10.30.0.1/24로 지정합니다. 이제 시스템에서 VR-Sales의 동일한 IP 주소로 구성할 수 있습니다. 왜냐하면 인터페이스는 두 개의 서로 다른 가상 라우터에 별도로 할당되기 때문입니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **5** 창고 서버용 네트워크 개체 생성-10.50.0.0/24 및 창고 게이트웨이에 대한 네트워크 개체 생성 -10.40.0.2/30:

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 선택합니다.

- 이름-이 예시로는 Warehouse-Server가 있습니다.
- 네트워크-Network(네트워크)를 클릭하고 10.50.0.0/24를 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

d) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 선택합니다.

- 이름-이 예시로는 Warehouse-Gateway가 있습니다.
- 네트워크)-Host를 클릭하고 10.40.0.2를 입력합니다.

e) **Save(**저장**)**를 클릭합니다.

단계 **6** VR-Warehouse 인터페이스를 가리키는 영업의 경로 유출을 정의합니다.

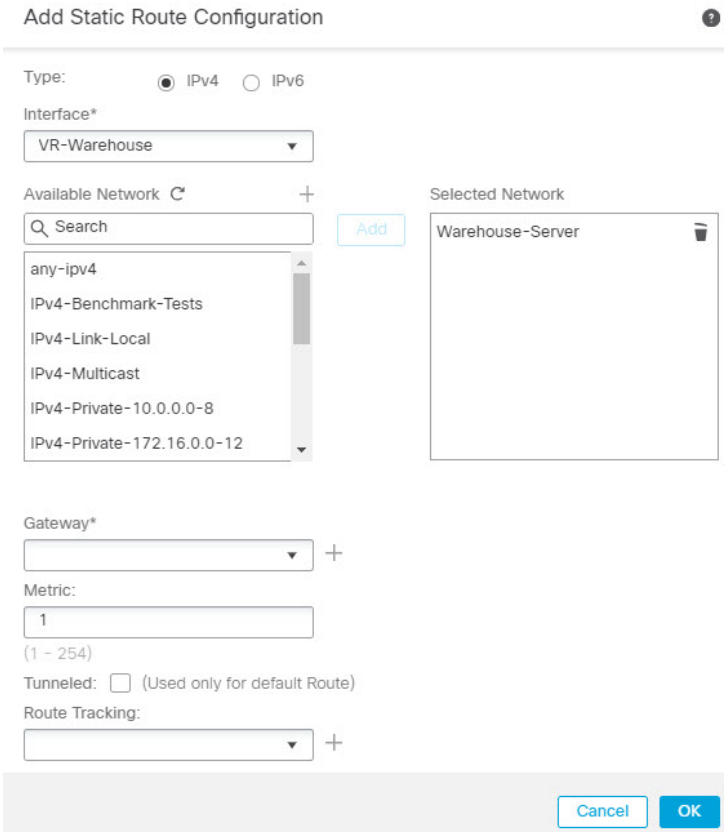
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 선택합니다.

c) 드롭다운에서 영업 가상 라우터를 선택한 다음 **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- 인터페이스-VR-Warehouse를 선택합니다.
- 네트워크 — Warehouse-Server 개체를 선택합니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.



e) **Ok(**확인**)**를 클릭합니다.

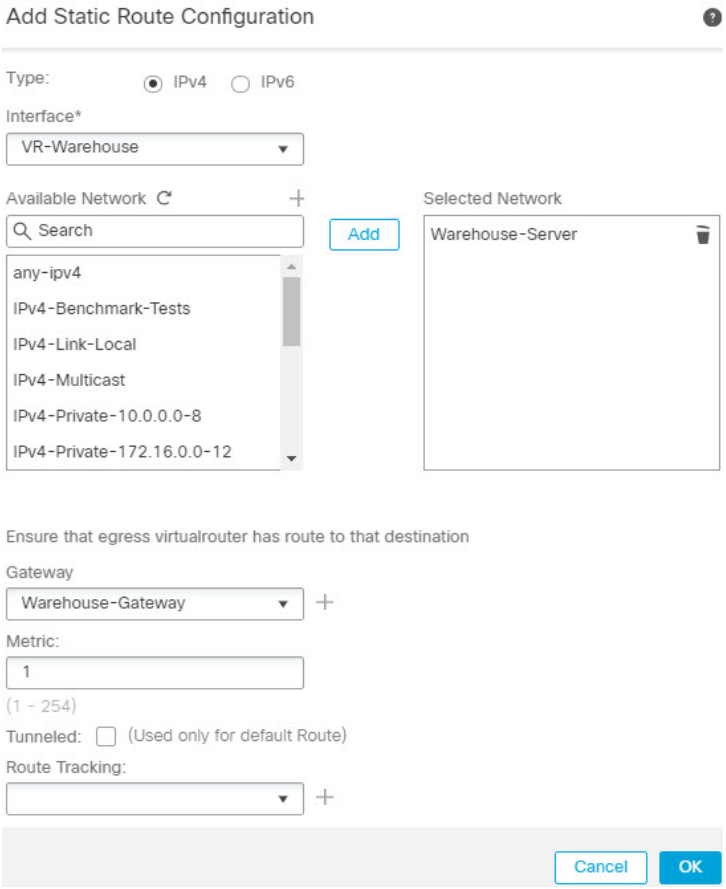
f) **Save(**저장**)**를 클릭합니다.

단계 **7** 창고 가상 라우터에서 창고 라우터 2 게이트웨이를 가리키는 경로를 정의합니다:

a) 드롭다운에서 창고 가상 라우터를 선택한 다음 **Static Route(**정적 경로**)**를 클릭합니다.

b) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- 인터페이스-VR-Warehouse를 선택합니다.
- 네트워크 — Warehouse-Server 개체를 선택합니다.
- 게이트웨이 — Warehouse-Gateway 개체를 선택합니다.



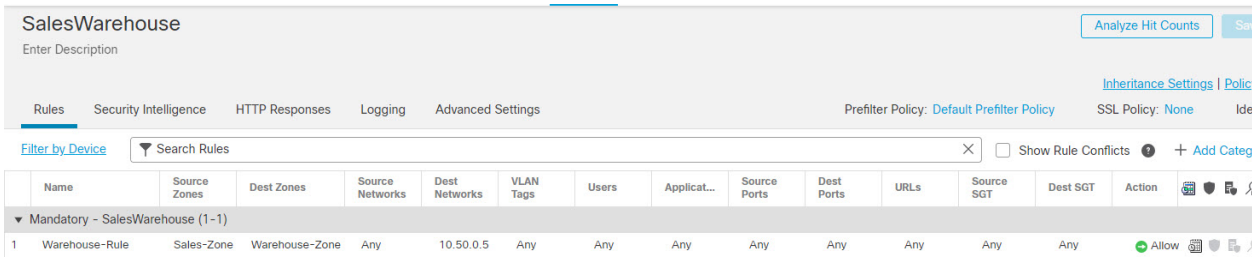
c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **8** 창고 서버에 대한 액세스를 허용하는 액세스 컨트롤 규칙을 구성합니다. 액세스 컨트롤 규칙을 생성하려면 보안 영역을 생성해야 합니다. **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**를사용합니다. **Add(**추가**)** > **Security Zone(**보안 영역**)**을 선택하고 VR-Sales와 VR-Warehouse에 대한 보안 영역을 생성합니다. Warehouse-Server 네트워크 개체의 경우, Warehouse-Server 인터페이스 그룹(**Add(**추가**)** > **Interface Group(**인터페이스 그룹**)** 선택)을 생성합니다.

단계 **9** 정책 > 액세스 컨트롤을 선택하고 액세스 컨트롤 규칙을 구성하여 영업 가상 라우터에 있는 소스 인터페이스의 트래픽을 대상 Warehouse-Server 네트워크 개체에 대한 창고 가상 라우터에 있는 대상 인터페이스로 전송할 수 있습니다.

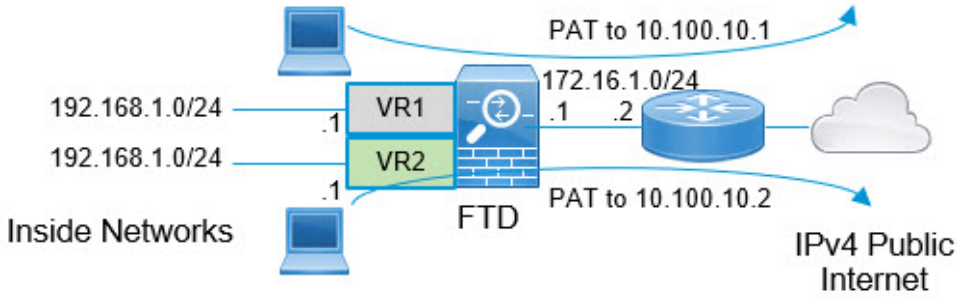
예를 들어 영업 가상 라우터에 있는 인터페이스가 Sales-Zone 보안 영역에 있을 경우, 창고 가상 라우터에 있는 해당 인터페이스는 Warehouse-Zone 보안 영역에 존재하며 액세스 제어 규칙은 다음과 유사합니다.



중복된 주소 공간에 인터넷 액세스를 제공하는 방법

가상 라우터를 사용할 경우, 별도의 라우터에 상주하는 인터페이스에 대해 동일한 네트워크 주소를 사용할 수 있습니다. 그러나 이러한 별도의 가상 라우터에서 라우팅되는 IP 주소는 동일하므로 개별 NAT/PAT 풀이 있는 각 인터페이스에 NAT/PAT 규칙을 적용하여 반환 트래픽이 올바른 대상으로 전달되도록 합니다. 이 예에서는 중복 주소 공간을 관리하기 위해 가상 라우터 및 NAT/PAT 규칙을 구성하는 절차를 제공합니다.

예를 들어 FTD에서 vr1-inside 및 vr2-inside 인터페이스를 정의하여 두 인터페이스가 모두 192.168.1.1/24라는 IP 주소를 사용하도록 하고 192.168.1.0/24 네트워크의 해당 세그먼트에서 엔드포인트를 관리할 수 있습니다. 동일한 주소 공간을 사용하는 두 개의 가상 라우터에서 인터넷 액세스를 허용하려면, 각 가상 라우터 내의 인터페이스에 개별적으로 NAT 규칙을 적용해야 합니다. 이 경우 별도의 NAT 또는 PAT 풀을 사용하는 것이 좋습니다. PAT를 사용하여 VR1의 소스 주소를 10.100.10.1로 변환하고, VR2의 소스 주소를 10.100.10.2로 변환할 수 있습니다. 아래 그림에는 이러한 설정이 나와 있습니다. 여기서 인터넷 연결 외부 인터페이스는 전역 라우터의 일부입니다. 소스 인터페이스(vr1-inside 및 vr2-inside)를 명시적으로 선택한 상태에서 NAT/PAT 규칙을 정의해야 합니다. 왜냐하면 "any"를 소스 인터페이스로 사용할 경우 2개의 서로 다른 인터페이스에 동일한 IP 주소가 존재할 수 있으므로, 시스템에서 올바른 소스를 식별하는 것이 불가능하기 때문입니다.



참고 중복된 주소 공간을 사용하지 않는 가상 라우터 내에 일부 인터페이스가 있는 경우에도 NAT 규칙을 소스 인터페이스로 정의하면 문제 해결을 더 쉽게 하고, 인터넷에 바인딩된 가상 라우터에서 나가는 트래픽을 더 명확하게 분리할 수 있습니다.

프로시저

단계 **1** VR1에 대한 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VR1에 할당할 인터페이스를 수정합니다.

- **Name(**이름**)** - 이 예에서는 vr1-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)**-192.168.1.1/24를 입력합니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** VR2에 대한 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VR2에 할당할 인터페이스를 수정합니다.

- **Name(**이름**)** - 이 예에서는 vr2-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 공백으로 둡니다. 아직 사용자 정의 가상 라우터를 생성하지 않았으므로 동일한 IP 주소의 인터페이스를 구성할 수 없습니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **3** 외부 인터페이스에 대한 정적 기본 경로 유출과 VR1을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VR1을 생성합니다.

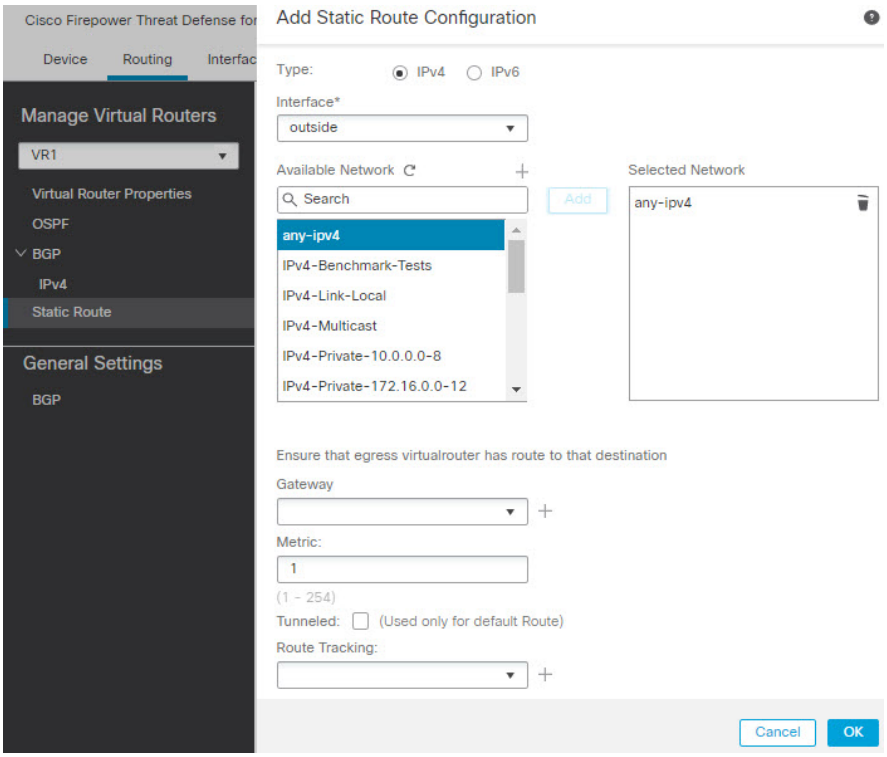
c) VR1의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 vr1-inside를 할당하고 저장합니다.

d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다. 이 네트워크가 VR1 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.

- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 제공하지 마십시오.



f) **Ok(**확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

단계 **4** 외부 인터페이스에 대한 정적 기본 경로 유출과 VR2을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

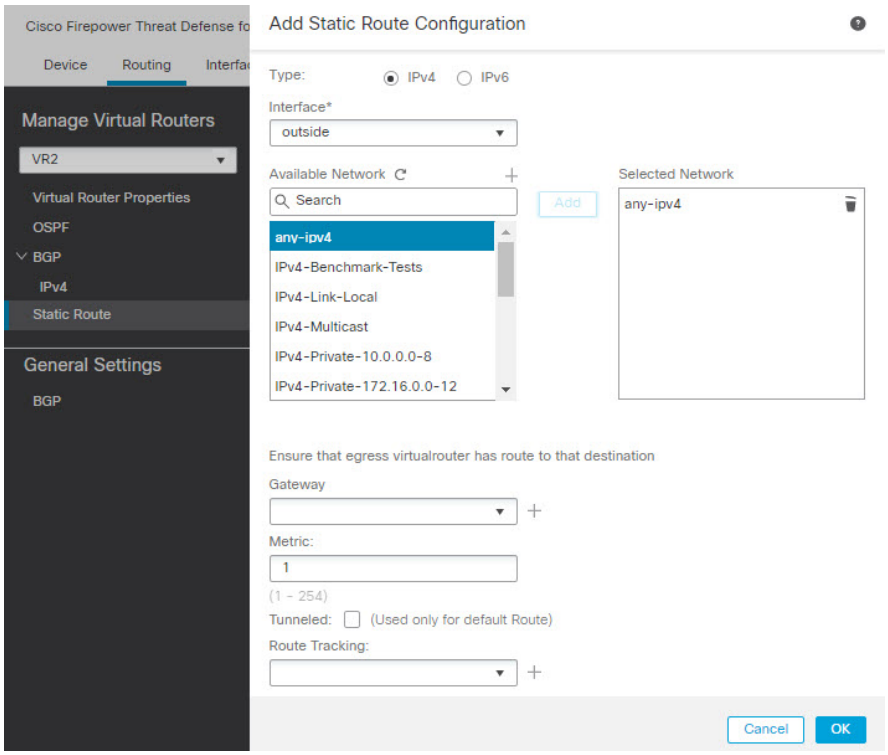
b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VR2를 생성합니다.

c) VR2의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 vr2-inside를 할당하고 저장합니다.

d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다. 이 네트워크가 VR2 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.



f) **Ok(**확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

단계 **5** 전역 라우터의 외부 인터페이스에서 IPv4 고정 기본 경로(즉, 172.16.1.2)를 구성합니다.

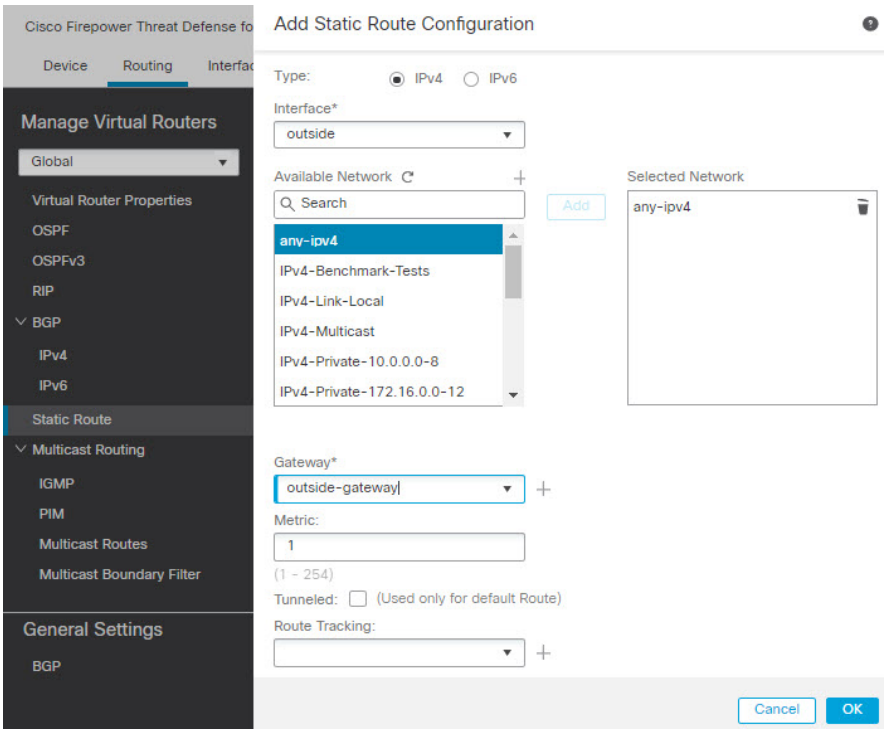
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 선택하고 전역 라우터 속성을 수정합니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다. 이 경로가 모든 IPv4 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)**-이미 생성된 경우 드롭 다운에서 호스트 이름을 선택합니다. 개체가 아직 생성되지 않았다면 **Add(**추가**)**를 클릭한 다음 외부 인터페이스에서 네트워크 링크의 다른 끝에 있는 게이트웨이의 IP 주소(이 예에서는 172.16.1.2)에 대한 호스트 개체를 정의합니다. 개체를 생성한 후 게이트웨이 필드에서 해당 개체를 선택합니다.



e) **Ok(**확인**)**를 클릭합니다.

f) **Save(**저장**)**를 클릭합니다.

단계 **6** vr2-inside 인터페이스 구성을 다시 확인합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) vr2-inside 인터페이스에 대해 **Edit(**편집**)**를 클릭합니다. IP 주소를 192.168.1.1/24로 지정합니다. 이제 시스템에서 vr1-inside의 동일한 IP 주소로 구성할 수 있습니다. 왜냐하면 인터페이스는 두 개의 서로 다른 가상 라우터에 별도로 할당되기 때문입니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **7** VR1의 외부 트래픽이 10.100.10.1로 향하도록 PAT inside에 대한 NAT 규칙을 생성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택합니다.

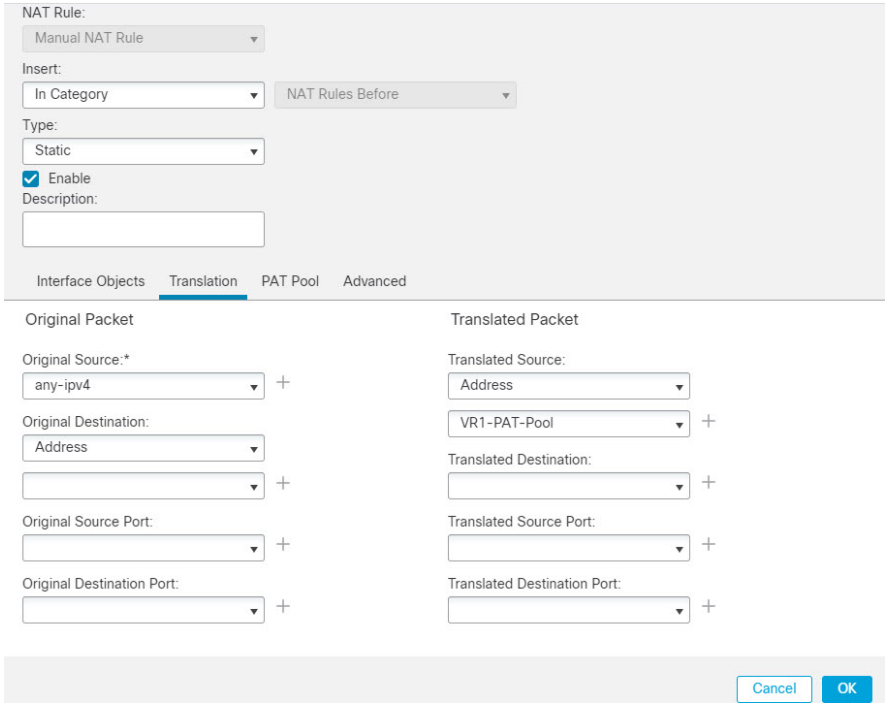
b) **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.

c) NAT 정책 이름으로 InsideOutsideNATRule을 입력하고 FTD 디바이스를 선택합니다. **Save(**저장**)**를 클릭합니다.

d) InsideOutsideNATRule 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 다음을 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- **Type(**유형**)** - Dynamic(동적)을 선택합니다.
- **Insert(**삽입**)**-동적 NAT 규칙이 있는 경우 위의 내용을 입력합니다.
- **Enable(**활성화**)**을 클릭합니다.

- **Interface Objects(**인터페이스 개체**)**에서 vr1-interface object(vr1-인터페이스 개체)를 선택하고 **Add to Source(**소스에 추가**)** 를 클릭합니다(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성). outside(외부)를 **Add to Destination(**대상에 추가**)**로 선택합니다.
- **Translation(**변환)에서 **Original Source(**원본 소스**)**로 any-ipv4를 선택합니다. **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 호스트 개체 VR1-PAT-Pool을 10.100.10.1로 정의합니다. 아래 그림과 같이 VR1-PAT-Pool을 선택합니다.



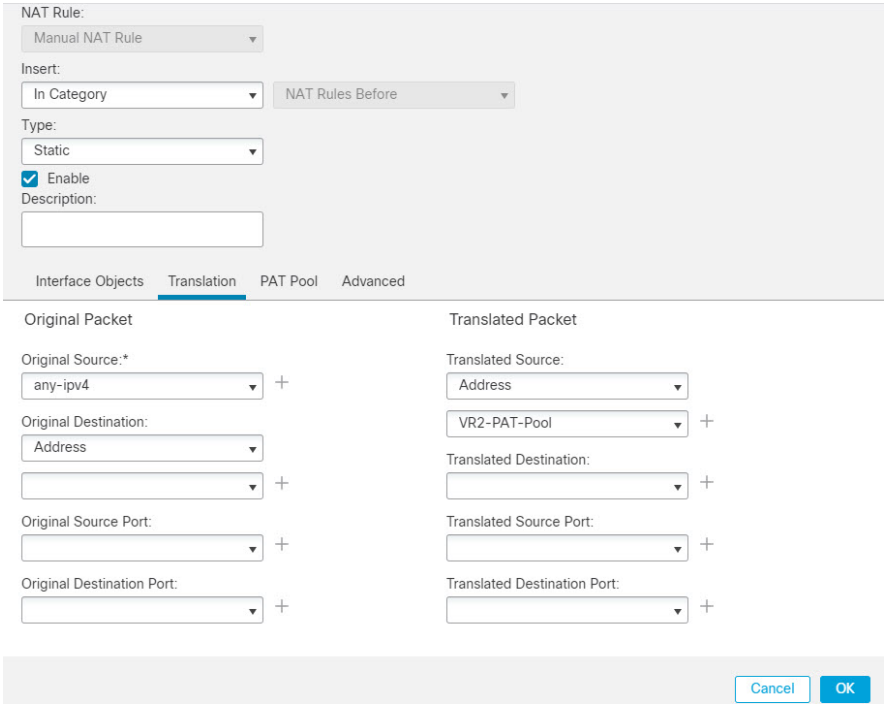
e) **Ok(**확인**)**를 클릭합니다.
f) **Save(**저장**)**를 클릭합니다.

단계 **8** VR2의 외부 트래픽이 10.100.10.2로 향하도록 PAT inside에 대한 NAT 규칙을 추가합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택합니다.
b) InsideOutsideNATRule을 수정하여 VR2 NAT 규칙을 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- **Type(**유형**)** - Dynamic(동적)을 선택합니다.
- **Insert(**삽입**)**-동적 NAT 규칙이 있는 경우 위의 내용을 입력합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 vr2-interface object(vr2-인터페이스 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성). outside(외부)를 **Add to Destination(**대상에 추가**)**로 선택합니다.

- **Translation(**변환)에서 **Original Source(**원본 소스)로 any-ipv4를 선택합니다. **Translated Source(**변환된 소스)에서 **Add(**추가)를 클릭하고 호스트 개체 VR2-PAT-Pool을 10.100.10.2로 정의합니다. 아래 그림과 같이 VR2-PAT-Pool을 선택합니다.



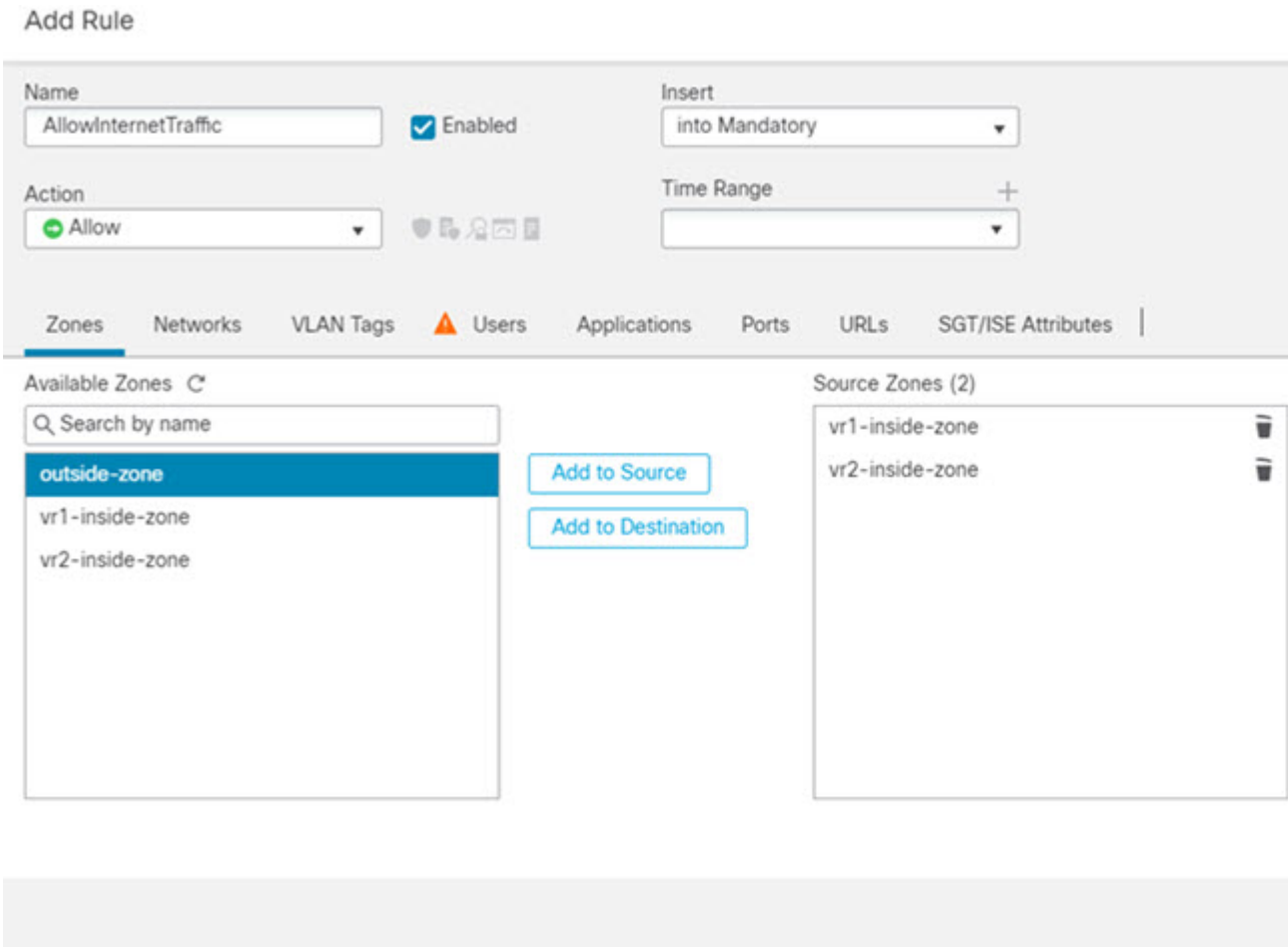
c) **Ok(**확인)를 클릭합니다.

d) **Save(**저장)를 클릭합니다.

단계 **9** vr1-inside 및 vr2-inside 인터페이스에서 외부 인터페이스로 향하는 트래픽을 허용하는 액세스 제어 정책을 구성하려면 보안 영역을 생성해야 합니다. **Object(**개체) > **Object Management(**개체 관리) > **Interface(**인터페이스)를 사용합니다. **Add(**추가) > **Security Zone(**보안 영역)을 선택하고 vr1-inside, vr2-inside 및 외부 인터페이스에 대한 보안 영역을 생성합니다.

단계 **10** **Policies(**정책) > **Access Control(**액세스 제어)을 선택하고, 트래픽이 vr1-inside-zone 및 vr2- inside-zone에서 outside_zone으로 향하도록 허용하는 액세스 제어 규칙을 구성합니다.

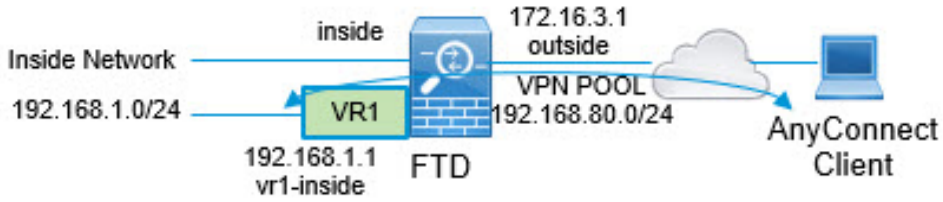
인터페이스의 이름을 딴 영역을 생성한다고 가정할 경우, 모든 트래픽이 인터넷으로 흐르도록 허용하는 기본 규칙은 다음과 같습니다. 이 액세스 제어 정책에 다른 매개 변수를 적용할 수 있습니다.



RA VPN 액세스를 가상 라우터의 내부 네트워크에 허용하는 방법

가상 라우팅이 활성화된 디바이스에서는 RA VPN이 전역 가상 라우터 인터페이스에서만 지원됩니다. 이 예에서는 AnyConnect 클라이언트 사용자가 사용자 정의 가상 라우터 네트워크에 연결할 수 있는 절차를 제공합니다.

다음 예에서 RA VPN 사용자(AnyConnect 클라이언트)는 172.16.3.1의 FTD 외부 인터페이스에 연결되며 192.168.80.0/24 풀 내에 IP 주소가 지정됩니다. 사용자는 전역 가상 라우터의 내부 네트워크에 액세스할 수 있습니다. 사용자 정의 가상 라우터 VR1(192.168.1.0/24)의 네트워크를 통한 트래픽 흐름을 허용하려면 전역 및 VR1에서 고정 경로를 구성하여 경로를 유출합니다.



시작하기 전에

이 예에서는 RA VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

프로시저

단계 **1** 전역 가상 라우터에서 사용자 정의 VR1으로의 경로 유출을 설정합니다.

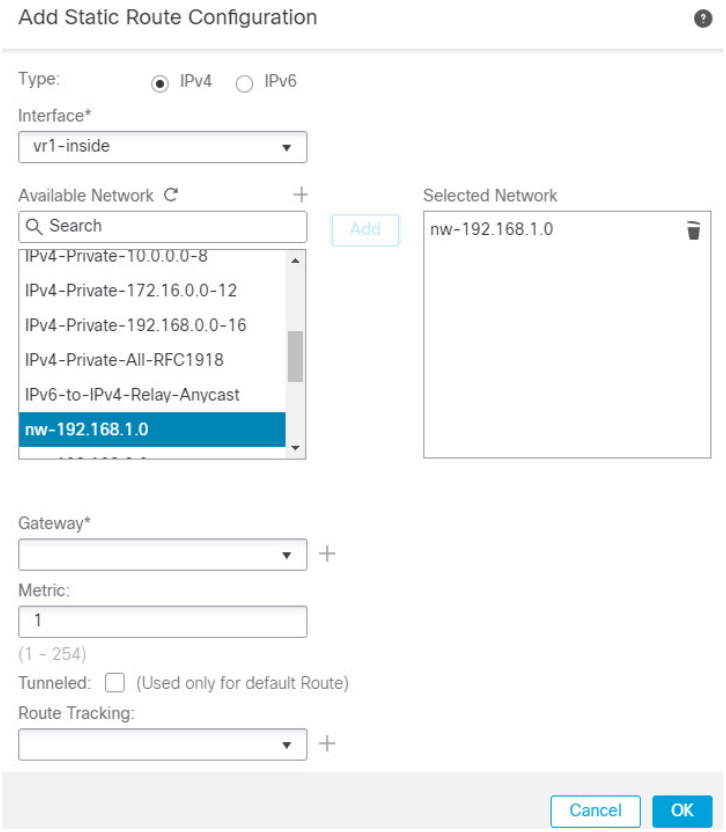
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 클릭합니다. 기본적으로 Global routing properties(전역 라우팅 속성) 페이지가 나타납니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- 인터페이스 - VR1 내부 인터페이스를 선택합니다.
- 네트워크 - VR1 가상 라우터 네트워크 개체를 선택합니다. **Add Object(**개체 추가**)** 옵션을 사용하여 생성할 수 있습니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.



경로 유출을 사용하면 VPN 풀에서 AnyConnect 클라이언트 할당 IP 주소로 VR1 가상 라우터에서 192.168.1.0/24 네트워크에 액세스할 수 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 설정합니다.

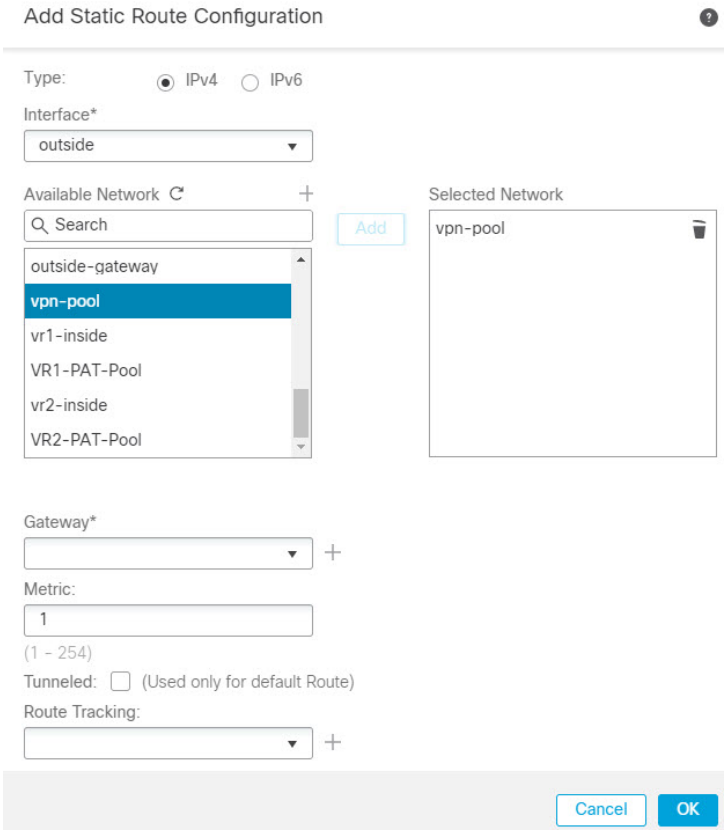
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 클릭하고 드롭다운에서 VR1을 선택합니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- 네트워크 - 전역 가상 라우터 네트워크 개체를 선택합니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.



구성된 정적 경로를 사용하면 192.168.1.0/24 네트워크(VR1)의 엔드포인트가 VPN 풀에서 AnyConnect 클라이언트 할당 IP 주소에 대한 연결을 시작할 수 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

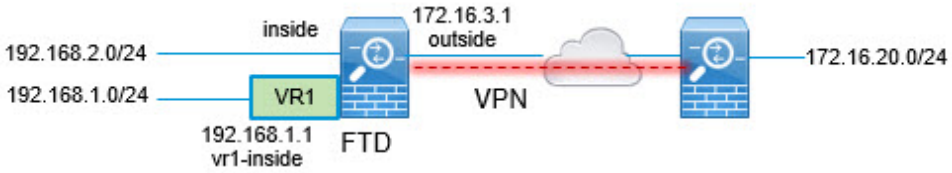
다음에 수행할 작업

RA VPN 주소 풀과 사용자 정의 가상 라우터의 IP 주소가 중복되는 경우 IP 주소에서 고정 NAT 규칙을 또한 사용하여 적절한 라우팅을 활성화해야 합니다. 또는 중복이 없도록 RA VPN 주소 풀을 변경할 수 있습니다.

사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법

가상 라우팅이 활성화된 디바이스에서는 사이트 간 VPN이 전역 가상 라우터 인터페이스에서만 지원됩니다. 사용자 정의 가상 라우터에 속한 인터페이스에서는 설정할 수 없습니다. 이 예에서는 사이트 간 VPN을 통해 사용자 정의 가상 라우터 내에서 호스팅되는 네트워크와의 연결을 보호할 수 있는 절차를 제공합니다. 또한 이러한 사용자 정의 가상 라우팅 네트워크를 포함하도록 사이트 간 VPN 연결을 업데이트해야 합니다.

지사 네트워크와 회사 본사 네트워크 사이에 사이트 간 VPN이 설정된 시나리오를 살펴보겠습니다. 가상 라우터가 있는 지사 사무실의 FTD입니다. 이 경우, 사이트 간 VPN은 172.16.3.1의 지사 외부 인터페이스에 정의됩니다. 내부 인터페이스는 전역 가상 라우터의 일부이므로 이 VPN에는 추가 설정 없이 내부 네트워크 192.168.2.0/24가 포함됩니다. 그러나 VR1 가상 라우터의 일부인 192.168.1.0/24 네트워크에 사이트 간 VPN 서비스를 제공하려면 전역 및 VR1에 정적 경로를 설정하여 경로를 유출하고 VR1 네트워크를 사이트 간 VPN 설정에 추가해야 합니다.



시작하기 전에

이 예에서는 192.168.2.0/24 로컬 네트워크와 172.16.20.0/24 외부 네트워트 간의 사이트 간 VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

프로시저

단계 **1** 전역 가상 라우터에서 사용자 정의 VR1으로의 경로 유출을 설정합니다.

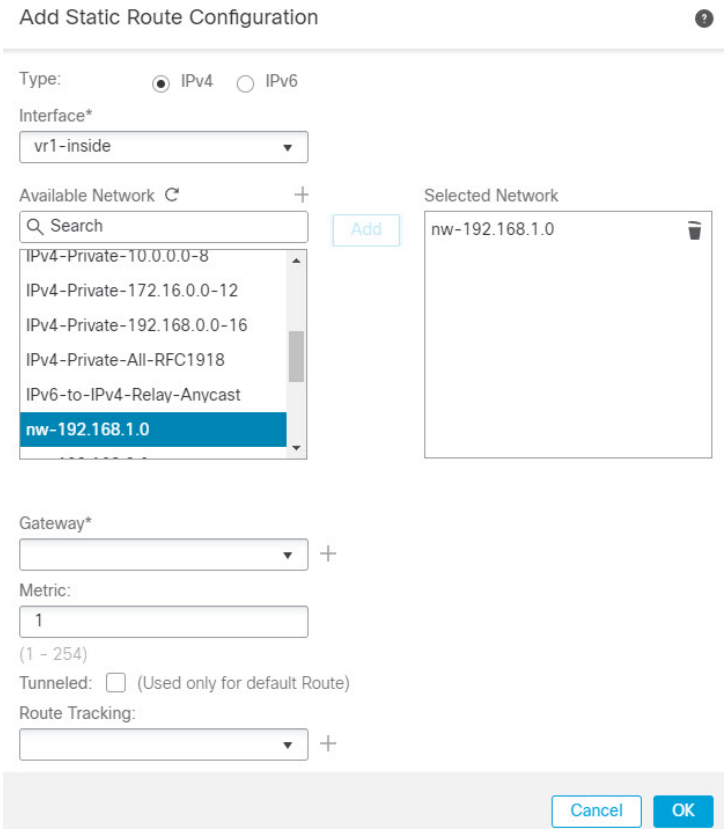
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 클릭합니다. 기본적으로 Global routing properties(전역 라우팅 속성) 페이지가 나타납니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- 인터페이스 - VR1 내부 인터페이스를 선택합니다.
- 네트워크 - VR1 가상 라우터 네트워크 개체를 선택합니다. **Add Object(**개체 추가**)** 옵션을 사용하여 생성할 수 있습니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.



이 경로 유출은 사이트 간 VPN의 외부(원격) 끝에서 보호하는 엔드포인트를 VR1 가상 라우터의 192.168.1.0/24 네트워크에 액세스하는 데 사용할 수 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 설정합니다.

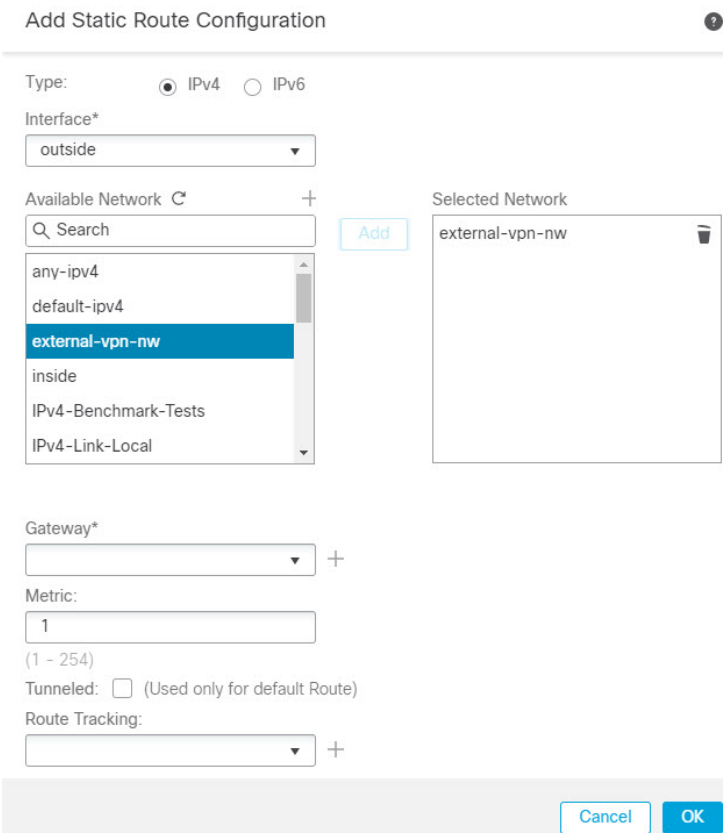
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 클릭하고 드롭다운에서 VR1을 선택합니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- 네트워크 - 전역 가상 라우터 네트워크 개체를 선택합니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.



이 정적 경로를 사용하면 192.168.1.0/24 네트워크(VR1)의 엔드포인트에서 사이트 간 VPN 터널을 통과하는 연결을 시작할 수 있습니다. 이 예에서는 원격 엔드포인트에서 172.16.20.0/24 네트워크를 보호하고 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

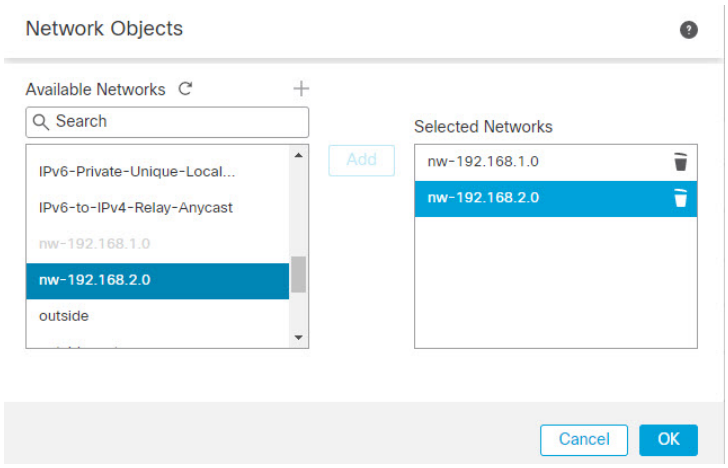
단계 **3** 사이트 간 VPN 연결 프로파일에 192.168.1.0/24 네트워크를 추가합니다.

a) **Devices(**디바이스**)** > **VPN** > **Site To Site(**사이트 간**)**를 선택하고 VPN 토폴로지를 편집합니다.

b) **Endpoints(**엔드포인트**)**에서 노드 A 엔드포인트를 편집합니다.

c) **Edit Endpoint(**엔드포인트 편집**)**의 **Protected Networks(**보호되는 네트워크**)** 필드에서 **Add New Network Object(**새 네트워크 개체 추가**)**를 클릭합니다.

d) 192.168.1.0 네트워크로 VR1 네트워크 개체를 추가합니다.

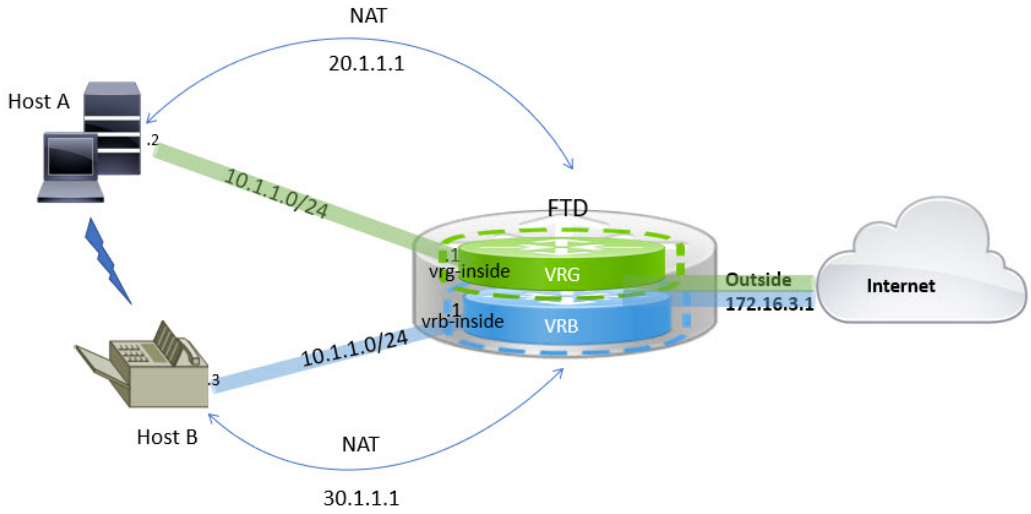


e) **OK(**확인**)**를 클릭하여 설정을 저장합니다.

가상 라우팅에서 두 개의 중복되는 네트워크 호스트 간에 트래픽을 라우팅하는 방법

동일한 네트워크 주소를 가진 가상 라우터에서 호스트를 구성할 수 있습니다. 호스트가 통신하려는 경우 NAT를 2회 구성할 수 있습니다. 이 예에서는 중복 네트워크 호스트를 관리하기 위해 NAT 규칙을 구성하는 절차를 제공합니다.

다음 예에서 호스트 A와 호스트 B의 두 호스트는 서로 다른 가상 라우터에 속합니다. VRG(인터페이스 vrg-inside), VRB(인터페이스 vrb-inside)는 각각 동일한 서브넷 10.1.1.0/24입니다. 두 호스트가 모두 통신할 수 있도록 VRG-Host 인터페이스 개체는 매핑된 NAT 주소 20.1.1.1을 사용하고, VRB-Host 인터페이스 개체는 매핑된 NAT 주소 30.1.1.1을 사용하는 NAT 정책을 생성합니다. 따라서 호스트 A는 30.1.1.1을 사용하여 호스트 B와 통신합니다. 호스트 B는 20.1.1.1을 사용하여 호스트 A에 연결합니다.



시작하기 전에

이 예시에서는 다음 항목을 이미 구성한 것으로 가정합니다.

- vrg-inside 및 vrb-inside 인터페이스는 가상 라우터(각각 VRG 및 VRB) 및 동일한 서브넷 주소(예: 10.1.1.0/24)로 구성된 vrg-inside 및 vrb-inside 인터페이스와 연결됩니다.
- 인터페이스 영역 VRG-Inf, VRB-Inf는 각각 vrg-inside 및 vrb-inside 인터페이스로 생성됩니다.
- vRG-inside를 기본 게이트웨이로 사용하는 VRG의 호스트 A. vrb-inside를 기본 게이트웨이로 사용하는 VRB의 호스트 B

프로시저

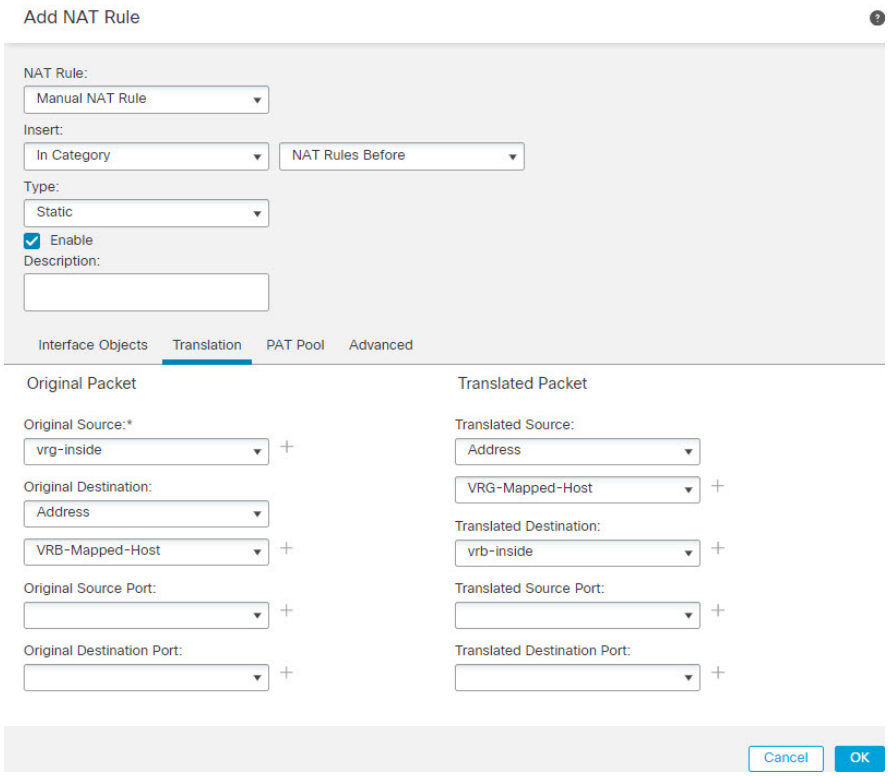
단계 **1** 호스트 A에서 호스트 B로의 트래픽을 처리할 NAT 규칙을 생성합니다. **Devices(**디바이스**)** > **NAT**를 선택합니다.

단계 **2** **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.

단계 **3** NAT 정책 이름을 입력하고 FTD 디바이스를 선택합니다. **Save(**저장**)**를 클릭합니다.

단계 **4** NAT 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 다음을 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- 유형 - Static(고정)을 선택합니다.
- **Insert (**삽입**)** - NAT 규칙이 있는 경우 Above(위에)를 선택합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 VRG-Inf object(VRG-Inf 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭하고(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성) VRB-Inf object(VRB-Inf 개체)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- **Translation(**변환**)**에서 다음을 선택합니다.
  - **Original Source(**원본 소스**)**: vrg-inside를 선택합니다.
  - **Original Destination(**원본 대상**)**에서 **Add(**추가**)**를 클릭하고 30.1.1.1로 개체 VRB-Mapped-Host를 정의합니다. VRB-Mapped-Host를 선택합니다.
  - **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 20.1.1.1로 개체 VRG-Mapped-Host를 정의합니다. VRG-Mapped-Host를 선택합니다.
  - **Translated Destination(**변환된 대상**)**에서 다음 그림과 같이 vrb-inside를 선택합니다.



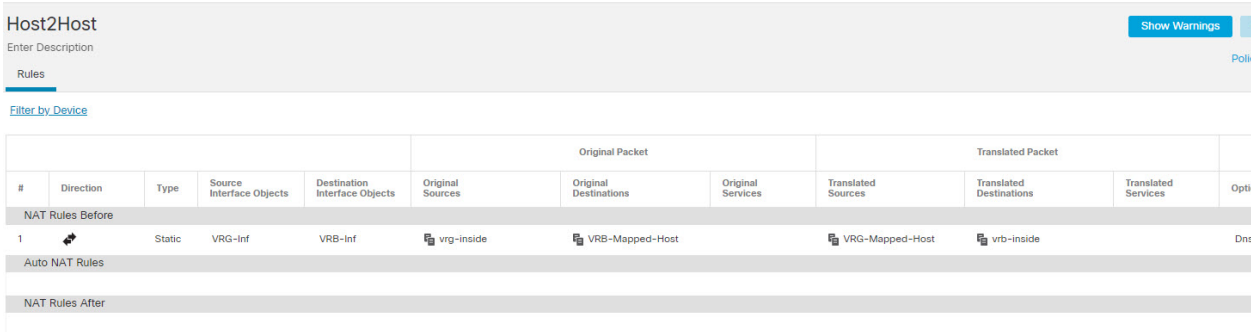
FTD 디바이스에서 **show nat detail** 명령을 실행하면 다음과 유사한 출력이 표시됩니다.

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
 vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

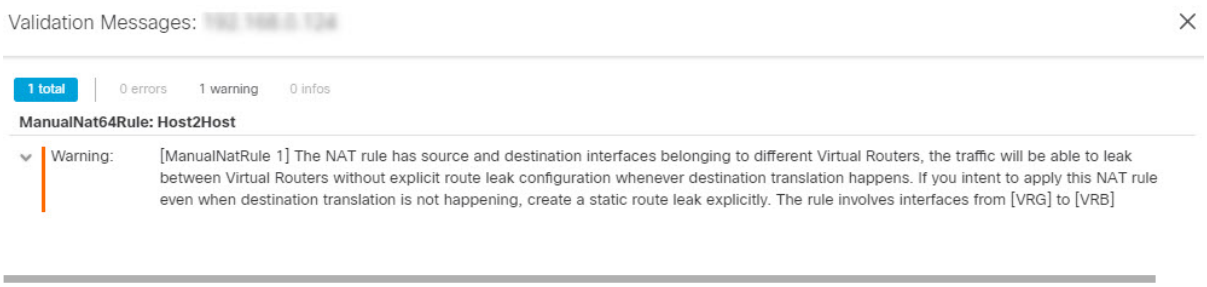
단계 **5** **Ok(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

NAT 규칙은 다음과 같습니다.



구성을 구축할 때 경고 메시지가 나타납니다.

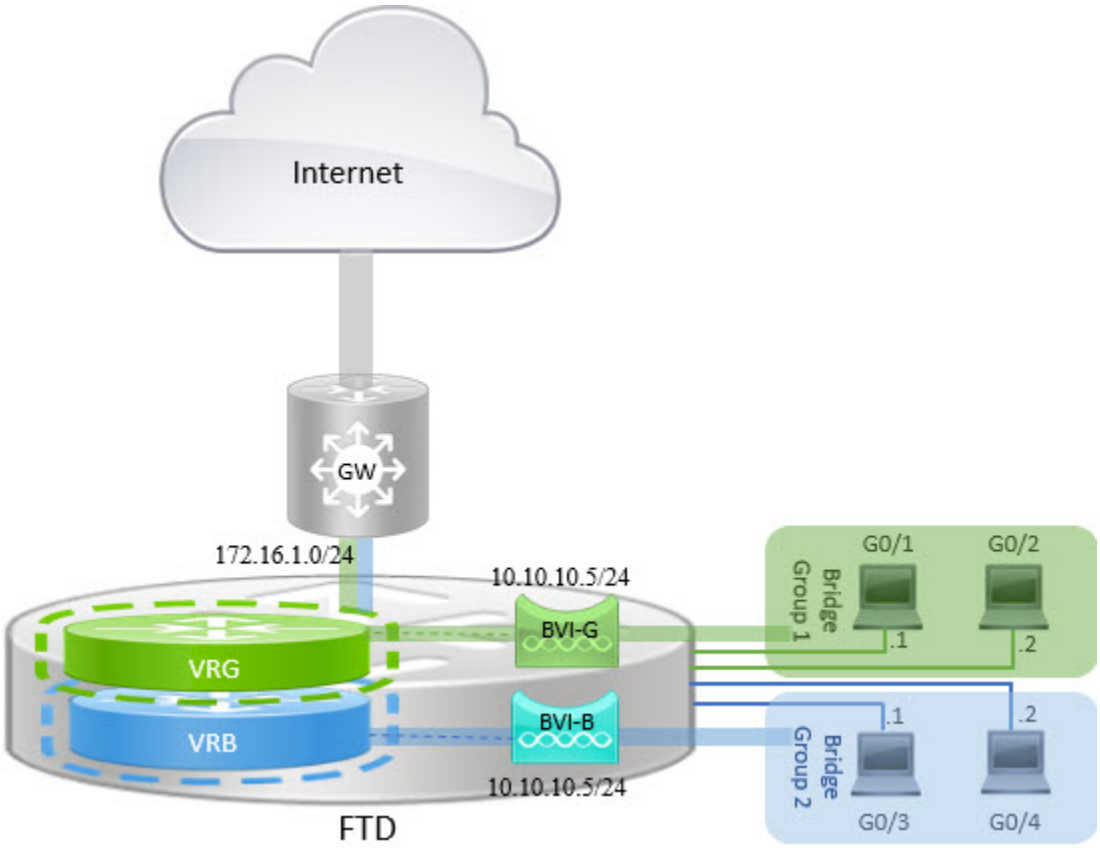


BVI 인터페이스를 사용하여 라우팅 방화벽 모드에서 중복 세그먼트를 관리하는 방법

여러 중복 네트워크 간에 투명하게 단일 FTD를 구축하거나 동일한 네트워크의 호스트 간에 방화벽을 구축할 수 있습니다. 이 구축을 수행하려면 가상 라우터별로 BVI를 설정합니다. 가상 라우터에서 BVI를 설정하는 절차는 여기에 설명되어 있습니다.

BVI는 일반적인 라우팅 인터페이스처럼 작동하는 라우터 내의 가상 인터페이스입니다. 브리징은 지원하지 않지만, 라우터 내에서 라우팅된 인터페이스와 비교 가능한 브리지 그룹을 나타냅니다. 이러한 브리지된 인터페이스를 오가는 모든 패킷은 BVI 인터페이스를 통과합니다. BVI의 인터페이스 번호는 가상 인터페이스가 나타내는 브리지 그룹의 번호입니다.

다음 예에서 BVI-G는 VRG에 설정되고, 브리지 그룹 1은 인터페이스 G0/1 및 G0/2에 대한 라우팅 인터페이스입니다. 마찬가지로, BVI-B는 VRB에서 설정되며, 브리지 그룹 2는 인터페이스 G0/3 및 G0/4의 라우팅 인터페이스입니다. 두 BVI 모두 동일한 IP 서브넷 주소(예: 10.10.10.5/24)를 가집니다. 가상 라우터 때문에 네트워크가 공유 리소스에서 격리됩니다.



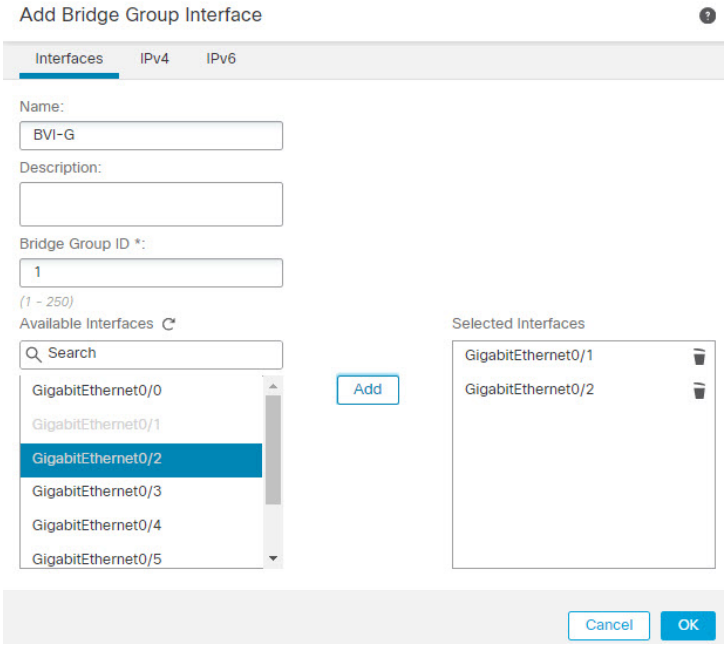
프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다. 필요한 디바이스를 편집합니다.

단계 **2** **Interfaces(**인터페이스**)**에서 **Add Interfaces(**인터페이스 추가**)** > **Bridge Group Interface(**브리지 그룹 인터페이스**)**를 선택합니다.

a) 다음 BVI-G 세부 사항을 입력합니다.

- **Name(**이름**)** - 이 예에서는 BVI-G입니다.
- **Bridge Group ID(**브리지 그룹 **ID)** - 이 예에서는 1입니다.
- **Available Interface(**사용 가능한 인터페이스**)** - 인터페이스를 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)** - 10.10.10.5/24를 입력합니다.

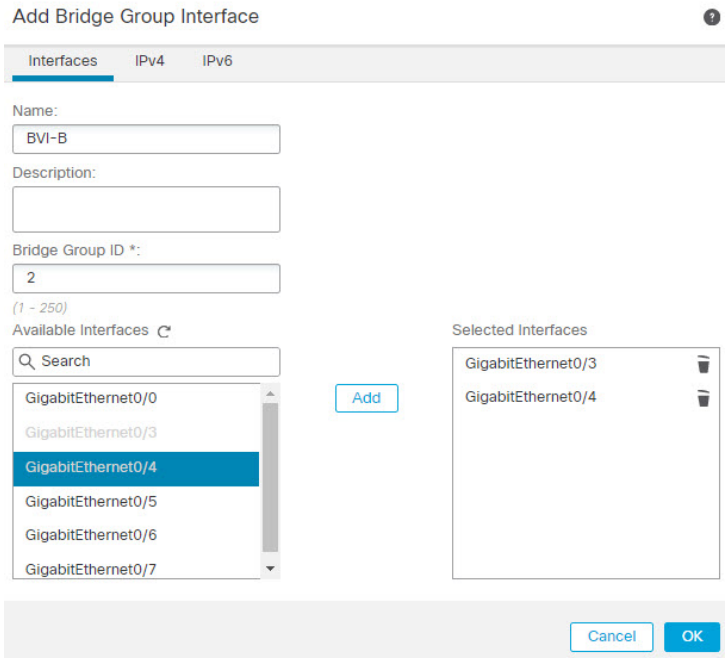


b) **Ok(**확인**)**를 클릭합니다.

c) **Save(**저장**)**를 클릭합니다.

a) 다음 BVI-B 세부 정보를 입력합니다.

- **Name(**이름**)** - 이 예에서는 BVI-B입니다.
- **Bridge Group ID(**브리지 그룹 **ID)** - 이 예에서는 2입니다.
- **Available Interface(**사용 가능한 인터페이스**)** - 하위 인터페이스를 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)** - 시스템에서 두 인터페이스의 IP 주소 중복을 허용하지 않으므로 이 필드를 비워 두십시오. 브리지 그룹을 다시 방문하여 가상 라우터 아래에 정렬한 후 동일한 IP 주소를 제공할 수 있습니다.



b) **Ok(**확인**)**를 클릭합니다.

c) **Save(**저장**)**를 클릭합니다.

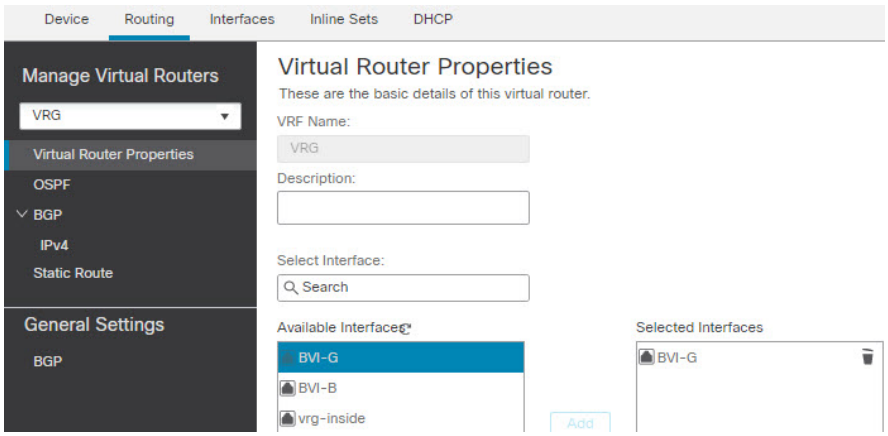
단계 **3** VRG라고 하는 가상 라우터를 생성하고 네트워크로 BVI-G를 선택합니다.

a) **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택합니다.

b) 디바이스를 편집하고 **Routing(**라우팅**) > Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다.

c) **Add Virtual Router(**가상 라우터 추가**)**를 클릭합니다. 가상 라우터의 이름을 입력하고 **Ok(**확인**)**를 클릭합니다.

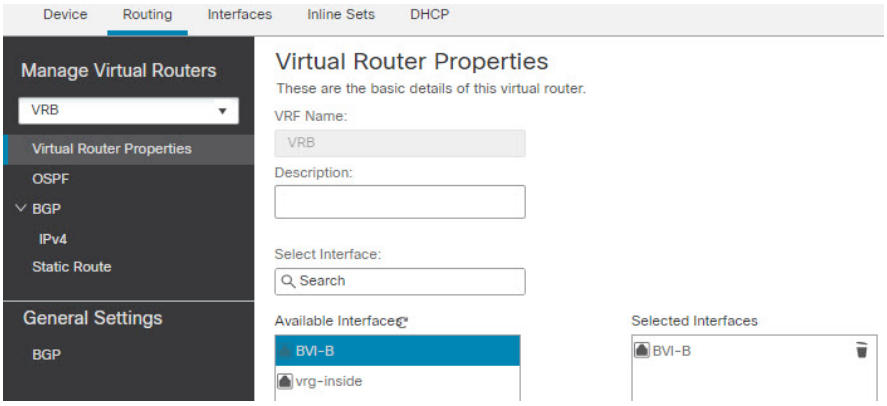
d) **Virtual Routing Properties(**가상 라우터 속성**)**에서 **BVI-G**를 선택하고 **Add(**추가**)**를 클릭합니다.



e) **Save(**저장**)**를 클릭합니다.

단계 **4** 가상 라우터를 생성하고(VRB라고 함) 네트워크로 BVI-B를 선택합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
b) 디바이스를 편집하고 **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다.
c) **Add Virtual Router(**가상 라우터 추가**)**를 클릭합니다. 가상 라우터의 이름을 입력하고 **Ok(**확인**)**를 클릭합니다.
d) **Virtual Routing Properties(**가상 라우터 속성**)**에서 **BVI-B**를 선택하고 **Add(**추가**)**를 클릭합니다.



e) **Save(**저장**)**를 클릭합니다.

단계 **5** BVI-B 설정을 다시 살펴봅니다.

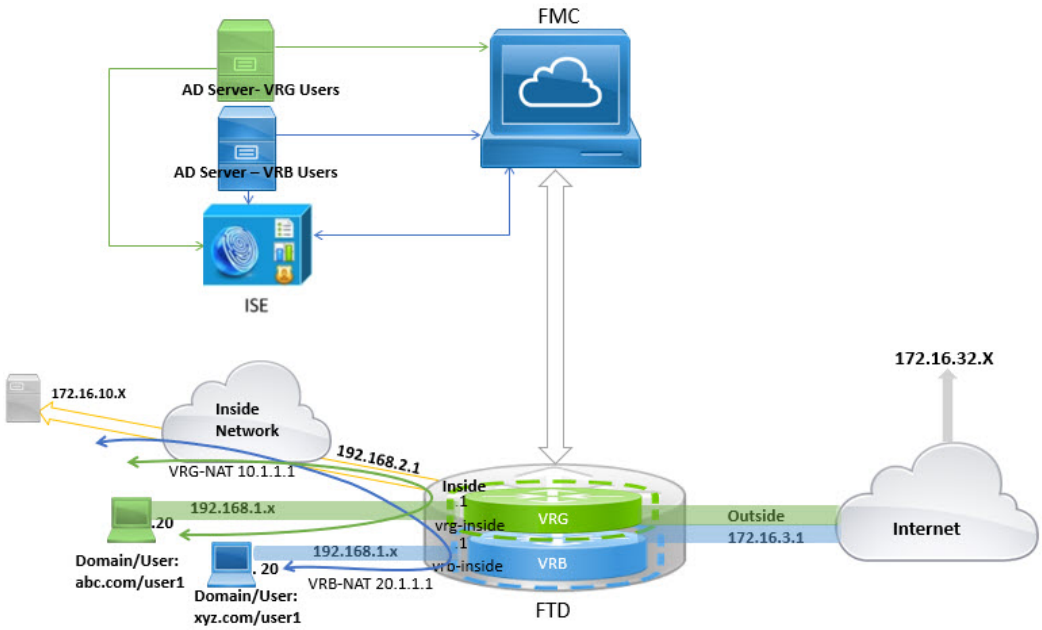
a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.
b) BVI-B 인터페이스에 대해 **Edit(**편집**)**을 클릭합니다. IP 주소를 10.10.10.5/24로 지정합니다. 인터페이스가 두 개의 서로 다른 가상 라우터에 별도로 할당되므로 이제 시스템에서 동일한 BVI-G IP 주소로 설정할 수 있습니다.
c) **Ok(**확인**)**를 클릭합니다.
d) **Save(**저장**)**를 클릭합니다.

BVI 간 통신을 활성화하려면 외부 라우터를 기본 게이트웨이로 사용합니다. 이 예와 같이 중복되는 BVI 시나리오에서는 NAT 외부 라우터를 게이트웨이로 두 번 사용하여 BVI 간 트래픽을 설정합니다. 브리지 그룹 멤버에 대해 NAT를 구성할 때는 멤버 인터페이스를 지정합니다. BVI(브리지 그룹 인터페이스) 자체에 대해서는 NAT를 구성할 수 없습니다. 브리지 그룹 멤버 인터페이스 간에 NAT를 수행할 때는 실제 및 매핑된 주소를 지정해야 합니다. 인터페이스로 "임의"를 지정할 수는 없습니다.

중복되는 네트워크로 사용자 인증을 구성하는 방법

가상 라우팅에서는 중복 IP 및 중복 사용자로 여러 가상 라우터를 구성할 수 있습니다. 이 예에서 VRG 및 VRB는 IP가 192.168.1.1/24로 중복되는 가상 라우터입니다. 서로 다른 두 도메인의 사용자가 네트워크 IP 192.168.1.20과 중복됩니다. VRG 및 VRB 사용자가 공유 서버 172.16.10.X에 액세스하는 경우 전역 가상 라우터로 라우트를 유출합니다. 소스 NAT를 사용하여 중복 IP를 처리합니다. VRG 및 VRB 사용자의 액세스를 제어하려면 FMC에서 사용자 인증을 설정해야 합니다. FMC는 영역, 활성 디렉토리, ID 소스, ID 규칙 및 정책을 사용하여 사용자 ID를 인증합니다. FTD는 사용자 인증에서 직접 역할

을 수행하지 않으므로 사용자 액세스는 액세스 제어 정책을 통해서만 관리됩니다. 중복되는 사용자의 트래픽을 제어하려면 ID 정책 및 규칙을 사용하여 액세스 제어 정책을 생성합니다.



시작하기 전에

이 예시에서는 사용자에게 다음 항목이 이미 있는 것으로 가정합니다.

- VRG 및 VRB 사용자용 AD 서버 2개
- AD 서버가 2개가 추가된 ISE.

프로시저

단계 **1** VRG에 대해 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VRG에 할당할 인터페이스를 편집합니다.

- **Name(**이름**)** - 이 예에서는 VRG-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)**-192.168.1.1/24를 입력합니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** VRB에 대해 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VRB에 할당할 인터페이스를 편집합니다.

- **Name(**이름**)** - 이 예에서는 VRB-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 공백으로 둡니다. 아직 사용자 정의 가상 라우터를 생성하지 않았으므로 동일한 IP 주소(10.30.0.1/24)의 인터페이스를 구성하는 것을 시스템에서 허용하지 않습니다.

c) **Ok(**확인**)**를 클릭합니다.

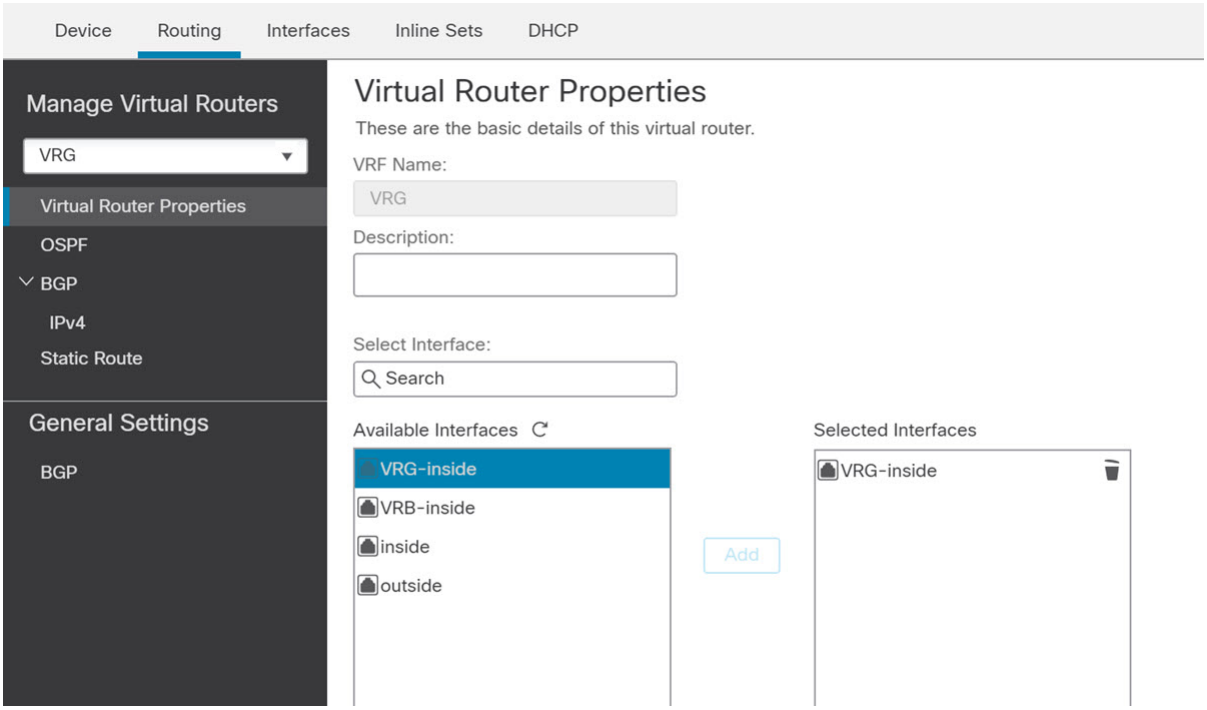
d) **Save(**저장**)**를 클릭합니다.

단계 **3** VRG 사용자가 공통 서버 172.16.10.1에 액세스할 수 있도록 전역 라우터의 내부 인터페이스에 대한 VRG 및 고정 기본 경로 유출을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VRG를 생성합니다.

c) VRG의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 VRG-inside를 할당하고 저장합니다.



d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 내부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 라우트를 유출할 경우에는 게이트웨이를 선택하지 마십시오.

f) **Ok(**확인**)**를 클릭합니다.

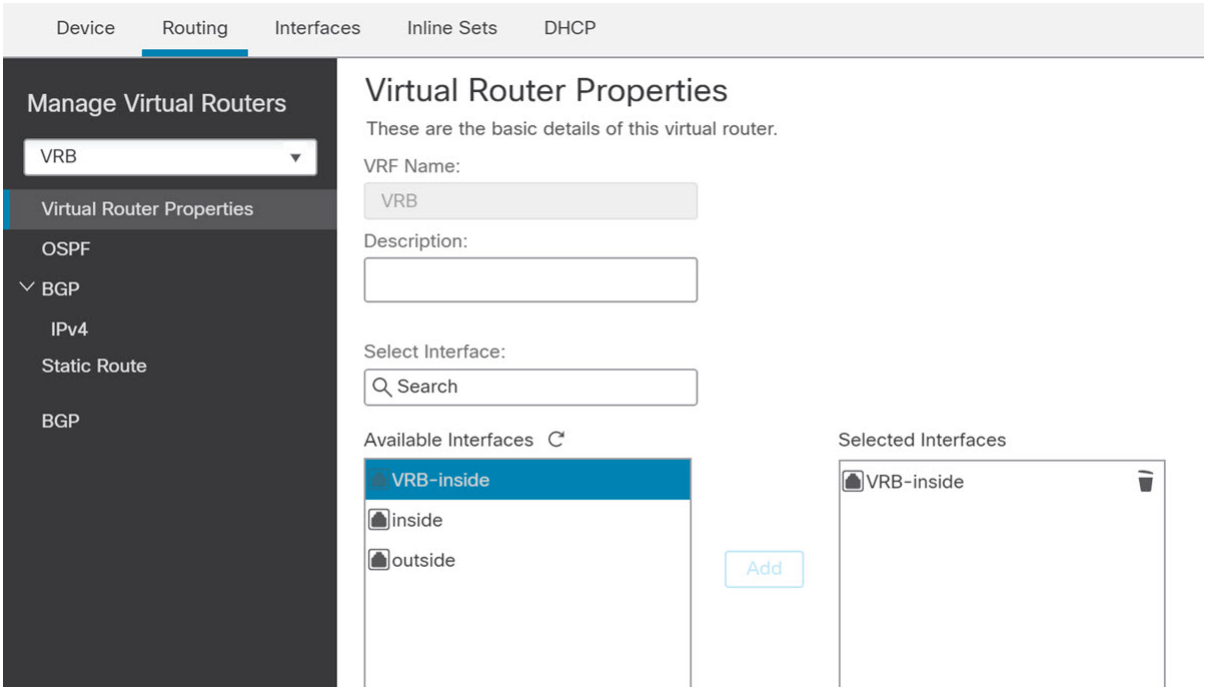
g) **Save(**저장**)**를 클릭합니다.

단계 **4** VRB 사용자가 공유 서버 172.16.10.x에 액세스할 수 있도록 전역 라우터의 내부 인터페이스에 대한 고정 기본 경로 유출을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VRB를 생성합니다.

c) VRB의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 VRB-inside를 할당하고 저장합니다.



d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 내부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다.

- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 라우트를 유출할 경우에는 게이트웨이를 선택하지 마십시오.

f) **Ok(**확인**)**를 클릭합니다.
g) **Save(**저장**)**를 클릭합니다.

단계 **5** VRB-inside 인터페이스 구성을 다시 확인합니다:

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.
b) VRB-inside 인터페이스에 대해 **Edit(**편집**)**를 클릭합니다. IP 주소를 192.168.1.1/24로 지정합니다. 이제 시스템에서 VRG-inside의 동일한 IP 주소로 구성할 수 있습니다. 왜냐하면 인터페이스는 두 개의 서로 다른 가상 라우터에 별도로 할당되기 때문입니다.
c) **Ok(**확인**)**를 클릭합니다.
d) **Save(**저장**)**를 클릭합니다.

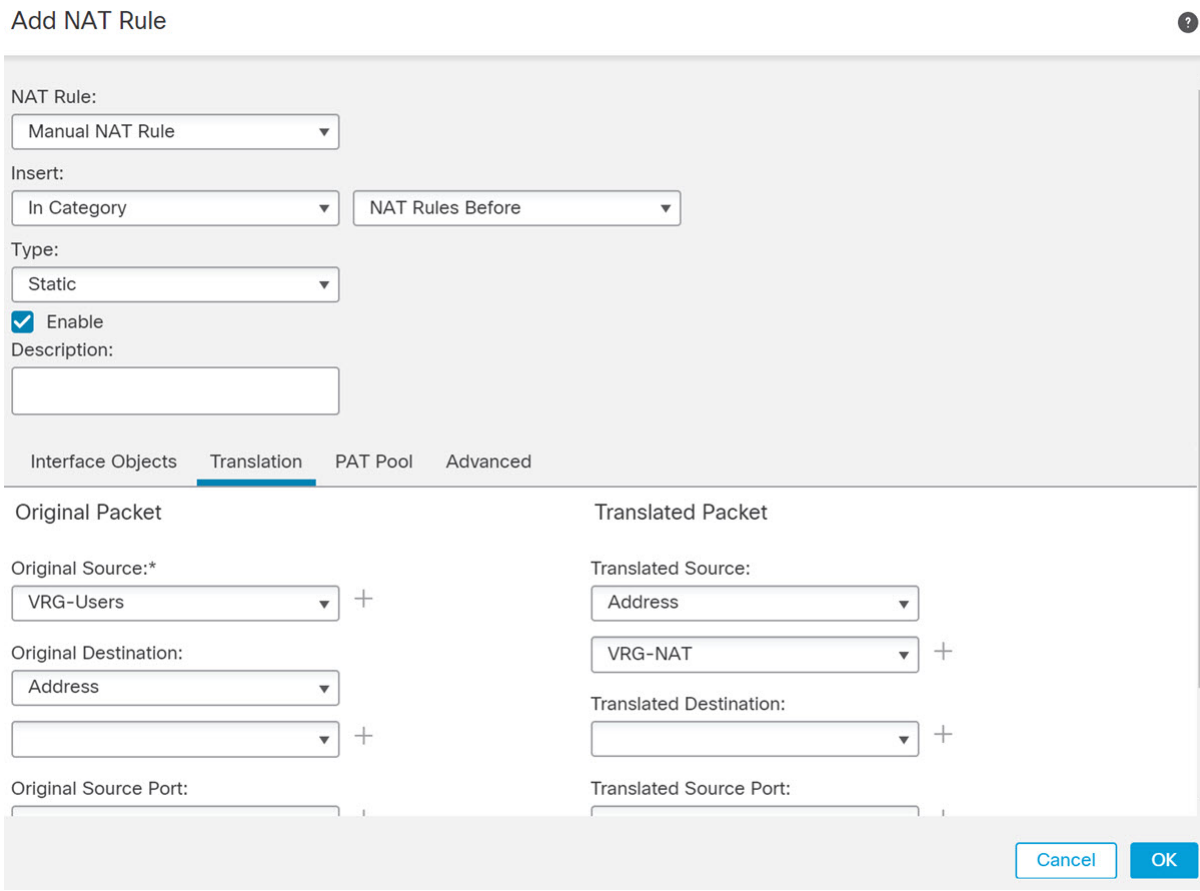
단계 **6** 소스 개체 VRG 및 VRB에 대한 NAT 규칙을 추가합니다. **Devices(**디바이스**)** > **NAT**를 클릭합니다.

단계 **7** **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.

단계 **8** NAT 정책 이름을 입력하고 FTD 디바이스를 선택합니다. **Save(**저장**)**를 클릭합니다.

단계 **9** NAT 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 VRG에 대해 다음 소스 NAT를 정의합니다.

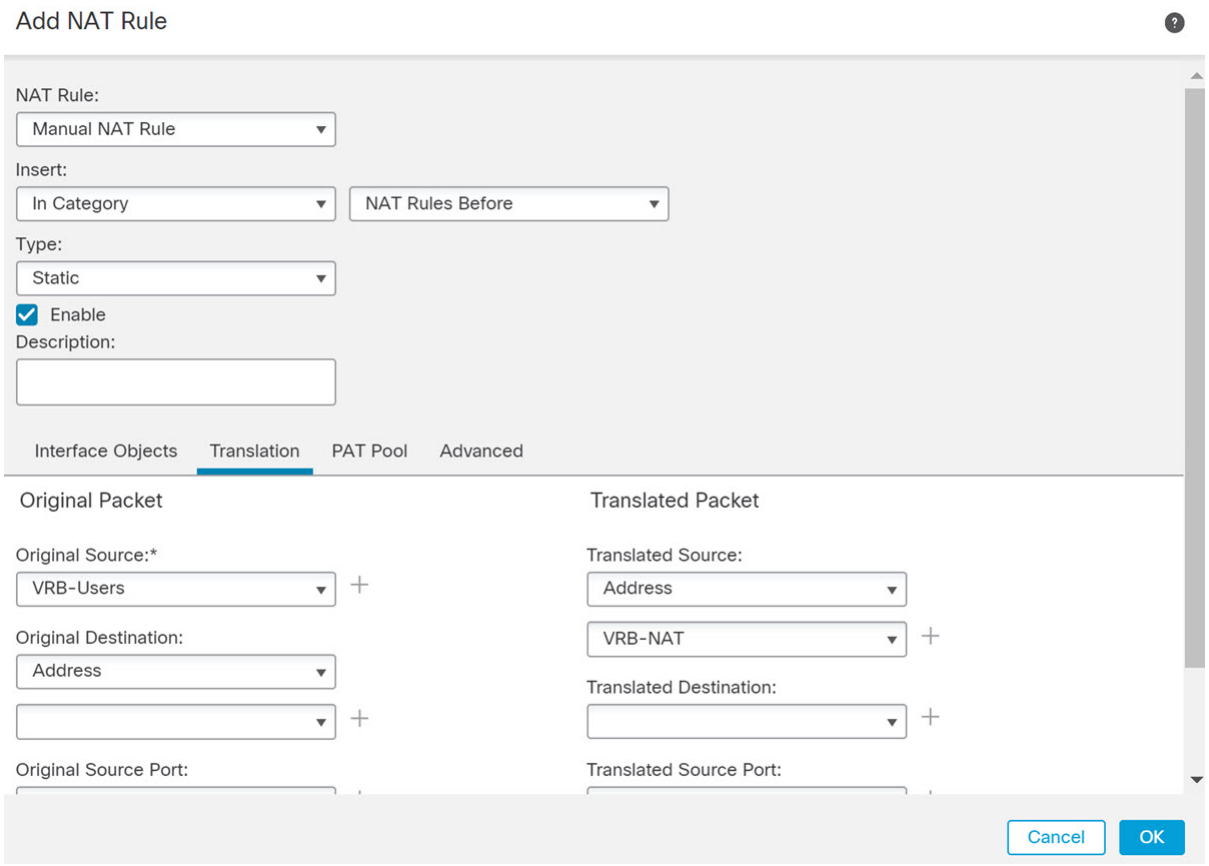
- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- 유형 - Static(고정)을 선택합니다.
- **Insert (**삽입**)** - NAT 규칙이 있는 경우 Above(위에)를 선택합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 VRG-Inside object(VRG-Inf 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭하고(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성) Global-Inside object(VRB-Inf 개체)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- **Translation(**변환**)**에서 다음을 선택합니다.
  - **Original Source(**원본 소스**)**에서 VRG-Users를 선택합니다.
  - **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 10.1.1.1로 개체 VRG-NAT를 정의합니다. 다음 그림과 같이 VRG-NAT를 선택합니다.



단계 **10** **Ok(**확인**)**를 클릭합니다.

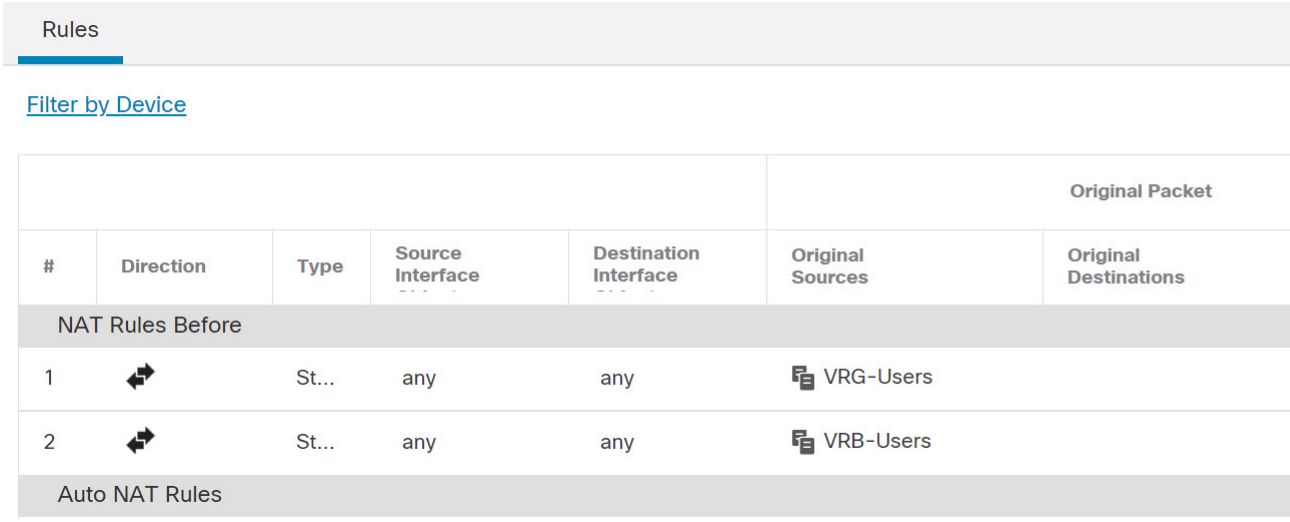
단계 **11** NAT 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 VRB에 대해 다음 소스 NAT를 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- 유형 - Static(고정)을 선택합니다.
- **Insert (**삽입**)** - NAT 규칙이 있는 경우 Above(위에)를 선택합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 VRB-Inside object(VRB-Inside 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭하고(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성) Global-Inside object(VRB-Inf 개체)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- **Translation(**변환**)**에서 다음을 선택합니다.
  - **Original Source(**원본 소스**)**에서 VRB-Users를 선택합니다.
  - **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 20.1.1.1로 개체 VRB-NAT를 정의합니다. 다음 그림과 같이 VRB-NAT를 선택합니다.



단계 **12** **Save(**저장**)**를 클릭합니다.

NAT 규칙은 다음과 같습니다.



단계 **13** 각 VRG 및 VRB 사용자에 대해 FMC에 고유한 AD 서버 2개를 추가합니다. **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**을 선택합니다.

단계 **14** **New Realm(**새 영역**)**을 클릭하고 필드를 완료합니다. 필드에 대한 자세한 내용은 영역 필드, 2467 페이지의 내용을 참조하십시오.

단계 **15** VRG 및 VRB 사용자의 액세스를 제어하려면 활성 디렉토리 2개를 정의합니다.를 참조하십시오.영역 디렉터리 설정, 2475 페이지의 내용을 참조하십시오.

단계 **16** FMC에 ISE 추가—**System(**시스템**)** > **Integration(**통합**)** > **Identity Sources(ID** 소스**)**를 선택합니다.

단계 **17** **Identity Services Engine(ID** 서비스 엔진**)**을 클릭하고 필드를 완료합니다. 필드에 대한 자세한 내용은 영역을 사용해 사용자 제어에 대한 ISE/ISE-PIC를 설정하는 방법, 2491 페이지의 내용을 참조하십시오.

단계 **18** ID 정책 및 규칙을 생성한 다음 VRG 및 VRB에서 중복되는 사용자의 액세스를 제어하기 위한 액세스 제어 정책을 정의합니다.

Firepower Threat Defense의 가상 라우터 기록

기능	버전	세부 사항
Firepower Threat Defense의 가상 라우터	6.6	Firepower Threat Defense의 가상 라우터가 도입되었습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** 페이지에서 가상 라우터를 생성하고 Threat Defense 인터페이스를 가상 라우터에 할당할 수 있습니다. 지원되는 플랫폼: Firepower Threat Defense
가상 라우터 대량 제거	6.7	Firepower Threat Defense에서 한 번에 여러 가상 라우터를 제거할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)** 페이지.

38 장

Firepower Threat Defense 정적 및 기본 경로

이 장에서는 FTD에서 고정 경로와 기본 경로를 구성하는 방법을 설명합니다.

- 고정 경로 및 기본 경로 소개, 1035 페이지
- 정적 경로 요구 사항 및 사전 요건, 1037 페이지
- 고정 경로 및 기본 경로를 위한 지침, 1038 페이지
- 고정 경로 추가, 1038 페이지

고정 경로 및 기본 경로 소개

비연결 호스트 또는 네트워크에 트래픽을 라우팅하려면 정적 또는 동적 라우팅을 사용하여 해당 호스트 또는 네트워크로 가는 경로를 정의해야 합니다. 일반적으로 최소한 하나의 고정 경로를 구성해야 합니다. 다른 방법으로는 기본 네트워크 게이트웨이(대개는 다음 홉 라우터)에 라우팅되지 않는 모든 트래픽을 위한 기본 경로입니다.

기본 라우터

가장 간단한 옵션은 트래픽을 라우팅해주는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 정적 경로를 컨피그레이션하는 것입니다. 기본 고정 경로는 FTD 디바이스가 학습 경로나 고정 경로를 가지고 있지 않은 모든 IP 패킷을 보낼 게이트웨이 IP 주소를 식별합니다. 기본 정적 경로는 대상 IP 주소가 0.0.0.0/0(IPv4) 또는 ::/0(IPv6)인 정적 경로일 뿐입니다.

항상 기본 경로를 정의해야 합니다.

고정 경로

다음과 같은 경우, 고정 경로를 사용할 수 있습니다.

- 네트워크에서 지원하지 않는 라우터 검색 프로토콜을 사용합니다.
- 네트워크 규모가 작고 고정 경로를 쉽게 관리할 수 있습니다.
- 트래픽이나 CPU 오버헤드를 라우팅 프로토콜과 연결하지 않는 것이 좋습니다.

- 기본 경로만으로 충분하지 않을 때도 있습니다. 기본 게이트웨이가 목적지 네트워크에 도달할 수 없는 경우가 있기 때문에 보다 구체적인 고정 경로도 구성해야 합니다. 예를 들어 기본 게이트웨이가 밖에 있는 경우 기본 경로는 FTD 디바이스에 직접 연결되지 않은 내부 네트워크로 트래픽을 안내할 수 없습니다.
- 동적 라우팅 프로토콜을 지원하지 않는 기능을 사용 중입니다.
- 가상 라우터는 고정 경로를 사용하여 경로 누수를 생성합니다. 경로 누수는 가상 라우터의 인터페이스에서 다른 가상 라우터의 다른 인터페이스로 향하는 트래픽 흐름을 활성화합니다. 자세한 내용은 인터커넥트 가상 라우터, 990 페이지를 참고하십시오.

원치 않는 트래픽을 지우기 위한 null0 인터페이스로의 경로

액세스 규칙을 통해 패킷 헤더의 정보에 따라 패킷을 필터링할 수 있습니다. null0 인터페이스에 대한 고정 경로는 액세스 규칙을 보완합니다. null0 경로를 사용하여 원치 않는 트래픽을 전달하여 트래픽이 삭제되도록 할 수 있습니다.

고정 null0 경로는 성능을 향상시킵니다. 또한 라우팅 루프를 방지하는 데 고정 null0 경로를 사용할 수 있습니다. BGP는 Remotely Triggered Black Hole 라우팅을 위해 고정 null0 경로를 활용할 수 있습니다.

경로 우선 순위

- 특정 대상을 식별하는 경로가 기본 경로보다 우선합니다.
- 동일한 목적지에 대한 여러 경로(고정 또는 동적)가 있을 경우 경로의 관리 영역에 따라 우선 순위가 결정됩니다. 고정 경로는 1로 설정되므로 대개 우선 순위가 높은 경로입니다.
- 동일한 관리 거리에서 동일한 대상에 대해 여러 고정 경로가 있는 경우, ECMP(Equal-Cost Multi-Path) 라우팅, 984 페이지를 참조하십시오.
- 터널링 옵션을 사용하여 터널로부터 생성된 트래픽의 경우 이 경로는 구성되었거나 학습된 다른 기본 경로를 무시합니다.

투명 방화벽 모드 및 브리지 그룹 경로

Firepower Threat Defense 디바이스에서 발생하고 브리지 그룹 멤버 인터페이스를 거쳐 직접 연결되지 않은 네트워크로 가는 트래픽의 경우, 기본 경로 또는 고정 경로를 구성하여 Firepower Threat Defense 디바이스에서 어떤 브리지 그룹 멤버 인터페이스로 트래픽을 보낼지 알 수 있게 해야 합니다. Firepower Threat Defense 디바이스에서 발생하는 트래픽은 syslog 서버 또는 SNMP 서버로의 통신을 포함할 수 있습니다. 단일 기본 경로를 통해 모두 도달할 수 없는 서버가 있다면 고정 경로를 구성해야 합니다. 투명 모드에서는 BVI를 게이트웨이 인터페이스로 지정할 수 없습니다. 멤버 인터페이스만 사용할 수 있습니다. 라우팅 모드의 브리지 그룹에 대해서는 고정 경로에서 BVI를 지정해야 합니다. 멤버 인터페이스는 지정할 수 없습니다. 자세한 내용은 MAC 주소 대 경로 조회 비교, 717 페이지를 참조하십시오.

고정 경로 추적

고정 경로의 문제 중 하나는 경로가 정상인지 다운되었는지 확인할 수 있는 내재적인 메커니즘이 없다는 것입니다. 다음 홉 게이트웨이가 사용할 수 없게 되어도 라우팅 테이블에 남습니다. 고정 경로는 Firepower Threat Defense 디바이스의 연결된 인터페이스가 다운되는 경우에만 라우팅 테이블에서 제거됩니다.

고정 경로 추적 기능은 고정 경로의 가용성을 추적하고 기본 경로가 실패할 경우 보조 경로를 설치하는 수단을 제공합니다. 예를 들어 기본 ISP를 사용할 수 없는 경우에 대비하여 ISP 게이트웨이로의 기본 경로와 보조 ISP로의 보조 기본 경로를 정의할 수 있습니다.

Firepower Threat Defense 디바이스에서는 Firepower Threat Defense 디바이스에서 ICMP 에코 요청을 통해 모니터링하는 목적지 네트워크의 모니터링 대상 호스트와 고정 경로를 연결하는 방법으로 고정 경로 추적을 구현합니다. 에코 응답이 지정된 시간 동안 수신되지 않으면 호스트는 다운된 것으로 간주되며 연결된 경로가 라우팅 테이블에서 제거됩니다. 메트릭이 높은 비추적 백업 경로를 제거된 경로 대신 사용합니다.

모니터링 대상을 선택할 때, ICMP 에코 요청에 응답할 수 있는지 확인해야 합니다. 대상은 사용자가 선택하는 아무 네트워크 객체나 될 수 있지만 다음을 사용할 것을 고려해야 합니다.

- ISP 게이트웨이(이중 ISP 지원) 주소
- 다음 홉 게이트웨이 주소(게이트웨이의 가용성이 우려되는 경우)
- syslog 서버와 같이 Firepower Threat Defense 디바이스가 통신해야 하는 대상 네트워크에 있는 서버
- 목적지 네트워크에 있는 지속적인 네트워크 객체

참고 야간에 꺼질 수 있는 PC는 좋은 선택이 아닙니다.

DHCP 나 PPPoE를 통해 얻은 고정으로 정의된 경로나 기본 경로를 위해 고정 경로 추적을 구성할 수 있습니다. 경로 추적이 구성된 여러 인터페이스에서만 PPPoE 클라이언트를 활성화할 수 있습니다.

정적 경로 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

고정 경로 및 기본 경로를 위한 지침

방화벽 모드 및 브리지 그룹

- 투명 모드의 경우, 정적 경로에서는 브리지 그룹 멤버 인터페이스를 게이트웨이로 사용해야 하며 BVI는 지정할 수 없습니다.
- 라우티드 모드에서는 BVI를 게이트웨이로 지정해야 하며 멤버 인터페이스는 지정할 수 없습니다.
- 브리지 그룹 멤버 인터페이스 또는 BVI에 대해서는 고정 경로 추적이 지원되지 않습니다.

IPv6

- 고정 경로 추적은 IPv6에서 지원되지 않습니다.

클러스터링 및 다중 상황 모드

- 클러스터링에서는 정적 경로 추적을 기본 유닛에서만 지원합니다.
- 정적 경로 추적은 상황 모드에서 지원되지 않습니다.

네트워크 개체 그룹

정적 경로를 구성하는 동안에는 IP 주소 범위를 포함하는 네트워크 개체 그룹 또는 네트워크 개체 범위를 사용할 수 없습니다.

고정 경로 추가

고정 경로는 특정 목적지 네트워크로 향하는 트래픽을 어디로 보낼지 정의합니다. 최소한 하나의 기본 경로를 정의해야 합니다. 기본 경로는 단순히 목적지 IP 주소가 0.0.0.0/0인 고정 경로입니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 정적 경로를 구성할 가상 라우터를 선택합니다.

단계 **4** 정적 경로를 선택합니다.

단계 **5** 경로 추가를 클릭합니다.

단계 **6** 추가하려는 정적 경로 유형에 따라 **IPv4** 또는 **IPv6**를 클릭합니다.

단계 **7** 고정 경로를 적용하려는 인터페이스를 선택합니다.

투명 모드에서는 브리지 그룹 멤버 인터페이스 이름을 선택합니다. 브리지 그룹에 라우팅된 모드에서 BVI 이름에 대해 둘 중 하나의 브리지 그룹 멤버 인터페이스를 선택할 수 있습니다. 원치 않는 트래픽을 "완전히 사라지게 하려면" **Null0** 인터페이스를 선택합니다.

가상 라우팅을 사용하는 디바이스의 경우 다른 가상 라우터에 속한 인터페이스를 선택할 수 있습니다. 이 가상 라우터에서 다른 가상 라우터로 트래픽을 누출해야 한다면 고정 경로를 생성하면 됩니다. 자세한 내용은 인터커넥트 가상 라우터, 990 페이지의 내용을 참고하십시오.

단계 **8** 사용 가능한 네트워크 목록에서 대상 네트워크를 선택합니다.

기본 경로를 정의하려면 주소 0.0.0.0/0 인 개체를 생성하고 여기에서 선택합니다.

참고 IP 주소 범위를 포함하는 네트워크 개체 그룹을 생성하고 선택할 수는 있지만, FMC는 정적 경로를 설정하는 동안 네트워크 개체 범위 사용을 지원하지 않습니다.

단계 **9** 게이트웨이 또는 **IPv6** 게이트웨이 필드에 입력하거나 이 경로의 다음 홉인 게이트웨이 라우터를 선택합니다. IP 주소 또는 네트워크/호스트 개체를 제공할 수 있습니다. 가상 라우터에 정적 경로 구성을 사용하여 경로 누수가 발생하는 경우 다음 홉 게이트웨이를 지정하지 마십시오.

단계 **10** 메트릭 필드에 대상 네트워크 홉의 개수를 입력합니다. 유효한 범위는 1~255이고 기본값은 1입니다. 메트릭은 특정 호스트에 상주하는 네트워크 홉(홉 수)를 기반으로 경로 "확대"에 대한 측정 항목입니다. 홉 수는 대상 네트워크를 포함해 네트워크 패킷이 최종 대상에 도달하기 전 통과해야 하는 네트워크의 수입니다. 메트릭은 다른 라우팅 프로토콜의 경로를 비교하는 데 사용됩니다. 고정 경로에서 기본 관리 영역은 1이므로 동적 라우팅 프로토콜로 검색되었으나 경로에 직접 연결되지 않은 경로보다 우선합니다. OSPF가 발견한 경로에 대한 기본 관리 영역은 110입니다. 고정 경로의 관리 영역이 동적 경로와 같다면 고정 경로가 우선합니다. 연결된 경로가 항상 고정 경로 또는 동적으로 발견된 경로보다 우선합니다.

단계 **11** (선택 사항) 기본 경로에서 터널링 체크 박스를 클릭하여 VPN 트래픽에 대해 별도의 기본 경로를 정의합니다.

VPN 트래픽이 비 VPN 트래픽과 다른 기본 경로를 사용하도록 하기 위해, VPN 트래픽에 대해 별도의 기본 경로를 정의할 수 있습니다. 예를 들어 VPN 연결에서 들어오는 트래픽은 내부 네트워크를 향하도록 쉽게 방향을 정할 수 있는 반면, 내부 네트워크의 트래픽은 외부를 향하도록 방향을 정할 수 있습니다. 터널링 옵션으로 기본 경로를 생성하면 학습 경로나 고정 경로를 이용하여 라우팅할 수 없는 디바이스에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다. 디바이스당 터널링된 기본 게이트웨이를 하나만 구성할 수 있습니다. 터널링 트래픽에 대한 ECMP는 지원되지 않습니다.

단계 **12** (IPv4 고정 경로 한정) 경로 가용성을 모니터링하려면 경로 추적 필드에서 모니터링 정책을 정의하는 SLA(Service Level Agreement) 모니터 개체의 이름을 선택합니다.

SLA 모니터 개체, 638 페이지의 내용을 참조하십시오.

단계 **13** **Ok(**확인**)**를 클릭합니다.

39 장

Firepower Threat Defense OSPF

이 장에서는 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용하여 FTD을 구성하는 방법을 설명합니다.

- Firepower Threat Defense OSPF, 1041 페이지
- OSPF 요구 사항 및 사전 요건, 1044 페이지
- OSPF에 대한 지침, 1045 페이지
- OSPFv2 구성, 1047 페이지
- OSPFv3 구성, 1060 페이지

Firepower Threat Defense OSPF

이 장에서는 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용하여 FTD을 구성하는 방법을 설명합니다.

OSPF 정보

OSPF는 경로 선택 시 거리 벡터 대신 링크 상태를 사용하는 내부 게이트웨이 라우팅 프로토콜입니다. OSPF는 라우팅 테이블 업데이트가 아닌 링크 상태 광고를 전파합니다. 전체 라우팅 테이블 대신 LSA만 교환되므로, OSPF 네트워크는 RIP 네트워크보다 더 빠르게 통합될 수 있습니다.

OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터에는 동일한 링크 상태 데이터베이스가 포함되며, 여기에는 각 라우터의 사용 가능한 인터페이스 및 연결 가능한 네이버 목록이 있습니다.

RIP를 능가하는 OSPF의 장점은 다음과 같습니다.

- OSPF 링크 상태 데이터베이스 업데이트는 RIP 업데이트보다 전송되는 빈도가 낮으며, 링크 상태 데이터베이스는 천천히 업데이트되지 않고 오래된 정보의 기간이 만료되는 즉시 업데이트됩니다.
- 라우팅 결정은 비용을 기준으로 하며, 이는 특정 인터페이스 전체에 패킷을 전송하는 데 필요한 오버헤드를 나타낸 것입니다. Firepower Threat Defense 디바이스에서는 목적지까지의 홉 개수가 아닌 링크 대역폭을 기준으로 인터페이스의 비용을 계산합니다. 비용을 구성하여 선호하는 경로를 지정할 수 있습니다.

최단 경로 우선 알고리즘의 단점은 CPU 주기 및 메모리가 많이 필요하다는 점입니다.

Firepower Threat Defense 디바이스에서는 OSPF 프로토콜의 프로세스 2개를 다른 인터페이스 집합에서 동시에 실행합니다. 동일한 IP 주소를 사용하는 인터페이스가 있을 경우 2개의 프로세스를 실행하고자 할 수 있습니다(NAT 사용 시 이러한 인터페이스가 공존할 수 있으나, OSPF에서는 중복 주소를 허용하지 않음). 또는 내부에서 한 프로세스를 실행하고 외부에서 다른 프로세스를 실행한 다음, 두 프로세스 간의 경로 하위 집합을 재분배하고자 할 수 있습니다. 이 경우에도 마찬가지로, 사설 주소를 공용 주소에서 분리해야 할 수 있습니다.

경로를 다른 OSPF 라우팅 프로세스, RIP 라우팅 프로세스 또는 OSPF 지원 인터페이스에서 구성된 고정 및 연결된 경로의 OSPF 라우팅 프로세스로 재분배할 수 있습니다.

Firepower Threat Defense 디바이스에서는 다음과 같은 OSPF 기능을 지원합니다.

- 영역 내, 영역 간 및 외부(유형 I 및 유형 II) 경로
- 가상 링크
- LSA 플러딩
- OSPF 패킷에 대한 인증(비밀번호 및 MD5 인증)
- Firepower Threat Defense 디바이스를 전용 라우터 또는 전용 백업 라우터로 구성. Firepower Threat Defense 디바이스는 ABR로 설정할 수도 있습니다.
- 스텁 영역 및 not-so-stubby 영역
- 영역 경계 라우터 유형 3 LSA 필터링

OSPF에서는 MD5 및 일반 텍스트 인접 디바이스 인증을 지원합니다. OSPF와 다른 프로토콜(예: RIP) 간의 경로 재분배 시 공격자가 라우팅 정보를 교란시키기 위해 이를 이용할 우려가 있으므로, 가능한 경우 모든 라우팅 프로토콜에 인증을 사용해야 합니다.

NAT를 사용하면 OSPF가 공용 및 사설 영역에서 가동되며, 주소 필터링이 필요한 경우 2개의 OSPF 프로세스를 실행해야 합니다. 하나는 공용 영역에 사용되는 프로세스이고 다른 하나는 사설 영역에서 사용되는 프로세스입니다.

여러 영역에 인터페이스가 있는 라우터는 ABR(영역 경계선 라우터)라고 합니다. OSPF를 사용하는 라우터와 다른 라우팅 프로토콜을 사용하는 라우터 간에 트래픽을 재분배하는 게이트웨이 역할을 수행하는 라우터를 ASBR(자동 시스템 경계 라우터)이라고 합니다.

ABR에서는 LSA를 사용하여 사용 가능한 경로에 대한 정보를 다른 OSPF 라우터로 전송합니다. ABR 유형 3 LSA 필터링을 사용할 경우, ABR 역할을 수행하는 ASA를 통해 별도의 사설 및 공용 영역을 확보할 수 있습니다. 유형 3 LSA(영역 간 경로)는 한 영역에서 다른 영역으로 필터링할 수 있으며, 이렇게 하면 사설 네트워크를 알리지 않고도 NAT와 OSPF를 함께 사용할 수 있습니다.

참고 유형 3 LSA만 필터링할 수 있습니다. 사설 네트워크에서 Firepower Threat Defense 디바이스를 ASBR로 구성하면 사설 네트워크를 설명하는 유형 5 LSA가 전송되며, 이 경우 공용 영역을 비롯한 전체 AS에 플러딩이 발생합니다.

NAT가 적용되었으나 공용 영역에서 OSPF만 실행 중인 경우, 공용 네트워크에 대한 경로가 사설 네트워크 내부에 기본 또는 유형 5 AS 외부 LSA로서 재배포될 수 있습니다. 그러나 Firepower Threat Defense 디바이스에서 보호하는 사설 네트워크에 대한 고정 경로를 구성해야 합니다. 또는 동일한 Firepower Threat Defense 디바이스 인터페이스에서 공용 네트워크와 사설 네트워크를 혼합할 수 없습니다.

Firepower Threat Defense 디바이스에서 하나는 RIP 라우팅 프로세스, 다른 하나는 EIGRP 라우팅 프로세스로 된 2개의 OSPF 라우팅 프로세스를 동시에 실행할 수 있습니다.

Fast Hello 패킷에 대한 OSPF 지원

OSPF의 Fast Hello 패킷 지원은 hello 패킷을 1초 미만의 간격으로 전송하도록 구성하는 방법을 제공합니다. 이러한 컨피그레이션을 통해 OSPF(Open Shortest Path First) 네트워크에서 통합 속도를 단축할 수 있습니다.

OSPF의 Fast Hello 패킷 지원 사전 요구 사항

OSPF는 네트워크에서 기존에 구성해야 하거나 OSPF의 Fast Hello 패킷 지원 기능과 동시에 구성해야 합니다.

OSPF Hello 간격 및 Dead 간격

OSPF Hello 패킷은 OSPF 프로세스에서 OSPF 네이버와의 연결을 유지하기 위해 이러한 네이버에 전송하는 패킷입니다. Hello 패킷은 구성 가능한 간격(초 단위)으로 전송됩니다. 기본값은 이더넷 링크의 경우 10초이고, 비 브로드캐스트 링크의 경우 30초입니다. Hello 패킷에는 Dead 간격 내에 수신된 Hello 패킷에 대한 모든 네이버 목록이 포함됩니다. Dead 간격도 구성 가능한 간격(초 단위)이며, 기본값은 Hello 간격 값의 4배로 설정됩니다. 모든 Hello 간격의 값은 네트워크 내에서 동일해야 합니다. 마찬가지로, 모든 Dead 간격의 값도 네트워크 내에서 동일해야 합니다.

이러한 두 간격의 상호 작용을 통해 링크가 작동 중임을 나타내어 연결을 유지할 수 있습니다. 라우터가 Dead 간격 내에 네이버에서 Hello 패킷을 수신하지 못할 경우, 해당 네이버는 중단된 것으로 선언됩니다.

OSPF Fast Hello 패킷

OSPF Fast Hello 패킷은 1초 미만의 간격으로 전송되는 Hello 패킷을 참조합니다. Fast Hello 패킷에 대한 내용을 이해하려면 OSPF Fast Hello 패킷과 Dead 간격 간의 관계에 대해서도 숙지해야 합니다. OSPF Hello 간격 및 Dead 간격, 1043 페이지의 내용을 참조하십시오.

OSPF Fast Hello 패킷 기능은 ospf dead-interval 명령을 사용하여 구현할 수 있습니다. Dead 간격은 1초로 설정되고, hello 승수 값은 1초 동안 전송하려는 Hello 패킷의 수로 설정되므로 1초 미만의 또는 "빠른" Hello 패킷이 제공됩니다.

Fast Hello 패킷이 인터페이스에서 구성되면, 이 인터페이스로 전송되는 Hello 패킷에서 광고되는 Hello 간격은 0으로 설정됩니다. 이 인터페이스를 통해 수신되는 Hello 패킷의 Hello 간격은 무시됩니다.

1초로 설정하든(Fast Hello 패킷의 경우) 다른 값으로 설정하든 Dead 간격은 세그먼트에서 일정해야 합니다. Hello 승수의 경우에는 Dead 간격 내에 최소 하나 이상의 Hello 패킷이 전송된다면 전체 세그먼트에서 동일하지 않아도 됩니다.

OSPF Fast Hello 패킷 기능의 이점

OSPF Fast Hello 패킷 기능의 이점은 OSPF 네트워크에서 Fast Hello 패킷을 사용하지 않는 경우와 비교했을 때 더 빠른 통합이 가능하다는 점입니다. 이 기능을 사용하면 1초 내에 손실된 네이버를 감지할 수 있습니다. 이 기능은 특히 OSI(Open System Interconnection) 물리적 레이어 및 데이터 링크 레이어로 감지할 수 없는 네이버가 손실된 LAN 세그먼트에 유용합니다.

OSPFv2와 OSPFv3의 구현 차이점

OSPFv3는 이전 버전인 OSPFv2와 호환되지 않습니다. OSPF를 사용하여 IPv4와 IPv6 트래픽을 모두 라우팅하려면 OSPFv2와 OSPFv3를 동시에 실행해야 합니다. 이들은 서로 공존하지만 상호 작용을 수행하지는 않습니다.

OSPFv3에서 제공하는 추가 기능은 다음과 같습니다.

- 링크당 프로토콜 처리
- 주소 지정 시맨틱 제거
- 플러딩 범위 추가
- 링크당 다중 인스턴스 지원
- IPv6 링크-로컬 주소를 사용하여 네이버 검색 및 기타 기능 지원
- LSA를 접두사와 접두사 길이로 표시
- LSA 유형 2개 추가
- 알 수 없는 LSA 유형 처리
- RFC-4552에 지정된 대로, OSPFv3 라우팅 프로토콜 트래픽에 IPsec ESP 표준을 사용한 인증 지원

OSPF 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

OSPF에 대한 지침

방화벽 모드 지침

OSPF에서는 라우팅 방화벽 모드만 지원합니다. OSPF에서는 투명 방화벽 모드를 지원하지 않습니다.

고가용성 지침

OSPFv2 및 OSPFv3는 스테이트풀 고가용성를 지원합니다.

IPv6 지침

- OSPFv2에서는 IPv6을 지원하지 않습니다.
- OSPFv3에서는 IPv6을 지원합니다.
- OSPFv3에서는 인증에 IPv6을 사용합니다.
- Firepower Threat Defense 디바이스에서는 OSPFv3 경로가 최상의 경로인 경우, 이를 IPv6 RIB에 설치합니다.

OSPFv3 Hello 패킷 및 **GRE**

일반적으로 OSPF 트래픽은 GRE 터널을 통과하지 않습니다. IPv6의 OSPFv3가 GRE 내부에서 캡슐화되는 경우 멀티캐스트 대상과 같은 보안 검사를 위한 IPv6 헤더 검증이 실패합니다. 이 패킷에는 대상 IPv6 멀티캐스트가 있으므로 암시적 보안 확인 검증으로 인해 패킷이 삭제됩니다.

GRE 트래픽을 우회하도록 사전 필터 규칙을 정의할 수 있습니다. 그러나 사전 필터 규칙을 사용하는 경우 검사 엔진에서 내부 패킷을 조사하지 않습니다.

클러스터링 지침

- OSPFv3 암호화는 지원되지 않습니다. 클러스터링 환경에서 OSPFv3 암호화를 구성하려고 할 경우 오류 메시지가 표시됩니다.
- Spanned 인터페이스 모드의 경우, 동적 라우팅은 관리 전용 인터페이스에서 지원되지 않습니다.
- 클러스터에서 마스터 역할이 변경될 경우 다음 동작이 발생합니다.
    - 스팬(spanned) 인터페이스 모드의 경우 라우터 프로세스는 제어 유닛에서만 액티브 상태이며 데이터 유닛에서는 일시 중단 상태입니다. 제어 유닛에서 구성이 동기화되었으므로 각

클러스터 유닛에서는 동일한 라우터 ID를 보유하게 됩니다. 결과적으로, 인접한 라우터에서는 역할이 변경되는 동안 클러스터의 라우터 ID 변경을 알 수 없습니다.

MPLS(Multiprotocol Label Switching) 및 OSPF 지침

MPLS 구성 라우터가 MPLS 헤더를 포함하는 불투명 Type-10 링크 상태 알림(LSA)이 포함된 링크 상태(LS) 업데이트 패킷을 전송하는 경우, 인증이 실패하고 어플라이언스가 이를 승인하지 않고 자동으로 업데이트 패킷을 삭제합니다. 결국 피어 라우터가 승인을 받지 않았기 때문에 피어 라우터는 네이버 관계를 종료합니다.

네이버 관계를 안정적으로 유지하려면 NSF(중단 없이 전달)가 어플라이언스에서 비활성화되었는지 확인하십시오.

- Firepower Management Center(Devices(디바이스) > Device Management(디바이스 관리)(원하는 디바이스 선택) > Routing(라우팅) > OSPF > Advanced(고급) > Non Stop Forwarding(중단 없이 전달))에서 **Non Stop Forwarding(**중단 없이 전달**)** 페이지로 이동합니다.

  Non Stop Forwarding Capability(중단 없이 전달 기능**)** 상자가 선택되어 있지 않은지 확인합니다.

경로 재배포 지침

OSPFv2 또는 OSPFv3에서 IPv4 또는 IPv6 접두사 목록을 사용하는 경로 맵 재배포는 지원되지 않습니다. 재배포를 위해 OSPF에서 연결된 경로를 사용합니다.

추가 지침

- OSPFv2 및 OSPFv3에서는 하나의 인터페이스에 여러 인스턴스를 지원합니다.
- OSPFv3에서는 클러스터링되지 않은 환경에서 ESP 헤더를 통해 암호화를 지원합니다.
- OSPFv3에서는 Non-Payload Encryption을 지원합니다.
- OSPFv2에서는 RFCs 4811, 4812 및 3623에서 각각 정의된 대로 Cisco NSF Graceful Restart 및 IETF NSF Graceful Restart 메커니즘을 지원합니다.
- OSPFv3에서는 RFC 5187에 정의된 대로 Graceful Restart 메커니즘을 지원합니다.
- 배포될 수 있는 내부 영역(유형 1) 경로의 수에는 제한이 있습니다. 이러한 경로의 경우, 단일 유형-1 LSA는 모든 접두사를 포함합니다. 시스템에서 패킷 크기에 35KB의 제한이 있으므로 3000개의 경로로 인해 패킷이 제한을 초과합니다. 2900개의 유형 1 경로를 지원되는 최대 수로 간주하십시오.
- 가상 라우팅을 사용하는 디바이스의 경우 전역 가상 라우터에 OSPFv2 및 OSPFv3를 구성할 수 있습니다. 그러나 사용자 정의 가상 라우터에서는 OSPFv2만 구성할 수 있습니다.
- 경로 업데이트가 링크의 최소 MTU보다 큰 경우 경로 업데이트가 삭제되어 인접성 플랩이 발생하지 않도록 하려면 링크의 양쪽에 있는 인터페이스에서 동일한 MTU를 구성해야 합니다.

OSPFv2 구성

이 섹션에서는 OSPFv2 라우팅 프로세스 구성과 관련된 작업을 설명합니다. 가상 라우팅을 사용하는 디바이스의 경우 전역 및 사용자 정의 가상 라우터에 대해 OSPFv2를 구성할 수 있습니다.

OSPF 영역, 범위 및 가상 링크 구성

설정 인증, 스텁 영역 정의, 기본 요약 경로에 특정 비용 할당 등 여러 OSPF 영역 파라미터를 구성할 수 있습니다. 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다. 각 OSPF 프로세스에는 고유한 관련 영역 및 네트워크가 있습니다. 인증에서는 영역에 무단 액세스를 차단하는 비밀번호 기반의 보호 기능을 제공합니다.

스텁 영역은 외부 경로에 대한 정보가 전송되지 않는 영역입니다. 그 대신, 스텁 영역에는 ABR에서 생성된 기본 외부 경로가 있으며 이는 자동 시스템 외부의 목적지를 위한 경로입니다. OSPF 스텁 영역 지원을 사용하려면 스텁 영역에서 기본 라우팅을 사용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 **4** **OSPF**를 클릭합니다.

단계 **5** 프로세스 **1**을선택합니다. 각 컨텍스트/가상 라우터에 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다. 영역 파라미터를 구성하려면 OSPF 프로세스를 선택해야 합니다.

디바이스에서 가상 라우팅을 사용하고 있다면 ID 필드에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 표시됩니다.

단계 **6** 드롭다운 목록에서 OSPF 역할을 선택하고 다음 필드에 설명을 입력합니다. 옵션으로는 내부, ABR 및 ASBR, ABR 및 ASBR이 있습니다. OSPF 역할에 대한 설명은 OSPF 정보, 1041 페이지의 내용을 참조하십시오.

단계 **7** **Area(**영역**)** > **Add(**추가**)**를 선택합니다.

수정( )를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **8** 각 OSPF 프로세스에 대한 다음 영역 옵션을 구성합니다.

- **OSPF Process(OSPF** 프로세스**)** - 프로세스 ID를 선택합니다. 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
- 영역 **ID** - 경로를 요약할 영역을 지정합니다.
- 영역 유형 - 옵션 중 하나를 선택합니다.

- 기본 - (기본값) 표준 OSPF 영역입니다.
- 스텁 - 스텁 영역의 경우 외부에 라우터 또는 영역이 없습니다. 스텁 영역은 AS(Autonomous System) 외부 LSA(Type 5 LSA)가 스텁 영역으로 플러딩되는 것을 방지합니다. 스텁 영역을 생성하면 스텁 요약 체크 박스의 선택을 취소하여 요약 LSA(Types 3 및 4)가 영역으로 플러딩되는 것을 방지할 수 있습니다.
- **NSSA** - NSSA(not-so-stubby) 영역을 지정합니다. NSSA는 Type 7 LSA를 승인합니다. 재분배 체크 박스의 선택을 취소하고 기본 정보 출처 체크 박스를 선택하여 경로 재분배를 비활성화할 수도 있습니다. **NSSA** 요약 체크 박스의 선택을 취소하고 LSA 요약이 영역으로 플러딩되는 것을 방지합니다.

- 메트릭 값 - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 기본값은 10입니다. 유효한 값의 범위는 0~16777214입니다.
- **Metric Type(**메트릭 유형**)** - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.
- 사용 가능한 네트워크 - 사용 가능한 네트워크 중 하나를 선택하고 **Add(**추가**)**를 클릭하거나 추가( )을 클릭하여 새 네트워크 개체를 추가합니다. 네트워크 추가 절차는 네트워크 개체, 571 페이지를 참조하십시오.
- 인증 - OSPF 인증을 선택합니다.
  - 없음 - (기본) OSPF 영역 인증을 비활성화합니다.
  - 비밀번호 - 영역 인증에 일반 텍스트 비밀번호를 제공하며 보안이 중요한 경우 권장하지 않습니다.
  - **MD5** - MD5 인증을 허용합니다.
- 기본 비용 - 대상까지 최단 경로를 결정하는 데 사용되는 OSPF 영역에 대한 기본 비용입니다. 유효한 값의 범위는 0~65535입니다. 기본값은 1입니다.

단계 **9** **OK**를 클릭하여 구성을 저장합니다.

단계 **10** **Range(**범위**)** > **Add(**추가**)**를 선택합니다.

- 사용 가능한 네트워크 및 알림 여부를 선택하거나
- 네트워크 개체를 추가하려면 추가( )을 클릭합니다. 네트워크 추가 절차는 네트워크 개체, 571 페이지의 내용을 참조하십시오.

단계 **11** **OK**를 클릭하여 설정 범위를 저장합니다.

단계 **12** **Virtual Link(**가상 링크**)**를 선택하고 **Add(**추가**)**를 클릭하여 각 OSPF 프로세스에 대해 다음 옵션을 구성합니다.

- 피어 라우터 - 피어 라우터의 IP 주소를 선택합니다. 새 피어 라우터를 추가하려면 추가( )을 클릭합니다. 네트워크 추가 절차는 네트워크 개체, 571 페이지의 내용을 참조하십시오.

- **Hello** 간격 - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. Hello 간격은 Hello 패킷에 광고되는 무부호 정수입니다. 이 값은 특정 네트워크의 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~65535입니다. 기본값은 10입니다.

  Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다.

- 전송 지연 - 인터페이스에서 LSA 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 지정합니다. 이 정수 값은 0보다 커야 합니다. 유효한 값의 범위는 1~8192입니다. 기본값은 1입니다.

  업데이트 패킷의 LSA에는 전송 전에 이 키워드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다.

- 재전송 간격 - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 재전송 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간입니다. 이 값은 예상 왕복 지연 시간보다 커야 하며 입력 가능한 범위는 1~65535입니다. 기본값은 5입니다.

  라우터에서 LSA를 네이버로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.

- 데드 간격 - 라우터가 중단되었음을 네이버가 나타내기까지 hello 패킷이 표시되지 않은 시간을 초 단위로 입력합니다. Dead 간격은 무부호 정수입니다. 기본값은 Hello 간격의 4배이거나 40초입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~65535입니다.

- 인증 - 다음 OSPF 가상 링크 인증 중 하나를 선택합니다.

  - 없음 - (기본) 가상 링크 영역 인증을 비활성화합니다.
  - 영역 인증 - MD5를 사용하여 활성화 영역을 인증합니다. **Add(**추가**)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(**확인**)**를 클릭합니다.
  - 비밀번호 - 가상 링크 인증에 일반 텍스트 비밀번호를 제공하며 보안이 중요한 경우 권장하지 않습니다.
  - **MD5** - MD5 인증을 허용합니다. **Add(**추가**)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(**확인**)**를 클릭합니다.

    참고 MD5 키 ID는 숫자만 입력합니다.

  - 키 체인 - 키 체인 인증을 허용합니다. **Add(**추가**)**를 클릭하고 키 체인을 생성한 뒤 **Save(**저장**)**을 클릭합니다. 자세한 절차는 키 체인 개체 생성, 636 페이지을 참조하십시오. 피어에 대해 동일한 인증 유형(MD5 또는 키 체인)과 키 ID를 사용하여 성공적인 인접성을 설정합니다.

단계 **13** **OK**를 클릭하여 설정을 저장합니다.

단계 **14** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPF 재배포 구성을 진행합니다.

OSPF 재배포 구성

Firepower Threat Defense 디바이스는 OSPF 라우팅 프로세스 간의 경로 재분배를 제어할 수 있습니다. 하나의 라우팅 프로세스에서 OSPF 라우팅 프로세스로 경로를 재분배하기 위한 규칙이 표시됩니다. RIP 및 BGP에서 검색된 경로를 OSPF 라우팅 프로세스로 재분배할 수 있습니다. 고정 경로 및 연결된 경로도 OSPF 라우팅 프로세스로 재분배할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 **4** **OSPF**를 클릭합니다.

단계 **5** **Distribution(**배포**)** > **Add(**추가**)**를 선택합니다.

수정( )을 클릭하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **6** 각 OSPF 프로세스에 대한 다음 재배포 옵션을 구성합니다.

- **OSPF Process(OSPF** 프로세스**)** - 프로세스 ID를 선택합니다. 가상 라우팅을 사용하는 디바이스의 드롭다운 목록에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 표시됩니다.
- 경로 유형 - 다음 유형 중 하나를 선택합니다.
  - 고정 - 고정 경로를 OSPF 라우팅 프로세스에 재배포합니다.
  - 연결됨 - 연결된 경로(인터페이스에서 IP 주소를 활성화하여 자동으로 설정된 경로)를 OSPF 연결 프로세스에 재배포합니다. 연결된 경로는 AS에 외부 경로로 재분배할 수 있습니다. (옵션) 목록에서 서브넷을 사용할지 여부를 선택할 수 있습니다.
  - **OSPF** - 내부, 외부 1 및 2, NSSA 외부 1 및 2 또는 서브넷을 사용할지 여부 등 다른 OSPF 라우팅 프로세스의 재분배 경로입니다. (옵션) 목록 아래에서 다음 옵션을 선택할 수 있습니다.
  - **BGP** - BGP 라우팅 프로세스에서 경로를 재분배합니다. AS 번호 및 서브넷 사용 여부를 추가합니다.

- **RIP** - RIP 라우팅 프로세스에서 경로를 재분배합니다. (옵션) 목록에서 서브넷을 사용할지 여부를 선택할 수 있습니다.

  참고 사용자 정의 가상 라우터는 RIP를 지원하지 않으므로 RIP에서 경로를 재배포할 수 없습니다.

- 메트릭 값 - 배포되는 경로의 메트릭 값입니다. 기본값은 10입니다. 유효한 값의 범위는 0 ~ 16777215입니다.

  하나의 OSPF 프로세스에서 동일한 디바이스의 다른 OSPF 프로세스로 재분배할 경우, 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재분배할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다.

- **Metric Type(**메트릭 유형**)** - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.

- 태그 값 - OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있는 각 외부 경로에 연결된 32비트 십진수 값입니다. 아무것도 지정하지 않을 경우, 원격 자동 시스템 번호가 BGP 및 EGP의 경로에 사용됩니다. 다른 프로토콜에는 0이 사용됩니다. 유효한 값은 0 ~ 4294967295입니다.

- **Route Map(**경로 맵**)** - 드롭다운 목록에서 경로 맵을 선택하여 소스 라우팅 프로토콜에서 현재 라우팅 프로토콜로 경로 가져오기를 필터링합니다. 이 매개변수를 지정하지 않으면 모든 경로가 재분배됩니다. 이 매개변수를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다. 또는 추가( )를 클릭하여 새 경로 맵을 추가할 수 있습니다. 새 경로 맵을 추가하려면 경로 맵을 참조하십시오.

단계 **7** **OK(**확인**)**를 클릭하여 재배포 구성을 저장합니다.

단계 **8** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPF 영역 간 필터링 구성, 1051 페이지를 계속 진행합니다.

OSPF 영역 간 필터링 구성

ABR Type 3 LSA 필터링은 OSPF를 실행하여 서로 다른 OSPF 영역 간 Type 3 LSA를 필터링하는 ABR의 기능을 확장합니다. 일단 접두사 목록이 구성되면 지정된 접두사만 하나의 OSPF 영역에서 다른 OSPF 영역으로 전송됩니다. 모든 다른 접두사는 OSPF 영역으로 제한됩니다. 이 영역 필터링 유형을 OSPF 영역에서 수신 또는 발신 트래픽에 적용하거나 해당 영역의 수신 및 발신 트래픽 모두에 적용할 수 있습니다.

접두사 목록의 여러 엔트리가 주어진 접두사와 일치하는 경우 순차 번호가 가장 낮은 엔트리가 사용됩니다. 목록 상단 근처의 가장 일반적인 일치 또는 거부에 가장 낮은 순차 번호를 할당하는 것이 효율적일 수 있습니다. 기본적으로 순차 번호는 5부터 시작하여 5씩 증가하며 자동으로 생성됩니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 2 **Routing(**라우팅**)**을 클릭합니다.

단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 4 **OSPF**를 클릭합니다.

단계 5 **InterArea(**영역 간**)** > **Add(**추가**)**를 선택합니다.

수정( )을 클릭하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 6 각 OSPF 프로세스에 대한 다음 필터링 옵션을 구성합니다.

- **OSPF Process(OSPF** 프로세스**)** - 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
- 영역 **ID** - 경로를 요약할 영역을 지정합니다.
- **PrefixList** - 접두사의 이름입니다. 새 접두사 목록 개체를 추가 하려면 5 단계를 참조하십시오.
- 트래픽 방향 - 인바운드 또는 아웃바운드입니다. OSPF 영역에 들어오는 LSA를 필터링하려면 Inbound(인바운드)를 선택하고, OSPF 영역 밖으로 나가는 LSA를 필터링하려면 Outbound(아웃바운드)를 선택합니다. 기존 필터 항목을 편집할 경우 이 설정은 변경할 수 없습니다.

단계 7 추가( )을 클릭하고 새 접두사 목록에 대한 이름을 입력하고 덮어쓰기 허용 여부를 선택합니다.

접두사 규칙을 구성하기 전에 접두사 목록을 구성해야 합니다.

단계 8 접두사 규칙을 구성하려면 추가를 클릭하고 다음 파라미터를 구성합니다.

- 작업 - 재배포 액세스에 대한 차단 또는 허용을 선택합니다.
- 시퀀스 없음 - 라우팅 시퀀스 번호입니다. 기본적으로 순차 번호는 5부터 시작하여 5씩 증가하며 자동으로 생성됩니다.
- **IP** 주소 - IP 주소 형식의 접두사 번호/마스크 길이를 지정합니다.
- 최소 접두사 길이 - (선택 사항) 최소 접두사 길이입니다.
- 최대 접두사 길이 - (선택 사항) 최대 접두사 길이입니다.

단계 9 확인 을 클릭하여 영역 간 필터링 구성을 저장합니다.

단계 10 Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPF 필터 규칙 구성, 1053 페이지를 계속 진행합니다.

OSPF 필터 규칙 구성

각 OSPF 프로세스에 대한 ABR Type 3 LSA 필터를 구성할 수 있습니다. ABR Type 3 LSA 필터는 지정된 접두사만 한 영역에서 다른 영역으로 전송되도록 허용하며 다른 모든 접두사는 제한합니다. 이러한 유형의 영역 필터링은 특정 OSPF 영역의 외부 또는 특정 OSPF 영역의 내부에 적용하거나, 동일한 OSPF 영역의 내부와 외부에 동시에 적용할 수 있습니다. OSPF ABR Type 3 LSA 필터링은 OSPF 영역 간의 경로 재분배 제어 기능을 개선합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 **4** **OSPF**를 클릭합니다.

단계 **5** **Filter Rule(**필터 규**)** > **Add(**추가**)**를 선택합니다.

수정( )을 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 필터 규칙을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **6** 각 OSPF 프로세스에 대한 다음 필터 규칙 옵션을 구성합니다.

- **OSPF Process(OSPF** 프로세스**)** - 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
- 액세스 목록 - 이 OSPF 프로세스에 대한 액세스 목록입니다. 새 표준 액세스 목록 개체를 추가하려면 추가( )을 클릭합니다. 표준 ACL 개체 설정, 646 페이지의 내용을 참조하십시오.
- 트래픽 방향 - 필터링할 트래픽 방향을 선택합니다. OSPF 영역에 들어오는 LSA를 필터링하려면 In을 선택하고, OSPF 영역 밖으로 나가는 LSA를 필터링하려면 Out을 선택합니다. 기존 필터 항목을 편집할 경우 이 설정은 변경할 수 없습니다.
- 인터페이스 - 이 필터 규칙에 대한 인터페이스입니다.

단계 **7** 확인을 클릭하여 필터 규칙 구성을 저장합니다.

단계 **8** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPF 요약 주소 구성, 1054 페이지를 계속 진행합니다.

OSPF 요약 주소 구성

다른 프로토콜의 경로가 OSPF에 재분배될 경우, 각 경로는 외부 LSA에 개별적으로 광고됩니다. 그러나 Firepower Threat Defense 디바이스를 구성하여 지정된 네트워크 주소 및 마스크에 포함되는 모든 재분배된 경로에 대한 단일 경로를 광고할 수 있습니다. 이렇게 구성하면 OSPF 링크 상태 데이터베이스의 크기가 줄어듭니다. 지정된 IP 주소 마스크 쌍과 일치하는 경로는 억제할 수 있습니다. 태그 값을 일치 값으로 사용하여 경로 맵을 통한 재분배를 제어할 수 있습니다.

다른 라우팅 프로토콜에서 학습된 경로를 요약할 수 있습니다. 요약 광고에 사용되는 메트릭은 특정 경로 중에서도 가장 작은 메트릭입니다. 요약 경로는 라우팅 테이블의 크기를 줄이는 데 도움이 됩니다.

OSPF에 요약 경로를 사용하면 OSPF ASBR에서는 단일한 외부 경로를 해당 주소에서 다루는 모든 재분배 경로의 취합본으로 광고하게 됩니다. OSPF로 재분배되는 다른 라우팅 프로토콜의 경로만 요약할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 **4** **OSPF**를 클릭합니다.

단계 **5** **Summary Address(**요약 주소**)** > **Add(**추가**)**를 선택합니다.

수정( )을 클릭하거나 메뉴를 오른쪽 클릭하여 주소를 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **6** 각 OSPF 프로세스에 대한 다음 요약 주소 옵션을 구성합니다.

- **OSPF Process(OSPF** 프로세스**)** - 가상 라우팅을 사용하는 디바이스의 드롭다운에는 선택한 가상 라우터에 대해 생성된 고유한 프로세스 ID가 나열됩니다.
- 사용 가능한 네트워크 - 요약 주소의 IP 주소입니다. 사용 가능한 네트워크 목록에서 하나를 선택하고 추가를 클릭하거나 새 네트워크를 추가하려면 추가( )을 클릭 합니다. 네트워크 추가 절차는 네트워크 개체, 571 페이지의 내용을 참조하십시오.
- 태그 - 각 외부 경로에 연결된 32비트 십진수 값이 표시됩니다. 이 값은 OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있습니다.
- 알림 - 요약 경로 알림입니다. 이 확인란의 선택을 취소하면 요약 주소에 속하는 경로가 억제됩니다. 기본적으로 이 확인란은 선택되어 있습니다.

단계 **7** **OK**를 클릭하여 주소 구성을 저장합니다.

단계 **8** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPF 인터페이스 및 네이버 구성, 1055 페이지를 계속 진행합니다.

OSPF 인터페이스 및 네이버 구성

필요한 경우 일부 인터페이스별 OSPFv2 매개변수를 변경할 수 있습니다. 이러한 파라미터는 변경할 필요가 없지만, hello 간격 및 dead 간격과 같은 인터페이스 파라미터는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 컨피그레이션할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

고정 OSPFv2 네이버를 정의하여 포인트-투-포인트 비 브로드캐스트 네트워크를 통해 OSPFv2 경로를 광고할 수 있습니다. 이 기능을 사용하면 GRE 터널에 광고를 캡슐화하지 않고도 기존 VPN 연결 전체에 OSPFv2 광고를 브로드캐스트할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 2 **Routing(**라우팅**)**을 클릭합니다.

단계 3 (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 4 **OSPF**를 클릭합니다.

단계 5 **Interface(**인터페이스**)** > **Add(**추가**)**를 선택합니다.

수정( )를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 6 각 OSPF 프로세스에 대한 다음 인터페이스 옵션을 구성합니다.

- **Interface(**인터페이스**)** - 구성 중인 인터페이스입니다.

  참고 디바이스에서 가상 라우팅을 사용하는 경우 이 드롭다운 목록에는 라우터에 속하는 인터페이스만 표시됩니다.

- 기본 비용 - 인터페이스를 통한 패킷 전송의 비용입니다. 기본값은 10입니다.
- 우선 순위 - 네트워크의 라우터 우선 순위를 결정합니다. 유효한 값의 범위는 0 ~ 255입니다. 기본값은 1입니다. 이 설정을 0으로 입력하면 해당 라우터는 전용 라우터 또는 백업 전용 라우터가 될 수 없습니다.

  네트워크에 라우터가 2개 연결될 경우, 두 라우터 모두 전용 라우터가 되려고 시도합니다. 라우터 우선 순위가 더 높은 디바이스가 전용 라우터가 됩니다. 연관성이 있을 경우, 라우터 ID가 더 높은 라우터가 전용 라우터가 됩니다. 이 설정은 포인트-투-포인트 인터페이스로 구성된 인터페이스에는 적용되지 않습니다.

- **MTU** 무시 - OSPF에서는 네이버가 공통 인터페이스의 동일한 MTU를 사용하고 있는지 여부를 확인합니다. 네이버가 DBD 패킷을 교환할 때 이러한 확인이 이루어집니다. DBD 패킷에 수신되는 MTU가 수신 인터페이스에 구성된 IP MTU보다 클 경우, OSPF 인접성이 설정되지 않습니다.

- 필터 해제 - 이 설정을 사용하여 동기화 및 플러딩이 진행되는 동안 발신 LSA 인터페이스를 필터링합니다. 기본적으로 OSPF에서는 새로운 LSA를 동일한 영역의 모든 인터페이스로 플러딩하며, LSA가 도달하는 인터페이스는 제외입니다. 완전히 메시된 토폴로지의 경우, 이러한 플러딩이 실행되면 대역폭을 낭비하고 링크 및 CPU를 과도하게 사용할 수 있습니다. 이 확인란을 선택하면 OSPF에서 선택된 인터페이스에 LSA 플러딩을 수행하지 않습니다.
- **Hello Interval(Hello** 간격**)** - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. 유효한 값은 1초 ~ 8192초입니다. 기본값은 10초입니다.

  Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다. 이 값은 특정 인터페이스의 모든 라우터 및 액세스 서버에서 동일해야 합니다.
- 전송 지연 - 인터페이스에서 LSA 패킷을 전송하는 예상 시간을 초 단위로 지정합니다. 유효한 값은 1초 ~ 65535초입니다. 기본값은 1초입니다.

  업데이트 패킷의 LSA에는 전송 전에 이 필드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다.
- **Retransmit Interval(**재전송 간격**)** - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1초 ~ 65535초입니다. 기본값은 5초입니다.

  라우터에서 LSA를 네이버로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.
- **Dead Interval(**중단 간격**)** - 인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간 기간(초)입니다. 값은 네트워크의 모든 노드에 대해 동일 해야 하며 1 ~ 65535 범위를 사용할 수 있습니다.
- **Hello Multiplier** - 필드에서 1초당 전송되는 Hello 패킷의 수를 지정합니다. 유효한 값은 3초 ~ 20초입니다.
- **Point-to-Point** - VPN 터널을 통해 OSPF 경로를 전송할 수 있습니다.
- 인증 - 다음에서 OSPF 인증 인터페이스를 선택합니다.
  - **None (**없음**)** - (기본) 비활성화 인터페이스 인증합니다.
  - 영역 인증 - MD5를 사용하여 활성화 인터페이스를 인증합니다. **Add(**추가**)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(**확인**)**를 클릭합니다.
  - 비밀번호 - 가상 링크 인증에 일반 텍스트 비밀번호를 제공하며 보안이 중요한 경우 권장하지 않습니다.
  - **MD5** - MD5 인증을 허용합니다. **Add(**추가**)**를 클릭하고 키 ID, 키, 키 확인을 입력하고 **OK(**확인**)**를 클릭합니다.

참고 MD5 키 ID는 숫자만 입력합니다.

- 키 체인 - 키 체인 인증을 허용합니다. **Add(**추가**)**를 클릭하고 키 체인을 생성한 뒤 **Save(**저장**)**을 클릭합니다. 자세한 절차는 키 체인 개체 생성, 636 페이지을 참조하십시오. 피어에 대해 동일한 인증 유형(MD5 또는 키 체인)과 키 ID를 사용하여 성공적인 인접성을 설정합니다.

- 비밀 번호 입력 - 비밀 번호 인증 유형으로 비밀 번호를 선택하는 경우를 구성합니다.
- 암호 확인 - 선택한 암호를 확인합니다.

단계 **7** **Neighbor(**네이버**)** > **Add(**추가**)**를 선택합니다.

수정( )를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **8** 각 OSPF 프로세스에 대해 다음 파라미터를 구성합니다.

- **OSPF Process(OSPF** 프로세스**)** - 1 또는 2를 선택합니다.
- 네이버-드롭다운 목록에서 네이버 중 하나를 선택하거나 추가( )을 클릭하여, 새로운 네이버를 추가 하고, 이름, 설명, 네트워크, 오버라이드 허용 여부를 입력하고 저장을 클릭합니다.
- **Interface(**인터페이스**)** - 필드에서 고정 네이버와 관련된 인터페이스를 선택합니다.

단계 **9** **OK**를 클릭하여 네이버 구성을 저장합니다.

단계 **10** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

OSPF 고급 속성 구성

Advanced Properties(고급 속성)를 사용하면 시스템 로그 메시지 생성, 관리 경로 거리, LSA 타이머 및 Graceful Restart와 같은 옵션을 구성할 수 있습니다.

Graceful Restart

Firepower Threat Defense 디바이스에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 전달에 영향을 미치지 않아야 합니다. NSF(Non-Stop Forwarding) 기능을 사용하면 알려진 경로를 계속 사용하여 데이터를 전달하는 동시에 라우팅 프로토콜 정보를 복원할 수 있습니다. 이 기능은 무중단(Hitless) 소프트웨어 업그레이드가 예정되어 있을 때 유용합니다. NSF Cisco(RFC 4811 및 RFC 4812) 또는 NSF IETF(RFC 3623)를 사용하여 OSPFv2에서 Graceful Restart를 구성할 수 있습니다.

참고 NSF 기능은 HA 모드 및 클러스터링에도 유용합니다.

NSF Graceful Restart 기능을 구성하려면 기능을 구성하고, 디바이스를 NSF 지원 또는 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. NSF 지원 디바이스는 해당 디바이스의 재시

작 작업을 네이버에 나타낼 수 있으며, NSF 인식 디바이스는 네이버를 초기화하도록 지원할 수 있습니다.

디바이스는 몇 가지 조건에 따라 NSF 지원 또는 NSF 인식 디바이스로 구성할 수 있습니다.

- 디바이스는 현재 속한 모드에 관계없이 NSF 인식 디바이스로 구성할 수 있습니다.
- NSF 지원 디바이스로 구성하려면 디바이스가 Failover 또는 Spanned Etherchannel(L2) 클러스터 모드에 있어야 합니다.
- NSF 인식 또는 NSF 지원 디바이스가 되려면, 필요에 따라 불투명 LSA(Link State Advertisements)/LLS(Link Local Signaling) 블록 처리 기능과 함께 디바이스를 구성해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 OSPF를 구성할 가상 라우터를 선택합니다.

단계 **4** **OSPF** > **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **5** **General(**일반**)**을 선택하고 다음을 설정합니다.

- 라우터 **ID**— 선택 자동 또는 라우터 ID에 대한 **IP** 주소 IP 주소를 선택하는 경우 IP Address(IP 주소) 필드에 IP 주소를 입력합니다.
- **LSA MOSFP** 무시 - 경로가 지원되지 않는 LSA Type 6 멀티캐스트 OSPF(MOSPF) 패킷을 수신하면 syslog 메시지를 차단합니다.
- **RFC 1583** 호환— 요약 경로 비용을 계산하는 데 사용하는 방법으로 호환성 RFC 1583를 구성합니다. RFC 1583 호환성이 활성화된 라우팅 루프가 발생할 수 있습니다. 라우팅 루프를 방지하기 위해 비활성화합니다. OSPF 라우팅 도메인의 모든 OSPF 라우터는 동일한 RFC 호환성이 있어야 합니다.
- **Adjacency Changes(**인접성 변경사항**)** - 시스템 로그 메시지가 전송될 수 있는 인접성 변경 사항을 정의합니다.

  OSPF 네이버가 작동 또는 중단될 경우 기본적으로 시스템 로그 메시지가 생성됩니다. OSPF 인접 노드가 중단될 때 시스템 로그 메시지를 보내고 각 상태에 대해 시스템 로그를 보내도록 라우터를 구성할 수 있습니다.

  - 로그 인접성 변경 - OSPF 네이버가 변경되면 Firepower Threat Defense 디바이스가 syslog 메시지를 전송합니다. 이 설정은 기본적으로 선택되어 있습니다.
  - 로그 인접성 변경 세부 사항 - OSPF 네이버가 변경될 때 뿐 아니라 상태 변화가 있을 때마다 Firepower Threat Defense 디바이스가 syslog 메시지를 전송합니다. 이 설정은 기본적으로 선택되어 있지 않습니다.

- **Administrative Route Distances(**관리 경로 거리**)** - 영역 간, 영역 내 및 외부 IPv6 경로에 대한 관리 경로 거리를 구성하는 데 사용된 설정을 수정할 수 있습니다. 관리 경로 영역의 값은 10 ~ 254의 정수입니다. 기본값은 110입니다.
- **LSA Group Pacing(LSA** 그룹 속도**)** - LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 초 단위로 지정합니다. 유효한 값의 범위는 10 ~ 1800입니다. 기본값은 240입니다.
- **Default information originate(**기본 정보 생성**)** - OSPFv3 라우팅 도메인에 기본 외부 경로를 생성하고 다음 옵션을 구성하려면 **Enable(**활성화**)** 확인란을 선택합니다.
  - 항상 기본 경로 광고— 기본 경로 광고 항상 보장 합니다.
  - 를 클릭합니다**.(**메트릭 값**)** - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 유효한 값의 범위는 0 ~ 16777214입니다. 기본값은 10입니다.
  - **Metric Type(**메트릭 유형**)** - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형입니다. 유효한 값은 1(유형 1 외부 경로) 및 2(유형 2 외부 경로)입니다. 기본값은 Type 2 외부 경로입니다.
  - **RouteMap(**경로 맵**)** - 경로 맵이 적절한 경우 기본 경로를 생성하는 라우팅 프로세스를 선택하거나 추가(+)을 클릭하여 새 경로를 추가합니다. 새 경로 맵을 추가하려면 경로 맵을 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭하여 일반 구성을 저장합니다.

단계 **7** **Non Stop Forwarding(**정지 없이 전송**)**을 선택하고 NSF 가능 또는 NSF 인식 디바이스에서 OSFPv2에 대해 Cisco NSF grasfue restart를 구성합니다.

참고 OSPFv2에 사용할 수 있는 두 가지 Graceful Restart 메커니즘은 Cisco NSF 및 IETF NSF입니다. ospf 인스턴스에는 Graceful Restart 메커니즘을 한 번에 하나만 구성할 수 있습니다. NSF 인식 장치는 Cisco NSF 헬퍼 및 IETF NSF 헬퍼 둘 다로 구성 될 수 있으 나 NSF 지원 장치는 OSPF 인스턴스를 위해 한 번에 Cisco NSF 또는 IETF NSF 모드에서 구성할 수 있습니다.

a) **Enable Cisco** 비 **Stop Forwarding** 기능 체크 박스 선택합니다.
b) (선택 사항) 필요한 경우 **Cancels NSF restart when non-NSF-aware neighboring networking devices are detected(NSF** 이외 인식 인접 네트워킹 디바이스가 감지된 경우 **NSF** 재시작 취소**)** 확인란을 선택합니다.
c) (선택 사항) **Enable Cisco** 비 **Stop Forwarding** 헬퍼 모드 체크 박스 NSF 인식 디바이스에서 헬퍼 모드를 비활성화하려면 선택하지 않았는지 확인합니다.

단계 **8** NSF 지원 또는 NSF 인식 디바이스에 대해 OSPFv2용 IETF NSF 정상 재시작을 구성합니다.

a) **Enable IETF** 비 **Stop Forwarding** 기능 확인란을 선택합니다.
b) (선택 사항) **Length of graceful restart interval(**정상 재시작 간격 길이**)** 필드에 재시작 간격을 초 단위로 입력합니다. 기본값은 120초입니다. 재시작 간격이 30초 미만일 경우 Graceful Restart가 종료됩니다.
c) (선택 사항) **Enable IETF nonstop** 착신 전환 **(NSF)** 헬퍼 모드에 대한 체크 박스 NSF 인식 디바이스에서 IETF NSF 헬퍼 모드를 비활성화 하려면 선택 하지 않은 있는지 확인합니다.

d) 엄격 링크 상태 알림 확인 활성화 - 활성화하면 재시작 라우터에 플러딩되는 LSA의 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다.

e) **Enable IETF** 비 **Stop Forwarding**— 활성화 되지 않은 전환에 따라 라우팅 프로토콜 정보를 복원되는 동안 알려진 경로 계속 하려면 데이터 패킷 전달할 수 있는 착신 전환 중단 방법입니다. OSPF 네이버 OSPF 디바이스에서의 상태를 복구 하기 위해 OSPF 프로토콜 확장을 사용합니다. 작동 하려면 복구를 위한 네이버 NSF 프로토콜 확장을 지원 하 고 다시 시작 되는 디바이스에 "helper" 역할을 할 수 해야 합니다. 네이버는 프로토콜 상태 복구 수행 하는 동안 다시 시작 되는 디바이스에 데이터 트래픽 전달 계속 해야 합니다.

OSPFv3 구성

이 섹션에서는 OSPFv3 라우팅 프로세스 구성과 관련된 작업을 설명합니다. 가상 라우팅을 사용하는 디바이스의 경우 OSPFv3는 전역 가상 라우터에만 구성할 수 있으며 사용자 정의 가상 라우터에는 구성할 수 없습니다.

OSPFv3 영역, 경로 요약 및 가상 링크 구성

OSPFv3를 활성화하려면 OSPFv3 라우팅 프로세스를 생성하고, OSPFv3에 대한 영역을 생성하고, OSPFv3에 대한 인터페이스를 활성화하고, 경로를 대상 OSPFv3 라우팅 프로세스에 재분배해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **OSPFv3**을 선택합니다.

단계 **3** 기본적으로 활성화 프로세스 **1** 선택 되어 있습니다. 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다.

단계 **4** 드롭다운 목록에서 OSPF 역할을 선택하고 다음 필드에 설명을 입력합니다. 옵션으로는 내부, ABR 및 ASBR, ABR 및 ASBR이 있습니다. 참조 OSPF 정보, 1041 페이지 OSPFv3 역할에 대 한 설명입니다.

단계 **5** **Area(**영역**)** > **Add(**추가**)**를 선택합니다.

수정( )를 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **6** **General(**일반**)**을 선택하고 각 OSPF 프로세스에 대해 다음 옵션을 구성합니다.

- 영역 **ID** - 경로를 요약할 영역을 지정합니다.
- 비용 - 목적지까지의 최단 경로를 결정하는 OSPF SPF 계산 과정에 사용되는 요약 경로의 메트릭 또는 비용을 입력합니다. 유효한 값의 범위는 0 ~ 16777215입니다.

- 유형-Normal, NSSA, Stub 지정 합니다. 일반을 선택 하는 경우에 다른 매개 변수가 구성 합니다. Stub을 선택 하는 경우 영역에 요약 Lsa를 전송 하도록 선택할 수 있습니다. NSSA를 선택 하는 경우에 다음 세 가지 옵션을 구성할 수 있습니다.
  - 요약 LSA를 영역으로 전송하도록 허용하려면 **Allow sending of summary LSAs into the area(**요약 **LSA**를 영역으로 전송하도록 허용**)** 확인란을 선택합니다.
  - 재배포 시 경로를 Normal 및 not-so-stubby 영역으로 가져오도록 허용하려면 **Redistribution imports routes to normal and NSSA areas(**재배포시 일반 및 **NSSA** 영역으로 경로 가져오기**)** 확인란을 선택합니다.
  - **default-information originate** - OSPF 라우팅 도메인에 기본 외부 경로를 생성합니다.
- **Metric(**메트릭**)** - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 기본값은 10입니다. 유효한 값의 범위는 0 ~ 16777214입니다.
- 메트릭 유형 - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.

단계 **7** **OK(**확인**)**를 클릭하여 일반 구성을 저장합니다.

단계 **8** **Route Summary(**경로 요약**)** > **Add Route Summary(**경로 요약 추가**)**를 선택합니다.

수정( )을 클릭하거나 메뉴를 오른쪽 클릭하여 라우트 요약을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **9** 각 OSPF 프로세스에 대 한 다음 경로 요약 옵션을 구성 합니다.

- **IPv6/Prefix-length**-IPv6 접두사. 네트워크 개체를 새로 추가하려면 추가( )을 클릭합니다. 네트워크 추가 절차는 네트워크 개체, 571 페이지의 내용을 참조하십시오.
- 비용 - 목적지까지의 최단 경로를 결정하는 OSPF SPF 계산 과정에 사용되는 요약 경로의 메트릭 또는 비용을 입력합니다. 유효한 값의 범위는 0 ~ 16777215입니다.
- 알림 - 요약 경로 알림입니다. 이 확인란의 선택을 취소하면 요약 주소에 속하는 경로가 억제됩니다. 기본적으로 이 확인란은 선택되어 있습니다.

단계 **10** 확인 을 클릭 하 여 경로 요약 구성을 저장 합니다.

단계 **11** 가상 링크를 선택하고 추가를 클릭하여 각 OSPF 프로세스에 대해 다음 옵션을 구성합니다.

- 피어 **RouterID**-피어 라우터 IP 주소를 선택합니다. 네트워크 개체를 새로 추가하려면 추가( )을 클릭합니다. 네트워크 추가 절차는 네트워크 개체, 571 페이지의 내용을 참조하십시오.
- **TTL** 보안— 활성화 TTL 보안 검사 합니다. Hop count에 대 한 값은 1에서 254 사이의 숫자입니다. 기본값은 1입니다.

  OSPF에서 0에서 255 TTL (Live) 값으로 IP 헤더 시간으로 발신 패킷을 전송하고 가능한 임계값보다 작은 TTL 값이 있는 수신 패킷을 구성합니다. 장치별 전달 하는 IP 패킷을 TTL 감소, 때문에 직접 (1 홉) 연결을 통해 수신 된 패킷 255의 값을 갖습니다. 두 개의 홉을 통과 하는 패킷은 254 등의 값을 갖고 있습니다. 수신 임계값은 패킷을 거리 있을 수 있는 홉의 최대 수 형태로 구성 됩니다.

- 데드 간격 - 라우터가 중단되었음을 네이버가 나타내기까지 hello 패킷이 표시되지 않은 시간을 초 단위로 입력합니다. 기본값은 Hello 간격의 4배이거나 40초입니다. 유효한 값의 범위는 1 ~ 65535입니다.

  Dead 간격은 무부호 정수입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다.

- **Hello** 간격 - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. 유효한 값의 범위는 1 ~ 65535입니다. 기본값은 10입니다.

  Hello 간격은 Hello 패킷에 광고되는 무부호 정수입니다. 이 값은 특정 네트워크의 모든 라우터 및 액세스 서버에서 동일해야 합니다. Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다.

- 재전송 간격 - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 재전송 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간입니다. 이 값은 예상 왕복 지연 시간보다 커야 하며 입력 가능한 범위는 1~65535입니다. 기본값은 5입니다.

  라우터에서 LSA를 네이버로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.

- 전송 지연 - 인터페이스에서 LSA 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 지정합니다. 이 정수 값은 0보다 커야 합니다. 유효한 값의 범위는 1 ~ 8192입니다. 기본값은 1입니다.

  업데이트 패킷의 LSA에는 전송 전에 이 키워드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다.

단계 **12** **OK**를 클릭하여 설정을 저장합니다.

단계 **13** 변경 사항을 저장 하려면 라우터 페이지에서 저장 을 클릭 합니다.

다음에 수행할 작업

OSPFv3 재배포 구성진행 합니다.

OSPFv3 재배포 구성

Firepower Threat Defense 디바이스는 OSPF 라우팅 프로세스 간의 경로 재분배를 제어할 수 있습니다. 하나의 라우팅 프로세스에서 OSPF 라우팅 프로세스로 경로를 재분배하기 위한 규칙이 표시됩니다. RIP 및 BGP에서 검색된 경로를 OSPF 라우팅 프로세스로 재분배할 수 있습니다. 고정 경로 및 연결된 경로도 OSPF 라우팅 프로세스로 재분배할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** 라우팅 > **OSPF**을 선택합니다.

단계 **3** **Redistribution(**재배포**)**을 선택하고 **Add(**추가**)**를 누릅니다.

수정( )을 클릭하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **4** 각 OSPF 프로세스에 대한 다음 재배포 옵션을 구성합니다.

- 소스 프로토콜 - 경로를 재배포하는 소스 프로토콜. 지원되는 프로토콜은 connected, static, OSPF입니다. OSPF를 선택 하는 경우에 프로세스 **ID** 필드에 프로세스 ID를 입력 해야 합니다. BCP를 선택 하는 경우에 **AS** 번호 필드에 AS 번호를 추가해야 합니다.
- 메트릭 -배포 되는 경로의 메트릭 값입니다. 기본값은 10입니다. 유효한 값의 범위는 0 ~ 16777215입니다.

  하나의 OSPF 프로세스에서 동일한 디바이스의 다른 OSPF 프로세스로 재분배할 경우, 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재분배할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다.
- **Metric Type(**메트릭 유형**)** - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 디폴트 라우터와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.
- **Tag(**태그**)** - 태그는 OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있는 각 외부 경로에 연결된 32비트 십진수 값을 지정합니다. 아무것도 지정하지 않을 경우, 원격 자동 시스템 번호가 BGP 및 EGP의 경로에 사용됩니다. 다른 프로토콜에는 0이 사용됩니다. 유효한 값은 0 ~ 4294967295입니다.
- **Route Map(**경로 맵**)** - 소스 라우팅 프로토콜에서 현재 라우팅 프로토콜까지 경로 가져오기의 필터링을 확인합니다. 이 매개변수를 지정하지 않으면 모든 경로가 재분배됩니다. 이 매개변수를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다. 또는 추가( )를 클릭하여 새 경로 맵을 추가할 수 있습니다. 경로 맵, 641 페이지의 절차를 참조하여 새로운 경로 맵을 추가합니다.
- **Process ID(**프로세스 **ID)** - OSPF 프로세스 ID(1 또는 2)입니다.

  참고 프로세스 ID가 활성화되면 OSPFv3 프로세스가 다른 OSPFv3 프로세스에서 학습한 경로를 재배포합니다.

- **Match(**연결**)** - 다른 라우팅 도메인에 재배포할 수 있도록 OSPF 경로를 활성화합니다.
  - **Internal(**내부**)** - 특정 자동 시스템의 내부에 있는 경로입니다.
  - **External 1(**외부 **1)** - 자동 시스템의 외부에 있지만, OSPFv3에 Type 1 외부 경로로서 가져온 경로입니다.

- **External 2(**외부 **2)** - 자동 시스템의 외부에 있지만, OSPFv3에 Type 2 외부 경로로서 가져온 경로입니다.
- **NSSA External 1(NSSA** 외부 **1)** - 자동 시스템의 외부에 있지만 IPv6를 지원하는 NSSA의 OSPFv3에 Type 1 외부 경로로서 가져온 경로입니다.
- **NSSA External(NSSA** 외부**)** - 자동 시스템의 외부에 있지만 IPv6를 지원하는 NSSA의 OSPFv3에 Type 2 외부 경로로서 가져온 경로입니다.

단계 **5** **OK(**확인**)**를 클릭하여 재배포 구성을 저장합니다.

단계 **6** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPFv3 요약 접두사 설정, 1064 페이지를 계속 진행합니다.

OSPFv3 요약 접두사 설정

지정된 IPv6 접두사 및 마스크 쌍과 일치하는 경로를 알리도록 Firepower Threat Defense 디바이스를 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **OSPFv3**을 선택합니다.

단계 **3** **Summary Prefix(**요약 접두사**)** > **Add(**추가**)**를 선택합니다.

수정( )을 클릭하거나 메뉴를 오른쪽 클릭하여 요약 접두사를 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **4** 각 OSPF 프로세스에 대한 다음 요약 접두사 옵션을 구성합니다.

- **IPv6 Prefix/Length(IPv6** 접두사/길이**)** - IPv6 접두사 및 프리픽스 길이 라벨입니다. 목록에서 하나를 선택하거나 추가( )을 클릭하여 새 네트워크 개체를 추가합니다. 네트워크 추가 절차는 네트워크 개체, 571 페이지를 참조하십시오.
- **Advertise(**알림**)** - 지정된 접두사 및 마스크 쌍과 일치하는 경로를 알립니다. 지정된 접두사 및 마스크 쌍과 일치하는 경로를 억제하려면 이 확인란의 선택을 취소합니다.
- (선택 사항) **Tag(**태그**)** - 경로 맵을 통해 재배포를 제어하기 위한 일치 값으로 사용할 수 있는 값입니다.

단계 **5** **OK(**확인**)**를 클릭하여 요약 접두사 구성을 저장합니다.

단계 **6** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

OSPFv3 인터페이스, 인증 및 네이버 설정, 1065 페이지를 계속 진행합니다.

OSPFv3 인터페이스, 인증 및 네이버 설정

필요한 경우 특정 인터페이스별 OSPFv3 매개변수를 변경할 수 있습니다. 이러한 파라미터는 변경할 필요가 없지만, hello 간격 및 dead 간격과 같은 인터페이스 파라미터는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 구성할 경우, 네트워크의 모든 라우터 구성에 호환되는 값이 있는지 확인해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **OSPFv3**을 선택합니다.

단계 **3** **Interface(**인터페이스**)** > **Add(**추가**)**를 선택합니다.

Edit(편집**)**을 클릭하여 편집하거나 메뉴를 오른쪽 클릭하여 영역을 잘라내기, 복사, 붙여넣기, 삽입, 삭제할 수 있습니다.

단계 **4** 각 OSPFv3 프로세스에 대해 다음 인터페이스 옵션을 구성합니다.

- **Interface(**인터페이스**)** - 구성 중인 인터페이스입니다.
- **Enable OSPFv3(OSPFv3** 활성화**)** - OSPFv3을 활성화합니다.
- **OSPF Process(OSPF** 프로세스**)** - 1 또는 2를 선택합니다.
- **Area(**영역**)** - 이 프로세스에 대한 영역 ID입니다.
- **Instance(**인스턴스**)** - 인터페이스에 할당할 영역 인스턴스 ID를 지정합니다. 하나의 인터페이스에는 하나의 OSPFv3 영역만 포함할 수 있습니다. 여러 인터페이스에서 동일한 영역을 사용할 수 있으며, 각 인터페이스에서는 다른 영역 인스턴스 ID를 사용할 수 있습니다.

단계 **5** **Properties(**속성**)**를 선택하고 각 OSPFv3 프로세스에 대해 다음 옵션을 구성합니다.

- **Filter Outgoing Link Status Advertisements(**발송 링크 상태 알림 필터링**)** - OSPFv3 인터페이스에 발신되는 LSA를 필터링합니다. 기본적으로 모든 발신 LSA는 인터페이스에 플러딩됩니다.
- **Disable MTU mismatch detection(MTU** 불일치 감지 비활성화**)** - DBD 패킷이 수신될 때 OSPF MTU 불일치 감지를 비활성화합니다. OSPF MTU 불일치 감지는 기본적으로 활성화되어 있습니다.
- **Flood Reduction(**플러딩 감소**)** - 정상 LSA를 Do not Age LSAs(LSA 기간 적용 안 함)로 변경하여 3600초마다 영역에 플러딩되지 않도록 합니다.

OSPF LSA는 3600초마다 새로 고침됩니다. 대규모 OSPF 네트워크에서 이는 영역 간에 많은 양의 불필요한 LSA 플러딩을 유발할 수 있습니다.

- **Point-to-Point Network(**포인트-투-포인트 네트워크**)** - VPN 터널을 통해 OSPF 경로를 전송할 수 있습니다. 인터페이스가 포인트-투-포인트 비 브로드캐스트로 구성된 경우, 다음과 같은 제한이 적용됩니다.
  - 인터페이스에 대해 하나의 네이버만 정의할 수 있습니다.
  - 네이버를 수동으로 구성해야 합니다.
  - 암호화 엔드포인트를 가리키는 고정 경로를 정의해야 합니다.
  - 인터페이스에서 터널을 통해 OSPF가 실행 중일 경우, 업스트림 라우터가 있는 일반 OSPF를 동일한 인터페이스에서 실행할 수 없습니다.
  - OSPF 네이버를 지정하기 전에 암호화 맵을 인터페이스에 바인딩하여 OSPF 업데이트가 VPN 터널을 통해 전달되도록 해야 합니다. OSPF 네이버를 지정한 후에 암호화 맵을 인터페이스에 바인딩한 경우, **clear local-host all** 명령을 사용하여 OSPF 연결을 지워 OSPF 인접성이 VPN 터널을 통해 설정될 수 있도록 합니다.
- **Broadcast(**브로드캐스트**)** - 인터페이스의 브로드캐스트 인터페이스 여부를 지정합니다. 기본적으로 이 확인란은 이더넷 인터페이스에 선택되어 있습니다. 인터페이스를 포인트-투-포인트 비 브로드캐스트 인터페이스로 지정하려면 이 확인란의 선택을 취소합니다. 인터페이스를 포인트-투-포인트 비 브로드캐스트 인터페이스로 지정하면 OSPF 경로를 VPN 터널을 통해 전송할 수 있습니다.
- **Cost(**비용**)** - 인터페이스에서 패킷을 전송하는 비용을 지정합니다. 이 설정의 유효한 값 범위는 0 ~ 255입니다. 기본값은 1입니다. 이 설정을 0으로 입력하면 해당 라우터는 전용 라우터 또는 백업 전용 라우터가 될 수 없습니다. 이 설정은 포인트-투-포인트 비 브로드캐스트 인터페이스로 구성된 인터페이스에는 적용되지 않습니다.

  네트워크에 라우터가 2개 연결될 경우, 두 라우터 모두 전용 라우터가 되려고 시도합니다. 라우터 우선 순위가 더 높은 디바이스가 전용 라우터가 됩니다. 연관성이 있을 경우, 라우터 ID가 더 높은 라우터가 전용 라우터가 됩니다.
- **Priority(**우선 순위**)** - 네트워크의 전용 라우터를 결정합니다. 유효한 값의 범위는 0 ~ 255입니다.
- **Dead Interval(**중단 간격**)** - 인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간 기간(초)입니다. 이 값은 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다.
- **Poll Interval(**폴링 간격**)** - 네이버와의 인접성이 설정되기 전에 라우터가 전송할 OSPF 패킷 사이의 시간 기간(초)입니다. 라우팅 디바이스가 활성 네이버를 감지하면 hello 패킷 간격은 폴링 간격에 지정된 시간에서 hello 간격에 지정된 시간으로 변경됩니다. 유효한 값의 범위는 1초 ~ 65535초입니다.
- **Retransmit Interval(**재전송 간격**)** - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 시간(초)입니다. 이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1초 ~ 65535초입니다. 기본값은 5초입니다.

- **Transmit Delay(**전송 지연**)** - 필드에 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간(초)입니다. 유효한 값의 범위는 1초 ~ 65535초입니다. 기본값은 1초입니다.

단계 **6** **OK(**확인**)**를 클릭하여 구성을 저장합니다.

단계 **7** **Authentication(**인증**)**을 선택하고 각 OSPFv3 프로세스에 대해 다음 옵션을 구성합니다.

- **Type(**유형**)** - 인증 유형입니다. 사용 가능한 옵션은 Area(영역), Interface(인터페이스), None(없음)입니다. None(없음) 옵션은 사용 중인 인증이 없음을 나타냅니다.
- **Security Parameters Index(**보안 파라미터 색인**)** - 256~4294967295 사이의 숫자입니다. 유형으로 Interface(인터페이스)를 선택한 경우 구성합니다.
- **Authentication(**인증**)** - 인증 알고리즘의 유형입니다. 지원되는 값은 SHA-1 및 MD5입니다. 유형으로 Interface(인터페이스)를 선택한 경우 설정합니다.
- **Authentication Key(**인증 키**)** - MD5 인증을 사용할 경우, 키는 32자 길이의 16진수 숫자(16바이트)여야 합니다. SHA-1 인증을 사용할 경우, 키는 40자 길이의 16진수 숫자(20바이트)여야 합니다.
- **Encrypt Authentication Key(**인증 키 암호화**)** - 인증 키 암호화를 활성화합니다.
- **Include Encryption(**암호화 포함**)** - 암호화를 활성화합니다.
- **Encryption Algorithm(**암호화 알고리즘**)** - 암호화 알고리즘의 유형입니다. 지원되는 값은 DES입니다. Null 항목은 암호화가 없음을 나타냅니다. **Include Encryption(**암호화 포함**)**을 선택하는 경우 구성합니다.
- **Encryption Key(**인증 키**)** - 인증 키를 입력합니다. **Include Encryption(**암호화 포함**)**을 선택하는 경우 구성합니다.
- **Encrypt Key(**키 암호화**)** - 키가 암호화되도록 활성화합니다.

단계 **8** **OK(**확인**)**를 클릭하여 구성을 저장합니다.

단계 **9** **Neighbor(**네이버**)**를 선택하고 **Add(**추가**)**를 클릭하여 각 OSPFv3 프로세스에 대해 다음 옵션을 구성합니다.

- **Link Local Address(**로컬 주소 연결**)** - 고정 네이버의 IPv6 주소입니다.
- **Cost(**비용**)** - 비용을 활성화합니다. **Cost(**비용**)** 필드에 비용을 입력한 다음, 알리려면 **Filter Outgoing Link State Advertisements(**발송 링크 상태 알림 필터링**)**를 선택합니다.
- (선택 사항) **Poll Interval(**폴링 간격**)** - 폴링 간격을 활성화합니다. **Priority(**우선 순위**)** 레벨 및 **Poll Interval(**폴링 간격**)**을 초 단위로 입력합니다.

단계 **10** 네이버를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **11** **OK(**확인**)**를 클릭하여 인터페이스 구성을 저장합니다.

OSPFv3 고급 속성 설정

Advanced Properties(고급 속성)를 사용하면 시스템 로그 메시지 생성, 관리 경로 거리, 수동 OSPFv3 라우팅, LSA 타이머 및 Graceful Restart와 같은 옵션을 설정할 수 있습니다.

Graceful Restart

Firepower Threat Defense 디바이스에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 전달에 영향을 미치지 않아야 합니다. NSF(Non-Stop Forwarding) 기능을 사용하면 알려진 경로를 계속 사용하여 데이터를 전달하는 동시에 라우팅 프로토콜 정보를 복원할 수 있습니다. 이 기능은 무중단(Hitless) 소프트웨어 업그레이드가 예정되어 있을 때 유용합니다. graceful-restart(RFC 5187)를 사용하여 OSPFv3에서 Graceful Restart를 구성할 수 있습니다.

참고 NSF 기능은 HA 모드 및 클러스터링에도 유용합니다.

NSF Graceful Restart 기능을 구성하려면 기능을 구성하고, 디바이스를 NSF 지원 또는 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. NSF 지원 디바이스는 해당 디바이스의 재시작 작업을 네이버에 나타낼 수 있으며, NSF 인식 디바이스는 네이버를 초기화하도록 지원할 수 있습니다.

디바이스는 몇 가지 조건에 따라 NSF 지원 또는 NSF 인식 디바이스로 구성할 수 있습니다.

- 디바이스는 현재 속한 모드에 관계없이 NSF 인식 디바이스로 구성할 수 있습니다.
- NSF 지원 디바이스로 구성하려면 디바이스가 Failover 또는 Spanned Etherchannel(L2) 클러스터 모드에 있어야 합니다.
- NSF 인식 또는 NSF 지원 디바이스가 되려면, 필요에 따라 불투명 LSA(Link State Advertisements)/LLS(Link Local Signaling) 블록 처리 기능과 함께 디바이스를 구성해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **OSPFv3** > **Advanced(**고급**)**를 선택합니다.

단계 **3** **Router ID(**라우터 **ID)**에서 **Automatic(**자동**)** 또는 **IP address(IP** 주소**)**를 선택합니다. IP 주소를 선택하는 경우 IP Address(IP 주소) 필드에 IP 주소를 입력합니다.

단계 **4** 경로가 지원되지 않는 LSA Type 6 멀티캐스트 OSPF(MOSPF) 패킷을 수신할 때 시스템 로그 메시지를 표시하지 않으려면 **Ignore LSA MOSPF(LSA MOSPF** 무시**)** 확인란을 선택합니다.

단계 **5** **General(**일반**)**을 선택하고 다음을 설정합니다.

- **Adjacency Changes(**인접성 변경사항**)** - 시스템 로그 메시지가 전송될 수 있는 인접성 변경 사항을 정의합니다.

OSPF 네이버가 작동 또는 중단될 경우 기본적으로 시스템 로그 메시지가 생성됩니다. OSPF 인접 노드가 중단될 때 시스템 로그 메시지를 보내고 각 상태에 대해 시스템 로그를 보내도록 라우터를 구성할 수 있습니다.

- **Adjacency Changes(**인접성 변경사항**)** - OSPF 네이버가 작동 또는 중단될 때마다 Firepower Threat Defense 디바이스에서 시스템 로그 메시지를 전송하도록 합니다. 이 설정은 기본적으로 선택되어 있습니다.
- **Include Details(**상세정보 포함**)** - Firepower Threat Defense 디바이스의 작동 또는 중단 뿐만 아니라 모든 상태가 변경될 때마다 에서 syslog 메시지를 전송하게 됩니다. 이 설정은 기본적으로 선택되어 있지 않습니다.

- **Administrative Route Distances(**관리 경로 거리**)** - 영역 간, 영역 내 및 외부 IPv6 경로에 대한 관리 경로 거리를 구성하는 데 사용된 설정을 수정할 수 있습니다. 관리 경로 영역의 값은 10 ~ 254의 정수입니다. 기본값은 110입니다.
- **Default information originate(**기본 정보 생성**)** - OSPFv3 라우팅 도메인에 기본 외부 경로를 생성하고 다음 옵션을 구성하려면 **Enable(**활성화**)** 확인란을 선택합니다.
  - **Always advertise(**항상 알림**)** - 기본 경로의 존재 여부에 상관없이 항상 기본 경로를 광고합니다.
  - **Metric(**메트릭**)** - 기본 경로를 생성하는 데 사용되는 메트릭입니다. 유효한 값의 범위는 0 ~ 16777214입니다. 기본값은 10입니다.
  - **Metric Type(**메트릭 유형**)** - 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형입니다. 유효한 값은 1(유형 1 외부 경로) 및 2(유형 2 외부 경로)입니다. 기본값은 Type 2 외부 경로입니다.
  - **Route Map(**경로 맵**)** - 경로 맵이 적절한 경우, 기본 경로를 생성하는 라우팅 프로세스를 선택하거나 추가(+)를 클릭하여 새 경로를 추가합니다. 경로 맵, 641 페이지를 참조하여 새로운 경로 맵을 추가합니다.

단계 **6** **OK(**확인**)**를 클릭하여 일반 구성을 저장합니다.

단계 **7** **Passive Interface(**패시브 인터페이스**)**를 선택하고 Available Interfaces(사용 가능한 인터페이스) 목록에서 패시브 OSPFv3 라우팅을 활성화할 인터페이스를 선택한 다음 **Add(**추가**)**를 클릭하여 Selected Interfaces(선택한 인터페이스) 목록으로 이동합니다.

패시브 라우팅에서는 OSPFv3 라우팅 정보의 광고를 제어할 수 있도록 지원하고, 인터페이스에서 OSPFv3 라우팅 업데이트의 전송 및 수신을 비활성화합니다.

단계 **8** **OK(**확인**)**를 클릭하여 패시브 인터페이스 구성을 저장합니다.

단계 **9** **Timer(**타이머**)**를 선택하고 다음 LSA 속도 및 SPF 계산 타이머를 설정합니다.

- **Arrival(**도착**)** - 네이버에서 도착하는 동일한 LSA를 수락하는 동안 소요될 수밖에 없는 최소 지연 시간을 밀리초 단위로 지정합니다. 범위는 0밀리초 ~ 6000,000밀리초입니다. 기본값은 1000밀리초입니다.

- **Flood Pacing(**플러딩 속도**)** - 업데이트 중 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5밀리초 ~ 100밀리초입니다. 기본값은 33밀리초입니다.
- **Group Pacing(**그룹 속도**)** - LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 초 단위로 지정합니다. 유효한 값의 범위는 10 ~ 1800입니다. 기본값은 240입니다.
- **Retransmission Pacing(**재전송 속도**)** - 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5밀리초 ~ 200밀리초입니다. 기본값은 66밀리초입니다.
- **Throttle Initial(**제한 초기**)** - LSA의 첫 번째 어커런스를 생성하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. 기본값은 0밀리초입니다. 최소값은 동일한 LSA를 시작하는 데 필요한 최소 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다. 최대값은 동일한 LSA를 시작하는 데 필요한 최대 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다.

  참고 LSA 제한의 경우 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3이 첫 번째 어커런스 값으로 자동으로 수정됩니다. 마찬가지로 지정된 최대 지연 시간이 최소 지연 시간보다 작으면 OSPFv3이 최소 지연 시간 값으로 자동으로 수정됩니다.

- **SPF Throttle(SPF** 제한**)** - SPF 계산의 변경 사항을 수신하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다. 최소값은 첫 번째와 두 번째 SPF 계산 사이의 지연 시간을 밀리초 단위로 지정합니다. 기본값은 10000밀리초입니다. 최대값은 SPF 계산에 소요되는 최대 대기 시간을 밀리초 단위로 지정합니다. 기본값은 10000밀리초입니다.

  참고 SPF 제한의 경우, 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3에서 첫 번째 어커런스 값을 자동으로 수정합니다. 마찬가지로 지정된 최대 지연 시간이 최소 지연 시간보다 작으면 OSPFv3이 최소 지연 시간 값으로 자동으로 수정됩니다.

단계 **10** **OK(**확인**)**를 클릭하여 LSA 타이머 구성을 저장합니다.

단계 **11** **Non Stop Forwarding(**무제한 전달**)**을 선택하고 **Enable graceful-restart helper(Graceful-Restart** 헬퍼 활성화**)** 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다. NSF 인식 디바이스에서 Graceful-Restart 헬퍼 모드를 비활성화하려면 이 확인란의 선택을 취소합니다.

단계 **12** **Enable link state advertisement(**링크 상태 알림 활성화**)** 확인란을 선택하여 strict 링크 상태 알림 확인을 활성화합니다.

이를 활성화하면 재시작 라우터에 플러딩되는 LSA의 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다.

단계 **13** **Enable graceful-restart (Use when Spanned Cluster or Failover Configured)(**스팬 클러스터 또는 페일오버가 구성된 경우 사용**)** 확인란을 선택하고 Graceful Restart 간격을 초 단위로 입력합니다. 범위는 1~1800입니다. 기본값은 120초입니다. 재시작 간격이 30초 미만일 경우 Graceful Restart가 종료됩니다.

단계 **14** **OK(**확인**)**를 클릭하여 Graceful Restart 구성을 저장합니다.

단계 **15** Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

40 장

Firepower Threat Defense BGP

이 섹션에서는 BGP(Border Gateway Protocol)를 이용하여 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 FTD를 구성하는 방법을 설명합니다.

- BGP 소개, 1073 페이지
- BGP 요구 사항 및 사전 요건, 1076 페이지
- BGP를 위한 지침, 1077 페이지
- BGP 구성, 1077 페이지

BGP 소개

BGP는 자율 시스템 간 라우팅 프로토콜과 자율 시스템 내부 라우팅 프로토콜입니다. 자율 시스템은 공통 관리와 공통 라우팅 정책에 따르는 네트워크 또는 네트워크 그룹입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다.

라우팅 테이블 변경 사항

네이버 간 TCP 연결이 처음 설정되면 BGP 네이버가 전체 라우팅 정보를 교환합니다. 라우팅 테이블 변경 사항이 감지되면 BGP 라우터가 변경된 경로만 네이버로 전송합니다. BGP 라우터는 주기적인 라우팅 업데이트를 전송하지 않고 BGP 라우팅 업데이트는 목적지 네트워크로의 최적의 경로만 알립니다.

참고 AS 루프 탐지는 전체 AS 경로를 검사하고(AS_PATH 특성에 지정된대로) 로컬 시스템의 AS 번호가 AS 경로에 나타나지 않는지 확인하여 수행됩니다. 기본적으로 EBGP는 학습된 경로를 동일한 피어에 알려서 루프 확인을 수행하는 데 있어 ASA의 추가 CPU 주기를 방지하고 기존 발신 업데이트 작업의 지연을 방지합니다.

BGP를 통해 학습된 경로에는 특정 목적지로 향하는 경로가 여럿일 때 최적의 경로를 결정하는 데 사용되는 속성이 포함되어 있습니다. 이러한 속성을 BGP 속성이라고 하며 경로 선택 과정에서 사용됩니다.

- Weight — 이는 Cisco가 정의한 라우터에 대한 로컬 속성입니다. 가중치 속성은 주변의 라우터에 알려지지 않습니다. 라우터가 동일한 목적지에 대하여 하나 이상의 경로를 학습한 경우 가중치가 가장 높은 경로가 우선합니다.
- Local preference — 로컬 기본 설정 속성은 로컬 AS로부터 출구 지점을 선택하는 데 사용됩니다. 가중치 속성과 달리 로컬 우선 속성은 로컬 AS 전체에 걸쳐 전파됩니다. AS에서 출구 지점이 여럿인 경우 로컬 우선 속성이 가장 높은 출구 지점이 특정 경로에 대한 출구 지점으로 사용됩니다.
- Multi-exit discriminator — MED(multi-exit discriminator) 또는 메트릭 속성은 메트릭에 알려지는 AS로의 우선 경로에 관한 외부 AS에 대한 제안으로 사용됩니다. MED를 수신하는 외부 AS가 경로 선택을 위해 다른 BGP 속성을 사용할 수도 있기 때문에 제안이라고 하는 것입니다. MED 메트릭이 낮은 경로가 우선합니다.
- Origin — 발신지 속성은 BGP가 특정 경로에 관해 어떻게 확인하는지 나타냅니다. 발신지 속성은 3가지 값을 가질 수 있으며 경로 선택에 사용됩니다.
  - IGP — 경로가 발신 AS 내부에 있습니다. 이 값은 경로를 BGP로 삽입하기 위해 네트워크 라우터 구성 명령을 사용할 때 설정됩니다.
  - EGP — 경로는 EBGP(Exterior Border Gateway Protocol)를 통해 확인됩니다.
  - Incomplete — 경로의 발신지가 알 수 없거나 확인되지 않았습니다. 경로가 BGP로 재배포되면 불완전한 발신지가 됩니다.
- AS_path — 경로 알림이 자율 시스템을 통과할 때 경로가 전달된 AS 번호의 주문 목록에 AS 번호가 추가됩니다. 가장 짧은 AS_path 목록을 가진 경로만 IP 라우팅 테이블에 설치됩니다.
- Next hop — EBGP next-hop 속성은 전달되는 라우터에 도달하기 위해 사용되는 IP 주소입니다. EBGP 피어의 경우 next-hop 주소는 피어 간 연결의 IP 주소입니다. IBGP의 경우 EBGP next-hop 주소가 로컬 AS로 전달됩니다.
- Community — 커뮤니티 속성은 라우팅 결정(허용, 우선, 재배포)을 적용할 수 있는 커뮤니티라는 대상 그룹화 방법을 제공합니다. 경로 맵은 커뮤니티 속성을 설정하는 데 사용됩니다. 미리 정의된 커뮤니티 속성은 다음과 같습니다.
  - no-export — 이 경로를 EBGP 피어에게 알리지 않습니다.
  - no-advertise — 이 경로를 어느 피어에게도 알리지 않습니다.
  - internet — 이 경로를 인터넷 커뮤니티에 알립니다. 네트워크의 모든 라우터가 여기 포함됩니다.

BGP를 사용해야 하는 시기

대학 및 기업과 같은 고객 네트워크는 일반적으로 네트워크 내 라우팅 정보 교환을 위해 OSPF와 같은 IGP(Interior Gateway Protocol)를 활용합니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. AS(autonomous system) 사이에서 BGP가 사용될 때 이 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때의 프로토콜은 IBGP(Interior BGP)라고 합니다.

BGP를 IPv6 네트워크를 통해 IPv6 접두사를 위한 라우팅 정보를 전달하는 데도 사용할 수 있습니다.

BGP 경로 선택

BGP는 같은 경로에 대해 서로 다른 소스로부터 여러 공지를 수신할 수 있습니다. BGP는 최적의 경로로 하나의 경로만 선택합니다. 이 경로가 선택된 경우 BGP는 선택된 경로를 IP 라우팅 테이블에 놓고 네이버에 전파합니다. BGP는 제시된 순서대로 다음 기준에 따라 목적지에 대한 경로를 선택합니다.

- 경로가 접근할 수 없는 next hop을 지정하면 업데이트를 삭제합니다.
- 가중치가 가장 높은 경로가 우선합니다.
- 가중치가 동일한 경우 로컬 우선이 가장 높은 경로가 우선합니다.
- 로컬 우선이 동일한 경우 이 라우터에서 실행 중인 BGP에서 발생한 경로가 우선합니다.
- 경로가 시작되지 않은 경우 AS_path가 가장 짧은 경로가 우선합니다.
- 모든 경로의 AS_path 길이가 같은 경우 발신지 유형이 가장 낮은 경로(IGP가 EGP보다 낮고 EGP가 incomplete보다 낮은 경로)가 우선합니다.
- 발신지 코드가 동일한 경우 MED 속성이 가장 낮은 경로가 우선합니다.
- MED가 같은 경로의 경우 내부 경로보다 외부 경로가 우선합니다.
- 그래도 경로가 동일한 경우 가장 가까운 IGP 네이버를 통한 경로가 우선합니다.
- 여러 경로에 BGP 다중 경로, 1075 페이지에 대한 라우팅 테이블에서의 설치 작업이 필요한지 결정합니다.
- 두 경로 모두 외부인 경우 먼저 수신된 경로가 우선합니다(오래된 경로).
- BGP 라우터 ID가 지정한 대로 IP 주소가 가장 낮은 경로가 우선합니다.
- 여러 경로의 발신자 또는 라우터 ID가 동일할 경우 클러스터 목록 길이가 가장 짧은 경로가 우선합니다.
- 가장 낮은 네이버 주소에서 시작하는 경로가 우선합니다.

BGP 다중 경로

BGP 다중 경로를 사용하면 동일한 대상 접두사에 대해 비용이 동일한 여러 BGP 경로의 IP 라우팅 테이블에 설치할 수 있습니다. 그러면 대상 접두사에 대한 트래픽이 모든 설치된 경로에서 공유됩니다.

이러한 경로는 로드 공유에 최적의 경로와 함께 테이블에 설치됩니다. BGP 다중 경로는 최적의 경로를 선택할 때는 영향을 주지 않습니다. 예를 들어, 라우터는 알고리즘에 따라 경로 중 하나를 계속해서 최적의 경로로 지정하고 BGP 피어에 이 최적의 경로를 알립니다.

다중 경로의 후보가 되려면 동일한 대상에 대한 경로에 최적의 경로 특성과 동일한 다음 특성이 있어야 합니다.

- 무게

- 로컬 기본 설정
- AS-PATH 길이
- 출처 코드
- MED(Multi Exit Discriminator)
- 다음 중 하나입니다.
  - 네이버 AS 또는 하위-AS(BGP 다중 경로 추가 전)
  - AS-PATH(BGP 다중 경로 추가 후)

일부 BGP 다중 경로 기능은 다중 경로 후보에게 다음과 같은 추가 요구 사항을 제시합니다.

- 경로는 외부 또는 연합-외부 네이버(eBGP)에서 확인되어야 합니다.
- BGP next hop에 대한 IGP 메트릭은 최적의 경로 IGP 메트릭과 동일해야 합니다.

다음은 내부 BGP(iBGP) 다중 경로 후보에 대한 추가 요구 사항입니다.

- 경로는 내부 네이버(iBGP)에서 확인되어야 합니다.
- 라우터가 동일하지 않은 비용의 iBGP 다중 경로에 대해 구성되지 않은 경우 BGP next hop에 대한 IGP 메트릭은 최적의 경로 IGP 메트릭과 동일해야 합니다.

BGP는 다중 경로 후보에서 가장 최근에 수신한 경로를 최대 *n*개까지 IP 라우팅 테이블에 삽입합니다. 이때 *n*은 라우팅 테이블에 설치할 경로의 수이며 BGP 다중 경로를 구성할 때 지정된 수입니다. 다중 경로가 비활성화된 경우 기본값은 1입니다.

비용이 동일하지 않은 로드 밸런싱에 BGP 링크 대역폭을 사용할 수도 있습니다.

참고 동일한 next-hop-self는 내부 피어에 전달되기 전에 eBGP 다중 경로 중에서 선택된 최적의 경로에서 수행됩니다.

BGP 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

BGP를 위한 지침

방화벽 모드 지침

투명한 방화벽 모드를 지원하지 않습니다. BGP는 라우티드 모드에서만 지원됩니다.

IPv6 지침

IPv6를 지원합니다. IPv6 주소군에 대해서는 graceful restart가 지원되지 않습니다.

가상 라우터 지침

BGP IPv4는 전역 및 사용자 정의 가상 라우터 모두에서 지원됩니다. 그러나 전역 가상 라우터에서는 BGP IPv6 구성만 지원됩니다.

추가 지침

- 시스템은 CP 경로 테이블에서 PPPoE를 통해 수신된 IP 주소에 대한 경로 항목을 추가하지 않습니다. BGP는 항상 TCP 경로 테이블에서 TCP 세션 시작을 확인하므로 BGP는 TCP 세션을 형성하지 않습니다.

  따라서 PPPoE를 통한 BGP는 지원되지 않습니다.
- 경로 업데이트가 링크의 최소 MTU보다 큰 경우 경로 업데이트가 삭제되어 인접성 플랩이 발생하지 않도록 하려면 링크의 양쪽에 있는 인터페이스에서 동일한 MTU를 구성해야 합니다.

BGP 구성

BGP를 구성하려면 다음 주제를 참조하십시오.

프로시저

단계 **1** BGP 기본 설정 구성, 1078 페이지
단계 **2** SNMP 일반 설정 구성, 1080 페이지
단계 **3** BGP 네이버 설정 구성, 1082 페이지
단계 **4** BGP 집계 주소 설정, 1086 페이지
단계 **5** BGPv4 필터링 설정, 1087 페이지

참고 필터링 섹션은 IPv4 설정에만 적용됩니다.

단계 **6** BGP 네트워크 설정, 1087 페이지
단계 **7** BGP 재배포 설정, 1088 페이지
단계 **8** BGP 라우트 삽입 설정, 1089 페이지

BGP 기본 설정 구성

BGP에 대한 많은 기본 설정을 구성할 수 있습니다.

가상 라우팅을 사용하는 디바이스의 경우, 이 섹션에 설명된 기본 설정이 **General Settings(**일반 설정**)**의 **BGP**페이지에 구성되어 있어야 합니다. 자세한 내용은 FMC 웹 인터페이스 라우팅 페이지에 대한 수정 사항, 995 페이지를 참고하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 선택합니다.

단계 **3** (가상 라우터 인식 디바이스의 경우) **General Settings(**일반 설정**)**에서 **BGP**를 클릭합니다.

단계 **4** BGP 라우팅 프로세스를 활성화하려면 **Enable BGP(BGP** 활성화**)** 확인란을 선택합니다.

단계 **5** **AS Number(AS** 번호**)** 필드에 BGP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호는 내부에 여러 자율 번호를 포함합니다. AS 번호는 1~4294967295 또는 1.0~65535.65535가 될 수 있습니다. AS 번호는 인터넷에서 각 네트워크를 식별하는 고유 할당 값입니다.

단계 **6** (선택 사항) **General(**일반**)**부터 시작하여 다양한 BGP 설정을 편집합니다. 이러한 설정의 기본값은 대부분의 경우에 적합하지만 네트워크의 필요에 맞게 조정할 수 있습니다. 그룹의 설정을 편집하려면 **Edit(**편집**)**(연필)을 클릭합니다.

a) **Router ID(**라우터 **ID)** 드롭다운 목록에서 Automatic(자동) 또는 Manual(수동)을 선택합니다. Automatic(자동)을 선택하면 Firepower Threat Defense 디바이스의 최상위 IP 주소가 라우터 ID로 사용됩니다. 고정된 라우터 ID를 사용하려면 Manual(수동)을 선택하고 **IP Address(IP** 주소**)** 필드에 IPv4 주소를 입력합니다. 기본값은 Automatic(자동)입니다. 가상 라우터 인식 디바이스의 경우, **Virtual Routers(**가상 라우터**)** > **BGP** 페이지에서 라우터 ID 설정을 재정의할 수 있습니다.

b) **AS_PATH** 속성에 **AS** 번호의 수를 입력합니다. AS _PATH 경로 속성은 소스와 대상 라우터 간 AS 번호 시퀀스로 패킷이 이동할 방향을 형성합니다. 유효한 값은 1~254입니다. 기본값은 None(없음)입니다.

c) **Log Neighbor Changes(**인접 네이버 변경사항**)** 확인란을 선택하여 BGP 네이버 변경사항(증가 또는 감소)과 재설정에 대한 로깅을 활성화합니다. 이는 네트워크 연결 문제 해결과 네트워크 안정성 측정에 도움이 됩니다. 기본적으로 활성화되어 있습니다.

d) **Use TCP Path MTU Discovery(TCP** 경로 **MTU** 검색 사용**)** 확인란을 선택하고 Path MTU 기술을 사용하여 두 IP 호스트 간 네트워크 경로에서 MTU(maximum transmission unit) 크기를 결정합니다. 이는 IP 단편화를 방지합니다. 기본적으로 활성화되어 있습니다.

e) **Reset session upon Failover(**장애 조치 시 세션 재설정**)** 확인란을 선택하여 링크 장애 시 즉시 외부 BGP 세션을 재설정합니다. 기본적으로 활성화되어 있습니다.

f) **Enforce that first AS is peer's AS for EBGP routes(**첫 번째 **AS**를 **EBGP** 경로에 대한 피어 **AS**로 적용**)** 확인란을 선택하여 AS 번호를 AS_PATH 속성의 첫 번째 세그먼트로 나열하지 않는 외부 BGP 피어에서 수신되는 업데이트를 버립니다. 이는 잘못 구성되거나 권한이 없는 피어가 마치 다른 자율 시스템에서 소싱된 것처럼 경로를 알림으로써 트래픽을 잘못 안내하지 않도록 예방합니다. 기본적으로 활성화되어 있습니다.

g) **Use dot notation for AS number(AS** 번호에 대해 점 표기법 사용**)** 확인란을 선택하여 전체 2진 4바이트 AS 번호를 각각 16비트의 두 단어로 마침표로 구분하여 나눕니다. 0 ~ 65553의 AS 번호는 10진수로 표시되고 65535보다 큰 AS 번호는 마침표를 통해 표시됩니다. 기본적으로 비활성화되어 있습니다.

h) **OK(**확인**)**를 클릭합니다.

단계 **7** (선택 사항) **Best Path Selection(**최적의 경로 선택**)** 섹션을 편집합니다.

a) **Default Local Preference(**기본 로컬 환경설정**)**을 0~4294967295 사이의 값으로 입력합니다. 기본값은 100입니다. 값이 높을수록 우선순위가 높습니다. 이 우선 값은 로컬 자율 시스템의 모든 라우터와 액세스 서버로 전송됩니다.

b) **Allow comparing MED from different neighbors(**다른 네이버의 **MED** 비교 허용**)** 확인란을 선택하여 서로 다른 자율 시스템의 네이버로부터 경로에 대한 MED(Multi Exit Discriminator)를 비교합니다. 기본적으로 비활성화되어 있습니다.

c) **Compare Router ID for identical EBGP paths(**동일 **EBGP** 경로의 라우터 **ID** 비교**)** 확인란을 선택하여 최적의 경로 선택 과정 중 외부 BGP 피어에서 수신된 비슷한 경로를 비교하고 최적의 경로를 라우터 ID가 가장 낮은 경로로 전환합니다. 기본적으로 비활성화되어 있습니다.

d) **Pick the best MED path among paths advertised from the neighboring AS(**인접 디바이스 **AS**에서 알려진 경로 중에 최적의 **MED** 경로 선택**)** 확인란을 선택하여 연합 피어에서 학습된 경로 간 MED 비교를 활성화합니다. MED 간 비교는 경로에 외부 자율 시스템이 없는 경우에만 이루어집니다. 기본적으로 비활성화되어 있습니다.

e) **Treat missing MED as the least preferred one(**누락된 **MED**를 최하위 순위로 처리**)** 확인란을 선택하여 누락 MED 속성 값을 무한으로 간주하고 이 경로를 최하위 순위로 만듭니다. 따라서 MED가 없는 경로가 최하위 순위가 됩니다. 기본적으로 비활성화되어 있습니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **8** (선택 사항) **Neighbor Timers(**네이버 타이머**)** 섹션을 편집합니다.

a) **Keepalive interval(Keepalive** 간격**)** 필드에 keepalive 메시지를 보내지 않은 후 BGP 네이버가 활성 상태를 유지하는 시간 간격을 입력합니다. 이 keepalive 간격이 지나면 전송된 메시지가 없는 경우 BGP 피어가 데드로 선언됩니다. 기본값은 60초입니다.

b) **Hold Time(**보류 시간**)** 필드에 BGP 연결이 개시 및 구성되는 동안 BGP 네이버가 활성 상태를 유지할 시간 간격을 입력합니다. 기본값은 180초입니다.

c) (선택 사항)**Min Hold Time(**최소 보류 시간**)** 필드에 BGP 연결이 개시 및 구성되는 동안 BGP 네이버가 활성 상태를 유지할 최소 시간 간격을 입력합니다. 0 ~ 65535 범위의 값을 지정합니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **9** (선택 사항) **Graceful Restart** 섹션을 편집합니다.

참고 이 섹션은 Firepower Threat Defense 디바이스가 페일오버 또는 스팬 클러스터 모드인 경우에만 사용할 수 있습니다. 이렇게 하면 페일오버 설정에 있는디바이스가 실패할 때 트래픽 흐름에서 패킷이 손실되지 않습니다.

a) **Enable Graceful Restart(Graceful Restart** 활성화**)** 확인란을 선택하여 FTD 피어가 전환 후 라우팅 플랩을 피할 수 있도록 합니다.

b) **Restart Time(**재시작 시간**)** 필드에 BGP 오픈 메시지를 수신하기 전에 이전 경로를 삭제하기까지 FTD 피어가 기다릴 시간을 지정합니다. 기본값은 120초입니다. 유효한 값은 1 ~ 3600초입니다.

c) **Stalepath Time(**오래된 경로 시간**)** 필드에 재시작하는 FTD에서 EOR(end of record) 메시지가 접수된 후 이전 경로를 삭제하기 전에 FTD에서 대기할 시간을 입력합니다. 기본값은 360초입니다. 유효한 값은 1 ~ 3600초입니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

단계 **11** BGP 기본 설정을 보려면 Virtual routers(가상 라우터) 드롭다운에서 원하는 라우터를 선택한 다음 **BGP**를 클릭합니다.

이 페이지에는 **Settings(**설정**)** 페이지에 구성된 기본 설정이 표시됩니다. 이 페이지에서 라우터 ID 설정을 편집할 수 있습니다.

단계 **12** 라우터 ID 설정을 편집하려면 **IP Address(IP** 주소**)** 필드에서 IP 주소를 수정합니다. 수정된 값이 **General Settings(**일반 설정**)**의 **BGP** 페이지에 구성된 라우터 ID 설정을 재정의합니다.

SNMP 일반 설정 구성

경로 맵, 관리 경로 거리, 동기화, Next-hop 및 패킷 전달을 구성합니다. 이러한 설정의 기본값은 대부분의 경우에 적합하지만 네트워크의 필요에 맞게 조정할 수 있습니다.

프로시저

단계 **1** **Device Management(**디바이스 관리**)** 페이지에서 **Routing(**라우팅**)**을 클릭합니다.

단계 **2** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운에서 BGP를 구성할 가상 라우터를 선택합니다.

단계 **3** **BGP** > **IPv4** 또는 **IPv6**을 선택합니다.

참고 IPv6 주소군을 이용한 BGP 구성은 사용자 정의 가상 라우터에서 지원되지 않습니다. 따라서 사용자 정의 가상 라우터를 선택할 경우 **IPv4** 설정만 사용할 수 있습니다.

단계 **4** **General(**일반**)**을 클릭합니다.

단계 **5** **General(**일반**)**에서 다음 섹션을 업데이트합니다.

a) **Settings(**설정**)** 섹션에서 **Route Map** 개체를 입력하거나 선택하고 next-hop 확인을 위해 BGP 라우터의 **Scanning Interval(**검색 간격**)**을 입력합니다. 유효한 값은 5초 ~ 75초입니다. 기본값은 60입니다. **OK(**확인**)**를 클릭합니다.

참고 **Route Map(**경로 맵**)** 필드는 IPv4 설정에만 적용됩니다.

b) **Routes and Synchronization(**경로 및 동기화**)** 섹션에서 필요에 따라 다음을 업데이트하고 **OK(**확인**)**를 클릭합니다.

- (선택 사항) **Generate Default Routes(**기본 경로 생성**)** - 기본 정보 출처를 구성하려면 이 옵션을 선택합니다.
- (선택 사항) **Summarize subnet routes into network-level routes(**네트워크 레벨 경로로의 서브넷 경로 요약**)** - 서브넷 경로를 네트워크 레벨 경로로 자동 요약하도록 구성하려면 이 옵션을 선택합니다. 이 확인란은 IPv4 설정에만 적용됩니다.
- (선택 사항) **Advertise inactive routes(**비활성 경로 알림**)** - RIB(routing information base)에 설치되지 않은 경로를 알리려면 이 옵션을 선택합니다.
- (선택 사항) **Synchronise between BGP and IGP system(BGP**와 **IGP** 시스템 간 동기화**)** - BGP와 IGP(Interior Gateway Protocol) 시스템 간의 동기화를 사용하려면 이 옵션을 선택합니다. 일반적으로 BGP 스피커는 경로가 로컬이거나 IGP에 존재하지 않는 한 외부 네이버에 경로를 전달하지 않습니다. 이 기능을 사용하면 자동 시스템 내의 라우터 및 액세스 서버가 BGP에서 다른 자동 시스템에 사용할 수 있도록 지정하기 전에 경로를 가질 수 있습니다.
- (선택 사항) **Redistribute IBGP into IGP(IGP**로 **IBGP** 재배포**)** - OSPF와 같은 IGP(Interior Gateway Protocol)로 iBGP 재배포를 구성하려면 이 옵션을 선택합니다.

c) **Administrative Route Distances(**관리 경로 거리**)** 섹션에서 필요에 따라 다음을 업데이트하고 **OK(**확인**)**를 클릭합니다.

- **External(**외부**)** - 외부 BGP 경로를 위한 관리 거리를 입력합니다. 외부 자동 시스템에서 학습한 경로는 외부 경로입니다. 이 인수 값 범위는 1 ~ 255입니다. 기본값은 20입니다.
- **Internal(**내부**)** - 내부 BGP 경로를 위한 관리 거리를 입력합니다. 로컬 자동 시스템의 피어에서 학습한 경로는 내부 경로입니다. 이 인수 값 범위는 1 ~ 255입니다. 기본값은 200입니다.
- **Local(**로컬**)** - 로컬 BGP 경로를 위한 관리 거리를 입력합니다. 로컬 경로는 다른 프로세스에서 재배포되는 라우터나 네트워크에 대한 네트워크 라우터 구성 표시 명령을 통해 종종 백도어로 나열된 네트워크입니다. 이 인수 값 범위는 1 ~ 255입니다. 기본값은 200입니다.

d) **Next Hop** 섹션에서 선택적으로 **Enable address tracking(**주소 추적 활성화**)** 확인란을 선택하여 BGP next hop 주소 추적을 활성화하고 라우팅 테이블에 설치된 next hop 업데이트 경로의 검사 사이의 **Delay Interval(**지연 간격**)**을 입력합니다. **OK(**확인**)**를 클릭합니다.

참고 **Next Hop** 섹션은 IPv4 설정에만 적용됩니다.

e) **Forward Packets over Multiple Paths(**여러 경로를 통해 패킷 전달**)** 섹션에서 필요에 따라 다음을 업데이트하 고 **OK(**확인**)**를 클릭합니다.

- (선택 사항) **Number of Paths(**경로 개수**)** - 라우팅 테이블에 설치 가능한 Border Gateway Protocol 경로의 최대 수를 지정합니다. 값의 범위는 1~8입니다. 기본값은 1입니다.

- (선택 사항) **IBGP Number of Paths(IBGP** 경로 개수**)** - 라우팅 테이블에 설치 가능한 병렬 내부 Border Gateway Protocol(iBGP) 경로의 최대 수를 지정합니다. 값의 범위는 1~8입니다. 기본값은 1입니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

BGP 네이버 설정 구성

BGP 라우터는 업데이트를 교환하기 전에 각 피어와 연결해야 합니다. 이러한 피어를 BGP 네이버라고 합니다. Neighbor(네이버)를 사용하여 BGP IPv4 또는 IPv6 네이버 및 네이버 설정을 정의합니다. 디바이스에서 가상 라우터를 활성화한 경우 사용자 정의 가상 라우터에 대해서는 BGP IPv4 네이버만 정의할 수 있습니다. 그러나 전역 가상 라우터의 경우 BGP IPv6도 정의할 수 있습니다.

프로시저

단계 **1** Device Management(디바이스 관리) 페이지에서 **Routing(**라우팅**)**을 클릭합니다.

단계 **2** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운에서 BGP를 구성할 가상 라우터를 선택합니다.

단계 **3** **BGP** > **IPv4** 또는 **IPv6**을 선택합니다.

참고 IPv6 주소군을 이용한 BGP 구성은 사용자 정의 가상 라우터에서 지원되지 않습니다. 따라서 사용자 정의 가상 라우터를 선택할 경우 **IPv4** 설정만 사용할 수 있습니다.

단계 **4** **Neighbor(**인접 디바이스**)**를 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭하여 BGP 네이버 및 네이버 설정을 정의합니다.

단계 **6** BGP 네이버 **IP** 주소를 입력합니다. 이 IP 주소는 BGP 네이버 테이블에 추가됩니다.

단계 **7** BGP 네이버 인터페이스를 선택합니다.

참고 **Interface(**인터페이스**)** 필드는 IPv6 설정에만 적용됩니다. 가상 라우팅을 사용하는 디바이스의 경우 이 필드는 전역 가상 라우터에 대해서만 나타납니다. 또한 라우터에 속한 인터페이스만 드롭다운에 나열됩니다.

단계 **8** BGP 네이버가 속하는 자율 시스템을 **Remote AS(**원격 **AS)** 필드에 입력합니다.

단계 **9** **Enabled address(**주소 활성화**)** 확인란을 선택하여 BGP 네이버와의 통신을 활성화합니다. 추가 네이버 설정은 Enabled address(주소 활성화) 확인란이 선택된 경우에만 구성됩니다.

단계 **10** (선택 사항) **Shutdown administratively(**관리자 권한으로 종료**)** 확인란을 선택하여 네이버 또는 피어 그룹을 비활성화합니다.

단계 **11** (선택 사항) **Configure graceful restart(Graceful Restart** 설정**)** 확인란을 선택하여 이 네이버에 대한 BGP Graceful Restart 기능의 구성을 활성화합니다. 이 옵션을 선택한 후에는 Graceful Restart(페일오버/스팬 모드) 옵션을 사용하여 Graceful Restart가 이 네이버에 대해 활성화 또는 비활성화되어야 하는지 여부를 지정해야 합니다.

참고 Graceful Restart 필드는 IPv4 설정에만 적용됩니다.

단계 **12** (선택 사항) **BFD Fallover(BFD** 페일오버**)** 확인란을 선택하여 BGP에 대한 BFD 지원 설정을 활성화합니다. 이 선택은 BGP 네이버를 등록해 BFD에서 전달 경로 탐지 실패 메시지를 수신하게 합니다.

단계 **13** (선택 사항) BGP 네이버에 대한 설명을 **Description(**설명**)**에 입력합니다.

단계 **14** (선택 사항) **Filtering Routes(**경로 필터링**)**에서 필요에 따라 액세스 목록, 경로 맵, 접두사 목록 및 AS 경로 필터를 사용하여 BGP 네이버 정보를 배포합니다. 다음 섹션을 업데이트합니다.

a) 적절한 수신 또는 발신 **Access List(**액세스 목록**)**를 입력하거나 선택하여 BGP 네이버 정보를 배포합니다.

참고 액세스 목록은 IPv4 설정에만 적용됩니다.

b) (선택 사항) 적절한 수신 또는 발신 **Route Maps(**경로 맵**)**를 입력하거나 선택하여 수신 또는 발신 경로에 경로 맵을 적용합니다.

c) 적절한 수신 또는 발신 **Prefix List(**접두사 목록**)**를 입력하거나 선택하여 BGP 네이버 정보를 배포합니다.

d) 적절한 수신 또는 발신 **AS** 경로 필터를 입력하거나 선택하여 BGP 네이버 정보를 배포합니다.

e) **Limit the number of prefixes allowed from the neighbor(**네이버로부터 허용되는 접두사의 수 제한**)** 확인란을 선택하여 네이버에서 수신할 수 있는 접두사 수를 제어합니다.

- **Maximum Prefixes(**최대 접두사**)** 필드에 특정 네이버에서 허용할 최대 접두사 개수를 입력합니다.
- **Threshold Level(**임계값 레벨**)** 필드에 라우터가 경고 메시지 생성을 시작할 최대 비율을 입력합니다. 유효한 값은 1부터 100 사이의 정수입니다. 기본값은 75입니다.

f) **Control prefixes received from the peer(**피어에서 수신한 프리픽스 제어**)** 확인란을 선택하여 피어에서 수신된 접두사에 대한 추가 제어를 지정합니다. 다음 중 하나를 수행합니다.

- **Terminate peering when prefix limit is exceeded(**접두사 제한 초과 시 피어링 종료**)**를 선택하여 접두사 한도에 도달할 때 BGP 네이버 디바이스를 중단합니다. **Restart interval(**재시작 간격**)** 필드에 BGP 네이버가 재시작하는 간격을 지정합니다.
- **Give only warning message when prefix limit is exceeded(**접두사 제한 초과 시 경고 메시지만 표시**)**를 선택하여 최대 접두사 한도가 초과되었을 때 로그 메시지를 생성합니다. 여기에서는 BGP 네이버가 종료되지 않습니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **15** (선택 사항) **Routes(**경로**)**에서 기타 네이버 경로 매개변수를 지정합니다. 다음 업데이트를 계속 진행합니다.

a) **Advertisment Interval(**알림 간격**)** 필드에 BGP 라우팅 업데이트 전송 최소 간격(초)을 입력합니다. 유효한 값은 1~600입니다.

b) **Remove private AS numbers from outbound routing updates(**아웃바운드 라우팅 업데이트에서 비공개 **AS** 번호 삭제**)**를 선택하여 아웃바운드 경로에서 비공개 AS 번호를 알림에서 제외합니다.

c) **Generate default routes(**기본 경로 생성**)** 확인란을 선택하여 로컬 라우터가 기본 경로 0.0.0.0을 네이버로 전송하도록 허용합니다. **Route map(**경로 맵**)** 필드에서 경로 0.0.0.0의 조건부 삽입을 허용할 경로 맵을 입력하거나 선택합니다.

d) 조건부 알림 경로를 추가하려면 Add Row(행 추가) **+** 기호를 클릭합니다. Add Advertised Route(알림 경로 추가) 대화 상자에서 다음을 수행합니다.

1. exist 맵 또는 non-exist 맵의 조건을 충족할 경우 **Advertise Map(**알림 맵**)** 필드에서 경로 맵을 추가하거나 선택합니다.
2. **Exist Map**을 선택하고 경로 맵 개체 선택기에서 경로 맵을 선택합니다. 이 경로 맵을 BGP 테이블의 경로와 비교하여 경로 맵을 알릴지 결정합니다.
3. **Non-Exist Map**을 선택하고 경로 맵 개체 선택기에서 경로 맵을 선택합니다. 이 경로 맵을 BGP 테이블의 경로와 비교하여 경로 맵을 알릴지 결정합니다.
4. **OK(**확인**)**를 클릭합니다.

단계 **16** **Timers(**타이머**)**에서 **Set Timers for the BGP Peer(BGP** 피어에 대한 타이머 설정**)** 확인란을 선택하여 keepalive 빈도, 보류 시간 및 최소 보류 시간을 설정합니다.

- **Keepalive frequency(Keepalive** 빈도**)** - FTD 디바이스에서 네이버에 keepalive 메시지를 보내는 빈도(초)를 입력합니다. 유효한 값은 0 ~ 65535입니다. 기본값은 60초입니다.
- **Hold time(**보류 시간**)** - FTD 디바이스가 데드 피어를 선언하는 keepalive 메시지를 수신하지 않은 후 간격(초)을 입력합니다. 유효한 값은 0 ~ 65535입니다. 기본값은 180초입니다.
- **Min hold time(**최소 보류 시간**)** - FTD 디바이스가 데드 피어를 선언하는 keepalive 메시지를 수신하지 않은 후 최소 간격(초)을 입력합니다. 유효한 값은 0 ~ 65535입니다. 기본값은 0초입니다.

단계 **17** **Advanced(**고급**)**에서 다음을 업데이트합니다.

a) (선택 사항) **Enable Authentication(**인증 활성화**)**을 선택하여 두 BGP 피어 사이의 TCP 연결에 대한 MD5 인증을 활성화합니다.

1. **Enable Encryption(**암호화 활성화**)** 드롭다운 목록에서 암호화 유형을 선택합니다.
2. **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다. **Confirm(**확인**)** 필드에 비밀번호를 다시 입력합니다. 비밀번호는 대/소문자를 구분하며 service password-encryption 명령이 활성화된 경우 최대 25자, service password-encryption 명령이 활성화되지 않은 경우 최대 81자입니다. 첫 번째 문자는 숫자가 될 수 없습니다. 문자열은 공백을 포함하여 모든 영숫자 문자를 포함할 수 있습니다.

   참고 number-space-anything 형식의 비밀번호는 지정할 수 없습니다. 숫자 뒤에 공백이 오면 인증이 실패할 수 있습니다.

b) (선택 사항) 커뮤니티 속성을 BGP 네이버에 전송해야 한다고 지정하려면 **Send Communty attribute to this neighbor(**이 네이버에 커뮤니티 속성 보내기**)** 확인란을 선택합니다.

c) (선택 사항) **Use FTD as next hop for this neighbor(**네이버의 **next hop**으로 **FTD** 사용**)** 확인란을 선택하여 라우터를 BGP speaking 네이버 또는 피어 그룹을 위한 next-hop으로 구성합니다.

d) **Disable connection verification(**연결 확인 비활성화**)** 확인란을 선택하여 single hop으로 도달 가능하지만 루프백 인터페이스에 구성되어 있거나 직접 연결되지 않은 IP 주소로 구성된 eBGP 피어링 세션에 대한 연결 확인 프로세스를 비활성화합니다. 선택이 해제되면(기본값) eBGP 피어가 기본적으로 동일한 네트워크 세그먼트에 직접 연결되어 있는지 확인하기 위해 BGP 라우팅 프로세스는 single-hop eBGP 피어링 세션(TTL=254)의 연결을 확인합니다. 피어가 동일한 네트워크에 직접 연결되어 있지 않은 경우 연결 확인을 수행하면 피어링 세션의 연결이 차단됩니다.

e) **Allow connections with neighbor that is not directly connected(**직접 연결되지 않은 네이버로의 연결 허용**)**를 선택하여 직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시도합니다. (선택 사항) TTL(time-to-live)을 **TTL hops(TTL** 홉**)** 필드에 입력합니다. 유효한 값은 1~255입니다. **Limited number of TTL hops to neighbor(**네이버에 대한 제한된 **TTL** 홉 수**)**를 선택하여 BGP 피어링 세션을 보호합니다. eBGP 피어를 구분하는 최대 홉 수를 **TTL hops(TTL** 홉**)** 필드에 입력합니다. 유효한 값은 1 ~ 254입니다.

f) (선택 사항) **Use TCP MTU path discovery(TCP** 경로 **MTU** 검색 사용**)** 확인란을 선택하여 BGP 세션에 대한 TCP 전송 세션을 활성화합니다.

g) **TCP Transport Mode(TCP** 전송 모드**)** 드롭다운 목록에서 TCP 연결 모드를 선택합니다. 옵션은 Default(기본), Active(액티브) 또는 Passive(패시브)입니다.

h) (선택 사항) BGP 네이버 연결에 대한 **Weight(**가중치**)**를 입력합니다.

i) 드롭다운 목록에서 FTD 디바이스가 수락할 **BGP Version(BGP** 버전**)**을 선택합니다. 버전을 4로 설정하여 소프트웨어가 지정된 네이버에서 버전 4만 사용하도록 강제할 수 있습니다. 기본값은 버전 4를 사용하고 요청 시 동적으로 버전 2까지 사용할 수 있도록 하는 것입니다.

단계 **18** AS 마이그레이션이 고려되는 경우에만 **Migration(**마이그레이션**)**을 업데이트합니다.

참고 AS 마이그레이션 맞춤 설정은 전환이 완료된 후 제거되어야 합니다.

a) (선택 사항) **Customize the AS number for routes received from the neighbor(**네이버에서 수신한 경로에 대한 **AS** 번호 맞춤화**)** 확인란을 선택하여 eBGP 네이버에서 수신된 경로에 대한 AS_PATH 속성을 맞춤화합니다.

b) **Local AS Number(**로컬 **AS** 번호**)** 필드에 로컬 자율 시스템 번호를 입력합니다. 유효한 값은 1~4294967295 또는 1.0~65535.65535 사이의 유효한 자율 시스템 번호입니다.

c) (선택 사항) 로컬 AS 번호가 eBGP 피어에서 수신된 모든 경로 앞에 추가되지 않도록 하려면 **Do not prepend local AS number for routes received from neighbor(**네이버에서 수신한 경로에 로컬 **AS** 번호를 접두사로 붙이지 않음**)** 확인란을 선택합니다.

d) (선택 사항) 실제 자율 시스템 번호를 eBGP 업데이트의 로컬 자율 시스템 번호로 바꾸려면 **Replace real AS number with local AS number in routes received from neighbor(**네이버에서 수신한 경로에서 실제 **AS** 번호를 로컬 **AS** 번호로 대체**)** 확인란을 선택합니다. 로컬 BGP 라우팅 프로세스에서의 자동 시스템 번호는 접두사로 추가되지 않습니다.

e) (선택 사항) eBGP 네이버가 실제 자율 시스템 번호(로컬 BGP 라우팅 프로세스)를 사용하거나 로컬 자율 시스템 번호를 사용하여 피어 세션을 설정하도록 eBGP 네이버를 구성하려면 **Accept either real AS number or local AS number in routes received from neighbor(**네이버에서 수신한 경로에서 실제 **AS** 번호 또는 로컬 **AS** 번호 중 하나를 허용**)** 확인란을 선택합니다.

단계 **19** **OK(**확인**)**를 클릭합니다.

단계 **20** **Save(**저장**)**를 클릭합니다.

BGP 집계 주소 설정

BGP 네이버는 라우팅 정보를 저장하고 교환하며 더 많은 BGP 스피커가 구성되면 라우팅 정보의 양이 증가합니다. 경로 어그리게이션은 여러 경로의 속성을 결합하여 하나의 경로만 알리는 프로세스입니다. 종합 접두사는 CIDR(Classless Interdomain Routing) 원칙을 사용하여 연속 네트워크를 라우팅 테이블에 요약할 수 있는 하나의 클래스리스 IP 주소 집합으로 결합합니다. 결과적으로 더 적은 경로를 알리게 됩니다. Add/Edit Aggregate Address(종합 주소 추가/편집) 대화 상자를 사용하여 특정 경로의 집합을 하나의 경로로 정의합니다.

프로시저

단계 **1** Firepower Threat Defense 디바이스를 편집할 경우 **Routing(**라우팅**)**을 클릭합니다.

단계 **2** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운에서 BGP를 구성할 가상 라우터를 선택합니다.

단계 **3** **BGP** > **IPv4** 또는 **IPv6**을 선택합니다.

참고 IPv6 주소군을 이용한 BGP 구성은 사용자 정의 가상 라우터에서 지원되지 않습니다. 따라서 사용자 정의 가상 라우터를 선택할 경우 **IPv4** 설정만 사용할 수 있습니다.

단계 **4** **Add Aggregate Address(**종합 주소 추가**)**를 클릭합니다.

단계 **5** **Aggregate Timer(**종합 타이머**)** 필드에서 종합 타이머 값(초)을 입력합니다. 유효한 값은 0 또는 6과 60 사이의 모든 값입니다. 기본값은 30입니다.

단계 **6** **Add(**추가**)**를 클릭하고 **Add Aggregate Address(**종합 주소 추가**)** 대화 상자를 업데이트합니다.

a) **Network(**네트워크**)** - IPv4 주소를 입력하거나 원하는 네트워크/호스트 개체를 선택합니다.

b) **Attribute Map(**속성 맵**)** - (선택 사항) 종합 경로 속성 설정에 사용할 경로 맵 이름을 입력하거나 선택합니다.

c) **Advertise Map(**알림 맵**)** - (선택 사항) AS_SET 오리진 커뮤니티 생성을 위한 경로 선택에 사용할 경로 맵 이름을 입력하거나 선택합니다.

d) **Suppress Map(**억제 맵**)** - (선택 사항) 억제할 경로를 선택하는 데 사용되는 경로 맵을 입력하거나 선택합니다.

e) **Generate AS set path Information(AS** 설정 경로 정보 생성**)** - (선택 사항) 확인란을 선택하여 자율 시스템 설정 경로 정보 생성을 활성화합니다.

f) **Filter all routes from updates(**업데이트의 모든 경로 필터링**)** - (선택 사항) 확인란을 선택하여 업데이트의 보다 구체적인 모든 경로를 필터링합니다.

g) **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- BGPv4 설정의 경우 다음과 같이 진행합니다. BGPv4 필터링 설정, 1087 페이지
- BGPv6 설정의 경우 다음과 같이 진행합니다. BGP 네트워크 설정, 1087 페이지

BGPv4 필터링 설정

필터링 설정은 발신 BGP 업데이트에서 수신된 경로나 네트워크를 필터링하는 데 사용됩니다. 필터링은 라우터가 학습하거나 알리는 라우팅 정보를 제한하는 데 사용됩니다.

시작하기 전에

필터링은 BGP IPv4 라우팅 정책에만 적용 가능합니다.

프로시저

단계 **1** Device Management(디바이스 관리) 페이지에서 **Routing(**라우팅**)**을 클릭합니다.

단계 **2** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운에서 BGP를 구성할 가상 라우터를 선택합니다.

단계 **3** **BGP** > **IPv4**를 선택합니다.

단계 **4** **Filtering(**필터링**)**을 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭하고 **Add Filter(**필터 추가**)** 대화 상자를 업데이트합니다.

a) **Access List(**액세스 목록**)** - 라우팅 업데이트에서 어떤 네트워크를 수신하고 어떤 네트워크를 억제할지 정의하는 액세스 제어 목록을 선택합니다.

b) **Direction(**방향**)** - 필터를 인바운드 업데이트에 적용할지 아웃바운드 업데이트에 적용할지 지정하는 방향을 선택합니다.

c) **Protocol(**프로토콜**)** - (선택 사항) 필터링할 라우팅 프로세스(None(없음), BGP, Connected(연결됨), OSPF, RIP 또는 Static(정적))를 선택합니다.

d) **Process ID(**프로세스 **ID)** - (선택 사항) OSPF 라우팅 프로토콜의 프로세스 ID를 입력합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

BGP 네트워크 설정

네트워크 설정은 BGP 라우팅 프로세스 및 경로 맵을 통해 알릴 네트워크를 추가하는 데 사용됩니다. 이때 알릴 네트워크는 경로 맵을 검사하여 필터링됩니다.

프로시저

단계 **1** **Device Management(**디바이스 관리**)** 페이지에서 **Routing(**라우팅**)**을 클릭합니다.

단계 **2** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운에서 BGP를 구성할 가상 라우터를 선택합니다.

단계 **3** **BGP** > **IPv4** 또는 **IPv6**을 선택합니다.

참고 IPv6 주소군을 이용한 BGP 구성은 사용자 정의 가상 라우터에서 지원되지 않습니다. 따라서 사용자 정의 가상 라우터를 선택할 경우 **IPv4** 설정만 사용할 수 있습니다.

단계 **4** **Networks(**네트워크**)**를 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭하고 **Add Networks(**네트워크 추가**)** 대화 상자를 업데이트합니다.

a) **Network(**네트워크**)** - BGP 라우팅 프로세스가 알릴 네트워크를 입력합니다.

b) (선택 사항) **Route Map(**경로 맵**)** - 알릴 네트워크를 필터링하기 위해 검사해야 할 경로 맵을 입력하거나 선택합니다. 지정하지 않으면 모든 네트워크를 재배포합니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

BGP 재배포 설정

재배포 설정을 통해 다른 라우팅 도메인의 경로로부터 BGP로 재배포하는 조건을 정의하기 위한 단계를 설명할 수 있습니다.

프로시저

단계 **1** **Device Management(**디바이스 관리**)** 페이지에서 **Routing(**라우팅**)**을 클릭합니다.

단계 **2** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운에서 BGP를 구성할 가상 라우터를 선택합니다.

단계 **3** **BGP** > **IPv4** 또는 **IPv6**을 선택합니다.

참고 IPv6 주소군을 이용한 BGP 구성은 사용자 정의 가상 라우터에서 지원되지 않습니다. 따라서 사용자 정의 가상 라우터를 선택할 경우 **IPv4** 설정만 사용할 수 있습니다.

단계 **4** **Redistribution(**재배포**)**을 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭하고 **Add Redistribution(**재배포 추가**)** 대화 상자를 업데이트합니다.

a) **Source Protocol(**소스 프로토콜**)** - Source Protocol(소스 프로토콜) 드롭다운 목록에서 BGP 도메인으로 경로를 재배포할 프로토콜을 선택합니다.

참고 사용자 정의 가상 라우터는 RIP의 재배포 트래픽을 지원하지 않습니다.

b) **Process ID(**프로세스 **ID)** - 선택한 소스 프로토콜의 식별자를 입력합니다. OSPF 프로토콜에 적용됩니다. 가상 라우팅을 사용하는 디바이스의 경우 BGP 설정을 구성할 가상 라우터에 할당된 프로세스 ID가 이 드롭다운에 나열됩니다.

c) **Metric(**메트릭**)** - (선택 사항) 재배포된 경로에 대한 메트릭을 입력합니다.

d) **Route Map(**경로 맵**)** - 재배포할 네트워크를 필터링하기 위해 검사해야 할 경로 맵을 입력하거나 선택합니다. 지정하지 않으면 모든 네트워크를 재배포합니다.

e) **Match(**일치**)** - 하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하는 데 사용되는 조건입니다. 경로는 재분배하려고 선택한 조건과 일치해야 합니다. 다음과 같은 하나 이상

의 일치 조건을 선택할 수 있습니다. OSPF를 소스 프로토콜을 선택한 경우에 이 옵션이 활성화됩니다.

- 내부
- 외부 1
- 외부 2
- NSSA 외부 1
- NSSA 외부 2

f) **OK(**확인**)**를 클릭합니다.

BGP 라우트 삽입 설정

라우트 삽입 설정을 통해 BGP 라우팅 테이블에 조건부로 삽입할 경로를 정의하기 위한 단계를 설명할 수 있습니다.

프로시저

단계 **1** **Device Management(**디바이스 관리**)** 페이지에서 **Routing(**라우팅**)**을 클릭합니다.

단계 **2** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운에서 BGP를 구성할 가상 라우터를 선택합니다.

단계 **3** **BGP** > **IPv4** 또는 **IPv6**을 선택합니다.

참고 IPv6 주소군을 이용한 BGP 구성은 사용자 정의 가상 라우터에서 지원되지 않습니다. 따라서 사용자 정의 가상 라우터를 선택할 경우 **IPv4** 설정만 사용할 수 있습니다.

단계 **4** **Route Injection(**경로 삽입**)**을 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭하고 **Add Route Injection(**라우트 삽입 추가**)** 대화 상자를 업데이트합니다.

a) **Inject Map(**삽입 맵**)** - 로컬 BGP 라우팅 테이블로 삽입할 접두사를 지정하는 경로 맵의 이름을 입력하거나 선택합니다.

b) **Exist Map(Exist** 맵**)** - BGP 스피커가 추적하는 접두사를 포함하는 경로 맵의 이름을 입력하거나 선택합니다.

c) **Injected routes will inherit the attributes of the aggregate route(**삽입된 경로가 종합 경로의 특성을 상속 받음**)** - 이 확인란을 선택하여 삽입된 경로가 종합 경로의 속성을 물려받도록 구성합니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

41 장

Firepower Threat Defense RIP

이 장에서는 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 RIP(Routing Information Protocol)를 사용하여 FTD를 구성하는 방법을 설명합니다. 가상 라우팅을 사용하는 디바이스의 경우 RIP는 전역 가상 라우터에만 구성할 수 있으며 사용자 정의 가상 라우터에는 구성할 수 없습니다.

- RIP 정보, 1091 페이지
- RIP에 대한 요구 사항 및 사전 요건, 1093 페이지
- RIP 가이드라인, 1093 페이지
- RIP 설정, 1094 페이지

RIP 정보

RIP(Routing Information Protocol)는 일반적으로 모든 라우팅 프로토콜 중에서 가장 오래 지속되는 프로토콜 중 하나입니다. RIP에는 라우팅 업데이트 프로세스, RIP 라우팅 메트릭, 라우팅 안정성 및 라우팅 타이머의 네 가지 기본 구성 요소가 있습니다. RIP를 지원하는 디바이스는 정기적인 간격으로 네트워크 토폴로지가 변경될 때 라우팅 업데이트 메시지를 전송합니다. 이러한 RIP 패킷에는 디바이스가 도달할 수 있는 네트워크 정보 및 패킷이 대상 주소에 도달하기 위해 통과해야 하는 라우터 또는 게이트웨이의 수가 포함됩니다. RIP는 OSPF보다 많은 트래픽을 생성하지만 더욱 쉽게 구성할 수 있습니다.

RIP는 경로 선택 항목을 메트릭으로 사용하는 거리 벡터 프로토콜입니다. 인터페이스에서 RIP가 활성화되면 해당 인터페이스는 인접 디바이스와 RIP 브로드캐스트를 교환하여 경로를 동적으로 학습하고 알립니다.

Firepower Threat Defense 디바이스에서는 RIP 버전 1과 RIP 버전 2를 모두 지원합니다. RIP 버전 1은 라우팅 업데이트를 통해 서브넷 마스크를 전송하지 않습니다. RIP 버전 2는 라우팅 업데이트를 통해 서브넷 마스크를 전송하고 가변 길이 서브넷 마스크를 지원합니다. 또한 RIP 버전 2는 라우팅 업데이트가 교환될 때 네이버 인증을 지원합니다. 이 인증은 Firepower Threat Defense 디바이스가 신뢰할 수 있는 소스에서 믿을 수 있는 라우팅 정보를 수신하도록 보장합니다.

RIP는 초기 구성이 간단하고 토폴로지가 변경될 때 구성을 업데이트할 필요가 없기 때문에 정적 경로에 비해 이점이 있습니다. RIP의 단점은 정적 라우팅보다 네트워크 및 처리 오버헤드가 많다는 것입니다.

라우팅 업데이트 프로세스

RIP는 정기적인 간격으로 네트워크 토폴로지가 변경될 때 라우팅 업데이트 메시지를 전송합니다. 라우터가 항목의 변경 사항을 포함하는 라우팅 업데이트를 수신하면 라우팅 테이블을 업데이트하여 새 경로를 반영합니다. 경로의 메트릭 값은 1이 증가하고 발신자는 next hop으로 표시됩니다. RIP 라우터는 최상의 경로(메트릭 값이 가장 낮은 경로)만 대상에 유지합니다. 라우팅 테이블을 업데이트한 후 라우터는 즉시 라우팅 업데이트 전송을 시작하여 다른 네트워크 라우터에 변경 사항을 알립니다. 이러한 업데이트는 RIP 라우터가 전송하는 정기적으로 예약된 업데이트와 별개로 전송됩니다.

RIP 라우팅 메트릭

RIP는 단일 라우팅 메트릭(홉 수)을 사용하여 소스 및 대상 네트워크 간의 거리를 측정합니다. 소스에서 대상까지의 경로에 있는 각 홉에는 홉 수 값이 할당되며 이는 일반적으로 1입니다. 라우터가 새 대상 네트워크 항목 또는 변경된 대상 네트워크 항목을 포함하는 라우팅 업데이트를 수신하면 라우터는 업데이트에 표시된 메트릭 값에 1을 더하고 라우팅 테이블에 네트워크를 입력합니다. 발신자의 IP 주소는 next hop으로 사용됩니다.

RIP 안정성 기능

RIP는 소스에서 대상까지 경로에 허용되는 홉 수에 대한 제한을 구현하여 라우팅 루프가 무기한 지속되지 않도록 방지합니다. 경로의 최대 홉 수는 15입니다. 라우터가 새 항목 또는 변경된 항목을 포함하는 라우팅 업데이트를 수신하고 메트릭 값을 1만큼 높여 메트릭이 무한대(16)가 되면 네트워크 대상이 도달할 수 없는 것으로 간주됩니다. 이 안정성 기능의 단점은 RIP 네트워크의 최대 직경을 16홉 미만으로 제한한다는 것입니다.

RIP에는 많은 라우팅 프로토콜에 공통적인 여러 다른 안정성 기능이 포함되어 있습니다. 이러한 기능은 네트워크 토폴로지의 급격한 변화에도 불구하고 안정성을 제공하도록 설계되었습니다. 예를 들어 RIP는 올바르지 않은 라우팅 정보가 전파되지 않도록 수평 분할(split horizon) 및 보류 메커니즘을 구현합니다.

RIP 타이머

RIP는 수많은 타이머를 사용하여 성능을 규제합니다. 여기에는 routing-update 타이머, route-timeout 타이머 및 route-flush 타이머가 포함됩니다. routing-update 타이머는 주기적인 라우팅 업데이트 간격을 측정합니다. 일반적으로 타이머가 재설정될 때마다 임의의 시간이 추가되어 30초로 설정됩니다. 이는 모든 라우터가 동시에 네이버 라우터를 업데이트하려고 시도할 때 발생할 수 있는 혼잡을 방지하는 데 도움이 됩니다. 각 라우팅 테이블 항목에는 route-timeout 타이머가 있습니다. route-timeout 타이머가 만료되면 경로가 무효로 표시되지만 route-flush 타이머가 만료될 때까지 테이블에 유지됩니다.

RIP에 대한 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

RIP 가이드라인

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

다음 정보는 RIP 버전 2에만 적용됩니다.

- 네이버 인증을 사용하는 경우 인터페이스에 RIP 버전 2 업데이트를 제공하는 모든 네이버 디바이스에서 인증 키와 키 ID가 동일해야 합니다.
- RIP 버전 2를 통해 Firepower Threat Defense 디바이스는 멀티캐스트 주소 224.0.0.9를 사용하여 기본 경로 업데이트를 전송하고 수신합니다. 패시브 모드에서는 해당 주소에서 경로 업데이트를 수신합니다.
- RIP 버전 2가 인터페이스에 구성되면 멀티캐스트 주소 224.0.0.9가 해당 인터페이스에 등록됩니다. RIP 버전 2 구성이 인터페이스에서 제거되면 해당 멀티캐스트 주소는 등록 취소됩니다.

제한 사항

- Firepower Threat Defense 디바이스는 인터페이스 간에 RIP 업데이트를 전달할 수 없습니다.
- RIP 버전 1은 가변 길이 서브넷 마스크를 지원하지 않습니다.
- RIP의 최대 홉 수는 15입니다. 홉 수가 15보다 큰 경로는 도달할 수 없는 것으로 간주됩니다.
- 통합 RIP는 다른 라우팅 프로토콜에 비해 상대적으로 느립니다.

• Firepower Threat Defense 디바이스에서 단일 RIP 프로세스만 활성화할 수 있습니다.

RIP 설정

RIP는 경로 선택 항목을 메트릭으로 사용하는 거리 벡터 프로토콜입니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 선택합니다.

단계 **3** 목차에서 **RIP**를 선택합니다.

단계 **4** RIP 설정을 구성하려면 **Enable RIP(RIP** 활성화**)** 확인란을 선택합니다.

단계 **5** **RIP Version(RIP** 버전**)** 드롭다운 목록에서 RIP 업데이트를 송수신하기 위한 RIP 버전을 선택합니다.

단계 **6** (선택 사항) 지정한 경로 맵에 따라 **Generate Default Route(**기본 경로 생성**)** 확인란을 선택하여 배포할 기본 경로를 생성합니다.

a) **Route Map(**경로 맵**)** 필드에서 기본 경로 생성에 사용할 경로 맵 이름을 지정합니다.
기본 경로 0.0.0.0/0은 **Route Map(**경로 맵**)** 필드에 지정된 경로 맵이 있을 때 특정 인터페이스를 통해 배포용으로 생성됩니다.

단계 **7** 송수신하기 위해 선택한 RIP 버전이 버전 2인 경우 **Enable Auto Summary(**자동 요약 활성화**)** 옵션을 사용할 수 있습니다. **Enable Auto Summary(**자동 요약 활성화**)** 확인란을 선택하는 경우 자동 경로 요약이 활성화되어 있습니다. 연결되지 않은 서브넷 간의 라우팅을 수행해야 하는 경우 자동 요약을 비활성화합니다. 자동 요약이 비활성화되면 서브넷이 알려집니다.

참고 RIP 버전 1은 항상 자동 요약 기능을 사용하므로 비활성화할 수 없습니다.

단계 **8** **Networks(**네트워크**)**를 클릭합니다. RIP 라우팅에 대 한 하나 이상의 네트워크를 정의 합니다. IP 주소를 입력하거나 원하는 네트워크/호스트 개체를 입력하거나 선택합니다. 보안 어플라이언스 구성에 추가할 수 있는 네트워크 수에는 제한이 없습니다. 이 명령으로 정의된 네트워크에 속하는 모든 인터페이스는 RIP 라우팅 프로세스에 참여합니다. RIP 라우팅 업데이트는 지정된 네트워크의 인터페이스를 통해서만 송수신됩니다. 또한, 인터페이스의 네트워크를 지정하지 않으면 RIP 업데이트가 인터페이스로 알려지지 않습니다.

참고 RIP는 IPv4 개체만 지원합니다.

단계 **9** (선택 사항) **Passive Interfaces(**패시브 인터페이스**)**를 클릭합니다. 어플라이언스에서 패시브 인터페이스를 지정하고 활성 인터페이스를 확장하려면 이 옵션을 사용합니다. 해당 디바이스는 패시브 인터페이스에서 RIP 라우팅 브로드캐스트를 수신하고 해당 정보를 사용하여 라우팅 테이블을 채우지만 패시브 인터페이스에서 라우팅 업데이트를 브로드캐스트 처리하지는 않습니다. 패시브로 지정되지 않은 인터페이스는 업데이트를 송수신합니다.

단계 **10** **Redistribution(**재배포**)**을 클릭하여 재배포 경로를 관리합니다. 이는 다른 라우팅 프로세스에서 RIP 라우팅 프로세스로 재배포되는 경로입니다.

a) 재분배 경로를 지정하려면 **Add(**추가**)**를 클릭합니다.
b) **Protocol(**프로토콜**)** 드롭다운 목록에서 RIP 라우팅 프로세스로 재배포할 라우팅 프로토콜을 선택합니다.

참고 OSPF 프로토콜에 대한 프로세스 ID를 지정합니다. 마찬가지로 BGP에 대한 AS 경로를 지정합니다. **Protocol(**프로토콜**)** 드롭다운 목록에서 Connected(연결됨) 옵션을 선택하면 직접 연결된 네트워크를 RIP 라우팅 프로세스로 재배포할 수 있습니다.

c) (선택 사항) OSPF 경로를 RIP 라우팅 프로세스로 재배포하는 경우 **Match(**일치**)** 드롭다운 목록에서 재배포할 OSPF 경로의 특정 유형을 선택할 수 있습니다. 다음과 같이 여러 유형을 선택하려면 ctrl 키를 클릭합니다.

- Internal – AS(Autonomous System) 내부의 경로가 재배포됩니다.
- External 1 - AS 외부의 유형 1 경로가 재배포됩니다.
- External 2 - AS 외부의 유형 2 경로가 재배포됩니다.
- NSSA External 1 - NSSA(not-so-stubby area) 외부의 유형 1 경로가 재배포됩니다.
- NSSA External 2 - NSSA 외부의 유형 2 경로가 재배포됩니다.

참고 기본값은 Internal, External 1 및 External 2와 일치합니다.

d) **Metric(**메트릭**)** 드롭다운 목록에서 재배포된 경로에 적용할 RIP 메트릭 유형을 선택합니다. 두 가지 선택 사항은 다음과 같습니다.

- Transparent(투명) – 현재 경로 메트릭을 사용합니다.
- Specified Value(지정된 값) - 특정 메트릭 값을 지정합니다. **Metric Value(**메트릭 값**)** 필드에 0~16 사이의 특정 값을 입력합니다.
- None(없음) - 메트릭이 지정되지 않습니다. 재배포된 경로에 적용하려면 메트릭 값을 사용하지 마십시오.

e) (선택 사항) 경로가 RIP 라우팅 프로세스로 재배포되기 전에 **Route Map(**경로 맵**)** 필드에 충족되어야 하는 경로 맵의 이름을 입력합니다. 경로는 IP 주소가 경로 맵 주소 목록의 allow 문과 일치하는 경우에만 재배포됩니다.
f) **OK(**확인**)**를 클릭합니다.

단계 **11** (선택 사항) RIP 정책에 대한 필터를 관리하려면 **Filtering(**필터링**)**을 클릭합니다. 이 섹션에서 필터는 인터페이스를 통한 라우팅 업데이트 방지, 라우팅 업데이트의 경로 알림 제어, 라우팅 업데이트 처리 및 라우팅 업데이트 소스 필터링에 사용됩니다.

a) **Add(**추가**)**를 클릭하여 RIP 필터를 추가합니다.
b) **Traffic Direction(**트래픽 방향**)** 필드에서 필터링할 트래픽 유형을 선택합니다(인바운드 또는 아웃바운드).

참고 트래픽 방향이 인바운드인 경우 인터페이스 필터만 정의할 수 있습니다.

c) **Filter On(**필터 켜기**)** 필드에서 해당 라디오 버튼을 선택하여 필터가 Interface(인터페이스) 또는 Route(경로) 기반인지 여부를 지정합니다. Interface(인터페이스)를 선택하는 경우 라우팅 업데이트를 필터링할 인터페이스의 이름을 입력하거나 선택합니다. Route(경로)를 선택하는 경우 경로 유형을 선택합니다.

- Static(정적) - 정적 경로만 필터링됩니다.
- Connected(연결됨) - 연결된 경로만 필터링됩니다.
- OSPF - 지정된 OSPF 프로세스에서 검색한 OSPFv2 경로만 필터링됩니다. 필터링할 OSPF 프로세스의 프로세스 ID를 입력합니다.
- BGP - 지정된 BGP 프로세스에서 검색한 BGPv4 경로만 필터링됩니다. 필터링할 BGP 프로세스의 AS 경로를 입력합니다.

d) **Access List(**액세스 목록**)** 필드에서 RIP 경로 알림에서 허용 또는 제거할 네트워크를 정의하는 하나 이상의 ACL(액세스 제어 목록)의 이름을 입력하거나 선택합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **12** (선택 사항) **Broadcast(**브로드캐스트**)**를 클릭하여 인터페이스 구성을 추가하거나 편집합니다. Broadcast(브로드캐스트)를 사용하여 인터페이스별로 전송 또는 수신할 전역 RIP 버전을 재정의할 수 있습니다. 인증을 구현하여 유효한 RIP 업데이트를 확인하려는 경우 인터페이스당 인증 파라미터를 정의할 수도 있습니다.

a) 인터페이스 구성을 추가하려면 **Add(**추가**)**를 클릭합니다.

b) **Interface(**인터페이스**)** 필드에서 이 어플라이언스에 정의된 인터페이스를 입력하거나 선택합니다.

c) Send(전송) 옵션에서 해당 상자를 선택하여 RIP **Version 1(**버전 **1)**, **Version 2(**버전 **2)**, 또는 둘 다를 사용하여 업데이트를 전송하도록 지정합니다. 이러한 옵션을 사용하면 지정된 인터페이스에 대해 지정된 전역 Send(전송) 버전을 재정의할 수 있습니다.

d) Receive(수신) 옵션에서 해당 상자를 선택하여 RIP **Version 1(**버전 **1)**, **Version 2(**버전 **2)**, 또는 둘 다를 사용하여 업데이트를 수락하도록 지정합니다. 이러한 옵션을 사용하면 지정된 인터페이스에 대해 지정된 전역 Receive(수신) 버전을 재정의할 수 있습니다.

e) RIP 브로드캐스트에 대해 이 인터페이스에서 사용되는 **Authentication(**인증**)**을 선택합니다.

- None(없음) - 인증 없음
- MD5 - MD5 사용
- Clear Text(일반 텍스트) - 사용할 일반 텍스트 인증

MD5 또는 Clear Text(일반 텍스트)를 선택하는 경우 다음 인증 파라미터도 제공해야 합니다.

- Key ID(키 ID) - 인증 키의 ID입니다. 유효한 값은 0 ~ 255입니다.
- Key(키) - 선택한 인증 방법에서 사용하는 키입니다. 최대 16자를 포함할 수 있습니다.
- Confirm(확인) - 확인을 위해 인증 키를 다시 입력합니다.

f) **OK(**확인**)**를 클릭합니다.

42 장

Firepower Threat Defense 멀티캐스트 라우팅

이 장에서는 멀티캐스트 라우팅 프로토콜을 사용하도록 Firepower Threat Defense 디바이스를 구성하는 방법을 설명합니다. 가상 라우팅을 사용하는 디바이스의 경우 RIP는 전역 가상 라우터에만 구성할 수 있으며 사용자 정의 가상 라우터에는 구성할 수 없습니다.

- 멀티캐스트 라우팅 정보, 1099 페이지
- 멀티캐스트 라우팅 요구 사항 및 사전 요건, 1103 페이지
- 멀티캐스트 라우팅 지침, 1104 페이지
- IGMP 기능 구성, 1104 페이지
- PIM 기능 구성, 1110 페이지
- 멀티캐스트 라우트 설정, 1116 페이지
- 멀티캐스트 경계 필터 설정, 1117 페이지

멀티캐스트 라우팅 정보

멀티캐스트 라우팅은 단일 정보 스트림을 수천 개의 기업 수신자와 가정으로 동시에 제공함으로써 트래픽을 줄이는 대역폭 절약 기술입니다. 멀티캐스트 라우팅을 활용하는 분야로는 화상 회의, 기업 통신, 원거리 학습, 소프트웨어 배포, 주식 시세 및 뉴스가 있습니다.

멀티캐스트 라우팅 프로토콜은 소스나 수신자에 추가적인 부담을 주지 않고 경쟁 기술 중에서도 가장 적은 네트워크 대역폭을 사용하여 소스 트래픽을 여러 수신자에게 보냅니다. 멀티캐스트 패킷은 PIM(Protocol Independent Multicast) 및 기타 지원 멀티캐스트 프로토콜로 활성화되는 Firepower Threat Defense 디바이스에 의해 네트워크에서 복제되어 여러 수신자에게 데이터를 가장 효율적으로 제공할 수 있습니다.

Firepower Threat Defense 디바이스는 stub 멀티캐스트 라우팅과 PIM 멀티캐스트 라우팅을 모두 지원합니다. 하지만 두 라우팅을 하나의 Firepower Threat Defense 디바이스에 동시에 구성할 수는 없습니다.

참고 멀티캐스트 라우팅에 대해 UDP 및 비 UDP 전송이 모두 지원됩니다. 그러나 비 UDP 전송에는 FastPath 최적화가 없습니다.

IGMP 프로토콜

IP 호스트가 IGMP(Internet Group Management Protocol)를 사용하여 그룹 멤버십을 직접 연결된 멀티캐스트 라우터로 보고합니다. IGMP는 특정 LAN의 멀티캐스트 그룹에서 개별 호스트를 동적으로 등록하는 데 사용됩니다. 호스트는 IGMP 메시지를 로컬 멀티캐스트 라우터로 전송함으로써 그룹 멤버십을 식별합니다. IGMP에서 라우터가 IGMP 메시지를 듣고 주기적으로 쿼리를 보내 특정 서브넷에서 어떤 그룹이 활성 상태이고 어떤 그룹이 비활성 상태인지 파악합니다.

IGMP는 그룹 주소(Class D IP 주소)를 그룹 식별자로 사용합니다. 호스트 그룹 주소 범위는 224.0.0.0 ~ 239.255.255.255입니다. 224.0.0.0 주소는 어떤 그룹에도 할당되지 않습니다. 224.0.0.1 주소는 서브넷의 모든 시스템에 할당됩니다. 224.0.0.2 주소는 서브넷의 모든 라우터에 할당됩니다.

참고 Firepower Threat Defense 디바이스에서 멀티캐스트 라우팅을 활성화할 경우 IGMP 버전 2가 모든 인터페이스에서 자동으로 활성화됩니다.

멀티캐스트 그룹으로의 쿼리 메시지

Firepower Threat Defense 디바이스는 쿼리 메시지를 보내 어떤 멀티캐스트 그룹이 인터페이스에 연결된 네트워크의 멤버인지 확인합니다. 멤버는 특정 그룹에 대한 멀티캐스트 패킷을 받고 싶다는 의미의 IGMP 보고 메시지로 응답합니다. 쿼리 메시지는 주소가 224.0.0.1이고 time-to-live 값이 1인 전체 시스템 멀티캐스트 그룹으로 전달됩니다.

이 메시지는 주기적으로 전송되어 Firepower Threat Defense 디바이스에 저장된 멤버십 정보를 새로 고침합니다. Firepower Threat Defense 디바이스가 아직 인터페이스에 연결된 멀티캐스트 그룹의 로컬 멤버가 없다고 확인하면 해당 그룹의 멀티캐스트 패킷을 연결된 네트워크로 더 이상 전달하지 않고 prune 메시지를 다시 패킷 소스로 전송합니다.

기본적으로 서브넷의 PIM 지정 라우터가 쿼리 메시지 전송을 담당합니다. 기본적으로 125초마다 한 번 전송됩니다.

쿼리 응답 시간을 변경할 경우 IGMP 쿼리에서 알려지는 최대 쿼리 응답 시간은 기본적으로 10초입니다. 이 시간 내에 Firepower Threat Defense 디바이스가 호스트 쿼리에 대한 응답을 받지 못하면 그 그룹이 삭제됩니다.

stub 멀티캐스트 라우팅

Stub 멀티캐스트 라우팅은 동적 호스트 등록을 제공하고 멀티캐스트 라우팅을 촉진합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 Firepower Threat Defense 디바이스는 IGMP 프록시 에이전트 역할을 합니다. 멀티캐스트 라우팅에 완전히 참여하는 대신 Firepower Threat Defense 디바이스는 IGMP 메시지를 업스트림 멀티캐스트 라우터로 전송하고 이 라우터가 멀티캐스트 데이터 전송을 설정합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 Firepower Threat Defense 디바이스는 PIM 스파스 또는 양방향 모드에 대해 구성될 수 없습니다. IGMP 스텁 멀티캐스트 라우팅에 참여 중인 인터페이스에서 PIM을 활성화해야 합니다.

Firepower Threat Defense 디바이스는 PIM-SM과 양방향 PIM을 모두 지원합니다. PIM-SM은 기본 유니캐스트 라우팅 정보 기반 또는 별도의 멀티캐스트 지원 라우팅 정보 기반을 사용하는 멀티캐스트

라우팅 프로토콜입니다. 또한 멀티캐스트 그룹당 단일 RP(랑데부 포인트)를 루트로 삼는 단방향 공유 트리를 구축하고 선택적으로 멀티캐스트 소스별로 최단 경로 트리를 생성합니다.

PIM 멀티캐스트 라우팅

양방향 PIM은 멀티캐스트 소스와 수신자를 연결하는 양방향 공유 트리를 구축하는 PIM-SM의 변형입니다. 양방향 트리는 멀티캐스트 토폴로지의 각 링크에서 작동하는 DF(Designated Forwarder) 선택 프로세스를 사용하여 구축됩니다. 멀티캐스트 데이터는 DF의 도움을 받아 소스에서 RP(랑데부 포인트)로 전달되고 따라서 소스별 상태 없이도 공유 트리에서 수신자를 따르게 됩니다. DF 선택은 RP 검색 중에 이루어지고 RP에 대한 기본 경로를 제공합니다.

참고 Firepower Threat Defense 디바이스가 PIM RP인 경우 Firepower Threat Defense 디바이스의 변환되지 않은 외부 주소를 RP 주소로 사용합니다.

PIM 소스별 멀티캐스트 지원

Firepower Threat Defense 디바이스는 PIM SSM(Source Specific Multicast) 기능 및 관련된 구성을 지원하지 않습니다. 그러나 Firepower Threat Defense 디바이스는 마지막 홉 라우터로 배치되는 경우를 제외하고 SSM 관련 패킷이 통과하도록 허용합니다.

SSM은 IPTV 같은 일대다 애플리케이션에 대한 데이터 전달 메커니즘으로 분류됩니다. SSM 모델은 (S,G) 쌍으로 표시된 "채널"의 개념을 사용하며, 여기서 S는 소스 주소이고 G는 SSM 대상 주소입니다. 채널 가입은 IGMPv3 같은 그룹 관리 프로토콜을 사용하여 수행됩니다. SSM이 특정 멀티캐스트 소스를 확인한 경우, 수신 클라이언트가 공유 RP(랑데부 포인트)에서 수신하는 대신 소스에서 직접 멀티캐스트 스트림을 수신하게 합니다. 액세스 제어 메커니즘은 현재 SM(Sparse Mode) 또는 SDM(Sparse-Dense Mode) 구현으로 사용할 수 없는 보안 향상을 제공하는 SSM 내에서 도입되었습니다.

PIM-SSM은 RP 또는 공유 트리를 사용하지 않는 점에서 PIM-SM과 다릅니다. 대신, 멀티캐스트 그룹의 소스 주소에 대한 정보가 IGMPv3(로컬 리시버십 프로토콜)를 통해 리시버에서 제공되고 소스별 트리를 직접 구축하는 데 사용됩니다.

멀티캐스트 양방향 PIM

멀티캐스트 양방향 PIM은 여러 소스와 수신자가 동시에 서로 통신하고 화상회의, Webex 회의 및 그룹 채팅에서 각 참가자가 멀티캐스트 트래픽의 소스 및 수신자가 될 수 있는 네트워크에 유용합니다. PIM 양방향 모드가 사용되면 RP는 공유 트리에 대해서만 (*, G) 항목을 만듭니다. (S, G) 항목은 없습니다. 각 (S, G) 항목의 상태 테이블이 유지되지 않으므로 RP에서 리소스가 보존됩니다.

PIM 스파스 모드에서 트래픽은 공유 트리 아래로만 흐릅니다. PIM 양방향 모드에서는 트래픽이 공유 트리의 위아래로 흐릅니다.

또한 PIM 양방향 모드는 PIM register/register-stop 메커니즘을 사용하여 소스를 RP에 등록하지 않습니다. 각 소스는 언제든지 소스로 전송을 시작할 수 있습니다. 멀티캐스트 패킷이 RP에 도착하면 공

유 트리(수신자가 있는 경우)로 전달되거나 삭제(수신자가 없는 경우)됩니다. 하지만 RP의 경우 소스에 멀티캐스트 트래픽 전송을 중지하도록 알릴 방법이 없습니다.

네트워크상의 소스와 수신자 사이의 중간에 RP가 있어야 하므로 RP의 위치를 생각해야 합니다.

PIM 양방향 모드에는 RPF(Reverse Path Forwarding) 확인이 없습니다. 대신 DF(Designated Forwarder) 개념을 사용하여 루프를 방지합니다. 이 DF는 멀티캐스트 트래픽을 RP에 전송할 수 있는 세그먼트의 유일한 라우터입니다. 멀티캐스트 트래픽을 전달하는 세그먼트당 하나의 라우터만 있으면 루프가 없습니다. DF는 다음 메커니즘을 사용하여 선택됩니다.

- RP에 가장 낮은 메트릭을 가진 라우터가 DF입니다.
- 메트릭이 동일한 경우 IP 주소가 가장 큰 라우터가 DF가 됩니다.

PIM BSR(부트스트랩 라우터)

PIM BSR(부트스트랩 라우터)은 그룹에 대해 RP 정보를 릴레이하기 위해, 그리고 RP 기능을 위해 후보 라우터를 사용하는 동적 RP(랑데부 포인트) 선택 모델입니다. RP 기능은 RP 검색을 포함하며 RP에 대한 기본 경로를 제공합니다. RP 기능은 이를 위해 디바이스 집합을 BSR 선택 프로세스에 참여하는 C-BSR(후보 BSR)로 구성하여 후보 중에서 BSR을 선택하는 방식을 이용합니다. BSR을 선택한 후 C-RP(후보 랑데부 포인트)로 구성된 디바이스는 선택한 BSR로 그룹 매핑을 전송하기 시작합니다. 그런 다음 BSR은 홉에 기반하여 PIM 라우터 간에 이동하는 BSR 메시지를 통해 멀티캐스트 트리 아래의 모든 기타 디바이스로 그룹-RP 매핑 정보를 배포합니다.

이 기능은 RP를 동적으로 확인하는 수단을 제공하는데, 이는 RP가 정기적으로 아래위로 이동할 수 있는 대규모의 복잡한 네트워크에서 매우 필수적입니다.

PIM BSR(부트스트랩 라우터) 용어

다음 조건은 PIM BSR 구성에서 자주 참조됩니다.

- BSR(부트스트랩 라우터) — BSR은 PIM을 사용하여 RP(랑데부 포인트) 정보를 다른 라우터에 홉별로 알립니다. 선택 프로세스 이후에 여러 후보 BSR 중에서 단일 BSR이 선택됩니다. 이 부트스트랩 라우터의 주목적은 모든 C-RP(Candidate-RP) 알림을 RP-set(RP 집합)이라고 하는 데이터베이스에 수집하고 이를 BSR 메시지로 60초마다 네트워크에 있는 다른 모든 라우터에 정기적으로 전송하는 것입니다.
- BSR(부트스트랩 라우터) 메시지 — BSR 메시지는 All-PIM-Routers(모든 PIM 라우터) 그룹에 대한 멀티캐스트입니다(TTL이 1). 이러한 메시지를 수신하는 모든 PIM 네이버는 메시지를 수신한 인터페이스를 제외한 모든 인터페이스 외부로 해당 메시지를 TTL을 1로 재전송합니다. BSR 메시지는 RP 집합 및 현재 활성 BSR의 IP 주소를 포함합니다. 이를 통해 C-RP는 자신의 C-RP 메시지를 유니캐스트할 위치를 확인합니다.
- C-BSR(후보 부트스트랩 라우터) — 후보-BSR로 구성된 디바이스는 BSR 선택 메커니즘에 참여합니다. 우선순위가 가장 높은 C-BSR은 BSR로 선택됩니다. C-BSR의 우선순위가 가장 높은 IP 주소는 타이 브레이커로 사용됩니다. BSR 선택 프로세스는 선점형입니다. 예를 들어, 우선순위가 더 높은 새로운 C-BSR이 가동되면 새로운 선택 프로세스가 트리거됩니다.
- C-RP(후보 랑데부 포인트) — RP는 소스 및 멀티캐스트 데이터의 수신자가 만나는 공간의 역할을 합니다. C-RP로 구성된 디바이스는 정기적으로 유니캐스트를 통해 선택한 BSR로 직접 멀티

캐스트 그룹 매핑 정보를 알립니다. 이러한 메시지에는 그룹 범위, C-RP 주소 및 보류 시간이 포함되어 있습니다. 현재 BSR의 IP 주소는 네트워크의 모든 라우터에서 수신하는 정기적인 BSR 메시지에서 확인됩니다. 이러한 방법으로 BSR은 현재 작동 중이며 연결 가능한 RP를 확인합니다.

참고 C-RP가 BSR 트래픽에 대한 필수 요구 사항인 경우에도 Firepower Threat Defense 디바이스는 C-RP로 작동하지 않습니다. 라우터만 C-RP로 작동할 수 있습니다. 따라서 BSR 테스트 기능을 위해 라우터를 토폴로지에 추가해야 합니다.

- BSR 선택 메커니즘 — 각 C-BSR은 BSR Priority(BSR 우선순위) 필드를 포함하는 부트스트랩 메시지(BSM)를 시작합니다. 도메인 내의 라우터는 도메인 전체에서 BSM을 플러딩합니다. 자신보다 우선순위가 높은 C-BSR를 알고 있는 C-BSR은 일정 기간 동안 추가 BSM 전송을 표시하지 않습니다. 나머지 단일 C-BSR은 선택된 BSR이 되며 해당 BSM은 도메인에 있는 모든 기타 라우터에 자신이 선택된 BSR임을 알립니다.

멀티캐스트 그룹 개념

멀티캐스트는 그룹 개념을 기반으로 합니다. 임의의 수신자 그룹이 특정 데이터 스트림 수신에 관심을 표현합니다. 이 그룹은 물리적 또는 지리적 경계가 없이 호스트가 인터넷의 어디에나 위치할 수 있습니다. 특정 그룹으로 향하는 데이터 수신에 관심이 있는 호스트는 IGMP를 사용하여 그룹에 참여해야 합니다. 호스트가 그룹의 일원이어야만 데이터 스트림을 받을 수 있습니다.

멀티캐스트 주소

멀티캐스트 주소는 그룹에 참여하고 이 그룹으로 전송된 트래픽을 수신하고자 하는 임의의 IP 호스트 그룹입니다.

클러스터링

멀티캐스트 라우팅은 클러스터링을 지원합니다. 스팬 EtherChannel 클러스터링에서 제어 유닛은 빠른 경로 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 전송합니다. fast-path 전달이 설정된 후에는 데이터 유닛이 멀티캐스트 데이터 패킷을 전송할 수 있습니다. 모든 데이터 흐름은 완전한 흐름입니다. Stub 전달 흐름도 지원됩니다. Spanned EtherChannel 클러스터링에서는 하나의 유닛만 멀티캐스트 패킷을 받기 때문에 제어 유닛으로의 리디렉션이 일반적입니다.

멀티캐스트 라우팅 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

멀티캐스트 라우팅 지침

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명 방화벽 모드는 지원되지 않습니다.

IPv6

IPv6를 지원하지 않습니다.

클러스터링

IGMP 및 PIM에 대한 클러스터링에서 이 기능은 기본 유닛에서만 지원됩니다.

추가 지침

- 멀티캐스트 호스트(예: 224.1.2.3)에 대한 트래픽을 허용하려면 인바운드 보안 영역에서 액세스 제어 또는 사전 필터 규칙을 구성해야 합니다. 그러나 규칙에 대한 대상 보안 영역을 지정하거나 초기 연결을 검증하는 동안 이를 멀티캐스트 연결에 적용할 수는 없습니다.
- PIM이 구성된 인터페이스는 비활성화 할 수 없습니다. 인터페이스에서 PIM을 구성한 경우(PIM 프로토콜 구성, 1110 페이지 참조) 멀티캐스트 라우팅 및 PIM을 비활성화해도 PIM 구성은 제거되지 않습니다. 인터페이스를 비활성화하려면 PIM 구성을 제거(삭제)해야합니다.
- PIM/IGMP 멀티캐스트 라우팅은 트래픽 영역의 인터페이스에서 지원되지 않습니다.

IGMP 기능 구성

IP 호스트가 IGMP를 사용하여 그룹 멤버십을 직접 연결된 멀티캐스트 라우터에 보고합니다. IGMP는 특정 LAN의 멀티캐스트 그룹에서 개별 호스트를 동적으로 등록하는 데 사용됩니다. 호스트는 IGMP 메시지를 로컬 멀티캐스트 라우터로 전송함으로써 그룹 멤버십을 식별합니다. IGMP에서 라우터가 IGMP 메시지를 듣고 주기적으로 쿼리를 보내 특정 서브넷에서 어떤 그룹이 활성 상태이고 어떤 그룹이 비활성 상태인지 파악합니다.

이 섹션에서는 인터페이스별로 선택적인 IGMP 설정을 구성하는 방법을 설명합니다.

프로시저

단계 1 멀티캐스트 라우팅 활성화, 1105 페이지
단계 2 IGMP 프로토콜 구성, 1106 페이지.
단계 3 IGMP 액세스 그룹 구성, 1107 페이지.
단계 4 IGMP 고정 그룹 구성, 1108 페이지.
단계 5 IGMP 조인 그룹 구성, 1109 페이지.

멀티캐스트 라우팅 활성화

Firepower Threat Defense 디바이스에서 멀티캐스트 라우팅을 활성화하면 모든 인터페이스에서 기본적으로 IGMP 및 PIM이 활성화됩니다. IGMP는 그룹에서 어떤 멤버가 직접 연결된 서브넷에 존재하는지 학습하는 데 사용됩니다. 호스트는 IGMP 보고 메시지를 전송함으로써 멀티캐스트 그룹에 참여합니다. PIM은 멀티캐스트 데이터 그램을 전달하기 위한 전달 테이블 유지에 사용됩니다.

참고 멀티캐스트 라우팅에 대해서는 UDP 전송 레이어만 지원됩니다.

다음 목록에는 특정 멀티캐스트 테이블에 대한 최대 항목 수가 나와 있습니다. 이 제한에 도달하면 새로운 엔트리가 삭제됩니다.

- MFIB—30,000
- IGMP 그룹-30,000
- PIM 경로 —72,000

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.
단계 2 **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.
단계 3 **Enable Multicast Routing(**멀티캐스트 라우팅 활성화**)** 확인란을 선택합니다.

이 확인란을 선택하면 Firepower Threat Defense 디바이스에서 IP 멀티캐스트 라우팅이 활성화됩니다. 이 확인란 선택을 취소하면 IP 멀티캐스트 라우팅이 비활성화됩니다. 기본적으로 멀티캐스트는 비활성화되어 있습니다. 멀티캐스트 라우팅을 활성화하면 모든 인터페이스에서 멀티캐스트가 활성화됩니다.

인터페이스별로 멀티캐스트를 비활성화할 수 있습니다. 이 정보는 특정 인터페이스에 멀티캐스트 호스트가 없음을 알고 있고 Firepower Threat Defense 디바이스가 해당 인터페이스로 호스트 쿼리 메시지를 보내는 것을 막고 싶을 때 유용합니다.

IGMP 프로토콜 구성

전달 인터페이스, 쿼리 메시지 및 시간 간격과 같은 인터페이스별로 IGMP 파라미터를 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.

단계 **3** **Protocol(**프로토콜**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add IGMP parameters(IGMP 파라미터 추가**)** 대화 상자를 사용하여 새 IGMP 파라미터를 Firepower Threat Defense 디바이스에 추가합니다. **Edit IGMP parameters(IGMP** 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** - 드롭다운 목록에서 구성하려는 IGMP 프로토콜에 대한 인터페이스를 선택합니다.
- **Enable IGMP(IGMP** 활성화**)** - IGMP를 활성화하려면 확인란을 선택합니다.

  참고 특정 인터페이스에 대한 IGMP 비활성화는 특정 인터페이스에 멀티캐스트 호스트가 없음을 알고 있고 Firepower Threat Defense 디바이스가 해당 인터페이스로 호스트 쿼리 메시지를 보내는 것을 막고 싶을 때 유용합니다.

- **Forward Interface(**인터페이스 전달**)** - 드롭다운 목록에서 IGMP 메시지를 전달할 특정 인터페이스를 선택합니다.

  대신 IGMP 프록시 에이전트 역할을 하고 IGMP 메시지를 하나의 인터페이스에 연결된 호스트에서 다른 인터페이스에 연결된 업스트림 멀티캐스트 라우터로 전달하도록 Firepower Threat Defense 디바이스를 구성합니다.

- **Version(**버전**)** - IGMP 버전 1 또는 2를 선택합니다.

  기본적으로 Firepower Threat Defense 디바이스는 몇 가지 추가 기능을 활성화하는 IGMP 버전 2를 실행합니다.

참고 서브넷의 모든 멀티캐스트 라우터는 같은 버전의 IGMP를 지원해야 합니다. Firepower Threat Defense 디바이스는 자동으로 버전 1 라우터를 감지하고 버전 1로 전환하지 않습니다. 그러나 IGMP 버전 1과 2 호스트를 서브넷에서 혼용할 수는 있습니다. IGMP 버전 2를 실행 중인 Firepower Threat Defense 디바이스는 IGMP 버전 1 호스트가 있을 때에도 정상 작동합니다.

- **Query Interval(**쿼리 간격**)** - 지정된 라우터가 IGMP 호스트 쿼리 메시지를 전송하는 간격(초 단위)입니다. 범위는 1~ 600입니다. 기본값은 125입니다.

  참고 Firepower Threat Defense 디바이스가 지정된 시간 초과 값 동안 쿼리 메시지를 받지 못하면 Firepower Threat Defense 디바이스가 지정 라우터가 되고 쿼리 메시지 전송을 시작합니다.

- **Response Time(**응답 시간**)** - Firepower Threat Defense 디바이스가 그룹을 삭제하기 전의 간격(초)입니다. 범위는 1~25입니다. 기본값은 10입니다.

  이 시간 내에 Firepower Threat Defense 디바이스가 호스트 쿼리에 대한 응답을 받지 못하면 그 그룹이 삭제됩니다.

- **Group Limit(**그룹 제한**)** - 인터페이스에 참여할 수 있는 호스트의 최대 수입니다. 범위는 1~500입니다. 기본값은 500입니다.

  인터페이스별로 IGMP 멤버십 보고에서 비롯되는 IGMP 멤버십 상태의 수를 제한할 수 있습니다. 구성된 제한을 초과하는 멤버십 보고는 IGMP 캐시에 입력되지 않고 초과된 멤버십 보고에 대한 트래픽은 전달되지 않습니다.

- **Query Timeout(**쿼리 시간 초과**)** - 이전 요청자가 역할을 중지한 후 Firepower Threat Defense 디바이스가 인터페이스의 요청자 역할을 대신하기 전까지의 시간(초)입니다. 범위는 60~300입니다. 기본값은 255입니다.

단계 **5** **OK(**확인**)**를 클릭하여 IGMP 프로토콜 구성을 저장합니다.

IGMP 액세스 그룹 구성

액세스 제어 목록을 사용하여 멀티캐스트 그룹에 대한 액세스를 제어할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **Access Group(**액세스 그룹**)**을 선택합니다.

단계 **3** **Access Group(**액세스 그룹**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add IGMP Access Group parameters(IGMP 액세스 그룹 파라미터 추가**)** 대화 상자를 사용하여 액세스 그룹 테이블에 새 액세스 그룹을 추가합니다. **Edit IGMP Access Group parameters(IGMP** 액세스 그룹 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

a) **Interface(**인터페이스**)** 드롭다운 목록에서 액세스 그룹이 연결된 인터페이스를 선택합니다. 기존 액세스 그룹을 편집할 때는 연결된 인터페이스를 변경할 수 없습니다.

b) 다음 중 하나를 클릭합니다.

- **Standard Access List(**표준 액세스 목록**) - Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 추가(+)를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정, 646 페이지를 참조하십시오.
- **Extended Access List(**확장 액세스 목록**) - Extended Access List(**확장 액세스 목록**)** 드롭다운 목록에서 확장 ACL을 선택하거나 추가(+)을 클릭하여 새 확장 ACL을 생성합니다. 절차는 확장 ACL 개체 설정, 645 페이지를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 액세스 그룹 구성을 저장합니다.

IGMP 고정 그룹 구성

그룹 멤버가 해당 그룹 멤버를 보고할 수 없거나 네트워크 세그먼트에 그룹 멤버가 없을 수 있지만 해당 그룹의 멀티캐스트 트래픽이 해당 네트워크 세그먼트로 전송되게 하려고 합니다. 고정 참여 IGMP 그룹을 구성하면 해당 그룹에 대한 멀티캐스트 트래픽을 해당 세그먼트로 보낼 수 있습니다. 이 방법을 통해 Firepower Threat Defense 디바이스는 패킷 자체를 수신하지 않고 전달만 합니다. 따라서 빠른 전환이 가능합니다. 발신 인터페이스가 IGMP 캐시에 나타나지만 이 인터페이스는 멀티캐스트 그룹의 멤버가 아닙니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.

단계 **3** **Static Group(**고정 그룹**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add IGMP Static Group parameters(IGMP 고정 그룹 파라미터 추가**)** 대화 상자를 이용하여 멀티캐스트 그룹을 고정으로 인터페이스에 할당합니다. **Edit IGMP Static Group(IGMP** 고정 그룹 수정**)** 대화 상자를 이용하여 기존 고정 그룹 할당을 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 멀티캐스트 그룹을 고정으로 할당할 인터페이스를 선택합니다. 기존 항목을 편집할 경우 이 값을 변경할 수 없습니다.

- **Multicast Groups(**멀티캐스트 그룹**)** 드롭다운 목록에서 인터페이스를 할당할 멀티캐스트 그룹을 선택하거나 추가(+)을 클릭하여 새 멀티캐스트 그룹을 만들 수 있습니다. 네트워크 개체 생성에서 절차를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 고정 그룹 구성을 저장합니다.

IGMP 조인 그룹 구성

인터페이스를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. Firepower Threat Defense 디바이스를 멀티캐스트 그룹에 참여하도록 구성하면 업스트림 라우터가 해당 그룹에 대한 멀티캐스트 라우팅 테이블 정보를 유지하고 해당 그룹에 대한 경로를 활성 상태로 유지하게 됩니다.

참고 특정 그룹에 대한 멀티캐스트 패킷을 인터페이스로 전달하면서 IGMP 고정 그룹 구성, 1108 페이지 디바이스에서 패킷을 해당 그룹의 일부로 수락하지 않도록 하려면 Firepower Threat Defense 섹션을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.

단계 **3** **Join Group(**조인 그룹**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add IGMP Join Group parameters(IGMP 조인 그룹 파라미터추가**)** 대화 상자에서 Firepower Threat Defense 디바이스를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. **Edit IGMP Join Group parameters(IGMP** 조인 그룹 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 멀티캐스트 그룹의 멤버로 정할 인터페이스를 선택합니다. 기존 항목을 편집할 경우 이 값을 변경할 수 없습니다.
- **Join Group(**조인 그룹**)** 드롭다운 목록에서 인터페이스를 할당할 멀티캐스트 그룹을 선택하거나 **Plus(**더하기**)**를 클릭하여 새 멀티캐스트 그룹을 만들 수 있습니다. 네트워크 개체 생성에서 절차를 참조하십시오.

PIM 기능 구성

라우터는 PIM을 사용하여 멀티캐스트 다이어그램 전달에 사용할 전달 테이블을 유지합니다. Firepower Threat Defense 디바이스에서 멀티캐스트 라우팅을 활성화할 경우 PIM 및 IGMP가 모든 인터페이스에서 자동으로 활성화됩니다.

참고 PIM은 PAT에서 지원되지 않습니다. PIM 프로토콜은 포트를 사용하지 않고 PAT는 포트를 사용하는 프로토콜에서만 작동합니다.

이 섹션은 선택적인 PIM 설정을 구성하는 방법을 설명합니다.

프로시저

단계 **1** PIM 프로토콜 구성, 1110 페이지
단계 **2** PIM 네이버 필터 구성, 1111 페이지
단계 **3** PIM 양방향 네이버 필터 구성, 1112 페이지
단계 **4** PIM 랑데부 포인트 설정, 1113 페이지
단계 **5** PIM 라우트 트리 설정, 1114 페이지
단계 **6** PIM 요청 필터 설정, 1115 페이지
단계 **7** 멀티캐스트 경계 필터 설정, 1117 페이지

PIM 프로토콜 구성

특정 인터페이스에서 PIM을 활성화하거나 비활성화할 수 있습니다.

지정된 라우터(DR) 우선 순위를 구성할 수도 있습니다. DR은 PIM 등록, 참여 및 prune 메시지를 RP로 보내는 것을 담당합니다. 네트워크 세그먼트에 멀티캐스트 라우터가 하나 이상 있는 경우 DR 선택은 DR 우선 순위를 따릅니다. 여러 디바이스의 DR 우선 순위가 동일한 경우 IP 주소가 가장 높은 디바이스가 DR이 됩니다. 기본적으로 Firepower Threat Defense의 DR 우선 순위는 1입니다.

PIM DR 선택을 위해 라우터 쿼리 메시지가 사용될 수 있습니다. PIM DR은 라우터 쿼리 메시지 전송을 담당합니다. 기본적으로 라우터 쿼리 메시지는 30초마다 전송됩니다. 또한 Firepower Threat Defense는 60초마다 PIM 참여 또는 prune 메시지를 보냅니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.
단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Protocol(**프로토콜**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add PIM parameters(PIM 파라미터 추가**)** 대화 상자를 사용하여 새 PIM 파라미터를 디바이스에 추가합니다. **Edit PIM parameters(PIM** 파라미터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** - 드롭다운 목록에서 구성하려는 PIM 프로토콜에 대한 인터페이스를 선택합니다.
- **Enable PIM(PIM** 활성화**)** - PIM을 활성화하려면 확인란을 선택합니다.
- **DR Priority(DR** 우선 순위**)** - 선택한 인터페이스에 대한 DR 값입니다. 서브넷에서 DR 우선 순위가 가장 높은 라우터가 지정 라우터가 됩니다. 유효한 값의 범위는 0 ~ 4294967294입니다. 기본 DR 우선 순위는 1입니다. 이 값을 0으로 설정하면 Firepower Threat Defense 디바이스 인터페이스가 기본 라우터가 될 자격을 잃게 됩니다.
- **Hello Interval(Hello** 간격**)** - 인터페이스에서 PIM hello 메시지를 보내는 간격(초)입니다. 범위는 1~3600입니다. 기본값은 30입니다.
- **Join Prune Interval(**조인 **Prune** 간격**)** - 인터페이스에서 PIM 조인 및 prune 알림을 전송하는 간격(초)입니다. 범위는 10~600입니다. 기본값은 60입니다.

단계 **5** **OK(**확인**)**를 클릭하여 PIM 프로토콜 구성을 저장합니다.

PIM 네이버 필터 구성

PIM 네이버가 될 수 있는 라우터를 정의할 수 있습니다. PIM 네이버가 될 수 있는 라우터를 필터링함으로써 다음을 할 수 있습니다.

- 권한이 없는 라우터가 PIM 네이버가 되는 것을 막습니다.
- 연결된 stub 라우터가 PIM에 참여하는 것을 막습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Neighbor Filter(**네이버 필터**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add PIM Neighbor Filter(PIM 네이버 필터 추가**)** 대화 상자를 사용하여 새 PIM 네이버 필터를 디바이스에 추가합니다. **Edit PIM Neighbor Filter(PIM** 네이버 필터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 PIM 네이버 필터를 추가할 인터페이스를 선택합니다.
- **Standard Access List(**표준 액세스 목록**) - Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 추가(+)를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정, 646 페이지를 참조하십시오.

  참고 **Add Standard Access List Entry(**표준 액세스 목록 항목 추가**)** 대화 상자에서 **Allow(**허용**)**를 선택하여 멀티캐스트 그룹 알림이 인터페이스를 통과하도록 합니다. **Block(**차단**)**을 선택하면 지정된 멀티캐스트 그룹 알림이 인터페이스를 통과할 수 없습니다. 인터페이스에서 멀티캐스트 경계가 구성된 경우 모든 멀티캐스트 트래픽은 네이버 필터 엔트리로 허용되지 않는 한 인터페이스를 통과할 수 없습니다.

단계 **5** **OK(**확인**)**를 클릭하여 PIM 네이버 필터 구성을 저장합니다.

PIM 양방향 네이버 필터 구성

PIM 양방향 네이버 필터는 네이버가 DF 선택에 참여할 수 있다고 정의하는 ACL입니다. 인터페이스에 대해 PIM 양방향 네이버 필터가 구성되지 않은 경우에는 제한 사항이 없습니다. PIM 양방향 네이버 필터가 구성된 경우 ACL에서 허용된 네이버만 DF 선택 프로세스에 참여할 수 있습니다.

양방향 PIM은 멀티캐스트 라우터가 축소된 상태 정보를 유지할 수 있게 합니다. 세그먼트의 모든 멀티캐스트 라우터가 양방향으로 활성화되어 있어야 DF를 선택할 수 있습니다.

PIM 양방향 네이버 필터가 활성화된 경우 ACL에 의해 허용된 라우터는 양방향을 지원하는 것으로 간주됩니다. 따라서 다음은 참입니다.

- 허용된 네이버가 양방향 모드를 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 네이버가 양방향 모드를 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 네이버가 양방향 모드를 지원하지 않을 경우 DF 선택이 일어날 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Bidirectional Neighbor Filter(**양방향 네이버 필터**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add PIM Bidirectional Neighbor Filter(PIM 양방향 네이버 필터 추가**)** 대화 상자를 사용하여 PIM 양방향 네이버 필터 ACL에 대한 ACL 항목을 생성합니다. **Edit PIM Bidirectional Neighbor Filter(PIM** 양방향 네이버 필터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 PIM 양방향 네이버 필터 ACL 항목을 구성할 인터페이스를 선택합니다.

- **Standard Access List(**표준 액세스 목록**) - Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 추가(+)를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정, 646 페이지를 참조하십시오.

  참고 **Add Standard Access List Entry(**표준 액세스 목록 항목 추가**)** 대화 상자에서 **Allow(**허용**)**를 선택하면 지정된 디바이스가 DR 선택 프로세스에 참여할 수 있습니다. **Block(**차단**)**을 선택하면 지정된 디바이스가 DF 선택 프로세스에 참여할 수 없습니다.

단계 **5** **OK(**확인**)**를 클릭하여 PIM 양방향 네이버 필터 구성을 저장합니다.

PIM 랑데부 포인트 설정

Firepower Threat Defense 디바이스가 하나 이상의 그룹에 대해 RP 역할을 하도록 구성할 수 있습니다. ACL에 지정된 그룹 범위가 PIM RP 그룹 매핑을 결정합니다. ACL이 지정되지 않은 경우 해당 그룹에 대한 RP가 전체 멀티캐스트 그룹 범위(224.0.0.0/4)에 적용됩니다. 양방향 PIM에 대한 자세한 내용은 멀티캐스트 양방향 PIM, 1101 페이지 섹션을 참조하십시오.

RP에는 다음 제한 사항이 적용됩니다.

- 동일한 RP 주소를 두 번 사용할 수 없습니다.
- 하나 이상의 RP에 All Groups를 지정할 수 없습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Rendezvous Points(**랑데부 포인트**)**에서 **Add(**추가**)** 또는 **Edit(**편집**)**을 클릭합니다.

Add Rendezvous Point(랑데부 포인트 추가**)** 대화 상자를 사용하여 랑데부 포인트 테이블에 새로운 항목을 생성합니다. **Edit Rendezvous Point(**랑데부 포인트 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Rendezvous Point IP address(**랑데부 포인트 **IP** 주소**)** 드롭다운 목록에서 RP 역할로 추가할 IP 주소를 선택하거나 추가(+)를 클릭하여 새 네트워크 개체를 만듭니다. 네트워크 개체 생성에서 절차를 참조하십시오.
- 지정된 멀티캐스트 그룹이 양방향 모드에서 작동하는 경우 **Use bi-directional forwarding(**양방향 전달 사용**)** 확인란을 선택하십시오. 양방향 모드에서 Firepower Threat Defense 디바이스가 멀티캐스트 패킷을 수신하고 직접 연결된 멤버나 PIM 네이버가 없는 경우 다시 소스로 prune 메시지를 보냅니다.

- **Use this RP for all Multicast Groups(**모든 멀티캐스트 그룹에 대해 이 **RP** 사용**)**를 선택하여 인터페이스의 모든 멀티캐스트 그룹에 대해 지정된 RP를 사용합니다.
- **Use this RP for all Multicast Groups as specified below(**아래 지정된 대로 멀티캐스트 그룹에 이 **RP** 사용**)**를 선택하여 지정된 RP와 함께 사용할 멀티캐스트 그룹을 지정한 다음 **Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 추가( )를 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정, 646 페이지를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 랑데부 포인트 구성을 저장합니다.

PIM 라우트 트리 설정

기본적으로 PIM 리프 라우터는 첫 번째 패킷이 새로운 소스에 도달한 직후 가장 짧은 경로의 트리에 참여합니다. 이 방법은 지연을 줄이지만 공유 트리보다 더 많은 메모리가 필요합니다. 모든 멀티캐스트 그룹에 대해 또는 특정 멀티캐스트 주소에 한정하여 Firepower Threat Defense 디바이스가 최단 경로 트리에 참여할지 아니면 공유 트리를 사용할지 구성할 수 있습니다.

Multicast Groups(멀티캐스트 그룹) 테이블에 지정되지 않은 그룹에 대해서는 최단 경로 트리가 사용됩니다. Multicast Groups(멀티캐스트 그룹) 테이블은 공유 트리를 사용할 멀티캐스트 그룹을 표시합니다. 테이블 엔트리는 위에서 아래로 처리됩니다. 특정 그룹에 대한 거부 규칙을 테이블 상단에 배치하고 멀티캐스트 그룹 범위에 대한 허용 규칙을 거부 구문 아래에 배치하면 일정한 범위의 멀티캐스트 그룹을 포함하되 해당 범위 내 특정 그룹을 제외하는 엔트리를 만들 수 있습니다.

참고 이 동작은 SPT(Shortest Path Switchover)로 알려져 있습니다. 항상 공유 트리 옵션을 사용하는 것이 좋습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Route Tree(**경로 트리**)**에서 경로 트리에 대한 경로를 선택합니다.

- **Shortest Path(**최단 경로**)**를 클릭하여 모든 멀티캐스트 그룹에 대해 최단 경로 트리를 사용합니다.
- **Shared Tree(**공유 트리**)**를 클릭하여 모든 멀티캐스트 그룹에 대해 공유 트리를 사용합니다.
- **Shared tree for below mentioned group(**아래 언급한 그룹에 대한 공유 트리**)**을 클릭하여 멀티캐스트 그룹 표에 명시된 그룹을 지정한 다음 **Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 추가( )을 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정, 646 페이지를 참조하십시오.

단계 4 **OK(**확인**)**를 클릭하여 경로 트리 구성을 저장합니다.

PIM 요청 필터 설정

Firepower Threat Defense 디바이스가 RP 역할을 수행하는 경우 특정 멀티캐스트 소스의 등록을 제한하여 권한이 없는 소스가 RP에 등록하지 못하도록 할 수 있습니다. Firepower Threat Defense 디바이스가 PIM 레지스터 메시지를 수락하는 멀티캐스트 소스를 정의할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 2 **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 3 **Request Filter(**요청 필터**)**에서 Firepower Threat Defense 디바이스가 RP 역할을 할 때 등록을 허용할 멀티캐스트 소스를 정의합니다.

- **Filter PIM register messages using:(**다음을 사용하여 **PIM** 등록 메시지 필터링**)** 드롭다운 목록에서 **None(**없음**)**, **Access List(**액세스 목록**)** 또는 **Route Map(**경로 맵**)**을 선택합니다.
- 드롭다운 목록에서 **Access List(**액세스 목록**)**를 선택하는 경우, 확장 ACL을 선택하거나 추가( )를 클릭하여 새 확장 ACL을 생성합니다. 절차는 확장 ACL 개체 설정, 645 페이지를 참조하십시오.

  참고 **Add Extended Access List Entry(**확장 액세스 목록 항목 추가**)** 대화 상자에서 드롭다운 목록의 **Allow(**허용**)**를 선택하여 지정된 멀티캐스트 트래픽의 지정된 소스를 Firepower Threat Defense 디바이스에 등록할 수 있도록 허용하는 규칙을 생성하거나 **Block(**차단**)**을 선택하여 지정된 멀티캐스트 트래픽의 지정된 소스를 Firepower Threat Defense 디바이스에 등록할 수 없도록 하는 규칙을 생성합니다.

- **Route Map(**경로 맵**)**을 선택하는 경우, **Route Map(**경로 맵**)** 드롭다운 목록에서 경로 맵을 선택하거나 추가( )를 클릭하여 새로운 경로 맵을 만들 수 있습니다. 네트워크 개체 생성에서 절차를 참조하십시오.

단계 4 **OK(**확인**)**를 클릭하여 요청 필터 구성을 저장합니다.

Firepower Threat Defense 디바이스를 후보 BSR(Bootstrap Router)로 구성

Firepower Threat Defense 디바이스를 후보 BSR로 구성할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **PIM**을 선택합니다.

단계 **3** **Bootstrap Router**에서 **Configure this FTD as a Candidate Bootstrap Router (C-BSR)(**이 **FTD**를 **C-BSR(Candidate Bootstrap Router)**로 구성**)** 확인란을 선택하여 C-BSR 설정을 수행합니다.

a) **Interface(**인터페이스**)** 드롭다운 목록에서 BSR 주소가 파생된 Firepower Threat Defense 디바이스에서 인터페이스를 선택하여 후보로 설정합니다.

이 인터페이스는 PIM을 사용하여 활성화되어야 합니다.

b) **Hash mask length(**해시 마스크 길이**)** 필드에서 해시 함수가 호출되기 전에 그룹 주소로 AND 처리할 마스크의 길이(최대 32비트)를 입력합니다. 시드 해시가 동일한 모든 그룹은 동일한 RP와 일치합니다. 예를 들어, 이 값이 24인 경우, 그룹 주소의 첫 번째 24비트만 중요합니다. 이를 통해 여러 그룹에 대해 하나의 RP를 얻을 수 있습니다. 범위는 0~32입니다.

c) **Priority(**우선 순위**)** 필드에서 후보 BSR의 우선 순위를 입력합니다. 더 큰 우선순위를 지닌 BSR이 우선시됩니다. 우선순위 값이 동일한 경우, 더 큰 IP 주소를 지닌 라우터는 BSR입니다. 범위는 0~255입니다. 기본값은 0입니다.

단계 **4** (선택 사항) 추가(+)을 클릭하여 PIM BSR 메시지가 전송 또는 수신되지 않는 인터페이스를 **Configure this FTD as a Border Bootstrap Router (BSR)(**이 **FTD**를 **Border Bootstrap Router**로 구성**)** 섹션에서 선택합니다.

- **Interface(**인터페이스**)** 드롭다운 목록에서 PIM BSR 메시지가 전송 또는 수신되지 않는 인터페이스를 선택합니다.

  RP 또는 BSR 알림은 RP 정보 교환의 두 도메인을 효과적으로 격리하여 필터링됩니다.

- BSR을 활성화하려면 **Enable Border BSR(Border BSR** 활성화**)** 확인란을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 부트스트랩 라우터 구성을 저장합니다.

멀티캐스트 라우트 설정

고정 멀티캐스트 경로를 구성함으로써 유니캐스트 트래픽에서 멀티캐스트 트래픽을 분리할 수 있습니다. 예를 들어 소스와 목적지 사이의 경로가 멀티캐스트 라우팅을 지원하지 않을 경우 해결책은 두 멀티캐스트 디바이스 사이에 GRE 터널을 구성하여 멀티캐스트 패킷을 터널을 통해 전송하는 것입니다.

PIM을 사용하는 경우 Firepower Threat Defense 디바이스는 유니캐스트 패킷을 다시 소스로 보내는 인터페이스와 같은 인터페이스에서 패킷을 수신할 것으로 기대합니다. 멀티캐스트 라우팅을 지원하지 않는 경로를 바이패스할 때와 같이 일부 경우에서는 유니캐스트 패킷이 하나의 경로를 따르고 멀티캐스트 패킷이 다른 경로를 따르도록 할 수 있습니다.

고정 멀티캐스트 경로가 알려지거나 재배포되지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **Multicast Routes(**멀티캐스트 경로**)** > **Add(**추가**)** 또는 **Edit(**편집**)**을 선택합니다.

Add Multicast Route Configuration(멀티캐스트 경로 구성 추가**)** 대화 상자를 사용하여 새로운 멀티캐스트 경로를 Firepower Threat Defense 디바이스에 추가합니다. **Edit Multicast Route Configuration(**멀티캐스트 경로 구성 편집**)** 대화 상자를 사용하여 기존 멀티캐스트 경로를 변경합니다.

단계 **3** **Source Network(**소스 네트워크**)** 드롭다운 상자에서 기존 네트워크를 선택하거나 추가(+)를 클릭하여 새 네트워크를 추가합니다. 네트워크 개체 생성에서 절차를 참조하십시오.

단계 **4** 경로를 전달하도록 인터페이스를 설정하려면 **Interface(**인터페이스**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)** 드롭다운 목록에서 멀티캐스트 경로에 대한 수신 인터페이스를 선택합니다.
- **Output Interface/Dense(**출력 인터페이스**/Dense)** 드롭다운 목록에서 경로가 전달되는 대상 인터페이스를 선택합니다.
- **Distance(**거리**)** 필드에 멀티캐스트 경로 거리를 입력합니다. 범위는 0~255입니다.

단계 **5** 경로를 전달하도록 RPF 주소를 설정하려면 **Address(**주소**)**를 클릭하고 탭에서 다음 옵션을 구성합니다.

- **RPF Address(RPF** 주소**)** 필드에 멀티캐스트 경로의 IP 주소를 입력합니다.
- **Distance(**거리**)** 필드에 멀티캐스트 경로 거리를 입력합니다. 범위는 0~255입니다.

단계 **6** **OK(**확인**)**를 클릭하여 멀티캐스트 경로 구성을 저장합니다.

멀티캐스트 경계 필터 설정

주소 범위 지정은 도메인 경계 필터를 정의하여 같은 IP 주소를 가진 RP 도메인이 서로 섞이지 않도록 합니다. 범위 지정은 대형 도메인 내 서브넷 경계와 도메인과 인터넷 사이의 경계에서 이루어집니다.

멀티캐스트 그룹 주소에 대한 인터페이스에서 관리적으로 범위가 지정된 경계 필터를 설정할 수 있습니다. IANA는 관리적으로 범위가 지정된 주소로 239.0.0.0~239.255.255.255의 멀티캐스트 주소 범위를 지정했습니다. 이 주소 범위는 다른 조직이 관리하는 도메인에서 재사용될 수 있습니다. 주소는 전역에서 고유한 주소가 아닌 로컬 주소로 간주됩니다.

표준 ACL은 영향을 받는 주소의 범위를 정의합니다. 경계 필터를 설정할 때 어느 방향으로도 경계를 건너는 멀티캐스트 데이터 패킷 흐름은 허용되지 않습니다. 경계 필터를 통해 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있습니다.

자동 RP 검색 및 알림 메시지를 관리적으로 범위가 지정된 경계에서 구성, 검사 및 필터링할 수 있습니다. 경계 ACL에 의해 거부된 Auto-RP 패킷의 모든 Auto-RP 패킷 그룹 범위 알림은 삭제됩니다. Auto-RP 그룹 범위 알림은 Auto-RP 그룹 범위의 모든 주소가 경계 ACL에 의해 허용된 경우에만 경계 필터에서 허용 및 통과됩니다. 주소가 하나라도 허용되지 않은 경우 전체 그룹 범위가 필터링되고 Auto-RP 메시지가 전달되기 전에 Auto-RP 메시지에서 삭제됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)** > **Multicast Routing(**멀티캐스트 라우팅**)** > **Multicast Boundary Filter(**멀티캐스트 경계 필터**)**를 선택한 다음 **Add(**추가**)** 또는 **Edit(**편집**)**를 클릭합니다.

Add Multicast Boundary Filter(멀티캐스트 경계 필터 추가**)** 대화상자를 사용하여 새 멀티캐스트 경계 필터를 Firepower Threat Defense 디바이스에 추가합니다. **Edit Multicast Boundary Filter(**멀티캐스트 경계 필터 편집**)** 대화 상자를 사용하여 기존 파라미터를 변경합니다.

관리적으로 범위가 지정된 멀티캐스트 주소에 대한 멀티캐스트 경계를 구성할 수 있습니다. 멀티캐스트 경계는 멀티캐스트 데이터 패킷 흐름을 제한하고 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있게 합니다. 인터페이스에서 특정 멀티캐스트 경계가 정의된 경우 필터 ACL에 의해 허용된 멀티캐스트 트래픽만 인터페이스를 통과합니다.

단계 **3** **Interface(**인터페이스**)** 드롭다운 목록에서 멀티캐스트 경계 필터 ACL을 구성할 인터페이스를 선택합니다.

단계 **4** **Standard Access List(**표준 액세스 목록**)** 드롭다운 목록에서 표준 ACL을 선택하거나 추가(+)을 클릭하여 새 표준 ACL을 생성합니다. 절차는 표준 ACL 개체 설정, 646 페이지를 참조하십시오.

단계 **5** 경계 ACL에 의해 거부된 소스에서 Auto-RP 메시지를 필터링하려면 **Remove any Auto-RP group range announcement from the Auto-RP packets that are denied by the boundary(**경계 **ACL**에 의해 거부된 **Auto-RP** 패킷의 모든 **Auto-RP** 패킷 그룹 범위 알림 제거**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 모든 Auto-RP 메시지가 전달됩니다.

단계 **6** **OK(**확인**)**를 클릭하여 멀티캐스트 경계 필터를 저장합니다.

X 부

Firepower Threat Defense VPN

- Firepower Threat Defense VPN 개요, 1121 페이지
- Site-to-Site VPN Firepower Threat Defense, 1133 페이지
- Remote Access VPN Firepower Threat Defense, 1155 페이지
- Firepower Threat Defense VPN 모니터링, 1231 페이지
- Firepower Threat Defense VPN 문제 해결, 1235 페이지

43 장

Firepower Threat Defense VPN 개요

VPN(Virtual Private Network)은 인터넷과 같은 공용 네트워크를 통해 엔드포인트 간에 보안 터널을 설정합니다.

이 장은 Firepower Threat Defense 디바이스의 Remote Access 및 Site-to-Site VPN에 적용됩니다. 여기에서는 Site-to-Site 및 Remote Access VPN을 구축하는 데 사용되는 IPsec(Internet Protocol Security) 및 ISAKMP(Internet Security Association and Key Management Protocol) 표준에 대해 설명합니다.

Firepower Management Center에서 게이트웨이 VPN 또는 Firepower VPN이라고 하는 7000 및 8000 Series 디바이스의 Site-to-Site VPN은 게이트웨이 VPN에 설명되어 있습니다.

- VPN 유형, 1121 페이지
- VPN 기본 사항, 1122 페이지
- VPN 패킷 플로우, 1124 페이지
- VPN 라이선싱, 1125 페이지
- VPN 연결의 보안 수준 결정, 1125 페이지
- 제거되었거나 사용되지 않는 해시 알고리즘, 암호화 알고리즘 및 Diffie-Hellman 모듈러스 그룹, 1128 페이지
- VPN 토폴로지 옵션, 1128 페이지

VPN 유형

Firepower Management Center에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

- Firepower Threat Defense 디바이스의 Remote Access VPN.

  Remote Access VPN은 원격 사용자와 회사의 프라이빗 네트워크 간에 보안, 암호화된 연결 또는 터널입니다. 연결은 VPN 클라이언트 기능이 있는 워크스테이션 또는 모바일 장치인 VPN 엔드포인트 장치 및 회사 프라이빗 네트워크의 에지에 있는 VPN 헤드엔드 장치 또는 보안 게이트웨이로 구성됩니다.

  Firepower Threat Defense 디바이스는 SSL을 통한 Remote Access VPN 또는 Firepower Management Center에 의한 IPsec IKEv2를 지원하도록 구성될 수 있습니다. 이 용량의 보안 게이트웨이로 작동하여 원격 사용자를 인증하고 액세스 권한을 부여하며 데이터를 암호화하여 네트워크에 대한

보안 연결을 제공합니다. Firepower Management Center에 의해 관리되는 다른 유형의 어플라이언스는 Remote Access VPN 연결을 지원하지 않습니다.

Firepower Threat Defense 보안 게이트웨이는 AnyConnect Secure Mobility Client 전체 터널 클라이언트를 지원합니다. 이 클라이언트는 원격 사용자에게 안전한 SSL IPsec IKEv2 연결을 제공해야 합니다. 이 클라이언트는 연결 시 클라이언트 플랫폼에 배포할 수 있으므로 네트워크 관리자가 원격 컴퓨터에 클라이언트를 설치하고 구성할 필요 없이 원격 사용자에게 클라이언트의 이점을 제공합니다. 이는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

- 7000 및 8000 Series 디바이스의 Site-to-Site VPN.

  이러한 Site-to-Site VPN은 Firepower Management Center에서 게이트웨이 VPN 또는 Firepower VPN이라고 합니다. 이 유형의 VPN 연결에 대한 정보는 게이트웨이 VPN 섹션을 참조하십시오.

VPN 기본 사항

터널링을 통해 인터넷과 같은 공용 TCP/IP 네트워크를 사용하고 원격 사용자와 사설 기업 네트워크 간의 안전한 연결을 생성할 수 있습니다. 각 보안 연결을 터널이라고 부릅니다.

IPsec 기반 VPN 기술은 ISAKMP/IKE(Internet Security Association and Key Management Protocol) 및 IPsec 터널링 표준을 사용하여 터널을 작성하고 관리합니다. ISAKMP 및 IPsec는 다음 사항을 수행합니다.

- 터널 파라미터 협상
- 터널 설정
- 사용자 및 데이터 인증
- 보안 키 관리
- 데이터 암호화 및 암호 해독
- 터널을 통한 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로 데이터 전송 인바운드 및 아웃바운드 관리

VPN의 디바이스는 양방향 터널 엔드포인트로 작동합니다. 사설 네트워크에서 일반 패킷을 수신하여 캡슐화하고 터널을 생성하며, 캡슐 해제하여 최종 대상에 전송하는 다른 쪽 터널의 끝으로 보낼 수 있습니다. 또한 공용 네트워크에서 캡슐화된 패킷을 수신하여 캡슐을 해제하여 사설 네트워크의 최종 대상에 보낼 수 있습니다.

사이트 대 사이트 VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다. 연결은 두 게이트웨이의 IP 주소와 호스트 이름, 그 뒤에 있는 서브넷, 두 게이트웨이가 상호 인증에 사용하는 방법으로 구성됩니다.

IKE(Internet Key Exchange)

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(Security Association, 보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다.

IKE 정책은 두 피어가 상호 간의 KIE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 보안 파라미터를 제시합니다. IKEv1(IKE 버전 1)의 경우 IKE 정책에는 단일 알고리즘 집합과 모듈러스 그룹이 포함됩니다. IKEv1과 달리 IKEv2 정책에서는 피어가 1단계 협상 중에 선택할 수 있는 여러 알고리즘 및 모듈러스 그룹을 선택할 수 있습니다. 단일 IKE 정책을 생성할 수도 있지만, 여러 정책을 생성해 가장 적절한 옵션에 더 높은 우선 순위를 지정할 수도 있습니다. 사이트 대 사이트 VPN의 경우에는 단일 IKE 정책을 생성할 수 있습니다.

IKE 정책을 정의하려면 다음 사항을 지정합니다.

- 고유한 우선 순위(1~65,543, 1이 우선 순위가 가장 높음)
- 데이터 및 개인정보를 보호하기 위한 IKE 협상의 암호화 방법
- 보낸사람의 ID를 확인하고 메시지가 전송 중에 수정되지 않았는지 확인할 HMAC(Hashed Message Authentication Codes, 해시 메시지 인증 코드) 방법(IKEv2에서는 무결성 알고리즘이라고 함)
- IKEv2의 경우 IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위한 알고리즘으로 사용되는 별도의 PRF(Pseudo Random Function, 의사 난수 함수). 옵션은 해시 알고리즘에 사용되는 것과 동일합니다.
- encryption-key-determination 알고리즘의 수준을 결정하는 Diffie-Hellman 그룹. 디바이스는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- 피어의 ID를 확인할 인증 방법
- 디바이스가 교체 전 암호화 키를 사용하는 시간제한

IKE 협상이 시작되면 협상을 시작한 피어가 모든 정책을 원격 피어로 보내고 원격 피어는 우선 순위대로 자신의 정책과 일치하는 정책을 검색합니다. 암호화, 해시(IKEv2의 경우 무결성 및 PRF), 인증 및 Diffie-Hellman 값이 동일하고 SA 수명이 전송된 정책의 수명보다 작거나 같으면 IKE 정책은 서로 일치하는 것으로 간주됩니다. 수명이 동일하지 않은 경우에는 원격 피어 정책의 더 짧은 수명이 적용됩니다. 기본적으로 Firepower Management Center에서는 협상이 정상적으로 진행되도록 모든 VPN 엔드포인트에 대해 가장 낮은 우선 순위의 IKEv1 정책을 구축합니다.

IPSec

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘의 조합에 의해 보호됩니다.

IPsec 제안 정책은 IPsec 터널에 필요한 설정을 정의합니다. IPsec 제안은 디바이스의 VPN 인터페이스에 적용되는 하나 이상의 암호화 맵 모음입니다. 암호화 맵은 다음과 같이 IPsec 보안 연결을 설정하는 데 필요한 모든 구성 요소를 결합합니다.

- IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합의 제안(변환 집합). IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 제안을 검색합니다. 검색된 제안은 해당 암호화 맵의 액세스 목록에 있는 데이터 흐름을 보호하는 SA를 생성하여 VPN의 트래픽을 보호하는 데 적용됩니다. IKEv1과 IKEv2에 대한 별도의 IPsec 제안이 있습니다. IKEv1 제안(또는 변환 집합)에서 각 파라미터에 대해 하나의 값을 설정합니다. IKEv2 제안의 경우 단일 제안에 여러 개의 암호화와 인증 유형 및 여러 개의 무결성 알고리즘을 구성할 수 있습니다.
- 암호화 맵은 IPsec SA를 정의하는 데 필요한 IPsec 규칙, 제안, 원격 피어 및 기타 파라미터를 비롯하여 IPsec SA(보안 연결)를 필요한 모든 구성 요소를 결합합니다. 두 피어에서 SA를 설정하려고 시도할 때 최소 1개 이상의 호환 가능한 암호화 맵이 있어야 합니다.

  알 수 없는 원격 피어가 로컬 허브와의 IPsec 보안 연결을 시작하려고 하면 동적 암호화 맵 정책이 Site-to-Site VPN에 사용됩니다. 허브는 보안 연결 협상의 이니시에이터가 될 수 없습니다. 동적 암호화 정책은 허브가 원격 피어의 ID를 알지 못하는 경우에도 원격 피어가 IPsec 트래픽을 로컬 허브와 교환할 수 있게 허용합니다. 동적 암호화 맵 정책은 기본적으로 모든 파라미터가 구성되지 않은 상태의 암호화 맵 항목을 생성합니다. 누락된 파라미터는 나중에 원격 피어의 요구사항과 일치하도록 동적으로 구성됩니다(IPsec 협상의 결과).

  동적 암호화 맵 정책은 허브 및 스포크와 및 지점 간 VPN 토폴로지 모두에 적용됩니다. 동적 암호화 맵 정책을 적용하려면 토폴로지의 피어 중 하나에 동적 IP 주소를 지정하고, 이 토폴로지에서 동적 암호화 맵이 활성화되어 있는지 확인합니다. Full-mesh VPN 토폴로지에서는 정적 암호화 맵 정책만 적용할 수 있습니다.

참고 동시 IKEv2 동적 암호화 맵은 FTD(Firepower Threat Defense)의 사이트 간 VPN 및 원격 액세스 모두에 대해 동일한 인터페이스에 지원되지 않습니다.

VPN 패킷 플로우

FTD 디바이스에서 기본적으로 명시적 권한 없이 액세스 컨트롤을 통과하도록 허용되는 트래픽은 없습니다. VPN 터널 트래픽도 Snort를 통과할 때까지 엔드포인트에 릴레이되지 않습니다. 수신 터널 패킷은 Snort 프로세스로 전송되기 전에 암호 해독됩니다. Snort는 암호화되기 전에 발신 패킷을 처리합니다.

VPN 터널의 각 엔드포인트 노드에 대해 보호된 네트워크를 식별하는 액세스 컨트롤은 FTD 디바이스를 통과해 엔드포인트로 이동할 수 있는 트래픽을 결정합니다. Remote Access VPN 트래픽의 경우 VPN 트래픽 흐름을 허용하도록 그룹 정책 필터 또는 액세스 컨트롤 규칙을 구성해야 합니다.

또한 터널이 다운된 상태에서는 공개 소스에 터널 트래픽을 보내지 않습니다.

VPN 라이선싱

Firepower Threat Defense VPN 활성화를 위한 특정 라이선싱은 없으므로 기본적으로 제공됩니다.

Firepower Management Center는 Smart Licensing 서버에서 제공하는 속성을 기준으로 하여 Firepower Threat Defense 디바이스에서 강력한 암호화 사용을 허용할지 아니면 차단할지를 결정합니다.

강력한 암호화 허용 여부는 Cisco Smart License Manager에 등록할 때 디바이스에서 내보내기 제어 기능을 허용하는 옵션을 선택했는지에 따라 제어됩니다. 평가 라이선스를 사용 중이거나 내보내기 제어 기능을 활성화하지 않은 경우에는 강력한 암호화를 사용할 수 없습니다.

평가 라이선스를 사용하여 VPN 설정을 생성한 후 라이선스를 평가에서 내보내기 제어 기능이 있는 스마트 라이선스로 업그레이드한 경우 더 강력한 암호화와 VPN이 제대로 작동하는지 암호화 알고리즘을 확인하고 업데이트하십시오. DES 기반 암호화는 더 이상 지원되지 않습니다.

VPN 연결의 보안 수준 결정

VPN 터널은 일반적으로 공용 네트워크(대개 인터넷)를 통과하므로 연결을 암호화하여 트래픽을 보호해야 합니다. IKE 정책 및 IPsec 제안을 사용하여 적용할 암호화 및 기타 보안 기술을 정의합니다.

디바이스 라이선스에서 강력한 암호화 적용이 허용되는 경우에는 광범위한 암호화 및 해시 알고리즘과 Diffie-Hellman 그룹 중에서 선택할 수 있습니다. 그러나 일반적으로는 터널에 적용하는 암호화가 강력할수록 시스템 성능은 더 나빠집니다. 따라서 효율성을 저하하지 않으면서 충분한 보호 기능을 제공하는 보안과 성능 간의 적절한 균형 지점을 찾아야 합니다.

Cisco는 선택할 수 있는 옵션에 대한 구체적인 지침을 제공하지는 않습니다. 대규모 기업이나 기타 조직 내에서 보안을 담당하는 경우 충족해야 하는 표준이 이미 정의되어 있을 수 있습니다. 그렇지 않은 경우, 선택할 수 있는 옵션에 대해 조사해야 합니다.

다음 주제에서는 사용 가능한 옵션에 대해 설명합니다.

보안 인증 요구 사항 준수

많은 VPN 설정에는 다양한 보안 인증 표준을 준수할 수 있는 옵션이 있습니다. VPN 구성을 계획하려면 인증 요구 사항 및 사용 가능한 옵션을 검토합니다. 규정 준수와 관련된 추가 시스템 정보는 보안 인증 컴플라이언스, 1469 페이지 섹션을 참조하십시오.

사용할 암호화 알고리즘 결정

IKE 정책 또는 IPsec 제안에 사용할 암호화 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다.

IKEv2의 경우 여러 암호화 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

IPsec 제안의 경우 알고리즘은 인증, 암호화 및 재생 방지 서비스를 제공하는 ESP(Encapsulating Security Protocol)에서 사용됩니다. ESP는 IP 프로토콜 유형 50입니다. IKEv1 IPsec 제안에서 알고리즘 이름에는 ESP- 접두사가 붙습니다.

디바이스 라이선스에 따라 강력한 암호화를 사용할 수 있는 경우 다음 암호화 알고리즘 중에서 선택할 수 있습니다. 강력한 암호화를 사용할 수 없으면 DES만 선택할 수 있습니다.

참고 평가 라이선스에서 스마트 라이선스로 업그레이드하기 전에 암호화 알고리즘을 확인하고 업데이트하여 더 강력한 암호화 및 VPN 설정이 제대로 작동하는지 확인하십시오. AES 기반 암호화를 선택합니다. DES 기반 암호화는 더 이상 지원되지 않습니다.

- AES-GCM - (IKEv2에만 해당됨) 기밀 유지 및 데이터 원본 인증 기능을 제공하는 블록 암호화 작동 모드인 AES-GCM(Advanced Encryption Standard in Galois/Counter Mode)은 AES보다 보안성이 뛰어납니다. AES-GCM은 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다. GCM은 NSA Suite B를 지원하는 데 필요한 AES의 모드입니다. NSA Suite B는 암호화 강도에 대한 연방 기준을 충족시키기 위해 디바이스가 지원해야 하는 암호화 알고리즘 세트입니다. .
- AES - AES(Advanced Encryption Standard)는 DES보다 보안성이 뛰어나며 3DES보다 계산 효율성이 높은 대칭 암호화 알고리즘입니다. AES는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.
- DES - 56비트 키를 사용하여 암호화를 수행하는 DES(Data Encryption Standard)는 대칭 보안 키 블록 알고리즘입니다. 라이선스 어카운트가 내보내기 제어에 대한 요건을 충족하지 않는 경우에는 이 옵션이 유일한 옵션입니다.
- null - null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이 알고리즘은 대개 테스트용으로만 사용됩니다.

사용할 해시 알고리즘 결정

IKE 정책에서 해시 알고리즘은 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성합니다. IKEv2에서 해시 알고리즘은 두 가지 옵션으로 구분됩니다. 그중 하나는 무결성 알고리즘 옵션이고 다른 하나는 PRF(Pseudo-Random Function: 의사 난수 함수) 옵션입니다.

IPsec 제안에서 해시 알고리즘은 인증을 위한 ESP(Encapsulating Security Protocol)에서 사용됩니다. IKEv2 IPsec 제안에서는 이러한 알고리즘을 무결성 해시라고 합니다. IKEv1 IPsec 제안에서는 알고리즘 이름에 ESP- 접두사가 붙으며 -HMAC(Hash Method Authentication Code) 접미사도 붙습니다.

IKEv2의 경우 여러 해시 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

다음 해시 알고리즘 중에서 선택할 수 있습니다.

- SHA(Secure Hash Algorithm) - 표준 SHA(SHA1)에서는 160비트 다이제스트를 생성합니다.

IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.

- SHA256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
- SHA384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
- SHA512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.

- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 AES-GCM 옵션 중 하나를 암호화 알고리즘으로 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null 이외의 옵션을 선택하더라도 이러한 암호화 표준에 대해서는 무결성 해시가 무시됩니다.

사용할 **Diffie-Hellman** 모듈러스 그룹 결정

다음 Diffie-Hellman 키 파생 알고리즘을 사용하여 IPsec 보안 연계(SA) 키를 생성할 수 있습니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에 일치하는 모듈러스 그룹이 있어야 합니다.

AES 암호화를 선택하는 경우 AES에 필요한 큰 키를 지원하려면 DH(Diffie-Hellman) 그룹 5 이상을 사용해야 합니다. IKEv1 정책에서는 아래에 나열된 그룹을 모두 지원하지는 않습니다.

NSA Suite B 암호화 사양을 구현하려면 IKEv2를 사용하고 ECDH(Elliptic Curve Diffie-Hellman) 옵션 19, 20, 21 중 하나를 선택합니다. 2048비트 모듈러스를 사용하는 엘립틱 커브 옵션과 그룹은 Logjam과 같은 공격에 노출될 가능성이 작습니다.

IKEv2의 경우에는 여러 그룹을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 15 - Diffie-Hellman 그룹 15: 3072비트 MODP 그룹
- 16 - Diffie-Hellman 그룹 16: 4096비트 MODP 그룹
- 19 - Diffie-Hellman 그룹 19: NIST(국내 표준 및 기술) 256비트 ECP(elliptic curve modulo a prime) 그룹
- 20 - Diffie-Hellman 그룹 20: NIST 384비트 ECP 그룹
- 21 - Diffie-Hellman 그룹 21: NIST 521비트 ECP 그룹

제거되었거나 사용되지 않는 해시 알고리즘, 암호화 알고리즘 및 **Diffie-Hellman** 모듈러스 그룹

보안 수준이 낮은 암호에 대한 지원이 제거되었습니다. VPN이 올바르게 작동하도록 FTD 6.70을 지원되는 DH 및 암호화 알고리즘으로 업그레이드하기 전에 VPN 설정을 업데이트하는 것이 좋습니다.

FTD 6.70에서 지원되는 것과 일치하도록 IKE 제안 및 IPSec 정책을 업데이트한 다음 설정 변경 사항을 구축합니다.

다음과 같이 안전성이 상대적으로 낮은 암호는 FTD 6.70 이상에서 제거되었거나 더 이상 사용되지 않습니다.

- **Diffie-Hellman GROUP 5**는 IKEv1에서 더 이상 사용되지 않으며 IKEv2에서 제거됩니다.
- Diffie-Hellman GROUP 2 및 24가 제거되었습니다.
- 암호화 알고리즘: 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256이 제거되었습니다.

참고

DES는 평가 모드에서 또는 강력한 암호화를 위한 내보내기 제어 항목을 충족하지 않는 사용자를 대상으로 계속 지원됩니다.

NULL은 IKEv2 정책에서 제거되지만, IKEv1 및 IKEv2 IPsec 변형 집합에서 모두 지원됩니다.

VPN 토폴로지 옵션

새 VPN 토폴로지를 생성할 때 고유한 이름을 부여하고 토폴로지 유형을 지정하고 IKE 버전을 선택해야 합니다. 각각 VPN 터널의 그룹을 포함하는 3가지 토폴로지 유형 중에서 선택할 수 있습니다.

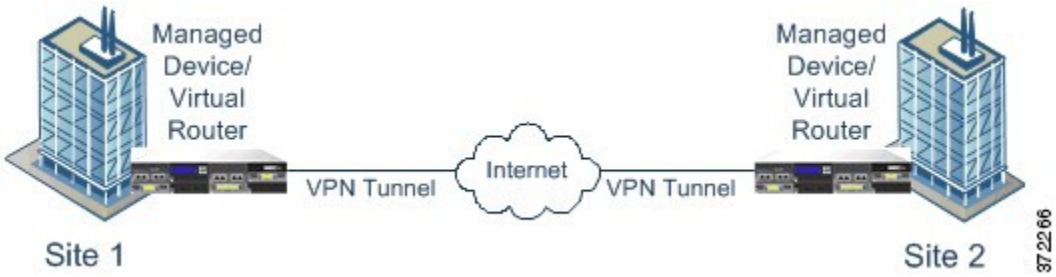
- Point-to-Point 토폴로지에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.
- 허브 앤 스포크 토폴로지는 허브 엔드포인트를 스포크 엔드포인트 그룹에 연결하는 VPN 터널 그룹을 설정합니다.
- 풀 메시 토폴로지는 일련의 엔드포인트 사이에 VPN 터널 그룹을 설정합니다.

VPN 인증을 위한 사전 공유 키를 수동 또는 자동으로 정의합니다. 기본 키는 없습니다. 자동을 선택하면 Firepower Management Center에서 사전 공유 키를 생성하고 토폴로지의 모든 노드에 할당합니다.

Point-to-Point VPN 토폴로지

포인트 투 포인트 VPN 토폴로지에서는 2개의 엔드포인트가 서로 직접 통신합니다. 두 엔드포인트를 피어 디바이스로 구성하며, 두 디바이스 중 하나가 보안 연결을 시작할 수 있습니다.

다음 다이어그램은 일반적인 포인트 투 포인트 VPN 토폴로지를 보여줍니다.

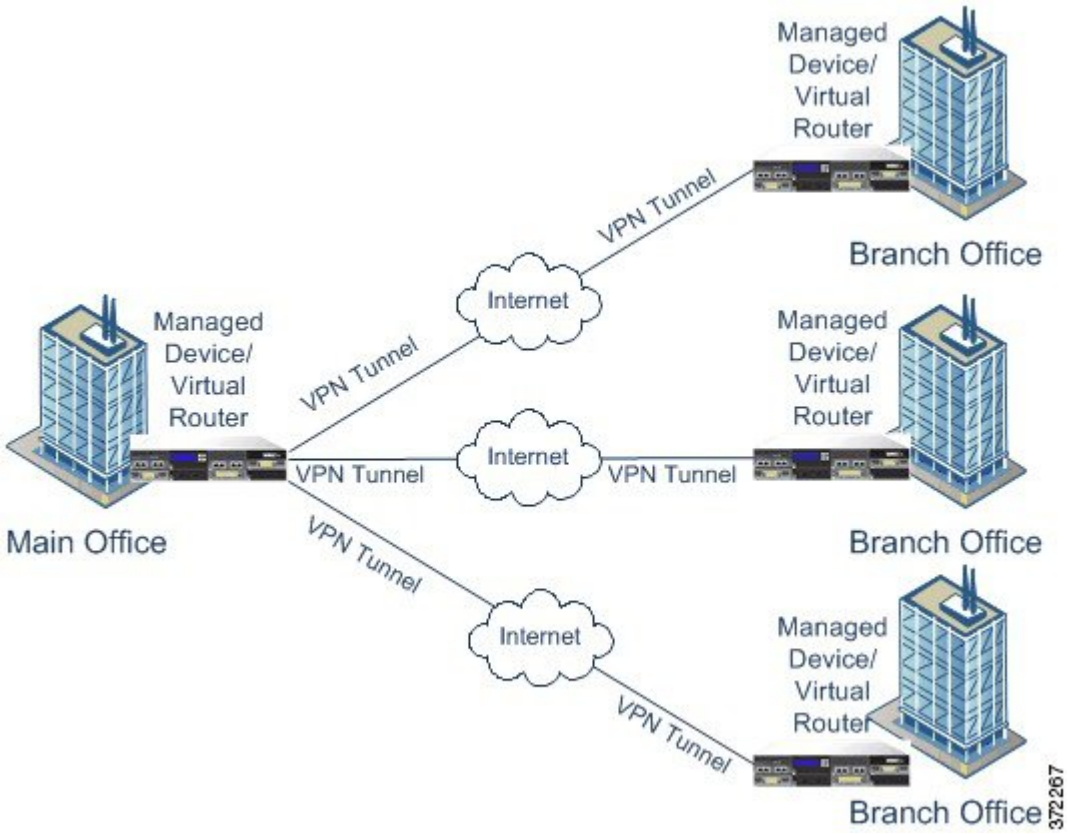


허브 앤 스포크 VPN 토폴로지

허브 앤 스포크 VPN 토폴로지에서 중앙 엔드포인트(허브 노드)는 여러 원격 엔드포인트(스포크 노드)와 연결됩니다. 허브 노드와 개별 스포크 엔드포인트 사이의 각 연결은 별도의 VPN 터널입니다. 스포크 노드 뒤에 있는 호스트는 허브 노드를 통해 서로 통신할 수 있습니다.

허브 앤 스포크 토폴로지는 주로 인터넷이나 기타 서드파티 네트워크를 통한 보안 연결을 사용하여 조직의 본사 및 지사 위치와 연결하는 VPN을 나타냅니다. 이러한 구축에서는 모든 직원이 조직의 네트워크에 대해 통제된 액세스 권한을 갖습니다. 일반적으로 허브 노드는 본사에 있습니다. 스포크 노드는 지사에 있으며 대부분의 트래픽을 시작합니다.

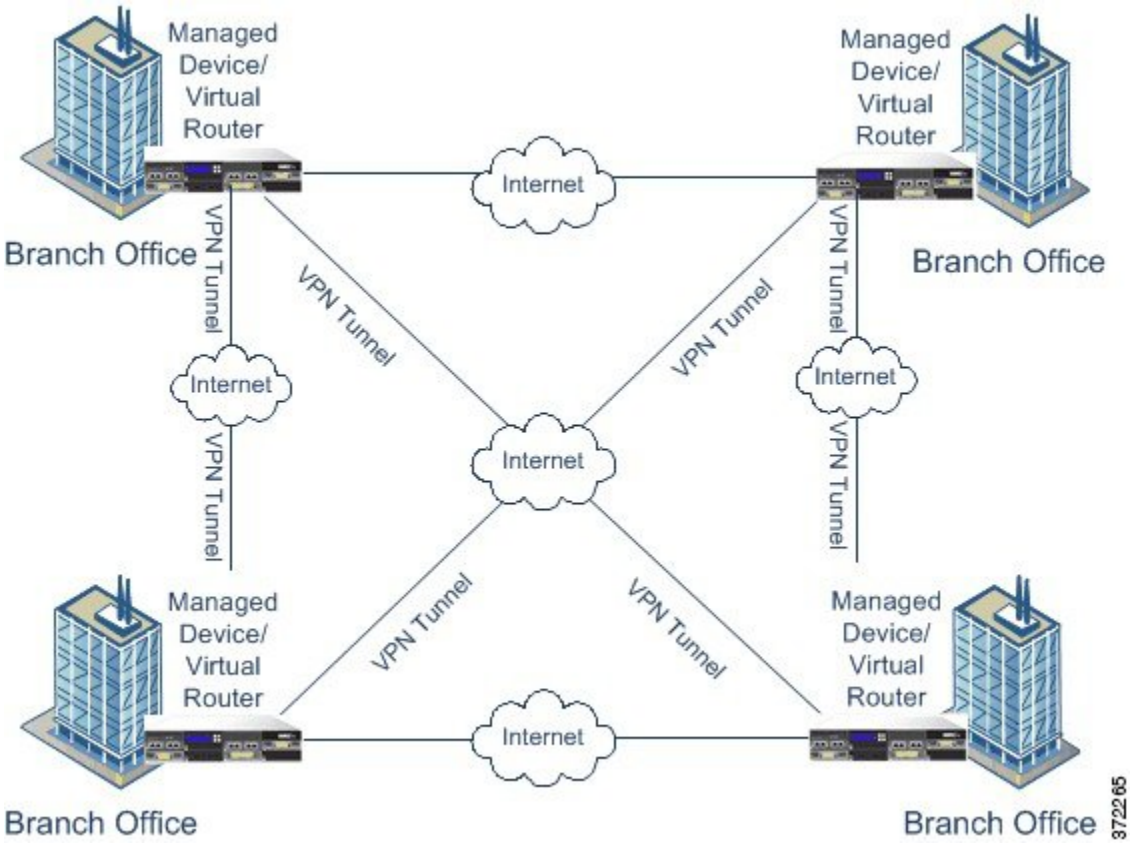
다음 다이어그램은 일반적인 허브 앤 스포크 VPN 토폴로지를 보여줍니다.



풀 메시 VPN 토폴로지

풀 메시 VPN 토폴로지에서는 모든 엔드포인트가 개별 VPN 터널을 통해 다른 모든 엔드포인트와 통신할 수 있습니다. 이 토폴로지에서는 한 엔드포인트에 장애가 발생할 경우에도 나머지 엔드포인트는 여전히 서로 통신할 수 있다는 점에서 이중화를 제공합니다. 이는 대개 분산된 지사의 위치를 연결하는 VPN에 사용됩니다. 이러한 구성으로 구축하는 VPN을 지원하는 관리 대상 디바이스의 수는 필요한 이중화 레벨에 따라 달라집니다.

다음 다이어그램은 일반적인 풀 메시 VPN 토폴로지를 보여줍니다.



암시적 토폴로지

세 가지 주요 VPN 토폴로지 외에도 이 토폴로지의 조합으로 더욱 복잡한 다른 토폴로지를 생성할 수 있습니다. 그 기능은 다음과 같습니다.

- 부분 메시 - 일부 디바이스가 풀 메시 토폴로지로 구성되고 다른 디바이스는 허브 앤 스포크 또는 일부 메시 디바이스에 대한 Point-to-Point 연결을 구성하는 네트워크입니다. 부분 메시는 전체 메시 토폴로지의 이중화 레벨을 제공하지는 않지만 구현하는 데 비용이 적게 듭니다. 부분 메시 토폴로지는 완전한 메시 백본에 연결되는 주변 장치 네트워크에 사용됩니다.
- 계층화된 허브 앤 스포크 - 디바이스가 하나 이상의 토폴로지에서 허브로 작동하고 다른 토폴로지에서 스포크로 작동할 수 있는 허브 앤 스포크 토폴로지의 네트워크입니다. 트래픽은 스포크 그룹에서 가장 즉각적인 허브까지 허용됩니다.
- 조인된 허브 앤 스포크 - Point-to-Point 터널을 형성하기 위해 연결되는 두 개의 토폴로지(허브 앤 스포크, 포인트 투 포인트 또는 풀 메시)의 조합입니다. 예를 들어 조인된 허브 앤 스포크 토폴로지는 Point-to-Point 토폴로지의 피어 디바이스로 작동하는 허브가 있는 두 개의 허브 앤 스포크 토폴로지로 구성될 수 있습니다.

44 장

Site-to-Site VPN Firepower Threat Defense

- Firepower Threat Defense Site-to-Site VPN 정보, 1133 페이지
- 사이트 간 VPN 요구 사항 및 사전 요건, 1135 페이지
- Firepower Threat Defense Site-to-Site VPN 관리, 1136 페이지
- Firepower Threat Defense Site-to-Site VPN 구성, 1137 페이지
- Virtual Tunnel Interface 정보, 1146 페이지
- Virtual Tunnel Interface에 대한 지침 및 제한 사항, 1147 페이지
- VTI 인터페이스 추가, 1148 페이지
- 라우트 기반 사이트 대 사이트 VPN 생성, 1149 페이지
- VTI에 대한 추가 구성, 1150 페이지
- 사이트 간 VPN 기록 , 1152 페이지

Firepower Threat Defense Site-to-Site VPN 정보

Firepower Threat Defense Site-to-Site VPN은 다음 기능을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 인증서 및 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 Site-to-Site VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.
- Firepower Management Center 및 FTD HA 환경에 대한 지원.
- 터널이 다운될 때 VPN 알림.
- FTD Unified CLI를 통해 사용 가능한 터널 통계.
- Point-to-Point 엑스트라넷 및 허브 앤 스포크 VPN에 대한 IKEv1 및 IKEv2 백업 피어 구성 지원.
- '허브 앤 스포크' 구축에서 허브로 작동하는 엑스트라넷 디바이스 지원.

- 'Point-to-Point' 구축에서 엑스트라넷 디바이스와 페어링된 관리 대상 엔드포인트의 동적 IP 주소 지원.
- 엔드포인트로 작동하는 엑스트라넷 디바이스의 동적 IP 주소 지원.
- '허브 앤 스포크' 구축에서 엑스트라넷으로 작동하는 허브 지원.

VPN 토폴로지

새로운 Site-to-Site VPN 토폴로지를 생성하려면 고유한 이름을 부여하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다를 선택해야 합니다. 또한 . 구성된 후 토폴로지를 Firepower Threat Defense 디바이스에 구축합니다. Firepower Management Center는 FTD 디바이스에서만 Site-to-Site VPN을 구성합니다.

하나 이상의 VPN 터널을 포함하는 3가지 토폴로지 유형 중에서 선택할 수 있습니다.

- Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.
- 허브 앤 스포크 구축은 허브 엔드포인트를 스포크 노드 그룹에 연결하는 VPN 터널 그룹을 설정합니다.
- 풀 메시 구축은 일련의 엔드포인트 사이에 VPN 터널 그룹을 설정합니다.

IPsec 및 IKE

Firepower Management Center에서 Site-to-Site VPN은 IKE 정책과 VPN 토폴로지에 할당된 IPsec 제안을 기반으로 구성됩니다. 정책 및 제안은 IPsec 터널에서 트래픽을 보호하는 데 사용되는 보안 프로토콜 및 알고리즘과 같은 Site-to-Site VPN의 특성을 정의하는 파라미터 집합입니다. VPN 토폴로지에 할당할 수 있는 전체 구성 이미지를 정의하려면 몇 가지 정책 유형이 필요할 수 있습니다.

인증

엑스트라넷 디바이스

각 토폴로지 유형에는 Firepower Management Center에서 관리되지 않는 디바이스인 엑스트라넷 디바이스가 포함될 수 있습니다. 예를 들면 다음과 같습니다.

- Firepower Management Center에서 지원하지만 조직에는 책임이 부여되지 않는 Cisco 디바이스. 회사 내의 다른 조직에서 관리하는 네트워크의 스포크 또는 서비스 제공자나 파트너의 네트워크에 대한 연결 등이 포함됩니다.
- 타사 디바이스. Firepower Management Center를 사용하여 타사 디바이스에 구성을 생성하거나 구축할 수 없습니다.

타사 디바이스 또는 Firepower Management Center가 관리하지 않는 Cisco 디바이스를 '엑스트라넷' 디바이스로 VPN 토폴로지에 추가합니다. 또한 각 원격 디바이스의 IP 주소를 지정합니다.

Firepower Threat Defense Site-to-Site VPN 지침 및 제한 사항

- VPN 연결은 현재 도메인에 존재하지 않는 엔드포인트에 대해 엑스트라넷 피어를 사용하여 도메인 전반에서만 수행될 수 있습니다.
- VPN 토폴로지는 도메인 간에 이동할 수 없습니다.
- '범위 '옵션이 있는 네트워크 개체는 VPN에서 지원되지 않습니다.
- Firepower Threat Defense VPN은 Firepower Management 백업을 통해서만 백업됩니다.
- Firepower Threat Defense VPN은 현재 PDF 내보내기 및 정책 비교를 지원하지 않습니다.
- Firepower Threat Defense VPN에는 터널별 또는 디바이스별 편집 옵션이 없으므로 전체 토폴로지만 편집할 수 있습니다.
- FTD VPN은 클러스터링된 환경에서 지원되지 않습니다.
- 터널 상태는 실시간으로 업데이트되지 않지만 Firepower Management Center에서 5분 간격으로 업데이트됩니다.
- 전송 모드는 지원되지 않으며 터널 모드만 지원됩니다. IPsec 터널 모드는 새 IP 패킷에서 페이로드가 되는 원래 IP 데이터그램 전체를 암호화합니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPSec이 구현되는 통상적인 방식입니다.
- "(큰 따옴표)는 사전 공유 키로 지원되지 않습니다. 사전 공유 키에서 "를 사용한다면, Firepower Threat Defense 6.30으로 업그레이드한 후에 해당 문자를 변경해야 합니다.

사이트 간 VPN 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

Leaf

사용자 역할

관리자

Firepower Threat Defense Site-to-Site VPN 관리

프로시저

단계 **1** VPN에 대한 인증서 인증의 경우 Firepower Threat Defense 인증서 기반 인증, 675 페이지에서 설명한 대로 신뢰 지점을 할당하여 디바이스를 준비해야 합니다.

단계 **2** **Devices(**디바이스**) > VPN > Site to Site(**사이트 대 사이트**)**를 선택하여 Firepower Threat Defense Site-to-Site VPN 구성 및 구축을 관리하십시오. 다음 중에서 선택합니다.

- 추가 - 새 VPN 토폴로지를 생성하려면 추가( )**Add VPN(VPN** 추가**) > Firepower Threat Defense Device(Firepower Threat Defense** 디바이스**)**를 클릭하고 Firepower Threat Defense Site-to-Site VPN 구성, 1137 페이지의 설명에 따라 계속 진행합니다.

  참고 VPN 토폴로지는 리프 도메인에서만 생성될 수 있습니다.

- 편집 - 기존 VPN 토폴로지의 설정을 수정하려면 수정( )을 클릭합니다. 수정 방법은 구성 방법과 비슷하며, 위의 설명에 따라 계속 진행합니다.

  참고 토폴로지 유형을 처음 저장한 후에는 편집할 수 없습니다. 토폴로지 유형을 변경하려면 토폴로지를 삭제하고 새 토폴로지를 생성합니다.

  사용자 두 명이 RA VPN 정책을 동시에 수정할 수 없으나, 웹 인터페이스에서는 동시 수정이 차단되지 않습니다.

- 삭제 - VPN 구축을 삭제하려면 삭제( )를 클릭합니다.

- VPN 상태 보기 - 이 상태는 Firepower VPN에만 적용됩니다. 현재 FTD VPN에 대한 상태는 표시되지 않습니다. FTD VPN 상태를 확인하려면 Firepower Threat Defense VPN 모니터링, 1231 페이지 섹션을 참조하십시오.

- 구축 - **Deploy(**구축**) > Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

  참고 일부 VPN 설정은 구축 도중에만 검증됩니다. 구축에 성공했는지 확인하십시오.

Firepower Threat Defense Site-to-Site VPN 구성

프로시저

단계 **1** **Devices(**장치**) > VPN > Site To Site(**사이트 대 사이트**)**. 그런 다음 **Add VPN(VPN** 추가**) > Firepower Threat Defense Device** 또는 나열된 VPN Topology(VPN 토폴로지)를 수정합니다.을(를) 선택합니다.

단계 **2** 고유한 토폴로지 이름을 입력합니다. FTD VPN 및 토폴로지 유형을 나타내기 위해 토폴로지의 이름을 지정하는 것이 좋습니다.

단계 **3** 사이트 대 사이트 VPN을 구성하려면 **Policy Based(Crypto Map)(**정책 기반**(**암호화 맵**)**를 클릭합니다.

단계 **4** 이 VPN에 대한 **Network Topology(**네트워크 토폴로지**)**를 선택합니다.

단계 **5** IKE 협상 중에 사용할 IKE 버전을 선택합니다. **IKEv1** 또는 **IKEv2**입니다.

기본값은 IKEv2입니다. 적절한 옵션 중 하나 또는 두 가지를 선택합니다. 토폴로지의 디바이스가 IKEv2를 지원하지 않으면 IKEv1을 선택합니다.

단계 **6** 필수: 토폴로지의 각 노드에 대한 추가(+)을 클릭하여 이 VPN 구축에 대한 엔드포인트를 추가합니다.

FTD VPN 엔드포인트 옵션, 1138 페이지의 설명에 따라 각 엔드포인트 필드를 구성합니다.

- Point-to-Point의 경우 노드 **A**와 노드 **B**를 구성합니다.
- 허브 앤 스포크의 경우 허브 노드 및 스포크 노드를 구성합니다.
- 풀 메시의 경우 여러 노드를 구성합니다.

단계 **7** (선택 사항) 설명에 따라 이 구축에 대해 기본값 이외의 IKE 옵션을 지정합니다. FTD VPN IKE 옵션, 1140 페이지

단계 **8** (선택 사항) 설명에 따라 이 구축에 대해 기본값 이외의 IPSec 옵션을 지정합니다. FTD VPN IPsec 옵션, 1141 페이지

단계 **9** (선택 사항) FTD 고급 Site-to-site VPN 구축 옵션, 1143 페이지FTD 고급 VPN 구축 옵션의 설명에 따라 이 구축에 대해 기본값 이외의 고급 옵션을 지정합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.
엔드포인트가 구성에 추가됩니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

참고 일부 VPN 설정은 구축 도중에만 검증됩니다. 구축에 성공했는지 확인하십시오.

VPN 세션이 가동 중일 때도 VPN 터널이 비활성 상태라는 알림이 표시되면 VPN 문제 해결 지침에 따라 VPN이 활성 상태인지 확인합니다. 자세한 내용은 Firepower Threat Defense VPN 모니터링, 1231 페이지 및 Firepower Threat Defense VPN 문제 해결, 1235 페이지 섹션을 참고하십시오.

FTD VPN 엔드포인트 옵션

탐색 경로

Devices(디바이스**) > VPN > Site To Site(**사이트 대 사이트**)**. 그런 다음 **ADD VPN(VPN** 추가**) > Firepower Threat Defense Device**, 또는 나열된 VPN Topology(VPN 토폴로지)를 수정합니다. **Endpoint(**엔드포인트**)** 탭을 엽니다.

필드

디바이스

다음과 같이 구축에 대한 엔드포인트 노드를 선택합니다.

- Firepower Management Center에서 관리되는 FTD 디바이스.
- Firepower Management Center에서 관리되는 FTD 고가용성 컨테이너.
- 이 Firepower Management Center에서 관리하지 않는 모든 디바이스인 엑스트라넷 디바이스(Cisco 또는 타사).

Device Name(디바이스 이름**)**

엑스트라넷 디바이스의 경우에만 이 디바이스의 이름을 제공합니다. 관리되지 않는 디바이스로 식별할 수 있도록 이름을 지정하는 것이 좋습니다.

인터페이스

매니지드 디바이스를 엔드포인트로 선택한 경우 해당 디바이스에서 인터페이스를 선택합니다.

'Point-to-Point' 구축의 경우 동적 인터페이스로 엔드포인트를 구성할 수도 있습니다. 동적 인터페이스가 있는 엔드포인트는 엑스트라넷 디바이스와 페어링될 수 있으며 매니지드 디바이스가 있는 엔드포인트와는 페어링할 수 없습니다.

Devices(디바이스**) > Device Management(**디바이스 관리**) > Add/Edit device(**디바이스 추가/편집**) > Interfaces(**인터페이스**)**에서 디바이스 인터페이스를 구성할 수 있습니다.

IP 주소

- Firepower Management Center에서 관리하지 않는 엑스트라넷 디바이스를 선택하는 경우 엔드포인트의 IP 주소를 지정합니다.

  엑스트라넷 디바이스에서 동적 엑스트라넷 디바이스를 허용하려면 **Static(**정적**)**을 선택하고 IP 주소를 지정하거나 **Dynamic(**동적**)**을 선택합니다.

- 매니지드 디바이스를 엔드포인트로 선택한 경우 드롭다운 목록에서 단일 IPv4 주소 또는 여러 IPv6 주소(이 관리되는 디바이스의 인터페이스에 이미 할당된 주소)를 선택합니다.
- 토폴로지의 모든 엔드포인트는 동일한 IP 주소 체계를 가져야 합니다. IPv4 터널은 IPv6 트래픽을 전달할 수 있으며 그 반대도 마찬가지입니다. 보호되는 네트워크는 터널링된 트래픽이 사용할 주소 체계를 정의합니다.
- 매니지드 디바이스가 고가용성 컨테이너인 경우 인터페이스 목록에서 선택합니다.

이 **IP**는 비공개입니다

엔드포인트가 네트워크 주소 변환(NAT) 기능을 갖춘 방화벽의 뒤에 상주할 경우 확인란을 선택합니다.

공용 **IP** 주소

This IP is Private(이 **IP**는 비공개입니다**)** 확인란을 선택한 경우 방화벽의 공용 IP 주소를 지정합니다. 엔드포인트가 responder일 경우 이 값을 지정합니다.

연결 유형

허용되는 협상을 양방향, 응답 전용 또는 시작 전용으로 지정합니다. 연결 유형에 대해 지원되는 조합은 다음과 같습니다.

표 ***81:*** 지원되는 연결 유형 조합

Remote 노드	**Central** 노드
Originate-Only	Answer-Only
양방향	Answer-Only
양방향	양방향

인증서 맵

사전 구성된 인증서 맵 개체를 선택하거나 추가(+)을 클릭하여 VPN 연결에 유효하도록 수신된 클라이언트 인증서에 필요한 정보를 정의하는 인증서 맵 개체를 추가합니다. 자세한 내용은 FTD 인증서 맵 개체, 665 페이지를 참조하십시오.

보호되는 네트워크

이 VPN 엔드포인트가 보호하는 네트워크를 정의합니다. 사용 가능한 네트워크 개체를 선택하거나 네트워크 개체를 인라인으로 추가하려면 추가(+)을 클릭합니다. 네트워크 개체 생성, 571 페이지의 내용을 참조하십시오. ACL(Access Control Lists)은 여기에서 선택한 항목에서 생성됩니다.

- **Subnet/IP Address (Network)(**서브넷**/IP** 주소**(**네트워크**))** - VPN 엔드포인트는 동일한 IP 주소를 가질 수 없으며 VPN 엔드포인트 쌍의 보호되는 네트워크는 중복될 수 없습니다. 어떤 엔드포인트의 보안 네트워크 목록에 IPv4 또는 IPv6 항목이 하나 이상 포함될 경우 나머지 엔드포인트의 보안 네트워크는 동일한 유형(즉 IPv4 또는 IPv6)의 항목을 하나 이상 가져야 합니다. 그렇지 않으면 나머지 엔드포인트의 IP 주소가 동일한 유형이고 또한 보안 네트워

크의 항목과 중복되지 않아야 합니다. (IPv4에는 /32 CIDR 주소 영역을, IPv6에는 /128 CIDR 주소 영역을 사용합니다.) 두 검사 모두 실패할 경우 엔드포인트 쌍은 잘못된 것입니다.

참고 역방향 경로 삽입은 **Firepower Management Center**에서 기본적으로 활성화되어 있습니다.

보호되는 네트워크를 *Any(*모두*)*로 선택하고 트래픽 기본 경로 트래픽의 삭제를 확인하면 **VPN**> **Site to Site** > edit a VPN(VPN 편집) > **IPsec** > **Enable Reverse Route Injection(Reverse Route Injection** 비활성화**)**에서 Reverse Route Injection을 비활성화합니다. 구성 변경 사항을 구축합니다. 이렇게 하면 암호화 맵 구성의 set reverse-route(Reverse Route Injection)가 제거되고 역방향 터널 트래픽이 삭제되도록 유도하는 VPN-advertised reverse route가 제거됩니다.

-

Advanced Settings(고급 설정**)**

동적 **RRI(Reverse Route Injection)** 활성화 - RRI(Reverse Route Injection)는 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 경로를 자동으로 삽입할 수 있는 기능입니다. 동적 RRI 경로는 IPsec SA(Security Associations)를 성공적으로 설정한 경우에만 생성됩니다.

참고
- 동적 RRI는 IKEv2에서만 지원되며 IKEv1 또는 IKEv1 + IKEv2에서는 지원되지 않습니다.
- 동적 RRI는 발신 전용 피어, 풀 메시 토폴로지 및 엑스트라 넷 피어에서 지원되지 않습니다.
- 포인트 투 포인트에서는 한 피어에서만 동적 RRI를 활성화할 수 있습니다.
- 허브와 스포크 간에는 엔드포인트 중 하나만 동적 RRI를 활성화할 수 있습니다.
- 동적 RRI는 동적 암호화 맵과 결합할 수 없습니다.

FTD VPN IKE 옵션

이 토폴로지에 대해 선택한 IKE 버전의 경우 **IKEv1/IKEv2** 설정을 지정합니다.

참고 이 대화 상자의 설정은 전체 토폴로지, 모든 터널 및 모든 매니지드 디바이스에 적용됩니다.

탐색 경로

Devices(디바이스**) > VPN > Site To Site(**사이트 대 사이트**)**. 그런 다음 **ADD VPN(VPN** 추가**) > Firepower Threat Defense Device**, 또는 나열된 VPN Topology(VPN 토폴로지)를 수정합니다. **IKE** 탭을 엽니다.

필드

정책
사전 정의된 IKEv1 또는 IKEv2 정책 개체를 선택하거나 사용할 정책 개체를 새로 만듭니다. 자세한 내용은 다음 섹션을 참조하십시오. FTD IKE 정책, 651 페이지

키 유형

- **Manual(**수동**)** - 이 VPN에 대해 사용되는 사전 공유 키를 수동으로 할당합니다. **Key(**키**)**를 지정하고 **Confirm Key(**확인 키**)**에 다시 입력합니다.
- **Automatic(**자동**)** - Management Center는 이 VPN에 사용되는 사전 공유 키를 자동으로 정의합니다. **Key Length(**키 길이**)**에 키의 문자 수(1~27)를 지정합니다.

FTD VPN IPsec 옵션

참고 이 대화 상자의 설정은 전체 토폴로지, 모든 터널 및 모든 매니지드 디바이스에 적용됩니다.

암호화 맵 유형
암호화 맵은 IPsec 보안 연결(SA)을 설정하는 데 필요한 모든 구성 요소를 결합합니다. 두 피어에서 SA를 설정하려고 시도할 때 최소 1개 이상의 호환 가능한 암호화 맵이 있어야 합니다. 암호화 맵 항목에 정의된 제안은 IPsec 보안 협상에 사용되어 해당 암호화 맵의 IPsec 규칙에 지정된 데이터 흐름을 보호합니다. 이 구축의 암호화 맵에 대해 정적 또는 동적 여부를 선택합니다.

- **Static(**정적**)** - Point-to-Point 또는 풀 메시 VPN 토폴로지에서 정적 암호화 맵을 사용합니다.
- **Dynamic(**동적**)** -동적 암호화 맵은 기본적으로 모든 파라미터가 구성되지 않은 상태의 암호화 맵 항목을 생성합니다. 누락된 파라미터는 나중에 원격 피어의 요구 사항과 일치하도록 동적으로 구성됩니다(IPsec 협상의 결과).

  동적 암호화 맵 정책은 허브 및 스포크와 및 지점 간 VPN 토폴로지 모두에 적용됩니다. 동적 암호화 맵 정책을 적용하려면 토폴로지의 피어 중 하나에 동적 IP 주소를 지정하고, 이 토폴로지에서 동적 암호화 맵이 활성화되어 있는지 확인합니다. Full-mesh VPN 토폴로지에서는 정적 암호화 맵 정책만 적용할 수 있습니다.

IKEv2 모드

IKEv2의 경우 터널에 ESP 암호화 및 인증을 적용하려면 캡슐화 모드를 지정합니다. 이는 원래 IP 패킷의 어느 부분에 ESP가 적용되어 있는지 결정합니다.

- **Tunnel(**터널**)** 모드 - (기본값) 캡슐화 모드가 터널 모드로 설정됩니다. Tunnel(터널) 모드는 전체 원래 IP 패킷(IP 헤드 및 데이터)에 ESP 암호화 및 인증을 적용하여 최종 소스 및 대상 주소를 숨기며 새 IP 패킷에서 페이로드가 됩니다.

  터널 모드의 주요 장점은 IPsec이 보장하는 이점을 위해 최종 시스템을 수정할 필요가 없다는 점입니다. 이 모드에서는 라우터와 같은 네트워크 디바이스가 IPsec 프록시 역할을 합니다. 즉, 라우터는 호스트를 대신하여 암호화를 수행합니다. 소스 라우터는 패킷을 암호화하고 IPsec 터널을 따라 패킷을 전달합니다. 대상 라우터는 원래 IP 데이터그램을 암호 해독하

고 대상 시스템으로 전달합니다. 터널 모드는 또한 트래픽 분석으로부터 보호 기능을 제공하므로 터널 모드를 통해 공격자는 터널 엔드포인트만 판단할 수 있으며 터널링된 패킷이 터널 엔드포인트와 동일하더라도 해당 소스 및 대상은 판단할 수 없습니다.

- **Transport preferred(**기본 설정 전송**)** - 피어가 지원하지 않는 경우 캡슐화 모드는 터널 모드에 대한 폴백 옵션을 사용하는 전송 모드로 설정됩니다. Transport(전송) 모드에서는 IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다. 따라서 관리자는 VPN 인터페이스 IP 주소와 일치하는 보호되는 네트워크를 선택해야 합니다.

  이 모드는 적은 바이트만 각각의 패킷에 추가하고 공용 네트워크에서 디바이스가 패킷의 최종 소스 및 대상을 확인할 수 있다는 이점이 있습니다. 전송 모드를 사용하면 IP 헤더의 정보에 기반하여 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다. 그러나 패킷 검사를 제한하는 Layer 4 헤더가 암호화됩니다.

- **Transport required(**전송 필요**)** - 캡슐화 모드가 전송 모드로 설정되며, 터널 모드의 폴백이 허용되지 않습니다. 협상을 지원하지 않는 하나의 엔드포인트로 인해 여러 엔드포인트가 전송 모드를 성공적으로 협상할 수 없는 경우 VPN 연결이 수행되지 않습니다.

제안

수정( )을 클릭하여 선택한 IKEv1 또는 IKEv2 방법에 대한 제안을 지정합니다. 사용 가능한 **IKEv1 IPsec** 제안 또는 **IKEv2 IPsec** 제안 개체 중에서 선택하거나 새로 생성한 다음 선택합니다. 자세한 내용은 IKEv1 IPsec 제안 개체 설정, 654 페이지 및 IKEv2 IPsec 제안 개체 설정, 655 페이지 섹션을 참조하십시오.

SA(Security Association) 강점 시행 활성화

이 옵션을 활성화하면 하위 IPsec SA에서 사용하는 암호화 알고리즘이 상위 IKE SA에 비해 키의 비트 수와 관련하여 더 강점을 보이지 않습니다.

Reverse Route Injection 활성화

Reverse Route Injection(RRI)은 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 정적 경로를 자동으로 삽입할 수 있도록 활성화합니다.

PFS(Perfect Forward Secrecy) 활성화

PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용할지를 결정합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. 이 옵션을 선택하는 경우 모듈러스 그룹 목록에서 PFS 세션 키를 생성할 때 사용할 Diffie-Hellman 키 파생 알고리즘도 선택합니다.

모듈러스 그룹

공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 자세한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 1127 페이지를 참조하십시오.

라이프타임

만료되기 전에 보안 연결이 있는 시간(초)입니다. 기본값은 28,800초입니다.

수명 크기

만료되기 전에 지정된 보안 연결을 사용하여 IPsec 피어 간에 전달할 수 있는 트래픽 볼륨(KB)입니다. 기본값은 4,608,000킬로바이트입니다. 무한 데이터는 허용되지 않습니다.

ESPv3 설정

수신 **ICMP** 오류 메시지 확인
IPsec 터널을 통해 수신되고 비공개 네트워크의 내부 호스트로 전달되는 이러한 ICMP 오류 메시지를 검증할지 여부를 선택합니다.

'Do Not Fragment(조각화 금지**)'** 정책 활성화
IPsec 하위 시스템에서 IP 헤더에 DF(Do Not Fragment) 비트가 설정된 대용량 패킷을 처리하는 방법을 정의합니다.

정책

- Copy DF bit(DF 비트 복사) - DF 비트를 유지합니다.
- Clear DF bit(DF 비트 지우기) - DF 비트를 무시합니다.
- Set DF bit(DF 비트 설정) - DF 비트를 설정하고 사용합니다.

TFC(Traffic Flow Confidentiality) 패킷 활성화
터널을 우회하는 트래픽 프로파일을 마스킹하는 더미 TFC 패킷을 활성화합니다. **Burst(**버스트**)**, **Payload Size(**페이로드 크기**)** 및 **Timeout(**시간 초과**)** 파라미터를 사용하여 지정된 SA에서 무작위 간격으로 임의 길이의 패킷을 생성할 수 있습니다.

FTD 고급 Site-to-site VPN 구축 옵션

다음 섹션에서는 구축에서 지정할 수 있는 고급 옵션에 대해 설명합니다. 이 설정은 전체 토폴로지, 모든 터널 및 모든 매니지드 디바이스에 적용됩니다.

FTD VPN 고급 IKE 옵션

Advanced(고급**) > IKE > ISAKAMP** 설정

IKE Keepalive

IKE Keepalive를 활성화 또는 비활성화합니다. 또는 EnableInfinite로 설정하여 디바이스가 자체적으로 Keepalive 모니터링을 시작하지 않도록 지정합니다.

임계값
IKE keep alive 신뢰 구간을 지정합니다. 이것은 keep alive 모니터링을 시작하기 전에 피어가 유휴 상태에 있도록 허용하는 시간(초)입니다. 기본값 및 최소값은 10초이고, 최대값은 3600초입니다.

다시 시도 간격
IKE keep alive 재시도 간에 대기할 시간(초)을 지정합니다. 기본값은 2초, 최대값은 10초입니다.

Identity Sent to Peer(피어로 전송되는 **ID)**
IKE 협상 중에 피어가 자신을 식별하는 데 사용할 Identity(ID)를 선택합니다.

- autoOrDN(기본값) — 연결 유형에 따라 IKE 협상을 결정합니다. 예: 사전 공유 키의 IP 주소 또는 인증서 인증의 Cert DN(지원하지 않음)

- ipAddress—ISAKMP ID 정보를 교환하는 호스트의 IP 주소를 사용합니다.
- hostname—ISAKMP ID 정보를 교환하는 호스트의 정규화된 도메인 이름을 사용합니다. 이 이름은 호스트 이름 및 도메인 이름으로 구성됩니다.

적극적인 모드 활성화
: 허브 앤 스포크 VPN 토폴로지에만 사용할 수 있습니다. IP 주소를 알 수 없고 DNS 확인을 디바이스에서 사용할 수 없는 경우, 키 정보 교환을 위해 이 협상 방법을 선택합니다. 협상은 호스트 이름 및 도메인 이름을 기반으로 합니다.

Advanced(고급) > IKE > IVEv2 Security Association (SA) Settings (IVEv2 보안 연결(SA) 설정)

IKE v2에서는 열려 있는 SA 수를 제한하는 세션 제어를 추가로 사용할 수 있습니다. 기본적으로 열려 있는 SA 수에는 제한이 없습니다.

쿠키 챌린지
: SA에 대한 응답으로 쿠키 챌린지를 피어 디바이스로 전송할지 여부에 따라 Dos(서비스 거부)공격을 차단할 수 있는 패킷이 시작됩니다. 기본적으로 사용 가능한 SA의 50%가 협상중인 경우 쿠키 챌린지를 사용합니다. 다음 옵션 중 하나를 선택합니다.

- 사용자 지정:
- Never(기본값)
- Always

수신 쿠키 챌린지 임계값
: 총 협상 허용 SA의 비율 이렇게 하면 이후의 모든 SA 협상에 대해 쿠키 챌린지가 트리거됩니다. 범위는 0~100%이고,

협상이 허용된 **SA** 수
: 언제든지 협상에 참여할 수 있는 최대 SA 수를 제한합니다. Cookie Challenge(쿠키 챌린지)와 함께 사용하는 경우 효과적인 교차 확인을 위해 쿠키 챌린지 임계값을 이 한도보다 낮은 값으로 구성합니다.

허용된 최대 **SA** 수
: 허용되는 IKEv2 연결 수를 제한합니다. 기본값은 무제한입니다.

Enable Notification on Tunnel Disconnect(터널 연결 해제 알림 활성화)
: SA에서 수신한 인바운드 패킷이 해당 SA의 트래픽 선택기와 일치하지 않는 경우, 관리자가IKE 알림 피어 전송을 활성화 또는 비활성화할 수 있습니다. 이 알림의 전송은 기본적으로 비활성화되어 있습니다.

FTD VPN 고급 IPsec 옵션

Advanced(고급) > IPsec > IPsec Settings(IPsec 설정)

Enable Fragmentation Before Encryption(암호화 이전 단편화 활성화)
: 이 옵션을 사용하면 트래픽이 IP 단편화를 지원하지 않는 NAT 디바이스를 통과할 수 있습니다. IP 단편화를 지원하는 NAT 디바이스의 작동을 방해하지 않습니다.

Path Maximum Transmission Unit Aging(경로 최대 전송 단위 에이징**)**
SA(Security Association)의 PMTU(Path Maximum Transmission Unit) 재설정 간격인 PMTU Aging 활성화를 선택합니다.

Value Reset Interval(값 재설정 간격**)**
SA(Security Association)의 PMTU 값이 원래 값으로 재설정되는 시간(분)을 입력합니다. 유효 범위는 10~30분이며, 기본값은 무제한입니다.

FTD 고급 Site-to-site VPN 터널 옵션

탐색 경로

Devices(디바이스**) > VPN > Site To Site(**사이트 대 사이트**)**, 그런 다음 **Add VPN(VPN** 추가**) > Firepower Threat Defense Device** 또는 나열된 VPN Topology를 수정합니다. **Advanced(**고급**)** 탭을 열고 탐색창에서 **Tunnel(**터널**)**을 선택합니다.

터널 옵션

허브 앤 스포크, 풀 메시 토폴로지만 사용할 수 있습니다. 이 섹션은 Point-to-Point 구성에 대해서는 표시되지 않습니다.

- **Enable Spoke to Spoke Connectivity through Hub(**허브를 통한 스포크 투 스포크 연결 활성화**)** - 기본적으로 비활성화되어 있습니다. 이 필드를 선택하면 스포크 양쪽 끝에 있는 디바이스가 허브 노드를 통해 다른 디바이스로 연결을 확장할 수 있습니다.

NAT 설정

- **Keepalive Messages Traversal(Keepalive** 메시지 순회**)** - NAT keepalive 메시지 순회 활성화 여부를 선택합니다. NAT 순회 keepalive는 VPN 연결 허브 및 스포크 사이에 위치한 디바이스(중간 디바이스)가 있는 경우 keepalive 메시지 전송에 사용되며, 해당 디바이스는 IPsec flow에서 NAT를 수행합니다.

  이 옵션을 선택하는 경우, 스포크와 중간 디바이스 간에 전송된 keepalive 신호 간격을 초 단위로 구성하고 해당 세션이 활성임을 표시합니다. 이 값의 범위는 5~3600초입니다. 기본값은 20초입니다.

인증서 맵 설정

- **Use the certificate map configured in the Endpoints to determine the tunnel(**엔드포인트에서 구성된 인증서 맵을 사용하여 터널 결정**)** - 이 옵션을 활성화(선택)하면 수신한 인증서의 내용을 엔드포인트 노드에 구성된 인증서 맵 개체와 연결하여 터널을 결정합니다.
- **Use the certificate OU field to determine the tunnel(**인증서 **OU** 필드를 사용하여 터널 결정**)** - 구성된 매핑(위의 옵션)을 기반으로 노드가 결정되지 않으면 수신된 인증서의 주체 DN(고유 이름)에 OU(조직 구성 단위) 값을 사용하여 터널을 결정합니다.
- **Use the IKE identity to determine the tunnel(IKE ID**를 사용하여 터널 결정**)** - 노드가 OU와 일치하는 규칙 또는 OU에서 가져온 옵션(위의 옵션)을 기반으로 결정되지 않으면 인증서 기반 IKE 세션이 phase1 IKE ID의 내용을 기반으로 터널에 매핑됩니다.

- **Use the peer IP address to determine the tunnel(**피어 **IP** 주소를 사용하여 터널 결정**)** - 터널이 OU 또는 IKE ID 방법과 일치하는 규칙이나 OU 또는 IKE ID 방법에서 가져온 옵션(위의 옵션)을 기반으로 결정되지 않으면 설정된 피어 IP 주소를 사용합니다.

Sysopt Connection Permit-vpn 옵션 활성화

암호 해독된 트래픽 검사를 생략하려면 다음 단계에 따라 *sysopt connection permit-vpn* 옵션을 활성화합니다. 하지만 AAA 서버에서 다운로드한 VPN 필터 ACL 및 인증 ACL이 여전히 VPN 트래픽에 적용됩니다.

프로시저

단계 **1** FMC 웹 인터페이스의 경우 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **Text Object(**텍스트 개체**)** > **Add Text Object(**텍스트 개체 추가**)**를 선택합니다.

단계 **2** **sysopt** 값이 있는 단일 항목인 텍스트 개체 변수(예: **vpnSysVar**)를 생성합니다.

단계 **3** **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)** > **Add FlexConfig Object(FlexConfig** 개체 추가**)**로 이동합니다.

단계 **4** **connection permit-vpn** 명령으로 FlexConfig 개체를 생성합니다.

단계 **5** 명령의 시작 부분에 FlexConfig 개체의 텍스트 개체 변수(예: **$vpnSysVar connection permit-vpn**)를 삽입하고 **Save(**저장**)**를 클릭합니다.

단계 **6** FlexConfig 개체 유형으로 **Append(**추가**)**를 적용하고 Deployment(구축)를 **Everytime(**항상**)**으로 선택합니다.

단계 **7** **Devices(**디바이스**)** > **FlexConfig**로 이동하여 및 기존 정책을 수정하거나 새로 생성합니다.

단계 **8** 새로 생성된 FlexConfig 개체를 추가하고 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

Virtual Tunnel Interface 정보

Firepower Management Center는 VTI(Virtual Tunnel Interface)라는 논리적 인터페이스를 지원합니다. 정책 기반 VPN 대신, 구성된 Virtual Tunnel Interface와 피어 간에 VPN 터널을 생성할 수 있습니다. 이는 각 터널 끝에 IPsec 프로파일이 연결된 라우팅 기반 VPN을 지원합니다. 그러면 동적 또는 정적 경로를 사용할 수 있습니다. VTI에서 이그레스(Egress)되는 트래픽은 암호화되어 피어로 전송되고, 연결된 SA가 VTI로 인그레스(Ingress)되는 트래픽의 암호를 해독합니다.

VTI를 사용하면 정적 암호화 맵 액세스 목록을 구성하고 이를 인터페이스에 매핑하기 위한 요구 사항이 없어집니다. 더 이상 모든 원격 서브넷을 추적하고 암호화 맵 액세스 목록에 포함하지 않아도 됩니다. 구축이 더 간편해지고, 동적 라우팅 프로토콜과 라우팅 기반 VPN을 지원하는 정적 VTI가 있

어 가상 프라이빗 클라우드의 많은 요구 사항도 충족합니다. FMC를 사용하면 암호화 맵 기반 VPN 설정에서 VTI 기반 VPN으로 쉽게 마이그레이션할 수 있습니다.

정적 가상 터널 인터페이스를 설정하여 FMC, FTD 디바이스 REST API 및 FDM에서 경로 기반 VPN을 설정할 수 있습니다. FMC는 VTI 또는 경로 기반 VPN을 설정하는 데 기본값을 사용하는 사이트 간 VPN 마법사를 지원합니다. 트래픽은 정적 경로 또는 BGP를 사용하여 암호화됩니다.

라우팅된 보안 영역을 생성하고 여기에 VTI 인터페이스를 추가하며 VTI 터널을 통해 해독된 트래픽 제어를 위한 액세스 제어 규칙을 정의할 수 있습니다.

VTI 기반 VPN은 다음 간에 생성할 수 있습니다.

- 두 대의 FTD 디바이스
- FTD 및 퍼블릭 클라우드
- FTD 및 서비스 제공자 리던던시가 있는 또 다른 FTD
- FTD 및 VTI 인터페이스가 설정된 기타 디바이스

Virtual Tunnel Interface에 대한 지침 및 제한 사항

IPv6 지원

- IPv6은 지원되지 않습니다.

제한 사항

- 20개의 고유한 IPSec 프로파일만 지원됩니다.
- 물리적 인터페이스당 100개의 VTI만 지원됩니다.
- 동적 VTI, OSPF 및 QoS는 지원되지 않습니다.
- VTI로 생성된 사이트 간 VPN 터널은 터널이 다운될 때 상태 알림을 생성하지 않습니다. VTI를 사용하는 VPN에서 패킷 손실이 발생하는 경우, VPN 설정을 확인하십시오.

일반 구성 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다.
- VTI는 IKE 버전 v1, v2를 지원하고 IPsec을 사용하여 터널의 소스와 대상 간에 데이터를 전송 및 수신합니다.
- 네트워크 주소 변환을 적용해야 할 경우, IKE 및 ESP 패킷이 UDP 헤더에서 캡슐화됩니다.

- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- 터널 그룹 이름은 피어가 IKEv1 또는 IKEv2 id로 전송하는 항목과 일치해야 합니다.
- LAN-to-LAN 터널 그룹에서 IKEv1의 경우, 터널 인증 방법이 디지털 인증서 및/또는 적극적인 모드를 사용하도록 구성된 피어인 경우, IP 주소가 아닌 이름을 사용할 수 있습니다.
- VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있으며 암호화 맵에 구성된 피어 주소를 제공하며 VTI에 대한 터널 대상은 서로 다릅니다.
- 기본적으로 VTI를 통해 전송되는 모든 트래픽이 암호화됩니다.
- VTI 인터페이스에 대한 보안 레벨 구성이 없습니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.

다중 인스턴스

VTI는 단일 인스턴스에서만 지원됩니다.

방화벽 모드

VTI는 라우팅 모드에서만 지원됩니다.

VTI 인터페이스 추가

경로 기반 사이트 간 VPN을 설정하려면 VTI 터널의 두 노드에 있는 디바이스에서 가상 터널 인터페이스를 생성해야 합니다. 새 VTI 인터페이스를 생성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** VTI 인터페이스를 생성하려는 디바이스 옆의 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Add Interfaces(**인터페이스 추가**)** 드롭다운 메뉴에서 **Virtual Tunnel Interface(**가상 터널 인터페이스**)**를 선택합니다.

단계 **4** **Name(**이름**)** 필드에 새 VTI의 이름을 입력합니다.

단계 **5** 인터페이스를 생성한 후 활성화하려면 **Enabled(**활성화됨**)** 확인란을 선택한 상태(기본값)로 유지합니다.

단계 **6** (선택 사항) 새 VTI의 설명을 입력합니다.

단계 **7** (선택 사항) **Security Zone(**보안 영역**)** 드롭다운 메뉴에서 해당 영역에 VTI 인터페이스를 추가할 보안 영역을 선택합니다. 보안 영역을 기준으로 트래픽 검사를 수행하려는 경우, 보안 영역에 VTI를 추가하고 액세스 제어 규칙을 설정할 수 있습니다. 터널을 통한 VPN 트래픽을 허용하려면 이 보안 영역이 있는 AC 규칙을 소스 영역으로 추가해야 합니다.

단계 **8** **Tunnel ID(**터널 **ID)** 필드에 0~10413 범위의 고유한 터널 ID를 입력합니다.

단계 9 **IP Address(IP 주소)** 필드에 터널 엔트포인트에 사용할 IP 주소와 서브넷을 입력합니다. 경로 기반 VPN의 두 엔드포인트 모두에 대한 VTI IP 주소는 동일한 서브넷에 있어야 합니다.

참고 Cisco는 FTD 예약 범위(169.254.1.x/24)를 제외하고 169.254.x.x/16 범위의 IP를 사용하기를 권장합니다. 또한 VTI 터널의 양 끝에 두 개의 주소만 최적으로 사용하려면 /30을 넷마스크로 사용하는 것이 좋습니다. 예: 169.254.100.1/30

단계 10 **Tunnel Source(터널 소스)** 드롭다운 메뉴에서 터널 소스 인터페이스를 선택합니다.

단계 11 **OK(확인)**를 클릭합니다.

라우트 기반 사이트 대 사이트 VPN 생성

두 노드간에 라우트 기반 사이트 대 사이트 VPN을 구성할 수 있습니다. VTI 기반 VPN을 구성하려면 터널의 두 노드에서 모두 가상 터널 인터페이스가 필요합니다.

VTI에 대한 자세한 내용은 Virtual Tunnel Interface 정보, 1146 페이지의 내용을 참조하십시오.

프로시저

단계 1 **Devices(디바이스) > Site To Site(사이트 대 사이트)**를 선택합니다.

단계 2 **Add VPN(VPN 추가)** 드롭다운 메뉴에서 **Firepower Threat Defense Device(Firepower Threat Defense 디바이스)**를 선택합니다.

단계 3 Topology Name(토폴로지 이름) 필드에 생성 중인 VPN 토폴로지의 이름을 입력합니다.

단계 4 토폴로지 유형으로 VTI(Route Based)를 선택합니다. 네트워크 토폴로지는 포인트 투 포인트로 선택되며 IKE 프로토콜 버전은 사이트 대 사이트 구성에 기본적으로 IKEv2로 선택됩니다.

단계 5 **Endpoints(엔드포인트)** 탭의 노드 **A** 아래에 있는 **Device(디바이스)** 드롭다운 메뉴에서 VTI 터널의 첫 번째 엔드포인트로 사용할 등록된 디바이스(FTD) 또는 엑스트라넷의 이름을 선택합니다.

단계 6 등록된 디바이스의 경우 노드 A에 대한 인터페이스를 지정할 수 있습니다.

- **Virtual Tunnel Interface(가상 터널 인터페이스)** 드롭다운 메뉴에서 노드 A로 선택한 FTD 디바이스에서 생성한 VTI 인터페이스를 선택합니다.
- 노드 A에서 새 인터페이스를 생성하려면 + 아이콘을 클릭하고 VTI 인터페이스 추가, 1148 페이지에 설명된 대로 필드를 채웁니다.
- 기존 VTI의 구성을 편집하려면 **Virtual Tunnel Interface(가상 터널 인터페이스)** 드롭다운 필드에서 VTI를 선택하고 **Edit VTI(VTI 편집)**를 클릭합니다.

  참고 선택한 터널 인터페이스는 노드 A의 소스 인터페이스이며 노드 B의 터널 대상이 됩니다.

단계 **7** 노드 A 디바이스가 NAT 디바이스 뒤에 있는 경우 **Tunnel Source IP is Private(**터널 소스 **IP**는 전용**)** 확인란을 선택합니다. **Tunnel Source Public IP Address(**터널 소스 공용 **IP** 주소**)** 필드에 터널 소스 공용 IP 주소를 입력합니다.

단계 **8** **Connection Type(**연결 유형**)** 드롭다운 메뉴에서 **Answer Only(**응답 전용**)** 또는 **Birectional(**양방향**)**을 선택합니다. IKE 프로토콜 버전을 IKEv1로 선택한 경우 노드 중 하나가 **Answer Only(**응답 전용**)**이어야 합니다.

단계 **9** **Additional Configuration(**추가 구성**)**에서 다음을 수행합니다.

- VTI로 트래픽을 라우팅하려면 **Routing Policy(**라우팅 정책**)**를 클릭합니다. FMC는 **Devices(**디바이스**)** > **Routing(**라우팅**)** 페이지를 표시합니다. VPN 트래픽에 대해 고정 또는 BGP 라우팅을 구성할 수 있습니다.
- VPN 트래픽을 허용하려면 **AC Policy(AC** 정책**)**를 클릭합니다. FMC는 디바이스의 액세스 제어 정책 페이지를 표시합니다. 계속해서 VTI의 보안 영역을 지정하는 허용/차단 규칙을 추가합니다. 백업 VTI가 구성된 경우 기본 VTI와 동일한 보안 영역에 백업 터널을 포함해야 합니다. AC 정책 페이지에는 백업 VTI에 대한 특정 설정이 필요하지 않습니다.

단계 **10** 엑스트라넷 피어의 경우 다음 매개변수를 지정합니다.

a) **Device Name(**디바이스 이름**)**에 디바이스 이름을 입력합니다.
b) **Endpoint IP address(**엔드포인트 **IP** 주소**)**에 기본 IP 주소를 입력합니다.
c) **IKE** 탭을 클릭하고 엑스트라넷에 제공된 사전 공유 키를 지정합니다.

참고 AWS VPC에는 기본 정책으로 **AES-SHA-SHA-LATEST**가 있습니다. 따라서 원격 피어가 AWS VPC에 연결되면 **Policy(**정책**)** 드롭다운 목록에서 **AES-SHA-SHA-LATEST**를 선택하여 AWS에서 기본값을 변경할 필요 없이 VPN 연결을 설정합니다.

단계 **11** 노드 B에 대해 위의 절차를 반복합니다.

VTI에 대한 추가 구성

두 디바이스에서 VTI 인터페이스 및 VTI 터널을 구성한 후에는 VTI 터널을 통해 디바이스간에 VTI 트래픽을 라우팅하도록 라우팅 정책을 구성해야 합니다. 암호화된 트래픽을 허용하도록 액세스 제어 규칙을 구성해야 합니다.

VTI를 위한 라우팅 구성

고정 경로

VTI 터널을 통해 디바이스 간의 트래픽 흐름을 라우팅하도록 두 디바이스(두 종단 모두)에서 고정 라우팅을 구성합니다.

VPN에 대해 백업 터널이 구성된 경우 백업 터널을 통한 트래픽 흐름의 페일오버를 처리할 수 있도록 다른 메트릭으로 고정 경로를 구성합니다.

고정 경로를 구성할 때 다음을 구성해야 합니다.

- **Interface(**인터페이스**)**-VPN에서 사용되는 VTI 인터페이스를 선택합니다.
- **Selected Network(**선택한 네트워크**)**-원격 피어의 보호된 네트워크(네트워크 개체로 추가됨)를 선택합니다.
-

고정 라우팅에 대한 자세한 내용은 고정 경로 추가, 1038 페이지을 참조하십시오.

BGP(Border Gateway Protocol)

다음 설정을 사용하여 라우팅 정보를 공유하고 터널을 통해 디바이스간에 트래픽 흐름을 라우팅하도록 두 디바이스 모두에서 BGP를 구성합니다.

- **General Settings(**일반 설정**)**> **BGP**에서 BGP를 활성화하고 로컬 디바이스의 AS 번호를 제공하고 라우터 ID를 추가합니다(수동을 선택한 경우).
- **BGP** 아래의 IPv4를 활성화하고 Neighbor(인접 항목) 탭에서 인접 항목을 구성합니다.
  - **IP Address(IP** 주소**)**-원격 피어의 VTI 인터페이스 IP 주소를 인접 항목의 IP 주소로 지정합니다.
  - **Remote AS(**원격 **AS)**-원격 피어의 AS 번호를 지정합니다.

BGP 구성에 대한 자세한 내용은 BGP 구성, 1077 페이지를 확인하십시오.

AC 정책 규칙

디바이스의 액세스 제어 정책에 액세스 제어 규칙을 추가하여 다음 설정으로 VTI 터널 간 암호화된 트래픽을 허용합니다.

- Allow(허용) 작업으로 규칙을 생성합니다.
- 로컬 디바이스의 VTI 보안 영역을 소스 영역으로 선택하고 원격 피어의 VTI 보안 영역을 대상 영역으로 선택합니다.
- 원격 피어의 VTI 보안 영역을 소스 영역으로 선택하고 로컬 디바이스의 VTI 보안 영역을 대상 영역으로 선택합니다.

액세스 제어 규칙 구성에 대한 자세한 내용은 액세스 제어 규칙 생성 및 수정, 1651 페이지을 참고하십시오.

참고 백업 VTI가 구성된 경우 기본 VTI와 동일한 보안 영역에 백업 터널을 포함해야 합니다. AC 정책 페이지에는 백업 VTI에 대한 특정 설정이 필요하지 않습니다.

사이트 간 VPN 기록

기능	버전	세부 사항
약한 암호 제거 및 사용 중단	6.7	

기능	버전	세부 사항
		보안 수준이 낮은 암호에 대한 지원이 제거되었습니다. VPN이 올바르게 작동하도록 FTD 6.70을 지원되는 DH 및 암호화 알고리즘으로 업그레이드하기 전에 VPN 설정을 업데이트하는 것이 좋습니다. FTD 6.70에서 지원되는 것과 일치하도록 IKE 제안 및 IPSec 정책을 업데이트한 다음 설정 변경 사항을 구축합니다. 다음과 같이 안전성이 상대적으로 낮은 암호는 FTD 6.70 이상에서 제거되었거나 더 이상 사용되지 않습니다. • **Diffie-Hellman GROUP 5**는 IKEv1에서 더 이상 사용되지 않으며 IKEv2에서 제거됩니다. • Diffie-Hellman GROUP 2 및 24가 제거되었습니다. • 암호화 알고리즘: 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256이 제거되었습니다. 참고 **DES**는 평가 모드에서 또는 강력한 암호화를 위한 내보내기 제어 항목을 충족하지 않는 사용자를 대상으로 계속 지원됩니다. **NULL**은 IKEv2 정책에서 제거되지만, IKEv1 및 IKEv2 IPsec 변형 집합에서 모두 지원됩니다.

기능	버전	세부 사항
동적 RRI 지원	6.7	동적 Reverse Route Injection은 IKEv2 기반 정적 암호화 맵에서 지원됩니다.
사이트 간 VPN을 위한 백업 피어	6.6	FMC를 사용하여 사이트 간 VPN 연결에 백업 피어를 추가할 수 있습니다. 예를 들어 ISP가 2개 있을 경우, 첫 번째 ISP에 대한 연결을 사용할 수 없게 되면 VPN 연결을 백업 ISP로 페일오버하도록 구성할 수 있습니다.

45 장

Remote Access VPN Firepower Threat Defense

- Firepower Threat Defense 원격 액세스 VPN 개요, 1155 페이지
- 원격 액세스 VPN 라이선스 요구 사항, 1162 페이지
- 원격 액세스 VPN 요구 사항 및 사전 요건, 1162 페이지
- Remote Access VPN에 대한 지침 및 제한 사항, 1162 페이지
- 새 Remote Access VPN 연결 구성, 1165 페이지
- 원격 액세스 VPN 정책 대상 디바이스 설정, 1173 페이지
- 선택적 Remote Access VPN 구성, 1173 페이지
- RADIUS 동적 권한 부여, 1198 페이지
- 이중 인증, 1199 페이지
- 보조 인증, 1203 페이지
- SAML 2.0을 사용한 SSO(Single Sign-On) 인증, 1206 페이지
- Remote Access VPN AAA 사용자 지정, 1208 페이지
- 권한 부여 서버에 그룹 정책 선택 위임, 1214 페이지
- Remote Access VPN 예시, 1219 페이지
- AnyConnect 관리 VPN 터널 구성, 1225 페이지
- 원격 액세스 VPN 히스토리, 1228 페이지

Firepower Threat Defense 원격 액세스 VPN 개요

Firepower Threat Defense 는 원격 액세스 SSL 및 IPsec IKEv2 VPN을 지원하는 보안 게이트웨이 기능을 제공합니다. 전체 터널 클라이언트인 AnyConnect Secure Mobility Client는 원격 사용자를 위해 보안 게이트웨이에 보안 SSL 및 IPsec-IKEv2 연결을 제공합니다. AnyConnect는 Firepower Threat Defense 디바이스에 원격 VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다. 이 클라이언트는 네트워크 관리자가 원격 컴퓨터에 클라이언트를 설치 및 구성하지 않아도 원격 사용자에게 SSL 또는 IPsec-IKEv2 VPN 클라이언트의 이점을 제공합니다. Windows, Mac, Linux 용 AnyConnect 모바일 클라이언트는 연결할 때 보안 게이트웨이에서 구축됩니다. Apple iOS 및 Android 디바이스용 AnyConnect 앱은 플랫폼 앱 스토어에서 설치됩니다.

Firepower Management Center의 Remote Access VPN 정책 마법사를 사용하여 기본 기능을 갖춘 SSL 및 IPsec-IKEv2 원격 액세스 VPN을 쉽고 빠르게 설정합니다. 그런 다음, 원하는 경우 정책 구성을 개선하고 Firepower Threat Defense 보안 게이트웨이 디바이스에 구축합니다.

원격 액세스 VPN 정책을 사용하여 다음 설정을 구성할 수 있습니다.

- 이중 인증, 1199 페이지
- 보조 인증, 1203 페이지
- 인증을 위한 LDAP 또는 Active Directory 설정, 1212 페이지
- VPN 세션에 대한 암호 변경 관리, 1211 페이지
- RADIUS 서버로 계정 기록 전송, 1213 페이지
- 그룹 정책 또는 기타 속성 선택을 권한 부여 서버로 재정의 , 1215 페이지
  - 사용자 그룹에 대한 VPN 액세스 거부, 1216 페이지
  - 사용자 그룹에 대한 연결 프로파일 선택 제한, 1217 페이지

다음 예시를 사용하여 제한된 대역폭을 VPN 사용자에게 할당하고, 사용자 ID 기반 액세스 제어 규칙에 VPN 식별을 사용할 수 있습니다.

- 사용자별 AnyConnect 대역폭을 제한하는 방법, 1219 페이지
- 사용자 ID 기반 액세스 제어 규칙에 VPN ID를 사용하는 방법, 1222 페이지

Remote Access VPN 기능

다음 섹션에서는 Firepower Threat Defense Remote Access VPN의 기능에 대해 설명합니다.

- Cisco AnyConnect Secure Mobility 클라이언트를 사용하는 SSL 및 IPsec-IKEv2 원격 액세스.
- Firepower Management Center IPv4 터널을 통한 IPv6와 같은 모든 조합을 지원합니다.
- FMC 및 FDM 모두에 대한 구성 지원. 디바이스별 재정의.
- Firepower Management Center 및 FTD HA 환경에 대한 지원.
- 여러 인터페이스 및 여러 AAA 서버에 대한 지원.
- RADIUS CoA 또는 RADIUS 동적 인증을 사용하여 Rapid Threat Containment 지원.
- Cisco AnyConnect Secure Mobility Client 버전 4.7 이상에서 DTLS v1.2 프로토콜을 지원합니다.
- AnyConnect 클라이언트 모듈은 RA VPN 연결을 위한 추가 보안 서비스를 지원합니다.

AAA

- 자체 서명 또는 CA 서명 ID 인증서를 사용하는 서버 인증.
- RADIUS 서버 또는 LDAP 또는 AD를 사용하는 AAA 사용자 이름 및 암호 기반 원격 인증.
- RADIUS 그룹 및 사용자 권한 부여 속성 및 RADIUS 계정.
- 2차 인증을 위해 추가 AAA 서버를 사용하는 이중 인증 지원.

- VPN ID를 사용하는NGFW Access Control 통합.
- Firepower Management Center 웹 인터페이스를 사용하는 LDAP 또는 AD 권한 부여 속성
- SAML 2.0을 사용하는 SSO(Single Sign-On) 지원

VPN 터널링

- 주소 할당
- 스플릿 터널링
- 스플릿 DNS
- Client Firewall ACL
- 최대 연결 및 유휴 시간에 대한 세션 시간 초과

모니터링

- 기간 및 클라이언트 애플리케이션 같은 다양한 속성으로 VPN 사용자를 표시하는 새로운 VPN 대시보드 위젯.
- 사용자 이름 및 OS 플랫폼과 같은 인증 정보를 포함하는 원격 액세스 VPN 이벤트.
- FTD Unified CLI를 통해 사용 가능한 터널 통계.

AnyConnect 구성 요소

AnyConnect Secure Mobility Client 구축

원격 액세스 VPN 정책에 AnyConnect 클라이언트 이미지 및 AnyConnect 클라이언트 프로파일을(를) 포함하여 연결 엔드포인트에 배포할 수 있습니다. 또는 다른 방법을 사용하여 클라이언트 소프트웨어를 배포할 수 있습니다. 알맞은 버전의 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 *AnyConnect* 구축 장을 참조하십시오.

이전에 설치된 클라이언트가 없는 경우 원격 사용자는 SSL 또는 IPsec-IKEv2 VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력합니다. 보안 어플라이언스가 http:// 요청을 https://로 리디렉션하도록 구성되어 있지 않은 경우, 사용자는 URL을 https://<*address*> 형식으로 입력해야 합니다. 사용자가 URL을 입력하면 브라우저가 해당 인터페이스로 연결되고 로그인 화면이 표시됩니다.

사용자가 로그인하면, 보안 게이트웨이에서 사용자가 VPN 클라이언트를 요청하는 것으로 식별하면 원격 컴퓨터의 운영 체제에 맞는 클라이언트가 다운로드됩니다. 다운로드 후에는 클라이언트가 자동으로 설치 및 구성되어 보안 연결을 설정하며, 연결이 중지되면 보안 어플라이언스 구성에 따라 그대로 유지되거나 자동으로 제거됩니다. 이전에 설치된 클라이언트의 경우, 로그인하면 Firepower Threat Defense 보안 게이트웨이가 클라이언트 버전을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.

AnyConnect Secure Mobility Client 작업

클라이언트가 보안 어플라이언스와 연결을 협상한다면, 클라이언트는 TLS(Transport Layer Security)를 사용하여 연결하고 선택에 따라 DTLS(Datagram Transport Layer Security)를 사용하여 연결합니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다.

IPsec-IKEv2 VPN 클라이언트가 보안 게이트웨이에 연결을 시작할 경우, 협상은 IKE(Internet Key Exchange)를 통한 디바이스 인증과 그다음에 수행되는 IKE Xauth(Extended Authentication)를 사용한 사용자 인증으로 구성됩니다. 그룹 프로파일이 VPN 클라이언트에 푸시되고 IPsec SA(security association)를 생성하여 VPN을 완료합니다.

AnyConnect 클라이언트 프로파일 및 편집기

AnyConnect 클라이언트 프로파일은 XML 파일에 저장된 구성 파라미터 그룹으로, VPN 클라이언트는 이를 사용하여 운영 및 모양을 구성합니다. 이러한 매개변수(XML 태그)에는 추가적인 클라이언트 기능을 활성화할 수 있는 호스트 컴퓨터 및 설정의 이름과 주소가 포함되어 있습니다.

AnyConnect 프로파일 편집기를 사용하여 프로파일을 구성할 수 있습니다. 이 편집기는 AnyConnect 소프트웨어 패키지의 일부로 제공되는 편리한 GUI 기반 구성 툴입니다. 이 툴은 Firepower Management Center외부에서 실행되는 독립 프로그램입니다.

Remote Access VPN 인증

Remote Access VPN 서버 인증

Firepower Threat Defense 보안 게이트웨이는 항상 인증서를 사용하여 VPN 클라이언트 엔드포인트에 대한 식별 및 인증을 수행합니다.

보안 게이트웨이의 인증서를 가져오는 것은 PKI 등록이라고도 하며, Firepower Threat Defense 인증서 기반 인증, 675 페이지에 설명되어 있습니다. 이 장에는 게이트웨이 인증서 구성, 등록 및 유지 관리에 대한 전체적인 설명이 포함되어 있습니다.

Remote Access VPN 클라이언트 AAA

SSL 및 IPsec-IKEv2 둘 다의 경우 원격 사용자 인증은 사용자 이름과 비밀번호만, 인증서만 또는 두 가지를 모두 사용하여 수행됩니다.

참고 구축에서 클라이언트 인증서를 사용하고 있는 경우, Firepower Threat Defense 또는 Firepower Management Center와 무관한 클라이언트 플랫폼에 해당 인증서를 추가해야 합니다. 클라이언트에 인증서를 입력할 수 있는 기능인 SCEP 또는 CA 서비스 등은 제공되지 않습니다.

AAA 서버는 보안 게이트웨이 역할의 매니지드 디바이스가 사용자(인증), 사용자가 수행하도록 허용된 작업(권한 부여) 및 사용자가 수행한 작업(계정)을 결정하도록 활성화합니다. AAA 서버의 몇 가지 예는 RADIUS, LDAP/AD, TACACS+ 및 Kerberos입니다. Firepower Threat Defense 디바이스에서 Remote Access VPN의 경우 인증에 대해 AD, LDAP 및 RADIUS AAA 서버가 지원됩니다.

Remote Access VPN 권한 부여에 대한 자세한 내용은 권한 및 속성 정책 시행 이해을 참조하십시오.

Remote Access VPN 정책을 추가하거나 편집하기 전에 지정하려는 영역 및 RADIUS 서버 그룹을 구성해야 합니다. 자세한 내용은 영역 생성, 2466 페이지 및 RADIUS 서버 그룹, 667 페이지를 참조하십시오.

구성된 DNS가 없으면 디바이스는 AAA 서버 이름, 이름이 지정된 URL 및 FQDN 또는 호스트 이름이 있는 CA 서버를 확인할 수 없으며 IP 주소만 확인할 수 있습니다.

플랫폼 설정을 사용하여 DNS를 구성할 수 있습니다. 자세한 내용은 DNS 구성, 1425 페이지 및 DNS 서버 그룹 개체, 637 페이지를 참조하십시오.

원격 사용자가 제공한 로그인 정보는 LDAP 또는 AD 영역 또는 RADIUS 서버 그룹에서 검증합니다. 이러한 엔터티는 Firepower Threat Defense 보안 게이트웨이와 통합됩니다.

참고 사용자가 Active Directory를 인증 소스로 사용하여 RA VPN으로 인증하는 경우 사용자 이름을 사용하여 로그인해야 합니다. `domain\username` 또는 `username@domain` 형식은 실패하게 됩니다. (Active Directory는 이 사용자 이름을 로그온 이름 또는 경우에 따라 `sAMAccountName`으로 참조합니다.) 자세한 내용은 MSDN의 User Naming Attributes를 참조하십시오.

RADIUS를 사용하여 인증하는 경우 사용자는 위의 형식 중 하나로 로그인할 수 있습니다.

VPN 연결을 통해 인증되면 원격 사용자는 *VPN ID*를 사용합니다. Firepower Threat Defense 보안 게이트웨이의 *ID* 정책에서 이 VPN ID를 사용하여 해당 원격 사용자에게 속하는 네트워크 트래픽을 인식하고 필터링합니다.

ID 정책은 네트워크 리소스에 대한 액세스 권한을 가진 사용자를 확인하는 액세스 제어 정책과 연결됩니다. 이러한 방식으로 원격 사용자는 네트워크 리소스에 대한 액세스가 차단되거나 허용됩니다.

자세한 내용은 영역 및 ID 정책 및 액세스 제어 정책, 1625 페이지 섹션을 참조하십시오.

관련 항목

Remote Access VPN에 대한 AAA 설정, 1177 페이지

권한 및 속성 정책 시행 이해

Firepower Threat Defense 디바이스는 AAA 서버(RADIUS) 또는 Firepower Threat Defense 디바이스에 정의된 그룹 정책에서 VPN 연결에 사용자 인증 속성(사용자 자격 또는 권한이라고도 함)을 적용하도록 지원합니다. Firepower Threat Defense 디바이스에서 그룹 정책에 구성된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

Firepower Threat Defense 디바이스에서는 다음 순서로 속성을 적용합니다.

1. **AAA** 서버의 사용자 속성 - 사용자 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이러한 특성을 반환합니다.
2. **Firepower Threat Defense** 디바이스에 구성된 그룹 정책 - RADIUS 서버에서 사용자에 대해 RADIUS CLASS 속성 IETF-Class-25(OU=group-policy) 값을 반환하면 Firepower Threat Defense 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.

3. 연결 프로파일에서 할당한 그룹 정책(터널 그룹으로 알려짐) - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다.

참고 Firepower Threat Defense 디바이스는 기본 그룹 정책인 *DfltGrpPolicy*에서 시스템 기본 속성 상속을 지원하지 않습니다. 연결 프로파일에 할당된 그룹 정책의 속성은 사용자 속성이나 AAA 서버의 그룹 정책에 의해 재정의되지 않는 경우 위에서 설명한 대로 사용자 세션에 사용됩니다.

관련 항목

Remote Access VPN에 대한 AAA 설정, 1177 페이지

AAA 서버 연결 이해

LDAP, AD 및 RADIUS AAA 서버는 사용자 ID 처리, VPN 인증 또는 두 가지 활동 모두와 같은 용도에 따라 Firepower Threat Defense 디바이스에서 연결할 수 있어야 합니다. AAA 서버는 Remote Access VPN에서 다음 활동을 위해 사용됩니다.

- 사용자 **ID** 처리 - 관리 인터페이스를 통해 서버에 연결할 수 있어야 합니다.

  Firepower Threat Defense 디바이스에서 관리 인터페이스는 VPN에서 사용하는 일반 인터페이스와는 다른별도의 라우팅 프로세스 및 구성을 갖습니다.

- **VPN** 인증 - 서버는 , 즉 진단 인터페이스 또는 데이터 인터페이스와 같은 일반 인터페이스 중 하나를 통해 연결할 수 있어야 합니다.

  일반 인터페이스에 대해 2개의 라우팅 테이블이 사용됩니다. 진단 인터페이스 및 관리 전용으로 구성된 기타 모든 인터페이스에 대한 관리 전용 라우팅 테이블 및 데이터 인터페이스에 사용되는 데이터 라우팅 테이블입니다. 경로 조회가 완료되면 먼저 관리 전용 라우팅 테이블을 확인한 다음 데이터 라우팅 테이블을 확인합니다. 첫 번째 일치 조건은 AAA 서버에 도달하기 위해 선택됩니다.

  참고 데이터 인터페이스에 AAA 서버를 배치하는 경우 관리 전용 라우팅 정책이 데이터 인터페이스로 향하는 트래픽과 일치하지 않아야 합니다. 예를 들어 진단 인터페이스를 통한 기본 경로가 있는 경우 트래픽이 데이터 라우팅 테이블로 폴백하지 않습니다. **show route management-only** 및 **show route** 명령을 사용하여 라우팅 결정을 확인합니다.

동일한 AAA 서버에 있는 두 가지 활동의 경우 사용자 ID 처리를 위해 관리 인터페이스를 통해 서버에 연결하는 것 외에도 다음 중 하나를 수행하여 동일한 AAA 서버에 대한 VPN 인증 액세스를 제공합니다.

- 관리 인터페이스와 동일한 서브넷의 IP 주소로 진단 인터페이스를 활성화하고 구성한 다음 이 인터페이스를 통해 AAA 서버에 대한 경로를 구성합니다. 진단 인터페이스 액세스는 VPN 활동, ID 처리를 위한 관리 인터페이스 액세스에 사용됩니다.

참고 이러한 방식으로 구성하면 진단 및 관리 인터페이스와 동일한 서브넷에 데이터 인터페이스를 가질 수도 없습니다. 예를 들어 디바이스 자체를 게이트웨이로 사용할 때와 같이 관리 인터페이스와 데이터 인터페이스가 동일한 네트워크에 있으면 진단 인터페이스를 비활성화 상태로 유지해야 하기 때문에 이 솔루션을 사용할 수 없습니다.

- 데이터 인터페이스를 통해 AAA 서버에 대한 경로를 구성합니다. 데이터 인터페이스 액세스는 VPN 활동, 사용자 ID 처리를 위한 관리 인터페이스 액세스에 사용됩니다.

참고 FQDN 또는 호스트 이름을 사용하여 AAA 서버 이름, 이름이 지정된 URL 및 CA 서버를 사용하려면 각 디바이스에 DNS를 구성해야 합니다. DNS가 없으면 시스템은 IP 주소만 구성하고 사용할 수 있습니다. 플랫폼 설정을 사용하여 DNS를 구성할 수 있습니다. 자세한 내용은 DNS 구성, 1425 페이지 및 DNS 서버 그룹 개체, 637 페이지를 참조하십시오.

여러 인터페이스에 대한 자세한 내용은 Firepower Threat Defense 일반 방화벽 인터페이스, 793 페이지 섹션을 참조하십시오.

구축 후 다음 CLI 명령을 사용하여 Firepower Threat Defense 디바이스에서 AAA 서버 연결을 모니터링하고 문제를 해결합니다.

- **show aaa-server** - AAA 서버 통계를 표시합니다.
- **show route management-only** - 관리 전용 라우팅 테이블 항목을 봅니다.
- **show network**과 **show network-static-routes**가 관리 인터페이스 기본 경로 및 고정 경로를 확인합니다.
- **show route** - 데이터 트래픽 라우팅 테이블 항목을 봅니다.
- **ping system**과 **traceroute system**가 관리 인터페이스를 통해 AAA 서버에 대한 경로를 확인합니다.
- **ping interface** *ifname* 및 **traceroute** *destination* - 진단 및 데이터 인터페이스를 통해 AAA 서버에 대한 경로를 확인합니다.
- **test aaa-server authentication** 및 **test aaa-server authorization** - AAA 서버에서 인증 및 권한 부여를 테스트합니다.
- **clear aaa-server statistics** *groupname* 또는 **clear aaa-server statistics protocol** *protocol* - 그룹 또는 프로토콜별로 AAA 서버 통계를 지웁니다.
- **aaa-server** *groupname* **active host** *hostname* - 실패한 AAA 서버를 활성화합니다. **aaa-server** *groupname* **fail host** *hostname* - AAA 서버에 실패합니다.
- **debug ldap leveldebug aaa authentication**, **debug aaa authorization** 및 **debug aaa accounting**.

원격 액세스 VPN 라이선스 요구 사항

FTD 라이센스

FTD 원격 액세스 VPN에는 AnyConnect에 대한 강력한 암호화 및 다음 라이선스 중 하나가 필요합니다.

- AnyConnect Plus
- AnyConnect Apex
- AnyConnect VPN만

원격 액세스 VPN 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

Remote Access VPN에 대한 지침 및 제한 사항

원격 액세스 **VPN** 정책 구성

- 신규 원격 접속 VPN 정책을 추가하려면 마법사를 사용해야만 합니다. 새 정책을 생성하려면 마법사 전체를 진행해야 합니다. 마법사를 완료하기 전에 취소할 경우 정책이 저장되지 않습니다.
- 사용자 두 명이 원격 접속 VPN 정책을 동시에 편집해서는 안 됩니다. 그러나 웹 인터페이스는 동시 편집을 차단하지 않습니다. 동시 수정이 일어날 경우, 마지막으로 저장된 컨피그레이션이 유지됩니다.
- 원격 액세스 VPN 정책이 해당 디바이스에 할당되어 있다면 한 도메인에서 다른 도메인으로 Firepower Threat Defense 디바이스를 이동할 수 없습니다.
- 클러스터 모드의 Firepower 9300 및 4100 시리즈는 원격 액세스 VPN 구성을 지원하지 않습니다.
- 잘못 구성된 FTD NAT 규칙이 있다면 원격 액세스 VPN 연결이 실패할 수 있습니다.

- 마법사를 사용하여 원격 액세스 VPN을 구성하는 동안 인라인 인증서 등록 개체를 만들 수 있지만 이를 사용하여 ID 인증서를 설치할 수는 없습니다. 인증서 등록 개체는 원격 액세스 VPN 게이트웨이로 구성되는 Firepower Threat Defense 디바이스에서 ID 인증서를 생성하는 데 사용됩니다. 디바이스에 원격 액세스 VPN 정책을 배포하기 전에 ID 인증서를 설치하십시오. 인증서 등록 개체를 기반으로 ID 인증서를 설치하는 방법에 대한 자세한 내용은 개체 관리자, 560 페이지 섹션을 참조하십시오.
- 원격 액세스 VPN 정책 구성을 변경한 후에는 변경 내용을 Firepower Threat Defense 디바이스에 다시 구축합니다. 구성 변경을 구축하는 데 걸리는 시간은 정책 및 규칙의 복잡성, 디바이스에 전송하는 구성 유형 및 볼륨, 메모리 및 디바이스 모델과 같은 여러 요소에 따라 다릅니다. 원격 액세스 VPN 정책 변경 사항을 구축하기 전에 구성 변경 사항 구축을 위한 모범 사례, 492 페이지 섹션을 검토하십시오.

동시 VPN 세션 용량 계획

최대 동시 VPN 세션은 플랫폼별 한도에 의해 관리되며 라이선스에 의존하지 않습니다. 디바이스 모델에 따라 디바이스에서 허용되는 동시 원격 액세스 VPN 세션 수에는 최대 제한이 적용됩니다. 이러한 제한은 시스템 성능이 부적절한 레벨로 저하되지 않도록 설계된 것입니다. 용량 계획 시에 이러한 제한을 사용하십시오.

디바이스 모델	최대 동시 원격 액세스 VPN 세션
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10000

다른 하드웨어 모델의 용량을 알고 싶다면 영업 담당자에게 문의하십시오.

참고 FTD 디바이스는 플랫폼 당 최대 세션 한도에 도달하면 VPN 연결을 거부합니다. 이 연결은 시스템 로그 메시지와 함께 거부됩니다. 시스템 로그 메시지 %ASA-4-113029 및 %ASA-4-113038는 시스템 로그 메시징 가이드를 참조하십시오. 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/security/asa/syslog-guide/syslogs.html을 참조해 주십시오.

VPN에 대한 암호 사용 제어

DES 보다 큰 암호 사용을 방지하기 위해 Firepower Management Center의 다음 위치에서 사전 구축 확인을 할 수 있습니다.

Devices(디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SSL Settings(SSL** 설정**)**

Devices(디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)** > **Advanced(**고급**)** > **IPsec**

SSL 설정 및 IPsec에 대한 자세한 내용은 SSL 설정 , 1431 페이지 및 Remote Access VPN IPsec/IKEv2 파라미터 구성, 1196 페이지을 참조하십시오.

인증, 권한 부여 및 계정 관리(AAA)

- Firepower Threat Defense 디바이스는 시스템 통합 인증 서버만 사용하는 원격 액세스 VPN 사용자의 인증을 지원하므로 로컬 사용자 데이터베이스는 지원되지 않습니다.
- 원격 액세스 VPN을 사용하려면 토폴로지의 각 디바이스에 DNS를 구성합니다. DNS가 없으면 디바이스는 AAA 서버 이름, 이름이 지정된 URL 및 FQDN 또는 호스트 이름이 있는 CA 서버를 확인할 수 없으며 IP 주소만 확인할 수 있습니다.

  플랫폼 설정을 사용하여 DNS를 구성할 수 있습니다. 자세한 내용은 DNS 구성, 1425 페이지 및 DNS 서버 그룹 개체, 637 페이지를 참조하십시오.

클라이언트 인증서

- 구축에서 클라이언트 인증서를 사용하고 있는 경우, Firepower Threat Defense 또는 Firepower Management Center와 무관한 클라이언트 플랫폼에 해당 인증서를 추가해야 합니다. 클라이언트에 인증서를 입력할 수 있는 기능인 SCEP 또는 CA 서비스 등은 제공되지 않습니다.

AnyConnect의 지원되지 않는 기능

지원되는 VPN 클라이언트는 Cisco AnyConnect Secure Mobility Client뿐입니다. 그 외의 클라이언트 또는 네이티브 VPN은 지원되지 않습니다. 클라이언트리스 VPN은 VPN 연결에는 지원되지 않으며, 웹 브라우저를 이용해 AnyConnect 클라이언트를 구축하는 용도로만 사용됩니다.

다음 AnyConnect 기능은 FTD 보안 게이트웨이에 연결할 때는 지원되지 않습니다.

- Hostscan, Endpoint Posture Assessment 및 클라이언트 포스처 기반의 동적 액세스 정책 등의 포스처 변수.
- AnyConnect 사용자 지정 및 현지화 지원. FTD 디바이스는 이러한 기능을 위해 AnyConnect를 구성하는 데 필요한 파일을 구성하거나 구축하지 않습니다.
- FTD에서는 AnyConnect 클라이언트에 대한 맞춤 설정 속성이 지원되지 않습니다. 따라서 맞춤 설정 속성을 사용하는 모든 기능이 지원되지 않습니다. 여기에는 데스크톱 클라이언트의 Deferred Upgrade(지연된 업그레이드) 및 모바일 클라이언트의 Per-App VPN(애플리케이션별 VPN)이 포함됩니다.
- 로컬 인증입니다. VPN 사용자는 FTD 보안 게이트웨이에 구성할 수 없습니다.

  로컬 CA의 경우 보안 게이트웨이는 Certificate Authority의 역할을 할 수 없습니다.
- TACACS, Kerberos(KCD 인증) 및 RSA SDI
- 브라우저 프록시
- VPN 로드 밸런싱

새 Remote Access VPN 연결 구성

이 섹션에서는 Firepower Threat Defense 디바이스를 VPN 게이트웨이로 사용하고 Cisco AnyConnect를 VPN 클라이언트로 이용해 새로운 원격 액세스 VPN 정책을 구성하는 방법을 설명합니다.

	수행해야 할 작업	추가 정보
1단계	지침 및 사전 요구 사항을 검토합니다.	Remote Access VPN에 대한 지침 및 제한 사항, 1162 페이지 Remote Access VPN 구성 사전 요구 사항, 1165 페이지
2단계	마법사를 사용하여 원격 액세스 VPN 정책을 생성합니다.	새 Remote Access VPN 정책 생성, 1166 페이지
3단계	디바이스에 구축한 액세스 제어 정책을 업데이트합니다.	Firepower Threat Defense 디바이스의 액세스 제어 정책 업데이트, 1168 페이지
4단계	(선택 사항) NAT가 디바이스에 구성된 경우 NAT 면제 규칙을 구성합니다.	(선택 사항) NAT 제외 설정, 1169 페이지
5단계	DNS를 구성합니다.	DNS 구성, 1170 페이지
6단계	AnyConnect 클라이언트 프로파일을 추가합니다.	AnyConnect 클라이언트 프로파일 XML 파일 추가, 1171 페이지
7단계	원격 액세스 VPN 정책을 구축합니다.	컨피그레이션 변경 사항 구축, 498 페이지
8단계	(선택 사항) 원격 액세스 VPN 정책 구성을 확인합니다.	구성 확인, 1172 페이지

Remote Access VPN 구성 사전 요구 사항

- Firepower Threat Defense 디바이스를 구축하고 내보내기 제어 기능이 활성화된 상태에서 필요한 라이선스로 디바이스를 관리하도록 Firepower Management Center을(를) 구성합니다. 자세한 내용은 VPN 라이선싱, 1125 페이지의 내용을 참고하십시오.
- 원격 액세스 VPN 게이트웨이 역할을 하는 각 Firepower Threat Defense 디바이스에 대한 ID 인증서를 얻는 데 사용되는 인증서 등록 개체를 구성합니다.
- Remote Access VPN 정책에서 사용 중인 RADIUS 서버 그룹 개체와 AD 또는 LDAP 영역을 구성합니다.
- Remote Access VPN 구성이 작동하려면 Firepower Threat Defense 디바이스에서 AAA 서버에 연결할 수 있는지 확인합니다. 라우팅을 구성(**Devices(**디바이스**) > Device Management(**디바이스

관리) > **Edit Device**(디바이스 편집) > **Routing**(라우팅))하여 AAA 서버에 대한 연결성을 보장합니다.

Remote Access VPN 이중 인증의 경우 해당 이중 인증 구성이 작동하려면 Firepower Threat Defense 디바이스에서 기본 및 보조 인증 서버에 모두 연결할 수 있는지 확인합니다.

- AnyConnect Plus, AnyConnect Apex 또는 AnyConnect VPN Only와 같은 Cisco AnyConnect 라이선스 중 하나를 구입하여 활성화하면 Firepower Threat Defense Remote Access VPN을 활성화할 수 있습니다.
- AnyConnect 이미지 파일을 Cisco 소프트웨어 다운로드 센터에서 다운로드하십시오.

  Firepower Management Center 웹 인터페이스에서 **Objects**(개체) > **Object Management**(개체 관리) > **VPN** > **AnyConnect File**(**AnyConnect** 파일)로 이동하고 새 AnyConnect 클라이언트 이미지 파일을 추가합니다.
- 사용자가 VPN 연결 시 액세스할 네트워크 인터페이스가 포함된 보안 영역 또는 인터페이스 그룹을 생성합니다. 보안 영역, 577 페이지의 내용을 참조하십시오.
- AnyConnect 클라이언트 프로파일을 생성하려면 Cisco 소프트웨어 다운로드 센터에서 AnyConnect Profile Editor를 다운로드합니다. 독립형 프로파일 편집기를 사용하여 새로운 AnyConnect 프로파일을 만들거나 기존 프로파일을 수정할 수 있습니다.

새 Remote Access VPN 정책 생성

Remote Access VPN Policy 마법사를 통해서만 새 원격 액세스 VPN 정책을 추가할 수 있습니다. 이 마법사는 기본 기능을 사용하여 Remote Access VPN을 쉽고 빠르게 설정할 수 있도록 안내합니다. 또한 원하는 대로 추가 속성을 지정하여 정책 구성을 개선하고 Firepower Threat Defense 보안 게이트웨이 디바이스에 구축할 수 있습니다.

시작하기 전에

- Remote Access VPN 구성 사전 요구 사항, 1165 페이지에 나열된 모든 전제 조건을 완료합니다.

프로시저

단계 **1** **Devices**(디바이스) > **VPN** > **Remote Access**(원격 액세스)을 선택합니다.

단계 **2** **(**추가(+))** 추가를 클릭하여 기본 정책 설정을 안내하는 마법사를 통해 새 Remote Access VPN 정책을 생성합니다.

마법사 전체를 진행하면서 새 정책을 생성해야 합니다. 마법사를 완료하기 전에 취소할 경우 어떤 정책도 저장되지 않습니다.

단계 **3** **Target Devices**(대상 디바이스) 및 **Protocols**(프로토콜)를 선택합니다.

여기에서 선택한 Firepower Threat Defense 디바이스는 VPN 클라이언트 사용자를 위한 Remote Access VPN 게이트웨이로 작동합니다. 목록에서 디바이스를 선택하거나 새 디바이스를 추가할 수 있습니다.

원격 액세스 VPN 정책을 생성하거나 나중에 변경할 때 Firepower Threat Defense 디바이스를 선택할 수 있습니다. 원격 액세스 VPN 정책 대상 디바이스 설정, 1173 페이지의 내용을 참조하십시오.

SSL 또는 **IPSec-IKEv2** 또는 두 VPN 프로토콜을 모두 선택할 수 있습니다. Firepower Threat Defense에서는 두 프로토콜을 모두 지원하여 VPN 터널을 통해 공용 네트워크에 대한 보안 연결을 설정합니다.

참고 Firepower Threat Defense NULL 암호화를 사용하는 IPSec 터널을 지원하지 않습니다. IPSec-IKEv2를 선택한 경우 IPSec IKEv2 제안에 대해 NULL 암호화를 선택하지 않아야 합니다. IKEv2 IPsec 제안 개체 설정, 655 페이지의 내용을 참조하십시오.

SSL 설정에 대해서는 SSL 설정 , 1431 페이지의 내용을 참조하십시오.

단계 **4** **Connection Profile(**연결 프로파일**)**과 **Group Policy(**그룹 프로파일**)** 설정을 구성합니다.

연결 프로파일은 원격 사용자가 VPN 디바이스에 연결하는 방법을 정의하는 파라미터 집합을 지정합니다. 이 파라미터에는 인증을 위한 설정 및 속성, VPN 클라이언트에 대한 주소 할당 및 그룹 정책이 포함됩니다. Firepower Threat Defense 디바이스는 Remote Access VPN 정책을 구성할 때 *DefaultWEBVPNGroup*이라는 기본 연결 프로파일을 제공합니다.

자세한 내용은 연결 프로파일 설정, 1173 페이지를 참고하십시오.

설정에 대한 자세한 내용은

- AAA 설정, 참조 Remote Access VPN에 대한 AAA 설정, 1177 페이지
- LDAP 특성 맵, 참조 LDAP 특성 매핑 구성, 1190 페이지
- SAML 2.0 SSO(Single Sign-On, 단일 인증) 인증, 참조 SAML SSO(Single Sign-On) 인증 구성, 1207 페이지

그룹 정책은 VPN 사용자의 원격 액세스 VPN 경험을 정의하는 그룹 정책 개체가 저장된 속성 및 값 쌍의 집합입니다. 그룹 정책을 이용해 사용자 인증 프로파일, IP 주소, AnyConnect 설정, VLAN 매핑, 사용자 세션 설정 등의 속성을 구성합니다. RADIUS 권한 서버는 그룹 정책을 할당하거나 현재 연결 프로파일에서 그룹 정책을 가져옵니다.

자세한 내용은 그룹 정책 구성, 1189 페이지를 참고하십시오.

단계 **5** VPN 사용자가 Remote Access VPN에 연결하는 데 사용할 **AnyConnect** 클라이언트 이미지를 선택합니다.

Cisco AnyConnect Secure Mobility Client는 기업 리소스에 대한 전체 VPN 프로파일링을 통해 원격 사용자에게 Firepower Threat Defense 디바이스에 대한 SSL 또는 IPSec(IKEv2) 연결을 제공합니다. Remote Access VPN 정책이 Firepower Threat Defense 디바이스에 구축된 후 VPN 사용자는 브라우저에 구성된 디바이스 인터페이스의 IP 주소를 입력하여 AnyConnect 클라이언트를 다운로드하고 설치할 수 있습니다.

AnyConnect 클라이언트 프로파일 및 클라이언트 모듈 구성에 대한 자세한 내용은 그룹 정책 AnyConnect 옵션, 659 페이지의 내용을 참고하십시오.

단계 **6** **Network Interface and Identity Certificate(**네트워크 인터페이스 및 **ID** 인증서**)**를 선택합니다.

인터페이스 개체는 네트워크를 세그먼트로 나눠 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다. 보안 영역은 인터페이스를 그룹화합니다. 이러한 그룹의 범위는 여러 디바이스를 포괄할 수 있으며, 단일 디바이스에서 여러 영역 인터페이스 개체를 구성할 수도 있습니다. 인터페이스 개체의 유형은 두 가지입니다.

- 보안 영역 — 하나의 인터페이스가 하나의 보안 영역에만 속할 수 있습니다.
- 인터페이스 그룹 — 하나의 인터페이스가 여러 인터페이스 그룹(및 하나의 보안 영역)에 속할 수 있습니다.

단계 **7** Remote Access VPN 정책 구성의 **Summary(**요약**)**를 봅니다.

Summary(요약) 페이지에는 지금까지 구성한 모든 Remote Access VPN 설정이 표시되고 선택한 디바이스에 Remote Access VPN 정책을 구축하기 전에 수행해야 하는 추가 구성에 대한 링크가 제공됩니다.

필요한 경우 **Back(**뒤로**)**을 클릭하여 구성을 변경합니다.

단계 **8** **Finish(**마침**)**를 클릭하여 Remote Access VPN 정책의 기본 구성을 완료합니다.

마법사를 사용하여 Remote Access VPN 정책을 완료하면 정책 목록 페이지로 돌아갑니다. 기본 RA VPN 정책 구성을 완료하려면 DNS 구성을 설정하고 VPN 사용자에 대한 액세스 제어를 구성하고 NAT 제외(필요한 경우)를 활성화합니다. 그런 다음 구성을 구축하고 VPN 연결을 설정합니다.

Firepower Threat Defense 디바이스의 액세스 제어 정책 업데이트

Remote Access VPN 정책을 구축하기 전에 대상 Firepower Threat Defense 디바이스의 액세스 제어 정책을 VPN 트래픽을 허용하는 규칙으로 업데이트해야 합니다. 이 규칙은 소스를 정의된 VPN 풀 네트워크로 지정하고 대상을 회사 네트워크로 지정하여 외부 인터페이스에서 들어오는 모든 트래픽을 허용해야 합니다.

참고 Access Interface(액세스 인터페이스) 탭에서 **Bypass Access Control policy for decrypted traffic(**암호해독된 트래픽에 대해 액세스 제어 정책 우회**)(sysopt permit-vpn)**을 선택한 경우 Remote Access VPN에 대한 액세스 제어 정책을 업데이트할 필요가 없습니다.

모든 VPN 연결에 대한 옵션을 활성화하거나 비활성화합니다. 이 옵션을 비활성화하는 경우, 액세스 제어 정책 또는 사전 필터 정책에서 트래픽을 허용해야 합니다.

자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 1184 페이지를 참고하십시오.

시작하기 전에

Remote Access VPN 정책 마법사를 사용하여 Remote Access VPN 정책 구성을 완료합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** Remote Access VPN 정책을 구축할 대상 디바이스에 할당된 액세스 제어 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭하여 새로운 규칙을 추가합니다.

단계 **4** 규칙에 대한 **Name(**이름**)**을 지정하고 **Enabled(**활성화됨**)**를 선택합니다.

단계 **5** **Action(**작업**)**, **Allow(**허용**)** 또는 **Trust(**신뢰**)**를 선택합니다.

단계 **6** **Zones(**영역**)** 탭에서 다음을 선택합니다.

a) Available Zones(사용 가능한 영역) 목록에서 외부 영역을 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다.

b) Available Zones(사용 가능한 영역) 목록에서 내부 영역을 선택하고 **Add to Destination(**대상에 추가**)**를 클릭합니다.

단계 **7** **Networks(**네트워크**)** 탭에서 다음을 선택합니다.

a) Available networks(사용 가능한 네트워크)에서 내부 네트워크(내부 인터페이스 및/또는 기업 네트워크)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.

b) **Available Networks(**사용 가능한 네트워크**)**에서 VPN address pool network(VPN 주소 풀 네트워크)를 선택하고 **Add to Source Networks(**소스 네트워크에 추가**)**를 클릭합니다.

단계 **8** 기타 필수 액세스 제어 규칙 설정을 구성하고 **Add(**추가**)**를 클릭합니다.

단계 **9** 규칙 및 액세스 제어 정책을 저장합니다.

(선택 사항) NAT 제외 설정

NAT 제외는 주소 변환을 제외하고 변환된 호스트와 원격 호스트가 모두 보호되는 호스트와의 연결을 시작할 수 있도록 허용합니다. ID NAT와 마찬가지로 특정 인터페이스의 호스트에 대한 변환은 제한하지 않습니다. 모든 인터페이스를 통한 연결에는 NAT 제외를 사용해야 합니다. 하지만 (정책 NAT처럼) NAT 제외는 변환할 실제 주소를 결정할 때 실제 주소와 대상 주소를 지정할 수 있게 활성화합니다. 고정 ID NAT를 사용하여 액세스 목록의 포트를 고려합니다.

시작하기 전에

Remote Access VPN 정책이 구축된 대상 디바이스에 NAT가 구성되어 있는지 확인합니다. NAT가 대상 디바이스에서 활성화된 경우, NAT VPN 트래픽을 제외하도록 NAT 정책을 정의해야 합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)** > **NAT**를 클릭합니다.

단계 **2** 업데이트할 NAT 정책을 선택하거나 **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭하여 모든 인터페이스를 통한 연결을 허용하는 NAT 규칙이 있는 NAT 정책을 생성합니다.

단계 **3** **Add Rule(**규칙 추가**)**을 클릭하여 NAT 규칙을 추가합니다.

단계 **4** Add NAT Rule(NAT 규칙 추가) 창에서 다음을 선택합니다.

a) NAT Rule(NAT 규칙)을 **Manual NAT Rule(**수동 **NAT** 규칙**)**으로 선택합니다.

b) Type(유형)을 **Static(**고정**)**으로 선택합니다.

c) **Interface Objects(**인터페이스 개체**)**를 클릭하고 소스 및 대상 인터페이스 개체를 선택합니다.

참고 이 인터페이스 개체는 Remote Access VPN 정책에서 선택한 인터페이스와 동일해야 합니다.

자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 1184 페이지의 내용을 참고하십시오.

a) **Translation(**변환**)**을 클릭하고 소스 및 대상 네트워크를 선택합니다.

- **Original Source(**원래 소스**)** 및 **Translated Source(**변환된 소스**)**
- **Original Destination(**원래 대상**)** 및 **Translated Destination(**변환된 대상**)**

단계 **5** Advanced(고급) 탭에서 **Do not proxy ARP on Destination Interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)**를 선택합니다.

Do not proxy ARP on Destination Interface(대상 인터페이스에서 **ARP** 프록시 설정 안 함**)** - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

DNS 구성

Remote Access VPN을 사용하려면 각 Firepower Threat Defense 디바이스에 DNS를 구성합니다. DNS가 없으면 디바이스는 AAA 서버 이름, 이름이 지정된 URL 및 FQDN 또는 호스트 이름이있는 CA 서버를 확인할 수 없습니다. IP 주소만 확인할 수 있습니다.

프로시저

단계 **1** 플랫폼 설정을 사용하여 DNS 서버 상세정보 및 도메인 조회 인터페이스를 구성합니다. 자세한 내용은 DNS 구성, 1425 페이지 및 DNS 서버 그룹 개체, 637 페이지의 내용을 참조하십시오.

단계 2 VNP 네트워크를 통해 DNS 서버에 연결할 수 있는 경우 그룹 정책에서 스플릿 터널을 구성하여 Remote Access VPN 터널을 통한 DNS 트래픽을 허용합니다. 자세한 내용은 그룹 정책 개체 설정, 656 페이지를 참고하십시오.

AnyConnect 클라이언트 프로파일 XML 파일 추가

AnyConnect 클라이언트 프로파일은 XML 파일에 저장된 구성 파라미터 그룹으로, 클라이언트는 이를 사용하여 운영 및 모양을 구성합니다. 이러한 매개변수(XML 태그)에는 추가적인 클라이언트 기능을 활성화할 수 있는 호스트 컴퓨터 및 설정의 이름과 주소가 포함되어 있습니다.

AnyConnect 프로파일 편집기를 사용하여 AnyConnect 클라이언트 프로파일을 생성할 수 있습니다. 이 편집기는 AnyConnect 소프트웨어 패키지의 일부로 제공되는 GUI 기반 구성 툴입니다. 이 툴은 Firepower Management Center 외부에서 실행되는 독립 프로그램입니다. AnyConnect 프로파일 편집기 사용에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서를 참조하십시오.

시작하기 전에

Firepower Threat Defense Remote Access VPN 정책을 사용하려면 AnyConnect 클라이언트 프로파일을 VPN 클라이언트에 할당해야 합니다. 클라이언트 프로파일이 그룹 정책에 연결됩니다.

Cisco 소프트웨어 다운로드 센터에서 AnyConnect 프로파일 편집기를 다운로드할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.
Remote Access VPN 정책에 대해 구성된 연결 프로파일이 나열됩니다.

단계 3 AnyConnect 클라이언트 프로파일을 업데이트할 연결 프로파일을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 4 **Add(**추가**)**를 클릭하여 그룹 정책을 추가하거나 **Edit Group Policy(**그룹 정책 편집**)** > **General(**일반**)** > **AnyConnect**를 클릭합니다.

단계 5 목록에서 Client Profile(클라이언트 프로파일)을 선택하거나 **Add(**추가**)** 아이콘을 클릭하여 새 프로파일을 추가합니다.

a) AnyConnect 프로파일 이름을 지정합니다.

b) **Browse(**찾아보기**)**를 클릭하고 AnyConnect 프로파일 XML 파일을 선택합니다.

참고 2단계 인증의 경우 AnyConnect 클라이언트 프로파일 XML 파일에서 시간 초과가 60 초 이상으로 업데이트되었는지 확인합니다.

c) **Save(**저장**)**를 클릭합니다.

(선택 사항) 스플릿 터널링 구성

스플릿 터널을 이용하면 보안 터널을 통한 원격 네트워크 VPN 연결이 가능하며, VPN 터널 외부의 네트워크에도 연결할 수 있습니다. VPN 사용자가 원격 액세스 VPN에 연결되어 있는 동안 외부 네트워크에 액세스하게 하려면, 분할 터널을 구성하면 됩니다. 스플릿 터널 목록을 구성하려면 표준 액세스 목록 또는 확장 액세스 목록을 생성해야 합니다.

자세한 내용은 그룹 정책 구성, 1189 페이지를 참고하십시오.

프로시저

단계 **1** **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** Connection Profile(연결 프로파일)을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭하여 그룹 정책을 추가하거나 **Edit Group Policy(**그룹 정책 편집**)** > **General(**일반**)** > **Split Tunneling(**스플릿 터널링**)**을 클릭합니다.

단계 **5** **IPv4 Split Tunneling(IPv4** 스플릿 터널링**)** 또는 **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)** 목록에서 **Exclude networks specified below(**아래에 지정된 네트워크 제외**)**를 선택하고, VPN 트래픽에서 제외할 네트워크를 선택합니다.
스플릿 터널링 옵션이 그대로 유지되면 엔드포인트의 모든 트래픽이 VPN 연결을 통해 이동합니다.

단계 **6** **Standard Access List(**표준 액세스 목록**)** 또는 **Extended Access List(**확장 액세스 목록**)**를 클릭하고 드롭다운 목록에서 액세스 목록을 선택하거나 새 목록을 추가합니다.

단계 **7** 새 표준 액세스 목록 또는 확장 액세스 목록을 추가하기로 선택한 경우 다음을 수행합니다.

a) 새 액세스 목록에 대한 이름을 지정하고 **Add(**추가**)**를 클릭합니다.
b) Action(동작) 드롭다운에서 **Allow(**허용**)**를 선택합니다.
c) VPN 터널에서 허용할 네트워크 트래픽을 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

액세스 목록, 644 페이지

구성 확인

프로시저

단계 **1** 외부 네트워크의 시스템에서 웹 브라우저를 엽니다.

단계 **2** 원격 액세스 VPN 게이트웨이로 구성된 FTD 디바이스의 URL을 입력합니다.

단계 **3** 메시지가 표시되면 사용자 이름 및 비밀번호를 입력하고 **Logon(**로그인**)**을 클릭합니다.

참고 시스템에 AnyConnect가 설치돼 있다면 VPN에 자동으로 연결됩니다.

AnyConnect가 설치되지 않았다면 AnyConnect 클라이언트를 다운로드하라는 메시지가 표시됩니다.

단계 4 설치되지 않았다면 AnyConnect를 다운로드하고 VPN에 연결합니다.
AnyConnect 클라이언트는 자체적으로 설치됩니다. 인증에 성공하면 Firepower Threat Defense 원격 액세스 VPN 게이트웨이에 연결됩니다. 해당하는 ID 또는 QoS 정책은 원격 액세스 VPN 정책 구성에 따라 적용됩니다.

원격 액세스 VPN 정책 대상 디바이스 설정

새 Remote Access VPN 정책을 생성하는 동안 대상 디바이스를 추가하거나 나중에 변경할 수 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 편집할 Remote Access VPN 정책 옆의 수정( )을 클릭합니다.

단계 3 **Policy Assignment(**정책 할당**)**를 클릭합니다.

단계 4 다음 중 하나를 수행합니다.

- 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹을 정책에 할당하려면 **Available Devices(**사용 가능한 디바이스**)** 목록에서 이를 선택하고 **Add(**추가**)**를 클릭합니다. 사용 가능한 디바이스를 끌어다 놓아 선택할 수도 있습니다.
- 디바이스 할당을 제거하려면 **Selected Devices(**선택한 디바이스**)** 목록의 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹 옆에 있는 삭제( )를 클릭합니다.

단계 5 **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

선택적 Remote Access VPN 구성

연결 프로파일 설정

Remote Access VPN 정책은 특정 디바이스를 대상으로 하는 연결 프로파일을 포함합니다. 이러한 정책은 터널 자체를 생성하는 방법 예를 들어 AAA를 구현하는 방법, VPN 클라이언트에 주소를 할당하는 방법(DHCP 또는 주소 풀)과 관련이 있습니다. 또한 Firepower Threat Defense 디바이스에 구성되거나 AAA 서버에서 다운로드한 그룹 정책에서 식별된 사용자 속성을 포함합니다. 디바이스는

*DefaultWEBVPNGroup*이라는 기본 연결 프로파일도 제공합니다. 마법사를 사용하여 구성된 연결 프로파일이 목록에 나타납니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Connection Profile(**연결 프로파일**)**을 선택하고 **Edit(**편집**)**을 클릭합니다.
연결 프로파일 편집 페이지가 표시됩니다.

단계 **4** (선택 사항) 여러 연결 프로파일을 추가합니다.
여러 연결 프로파일 설정, 1174 페이지

단계 **5** VPN 클라이언트에 대한 IP 주소를 구성합니다.
VPN 클라이언트에 대한 IP 주소 설정, 1175 페이지

단계 **6** (선택 사항) Remote Access VPN에 대한 AAA 설정을 업데이트합니다.
Remote Access VPN에 대한 AAA 설정, 1177 페이지

단계 **7** (선택 사항) 별칭을 생성하거나 업데이트합니다.
연결 프로파일에 대한 별칭 생성 또는 업데이트, 1183 페이지

단계 **8** 연결 프로파일을 저장합니다.

여러 연결 프로파일 설정

다른 VPN 사용자 그룹에 다른 권한을 부여하기로 결정한 경우 각 사용자 그룹에 대해 특정 연결 프로파일이나 그룹 정책을 구성할 수 있습니다. 예를 들어 금융 그룹에서 사설 네트워크의 특정 부분에 액세스하고 고객 지원 그룹에서 다른 부분에 액세스하며 MIS 그룹에서 기타 부분에 액세스하도록 허용할 수 있습니다. 또한, MIS 내에 있는 특정 사용자가 다른 MIS 사용자는 액세스할 수 없는 시스템에 액세스하도록 허용할 수도 있습니다. 연결 프로파일 및 그룹 정책은 이 작업을 안전하게 수행할 수 있도록 유연성을 제공합니다.

원격 액세스 정책 마법사를 사용하여 VPN 정책을 생성할 때 하나의 연결 프로파일만 구성할 수 있습니다. 나중에 더 많은 연결 프로파일을 추가할 수 있습니다. 디바이스는 *DefaultWEBVPNGroup*이라는 기본 연결 프로파일도 제공합니다.

시작하기 전에

연결 프로파일과 함께 원격 액세스 정책 마법사를 사용하여 Remote Access VPN을 구성했는지 확인합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.
기존 원격 액세스 정책이 나열됩니다.

단계 **2** 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭하고 Add Connection Profile(연결 프로파일 추가) 창에서 다음을 지정합니다.

a) **Connection Profile(**연결 프로파일**)**—원격 사용자가 VPN 연결에서 사용하는 이름을 제공합니다. 연결 프로파일은 원격 사용자가 VPN 디바이스에 연결하는 방법을 정의하는 파라미터 집합을 포함하고 있습니다.

b) **Client Address Assignment(**클라이언트 주소 할당**)** - 로컬 IP 주소 풀, DHCP 서버와 AAA 서버에서 원격 클라이언트에 대한 IP 주소를 할당합니다.

c) **AAA** - AAA 서버를 구성하여 보안 VPN 게이트웨이 역할의 매니지드 디바이스가 사용자(인증), 사용자가 수행하도록 허용된 작업(권한 부여) 및 사용자가 수행한 작업(계정)을 결정하도록 활성화합니다.

d) **Aliases(**별칭**)** - 연결 프로파일에 대한 대체 이름 또는 URL을 입력합니다. Remote Access VPN 관리자는 Alias name(별칭 이름) 및 Alias URL(별칭 URL)을 활성화 또는 비활성화할 수 있습니다. VPN 사용자는 AnyConnect VPN 클라이언트를 사용하여 Firepower Threat Defense 디바이스 Remote Access VPN에 연결할 때 별칭 이름을 선택할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 1173 페이지

VPN 클라이언트에 대한 IP 주소 설정

클라이언트 주소 할당은 원격 액세스 VPN 사용자에게 IP 주소를 할당하는 방법을 제공합니다.

로컬 IP 주소 풀, DHCP 서버와 AAA 서버에서 원격 VPN 클라이언트에 대한 IP 주소를 지정하도록 구성할 수 있습니다. AAA 서버에 먼저 할당한 후 다른 서버에 할당합니다. **Client Address Assignment(**클라이언트 주소 할당**)** 정책을 **Advanced(**고급**)**탭에서 구성하고 할당 기준을 정의합니다. 이 연결 프로파일에 정의된 IP 풀은 연결 프로파일 관련 그룹 정책 또는 시스템 기본 그룹 정책인 **DfltGrpPolicy**에서 정의된 IP 풀이 없을 때만 사용됩니다.

IPv4 Address Pools(IPv4 주소 풀**)**—SSL VPN 라이언트가 Firepower Threat Defense 디바이스에 연결할 때 새 IP 주소가 제공됩니다. 주소 풀은 원격 클라이언트에 제공할 수 있는 주소 범위를 정의합니다. 기존 IP 주소 풀을 선택합니다. IPv4 주소 및 IPv6 주소 각각에 최대 6개의 풀을 추가할 수 있습니다.

참고 Firepower Management Center에 있는 기존 IP 풀에서 IP 주소를 사용하거나 **Add(**추가**)** 옵션을 사용하여 새 풀을 생성할 수 있습니다. Firepower Management Center에서 **Objects(**개체**) > Object Management(**개체 관리**) > Address Pools(**주소 풀**)** 경로를 사용해 IP 풀을 생성할 수 있습니다. 자세한 내용은 주소 풀, 666 페이지를 참고하십시오.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.
기존 원격 액세스 정책이 나열됩니다.

단계 2 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 업데이트하려는 연결 프로파일을 선택하고 **Edit(**편집**)** > **Client Address Assignment(**클라이언트 주소 할당**)**를 클릭합니다.

단계 4 **Address Pools(**주소 풀**)**에 대해 다음을 선택합니다.

a) **Add(**추가**)**를 클릭하여 IP 주소를 추가하고 **IPv4** 또는 **IPv6**를 선택하여 해당 주소 풀을 추가합니다. Available Pools(사용 가능한 풀)에서 IP 주소 풀을 선택하고 **Add(**추가**)**를 클릭합니다.

참고 여러 Firepower Threat Defense 디바이스에서 Remote Access VPN 정책을 공유하는 경우, 디바이스 레벨 개체 재정의를 사용하여 전역 정의를 각 디바이스의 고유 주소 풀로 대체하지 않으면 모든 디바이스가 동일한 주소 풀을 공유합니다. 고유 주소 풀은 디바이스가 NAT를 사용하지 않는 경우 주소 중복을 방지하기 위해 필요합니다.

b) **Add(**추가**)** 아이콘을 **Address Pools(**주소 풀**)**창에서 선택하고 새 IPv4 또는 IPv6 주소 풀을 선택합니다. IPv4 풀을 선택하는 경우 시작 및 종료 IP 주소를 제공합니다. 새 IPv6 주소 풀을 포함시키려면 **Numver of Addresses(**주소 수**)** 를 1~16384 범위에서 입력합니다. 개체가 여러 디바이스에서 공유되는 경우 IP 주소와 충돌을 방지하기 위해 **Allow Overrides(**재정의 허용**)**를 선택합니다. 자세한 내용은 주소 풀, 666 페이지를 참고하십시오.

c) **OK(**확인**)**를 클릭합니다.

단계 5 **DHCP Servers(DHCP** 서버**)**에 대해 다음을 선택합니다.

참고 DHCP 서버 주소는 IPv4 주소와만 구성할 수 있습니다.

a) 이름 및 DHCP(Dynamic Host Configuration Protocol) 서버 주소를 네트워크 개체로 지정합니다. **Add(**추가**)**를 클릭하여 개체 목록에서 서버를 선택합니다. DHCP 서버를 삭제하려면 **Delete(**삭제**)**를 클릭합니다.

b) 네트워크 개체를 추가하려면 **New Objects(**새 개체**)** 페이지에서 **Add(**추가**)**를 클릭합니다. 새 개체 이름, 설명, 네트워크를 입력하고 해당하는 경우 **Allow Overrides(**재정의 허용**)** 옵션을 선택합니다. 자세한 내용은 네트워크 개체 생성, 571 페이지 및 개체 재정의 허용, 570 페이지를 참조하십시오.

c) **OK(**확인**)**를 클릭합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 1173 페이지

Remote Access VPN에 대한 AAA 설정

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** 연결 프로파일을 선택하여 AAA 설정을 업데이트하고 **Edit(**편집**)** > **AAA**를 클릭합니다.

단계 **4** **Authentication(**인증**)**에 대해 다음을 선택합니다.

- **Authentication Method(**인증 방법**)** - 네트워크 및 네트워크 서비스에 대한 액세스를 허용하기 전에 사용자를 식별하는 방법을 결정합니다. 유효한 사용자 자격 증명(일반적으로 사용자 이름 및 암호)을 요구하여 액세스를 제어합니다. 클라이언트에서 인증서를 포함할 수도 있습니다. 지원되는 인증 방법은 **AAA** 전용, 클라이언트 인증서 전용 및 **AAA +** 클라이언트 인증서입니다.

  다음과 같이 **Authentication Method(**인증 방법**)**를 선택하는 경우:

  - **AAA Only(AAA** 전용**)** - **Authentication Server(**인증 서버**)**를 **RADIUS**로 선택하는 경우 Authorization Server(권한 부여 서버)는 기본적으로 동일한 값을 가집니다. 드롭다운 목록에서 **Accounting Server(**과금 서버**)**를 선택합니다. Authentication Server(인증 서버) 드롭다운 목록에서 **AD** 및 **LDAP**를 선택할 때마다 **Authorization Server(**권한 부여 서버**)** 및 **Accounting Server(**과금 서버**)**를 각각 수동으로 선택해야 합니다.

  - **Client Certificate Only(**클라이언트 인증서 전용**)** - 각 사용자가 클라이언트 인증서로 인증합니다. 클라이언트 인증서는 VPN 클라이언트 엔드포인트에서 구성해야 합니다. 기본적으로 사용자 이름은 클라이언트 인증서 필드 CN 및 OU에서 파생됩니다. 사용자 이름이 클라이언트 인증서의 다른 필드에 지정된 경우 'Primary(기본)' 및 'Secondary(보조)' 필드를 사용하여 해당 필드를 매핑합니다.

    클라이언트 인증서의 사용자 이름을 포함하는 **Map specific field(**특정 필드 매핑**)** 옵션을 선택하면 **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에 **CN(Common Name)** 및 **OU(Organizational Unit)**의 기본값이 표시됩니다. **Use entire DN as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다. 고유 이름(DN)은 사용자를 연결 프로파일과 연결할 때 식별자로 사용할 수 있는 개별 필드로 구성된 고유한 ID입니다. DN 규칙은 향상된 인증서 인증에 사용됩니다.

    Map specific field(특정 필드 매핑**)** 옵션과 관련된 기본 및 보조 필드는 다음 공통 값을 포함합니다.

    - C(국가)
    - CN(이름)
    - DNQ(DN 한정자)
    - EA(이메일 주소)
    - GENQ(세대 한정자)
    - GN(이름)

- I(이니셜)
- L(시/군/구)
- N(이름)
- O(조직)
- OU(조직 단위)
- SER(일련 번호)
- SN(성)
- SP(시/도)
- T(제목)
- UID(사용자 ID)
- UPN(사용자 계정 이름)

- **Client Certificate & AAA(**클라이언트 인증서 및 **AAA)** - 각 사용자가 클라이언트 인증서와 AAA 서버로 인증합니다. 인증에 필요한 인증서 및 AAA 설정을 선택합니다.

  어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

- **SAML** - 각 사용자가 SAML SSO(Single Sign-On) 서버를 사용하여 인증됩니다. 자세한 내용은 SAML 2.0을 사용한 SSO(Single Sign-On) 인증, 1206 페이지를 참고하십시오.

- 인증 서버 - 인증은 네트워크 및 네트워크 서비스에 대한 액세스를 허용하기 전에 사용자를 식별하는 방법입니다. 인증에는 유효한 사용자 자격 증명, 인증서 또는 둘 모두가 필요합니다. 인증을 단독으로 사용하거나 권한 부여 및 어카운팅과 함께 사용할 수 있습니다.

  목록에서 영역, RADIUS 서버 그룹 또는 SSO(Single Sign-On) 서버를 선택합니다. 또는 Add(추가)를 클릭하여 인증 서버를 생성합니다.

  - **Realm(**영역**)** - LDAP 또는 AD 영역을 설정합니다. 영역 생성, 2466 페이지의 내용을 참조하십시오.
  - **RADIUS Server Group(RADIUS** 서버 그룹**)** - RADIUS 서버에 RADIUS 서버 그룹 개체를 추가합니다. RADIUS 서버 그룹, 667 페이지의 내용을 참조하십시오.
  - **Single Sign-On Server(SSO** 서버**)** - SAML 인증을 위한 SSO(Single Sign-On) 서버 개체를 생성합니다. SSO(Single Sign-On) 서버 추가, 670 페이지의 내용을 참조하십시오.

- **2**차 인증 사용 - VPN 세션에 대한 추가 보안을 제공하기 위해 기본 인증 외에 2차 인증이 구성됩니다. 2차 인증은 **AAA** 전용 및 클라이언트 인증서 및 **AAA** 인증 방법에만 적용됩니다.

보조 인증은 VPN 사용자가 AnyConnect 로그인 화면에 사용자 이름 및 암호 모음 2개를 입력해야 하는 선택적 기능입니다. 인증 서버 또는 클라이언트 인증서에서 2차 사용자 이름이 미리 입력되도록 구성할 수도 있습니다. 원격 액세스 VPN 인증은 기본 인증과 보조 인증을 모두 성공한 경우에만 부여됩니다. 인증 서버 중 하나에 연결할 수 없거나 한쪽 인증에서 장애가 발생하면 VPN 인증이 거부됩니다.

보조 인증을 구성하기 전에, 두 번째 사용자 이름과 암호에 대해 보조 인증 서버 그룹(AAA 서버)을 구성해야 합니다. 예를 들어 기본 인증 서버는 LDAP나 Active Directory 영역으로, 보조 인증은 RADIUS 서버로 설정할 수 있습니다.

참고 기본적으로 보조 인증이 필수가 아닙니다.

인증 서버 - VPN 사용자에게 보조 사용자 이름 및 암호를 제공하는 보조 인증 서버입니다.

보조 인증용 사용자 이름에서 다음을 선택하십시오.

- 프롬프트: VPN 게이트웨이에 로그인하는 동안 사용자에게 사용자 이름과 암호를 입력하라는 메시지를 표시합니다.
- 기본 인증 사용자 이름 사용: 사용자 이름은 기본 인증 서버와 2차 인증 모두에 대해 기본 인증 서버에서 가져옵니다. 두 개의 암호를 입력해야 합니다.
- 클라이언트 인증서의 사용자 이름 매핑: 클라이언트 인증서의 보조 사용자 이름을 미리 채웁니다.
  - **Map specific field(**특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN (Distinguished Name) as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다.

    기본 및 보조 필드 매핑에 대한 자세한 내용은 인증 방법 설명을 참조하십시오.
  - 인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기: AnyConnect VPN 클라이언트를 통해 사용자가 연결할 때 클라이언트 인증서에서 보조 사용자 이름을 미리 채웁니다.
    - 로그인 창에서 사용자 이름 숨기기: 보조 사용자 이름은 클라이언트 인증서에서 미리 채워지지만 미리 채워진 사용자 이름은 수정을 방지하기 위해 사용자에게 표시되지 않습니다.
- **VPN** 세션에 보조 사용자 이름 사용: 보조 사용자 이름은 VPN 세션 중에 사용자 활동을보고하는 데 사용됩니다.

단계 **5** **Authorization(**권한 부여**)**에 대해 다음을 선택합니다.

- **Authorization Server(**권한 부여 서버**)** - 인증이 완료되면 권한 부여 기능에서 인증된 각 사용자에게 사용할 수 있는 서비스 및 명령을 제어합니다. 권한 부여 기능은 사용자가 수행할 수 있도록 인가를 받은 것이 무엇인지, 즉 사용자의 실제 능력 및 제한 사항을 설명하는 일련의 속성을

결합함으로써 작동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게 동일한 액세스 권한을 제공합니다. 권한 부여에는 인증이 필요합니다.

원격 액세스 VPN 인증 작업 방식에 대한 자세한 내용은 권한 및 속성 정책 시행 이해, 1159 페이지의 내용을 참조하십시오.

연결 프로파일에서 사용자 인증을 위해 RADIUS 서버를 구성하면 Remote Access VPN 시스템 관리자는 사용자 또는 사용자 그룹에 대해 여러 권한 부여 속성을 구성할 수 있습니다. RADIUS 서버에 구성된 권한 부여 속성은 사용자 또는 사용자 그룹에 고유할 수 있습니다. 사용자가 인증되면 이러한 특정 권한 부여 속성이 Firepower Threat Defense 디바이스에 푸시됩니다.

참고 인증 서버에서 가져온 AAA 서버 속성은 그룹 정책 또는 연결 프로파일에서 이전에 구성되었을 속성 값보다 우선합니다.

- 필요한 경우 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택합니다.

  활성화된 경우 시스템은 클라이언트의 사용자 이름이 권한 부여 데이터베이스에 있어야 연결이 허용되는지 여부를 확인합니다. 사용자 이름이 권한 부여 데이터베이스에 존재하지 않으면 연결이 거부됩니다.

- 권한 부여 서버로 영역을 선택할 경우, LDAP 속성 맵을 설정해야 합니다. 인증 및 권한 부여를 위한 단일 서버 또는 다른 서버를 선택할 수 있습니다. **Configure LDAP Attribute Map(LDAP** 속성 맵 설정**)**을 클릭하여 권한 부여를 위한 LDAP 속성 맵을 추가합니다.

  참고 Firepower Threat Defense는 SAML ID 제공자를 권한 부여 서버로 지원하지 않습니다. FMC 및 FTD를 통해 SAML ID 제공자 뒤에 있는 Active Directory에 연결할 수 있는 경우, 다음 단계에 따라 권한 부여를 설정할 수 있습니다.

  - AD 서버용 영역을 추가합니다. 영역 생성, 2466 페이지의 내용을 참조하십시오.
  - 원격 액세스 VPN 연결 프로파일에서 권한 부여 서버로 영역 개체를 선택합니다.
  - 선택한 영역에 대한 LDAP 속성 맵을 설정합니다.

LDAP 속성 맵을 설정하는 방법은 LDAP 특성 매핑 구성, 1190 페이지의 내용을 참조하십시오.

단계 **6** **Accounting(**계정**)**에 대해 다음을 선택합니다.

- **Accounting Server(**과금 서버**)** - 계정은 사용자가 액세스하고 있는 서비스 및 사용 중인 네트워크 리소스의 양을 추적하는 데 사용됩니다. AAA 계정이 활성화되면 네트워크 액세스 서버는 사용자 활동을 RADIUS 서버에 보고합니다. 계정 관리 정보에는 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속 시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대해 이 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

  Remote Access VPN 세션을 설명하는 데 사용할 RADIUS 서버 그룹 개체를 지정합니다.

단계 **7** 다음 **Advanced Settings(**고급 설정**)**를 선택합니다.

- **Strip Realm from username(**사용자 이름에서 영역 제거**)** - AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 영역을 제거하려면 선택합니다. 예를 들어 이 옵션을 선택하고 사용자가 *domain\username*을 입력하는 경우, 도메인은 사용자 이름에서 제거되고 인증을 위해 AAA 서버로 전송됩니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.
- **Strip Group from username(**사용자 이름에서 그룹 제거**)** - AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 그룹 이름을 제거하려면 선택합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

  참고 영역은 관리 도메인입니다. 이러한 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구문 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.

- **Password Management(**암호 관리**)** - Remote Access VPN 사용자의 암호 관리를 활성화합니다. 암호 만료 전 또는 암호가 만료되는 날에 미리 알리려면 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

권한 및 속성 정책 시행 이해, 1159 페이지
영역 관리, 2479 페이지

RADIUS 서버 속성 Firepower Threat Defense

Firepower Threat Defense 디바이스는 Remote Access VPN 정책에서 인증 및/또는 권한 부여를 위해 구성된 외부 RADIUS 서버의 VPN 연결에 사용자 권한 속성(사용자 자격 또는 권한이라고도 함)을 적용하도록 지원합니다.

참고 Firepower Threat Defense 디바이스에서는 벤더 ID가 3076인 속성을 지원합니다.

다음 사용자 권한 부여 속성은 RADIUS 서버에서 Firepower Threat Defense 디바이스로 전송됩니다.

- RADIUS 속성 146 및 150은 인증 및 권한 부여 요청을 위해 Firepower Threat Defense 디바이스에서 RADIUS 서버로 전송됩니다.
- 세 개의 속성(146, 150, 151)은 모두 계정 관리 시작, 중간 업데이트, 중단 요청을 위해 Firepower Threat Defense 디바이스에서 RADIUS 서버로 전송됩니다.

표 ***82: Firepower Threat Defense***에서 ***RADIUS*** 서버로 전송되는 속성

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
연결 프로파일 이름 또는 터널 그룹 이름	146	문자열	단일	1자 ~ 253자

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
클라이언트 유형	150	정수	단일	2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2)
세션 유형	151	정수	단일	1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPsec VPN (IKEv2)

표 ***83: RADIUS*** 속성이 전송되는 대상***: Firepower Threat Defense***

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Access-List-Inbound	86	문자열	단일	두 Acess-List(액세스 목록) 속성 모두 FTD 디바이스에 구성된 ACL의 이름을 따릅니다. 스마트 CLI 확장 액세스 목록 개체 유형을 사용해 이 ACL을 생성합니다(**Device(**장치**)** > **Advanced Configuration(**고급 컨피그레이션**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)** 선택). 이 ACL에서는 인바운드(FTD 디바이스로 들어가는 트래픽) 또는 아웃바운드(FTD 디바이스에서 나가는 트래픽) 방향으로 트래픽 흐름을 제어합니다.
Access-List-Outbound	87	문자열	단일	
Address-Pools	217	문자열	단일	RA VPN에 접속하는 클라이언트에 대한 주소 풀로 사용될 서브넷을 식별하는 FTD 디바이스에 정의된 네트워크 개체의 이름입니다. **Objects(**개체**)** 페이지에서 네트워크 개체를 정의합니다.
Banner1	15	문자열	단일	사용자가 로그인하면 표시할 배너입니다.
Banner2	36	문자열	단일	사용자가 로그인하면 표시할 배너의 두 번째 부분입니다. 배너2는 배너1에 추가됩니다.
다운로드 가능한 ACL	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Cisco-AV-Pair 구성을 통해 지원됩니다.
필터 ACL	86, 87	문자열	단일	필터 ACL은 RADIUS 서버의 ACL 이름으로 참조됩니다. ACL 구성이 이미 Firepower Threat Defense 디바이스에 있어야 하므로 RADIUS 권한 부여 중에 ACL 구성을 사용할 수 있습니다. 86 = 액세스 목록-인바운드 87 = 액세스 목록-아웃 바운드

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Group-Policy	25	문자열	단일	연결에 사용할 그룹 정책입니다. RA VPN **Group Policy(**그룹 정책**)** 페이지에서 그룹 정책을 생성해야 합니다. 다음 형식 중 하나를 사용할 수 있습니다. • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	정수	단일	사용자가 설정하도록 허용되는 별도의 동시 연결 개수입니다(0~2147483647).
VLAN	140	정수	단일	사용자의 연결을 제한할 VLAN입니다(0~4094). 또한 FTD 디바이스의 하위 인터페이스에 이 VLAN을 컨피그레이션해야 합니다.

연결 프로파일에 대한 별칭 생성 또는 업데이트

별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. Remote Access VPN 관리자는 별칭 이름 및 별칭 URL을 활성화 또는 비활성화할 수 있습니다. VPN 사용자는 Firepower Threat Defense 디바이스에 연결하는 경우 별칭 이름을 선택할 수 있습니다. 이 디바이스에 구성된 모든 연결에서 별칭 이름 표시 기능은 켜거나 끌 수 있습니다. 또한 Remote Access VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 별칭 URL 목록을 구성할 수 있습니다. 사용자가 별칭 URL을 사용하여 연결하는 경우, 시스템에서는 이 URL과 일치하는 연결 프로파일을 자동으로 로깅합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Connection Profile(**연결 프로파일**)**을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **Aliases(**별칭**)**를 클릭합니다.

단계 **5** 별칭 이름을 추가하려면 다음을 수행합니다.

a) Alias Names(별칭 이름)에 **Add(**추가**)**를 클릭합니다.

b) **Alias Name(**별칭 이름**)**을 지정합니다.

c) 별칭을 활성화하려면 각 창에 있는 **Enabled(**활성화**)** 확인란을 선택합니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **6** 별칭 URL을 추가하려면 다음을 수행합니다.

a) Alias URLs(별칭 URL)에 **Add(**추가**)**를 클릭합니다.

b) 목록에서 **Alias URL(**별칭 **URL)**을 선택하거나 새 URL 개체를 생성합니다. 자세한 내용은 URL 개체 생성, 575 페이지를 참조하십시오.
c) 별칭을 활성화하려면 각 창에 있는 **Enabled(**활성화**)** 확인란을 선택합니다.
d) **OK(**확인**)**를 클릭합니다.

- **Edit(**편집**)**을 클릭하고 별칭 이름 또는 별칭 URL을 편집합니다.
- Alias name(별칭 이름) 또는 Alias URL(별칭 URL)을 삭제하려면 해당 행에 있는 **Delete(**삭제**)(**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 1173 페이지

Remote Access VPN을 위한 액세스 인터페이스 구성

Access Interface(액세스 인터페이스**)** 테이블에는 디바이스 인터페이스가 포함된 인터페이스 그룹과 보안 영역이 나열됩니다. 이는 Remote Access SSL 또는 IPsec IKEv2 VPN 연결을 위해 구성됩니다. 해당 테이블에는 각 인터페이스 그룹 또는 보안 영역의 이름, 인터페이스에서 사용하는 인터페이스 신뢰 지점 및 DTLS(Datagram Transport Layer Security)의 사용 여부가 표시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.
단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.
단계 **3** **Access Interface(**액세스 인터페이스**)**를 클릭합니다.
단계 **4** 액세스 인터페이스를 추가하려면 **Add(**추가**)**를 선택하고 **Add Access Interface(**액세스 인터페이스 추가**)** 창에서 다음에 대한 값을 지정합니다.

a) **Access Interface(**액세스 인터페이스**)** - 인터페이스가 속한 인터페이스 그룹 또는 보안 영역을 선택합니다.

인터페이스 그룹 또는 보안 영역은 라우팅 유형이어야 합니다. Remote Access VPN 연결에는 다른 인터페이스 유형이 지원되지 않습니다.

b) 다음 옵션을 선택하여 액세스 인터페이스와 프로토콜 개체를 연결합니다.

- **Enable IPSet-IKEv2(IPSet-IKEv2** 활성화**) - IKEv2** 설정을 활성화하려면 이 옵션을 선택합니다.
- **Enable SSL(SSL** 활성화**) - SSL** 설정을 활성화하려면 이 옵션을 선택합니다.
  - **Enable Datagram Transport Layer Security(Datagram Transport Layer Security** 활성화**)**를 선택합니다.

선택하면 인터페이스에서 DTLS(Datagram Transport Layer Security)를 활성화하며 SSL VPN 연결을 설정하는 AnyConnect VPN 클라이언트가 동시에 2개의 터널(SSL 터널 및 DTLS 터널)을 사용하도록 허용합니다.

DTLS를 활성화하면 특정 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다.

SSL 설정, TLS 및 DTLS 버전을 구성하려면 SSL 설정 정보, 1432 페이지의 내용을 참조하십시오.

AnyConnect VPN 클라이언트에 대한 SSL 설정을 구성하려면 그룹 정책 AnyConnect 옵션, 659 페이지의 내용을 참조하십시오.

- **Configure Interface Specific Identity Certificate(**인터페이스별 **ID** 인증서 구성**)** 확인란을 선택하고 드롭다운 목록에서 **Interface Identity Certificate(**인터페이스 **ID** 인증서**)**를 선택합니다.

  인터페이스 ID 인증서를 선택하지 않는 경우 **Trustpoint(**신뢰 지점**)**가 기본적으로 사용됩니다.

  인터페이스 ID 인증서 또는 신뢰 지점을 선택하지 않는 경우 **SSL Global Identity Certificate(SSL** 전역 **ID** 인증서**)**가 기본적으로 사용됩니다.

c) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **5** **Access Settings(**액세스 설정**)**에서 다음을 선택합니다.

- **Allow Users to select connection profile while logging in(**사용자가 로그인 상태에서 연결 프로파일을 선택할 수 있음**)** - 여러 연결 프로파일이 있는 경우 이 옵션을 선택하면 사용자가 로그인 중에 올바른 연결 프로파일을 선택할 수 있습니다. **IPsec IKEv2** VPN에 대해 이 옵션을 선택해야 합니다.

단계 **6** **SSL Settings(SSL** 설정**)**를 구성하려면 다음 옵션을 사용합니다.

- **Web Access Port Number(**웹 액세스 포트 번호**)** - VPN 세션에 사용할 포트입니다. 기본 포트는 443입니다.
- **DTLS Port Number(DTLS** 포트 번호**)** - DTLS 연결에 대해 사용할 UDP 포트입니다. 기본 포트는 443입니다.
- **SSL Global Identity Certificate(SSL** 전역 **ID** 인증서**)** - **Interface Specific Identity Certificate(**인터페이스별 **ID** 인증서**)**가 제공되지 않으면 선택한 **SSL Global Identity Certificate(SSL** 전역 **ID** 인증서**)**가 모든 관련 인터페이스에 사용됩니다.

단계 **7** **IPsec-IKEv2 Settings(IPsec IKEv2** 설정**)**에서 목록의 **IKEv2 Identity Certificate(IKEv2 ID** 인증서**)**를 선택하거나 ID 인증서를 추가합니다.

단계 **8** **Save(**저장**)**를 클릭하여 액세스 인터페이스 변경 사항을 저장합니다.

관련 항목

보안 영역, 577 페이지

Remote Access VPN 고급 옵션 설정

Cisco AnyConnect Secure Mobility Client 이미지

Cisco AnyConnect Secure Mobility Client 이미지

Cisco AnyConnect Secure Mobility Client는 기업 리소스에 대한 전체 VPN 프로파일링을 통해 원격 사용자에게 Firepower Threat Defense 디바이스에 대한 SSL 또는 IPsec(IKEv2) 연결을 제공합니다. 이전에 설치된 클라이언트가 없는 경우 원격 사용자는 브라우저에서 클라이언트리스 VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력하여 AnyConnect 클라이언트를 다운로드하고 설치합니다. Firepower Threat Defense 디바이스는 원격 컴퓨터의 운영 체제와 일치하는 클라이언트를 다운로드합니다. 다운로드한 후 클라이언트는 보안 연결을 설치하고 설정합니다. 클라이언트를 이미 설치한 경우 사용자가 인증을 통과하면 Firepower Threat Defense 디바이스에서 클라이언트의 버전을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.

Remote Access VPN 관리자는 새 AnyConnect 클라이언트 이미지 또는 추가 이미지를 VPN 정책에 연결합니다. 관리자 지원되지 않거나 단종되었으며 더 이상 필요하지 않은 클라이언트 패키지의 연결을 해제할 수 있습니다.

Firepower Management Center에서는 파일 패키지 이름을 사용하여 운영 체제의 유형을 결정합니다. 사용자가 운영 체제 정보를 나타내지 않고 파일의 이름을 바꾼 경우 유효한 운영 체제 유형을 목록 상자에서 선택해야 합니다.

AnyConnect 클라이언트 이미지 파일을 Cisco 소프트웨어 다운로드 센터에서 다운로드합니다.

관련 항목

Cisco AnyConnect Mobility Client 이미지 추가: Firepower Management Center, 1186 페이지

Cisco AnyConnect Mobility Client 이미지 추가: Firepower Management Center

AnyConnect File 개체를 사용하여 Cisco AnyConnect Mobility Client 이미지를 Firepower Management Center에 업로드할 수 있습니다. 자세한 내용은 FTD 파일 개체, 663 페이지를 참고하십시오. 클라이언트 이미지에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility Client 이미지, 1186 페이지 섹션을 참조하십시오.

Show re-order(순서 재구성 표시**)** 링크를 클릭하여 특정 클라이언트 이미지를 확인합니다.

참고 이미 설치된 Cisco AnyConnect 클라이언트 이미지를 삭제하려면 해당 행의 **Delete(**삭제**)**를 클릭합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**) > VPN > Remote Access(**원격 액세스**)**, 나열된 RA VPN 정책을 선택한 다음 **Advanced(**고급**)** 탭을 선택합니다.를 선택합니다.

단계 2 **AnyConnect Images(AnyConnect** 이미지**)** 대화 상자의 **Available AnyConnect Images(**사용 가능한 **AnyConnect** 이미지**)** 부분에서 **Add(**추가**)**를 클릭합니다.

단계 3 사용 가능한 AnyConnect 이미지의 이름, 파일 이름 및 설명을 입력합니다.

단계 4 **Browse(**찾아보기**)**를 클릭하여 업로드할 클라이언트 이미지를 선택할 위치로 이동합니다.

단계 5 Firepower Management Center에서 **Save(**저장**)**를 클릭하여 이미지를 업로드합니다.

Firepower Management Center에 클라이언트 이미지를 업로드하면 운영 체제는 Firepower Management Center에 업로드한 이미지에 대한 플랫폼 정보를 표시합니다.

관련 항목

Cisco AnyConnect Secure Mobility Client 이미지, 1186 페이지

Remote Access VPN 클라이언트에 대한 AnyConnect 이미지 업데이트

Cisco AnyConnect 클라이언트 업데이트가 Cisco 소프트웨어 다운로드 센터에서 제공되면 패키지를 수동으로 다운로드하여 VPN 정책에 추가할 수 있으며, 이에 따라 새 AnyConnect 패키지가 운영 체제에 따라 VPN 클라이언트 시스템에서 업그레이드되도록 할 수 있습니다.

시작하기 전에

이 섹션의 지침은 새 AnyConnect 클라이언트 이미지를 Firepower Threat Defense VPN 게이트웨이에 연결하는 Remote Access VPN 클라이언트로 업데이트하는 데 도움이 됩니다. AnyConnect 이미지를 업데이트하기 전에 다음 구성이 완료되었는지 확인합니다.

- AnyConnect 이미지 파일을 Cisco 소프트웨어 다운로드 센터에서 다운로드하십시오.
- Firepower Management Center 웹 인터페이스에서 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**로 이동하고 새 AnyConnect 클라이언트 이미지 파일을 추가합니다.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 목록에서 기존 원격 액세스 정책을 선택하고 해당 **Edit(**편집**)**을 클릭합니다.

단계 3 **Advanced(**고급**)** > **AnyConnect Client Image(AnyConnect** 클라이언트 이미지**)** > **Add(**추가**)**를 클릭합니다.

단계 4 **Available AnyConnect Images(**사용 가능한 **AnyConnect** 이미지**)**에서 클라이언트 이미지 파일을 선택하고 **Add(**추가**)**를 클릭합니다.

필요한 AnyConnect 클라이언트 이미지가 목록에 없는 경우, **Add(**추가**)**를 클릭하여 이미지를 찾아 업로드합니다.

단계 5 Remote Access VPN 정책을 저장합니다.

Remote Access VPN 정책 변경 사항이 구축되면 Remote Access VPN 게이트웨이로 구성된 Firepower Threat Defense 디바이스에서 새 AnyConnect 클라이언트 이미지가 업데이트됩니다. 새로운 VPN 사용자가 VPN 게이트웨이에 연결하면 사용자는 클라이언트 시스템의 운영 체제에 따라 새로운 AnyConnect 클라이언트 이미지를 다운로드합니다. 기존 VPN 사용자의 경우 다음 VPN 세션에서 AnyConnect 클라이언트 이미지가 업데이트됩니다.

관련 항목

Remote Access VPN 연결 프로파일 옵션

Remote Access VPN 주소 할당 정책

Firepower Threat Defense 디바이스는 IPv4 또는 IPv6 정책을 사용하여 Remote Access VPN 클라이언트에 IP 주소를 할당할 수 있습니다. 둘 이상의 주소 할당 방법을 구성한 경우에는 Firepower Threat Defense 디바이스에서 IP 주소를 찾을 때까지 각 옵션을 검색합니다.

IPv4 또는 **IPv6** 정책

IPv4 또는 IPv6 정책을 사용하여 Remote Access VPN 클라이언트의 IP 주소를 지정할 수 있습니다. 먼저 IPv4 정책을 시도한 다음 나중에 IPv6 정책을 시도해야 합니다.

- **Use Authorization Server(**인증 서버 사용**)** - 외부 권한 부여 서버에서 사용자별로 주소를 검색합니다. IP 주소가 구성된 권한 부여 서버를 사용하는 경우 이 방법을 사용하는 것이 좋습니다. 주소 할당은 RADIUS 기반 인증 서버에서만 지원됩니다. AD/LDAP에는 지원되지 않습니다. IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.
- **Use DHCP(DHCP** 사용**)** - 연결 프로파일에 구성된 DHCP 서버에서 IP 주소를 가져옵니다. 또한 그룹 정책에서 DHCP 네트워크 범위를 구성하여 DHCP 서버가 사용할 수 있는 IP 주소 범위를 정의할 수도 있습니다. DHCP를 사용하는 경우 **Objects(**개체**)> Object Management(**개체 관리**)> Network(**네트워크**)** 창에서 서버를 구성합니다. IPv4 할당 정책에 이 방법을 사용할 수 있습니다.

  DHCP 네트워크 범위 설정에 대한 자세한 내용은 그룹 정책 일반 옵션, 657 페이지의 내용을 참조하십시오.
- **Use an internal address pool(**내부 주소 풀 사용**)** - 내부적으로 구성된 주소 풀은 주소 풀 할당을 구성하는 가장 간편한 방법입니다. 이 방법을 사용하는 경우 **Objects(**개체**) > Object Management(**개체 관리**) > Address Pools(**주소 풀**)** 창에서 IP 주소 풀을 만들고 연결 프로파일에서 선택합니다. IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.
- **Reuse an IP address so many minutes after it is released(**릴리스된 후 **IP** 주소 다시 사용**)** - IP 주소가 주소 풀로 반환된 이후에 해당 IP 주소의 재사용을 지연시킵니다. 지연을 추가하면 IP 주소가 신속하게 재할당될 경우 방화벽에서 발생할 수 있는 문제를 방지하는 데 도움이 됩니다. 기본적으로 지연은 0으로 설정됩니다. 즉, Firepower Threat Defense 디바이스가 IP 주소 재사용에 지연을 적용하지 않는다는 의미입니다. 지연을 확장하려면 해당 상자를 선택하고 0분부터 480분의 범위에서 IP 주소 재할당을 지연시킬 기간(분)을 입력합니다. 이 구성 요소는 IPv4 할당 정책에 사용할 수 있습니다.

관련 항목

연결 프로파일 설정, 1173 페이지

Remote Access VPN 인증, 1158 페이지

인증서 맵 구성

인증서 맵을 사용하면 인증서 필드의 내용을 기반으로 사용자 인증서와 연결 프로파일을 일치시키는 규칙을 정의할 수 있습니다. 인증서 맵은 보안 게이트웨이의 인증서 인증에 사용됩니다.

규칙 또는 인증서 맵은 FTD 인증서 맵 개체, 665 페이지에서 정의됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Advanced(**고급**)** > **Certificate Maps(**인증서 맵**)**를 클릭합니다.

단계 **4** **General Settings for Certificate Group Matching(**인증서 그룹 일치에 대한 일반 설정**)** 창에서 다음 옵션을 선택합니다.

선택 사항은 우선 순위 기반이며 첫 번째 선택 항목과 일치하는 항목이 없는 경우 일치하는 옵션 목록이 계속됩니다. 규칙을 모두 충족할 때 매핑이 수행됩니다. 규칙이 충족되지 않으면 기본 연결 프로파일(하단에 나열됨)이 이 연결에 사용됩니다. 다음 옵션 중 일부 또는 전부를 선택하여 인증을 설정하고 클라이언트에 매핑되어야 하는 연결 프로파일(터널 그룹)을 결정합니다.

- 그룹 **URL**과 인증서 맵이 서로 다른 연결 프로파일과 일치하는 경우 그룹 **URL** 사용
- **Use the configured rules to match a certificate to a Connection Profile(**구성된 규칙을 사용하여 연결 프로파일에 인증서 일치**)** - 연결 프로파일 맵에서 여기에 정의된 규칙을 사용하도록 활성화합니다.

참고 인증서 매핑을 구성하는 작업은 인증서 기반 인증을 의미합니다. 원격 사용자에게는 구성된 인증 방법과 상관없이 클라이언트 인증서를 요구하는 메시지가 표시됩니다.

단계 **5** **Certificate to Connection Profile Mapping(**연결 프로파일에 인증서 매핑**)** 섹션에서 **Add Mapping(**매핑 추가**)**를 클릭하여 이 정책에 대한 연결 프로파일 매핑 인증서를 생성합니다.

a) **Certificate Map(**인증서 맵**)** 개체를 선택하거나 생성합니다.

b) 인증서 맵 개체의 규칙이 충족될 경우 사용해야 하는 **Connection Profile(**연결 프로파일**)**을 선택합니다.

c) 매핑을 생성하려면 **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

그룹 정책 구성

그룹 정책은 원격 액세스 VPN 경험을 정의하는 그룹 정책 개체가 저장된 속성 및 값 쌍의 집합입니다. 예를 들어 그룹 정책 개체에서는 주소, 프로토콜, 연결 설정 등 일반 속성을 구성합니다.

VPN 터널이 설정된 경우 사용자에게 적용되는 그룹 정책이 결정됩니다. RADIUS 권한 서버는 그룹 정책을 할당하거나 현재 연결 프로파일에서 그룹 정책을 가져옵니다.

참고 FTD에 그룹 정책 속성 상속이 없습니다. 그룹 정책 개체 전체가 사용자에 대해 사용됩니다. 로그인 시 AAA 서버에서 식별된 그룹 정책 개체가 사용됩니다. 이를 지정하지 않은 경우, VPN 연결을 위해 구성된 기본 그룹 정책이 사용됩니다. 제공된 기본 그룹 정책은 기본값으로 설정할 수 있으나, 해당 정책이 연결 프로파일에 할당되어 있고 사용자의 다른 그룹 정책이 식별되지 않은 경우에만 사용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Advanced(**고급**)** > **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 **4** 이 원격 액세스 VPN 정책과 연결할 하나 이상의 그룹 정책을 선택합니다. 원격 액세스 VPN 정책 생성에서 할당된 기본 그룹 정책보다 더 많습니다. **Add(**추가**)**를 클릭합니다.

Refresh(새로 고침**)** 및 **Search(**검색**)** 유틸리티를 사용하여 그룹 정책을 찾습니다. 필요하다면 새 그룹 정책 개체를 추가합니다.

단계 **5** 사용 가능한 그룹 정책에서 그룹 정책을 선택하고 **Add(**추가**)**를 클릭하여 선택합니다.

단계 **6** **OK (**확인**)**를 클릭하여 그룹 정책 선택을 완료합니다.

관련 항목

그룹 정책 개체 설정, 656 페이지

LDAP 특성 매핑 구성

LDAP 속성 이름은 LDAP 사용자 또는 그룹 속성 이름을 Cisco에서 이해할 수 있는 이름에 매핑합니다. 속성 맵은 AD(Active Directory) 또는 LDAP 서버에 있는 속성을 Cisco 속성 이름과 동일시합니다. 모든 표준 LDAP 속성은 잘 알려진 벤더별 속성(VSA)에 매핑할 수 있습니다. 하나 이상의 LDAP 속성을 하나 이상의 Cisco LDAP 속성에 매핑할 수 있습니다. 원격 액세스 VPN 연결을 설정하는 동안 AD 또는 LDAP 서버에서 FTD 디바이스에 인증을 반환하면 FTD 디바이스에서 이 정보를 사용하여 AnyConnect 클라이언트가 연결을 완료하는 방법을 조정할 수 있습니다.

VPN 사용자에게 다른 액세스 권한 또는 VPN 콘텐츠를 제공하려는 경우 VPN 서버에서 서로 다른 VPN 정책을 설정하고 인증서를 기준으로 각 사용자에게 이러한 정책 집합을 할당할 수 있습니다. LDAP 특성 맵을 사용하여 LDAP 권한 부여를 설정하여 FTD에서 이를 수행할 수 있습니다. LDAP를 사용하여 사용자에게 그룹 정책을 할당하려면 AD(Active Directory) 특성 **memberOf**와 같은 LDAP 특성을 VPN 헤드 엔드에서 인식하는 **VPN-Group** 속성에 매핑하는 맵을 설정해야 합니다.

LDAP 특성 맵은 세 가지 구성 요소로 이루어집니다.

- **Name(**이름**)**-LDAP 속성 맵의 이름을 지정합니다. 선택한 영역을 기반으로 이름이 생성됩니다.

- **Attribute Name Mapping(**속성 이름 매핑**)** - LDAP 사용자 또는 그룹 속성 이름을 Cisco에서 이해할 수 있는 이름에 매핑합니다.
- **Attribute Value Mapping(**속성 값 매핑**)** - LDAP 사용자 또는 그룹 속성의 값을 선택한 이름 매핑에 대한 Cisco 속성의 값에 매핑합니다.

사용자가 FTD 원격 액세스 VPN에 연결할 때 **memberOf** 필드가 설정된 값과 일치하는 경우 그룹 정책 **VPN-Group**이 사용자의 VPN 세션에 적용됩니다.

LDAP 특성 맵에 사용된 그룹 정책은 원격 액세스 VPN 설정의 그룹 정책 목록에 추가됩니다. 원격 액세스 VPN 설정에서 그룹 정책이 제거되면 연결된 LDAP 특성 매핑도 제거됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 목록에서 기존 원격 액세스 VPN 정책을 선택하고 해당 **Edit(**편집**)** 아이콘을 클릭합니다.

단계 **3** **Advanced(**고급**)** > **LDAP Attribute Mapping(LDAP** 특성 매핑**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** Configure LDAP Attribute Map(LDAP 특성 맵 설정) 페이지에서 속성 맵을 설정할 영역을 선택합니다.

LDAP 특성 맵의 이름은 선택한 영역을 기반으로 생성됩니다. 영역을 변경하면 LDAP 특성 이름도 변경됩니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

여러 속성 맵을 설정할 수 있습니다. 각 속성 맵에서는 이름 맵 및 값 맵을 구성해야 합니다.

참고 LDAP 특성 맵을 생성할 때 다음 지침을 따르십시오.

- LDAP 특성에 대해 하나의 매핑을 설정해야 합니다. 동일한 LDAP 특성 이름의 여러 매핑은 허용되지 않습니다.
- LDAP 특성 맵을 생성하려면 하나 이상의 이름 맵을 설정해야 합니다.
- 속성 맵이 원격 액세스 VPN 설정의 연결 프로파일과 연결되지 않은 경우 LDAP 특성 맵을 제거합니다.
- Cisco 및 LDAP 특성 이름과 값 모두에 대해 LDAP 특성 맵에서 올바른 철자와 대문자를 사용합니다.

a) **LDAP** 특성 이름을 지정한 다음 목록에서 필요한 **Cisco** 속성 이름을 선택합니다.

b) **Add Value Map(**값 맵 추가**)**을 클릭하고 **LDAP Attribute Value(LDAP** 특성 값**)** 및 **Cisco Attribute Value(Cisco** 속성 값**)**를 지정합니다.

값 맵을 더 추가하려면 이 단계를 반복합니다.

각각의 **Delete(**삭제**)** 아이콘을 클릭하여 LDAP 특성 맵, 이름 맵 또는 값 맵을 삭제할 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭하여 LDAP 특성 맵 설정을 완료합니다.

단계 8 LDAP 특성 매핑에 변경 사항을 저장하려면 **Save(**저장**)**를 클릭합니다.

관련 항목

Remote Access VPN에 대한 AAA 설정, 1177 페이지
권한 및 속성 정책 시행 이해, 1159 페이지

Remote Access VPN에 대한 IPsec 설정 구성

IPsec 설정은 Remote Access VPN 정책을 구성하는 동안 VPN 프로토콜로 IPsec을 선택한 경우에만 적용할 수 있습니다. 그렇지 않은 경우 Edit Access Interface(액세스 인터페이스 편집) 대화 상자를 사용하여 IKEv2를 활성화할 수 있습니다. 자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 1184 페이지를 참조하십시오.

프로시저

단계 1 **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 2 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 3 **Advanced(**고급**)**를 클릭합니다.

IPsec 설정 목록이 화면 왼쪽의 탐색창에 나타납니다.

단계 4 탐색창을 사용하여 다음 IPsec 옵션을 편집합니다.

a) **Crypto Maps(**암호화 맵**)** - Crypto Maps(암호화 맵) 페이지는 IKEv2 프로토콜이 활성화된 인터페이스 그룹을 나열합니다. 암호화 맵은 IKEv2 프로토콜이 활성화된 인터페이스에 대해 자동으로 생성됩니다. 암호화 맵을 편집하려면 Remote Access VPN 암호화 맵 설정, 1192 페이지 섹션을 참조하십시오. **Access Interface(**액세스 인터페이스**)**에서 선택한 VPN 정책에 인터페이스 그룹을 추가하거나 제거할 수 있습니다. 자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 1184 페이지를 참조하십시오.

b) **IKE Policy(IKE** 정책**)** - IKE Policy(IKE 정책) 페이지에는 AnyConnect 엔드포인트가 IPsec 프로토콜을 사용하여 연결할 때 선택된 VPN 정책에 적용할 수 있는 모든 IKE 정책 개체가 나열됩니다. 자세한 내용은 Remote Access VPN의 IKE 정책, 1195 페이지를 참조하십시오. 새 IKE 정책을 추가하려면 IKEv2 정책 개체 구성 , 652 페이지 섹션을 참조하십시오. FTD에서는 AnyConnect IKEv2 클라이언트만 지원합니다. 타사 표준 IKEv2 클라이언트는 지원되지 않습니다.

c) **IPsec/IKEv2 Parameters(IPsec/IKEv2** 파라미터**)** - IPsec/IKEv2 Parameters(IPsec/IKEv2 파라미터) 페이지에서 IKEv2 세션 설정, IKEv2 보안 연결 설정, IPsec 설정 및 NAT Transparency 설정을 수정할 수 있습니다. 자세한 내용은 Remote Access VPN IPsec/IKEv2 파라미터 구성, 1196 페이지를 참조하십시오.

단계 5 **Save(**저장**)**를 클릭합니다.

Remote Access VPN 암호화 맵 설정

암호화 맵은 IPsec-IKEv2 프로토콜이 활성화된 인터페이스에 대해 자동으로 생성됩니다. **Access Interface(**액세스 인터페이스**)**에서 선택한 VPN 정책에 인터페이스 그룹을 추가하거나 제거할 수 있

습니다. 자세한 내용은 Remote Access VPN을 위한 액세스 인터페이스 구성, 1184 페이지를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Advanced(**고급**)** > **Crypto Maps(**암호화 맵**)**를 클릭하고 테이블에서 행을 선택하고 **Edit(**편집**)**을 클릭하여 암호화 맵 옵션을 편집합니다.

단계 **4** **IKEv2 IPsec Proposals(IKEv2 IPsec** 제안**)**를 선택하고 터널에서 트래픽을 보호하는 데 사용할 인증 및 암호화 알고리즘을 지정하는 변환 집합을 선택합니다.

단계 **5** **Enable Reverse Route Injection(Reverse Route Injection** 활성화**)**을 선택하여 원격 터널 엔드포인트로 보호되는 네트워크 및 호스트에 대한 라우팅 프로세스에 정적 경로를 자동으로 삽입할 수 있도록 활성화합니다.

단계 **6** **Enable Client Services(**클라이언트 서비스 활성화**)**를 선택하고 포트 번호를 지정합니다.

Client Services Server는 AnyConnect Downloader가 AnyConnect 클라이언트가 요구하는 소프트웨어 업그레이드, 프로파일, 지역화 및 사용자 정의 파일, CSD, SCEP 및 기타 파일 다운로드를 수신할 수 있도록 HTTPS(SSL) 액세스를 제공합니다. 이 옵션을 선택하는 경우 클라이언트 서비스 포트 번호를 지정합니다. Client Services Server를 활성화하지 않으면 사용자가 AnyConnect 클라이언트에 필요할 수있는 파일을 다운로드할 수 없습니다.

참고 동일한 디바이스에서 실행 중인 SSL VPN에 사용하는 것과 동일한 포트를 사용할 수 있습니다. SSL VPN이 구성되어 있는 경우에도 IPsec-IKEv2 클라이언트에 대해 SSL을 통한 파일 다운로드를 활성화하려면 이 옵션을 선택해야 합니다.

단계 **7** **Enable Perfect Forward Secrecy(Perfect Forward Secrecy** 활성화**)**를 선택하고 **Modulus group(**모듈러스 그룹**)**을 선택합니다.

PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. 이 옵션을 선택하는 경우 **Modulus Group(**모듈러스 그룹**)** 목록에서 PFS 세션 키를 생성할 때 사용할 Diffie-Hellman 키 파생 알고리즘도 선택합니다.

모듈러스 그룹은 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. Remote Access VPN 구성에서 허용할 모듈러스 그룹을 선택합니다.

- 1 - Diffie-Hellman 그룹 1(768비트 모듈러스).
- 2 - Diffie-Hellman 그룹 2(1024비트 모듈러스).
- 5 - Diffie-Hellman 그룹 5(1536비트 모듈러스, 128비트 키에 적합한 보호를 제공하지만 14 그룹이 더 효과적임). AES 암호화를 사용하는 경우 이 그룹(또는 그 이상)을 사용하십시오.

- 14 - Diffie-Hellman 그룹 14(2048비트 모듈러스, 128비트 키에 적합한 보호를 제공함).
- 19 - Diffie-Hellman 그룹 19(256비트 엘립틱 커브 필드 크기).
- 20 - Diffie-Hellman 그룹 20(384비트 엘립틱 커브 필드 크기).
- 21 - Diffie-Hellman 그룹 21(521비트 엘립틱 커브 필드 크기).
- 24 - Diffie-Hellman 그룹 24(2048비트 모듈러스 및 256비트 소수 위수 하위 그룹).

단계 **8** 라이프타임 기간**(**초**)**을 지정합니다.

보안 연결(SA)의 라이프타임(초)입니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다.

120~2147483647초 사이의 값을 지정할 수 있습니다. 기본값은 28800초입니다.

단계 **9** **Lifetime Size (kbytes)(**라이프타임 크기**(kbyte))**를 지정합니다.

만료되기 전에 지정된 보안 연결을 사용하여 IPsec 피어 간에 전달할 수 있는 트래픽 볼륨(KB)입니다.

10~2147483647kbyte 사이의 값을 지정할 수 있습니다. 기본값은 4,608,000킬로바이트입니다. 무제한 데이터를 허용하는 사양은 없습니다.

단계 **10** 다음 **ESPv3 Settings(ESPv3** 설정**)**를 선택합니다.

- **Validate incoming ICMP error messages(**들어오는 **ICMP** 오류 메시지 확인**)** - IPsec 터널을 통해 수신되고 비공개 네트워크의 내부 호스트로 전달되는 이러한 ICMP 오류 메시지를 검증할지 여부를 선택합니다.
- **Enable 'Do Not Fragment' Policy('**조각화 금지' 정책 활성화**)** - IPsec 하위 시스템에서 IP 헤더에 DF(Do Not Fragment) 비트가 설정된 대용량 패킷을 처리하는 방법을 정의하고 **Policy(**정책**)** 목록에서 다음 중 하나를 선택합니다.
  - Copy(복사) - DF 비트를 유지합니다.
  - Clear(지우기) - DF 비트를 무시합니다.
  - Set(설정) - DF 비트를 설정하고 사용합니다.
- Enable Traffic Flow Confidentiality (TFC) packets(TFC(Traffic Flow Confidentiality) 선택 - 패킷 활성화) - 터널을 우회하는 트래픽 프로파일을 마스킹하는 더미 TFC 패킷을 활성화합니다. **Burst(**버스트**)**, **Payload Size(**페이로드 크기**)** 및 **Timeout(**시간 초과**)** 파라미터를 사용하여 지정된 SA에서 무작위 간격으로 임의 길이의 패킷을 생성할 수 있습니다.
  - Burst(버스트) - 1~16 바이트 사이의 값을 지정합니다.
  - Payload Size(페이로드 크기) - 64~1024 바이트의 값을 지정합니다.
  - Timeout(시간 초과) - 10~ 60초 사이의 값을 지정합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

관련 항목

보안 영역, 577 페이지

Remote Access VPN의 IKE 정책

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다. IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

참고 FTD Remote Access VPN용 IKEv2만 지원합니다.

IKEv1과는 달리 IKEv2 제안의 경우, 한 그룹에서 여러 알고리즘과 모듈러스 그룹을 선택할 수 있습니다. 피어가 1단계 협상 중에 선택하기 때문에 단일 IKE 제안을 생성할 수 있도록 하지만 가장 원하는 옵션에 더 높은 우선 순위를 부여하는 여러 다른 제안을 고려하십시오. IKEv2의 경우 정책 개체가 인증을 지정하지 않으면 다른 정책이 인증 요건을 정의해야 합니다.

IKE 정책은 원격 액세스 IPsec VPN을 구성할 때 필요 합니다.

Remote Access VPN IKE 정책 구성

IKE 정책 테이블은 AnyConnect 엔드포인트가 IPsec 프로토콜을 사용하여 연결할 때 선택된 VPN 구성에 적용할 수 있는 모든 IKE 정책 개체를 지정합니다. 자세한 내용은 Remote Access VPN의 IKE 정책, 1195 페이지를 참고하십시오.

참고 FTD Remote Access VPN용 IKEv2만 지원합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Advanced(**고급**)** > **IKE Policy(IKE** 정책**)**를 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭하여 사용 가능한 IKEv2 정책 중에서 선택하거나 새 IKEv2 정책을 추가하고 다음을 지정합니다.

- **Name(**이름**)** - IKEv2 정책의 이름입니다.
- **Description(**설명**)** - IKEv2 정책에 대한 설명(선택 사항)입니다.

- **Priority(**우선 순위**)** - 우선 순위 값에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다.
- **Lifetime** - 보안 연결(SA)의 라이프타임(초)입니다.
- **Integrity(**무결성**)** - IKEv2 정책에 사용되는 해시 알고리즘의 무결성 알고리즘 부분입니다.
- **Encryption(**암호화**)** - 2단계 협상 보호를 위한 1단계 SA를 설정하는 데 사용되는 암호화 알고리즘입니다.
- **PRF Hash(PRF** 해시**)** - IKE 정책에 사용되는 해시 알고리즘의 의사 난수 함수(PRF) 부분입니다. IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다.
- **DH** 그룹— 암호화에 사용 되는 Diffie-hellman 그룹.

단계 **5** **Save(**저장**)**를 클릭합니다.

관련 항목

Remote Access VPN 액세스 인터페이스 옵션

Remote Access VPN IPsec/IKEv2 파라미터 구성

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** 사용 가능한 VPN 정책 목록에서 설정을 수정하려는 정책을 선택합니다.

단계 **3** **Advanced(**고급**)** > **IPsec**> **IPsec/IKEv2 Parameters(IPsec/IKEv2** 파라미터**)**를 클릭합니다.

단계 **4** **IKEv2 Session Settings(IKEv2** 세션 설정**)**에 대해 다음을 선택합니다.

- **Identity Sent to Peer(**피어로 전송되는 **ID)** - IKE 협상 중에 피어가 자신을 식별하는 데 사용할 ID를 선택합니다.
  - **Auto(**자동**)** - 연결 유형에 따라 IKE 협상을 결정합니다. 예: 사전 공유 키의 IP 주소 또는 인증서 인증의 Cert DN(지원하지 않음)
  - **IP address(IP** 주소**)** - ISAKMP ID 정보를 교환하는 호스트의 IP 주소를 사용합니다.
  - **Hostname(**호스트 이름**)** - ISAKMP ID 정보를 교환하는 호스트의 FQDN(Fully Qualified Domain Name)을 사용합니다. 이 이름은 호스트 이름 및 도메인 이름으로 구성됩니다.
- **Enable Notification on Tunnel Disconnect(**터널 연결 해제 알림 활성화**)** - SA에서 수신한 인바운드 패킷이 해당 SA의 트래픽 선택기와 일치하지 않는 경우, 관리자가IKE 알림 피어 전송을 활성화 또는 비활성화할 수 있습니다. 이 알림의 전송은 기본적으로 비활성화되어 있습니다.
- **Do not allow device reboot until all sessions are terminated(**모든 세션이 종료될 때까지 디바이스 재부팅 허용 안 함**)** - 시스템 재부팅 전에 모든 활성 세션이 자발적으로 종료될 때까지 대기 활성화를 선택합니다. 기본적으로 비활성화되어 있습니다.

단계 **5** **IKEv2 Security Association (SA) Settings(IKEv2** 보안 연결**(SA)** 설정**)**에 대해 다음을 선택합니다.

- **Cookie Challenge(**쿠키 챌린지**)** - SA 개시 패킷에 대한 응답으로 쿠키 챌린지를 피어 디바이스로 전송할지 여부. 이는 Dos(서비스 거부) 공격 차단에 도움이 됩니다. 기본적으로 사용 가능한 SA의 50%가 협상중인 경우 쿠키 챌린지를 사용합니다. 다음 옵션 중 하나를 선택합니다.
  - **Custom(**사용자 정의**)** - 협상 중인 허용 SA 합계의 백분율인 수신 쿠키 챌린지 임계값을 지정합니다. 이렇게 하면 이후의 모든 SA 협상에 대해 쿠키 챌린지가 트리거됩니다. 범위는 0~100%이고, 기본값은 50%입니다.
  - Always(항상) - 항상 피어 디바이스에 쿠키 챌린지를 보내려면 선택합니다.
  - Never(안 함) - 피어 디바이스에 쿠키 챌린지를 보내지 않으려면 선택합니다.
-
- **Number of SAs Allowed in Negotiation(**협상에서 허용되는 **SA** 수**)** - 언제든지 협상에 참여할 수 있는 최대 SA 수를 제한합니다. Cookie Challenge(쿠키 챌린지)와 함께 사용하는 경우 효과적인 교차 확인을 위해 쿠키 챌린지 임계값을 이 한도보다 낮은 값으로 구성합니다. 기본값은 100%입니다.
- **Maximum number of SAs Allowed(**허용되는 최대 **SA** 수**)** - 허용되는 IKEv2 연결 수를 제한합니다.

단계 **6** **IPsec Settings(IPsec** 설정**)**에 대해 다음을 선택합니다.

- **Enable Fragmentation Before Encryption(**암호화 이전 단편화 활성화**)** - 이 옵션을 사용하면 트래픽이 IP 단편화를 지원하지 않는 NAT 디바이스를 통과할 수 있습니다. IP 단편화를 지원하는 NAT 디바이스의 작동을 방해하지 않습니다.
- **Path Maximum Transmission Unit Aging(**경로 최대 전송 단위 에이징**)** - SA(Security Association)의 PMTU(Path Maximum Transmission Unit) 재설정 간격인 PMTU Aging 활성화를 선택합니다.
- **Value Reset Interval(**값 재설정 간격**)** - SA(Security Association)의 PMTU 값이 원래 값으로 재설정되는 시간(분)을 입력합니다. 유효 범위는 10~30분이며, 기본값은 무제한입니다.

단계 **7** **NAT Settings(NAT** 설정**)**에 대해 다음을 선택합니다.

- **Keepalive Messages Traversal(Keepalive** 메시지 순회**)** - NAT keepalive 메시지 순회 활성화 여부를 선택합니다. NAT 순회 킵얼라이브는 VPN 연결 허브 및 스포크 사이에 위치한 디바이스(중간 디바이스)가 있는 경우 킵얼라이브 메시지 전송에 사용되며, 해당 디바이스는 IPsec flow에서 NAT를 수행합니다. 이 옵션을 선택하는 경우, 스포크와 중간 디바이스 간에 전송된 킵얼라이브 신호 간격을 초 단위로 구성하고 해당 세션이 활성임을 표시합니다. 이 값의 범위는 10~3600초입니다. 기본값은 20초입니다.
- **Interval(**간격**)** - NAT keepalive 간격을 10~3600초 범위로 설정합니다. 기본값은 20초입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

RADIUS 동적 권한 부여

Firepower Threat Defense 에서는 동적 ACL 또는 사용자별 ACL 이름을 사용하는 VPN 원격 액세스 및 방화벽 cut-through-proxy 세션의 사용자 권한 부여에 RADIUS 서버를 이용할 수 있습니다. 동적 인증 또는 RADIUS CoA(RADIUS Change of Authorization)에 동적 ACL을 구현하려면, 이를 지원하는 RADIUS 서버를 구성해야 합니다. 사용자가 인증을 시도하면 RADIUS 서버가 다운로드 가능한 ACL 또는 ACL 이름을 Firepower Threat Defense로 전송합니다. 지정된 서비스에 대한 액세스는 ACL에 의해 허용되거나 거부됩니다. Firepower Threat Defense는 인증 세션이 만료되면 ACL을 삭제합니다.

관련 항목

RADIUS 서버 그룹, 667 페이지
보안 영역, 577 페이지
RADIUS 동적 권한 부여 구성, 1198 페이지
RADIUS 서버 속성 Firepower Threat Defense, 1181 페이지

RADIUS 동적 권한 부여 구성

시작하기 전에

- RADIUS 서버에서 참조되는 경우 보안 영역 또는 인터페이스 그룹에 하나의 인터페이스만 구성할 수 있습니다.
- 동적 권한 부여가 활성화된 RADIUS 서버는 동적 권한 부여가 작동하려면 Firepower Threat Defense 6.3 이상이 필요합니다.
- Firepower Threat Defense 6.2.3 또는 이전 버전에서는 RADIUS 서버의 인터페이스 선택이 지원되지 않습니다. 인터페이스 옵션은 구축하는 동안 재정의됩니다.

표 ***84:*** 절차

	수행해야 할 작업	추가 정보
1단계	Firepower Management Center 웹 인터페이스에 로그인합니다.	
2단계	동적 권한 부여를 위해 RADIUS 서버 개체를 구성합니다.	RADIUS 서버 그룹 옵션, 668 페이지
3단계	CoA(Change of Authorization)가 활성화된 인터페이스를 통해 ISE 서버에 대한 경로를 구성하여 라우팅 또는 특정 인터페이스를 통한 Firepower Threat Defense에서 RADIUS 서버로의 연결을 설정합니다.	RADIUS 서버 그룹 옵션, 668 페이지 사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지

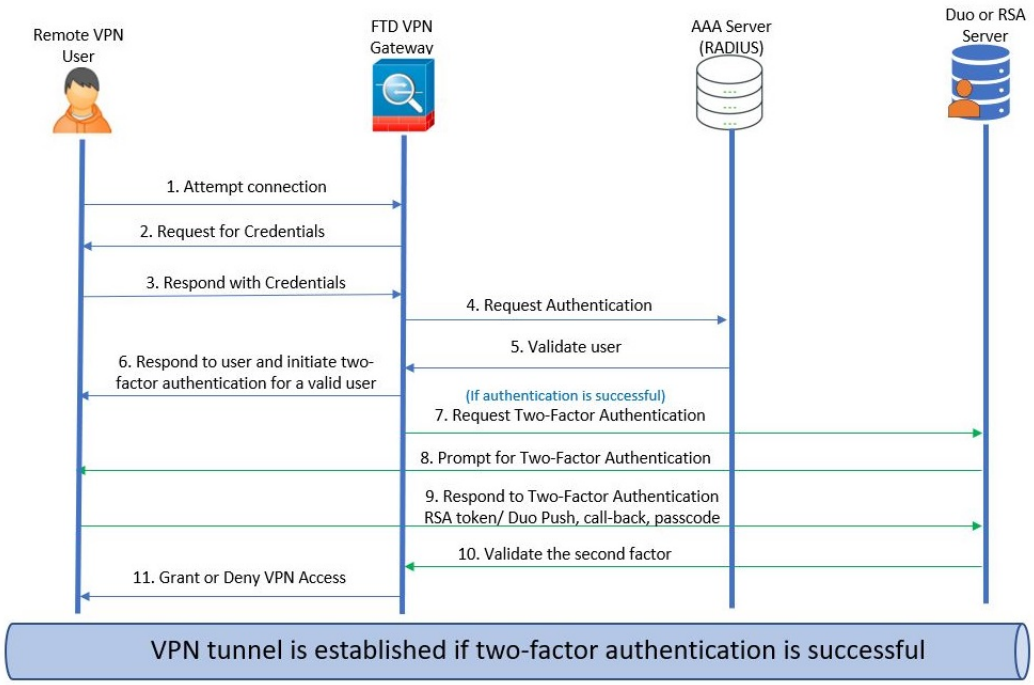
	수행해야 할 작업	추가 정보
4단계	Remote Access VPN 정책을 구성하고 동적 인증을 사용하여 만든 RADIUS 서버 그룹 개체를 선택합니다.	새 Remote Access VPN 정책 생성, 1166 페이지
5단계	플랫폼 설정을 사용하여 DNS 서버 상세 정보 및 도메인 조회 인터페이스를 구성합니다.	DNS 구성, 1170 페이지 DNS 서버 그룹 개체, 637 페이지
6단계	VNP 네트워크를 통해 DNS 서버에 연결할 수 있는 경우 그룹 정책에서 스플릿 터널을 구성하여 Remote Access VPN 터널을 통한 DNS 트래픽을 허용합니다.	그룹 정책 개체 설정, 656 페이지
7단계	구성 변경 사항을 구축합니다.	컨피그레이션 변경 사항 구축, 498 페이지

이중 인증

Remote Access VPN에 대한 이중 인증을 구성할 수 있습니다. 이중 인증의 경우, 사용자는 사용자 이름 및 정적 암호뿐 아니라 RSA 토큰 또는 암호 같은 추가 항목도 제공해야 합니다. 이중 인증이 두 번째 인증 소스를 사용하는 것과 다른 점은 두 가지 인증 요소가 기본 인증 소스와 연결된 RSA 서버와의 관계에 따라 단일 인증 소스에서 구성된다는 것입니다.

Firepower Threat Defense 이중 인증 프로세스에서 첫 번째 요소인 RADIUS 또는 AD 서버와 함께 RSA 토큰과 Duo Mobile에 대한 Duo 푸시 인증 요청이 두 번째 요소로 지원됩니다.

그림 *37:* 이중 인증



RSA 이중 인증 구성

이 작업 관련 정보:

RADIUS 또는 AD 서버를 RSA 서버의 인증 에이전트로 구성하고 Firepower Management Center의 서버를 Remote Access VPN의 기본 인증 소스로 사용할 수 있습니다.

이 접근 방식을 사용하는 경우, 사용자는 RADIUS 또는 AD 서버에 구성된 사용자 이름을 사용하여 인증하고 암호와 토큰을 쉼표로 구분하여(암호,토큰) 암호를 일회용 임시 RSA 토큰과 연결해야 합니다.

이 컨피그레이션에서는 별도의 RADIUS 서버(예: Cisco ISE에서 제공되는 것)를 사용하여 권한 부여 서비스를 제공하는 것이 일반적입니다. 두 번째 RADIUS 서버를 권한 부여 서버 및 과금 서버(선택 사항)로 컨피그레이션합니다.

시작하기 전에

Firepower Threat Defense에서 RADIUS 이중 인증을 구성하기 전에 다음 구성이 완료되었는지 확인합니다.

RSA 서버

- RADIUS 또는 Active Directory 서버를 인증 에이전트로 구성합니다.
- 구성(*sdconf.rec*) 파일을 생성하고 다운로드합니다.

- 토큰 프로파일을 생성하고 사용자에게 토큰을 할당한 후 토큰을 사용자에게 배포합니다. VPN 클라이언트 시스템에 토큰을 다운로드하고 설치합니다.

자세한 내용은 RSA SecureID Suite 설명서를 참조하십시오.

ISE 서버

- RSA 서버에서 생성된 구성(*sdconf.rec*) 파일을 가져옵니다.
- RSA 서버를 외부 ID 소스로 추가하고 공유 암호를 지정합니다.

표 ***85:*** 절차

	수행해야 할 작업	추가 정보
1단계	Firepower Management Center 웹 인터페이스에 로그인합니다.	
2단계	새 RADIUS 서버 그룹을 생성합니다.	RADIUS 서버 그룹 옵션, 668 페이지
3단계	새 RADIUS 서버 그룹 내에 RADIUS 서버 또는 AD 서버를 호스트로 사용하고 시간 초과가 60초 이상인 RADIUS 서버 개체를 만듭니다.	RADIUS 서버 옵션, 669 페이지 참고 RADIUS 또는 AD 서버는 RSA 서버에서 인증 에이전트로 구성된 서버와 동일해야 합니다. 2단계 인증의 경우 AnyConnect 클라이언트 프로파일 XML 파일에서 시간 초과가 60 초 이상으로 업데이트되었는지도 확인합니다.
4단계	마법사를 사용하여 새 Remote Access VPN 정책을 구성하거나 기존 Remote Access VPN 정책을 편집합니다.	새 Remote Access VPN 정책 생성, 1166 페이지
5단계	RADIUS를 인증 서버로 선택한 다음 새로 생성된 RADIUS 서버 그룹을 인증 서버로 선택합니다.	Remote Access VPN에 대한 AAA 설정, 1177 페이지
7단계	구성 변경 사항을 구축합니다.	컨피그레이션 변경 사항 구축, 498 페이지

듀오 이중 인증 구성

이 작업 관련 정보:

듀오 RADIUS 서버를 기본 인증 소스로 컨피그레이션할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다. (LDAPS를 통한 듀오 클라우드 서비스와의 직접 연결은 사용할 수 없습니다.)

듀오를 구성하는 자세한 단계는 https://duo.com/docs/cisco-firepower를 참조하십시오.

그런 다음, 프록시 서버로 가는 인증 요청을 전달하여 다른 RADIUS 서버 또는 AD 서버를 첫 번째 인증 요소로 사용하고 듀오 클라우드 서비스는 두 번째 요소로 사용하도록 컨피그레이션합니다.

이 접근 방식을 사용한다면, 사용자는 듀오 클라우드나 웹 서버 중 하나 및 RADIUS 서버에 구성된 사용자 이름을 사용하여 인증해야 합니다. 사용자는 RADIUS 서버에서 구성한 비밀번호를 입력하고, 다음 듀오 코드 중 하나를 입력해야 합니다.

- **Dou-passcode**. 예: *my-password*,123456.
- **push**. 예: *my-password*,**push**. 푸시를 사용하여 듀오에게 듀오 모바일 앱으로 푸시 인증을 전송하도록 지시합니다. 사용자는 이미 이 앱을 설치하여 등록했어야 합니다.
- **SMS**. 예: *my-password*,**SMS**. **SMS**를 사용하여 듀오에게 사용자의 모바일 디바이스로 새로운 암호 배치가 포함된 SMS 메시지를 전송하도록 지시합니다. **SMS**를 사용하는 경우, 사용자의 인증 시도가 실패합니다. 그러면 사용자는 다시 인증하고 두 번째 요인으로 새 암호를 입력해야 합니다.
- **phone(**전화**)**. 예: *my-password*,**phone**. 전화기 콜백으로 인증하려면 **phone(**전화기**)**를 사용합니다.

예시가 포함된 로그인 옵션 관련 정보는 https://guide.duo.com/anyconnect의 내용을 참조하십시오.

시작하기 전에

Firepower Threat Defense에서 듀오 인증 프록시를 이용한 2단계 인증을 구성하기 전에, 다음 구성을 완료했는지 확인합니다.

- 듀오 구축을 시작하기 전에 원격 액세스 VPN 사용자에 대해 작동하는 기본 인증(RADIUS 또는 AD)을 구성합니다.
- 듀오 프록시 서버를 네트워크의 Windows 또는 Linux 장치에 설치해 듀오를 Firepower Threat Defense 원격 액세스 VPN과 통합합니다. 이 듀오 프록시 서버는 RADIUS 서버 역할도 합니다.

  다음 위치에서 최신 듀오 인증 프록시를 다운로드하여 설치합니다.

  - **Windows**: https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**: https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - https://duo.com/docs/checksums#duo-authentication-proxy에서 체크섬을 확인합니다.
- 듀오 인증 파일 `authproxy.cfg`를 구성합니다. https://duo.com/docs/cisco-firepower#configure-the-proxy 페이지의 지침에 따라 인증 구성 설정을 구성합니다.

`authproxy.cfg` 구성 파일에는 RADIUS 또는 ISE 서버, Firepower Threat Defense 디바이스, 듀오 프록시 서버 상세정보, 통합 키, 비밀 키 및 API 호스트 상세정보가 있어야 합니다.

- `authproxy.cfg` 파일에 올바른 API 호스트 정보가 있는지 확인합니다.
- **Duo Security Server(**듀오 보안 서버**)** > **Duo Admin Panel(**듀오 관리자 창**)** > **Applications(**애플리케이션**)** > **CISCO RADIUS VPN**에서 새로 설치한 듀오 프록시 서버의 기타 필수 설정(보조 인증 요소 등)을 구성합니다.

표 ***86:*** 절차

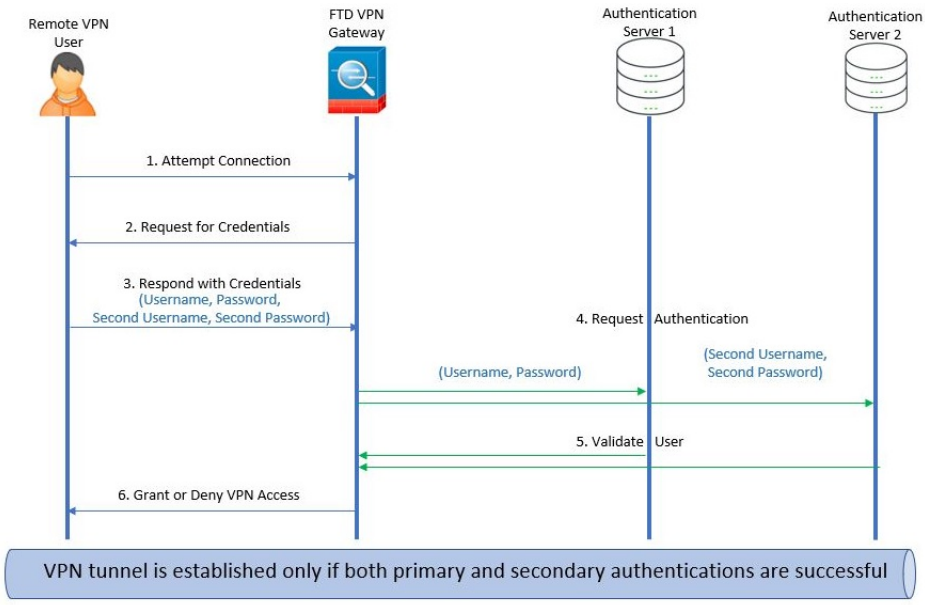
	수행해야 할 작업	추가 정보
1단계	Firepower Management Center 웹 인터페이스에 로그인합니다.	
2단계	새 RADIUS 서버 그룹을 생성합니다.	RADIUS 서버 그룹 옵션, 668 페이지
3단계	새 RADIUS 서버 그룹 내에 듀오 프록시 서버를 호스트로 사용하고 시간 초과가 60초 이상인 RADIUS 서버 개체를 만듭니다.	RADIUS 서버 옵션, 669 페이지 참고 2단계 인증의 경우 AnyConnect 클라이언트 프로파일 XML 파일에서 시간 초과가 60 초 이상으로 업데이트되었는지도 확인합니다.
4단계	마법사를 사용하여 새 Remote Access VPN 정책을 구성하거나 기존 Remote Access VPN 정책을 편집합니다.	새 Remote Access VPN 정책 생성, 1166 페이지
5단계	RADIUS를 인증 서버로 선택한 다음, 듀오 프록시 서버로 생성한 RADIUS 서버 그룹을 인증 서버로 선택합니다.	Remote Access VPN에 대한 AAA 설정, 1177 페이지
7단계	구성 변경 사항을 구축합니다.	컨피그레이션 변경 사항 구축, 498 페이지

보조 인증

Firepower Threat Defense의 보조 인증 또는 이중 이중은 서로 다른 인증 서버 2개를 이용해 원격 액세스 VPN 연결에 레이어를 추가합니다. 보조 인증을 활성화하면, AnyConnect VPN 사용자는 자격 증명 모음 2개를 입력해야 VPN 게이트웨이에 로그인할 수 있습니다.

Firepower Threat Defense 원격 액세스 VPN은 AAA 전용과 클라이언트 인증서 및 AAA 인증 방법에서만 지원됩니다.

그림 *38: Remote Access VPN* 보조 또는 이중 인증



관련 항목

Remote Access VPN 보조 인증 구성, 1204 페이지

Remote Access VPN 보조 인증 구성

Remote Access VPN 인증이 클라이언트 인증서와 인증 서버를 모두 사용하도록 구성되면 VPN 클라이언트 인증은 클라이언트 인증서 유효성 검사와 AAA 서버를 사용하여 수행됩니다.

시작하기 전에

- 인증 (AAA) 서버 2개, 즉 기본 및 보조 인증 서버를 구성하고, 필요한 ID 인증서를 구성합니다. 인증 서버는 RADIUS 서버나 AD 또는 LDAP 영역이 될 수 있습니다.
- 원격 액세스 VPN 구성이 작동하려면 Firepower Threat Defense 디바이스에서 AAA 서버에 연결할 수 있는지 확인합니다. 라우팅을 구성(**Devices(**디바이스**) > Device Management(**디바이스 관리**) > Edit Device(**디바이스 편집**) > Routing(**라우팅**)**하여 AAA 서버에 대한 연결성을 보장합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** 새 Remote Access VPN 정책의 경우 연결 프로파일 설정을 선택하는 동안 인증을 구성합니다. 기존 구성의 경우 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **AAA** > **Authentication Method(**인증 방법**)**, **AAA** 또는 **Client Certificate & AAA(**클라이언트 인증서 및 **AAA)**를 클릭합니다.

- 다음과 같이 **Authentication Method(**인증 방법**)**를 선택하는 경우:

  Client Certificate & AAA(클라이언트 인증서 및 **AAA)** - 클라이언트 인증서와 AAA 서버를 모두 이용해 인증합니다.

  - **AAA - Authentication Server(**인증 서버**)**를 **RADIUS**로 선택하는 경우 Authorization Server(권한 부여 서버)는 기본적으로 동일한 값을 가집니다. 드롭다운 목록에서 **Accounting Server(**과금 서버**)**를 선택합니다. Authentication Server(인증 서버) 드롭다운 목록에서 **AD** 및 **LDAP**를 선택할 때마다 **Authorization Server(**권한 부여 서버**)** 및 **Accounting Server(**과금 서버**)**를 각각 수동으로 선택해야 합니다.
  - 어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

- **2**차 인증 사용 - VPN 세션에 대한 추가 보안을 제공하기 위해 기본 인증 외에 2차 인증이 구성됩니다. 2차 인증은 **AAA** 전용 및 클라이언트 인증서 및 **AAA** 인증 방법에만 적용됩니다.

  보조 인증은 VPN 사용자가 AnyConnect 로그인 화면에 사용자 이름 및 암호 모음 2개를 입력해야 하는 선택적 기능입니다. 인증 서버 또는 클라이언트 인증서에서 2차 사용자 이름이 미리 입력되도록 구성할 수도 있습니다. 원격 액세스 VPN 인증은 기본 인증과 보조 인증을 모두 성공한 경우에만 부여됩니다. 인증 서버 중 하나에 연결할 수 없거나 한쪽 인증에서 장애가 발생하면 VPN 인증이 거부됩니다.

  보조 인증을 구성하기 전에, 두 번째 사용자 이름과 암호에 대해 보조 인증 서버 그룹(AAA 서버)을 구성해야 합니다. 예를 들어 기본 인증 서버는 LDAP나 Active Directory 영역으로, 보조 인증은 RADIUS 서버로 설정할 수 있습니다.

  참고 기본적으로 보조 인증이 필수가 아닙니다.

  인증 서버 - VPN 사용자에게 보조 사용자 이름 및 암호를 제공하는 보조 인증 서버입니다.

  보조 인증용 사용자 이름에서 다음을 선택하십시오.

  - 프롬프트: VPN 게이트웨이에 로그인하는 동안 사용자에게 사용자 이름과 암호를 입력하라는 메시지를 표시합니다.
  - 기본 인증 사용자 이름 사용: 사용자 이름은 기본 인증 서버와 2차 인증 모두에 대해 기본 인증 서버에서 가져옵니다. 두 개의 암호를 입력해야 합니다.
  - 클라이언트 인증서의 사용자 이름 매핑: 클라이언트 인증서의 보조 사용자 이름을 미리 채웁니다.
    - **Map specific field(**특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN (Distinguished**

Name) as username(전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다.

기본 및 보조 필드 매핑에 대한 자세한 내용은 인증 방법 설명을 참조하십시오.

- 인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기: AnyConnect VPN 클라이언트를 통해 사용자가 연결할 때 클라이언트 인증서에서 보조 사용자 이름을 미리 채웁니다.
  - 로그인 창에서 사용자 이름 숨기기: 보조 사용자 이름은 클라이언트 인증서에서 미리 채워지지만 미리 채워진 사용자 이름은 수정을 방지하기 위해 사용자에게 표시되지 않습니다.

- **VPN** 세션에 보조 사용자 이름 사용: 보조 사용자 이름은 VPN 세션 중에 사용자 활동을보고하는 데 사용됩니다.

자세한 내용은 Remote Access VPN에 대한 AAA 설정, 1177 페이지를 참고하십시오.

관련 항목

연결 프로파일 설정, 1173 페이지

SAML 2.0을 사용한 SSO(Single Sign-On) 인증

SAML SSO(Single Sign-On) 인증 관련 정보

SAML(Security Assertion Markup Language)은 다른 상황에서 사용자의 세션을 기반으로 애플리케이션에 사용자를 로그인하기 위한 개방형 표준입니다. 조직은 사용자가 AD(Active Directory) 도메인 또는 인트라넷에 로그인할 때 사용자의 ID를 이미 알고 있습니다. 이들은 이 ID 정보를 사용하여 SAML을 사용하는 웹 기반 애플리케이션과 같은 다른 애플리케이션에 사용자를 로그인합니다. 개별 애플리케이션은 자격 증명을 저장할 필요가 없으며, 사용자는 개별 애플리케이션에 대해 서로 다른 자격 증명 집합을 기억하고 관리할 필요가 없습니다. SAML SSO(Sing Sign-On)는 한 위치(ID 제공자)에서 다른 위치(서비스 제공자)로 사용자 ID를 전송하는 방식으로 작동합니다.

SAML Single Sign-On Firepower Threat Defense

Firepower Threat Defense 디바이스는 AnyConnect Secure Mobility Client를 사용하는 원격 액세스 VPN 연결을 위한 SAML 2.0 SSO(Single Sign-On) 인증을 지원합니다. Firepower Threat Defense에서 SAML 2.0 SSO를 설정하려면 다음이 필요합니다.

- **IdP(Identity Provider)** - Duo Access Gateway는 사용자 인증을 수행하고 어설션을 발급하는 ID 제공자 역할을 합니다.
- **SP(Service Provider)** - FTD 디바이스가 서비스 제공자 역할을 하며 ID 제공자로부터 인증 어설션을 가져옵니다.

- **VPN** 클라이언트 - AnyConnect Security Mobility Client는 임베디드 브라우저를 통해 SAML 2.0 인증을 수행합니다.

SAML SSO(Single Sign-On) 인증 구성

시작하기 전에

FTD 원격 액세스 VPN으로 SAML 단일 로그인을 설정하기 전에 다음을 수행했는지 확인합니다.

- Duo로 계정 생성
- Duo Access Gateway 다운로드 및 설치
- SAML ID 제공자(Duo)에서 다음 정보를 얻습니다.
  - ID 제공자 엔티티 ID URL
  - 로그인 URL
  - 로그아웃 URL
  - ID 공급자 인증서
- **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(ASA** 서버**)** > **Single Sign-on Server(SSO(Single Sign-On)** 서버**)**에서 SAML SSO(Single Sign-On) 서버 개체를 생성합니다.

참고 마법사를 사용하여 새 원격 액세스 VPN 설정을 생성할 때 연결 프로파일 설정에서 SSO(Single Sign-On) 서버 개체를 생성할 수도 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**을 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN을 생성하거나 기존 VPN 설정을 편집합니다.

단계 **3** **Connection Profile(**연결 프로파일**)** > **AAA** 설정을 구성하고 **Authentication Method(**인증 방법**)** > **SAML**을 선택합니다.

단계 **4** 필요한 SAML SSO(Single Sign-On) 서버를 인증 서버로 선택합니다.

참고 새 원격 액세스 VPN 설정의 경우: 연결 프로파일 설정을 구성할 때 **Authentication Server(**인증 서버**)** 목록 옆의 +를 클릭하여 새 SAML SSO(Single Sign-On) 서버 개체를 생성할 수 있습니다.

SSO 서버 개체 생성에 대한 자세한 내용은 SSO(Single Sign-On) 서버 추가, 670 페이지의 내용을 참조하십시오.

단계 **5** 원격 액세스 VPN에 대한 필요한 설정을 구성합니다.

단계 **6** 원격 액세스 VPN 설정을 저장하고 Firepower Threat Defense 디바이스에 구축합니다.

관련 항목

Remote Access VPN에 대한 AAA 설정, 1177 페이지

Remote Access VPN AAA 사용자 지정

이 섹션에서는 원격 액세스 VPN에 대 한 AAA 기본 설정을 사용자 지정하는 방법을 설명합니다. 자세한 내용은 Remote Access VPN에 대한 AAA 설정, 1177 페이지를 참고하십시오.

클라이언트 인증서를 통한 VPN 사용자 인증

마법사를 사용하여 새 Remote Access VPN 정책을 생성하거나 이후 정책을 편집할 때 클라이언트 인증서를 사용하여 Remote Access VPN 인증을 구성할 수 있습니다.

시작하기 전에

VPN 게이트웨이 역할을 하는 각 Firepower Threat Defense 디바이스에 대한 ID 인증서를 얻는 데 사용되는 인증서 등록 개체를 구성합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** 새 Remote Access VPN 정책의 경우 연결 프로파일 설정을 선택하는 동안 인증을 구성합니다. 기존 구성의 경우 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **AAA** > **Authentication Method(**인증 방법**)** > **Client Certificate Only(**클라이언트 인증서 전용**)**를 클릭합니다.

이 인증 방법을 통해 사용자는 클라이언트 인증서를 사용하여 인증됩니다. VPN 클라이언트 엔드포인트에서 클라이언트 인증서를 구성해야 합니다. 기본적으로 사용자 이름은 각각 클라이언트 인증서 필드 CN 및 OU에서 파생됩니다. 사용자 이름이 클라이언트 인증서의 다른 필드에 지정된 경우 'Primary(기본)' 및 'Secondary(보조)' 필드를 사용하여 해당 필드를 매핑합니다.

Map specific field(특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다. 고유 이름(DN)은 사용자를 연결 프로파일과 연결할 때 식별자로 사용할 수 있는 개별 필드로 구성된 고유한 ID입니다. DN 규칙은 향상된 인증서 인증에 사용됩니다.

- **Map specific field(**특정 필드 매핑**)** 옵션과 관련된 기본 및 보조 필드는 다음 공통 값을 포함합니다.
  - C(국가)
  - CN(이름)
  - DNQ(DN 한정자
  - EA(이메일 주소)
  - GENQ(세대 한정자)
  - GN(이름)
  - I(이니셜)
  - L(시/군/구)
  - N(이름)
  - O(조직)
  - OU(조직 단위)
  - SER(일련 번호)
  - SN(성)
  - SP(시/도)
  - T(제목)
  - UID(사용자 ID)
  - UPN(사용자 계정 이름)
- 어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

자세한 내용은 Remote Access VPN에 대한 AAA 설정, 1177 페이지를 참고하십시오.

관련 항목

연결 프로파일 설정, 1173 페이지
인증서 등록 개체 추가, 630 페이지

클라이언트 인증서 및 AAA 서버를 통한 Remote Access VPN 로그인 설정

Remote Access VPN 인증이 클라이언트 인증서와 인증 서버를 모두 사용하도록 구성되면 VPN 클라이언트 인증은 클라이언트 인증서 유효성 검사와 AAA 서버를 사용하여 수행됩니다.

시작하기 전에

- VPN 게이트웨이 역할을 하는 각 Firepower Threat Defense 디바이스에 대한 ID 인증서를 얻는 데 사용되는 인증서 등록 개체를 구성합니다.
- 이 Remote Access VPN 정책에서 사용 중인 RADIUS 서버 그룹 개체와 AD 또는 LDAP 영역을 구성합니다.
- Remote Access VPN 구성이 작동하려면 Firepower Threat Defense 디바이스에서 AAA 서버에 연결할 수 있는지 확인합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 기존 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 **Add(**추가**)**를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** 새 Remote Access VPN 정책의 경우 연결 프로파일 설정을 선택하는 동안 인증을 구성합니다. 기존 구성의 경우 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **AAA** > **Authentication Method(**인증 방법**)**, **Client Certificate & AAA(**클라이언트 인증서 및 **AAA)**를 클릭합니다.

- 다음과 같이 **Authentication Method(**인증 방법**)**를 선택하는 경우:

  Client Certificate & AAA(클라이언트 인증서 및 **AAA)** - 두 가지 인증 유형이 모두 수행됩니다.

  - **AAA - Authentication Server(**인증 서버**)**를 **RADIUS**로 선택하는 경우 Authorization Server(권한 부여 서버)는 기본적으로 동일한 값을 가집니다. 드롭다운 목록에서 **Accounting Server(**과금 서버**)**를 선택합니다. Authentication Server(인증 서버) 드롭다운 목록에서 **AD** 및 **LDAP**를 선택할 때마다 **Authorization Server(**권한 부여 서버**)** 및 **Accounting Server(**과금 서버**)**를 각각 수동으로 선택해야 합니다.
  - **Client Certificate(**클라이언트 인증서**)** - 사용자가 클라이언트 인증서로 인증합니다. 클라이언트 인증서는 VPN 클라이언트 엔드포인트에서 구성해야 합니다. 기본적으로 사용자 이름은 각각 클라이언트 인증서 필드 CN & OU에서 파생됩니다. 사용자 이름이 클라이언트 인증서의 다른 필드에 지정된 경우 'Primary(기본)' 및 'Secondary(보조)' 필드를 사용하여 해당 필드를 매핑합니다.

    Map specific field(특정 필드 매핑**)** 옵션을 선택하면 클라이언트 인증서의 사용자 이름이 포함됩니다. **Primary(**기본**)** 및 **Secondary(**보조**)** 필드에는 **CN(Common Name)** 및 **OU(Organizational Unit)** 각각의 기본값이 표시됩니다. **Use entire DN as username(**전체 **DN**을 사용자 이름으로 사용**)** 옵션을 선택하는 경우 시스템은 자동으로 사용자 ID를 검색합니다. 고유 이름(DN)은 사용자를 연결 프로파일과 연결할 때 식별자로 사용할 수 있는 개별 필드로 구성된 고유한 ID입니다. DN 규칙은 향상된 인증서 인증에 사용됩니다.

    Map specific field(특정 필드 매핑**)** 옵션과 관련된 기본 및 보조 필드는 다음 공통 값을 포함합니다.

- C(국가)
- CN(이름)
- DNQ(DN 한정자
- EA(이메일 주소)
- GENQ(세대 한정자)
- GN(이름)
- I(이니셜)
- L(시/군/구)
- N(이름)
- O(조직)
- OU(조직 단위)
- SER(일련 번호)
- SN(성)
- SP(시/도)
- T(제목)
- UID(사용자 ID)
- UPN(사용자 계정 이름)

- 어떤 인증 방법을 선택하든 **Allow connection only if user exists in authorization database(**사용자가 권한 부여 데이터베이스에 있는 경우에만 연결 허용**)**를 선택하거나 선택 취소합니다.

자세한 내용은 Remote Access VPN에 대한 AAA 설정, 1177 페이지를 참고하십시오.

관련 항목

연결 프로파일 설정, 1173 페이지
인증서 등록 개체 추가, 630 페이지

VPN 세션에 대한 암호 변경 관리

암호 관리를 사용하면 Remote Access VPN 관리자는 암호 만료 시 Remote Access VPN 사용자에 대한 알림 설정을 구성할 수 있습니다. 암호 관리는 인증 방법 AAA Only(AAA 전용) 및 Client Certificate & AAA(클라이언트 인증서 및 AAA)를 통해 AAA 설정에서 사용할 수 있습니다. 자세한 내용은 Remote Access VPN에 대한 AAA 설정, 1177 페이지를 참고하십시오.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 원격 액세스 정책을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 AAA 설정이 포함된 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 4 **AAA** > **Advanced Settings(**고급 설정**)** > **Password Management(**비밀번호 관리**)**를 선택합니다.

단계 5 **Enable Password Management(**비밀번호 관리 활성화**)**를 선택하고 다음 중 하나를 선택합니다.

- Notify User(사용자에게 알림) - 비밀번호가 만료되기 전에 사용자에게 알립니다. 입력란에 일 수를 지정합니다.
- Notify user on the day password expiration(비밀번호 만료 당일에 사용자에게 알림) - 비밀번호가 만료되는 당일에만 사용자에게 알립니다.

단계 6 **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 1173 페이지

인증을 위한 LDAP 또는 Active Directory 설정

인증을 위해 LDAP 또는 Active Directory(AD) 서버에서 VPN을 구성하려는 경우 Firepower Management Center 웹 인터페이스에서 속성 맵이 직접 지원되지 않으므로 FlexConfig 개체를 사용하여 속성 맵을 구성해야 합니다.

시작하기 전에

LDAP 또는 AD에 대한 영역 개체를 생성했는지 확인합니다.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 LDAP 또는 AD 영역 개체를 인증 서버로 사용하여 Remote Access VPN 정책을 생성합니다. 또는 기존 Remote Access VPN 구성을 편집하고 LDAP 또는 AD 영역을 인증 서버로 선택합니다.

단계 3 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.

단계 4 FlexConfig 정책을 생성하고 append 섹션에 다음 두 FlexConfig 개체를 생성 및 할당합니다.

FlexConfig 정책 설정, 1299 페이지의 내용을 참조하십시오.

a) **Deployment type**: Once 및 **Type**: Append를 사용하여 LDAP 특성 맵용 FlexConfig 개체를 생성합니다.

개체 본문에 다음을 입력합니다.

```
lda attribute-map <LDAP_Map_for_VPN_Access>
          map-name  memberOf Group-Policy
          map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
LabAdminAccessGroupPolicy
          map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com
VPNAccessGroupPolicy
```

b) **Deployment type**: Everytime 및 **Type**: Append를 사용하여 LDAP 특성 맵에 연결되는 FlexConfig 개체를 생성합니다.

참고 Firepower Management Center에 의해 무효화되므로 LDAP-attribute-map 연결을 복원하기 위해 이 매핑이 필요합니다.

개체 본문에 다음을 입력합니다.

```
aaa-server <LDAP/AD_Realm_name> host <AD Server IP>
          ldap-attribute-map <LDAP_Map_for_VPN_Access>
          exit
```

Remote Access VPN 정책 구성에 추가한 연결 프로파일의 AAA 서버 설정에 사용된 LDAP 영역 이름과 동일한 *aaa-server*를 사용합니다.

자세한 내용은 FlexConfig 텍스트 개체 설정, 1298 페이지를 참고하십시오.

a) **Save(**저장**)**를 클릭합니다.

FlexConfig 정책에서 FlexConfig 개체의 순서가 LDAP 특성 맵 FlexConfig 개체이고 그 뒤에 AAA 서버 개체가 오는지 확인합니다.

이렇게 하면 LDAP 특성 맵이 구성되어 Firepower Threat Defense 디바이스의 LDAP 서버 구성과 연결됩니다.

관련 항목

FlexConfig 개체 구성, 1293 페이지

RADIUS 서버로 계정 기록 전송

Remote Access VPN의 계정 기록은 VPN 관리자가 사용자가 액세스하는 서비스 및 사용자가 사용하는 네트워크 리소스의 양을 추적할 수 있도록 도와줍니다. 계정 관리 정보에는 사용자 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대해 이 데이터를 분석할 수 있습니다.

관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다. AAA 계정을 활성화하면 네트워크 액세스 서버가 구성된 계정 서버에 사용자 작업을 보고합니다. 모든 사용자 활동 정보가 Firepower Management Center에서 RADIUS 서버로 전송되도록 RADIUS 서버를 과금 서버로 구성할 수 있습니다.

참고 Remote Access VPN AAA 설정에서 인증, 권한 부여 및 계정을 위해 동일한 RADIUS 서버 또는 별도의 RADIUS 서버를 사용할 수 있습니다.

시작하기 전에

인증 요청이나 계정 기록을 전송할 RADIUS 서버로 RADIUS 그룹 개체를 구성합니다. RADIUS 서버 그룹 옵션, 668 페이지의 내용을 참조하십시오.

Firepower Threat Defense 디바이스에서 RADIUS 서버에 연결할 수 있는지 확인합니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit Device(**디바이스 편집**)** > **Routing(**라우팅**)**에서 Firepower Management Center에 대한 라우팅을 구성하여 RADIUS 서버에 대한 연결성을 보장합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭하거나 새 원격 액세스 VPN 정책을 생성합니다.

단계 **3** AAA 설정이 포함된 연결 프로파일을 선택하고 **Edit(**편집**)** > **AAA**를 클릭합니다.

단계 **4** RADIUS 서버를 **Accounting Server(**과금 서버**)**로 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관련 항목

연결 프로파일 설정, 1173 페이지
Remote Access VPN에 대한 AAA 설정, 1177 페이지

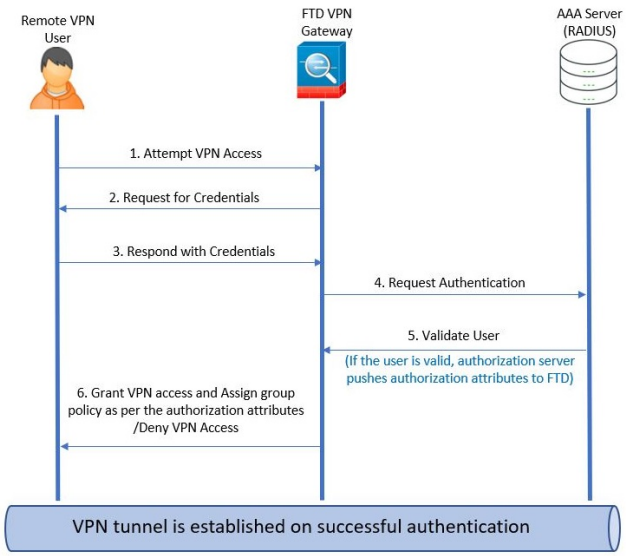
권한 부여 서버에 그룹 정책 선택 위임

VPN 터널이 설정된 경우 사용자에게 적용되는 그룹 정책이 결정됩니다. 마법사를 사용하여 원격 액세스 VPN을 생성하는 동안 연결 프로파일 그룹 정책을 선택하거나, 나중에 연결 프로파일의 연결 정책을 업데이트하면 됩니다. 하지만 AAA(RADIUS) 서버를 그룹 정책을 할당하도록 구성하거나, 현재 연결 프로파일에서 가져올 수도 있습니다. Firepower Threat Defense 디바이스에서 연결 프로파일에 구성된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

IETF RADIUS 속성 25를 전송하고 해당 그룹 정책 이름에 매핑하여, 사용자 또는 사용자 그룹에 대한 인증 프로파일을 설정하도록 ISE 또는 RADIUS 서버를 구성할 수 있습니다. 특정 그룹 정책을 사용자 또는 사용자 그룹에 지정하여 다운로드 가능한 ACL을 푸시하고, 배너를 설정하고, VLAN을 제한하고, 세션에 SGT을 적용하는 고급 옵션을 구성할 수 있습니다. 이러한 속성은 VPN 연결이 설정될 때 해당 그룹에 속한 모든 사용자에게 적용됩니다.

자세한 내용은 Cisco Identity Services Engine 관리자 가이드의 Configure Standard Authorization Policies(표준 인증 정책 구성) 섹션과 RADIUS 서버 속성 Firepower Threat Defense, 1181 페이지의 내용을 참조하십시오.

그림 ***39: AAA*** 서버의 ***Remote Access VPN*** 그룹 정책 선택



관련 항목

그룹 정책 개체 설정, 656 페이지
연결 프로파일 설정, 1173 페이지

그룹 정책 또는 기타 속성 선택을 권한 부여 서버로 재정의

Remote Access VPN 사용자가 VPN에 연결할 때 연결 프로파일에 구성된 그룹 정책 및 기타 속성이 사용자에게 할당됩니다. 하지만 원격 액세스 VPN 시스템 관리자는 사용자 또는 사용자 그룹에 대한 권한 부여 프로파일을 설정하기 위해 ISE 또는 RADIUS 서버를 구성하여 그룹 정책 및 기타 속성의 선택 사항을 권한 부여 서버에 위임할 수 있습니다. 사용자가 인증되면 이러한 특정 권한 부여 속성이 Firepower Threat Defense 디바이스에 푸시됩니다.

시작하기 전에

RADIUS를 인증 서버로 사용하여 Remote Access VPN 정책을 구성해야 합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** 아직 구성되지 않은 경우 권한 부여 서버로 RADIUS 또는 ISE를 선택합니다.

단계 4 **Advanced(**고급**)** > **Group Policies(**그룹 정책**)**를 선택하고 필요한 그룹 정책을 추가합니다. 그룹 정책 개체에 대한 세부 정보는 그룹 정책 개체 설정, 656 페이지의 내용을 참조하십시오.

하나의 그룹 정책 연결 프로 파일, 매핑할 수 있습니다. 그러나 Remote Access VPN 정책에서 여러 그룹 정책을 만들 수 있습니다. 이러한 그룹 정책은 ISE 또는 RADIUS 서버에서 참조될 수 있으며 권한 부여 서버에 권한 부여 속성을 지정하여 연결 프로파일에 구성된 그룹 정책을 대체하도록 구성할 수 있습니다.

단계 5 대상 Firepower Threat Defense 디바이스에서 구성을 구축합니다.

단계 6 권한 서버에서 IP 주소 및 다운로드할 수 있는 ACL에 대한 RADIUS 속성을 사용하여 권한 부여 프로파일을 생성합니다.

그룹 정책이 Remote Access VPN에 대해 선택된 권한 부여 서버에서 구성되면 그룹 정책은 사용자가 인증된 후 Remote Access VPN 사용자에 대한 연결 프로파일에 구성된 그룹 정책보다 우선합니다.

관련 항목

그룹 정책 개체 설정, 656 페이지

사용자 그룹에 대한 VPN 액세스 거부

인증된 사용자 또는 사용자 그룹이 VPN을 사용할 수 없도록 하려는 경우 그룹 정책을 구성하여 VPN 액세스를 거부할 수 있습니다. Remote Access VPN 정책에서 그룹 정책을 구성하고 권한 부여를 위해 ISE 또는 RADIUS 서버 구성에서 이 정책을 참조할 수 있습니다.

시작하기 전에

원격 액세스 정책 마법사를 사용하여 Remote Access VPN을 구성하고 Remote Access VPN 정책에 대한 인증 설정을 구성했는지 확인합니다.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 2 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 3 **Advanced(**고급**)** > **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 4 그룹 정책을 선택하고 새 그룹 정책 **Edit(**편집**)**를 클릭하거나 새 그룹 정책을 추가합니다.

단계 5 **Advanced(**고급**)** > **Session Settings(**세션 설정**)**를 선택하고 **Simultaneous Login Per User(**사용자별 동시 로그인**)**를 0으로 설정합니다.
이렇게 하면 사용자 또는 사용자 그룹이 VPN에 한 번도 연결되지 않습니다.

단계 6 **Save(**저장**)**를 클릭하여 그룹 정책을 저장한 다음 Remote Access VPN 구성을 저장합니다.

단계 7 해당 사용자/사용자 그룹에 대한 권한 부여 프로파일을 설정하여 IETF RADIUS 속성 25를 전송하고 해당 그룹 정책 이름에 매핑하도록 ISE 또는 RADIUS 서버를 구성합니다.

단계 8 ISE 또는 RADIUS 서버를 원격 액세스 VPN 정책의 인증 서버로 구성합니다.

단계 **9** 원격 액세스 VPN 정책을 저장하고 구축합니다.

관련 항목

연결 프로파일 설정, 1173 페이지

사용자 그룹에 대한 연결 프로파일 선택 제한

사용자 또는 사용자 그룹에 단일 연결 프로파일을 적용하려는 경우 연결 프로파일을 비활성화할 수 있으며, 이에 따라 사용자가 AnyConnect VPN 클라이언트를 사용하여 연결할 때 그룹 별칭 또는 URL을 선택할 수 없습니다.

예를 들어 조직에서 휴대폰 사용자, 회사에서 발급한 노트북 사용자 또는 개인 노트북 사용자와 같은 다른 VPN 사용자 그룹에 특정 구성을 사용하려는 경우 이러한 각 사용자 그룹에 특정한 프로파일 연결을 구성하고 사용자가 VPN에 연결할 때 적절한 연결 프로파일을 적용할 수 있습니다.

AnyConnect 클라이언트는 기본적으로 Firepower Management Center에서 구성되고 Firepower Threat Defense에 구축된 연결 프로파일 목록(연결 프로파일 이름, 별칭 또는 별칭 URL 기준)을 표시합니다. 사용자 정의 연결 프로파일이 구성되지 않은 경우 AnyConnect는 *DefaultWEBVPNGroup* 연결 프로파일을 표시합니다. 다음 절차를 사용하여 사용자 그룹에 단일 연결 프로파일을 적용합니다.

시작하기 전에

- Firepower Management Center 웹 인터페이스에서 인증 방법과 함께 Remote Access VPN 정책 마법사를 사용하여 'Client Certificate Only(클라이언트 인증서 전용)' 또는 'Client Certificate + AAA(클라이언트 인증서 + AAA)'로 Remote Access VPN을 구성합니다. 인증서에서 사용자 이름 필드를 선택합니다.
- 권한 부여를 위해 ISE 또는 RADIUS 서버를 구성하고 그룹 정책을 권한 부여 서버와 연결합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** **Access Interfaces(**액세스 인터페이스**)**를 선택하고 **Allow Users to select connection profile while logging in(**사용자가 로그인 상태에서 연결 프로파일을 선택할 수 있음**)**을 비활성화합니다.

단계 **4** **Advanced(**고급**)** > **Certificate Maps(**인증서 맵**)**를 클릭합니다.

단계 **5** **Use the configured rules to match a certificate to a Connection Profile(**구성된 규칙을 사용하여 연결 프로파일에 인증서 일치**)**을 선택합니다.

단계 **6** **Certificate Map Name(**인증서 맵 이름**)**을 선택하거나 **Add(**추가**)** 아이콘을 클릭하여 인증서 규칙을 추가합니다.

단계 **7** **Connection Profile(**연결 프로파일**)**을 선택하고 **Ok(**확인**)**를 클릭합니다.

이 구성을 사용하면 사용자가 AnyConnect 클라이언트에서 연결할 때 사용자가 매핑된 연결 프로파일을 갖게 되며 VPN을 사용하도록 인증됩니다.

관련 항목

그룹 정책 개체 설정, 656 페이지
연결 프로파일 설정, 1173 페이지

Remote Access VPN 클라이언트에 대한 AnyConnect 클라이언트 프로파일 업데이트

AnyConnect 클라이언트 프로파일은 AnyConnect의 일부로 VPN 클라이언트 시스템에 구축할 관리자 정의 최종 사용자 요구 사항 및 인증 정책이 포함된 XML 파일입니다. 사전 구성된 네트워크 프로파일을 최종 사용자가 사용할 수 있게 지원합니다.

독립적인 구성 도구인 GUI 기반 AnyConnect 프로파일 편집기를 사용하여 AnyConnect 클라이언트 프로파일을 생성할 수 있습니다. 독립형 프로파일 편집기를 사용하여 새로운 AnyConnect 프로파일을 만들거나 기존 프로파일을 수정할 수 있습니다. Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드할 수 있습니다.

자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드에서 해당 릴리스의 AnyConnect 프로파일 편집기 장을 참조하십시오.

시작하기 전에

- 원격 액세스 정책 마법사를 사용하여 Remote Access VPN을 구성하고 Firepower Threat Defense 디바이스에 구성을 구축했는지 확인합니다. 새 Remote Access VPN 정책 생성, 1166 페이지의 내용을 참조하십시오.
- Firepower Management Center 웹 인터페이스에서 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**로 이동하고 새 AnyConnect 클라이언트 이미지를 추가합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** 편집할 클라이언트 프로파일을 포함하는 연결 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **Edit Group Policy(**그룹 정책 편집**)** > **AnyConnect** > **Profiles(**프로파일**)**를 클릭합니다.

단계 **5** 목록에서 클라이언트 프로파일 XML 파일을 선택하거나 **Add(**추가**)**를 클릭하여 새 클라이언트 프로파일을 추가합니다.

단계 **6** 그룹 정책, 연결 프로파일 및 Remote Access VPN 정책을 저장합니다.

단계 **7** 변경 사항을 구축하고

클라이언트 프로파일에 대한 변경 사항은 VPN 클라이언트가 Remote Access VPN 게이트웨이에 연결할 때 업데이트됩니다.

관련 항목

그룹 정책 개체 설정, 656 페이지

Remote Access VPN 예시

사용자별 AnyConnect 대역폭을 제한하는 방법

이 섹션에서는 사용자가 Cisco AnyConnect VPN 클라이언트를 이용해 Firepower Threat Defense 원격 액세스 VPN 게이트웨이에 연결할 때, VPN 사용자가 사용하는 최대 대역폭을 제한하는 방법을 설명합니다. 단일 사용자 또는 사용자 그룹이 전체 리소스를 차지하지 않도록, Firepower Threat Defense에서 QoS(Quality of service)를 이용해 최대 대역폭을 제한할 수 있습니다. 이 구성을 이용하면 중요한 트래픽에 우선순위를 부여하고, 대역폭 독점을 방지하고, 네트워크를 관리할 수 있습니다. 트래픽이 최대 속도를 초과하면 Firepower Threat Defense에서 초과 트래픽을 취소합니다.

	수행해야 할 작업	추가 정보
1단계	영역을 만들고 설정합니다.	Active Directory 영역 생성 및 설정, 1219 페이지.
2단계	새로 생성한 영역에서 사용 가능한 사용자 또는 그룹에 대한 QoS 정책 및 QoS 규칙을 생성합니다.	QoS 정책 및 규칙 생성, 1220 페이지
3단계	원격 액세스 VPN 정책을 구성하고 사용자 인증을 위해 새로 생성한 영역을 선택합니다.	Remote Access VPN 정책 생성 또는 업데이트, 1221 페이지
4단계	원격 액세스 VPN 정책을 구축합니다.	컨피그레이션 변경 사항 구축, 498 페이지

Active Directory 영역 생성 및 설정

이 섹션에서는 영역을 생성하고, 활동을 모니터링할 VPN 사용자 및 사용자 그룹을 지정하는 방법을 설명합니다.

프로시저

단계 1 Firepower Management Center 웹 인터페이스에서 **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**를 선택합니다.

단계 2 **New realm(**새 영역**)**을 클릭하고, 영역 상세정보를 지정한 다음 **OK(**확인**)**를 클릭합니다.

단계 **3** 표시되는 탭에 필요한 상세정보를 입력하고 **Save(**저장**)**를 클릭합니다.

- **Directory(**디렉터리**)** - 한 영역에 하나 이상의 디렉터리를 지정할 수 있으며, 이 경우 사용자 제어를 위해 각 도메인 컨트롤러는 영역의 **Directory(**디렉터리**)** 페이지에 나열된 순서에 따라 사용자 및 그룹 인증서에 맞게 쿼리됩니다.

  영역 디렉터리 설정, 2475 페이지의 내용을 참조하십시오.

- **Realm Configuration(**영역 구성**)** - 영역을 생성하는 동안 입력한 영역 설정을 업데이트할 수 있습니다.

- **User Download(**사용자 다운로드**)** - 사용자와 그룹을 Firepower Management Center에 대한 다운로드 대상에 추가하거나 대상에서 제외할 수 있습니다.

단계 **4** **State(**상태**)**를 오른쪽으로 밀어 사용자 제어용으로 영역을 사용할 수 있게 합니다. 영역 관리, 2479 페이지의 내용을 참조하십시오.

단계 **5** 다운로드를 클릭해 사용자와 사용자 그룹을 Firepower Management Center에 다운로드합니다. 의 내용을 참조하십시오.사용자 및 그룹 다운로드, 2476 페이지의 내용을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

영역 생성, 2466 페이지

QoS 정책 및 규칙 생성

매니지드 디바이스의 속도 제한을 제어하기 위해 구축된 QoS 정책 영역을 선택해 QoS 정책을 생성하여 사용자나 사용자 그룹이 사용할 수 있는 VPN 대역폭을 제한할 수 있습니다. 각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)** > **QoS** > **New Policy(**새 정책**)**를 선택합니다.

단계 **2** **Name(**이름**)**을 입력하고 필요한 경우, **Description(**설명**)**을 입력합니다.

단계 **3** QoS 정책을 구축할 **Available Devices(**사용 가능한 디바이스**)**를 선택하고 **Add to Policy(**정책에 추가**)**를 클릭하거나, **Selected Devices(**선택한 디바이스**)**로 끌어다 놓습니다.

참고 원격 액세스 VPN 정책을 구축하려는 디바이스와 동일한 디바이스를 선택합니다. 정책을 구축하기 전에 디바이스를 할당해야 합니다.

단계 **4** QoS 정책 **Rules(**규칙**)**에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **5** **Name(**이름**)**을 입력합니다.

단계 **6** 규칙 구성 요소를 구성합니다.

- **Enabled(**활성화**)** - 규칙이 Enabled(활성화) 상태인지 여부를 지정합니다.

- **Apply QoS On(QoS** 적용 켜기**)** - 대상 인터페이스 개체의 인터페이스 또는 소스 인터페이스 개체의 인터페이스 중 속도를 제한하려는 인터페이스를 선택합니다. 이때 선택은 생성된 인터페이스 제약(Any(모든)이 아닌)에 일치해야 합니다.
- **Traffic Limit Per Interface(**인터페이스별 트래픽 제한**)** - Mbit/초 단위로 다운로드 제한 용량 및 업로드 제한 용량을 입력합니다. Unlimited(무제한) 기본값은 해당 방향의 일치하는 트래픽의 속도 제한을 방지합니다.
- **Users(**사용자**)** - **Users(**사용자**)** 탭을 클릭하고 VPN 트래픽을 제한할 새로 생성한 영역 및 사용자를 선택합니다. 추가할 조건에 해당하는 다른 탭을 클릭합니다. Apply QoS On(QoS 적용)에 대한 선택에 해당하는 소스 또는 대상 인터페이스 조건을 구성해야 합니다.
- **Comments(**코멘트**)** - Comments(코멘트) 탭을 클릭하고, 코멘트를 추가하고, **OK(**확인**)**를 클릭합니다.

단계 **7** 규칙을 저장합니다.

정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다. 규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

단계 **8** **Save**를 클릭하여 정책을 저장합니다.

관련 항목

QoS 정책 생성, 882 페이지
QoS 정책을 사용한 속도 제한, 881 페이지

Remote Access VPN 정책 생성 또는 업데이트

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 마법사를 사용하여 원격 액세스 VPN 정책을 생성합니다. 새로 생성한 영역을 인증 서버로 선택하거나 기존 원격 액세스 VPN 정책을 편집하고 다음을 수행합니다.

a) VPN 사용자에게 할당할 연결 프로파일을 선택하고 **Edit(**편집**)**을 클릭합니다.
b) **AAA** > **Authentication Method(**인증 방법**)** > **AAA or Certificate & AAA(AAA** 또는 인증서 및 **AAA)**를 선택합니다.
c) 필요한 영역을 인증 서버로 선택합니다.
d) 필요하다면 다른 연결 프로파일 옵션을 업데이트하고 연결 프로파일을 저장합니다.

단계 **3** 원격 액세스 VPN 정책에 필요한 구성을 완료하고 **Save(**저장**)**를 클릭합니다.

관련 항목

새 Remote Access VPN 연결 구성, 1165 페이지
연결 프로파일 설정, 1173 페이지

사용자 ID 기반 액세스 제어 규칙에 VPN ID를 사용하는 방법

	수행해야 할 작업	추가 정보
1단계	영역을 만들고 설정합니다.	Active Directory 영역 생성 및 설정, 1219 페이지.
2단계	ID 정책을 생성하고 ID 규칙을 추가합니다.	ID 정책 및 ID 규칙 생성, 1223 페이지.
3단계	ID 정책을 액세스 제어 정책과 연결합니다.	ID 정책을 액세스 제어 정책과 연결, 1223 페이지
4단계	원격 액세스 VPN 정책을 구성하고 사용자 인증을 위해 새로 생성한 영역을 선택합니다.	Remote Access VPN 정책 생성 또는 업데이트, 1221 페이지
5단계	원격 액세스 VPN 정책을 구축합니다.	컨피그레이션 변경 사항 구축, 498 페이지

Active Directory 영역 생성 및 설정

이 섹션에서는 영역을 생성하고, 활동을 모니터링할 VPN 사용자 및 사용자 그룹을 지정하는 방법을 설명합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**를 선택합니다.

단계 **2** **New realm(**새 영역**)**을 클릭하고, 영역 상세정보를 지정한 다음 **OK(**확인**)**를 클릭합니다.

단계 **3** 표시되는 탭에 필요한 상세정보를 입력하고 **Save(**저장**)**를 클릭합니다.

- **Directory(**디렉터리**)** - 한 영역에 하나 이상의 디렉터리를 지정할 수 있으며, 이 경우 사용자 제어를 위해 각 도메인 컨트롤러는 영역의 **Directory(**디렉터리**)** 페이지에 나열된 순서에 따라 사용자 및 그룹 인증서에 맞게 쿼리됩니다.

  영역 디렉터리 설정, 2475 페이지의 내용을 참조하십시오.

- **Realm Configuration(**영역 구성**)** - 영역을 생성하는 동안 입력한 영역 설정을 업데이트할 수 있습니다.

- **User Download(**사용자 다운로드**)** - 사용자와 그룹을 Firepower Management Center에 대한 다운로드 대상에 추가하거나 대상에서 제외할 수 있습니다.

단계 **4** **State(**상태**)**를 오른쪽으로 밀어 사용자 제어용으로 영역을 사용할 수 있게 합니다. 영역 관리, 2479 페이지의 내용을 참조하십시오.

단계 **5** 다운로드를 클릭해 사용자와 사용자 그룹을 Firepower Management Center에 다운로드합니다. 의 내용을 참조하십시오.사용자 및 그룹 다운로드, 2476 페이지의 내용을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

영역 생성, 2466 페이지

ID 정책 및 ID 규칙 생성

ID 정책에는 트래픽과 관련된 영역 및 인증 방법에 따라 사용자 인증을 수행하는 ID 규칙이 포함됩니다. ID 규칙은 트래픽 집합을 영역 및 인증 방법(패시브 인증, 활성 인증, 인증 없음)과 연결합니다. 사용하려는 영역 및 인증 방법을 완전히 구성해야 ID 규칙에서 해당 영역과 방법을 호출할 수 있습니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)**를 선택하고 **New Policy(**새 정책**)**를 클릭합니다.

단계 **2** **Name(**이름**)**과 **Description(**설명**)**을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **3** 정책에 규칙을 추가하려면 **Add Rule(**규칙 추가**)**를 클릭하고 **Name(**이름**)**을 입력합니다.

단계 **4** 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.

단계 **5** 기존 카테고리에 규칙을 추가하려면 규칙을 **Insert(**삽입**)**할 위치를 나타냅니다. 새 카테고리를 추가하려면 **Add Category(**카테고리 추가**)**를 클릭합니다.

단계 **6** 목록에서 규칙 **Action(**작업**)**을 선택하고 원격 액세스 VPN에서 소스 인터페이스로 구성한 인터페이스를 선택합니다.

단계 **7** **Realms & Settings(**영역 및 설정**)**를 클릭하고, **Realms(**영역**)** 목록에서 ID 규칙에 대해 생성한 새 영역을 선택합니다. 원격 액세스 VPN 정책에서 사용자 인증을 위해 선택한 것과 같은 영역을 선택했는지 확인합니다.

단계 **8** 선택한 영역에서 있는 사용자의 기본 설정을 구성하고 기타 필요한 규칙 옵션을 선택합니다.

단계 **9** **Add(**추가**)**를 클릭하여 규칙을 저장한 다음 ID 정책을 저장합니다.

관련 항목

ID 정책 생성 및 관리, 2529 페이지

ID 정책을 액세스 제어 정책과 연결

원격 액세스 VPN 정책을 구축할 Firepower Threat Defense 디바이스에 구축한 액세스 제어 정책을 ID 정책과 연결해야 합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** 필요한 액세스 제어 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.

단계 **3** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **4** **Identity Policy Settings(ID** 정책 설정**)** 영역에서 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **5** 드롭다운 목록에서 ID 정책을 선택합니다.

편집을 클릭하여 ID 정책을 수정할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

관련 항목

ID 정책 생성 및 관리, 2529 페이지

Remote Access VPN 정책 생성 또는 업데이트

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 **Devices(**디바이스**)**> **VPN** > **Remote Access(**원격 액세스**)**를 선택합니다.

단계 **2** 마법사를 사용하여 원격 액세스 VPN 정책을 생성합니다. 새로 생성한 영역을 인증 서버로 선택하거나 기존 원격 액세스 VPN 정책을 편집하고 다음을 수행합니다.

a) VPN 사용자에게 할당할 연결 프로파일을 선택하고 **Edit(**편집**)**을 클릭합니다.

b) **AAA** > **Authentication Method(**인증 방법**)** > **AAA or Certificate & AAA(AAA** 또는 인증서 및 **AAA)**를 선택합니다.

c) 필요한 영역을 인증 서버로 선택합니다.

d) 필요하다면 다른 연결 프로파일 옵션을 업데이트하고 연결 프로파일을 저장합니다.

단계 **3** 원격 액세스 VPN 정책에 필요한 구성을 완료하고 **Save(**저장**)**를 클릭합니다.

관련 항목

새 Remote Access VPN 연결 구성, 1165 페이지
연결 프로파일 설정, 1173 페이지

AnyConnect 관리 VPN 터널 구성

관리 VPN 터널은 VPN 사용자가 VPN에 연결하지 않고도 클라이언트 시스템의 전원을 켤 때마다 회사 네트워크에 대한 연결을 제공합니다. 이를 통해 조직은 소프트웨어 패치 및 업데이트를 통해 엔드포인트를 최신 상태로 유지할 수 있습니다. 사용자 시작 VPN 터널이 설정되면 관리 터널의 연결이 끊어집니다.

이 섹션에서는 FTD에서 AnyConnect 관리 VPN 터널을 구성하는 방법에 대해 설명합니다. FMC 웹 인터페이스를 사용하여 FTD에서 AnyConnect 관리 터널을 구성하려면 다음 설정이 필요합니다.

- 인증서 기반 인증 및 그룹 URL이 있는 연결 프로파일
- **AnyConnect** 관리 **VPN** 프로파일 파일, 필요한 경우 그룹 URL 및 백업 서버로 서버를 구성했습니다.
- 관리 VPN 프로파일이 포함된 그룹 정책, 명시적으로 포함된 네트워크가 포함된 스플릿 터널링, 클라이언트 바이 패스 프로토콜, 배너 없음

AnyConnect 관리 VPN 터널을 구성하는 자세한 지침은 FTD에서 AnyConnect 관리 VPN 터널 구성, 1226 페이지의 내용을 참조하십시오.

AnyConnect 관리 VPN 터널 요구 사항 및 사전 요건

소프트웨어 및 설정 요구 사항

FMC 웹 인터페이스를 통해 FTD를 사용하여 AnyConnect 관리 터널을 설정하기 전에 다음 사항을 확인하십시오.

- FTD 및 FMC 버전 6.7.0 이상을 사용하고 있는지 확인합니다.
- AnyConnect VPN Webdeploy 패키지 4.7 이상을 다운로드하여 FTD 원격 액세스 VPN에 업로드합니다.
- 인증서 인증이 연결 프로파일에 설정되어 있는지 확인합니다.
- 그룹 정책에 배너가 설정되어 있지 않은지 확인합니다.
- 관리 터널 그룹 정책에서 스플릿 터널링 설정을 확인합니다.

인증서 요구 사항

- FTD에는 원격 액세스 VPN에 대한 유효한 ID 인증서가 있어야 하며, 로컬 인증 기관(CA)의 루트 인증서가 FTD에 있어야 합니다.
- 관리 VPN 터널에 연결하는 엔드포인트에는 유효한 ID 인증서가 있어야 합니다.
- FTD의 ID 인증서에 대한 CA 인증서는 엔드포인트에 설치해야 하며, 엔드포인트에 대한 CA 인증서는 FTD에 설치해야 합니다.

- 동일한 로컬 CA에서 발급한 ID 인증서가 머신 저장소에 있어야 합니다.

  Windows의 경우에는 인증서 저장소고, macOS의 경우에는 시스템 키체인입니다.

AnyConnect 관리 VPN 터널의 제한 사항

- AnyConnect 관리 VPN 터널은 인증서 인증만 지원하며 AAA 기반 인증은 지원하지 않습니다.
- 공용 또는 프라이빗 프록시 설정은 지원되지 않습니다.
- 관리 VPN 터널이 연결되어 있으면 AnyConnect 클라이언트 업그레이드 및 AnyConnect 모듈 다운로드가 지원되지 않습니다.

FTD에서 AnyConnect 관리 VPN 터널 구성

프로시저

단계 **1** 마법사를 사용하여 원격 액세스 **VPN** 정책을 생성:

원격 액세스 VPN 구성에 대한 자세한 내용은 새 Remote Access VPN 연결 구성, 1165 페이지을 참조하십시오.

단계 **2** 관리 **VPN** 터널에 대한 연결 프로파일 설정을 구성:

참고 AnyConnect 관리 VPN 터널에만 사용할 새 연결 프로파일을 생성하는 것이 좋습니다.

a) 생성한 원격 액세스 VPN 정책을 수정합니다.
b) 관리 VPN 터널에 사용할 연결 프로파일을 선택하고 수정합니다.
c) **AAA** > **Authentication Method**(인증 방법)을 클릭하고 **Client Certificate Only**(클라이언트 인증서만)를 선택합니다. 필요에 따라 인증 및 계정 설정을 구성합니다.
d) 연결 프로파일의 **Aliases**(별칭) 탭을 클릭합니다.
e) 연결 프로파일에 대해 URL 별칭 아래에서 **Add**(+)(추가(+)) 그리고 **URL Alias**(URL 별칭)를 클릭합니다.
f) **Enabled**(활성화됨)를 클릭하여 URL을 활성화합니다.
g) **OK**(확인)를 클릭한 다음 **Save**(저장)를 클릭하여 연결 프로파일 설정을 저장합니다.

연결 프로파일 설정에 대한 자세한 내용은 연결 프로파일 설정, 1173 페이지의 내용을 참조하십시오.

단계 **3** **AnyConnect** 프로파일 편집기를 사용하여 관리 터널 프로파일을 생성:

a) **Cisco** 소프트웨어 다운로드 센터에서 AnyConnect VPN 관리 터널 독립형 프로파일 편집기를 아직 다운로드하지 않은 경우 다운로드합니다.
b) VPN 사용자에 대한 필수 설정으로 관리 터널 프로파일을 생성하고 파일을 저장합니다.
c) 연결 프로파일에서 구성한 그룹 URL을 사용하여 서버 목록의 서버를 구성합니다.

프로파일 편집기를 사용한 관리 프로파일 생성에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide*를 참조하십시오.

단계 **4** 관리 터널 개체 생성:

a) Firepower Management Center 웹 인터페이스에서 **Object(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**로 이동합니다
b) **Add AnyConnect File(AnyConnect** 파일 추가**)**을 클릭합니다.
c) AnyConnect 파일의 이름을 지정합니다.
d) **Browse(**찾아보기**)**를 클릭하고 저장한 관리 터널 프로파일 파일을 선택합니다.
e) **File Type(**파일 유형**)** 드롭 다운을 클릭하고 **AnyConnect Management VPN Profile (AnyConnect** 관리 **VPN** 프로필**)**을 선택합니다.
f) **Save(**저장**)**를 클릭합니다.

참고 또한 그룹 정책에 대한 AnyConnect 설정을 생성하거나 업데이트할 때 관리 터널 개체를 생성합니다. 그룹 정책 AnyConnect 옵션, 659 페이지의 내용을 참조하십시오.

단계 **5** 관리 프로파일을 그룹 정책과 연결하고 그룹 정책 설정을 구성:

관리 터널 VPN 연결에 사용되는 연결 프로파일과 연결된 그룹 정책에 관리 VPN 프로파일을 추가해야 합니다. 사용자가 연결하면 그룹 정책에 이미 매핑된 사용자 VPN 프로파일과 함께 관리 VPN 프로파일이 다운로드되어 관리 VPN 터널 기능을 활성화합니다.

주의 **No Banner(**배너 없음**)**: 그룹 정책 설정에 배너가 구성되어 있지 않은지 확인합니다. **Group Policy(**그룹 정책**)** > **General Settings(**일반 설정**)** > **Banner(**배너**)**에서 배너 설정을 확인할 수 있습니다.

a) 관리 VPN 터널 용으로 생성한 연결 프로파일을 수정합니다.
b) **Edit Group Policy(**그룹 정책 편집**)** > **AnyConnect** > **Management Profiles(**관리 프로파일**)**를 클릭합니다.
c) **Management VPN Profile(**관리 **VPN** 프로파일**)** 드롭 다운을 클릭하고 생성한 관리 프로파일 파일 개체를 선택합니다.

참고 +를 클릭하고 새 AnyConnect 관리 VPN 프로파일 개체를 추가할 수도 있습니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **6** 그룹 정책에서 스플릿 터널링 구성:

a) **Edit Group Policy(**그룹 정책 편집**)** > **General(**일반**)** > **Split Tunneling(**스플릿 터널링**)**을 클릭합니.
b) IPv4 또는 IPv6 스플릿 터널링 드롭 다운에서 **Tunnel networks specified below(**아래 지정된 터널 네트워크**)**를 선택합니다.
c) 스플릿 터널 네트워크 목록 유형, 즉 **Standard Access List(**표준 액세스 목록**)** 또는 **Extended Access List(**확장 액세스 목록**)**를 선택한 다음 관리 VPN 터널을 통한 트래픽을 허용하는 데 필요한 액세스 목록을 선택합니다.
d) 스플릿 터널 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

AnyConnect 맞춤형 속성

AnyConnect 관리 VPN 터널에는 기본적으로 스플릿에 터널링 구성이 포함되어야 합니다. 모든 터널링을 위해 스플릿 터널링이 포함된 관리 VPN 터널을 구축하도록 그룹 정책에서 AnyConnect 맞춤 속성을 구성하는 경우 FMC 6.7 웹 인터페이스가 AnyConnect 맞춤 속성을 지원하지 않으므로 FlexConfig를 사용하여 해당 구성을 수행할 수 있습니다.

다음은 AnyConnect 맞춤 속성에 대한 명령 예입니다.

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

단계 **7** 원격 액세스 **VPN** 정책 구축**,** 확인 및 모니터링:

a) 관리 VPN 터널 구성을 FTD에 구축합니다.

참고 클라이언트 시스템은 관리 터널 VPN 프로파일을 클라이언트 머신에 다운로드하려면 FTD 원격 액세스 VPN에 한 번 연결해야 합니다.

b) **AnyConnect Secure Mobility Client** > **VPN** > **Statistics(**통계**)**에서 AnyConnect 관리 VPN 터널을 확인할 수 있습니다.

show vpn-sessiondb anyconnect 명령을 사용하여 FTD 명령 프롬프트에서 관리 VPN 세션 세부 정보를 확인할 수도 있습니다.

c) FMC 웹 인터페이스에서 **Analysis(**분석**)**를 클릭하여 관리 터널 세션 정보를 확인합니다.

관련 항목

연결 프로파일 설정, 1173 페이지
FTD 그룹 정책 개체, 656 페이지

원격 액세스 VPN 히스토리

기능	버전	세부 사항
다중 인증서 인증	7.0	Firepower Management Center 다중 인증서 기반 인증을 통해 FTD는 사용자의 ID 인증서를 인증하는 것 외에도 머신 또는 디바이스 인증서를 검증, 즉 디바이스가 기업 발행 디바이스라는 점을 보장하고 AnyConnect 클라이언트를 사용하여 RAVPN 액세스를 허용합니다.

기능	버전	세부 사항
VPN 로드 밸런싱	7.0	VPN로드 밸런싱은 둘 이상의 디바이스를 논리적으로 그룹화하고 처리량 및 기타 트래픽 매개변수를 고려하지 않고 그룹화된 디바이스간에 원격 액세스 VPN 세션을 동일하게 분산합니다.
AnyConnect 맞춤형 속성	7.0	Firepower Management Center AnyConnect 맞춤형 속성을 지원하며, FTD에서 이러한 기능에 대한 하드 코딩된 지원을 추가하지 않고도 AnyConnect 클라이언트 기능을 구성할 수 있는 인프라를 제공합니다.
선택적 정책 구축	7.0	이제 구축 중에 원격 액세스 VPN 및 사이트 대 사이트 VPN 구성에 대한 변경 사항을 포함하거나 제외하도록 선택할 수 있습니다.
AnyConnect 모듈 구성 지원	6.7	Firepower Management Center 이제 추가 보안을 위해 AnyConnect 모듈 및 프로파일을 구성할 수 있습니다.
LDAP 권한 부여 지원	6.7	Firepower Management Center를 사용하여 원격 액세스 VPN에 대한 LDAP 권한 부여를 구성할 수 있습니다.
원격 액세스 VPN에 대한 SAML SSO(Single Sign-On) 지원	6.7	원격 액세스 VPN에 대한 인증서버로 SAML 2.0 서버를 구성할 수 있습니다.
AnyConnect 관리 VPN 터널 지원	6.7	FTD 원격 액세스 VPN은 VPN 사용자가 VPN에 연결하지 않고도 회사 엔드포인트의 전원을 켤 때 엔드포인트에 대한 VPN 연결을 허용하는 AnyConnect 관리 VPN 터널 구성을 지원합니다.
DTLS(Datagram Transport Layer Security) 1.2 지원	6.6	DTLS 1.2는 이제 기본 SSL 암호 그룹의 일부이며 TLS 1.2와 함께 구성할 수 있습니다.

46 장

Firepower Threat Defense VPN 모니터링

이 장에서는 Firepower Threat Defense VPN 모니터링 툴, 파라미터 및 통계 정보에 대해 설명합니다.

- VPN 요약 대시보드, 1231 페이지
- VPN 세션 및 사용자 정보, 1232 페이지
- VPN 상태 이벤트, 1233 페이지

VPN 요약 대시보드

Firepower System 대시보드는 시스템에 의해 수집 및 생성된 이벤트에 대한 데이터를 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기를 제공합니다. VPN 대시보드를 사용하여 현재 사용자 상태, 디바이스 유형, 클라이언트 애플리케이션, 사용자 위치 정보 및 연결 기간을 포함하여 VPN 사용자에 대한 통합 정보를 볼 수 있습니다.

VPN 요약 대시보드 보기

Remote Access VPN은 원격 사용자(예: 휴대폰 사용자 또는 재택 근무자)에 대한 보안 연결을 제공합니다. 이러한 연결을 모니터링하면 연결 및 사용자 세션 성능에 대한 중요한 지표를 얻을 수 있습니다.

이 작업을 수행하려면 리프 도메인의 관리자 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Access Controlled User Statistics(**액세스 제어 사용자 통계**)** > **VPN**을 선택합니다.

단계 **2** 다음과 같은 Remote Access VPN 정보 위젯을 확인합니다.

- 지속기간별 현재 VPN 사용자
- 클라이언트 애플리케이션별 현재 VPN 사용자
- 디바이스별 현재 VPN 사용자
- 전송된 데이터별 VPN 사용자

- 지속기간별 VPN 사용자
- 클라이언트 애플리케이션별 VPN 사용자
- 클라이언트 국가별 VPN 사용자

다음에 수행할 작업

VPN 대시보드는 철저 한 데이터를 제공 하는 복잡 한 사용자 정의 가능한 모니터링 기능입니다.

- Firepower System에서 대시보드를 사용하는 방법에 대한 자세한 내용은 대시보드, 363 페이지 섹션을 참조하십시오.
- VPN 대시보드 위젯을 수정하는 방법에 대한 자세한 내용은 위젯 환경설정 구성, 380 페이지 섹션을 참조하십시오.

VPN 세션 및 사용자 정보

Firepower System은 네트워크에서 VPN 관련 활동을 포함한 사용자 활동의 세부사항을 전달하는 이벤트를 생성합니다. Firepower System 모니터링 기능을 통해 Remote Access VPN 문제가 있는지 여부와 존재 여부를 신속하게 확인할 수 있습니다. 그런 다음 이 정보를 적용하고 네트워크 관리 도구를 사용하여 네트워크 및 사용자의 문제를 줄이거나 없앨 수 있습니다. 필요한 경우 Remote Access VPN 사용자를 로그아웃할 수도 있습니다(선택 사항).

Remote Access VPN 활성 세션 보기

Analysis(분석) > Users(사용자) > Active Sessions(활성 세션)

사용자 이름, 로그인 기간, 인증 유형, 할당/공용 IP 주소, 디바이스 상세정보, 클라이언트 버전, 엔드포인트 정보, 처리량, 대역폭 소비 그룹 정책, 터널 그룹 등과 같은 지원 정보를 사용하여 현재 로그인한 VPN 사용자를 특정 시점에서 볼 수 있습니다. 또한 시스템은 현재 사용자 정보를 필터링하고 사용자를 로그아웃하며 요약 목록에서 사용자를 삭제하는 기능을 제공합니다.

참고 고가용성 구축에서 VPN을 구성한 경우 활성 VPN 세션에 대해 표시되는 디바이스 이름은 사용자 세션을 식별한 기본 또는 보조 디바이스일 수 있습니다.

- 활성 세션에 대한 자세한 내용은 활성 세션 데이터 보기, 3083 페이지 섹션을 참조하십시오.
- 활성 세션 테이블의 열에 대한 내용을 자세히 알아보십시오(활성 세션, 사용자 및 사용자 활동 데이터, 3076 페이지 참조).

Remote Access VPN 사용자 활동 보기

Analysis(분석) > Users(사용자) > User Activity(사용자 활동)

네트워크에서 사용자 활동의 상세정보를 볼 수 있습니다. 시스템은 기록 이벤트를 기록하고 연결 프로파일 정보, IP 주소, 지오로케이션 정보, 연결 기간, 처리량 및 디바이스 정보와 같은 VPN 관련 정보를 포함합니다.

- 사용자 활동에 대한 자세한 내용은 사용자 활동 데이터 보기, 3089 페이지 섹션을 참조하십시오.
- 사용자 활동 테이블의 열에 대한 내용을 자세히 알아보십시오(활성 세션, 사용자 및 사용자 활동 데이터, 3076 페이지 참조).

VPN 상태 이벤트

Health Events(상태 이벤트) 페이지에서는 irepower Management Center의 상태 모니터에서 기록한 VPN 상태 이벤트를 볼 수 있습니다. Firepower System 디바이스 간에 하나 이상의 VPN 터널이 다운되면 다음 이벤트가 추적됩니다.

- 다음에 대한 VPN 7000 및 8000 Series
- Site-to-Site VPN Firepower Threat Defense
- 원격 액세스 VPN Firepower Threat Defense

상태 모니터를 사용하여 Firepower System 구축에서 중요한 기능의 상태를 확인하는 방법에 대한 자세한 내용은 상태 모니터링, 387 페이지 섹션을 참조하십시오.

VPN 상태 이벤트 보기

Firepower Management Center의 Health Events(상태 이벤트) 페이지에서 상태 이벤트에 액세스하면 모든 관리되는 어플라이언스에 대한 모든 상태 이벤트가 검색됩니다. 확인하려는 상태 이벤트를 생성한 모듈을 지정하여 이벤트 범위를 좁힐 수 있습니다.

이 작업을 수행하려면 관리자, 유지 보수 사용자 또는 보안 분석가여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Events(**이벤트**)**를 선택합니다.

단계 **2** **Module Name(**모듈 이름**)** 열에서 **VPN Status(VPN** 상태**)**를 선택합니다.

시스템 상태 이벤트에 대한 자세한 내용은 상태 이벤트 보기, 421 페이지 섹션을 참조하십시오.

47 장

Firepower Threat Defense VPN 문제 해결

이 장에서는 Firepower Threat Defense VPN 문제 해결 툴 및 디버그 정보에 대해 설명합니다.

- 시스템 메시지, 1235 페이지
- VPN 시스템 로그, 1235 페이지
- 디버그 명령, 1236 페이지

시스템 메시지

Message Center는 문제 해결을 시작할 수있는 장소입니다. 이 기능을 사용하면 지속적으로 생성되는 시스템 활동 및 상태에 대한 메시지를 볼 수 있습니다. Message Center를 열려면 메인 메뉴의 **Deploy(**구축**)** 버튼 오른쪽의 **System Status(**시스템 상태**)**를 클릭합니다. Message Center 사용에 대한 자세한 내용은 시스템 메시지, 441 페이지 섹션을 참조하십시오.

VPN 시스템 로그

FTD 디바이스에 대한 시스템 로그를 활성화할 수 있습니다. 기록 정보는 네트워크 또는 디바이스 구성 관련 문제를 식별하고 격리하는 데 도움이 됩니다. VPN 기록을 활성화하면 이러한 시스템 로그가 분석 및 보관을 위해 FTD 디바이스에서 Firepower Management Center로 전송됩니다.

표시되는 VPN 시스템 로그의 기본 심각도는 'ERROR' 이상입니다(변경되지 않은 경우). VPN 기록은 FTD 플랫폼 설정을 통해 관리됩니다. 대상 디바이스(**Platform Settings(**플랫폼 설정**)** > **Syslog(**시스템 로그**)** > **Logging Setup(**기록 설정**)**에 대한 FTD 플랫폼 설정 정책에서 **VPN Logging Settings(VPN** 기록 설정**)**를 편집하여 메시지 심각도 수준을 조정할 수 있습니다. VPN 기록 활성화, 시스템 로그 서버 구성 및 시스템 로그 보기에 대한 자세한 내용은 시스템 로그 구성 관련 정보, 1445 페이지 섹션을 참조하십시오.

참고 디바이스가 Site-to-Site VPN 또는 Remote Access VPN으로 구성될 때마다 기본적으로 VPN 시스템 로그가 Firepower Management Center에 자동으로 전송되도록 설정됩니다.

VPN 시스템 이벤트 로그 보기

Firepower System은 VPN 문제의 소스에 대한 추가 정보를 수집하는 데 도움이 되는 이벤트 정보를 수집합니다. 표시되는 VPN 시스템 로그의 기본 심각도는 'ERROR' 이상입니다(변경되지 않은 경우). 기본적으로 행은 **Time(**시간**)** 열에 따라 정렬됩니다.

이 작업을 수행하려면 리프 도메인의 관리자 사용자여야 합니다.

시작하기 전에

FTD 플랫폼 설정(**Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Syslog(**시스템 로그**)** > **Logging Setup(**기록 설정**)**)에서 **Enable Logging to FMC(FMC**에 대한 기록 활성화**)** 확인란을 선택하여 VPN 기록을 활성화합니다. VPN 기록 활성화, 시스템 로그 서버 구성 및 시스템 로그 보기에 대한 자세한 내용은 시스템 로그 구성 관련 정보, 1445 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Troubleshooting(**문제 해결**)**을 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Search(검색) - 현재 메시지 정보를 필터링하려면 **Edit Search(**검색 편집**)**를 클릭합니다.
- View(보기) - 보기에서 선택된 메시지와 관련된 VPN 상세정보를 보려면 **View(**보기**)**를 클릭합니다.
- View All(모두 보기) - 보기에서 모든 메시지에 대한 VPN 상세정보를 보려면 **View All(**모두 보기**)**을 클릭합니다.
- Delete(삭제) - 데이터베이스에서 선택한 메시지를 삭제하려면 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 모든 메시지를 삭제합니다.

디버그 명령

이 섹션에서는 디버그 명령을 사용하여 VPN 관련 문제점을 진단하고 해결하는 방법을 설명합니다. 이 섹션에서 사용 가능한 모든 디버그 명령을 설명하지는 않습니다. 여기에 있는 명령은 VPN 관련 문제점을 진단하는 데 도움이 되는 유용성에 따라 포함되어 있습니다.

사용 가이드라인

디버깅 출력은 CPU 프로세스에서 높은 우선순위가 할당되기 때문에 시스템을 사용할 수 없게 만들 수 있습니다. 따라서 **debug** 명령은 특정 문제를 해결하는 경우나 Cisco TAC(Technical Assistance Center)를 통한 문제 해결 세션 중에만 사용해야 합니다. 또한, 네트워크 트래픽과 사용자 수가 적은 기간에 **debug** 명령을 사용하는 것이 가장 좋습니다. 그러한 기간에 디버깅하면 **debug** 명령의 처리 오버헤드 증가로 인해 시스템 사용에 지장이 생길 가능성이 줄어듭니다.

디버그 출력은 CLI 세션에서만 확인할 수 있습니다. 콘솔 포트에 연결하거나 **system support diagnostic-cli**를 입력하여 진단 CLI를 사용할 때는 출력을 직접 사용할 수 있습니다. **show console-output** 명령을 사용하여 일반 Firepower Threat Defense CLI에서 출력을 확인할 수도 있습니다.

지정된 기능에 대한 디버깅 메시지를 표시하려면 **debug** 명령을 사용합니다. 디버그 메시지의 표시를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. **no debug all**은 모든 디버깅 명령을 끄는 데 사용합니다.

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

feature	디버깅을 활성화하려는 기능을 지정합니다. 사용 가능한 기능을 보려면 CLI 도움말에 대한 **debug ?** 명령을 사용합니다.
subfeature	(선택 사항) 기능에 따라 하나 이상의 하위 기능에 대한 디버그 메시지를 활성화할 수 있습니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
level	(선택 사항) 디버깅 레벨을 지정합니다. 모든 기능에서 이 레벨을 사용할 수 있는 것은 아닙니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

Command Default

기본 디버깅 레벨은 1입니다.

예

원격 액세스 VPN에서 실행 중인 다중 세션에서는 지정된 로그의 크기 때문에 문제 해결이 어려울 수 있습니다. **debug webvpn condition** 명령을 사용하여 더 정확하게 디버그 프로세스를 대상으로 필터를 설정할 수 있습니다.

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

여기서 각 항목은 다음을 나타냅니다.

- 그룹 정책(터널 그룹 또는 연결 프로파일 이외)의 **group** *name* 필터.
- 클라이언트의 공용 IP 주소에 대한 **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] 필터. 서브넷 마스크(IPv4용) 또는 접두사(IPv6용)는 선택 사항입니다.
- **reset** 모든 필터 재설정. **no debug webvpn condition** 명령을 사용하여 특정 필터를 끌 수 있습니다.
- 사용자 이름을 기준으로 하는 **user** *name* 필터.

조건을 여러 개 구성하는 경우 조건이 결합되어(AND로 처리되어) 모든 조건이 충족될 경우에만 디버그가 표시됩니다.

조건 필터를 설정한 후 기본 **debug webvpn** 명령을 사용하여 디버그를 켭니다. 조건을 설정하는 것만으로 디버그가 활성화되지는 않습니다. 현재 디버깅 상태를 보려면 **show debug** 및 **show webvpn debug-condition** 명령을 사용합니다.

다음은 사용자 jdoe에 대해 조건부 디버그를 활성화하는 예를 보여줍니다.

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
```

```
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Related Commands

Command(명령)	설명
show debug	현재 활성 디버그 설정을 표시합니다.
undebug	기능에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug**에 대한 동의어입니다.

debug aaa

인증, 권한 부여 및 계정(AAA, "트리플 A"로 발음)과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *aaa* [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Syntax Description

aaa	AAA 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
accounting	(선택 사항) AAA 계정 디버깅을 활성화합니다.
authentication	(선택 사항) AAA 인증 디버깅을 활성화합니다.
authorization	(선택 사항) AAA 권한 부여 디버깅을 활성화 합니다.
common	(선택 사항) 일반적인 AAA 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
internal	(선택 사항) AAA 내부 디버깅을 활성화합니다.
shim	(선택 사항) AAA shim 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
url-redirect	(선택 사항) AAA url-redirect 디버깅을 활성화합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug aaa	AAA의 현재 활성 디버그 설정을 표시합니다.
undebug aaa	AAA 디버깅을 비활성화합니다. 이 명령은 **no debug aaa**에 대한 동의어입니다.

debug crypto

암호화와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto* [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Syntax Description

crypto	*crypto* 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
ca	(선택 사항) PKI 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
condition	(선택 사항) IPsec/ISAKMP 디버그 필터를 지정합니다. ?를 사용하여 사용 가능한 필터를 확인합니다.
engine	(선택 사항) Crypto engine 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ike-common	(선택 사항) 일반적인 IKE 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ikev1	(선택 사항) IKE 버전 1 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ikev2	(선택 사항) IKE 버전 2 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ipsec	(선택 사항) IPsec 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
condition	(선택 사항) Crypto Secure Socket API 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
vpnclient	(선택 사항) EasyVPN 클라이언트 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto	crypto ca의 현재 활성 디버그 설정을 표시합니다.
undebug crypto	crypto ca 디버깅을 비활성화합니다. 이 명령은 **no debug crypto**에 대한 동의어입니다.

debug crypto ca

crypto ca와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Syntax Description

crypto ca	*crypto ca*에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
cluster	(선택 사항) PKI 클러스터 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
cmp	(선택 사항) CMP 트랜잭션 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
messages	(선택 사항) PKI 입/출력 메시지 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
periodic-authentication	(선택 사항) PKI periodic-authentication 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
scep-proxy	(선택 사항) SCEP 프록시 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
server	(선택 사항) 로컬 CA 서버 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
transactions	(선택 사항) PKI 트랜잭션 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
trustpool	(선택 사항) 신뢰 풀 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto ca	crypto ca의 현재 활성 디버그 설정을 표시합니다.

Command(명령)	설명
undebug	crypto ca에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ca**에 대한 동의어입니다.

debug crypto ikev1

Internet Key Exchange 버전 1(IKEv1)과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ikev1* [*timers*] [*1-255*]

Syntax Description

ikev1	*ikev1*에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
timers	(선택 사항) IKEv1 타이머에 대한 디버깅을 활성화합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto ikev1	IKEv1에 대한 현재 활성 디버그 설정을 표시합니다.
undebug crypto ikev1	IKEv1에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ikev1**에 대한 동의어입니다.

debug crypto ikev2

Internet Key Exchange 버전 2(IKEv2)와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ikev2* [*ha* | *platform* | *protocol* | *timers*]

Syntax Description

ikev2	*ikev2* 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
ha	(선택 사항) IKEv2 HA 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
platform	(선택 사항) IKEv2 플랫폼 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
protocol	(선택 사항) IKEv2 프로토콜 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

timers	(선택 사항) IKEv2 타이머에 대한 디버깅을 활성화합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto ikev2	IKEv2에 대한 현재 활성 디버그 설정을 표시합니다.
undebugcrypto ikev2	IKEv2에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ikev2**에 대한 동의어입니다.

debug crypto ipsec

IPsec과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ipsec* [*1-255*]

Syntax Description

ipsec	*ipsec*에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto ipsec	IPsec에 대한 현재 활성 디버그 설정을 표시합니다.
undebugcrypto ipsec	IPsec에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ipsec**에 대한 동의어입니다.

debug ldap

LDAP(Lightweight Directory Access Protocol)와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *ldap* [*1-255*]

Syntax Description

ldap	LDAP에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug ldap	LDAP에 대한 현재 활성 디버그 설정을 표시합니다.
undebugldap	LDAP에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug ldap**에 대한 동의어입니다.

debug ssl

SSL 세션과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *ssl* [*cipher* | *device*] [*1-255*]

Syntax Description

ssl	SSL 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
cipher	(선택 사항) SSL 암호 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
device	(선택 사항) SSL 디바이스 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug ssl	SSL의 현재 활성 디버그 설정을 표시합니다.
undebug ssl	SSL 디버깅을 비활성화합니다. 이 명령은 **no debug ssl**에 대한 동의어입니다.

debug webvpn

WebVPN과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Syntax Description

webvpn	WebVPN 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
anyconnect	(선택 사항) WebVPN AnyConnect 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

chunk	(선택 사항) WebVPN chunk 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
cifs	(선택 사항) WebVPN CIFS 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
citrix	(선택 사항) WebVPN Citrix 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
compression	(선택 사항) WebVPN 압축 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
condition	(선택 사항) WebVPN 필터 조건 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
cstp-auth	(선택 사항) WebVPN CSTP 인증 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
customization	(선택 사항) WebVPN customization 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
failover	(선택 사항) WebVPN 페일오버 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
html	(선택 사항) WebVPN HTML 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
javascript	(선택 사항) WebVPN Javascript 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
kcd	(선택 사항) WebVPN KCD 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
listener	(선택 사항) WebVPN 리스너 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
mus	(선택 사항) WebVPN MUS 디버그 레벨을 지정 합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
nfs	(선택 사항) WebVPN NFS 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
request	(선택 사항) WebVPN 요청 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
response	(선택 사항) WebVPN 응답 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
saml	(선택 사항) WebVPN SAML 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

session	(선택 사항) WebVPN 세션 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
task	(선택 사항) WebVPN 작업 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
transformation	(선택 사항) WebVPN 변환 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
url	(선택 사항) WebVPN URL 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
util	(선택 사항) WebVPN 유틸리티 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
xml	(선택 사항) WebVPN XML 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug webvpn	WebVPN의 현재 활성 디버그 설정을 표시합니다.
undebug webvpn	WebVPN 디버깅을 비활성화합니다. 이 명령은 **no debug webvpn**에 대한 동의어입니다.

XI 부

Firepower Threat Defense 고급 설정

- Threat Defense Service 정책, 1249 페이지
- Firepower Threat Defense에 대한 FlexConfig 정책, 1269 페이지
- Cisco ISA 3000에 대한 알람, 1323 페이지

48 장

Threat Defense Service 정책

특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 구성을 만드는 서비스 정책을 사용할 수 있습니다. 서비스 정책은 인터페이스에 적용되거나 전역으로 적용되는 여러 작업 또는 규칙으로 구성됩니다.

- Firepower Threat Defense Service 정책 정보, 1249 페이지
- 서비스 정책을 위한 요구 사항 및 사전 요건, 1251 페이지
- 서비스 정책 가이드라인 및 제한 사항, 1252 페이지
- Firepower Threat Defense Service 정책 설정, 1252 페이지
- 서비스 정책 규칙 예시, 1261 페이지
- 서비스 정책 모니터링, 1267 페이지
- Firepower Threat Defense Service 정책 기록, 1268 페이지

Firepower Threat Defense Service 정책 정보

특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 서비스 정책을 사용하면 디바이스 또는 특정 인터페이스에 진입하는 모든 연결에 동일한 서비스를 적용하는 데 제한이 없습니다.

트래픽 클래스는 인터페이스와 확장 ACL(액세스 제어 목록)의 조합입니다. ACL "허용" 규칙은 클래스에 속한 연결을 확인합니다. ACL의 "거부" 트래픽에는 서비스가 적용되지 않았으며 이러한 연결은 실제로 삭제되지 않습니다. IP 주소와 TCP/UDP 포트를 사용하여 필요에 따라 일치하는 연결을 식별할 수 있습니다.

두 가지 유형의 트래픽 클래스는 다음과 같습니다.

- 인터페이스 기반 규칙 - 서비스 정책 규칙에 보안 영역 또는 인터페이스 그룹을 지정하는 경우 이 규칙은 인터페이스 개체의 일부인 인터페이스를 통과하는 ACL "허용" 트래픽에 적용됩니다.

  지정된 기능의 경우 인그레스 인터페이스에 적용된 인터페이스 기반 규칙이 항상 전역 규칙보다 우선합니다. 즉, 인그레스 인터페이스 기반 규칙이 연결에 적용되는 경우 일치하는 전역 규칙은 무시됩니다. 인그레스 인터페이스 또는 전역 규칙이 적용되지 않으면 이그레스 인터페이스의 인터페이스 서비스 규칙이 적용됩니다.

- 전역 규칙 - 이 규칙은 모든 인터페이스에 적용됩니다. 인터페이스 기반 규칙이 연결에 적용되지 않으면 전역 규칙이 검사되며 ACL에서 "허용"하는 모든 연결에 적용됩니다. 아무 것도 적용되지 않는 경우 서비스의 적용 없이 연결이 진행됩니다.

지정된 연결은 지정된 기능에 대해 인터페이스 기반 또는 전역 중 하나의 트래픽 클래스만 일치시킬 수 있습니다. 지정된 인터페이스 개체/트래픽 흐름 조합에 대한 규칙이 적어도 하나는 있어야 합니다.

서비스 정책 규칙은 액세스 제어 규칙 이후에 적용됩니다. 이러한 서비스는 허용된 연결에 대해서만 구성됩니다.

서비스 정책과 FlexConfig 및 기타 기능의 관계

버전 6.3(0) 이전에는 TCP_Embryonic_Conn_Limit 및 TCP_Embryonic_Conn_Timeout 사전 정의된 FlexConfig 개체를 사용하여 연결 관련 서비스 규칙을 구성할 수 있었습니다. Firepower Threat Defense Service 정책을 사용하여 이러한 개체를 제거하고 규칙을 다시 실행해야 합니다. 이러한 연결 관련 기능(**set connection** 명령)을 구현하기 위해 사용자 정의 FlexConfig 개체를 생성한 경우 해당 개체를 제거하고 서비스 정책을 통해 기능을 구현해야 합니다.

연결 관련 서비스 정책 기능은 다른 서비스 규칙 구현 기능과는 별도의 기능 그룹으로 처리되므로 중복되는 트래픽 클래스 문제가 발생하지 않아야 합니다. 하지만 다음과 같이 구성할 때 주의를 기울여야 합니다.

- QoS 정책 규칙은 서비스 정책 CLI를 사용하여 구현됩니다. 이러한 규칙은 연결 기반 서비스 정책 규칙보다 먼저 적용됩니다. 하지만 QoS 및 연결 설정은 동일하거나 중복되는 트래픽 클래스에 적용될 수 있습니다.
- FlexConfig 정책을 사용하여 사용자 정의 애플리케이션 검사 및 NetFlow를 구현할 수 있습니다. **show running-config** 명령을 사용하여 **policy-map**, **class-map**, **service-policy** 명령을 포함하여 서비스 규칙을 이미 구성하는 CLI를 검사하십시오. Netflow 및 애플리케이션 검사는 QoS 및 연결 설정과 호환되지만 FlexConfig를 구현하기 전에 기존 구성을 이해해야 합니다. 연결 설정은 애플리케이션 검사 및 Netflow 전에 적용됩니다.

참고 Firepower Threat Defense Service 정책에서 생성된 트래픽 클래스의 이름은 **class_map_***ACLname*입니다. 여기서 *ACLname*은 서비스 정책 규칙에 사용된 확장 ACL 개체의 이름입니다.

연결 설정이란?

연결 설정은 Firepower Threat Defense 디바이스를 통한 TCP 흐름 등 트래픽 연결 관리에 관련된 다양한 기능으로 구성되어 있습니다. 일부 기능은 특정 서비스 제공을 구성하는 구성 요소로 이름이 지정되어 있습니다.

연결 설정은 다음과 같습니다.

- **Global timeouts for various protocols(**다양한 프로토콜을 위한 전역 시간 제한**)** - 모든 전역 시간 제한에는 기본값이 있으므로 예기치 않은 연결 손실이 발생한 경우에만 전역 시간 제한을 변경

해야 합니다. Firepower Threat Defense Platform 정책에서 전역 시간 초과를 구성합니다. **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택합니다.

- **Connection timeouts per traffic class(**트래픽 클래스당 연결 시간 제한**)** - 서비스 정책을 사용하여 특정 트래픽 유형에 전역 시간 제한을 재정의할 수 있습니다. 트래픽 클래스 시간 제한에는 모두 기본값이 있으므로 따로 설정하지 않아도 됩니다.
- **Connection limits and TCP Intercept(**연결 제한 및 **TCP** 가로채기**)** - 기본적으로 Firepower Threat Defense 디바이스를 통과하거나 이동할 수 있는 연결 수에는 제한이 없습니다. DoS(서비스 거부) 공격으로부터 서버를 보호하기 위해 서비스 정책 규칙을 사용하여 특정 트래픽 클래스에 제한을 설정할 수 있습니다. 특히 TCP 핸드셰이크를 완료하지 않은 원시 연결에 제한을 설정하면 SYN 플러딩 공격을 방지할 수 있습니다. 원시 연결 시간 제한이 초과되면 TCP 가로채기 구성 요소가 프록시 연결에 개입하여 공격을 제한합니다.
- **Dead Connection Detection (DCD)(**끊어진 연결 탐지**(DCD))** - 유효하지만 종종 유휴 상태가 되는 지속 연결이 있고 이러한 연결이 유휴 시간 제한 설정을 초과해 닫히는 경우, DCD(Dead Connection Detection)를 활성화하여 유휴 타이머를 재설정함으로써 유휴 상태지만 유효한 연결을 식별하고 유지할 수 있습니다. 유휴 시간이 초과되면 DCD가 연결의 양쪽을 프로브하여 양쪽 연결 모두 연결이 유효한 것에 동의하는지 확인합니다. **show service-policy** 명령 출력은 DCD의 작업 양을 표시하는 카운터를 포함합니다. **show conn detail** 명령을 사용하여 이니시에이터 및 응답자 관련 정보와 프로브 전송 빈도를 확인할 수 있습니다.
- **TCP sequence randomization(TCP** 시퀀스 임의 설정**)** - 각 TCP 연결에는 각각 클라이언트와 서버에서 생성된 두 개의 ISN(초기 시퀀스 번호)이 있습니다. 기본적으로 Firepower Threat Defense 디바이스는 인바운드와 아웃바운드 두 방향 모두로 전달되는 TCP SYN의 ISN을 임의로 설정합니다. ISN을 임의로 설정하면 공격자가 새 연결을 위한 다음 ISN을 예측하지 못하며 잠재적으로 새 세션의 가로채기가 방지됩니다. 원하는 경우 트래픽 클래스별 임의 설정을 비활성화할 수 있습니다.
- **TCP Normalization(TCP** 정규화**)** - TCP 노멀라이저는 비정상 패킷을 방지합니다. 트래픽 클래스에서 일부 패킷 이상 유형을 처리하는 방식을 구성할 수 있습니다. FlexConfig 정책을 사용하여 TCP 정규화를 구성할 수 있습니다.
- **TCP State Bypass(TCP** 상태 우회**)** - 네트워크에서 비대칭 라우팅을 사용하는 경우 TCP 상태 검사를 우회할 수 있습니다.

서비스 정책을 위한 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

서비스 정책 가이드라인 및 제한 사항

- 서비스 정책은 라우팅 모드 또는 투명 모드에서 라우팅된 인터페이스 또는 스위치 인터페이스에만 적용됩니다. 인라인 집합 또는 수동 인터페이스에는 적용되지 않습니다.
- 특정 인터페이스 또는 전역 정책에 대해 최대 25개의 트래픽 클래스를 가질 수 있습니다. 이는 특정 보안 영역 또는 인터페이스 그룹의 전역 정책에 대해 25개를 초과하는 서비스 정책 규칙을 가질 수 없음을 의미합니다. 하지만 인터페이스의 경우 동일한 인터페이스가 보안 영역과 인터페이스 그룹 모두에 나타날 수 있기 때문에 실제로 영역/그룹이 아닌 인터페이스를 기반으로 제한이 있다는 점에 유의하십시오. 따라서 영역/그룹의 멤버 수에 따라 영역/그룹당 25개의 규칙을 가질 수 없습니다.
- 특정 인터페이스 개체/트래픽 흐름 조합에 대한 규칙이 적어도 하나 이상 있을 수 있습니다.
- 서비스 정책 변경 사항을 구성에 적용하면 모든 새 연결에서 새로운 서비스 정책을 사용합니다. 기존 연결에서는 연결 설정 당시에 구성된 정책을 계속 사용합니다. 모든 연결에서 새 정책을 즉시 사용하려면 새 정책을 사용하여 다시 연결할 수 있도록 현재 연결을 해제해야 합니다. SSH 또는 콘솔 CLI 세션에서 **clear conn** 또는 **clear local-host** 명령을 입력합니다.

Firepower Threat Defense Service 정책 설정

특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 구성을 만드는 서비스 정책을 사용할 수 있습니다. 서비스 정책은 인터페이스에 적용되거나 전역으로 적용되는 여러 작업 또는 규칙으로 구성됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 선택하고 Firepower Threat Defense Service 정책을 편집하려는 액세스 제어 정책의 수정( )을 클릭합니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **Threat Defense Service Policy(Threat Defense Service** 정책**)** 그룹에서 수정( )을 클릭합니다.

기존 정책을 보여 주는 대화 상자가 열립니다. 정책은 전역 규칙(모든 인터페이스에 적용)과 인터페이스 기반 규칙으로 구분된 규칙의 정렬 목록으로 구성됩니다. 테이블에는 인터페이스 개체 및 확장된 액세스 제어 목록 이름(결합된 규칙에 대한 트래픽 클래스 정의) 및 적용된 서비스가 표시됩니다.

단계 **4** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)**을 클릭하여 새로운 규칙을 추가합니다. 서비스 정책 규칙 구성, 1253 페이지의 내용을 참조하십시오.
- 수정( )을 클릭하여 기존 규칙을 수정합니다. 서비스 정책 규칙 구성, 1253 페이지의 내용을 참조하십시오.
- 삭제( )을 클릭하여 규칙을 삭제합니다.
- 규칙을 클릭하고 새 위치로 드래그하여 옮깁니다. 인터페이스와 전역 목록 간에 규칙을 드래그할 수는 없지만 대신 규칙을 편집하여 인터페이스/전역 설정을 변경해야 합니다. 연결과 일치하는 목록의 첫 번째 규칙이 연결에 적용됩니다.

단계 **5** 정책 편집이 완료되면 **OK(**확인**)**를 클릭합니다.

단계 **6** **Advanced(**고급**)** 창에서 **Save(**저장**)**를 클릭합니다. 저장을 클릭할 때까지 변경 사항이 저장되지 않습니다.

서비스 정책 규칙 구성

특정 트래픽 클래스에 서비스를 적용하기 위해 서비스 정책 규칙을 구성할 수 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)** > **Access List(**액세스 목록**)** > **Extended(**확장**)**로 이동하고 규칙이 적용되는 트래픽을 정의하는 확장된 액세스 목록을 생성합니다. 이 규칙은 확장된 액세스 목록의 허용 규칙과 일치하는 모든 연결에 적용됩니다. ACL 규칙을 정확하게 정의하여 서비스 정책 규칙이 서비스가 필요한 트래픽에만 적용되도록 하십시오.

인터페이스 기반 규칙을 생성하는 경우 할당된 디바이스에서 인터페이스를 구성하고 보안 영역이나 인터페이스 그룹에 인터페이스를 추가해야 합니다.

프로시저

단계 **1** 아직 Firepower Threat Defense Service Policy(Firepower Threat Defense Service 정책) 대화 상자에 존재하지 않는 경우, **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 선택하고 액세스 제어 정책을 편집한 다음 **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**를 편집합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)**을 클릭하여 새로운 규칙을 추가합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

서비스 정책 규칙 마법사가 열리고 규칙을 구성하는 과정을 단계별로 안내합니다.

단계 **3** **Interface Object(**인터페이스 개체**)** 단계에서 정책을 사용하는 인터페이스를 정의하는 옵션을 선택합니다.

- **Apply Globally(**전역으로 적용**)** - 모든 인터페이스에 적용되는 전역 규칙을 생성하려면 이 옵션을 선택합니다.
- **Select Interface Objects(**인터페이스 개체 선택**)** - 인터페이스 기반 규칙을 생성하려면 이 옵션을 선택합니다. 그런 다음 원하는 인터페이스가 포함된 보안 영역 또는 인터페이스 개체를 선택하고 >를 클릭하여 **Next**selected 목록으로 이동합니다. 서비스 정책 규칙은 선택한 개체에 포함된 각 인터페이스에 구성되며 영역/그룹 자체에는 구성되지 않습니다.

인터페이스 기준이 완료되면 클릭합니다.

단계 **4** **Traffic Flow(**트래픽 흐름**)** 단계에서 규칙이 적용되는 연결을 정의하는 확장 ACL 개체를 선택한 후 **Next(**다음**)**를 클릭합니다.

단계 **5** **Connection Setting(**연결 설정**)** 단계에서 이 트래픽 클래스에 적용할 서비스를 구성합니다.

- **Enable TCP State Bypass(TCP** 상태 우회 활성화**)**(TCP 연결만 해당) - TCP 상태 우회를 구현합니다. TCP 상태 우회가 적용되는 연결은 검사 엔진의 검사 대상이 아니며 모든 TCP 상태 검사 및 TCP 정규화를 우회합니다. 자세한 내용은 비동기 라우팅의 TCP 상태 검사 우회(TCP 상태 우회), 1256 페이지의 내용을 참조하십시오.

  참고 문제 해결 목적 또는 비대칭 라우팅을 해결할 수 없는 경우 TCP 상태 우회를 사용합니다. 이 기능은 좁은 범위로 정의된 트래픽 클래스로 제대로 구현되지 않는 경우 많은 수의 연결을 유발할 수 있는 여러 보안 기능을 비활성화합니다.

- **Randomize TCP Sequence Number(TCP** 일련 번호 임의 지정**)**(TCP 연결만 해당) - TCP 시퀀스 번호 임의 설정을 활성화하거나 비활성화합니다. 임의 설정은 기본적으로 활성화되어 있습니다. 자세한 내용은 TCP 시퀀스 임의 설정 비활성화, 1260 페이지를 참고하십시오.

- **Enable Decrement TTL(TTL** 감소 활성화**)**(TCP 연결만 해당) - 클래스와 일치하는 패킷의 TTL(time-to-live)을 줄입니다. TTL(time-to-live)을 줄이면 TTL이 1인 패킷이 삭제되지만, 연결이 더 큰 TTL이 있는 패킷을 포함할 수 있다는 가정하에 세션에 대한 연결이 열립니다. OSPF Hello 패킷과 같은 일부 패킷은 TTL 이 1로 전송되어 TTL을 줄이면 예기치 않은 결과가 발생할 수 있습니다.

  참고 Firepower Threat Defense 디바이스를 트레이스라우트(traceroute)에 표시하려면 감소 TTL 옵션을 구성하고 플랫폼 설정 정책에서 ICMP 연결 불가 속도 제한을 설정해야 합니다. Firepower Threat Defense 디바이스가 트레이스라우트(traceroute)에 표시되도록 설정, 1265 페이지의 내용을 참조하십시오.

- **Connections(**연결**)** - 전체 클래스에 대해 허용된 연결의 수를 제한합니다. 이러한 옵션을 구성할 수 있습니다.
  - **Maximum TCP and UDP(**최대 **TCP** 및 **UDP)**(TCP/UDP 연결만 해당) - 전체 클래스에 대해 허용되는 최대 동시 연결 수(0~2000000)입니다. TCP의 경우 이 수는 설정된 연결에만 적용됩니다. 기본값은 무제한 연결을 허용하는 0입이다. 클래스에 제한이 적용되므로 하나의 공격 호스트가 모든 연결을 사용하여 클래스에 일치하는 호스트를 남겨 두지 않을 수 있습니다. 이 문제를 개선하기 위해 클라이언트당 제한을 설정합니다.

- **Maximum Embryonic(**최대 원시**)**(TCP 연결만 해당) - 허용되는 최대 동시 원시 TCP 연결 수(TCP 핸드셰이크를 완료하지 않은 TCP 연결 수)입니다(0~2000000). 기본값은 무제한 연결을 허용하는 0입이다. 0이 아닌 제한을 설정하면 TCP 가로채기가 활성화되며, 이렇게 하면 TCP SYN 패킷을 인터페이스에 플러딩하여 시행된 DoS 공격으로부터 내부 시스템을 보호할 수 있습니다. 또한 SYN 플러딩을 방지하려면 클라이언트당 옵션을 설정합니다. 자세한 내용은 SYN 플러딩 DoS 공격(TCP 가로채기)로부터 서버 보호, 1262 페이지를 참고하십시오.

- **Connections Per Client(**클라이언트당 연결**)** - 특정 클라이언트(소스 IP 주소)에 허용된 연결에 대한 제한입니다. 이러한 옵션을 구성할 수 있습니다.
  - **Maximum TCP and UDP(**최대 **TCP** 및 **UDP)**(TCP/UDP 연결만 해당) - 클라이언트당 허용되는 최대 동시 연결 수(0~2000000)입니다. TCP의 경우 설정된 연결, 원시(절반이 열림) 연결 및 절반이 닫힌 연결을 포함합니다. 기본값은 무제한 연결을 허용하는 0입이다. 이 옵션은 해당 클래스에 일치하는 각 호스트에 대해 허용되는 동시 연결의 최대 수를 제한합니다.
  - **Maximum Embryonic(**최대 원시**)**(TCP/UDP 연결만 해당) - 클라이언트당 허용되는 최대 동시 원시 TCP 연결 수(0~2000000)입니다. 기본값은 무제한 연결을 허용하는 0입이다. 자세한 내용은 SYN 플러딩 DoS 공격(TCP 가로채기)로부터 서버 보호, 1262 페이지를 참고하십시오.

- **Connections Timeout(**연결 시간 초과**)** - 트래픽 클래스에 적용할 시간 초과 설정입니다. 이러한 시간 초과는 플랫폼 설정 정책에 정의된 전역 시간 초과 값보다 우선합니다. 다음을 구성할 수 있습니다.
  - **Embryonic(**원시**)**(TCP 연결만 해당) - TCP 원시(절반이 열림) 연결이 닫힐 때까지의 시간 제한 기간(0:0:5~1193:00:00)입니다. 기본값은 0:0:30입니다.
  - **Half Closed(**절반이 닫힘**)**(TCP 연결만 해당) - 절반이 닫힌 연결이 닫힐 때까지의 유휴 시간 제한 기간(0:0:30~1193:0:0)입니다. 기본값은 0:10:0입니다. 절반이 닫힌 연결은 DCD(Dead Connection Detection)의 영향을 받지 않습니다. 또한 해당 시스템은 절반이 닫힌 연결을 해제할 때 재설정을 보내지 않습니다.
  - **Idle(**유휴**)**(TCP, UDP, ICMP, IP 연결) - 프로토콜의 기존 연결이 닫히기까지의 유휴 시간 제한 기간(0:0:1~1193:0:0)입니다. 기본값이 0:2:0인 TCP State Bypass(TCP 상태 우회) 옵션을 선택하지 않는 경우 기본값은 1:0:0입니다.
  - **Reset Connection Upon Timeout(**시간 초과 시 연결 재설정**)**(TCP 연결만 해당) - 유휴 연결이 제거된 후 양방향 시스템에 TCP RST 패킷을 보낼지 여부입니다.

- **Detect Dead Connections(**끊어진 연결 탐지**)** - DCD(Dead Connection Detection)를 활성화할 것인지 지정합니다. 유휴 연결이 만료되기 전에 시스템에서 종단 호스트에 프로브를 보내 연결이 유효한지 확인합니다. 두 호스트가 모두 응답하면 연결이 유지되고 그렇지 않으면 연결이 해제됩니다. 투명 방화벽 모드에서 작동하는 경우 엔드포인트에 대한 정적 경로를 구성해야 합니다. 오프로드된 연결에서는 DCD를 설정할 수 없으므로 사전 필터 정책에서 빠른 경로를 지정하는 연결에서는 DCD를 설정하지 마십시오.FTD CLI에서 **show conn detail** 명령을 사용하여 이니시에이터와 응답자가 전송한 DCD 프로브 수를 추적합니다.

  다음 옵션을 구성합니다.

- **Detection Timeout(**탐지 시간 초과**)** - DCD 프로브에서 응답이 없을 때 또 다른 프로브를 보내기까지 대기하는 시간을 hh:mm:ss 형식으로 설정합니다(0:0:1~24:0:0). 기본값은 0:0:15입니다.

  클러스터 또는 고가용성 구성에서 작동하는 시스템의 경우, 간격을 1분 미만(0:1:0)으로 설정하지 것은 좋지 않습니다. 연결을 다른 시스템으로 옮겨야 한다면, 이러한 변경은 30초 이상 걸리며 변경이 완료되기 전에 연결이 삭제될 수 있습니다.

- **Detection Retries(**탐지 재시도**)** - 연결이 끊어진 상태임을 선언하기 전 DCD에 대한 연속 실패 재시도 횟수를 설정합니다(1~255). 기본값은 5입니다.

단계 **6** 변경 사항을 저장하려면 **Finish(**마침**)**를 클릭합니다.

규칙은 해당 목록의 맨 아래(Interfaces(인터페이스) 또는 Global(전역))에 추가됩니다. 전역 규칙은 하향식 순서로 연결됩니다. 인터페이스 목록의 규칙은 각 인터페이스 개체의 하향식 순서로 연결됩니다. 광범위한 규칙 위에 좁은 범위로 정의된 트래픽 클래스에 대한 규칙을 적용하여 적절한 서비스가 적용되도록 하십시오. 드래그 앤 드롭을 사용하여 각 목록 내에서 규칙을 이동할 수 있습니다. 규칙 목록 간에는 이동할 수 없습니다.

비동기 라우팅의 TCP 상태 검사 우회(TCP 상태 우회)

특정 연결의 인바운드 및 아웃바운드 흐름이 두 개의 다른 Firepower Threat Defense 디바이스를 통과하는 비동기 라우팅 환경이 네트워크에 있는 경우, 영향을 받는 트래픽에 TCP 상태 우회를 구현해야 합니다.

그러나 TCP 상태 우회는 네트워크의 보안을 약화시키므로 매우 제한된 특정 트래픽 클래스에만 우회를 적용해야 합니다.

다음 주제에서는 이러한 문제와 해결책에 대해 자세하게 설명합니다.

비동기 라우팅 문제

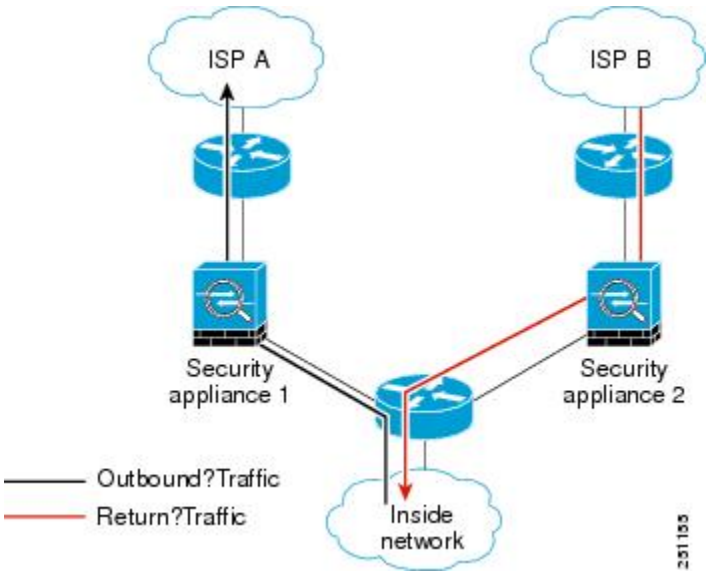
기본적으로 Firepower Threat Defense 디바이스를 통과하는 모든 트래픽은 ASA(Adaptive Security Algorithm)를 사용하여 검사되며, 보안 정책에 따라 통과하도록 허용되거나 삭제됩니다. Firepower Threat Defense 디바이스는 각 패킷의 상태(새 연결인지 설정된 연결인지)를 확인하고 이를 세션 관리 경로(새 연결 SYN 패킷), 빠른 경로(설정된 연결) 또는 제어 평면 경로(고급 검사)에 할당하여 방화벽 성능을 극대화합니다.

빠른 경로에 있는 기존 연결과 일치하는 TCP 패킷은 보안 정책의 모든 사항을 다시 확인하지 않고 Firepower Threat Defense 디바이스를 통과할 수 있습니다. 이 기능은 성능을 극대화합니다. 그러나 SYN 패킷을 사용하여 빠른 경로에서 세션을 설정하는 방법과 빠른 경로에서 발생하는 확인(예: TCP 시퀀스 번호)은 비동기 라우팅 솔루션을 방해할 수 있습니다. 연결의 아웃바운드 및 인바운드 흐름이 모두 동일한 Firepower Threat Defense 디바이스를 통과해야 합니다.

예를 들어, 새로운 연결은 보안 어플라이언스 1로 연결됩니다. SYN 패킷은 세션 관리 경로를 통과하며 연결 항목이 빠른 경로 테이블에 추가됩니다. 이 연결의 후속 패킷이 보안 어플라이언스 1을 통과하는 경우 이러한 패킷은 빠른 경로의 항목과 일치하므로 통과됩니다. 그러나 후속 패킷이 세션 관리

경로를 통과한 SYN 패킷이 없는 Security Appliance 2로 이동하는 경우에는 빠른 경로에 연결을 위한 항목이 없으므로 패킷이 삭제됩니다. 다음 그림에서는 아웃바운드 트래픽이 다른 Firepower Threat Defense 디바이스를 통과한 다음 인바운드 트래픽을 통과하는 비대칭 라우팅 예를 보여줍니다.

그림 *40:* 비대칭 라우팅



업스트림 라우터에서 비동기 라우팅을 구성하고 트래픽이 두 개의 Firepower Threat Defense 디바이스 사이에서 번갈아 전송되는 경우 특정 트래픽에 대한 TCP 상태 우회를 구성할 수 있습니다. TCP 상태 우회는 빠른 경로에서 세션이 설정되는 방식을 변경하고 빠른 경로 확인을 비활성화합니다. 이 기능은 UDP 연결을 처리하듯 TCP 트래픽을 처리합니다. 지정된 네트워크와 일치하는 비 SYN 패킷이 Firepower Threat Defense 디바이스로 들어가고 빠른 경로 항목이 없으면, 빠른 경로에서 연결을 설정할 수 있도록 패킷이 세션 관리 경로로 들어가게 됩니다. 빠른 경로에 있게 되면 이 트래픽은 빠른 경로 확인을 우회합니다.

TCP 상태 우회 가이드라인 및 제한 사항

TCP 상태 우회지원되지 않는 기능

다음 기능은 TCP 상태 우회를 사용할 때 지원되지 않습니다.

- 애플리케이션 검사 - 검사를 수행하려면 인바운드 트래픽과 아웃바운드 트래픽이 모두 동일한 Firepower Threat Defense 디바이스를 통과해야 하므로 검사는 TCP 상태 우회 트래픽에 적용되지 않습니다.
- Snort 검사 - 검사에서는 인바운드 및 아웃바운드 트래픽이 동일한 디바이스를 통과해야 합니다. 하지만 Snort 검사는 TCP 상태 우회 트래픽에 대해 자동으로 우회하지 않습니다. 또한 TCP 상태 우회를 구성할 동일한 트래픽 클래스에 대해 사전 필터 fastpath 규칙을 구성해야 합니다.
- TCP 가로채기, 최대 원시 연결 제한, TCP 시퀀스 번호 임의 설정 - Firepower Threat Defense 디바이스는 연결 상태를 추적하지 않으므로 이러한 기능은 적용되지 않습니다.
- TCP 정규화 - TCP 노멀라이저는 사용되지 않습니다.

- 상태 기반 시스템 대체 작동

TCP 상태 우회 NAT 지침

변환 세션은 Firepower Threat Defense 디바이스에 대해 별도로 설정되기 때문에 두 디바이스 모두에서 TCP 상태 우회 트래픽에 대한 상태 NAT를 구성해야 합니다. 동적 NAT를 사용하는 경우 디바이스 1의 세션에 대해 선택되는 주소는 디바이스 2의 세션에 대해 선택되는 주소와 다릅니다.

TCP 상태 우회 구성

비동기 라우팅 환경에서 TCP 상태 검사를 우회하려면 영향을 받는 호스트 또는 네트워크에만 적용되도록 트래픽 클래스를 신중하게 정의한 다음, 서비스 정책을 사용하여 트래픽의 TCP 상태 우회를 활성화합니다. 또한 트래픽이 검사를 우회할 수 있도록 동일한 트래픽에 대해 해당 사전 필터 fastpath 정책을 구성해야 합니다.

우회는 네트워크의 보안을 약화시키므로 가능한 한 애플리케이션을 제한합니다.

프로시저

단계 **1** 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 10.1.1.1에서 10.2.2.2까지의 TCP 트래픽에 대한 트래픽 클래스를 정의하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: bypass).
e) **Add(**추가**)**를 클릭하여 규칙을 추가합니다.
f) 작업에 대해 **Allow(**허용**)**를 유지합니다.
g) **Source(**소스**)** 목록 아래에 10.1.1.1을 입력하고 **Add(**추가**)**를 클릭하고 **Destination(**대상**)** 목록 아래에 있는 10.2.2.2를 클릭하고 **Add(**추가**)**를 클릭합니다.
h) **Port(**포트**)**를 클릭하고 **Selected Source Ports(**선택한 소스 포트**)** 목록 아래에 있는 **TCP (6)**를 선택한 다음 **Add(**추가**)**를 클릭합니다. 포트 번호는 입력하지 마십시오. 모든 포트를 포함하는 TCP를 프로토콜로 추가하면 됩니다.
i) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.
j) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** TCP 상태 우회 서비스 정책 규칙을 구성합니다.

예를 들어 이 트래픽 클래스에 대해 TCP 상태 우회를 전역적으로 구성하려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.

b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**에 대해 수정( )을 클릭합니다.
c) **Add Rule(**규칙 추가**)**을 클릭합니다.
d) **Apply Globally(**전역으로 적용**)** > **Next(**다음**)**를 선택합니다.
e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.
f) **Enable TCP State Bypass(TCP** 상태 우회 활성화**)**를 선택합니다.
g) (선택 사항). 우회 연결에 대한 **Idle(**유휴**)** 시간 초과를 조정합니다. 기본은 2분입니다.
h) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.
i) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.
j) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

단계 **3** 트래픽 클래스에 대한 사전 필터 fastpath 규칙을 구성합니다.

사전 필터 규칙에서 ACL 개체를 사용할 수 없으므로 사전 필터 규칙에서 직접 트래픽 클래스를 다시 생성하거나, 먼저 클래스를 정의하는 네트워크 개체를 생성해야 합니다.

다음 절차는 사용자가 이미 액세스 제어 정책에 사전 필터 정책을 연결했다고 가정합니다. 사전 필터 정책을 아직 생성하지 않은 경우 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Prefilter(**사전 필터**)**로 이동하여 먼저 정책을 생성합니다. 그런 다음 이 절차에 따라 액세스 제어 정책에 연결하고 규칙을 생성할 수 있습니다.

이 절차는 예제를 유지하면서 10.1.1.1에서 10.2.2.2까지의 TCP 트래픽에 대한 fastpath 규칙을 생성합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 TCP 우회 서비스 정책 규칙이 있는 정책을 편집합니다.
b) 정책 설명 바로 아래 왼쪽에 있는 **Prefilter Policy(**사전 필터 정책**)**의 링크를 클릭합니다.
c) Prefilter Policy(사전 필터 정책) 대화 상자에서 올바른 정책이 선택되지 않은 경우 디바이스에 할당할 정책을 선택합니다. 아직 OK(확인)를 클릭하지 마십시오.

   기본 사전 필터 정책에 규칙을 추가할 수 없으므로 사용자 정의 정책을 선택해야 합니다.

d) Prefilter Policy(사전 필터 정책) 대화 상자에서 수정( )을 클릭합니다. 이 작업을 수행하면 정책을 편집할 수 있는 새 브라우저 창이 열립니다.
e) **Add Prefilter Rule(**사전 필터 규칙 추가**)**을 클릭하고 다음 속성이 있는 규칙을 구성합니다.
   - **Name(**이름**)** - TCP Bypass와 같이 유의미한 이름을 사용할 수 있습니다.
   - **Action(**작업**)** - **Fastpath**를 선택합니다.
   - **Interface Objects(**인터페이스 개체**)** - 전역 규칙으로 TCP 상태 우회를 설정한 경우, 소스와 대상 모두 기본값(any)으로 유지합니다. 인터페이스 기반 규칙을 생성한 경우 **Source Interface Objects(**소스 인터페이스 개체**)** 목록에서 규칙에 사용한 인터페이스 개체와 동일한 인터페이스 개체를 선택하고 any를 대상으로 유지합니다.
   - **Networks(**네트워크**)** - **Source Networks(**소스 네트워크**)** 목록에 10.1.1.1을 추가하고 **Destination Networks(**대상 네트워크**)** 목록에 10.2.2.2를 추가합니다. 네트워크 개체를 사용하거나 수동으로 주소를 추가할 수 있습니다.

- **Ports(**포트**) - Selected Source Ports(**선택한 소스 포트**)**에서 TCP(6), **do not enter a port(**포트 입력 안 함**)**를 선택하고 **Add(**추가**)**를 클릭합니다. 이렇게 하면 TCP 포트 번호에 관계없이 모든(및 유일한) TCP 트래픽에 규칙이 적용됩니다.

f) **Add(**추가**)**를 클릭하여 사전 필터 정책에 규칙을 추가합니다.

g) 사전 필터 정책에 변경 사항을 저장하려면 **Save(**저장**)**를 클릭합니다.

이제 사전 필터 편집 창을 닫고 액세스 제어 정책 편집 창으로 돌아갈 수 있습니다.

h) 액세스 제어 정책 편집 창에서 여전히 Prefilter Policy(사전 필터 정책) 대화 상자가 열려 있어야 합니다. 사전 필터 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.

i) 변경한 경우, 변경된 사전 필터 정책 할당을 저장하려면 액세스 제어 정책에서 **Save(**저장**)**를 클릭합니다.

이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

TCP 시퀀스 임의 설정 비활성화

각 TCP 연결에는 각각 클라이언트와 서버에서 생성된 두 개의 ISN(초기 시퀀스 번호)이 있습니다. Firepower Threat Defense 디바이스는 인바운드와 아웃바운드 두 방향 모두로 전달되는 TCP SYN의 ISN을 임의로 설정합니다.

보호된 호스트의 ISN을 임의로 설정하면 공격자가 새 연결을 위한 다음 ISN을 예측하지 못하며 잠재적으로 새 세션의 가로채기가 방지됩니다.

필요한 경우 예를 들어 데이터 암호화로 인해 TCP 초기 시퀀스 번호 임의 설정을 사용 해제할 수 있습니다. 다음은 임의 지정을 비활성화할 수 있는 몇 가지 상황입니다.

- 다른 인라인 방화벽에서도 초기 시퀀스 번호를 임의로 설정하는 경우에는 두 방화벽 모두 이 작업을 수행할 필요가 없습니다. 이는 이 작업이 트래픽에 영향을 주지 않는 경우에도 마찬가지입니다.
- 디바이스를 통해 eBGP 멀티 홉을 사용하는 경우 eBGP 피어는 MD5를 사용합니다. 임의 설정은 MD5 체크섬을 중단합니다.
- 연결의 시퀀스 번호를 임의 설정하지 않으려면 Firepower Threat Defense 디바이스가 필요한 WAAS 디바이스를 사용합니다.
- ISA 3000에서 하드웨어 우회를 활성화하면 ISA 3000이 더 이상 데이터 경로의 일부가 아닐 때 TCP 연결이 끊어집니다.

프로시저

단계 **1** 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 호스트에서 10.2.2.2까지의 TCP 트래픽에 대한 트래픽 클래스를 정의하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: preserve-sq-no).
e) **Add(**추가**)**를 클릭하여 규칙을 추가합니다.
f) 작업에 대해 **Allow(**허용**)**를 유지합니다.
g) **Source(**소스**)** 목록을 빈 상태로 두고 **Destination(**대상**)** 목록 아래에 10.2.2.2를 입력하고 **Add(**추가**)**를 클릭합니다.
h) **Port(**포트**)**를 클릭하고 **Selected Source Ports(**선택한 소스 포트**)** 목록 아래에 있는 **TCP (6)**를 선택한 다음 **Add(**추가**)**를 클릭합니다. 포트 번호는 입력하지 마십시오. 모든 포트를 포함하는 TCP를 프로토콜로 추가하면 됩니다.
i) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.
j) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** TCP 시퀀스 번호 임의 지정을 비활성화하는 서비스 정책 규칙을 구성합니다.

예를 들어 이 트래픽 클래스에 대해 임의 지정을 비활성화하려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.
b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(**위협 방어 서비스 정책**)**에 대해 수정( )을 클릭합니다.
c) **Add Rule(**규칙 추가**)**을 클릭합니다.
d) **Apply Globally(**전역으로 적용**)** > **Next(**다음**)**를 선택합니다.
e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.
f) **Randomize TCP Sequence Number(TCP** 일련 번호 임의 지정**)**를 선택 취소합니다.
g) (선택 사항). 필요에 따라 다른 연결 옵션을 조정합니다.
h) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.
i) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.
j) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

서비스 정책 규칙 예시

다음 항목에서는 서비스 정책 규칙의 예를 제공합니다.

SYN 플러딩 DoS 공격(TCP 가로채기)로부터 서버 보호

공격자가 호스트에 일련의 SYN 패킷을 보낼 때 SYN 플러딩 DoS(Denial of Service: 서비스 거부) 공격이 발생합니다. 일반적으로 이러한 패킷은 스푸핑된 IP 주소에서 시작합니다. SYN 패킷에 대한 지속적인 플러딩은 서버 SYN 큐를 꽉 찬 상태로 유지하여 합법적인 사용자의 연결 요청에 대응하지 못하도록 합니다.

원시 연결 수를 제한하면 SYN 플러딩 공격을 방지하는 데 도움이 될 수 있습니다. 원시 연결은 소스와 대상 간에 필요한 핸드셰이크를 완료하지 않은 연결 요청입니다.

어떤 연결의 최초 연결 임계값을 초과하면 Firepower Threat Defense 디바이스는 SYN 쿠키 메서드(SYN 쿠키에 대한 자세한 내용은 Wikipedia 참조)를 사용하여 서버의 프록시 역할을 하면서 클라이언트 SYN 요청에 대해 SYN-ACK 응답을 생성합니다. Firepower Threat Defense 디바이스는 클라이언트에서 ACK를 다시 받은 후 클라이언트가 실제 클라이언트인지 인증하고 서버에 연결하도록 허용합니다. 프록시를 수행하는 구성 요소를 TCP 가로채기라고 합니다.

연결 제한을 설정하면 SYN 플러드 공격으로부터 서버를 보호할 수 있습니다. 선택적으로 TCP 가로채기 통계를 활성화하고 정책 결과를 모니터링할 수 있습니다. 다음 절차에서는 이러한 엔드 투 엔드 프로세스에 대해 설명합니다.

시작하기 전에

- 보호하려는 서버의 TCP 백로그 큐보다 원시 연결 제한을 낮게 설정해야 합니다. 그렇지 않을 경우 SYN 공격이 이루어지는 동안 유효한 클라이언트가 서버에 더 이상 액세스할 수 없게 됩니다. 원시 제한에 합당한 값을 정하려면 서버의 용량, 네트워크, 서버 사용량을 신중하게 분석합니다.
- Firepower Threat Defense 디바이스 모델의 CPU 코어 수에 따라 각 코어에서 연결을 관리하는 방식으로 인해 최대 동시 및 원시 연결이 구성된 개수를 초과할 수도 있습니다. 최악의 경우 디바이스는 최대 n-1개(여기서 n은 코어 수)의 추가 연결 및 원시 연결을 허용합니다. 예를 들어 모델에 4개의 코어가 있는 경우 6개의 동시 연결과 4개의 원시 연결을 구성하면 유형별로 3개가 추가될 수 있습니다. 모델의 코어 수를 확인하려면 디바이스 CLI에 **show cpu core** 명령을 입력합니다.

프로시저

단계 **1** 보호하려는 서버 목록인 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 트래픽 클래스를 정의하여 웹 서버를 IP 주소 10.1.1.5 및 10.1.1.6로 보호하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: protected-servers).
e) **Add(**추가**)**를 클릭하여 규칙을 추가합니다.
f) 작업에 대해 **Allow(**허용**)**를 유지합니다.

g) **Source(**소스**)** 목록을 빈 상태로 두고 **Destination(**대상**)** 목록 아래에 10.1.1.5를 입력하고 **Add(**추가**)**를 클릭합니다.

h) 또한 **Destination(**대상**)** 목록 아래에 10.1.1.6을 입력하고 **Add(**추가**)**를 클릭합니다.

i) **Port(**포트**)**의 사용 가능한 포트 목록에서 **HTTP**를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다. 서버가 HTTPS 연결도 지원하는 경우 해당 포트도 추가합니다.

j) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.

k) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** 원시 연결 제한을 설정하는 서비스 정책 규칙을 구성합니다.

예를 들어 총 동시 원시 제한을 1000개의 연결로 설정하고 클라이언트당 제한을 50개의 연결로 설정하려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.

b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**에 대해 수정( )을 클릭합니다.

c) **Add Rule(**규칙 추가**)**을 클릭합니다.

d) **Apply Globally(**전역으로 적용**)** > **Next(**다음**)**를 선택합니다.

e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.

f) **Connections(**연결**)** > **Maximum Embryonic(**최대 원시**)**에 1000을 입력합니다.

g) **Connections Per Client(**클라이언트당 연결**)** > **Maximum Embryonic(**최대 원시**)**에 50을 입력합니다.

h) (선택 사항). 필요에 따라 다른 연결 옵션을 조정합니다.

i) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.

j) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.

k) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

단계 **3** (선택 사항). TCP 가로채기 통계의 속도를 구성합니다.

TCP 가로채기는 다음 옵션을 사용하여 통계를 수집하는 속도를 결정합니다. 모든 옵션에는 기본값이 있으므로 이러한 비율이 적합한 경우 이 단계를 건너뛸 수 있습니다.

- Rate Interval(속도 간격) - 기록 모니터링 기간의 크기입니다(1~1440분). 기본값은 30분입니다. 이 간격 동안 시스템은 30회의 공격을 샘플링합니다.
- Burst Rate(버스트 속도) - 시스템 로그 메시지 생성의 임계값입니다(25~2147483647). 기본값은 400/초입니다. 버스트 속도가 초과되면 디바이스에서 시스템 로그 메시지 733104를 생성합니다.
- Average Rate(평균 속도) - 시스템 로그 메시지 생성의 평균 속도 임계값입니다(25~2147483647). 기본값은 200/초입니다. 평균 속도가 초과되면 디바이스에서 시스템 로그 메시지 733105를 생성합니다.

이 옵션을 조정하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) **FlexConfig** > **Text Object(**텍스트 개체**)**를 선택합니다.
c) threat_defense_statistics 시스템 정의 개체에 대해 수정( )을 클릭합니다.
d) 값을 직접 변경할 수는 있지만 **Override(**재정의**)**섹션을 열고 **Add(**추가**)**를 클릭하여 디바이스 재정의를 생성하는 것이 좋습니다.
e) 액세스 제어 정책 할당을 통해 서비스 정책을 할당할 디바이스를 선택하고 **Add(**추가**)**를 클릭하여 선택한 목록으로 이동합니다.
f) **Override(**재정의**)**를 클릭합니다.
g) 개체에는 3개의 항목이 있어야 하므로 3개가 될 때까지 필요에 따라 **Count(**개수**)**를 클릭합니다.
h) 속도 간격, 버스트 속도 및 평균 속도와 같이 1~3의 순서로 필요한 값을 입력합니다. 값을 올바른 순서로 입력했는지 확인하려면 개체 설명을 참조하십시오.
i) Object Override(개체 재정의) 대화 상자에서 **Add(**추가**)**를 클릭합니다.
j) Edit Text Object(텍스트 개체 편집) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **4** TCP 가로채기 통계를 활성화합니다.

TCP 가로채기 통계를 활성화하려면 FlexConfig 정책을 구성해야 합니다.

a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.
b) 이미 디바이스에 정책이 할당되어 있는 경우 편집합니다. 그렇지 않으면 새 정책을 생성하고 영향을 받는 디바이스에 할당합니다.
c) **Available FlexConfig(**사용 가능한 **FlexConfig)** 목록에서 **Threat_Detection_Configure** 개체를 선택하고 **>>**를 클릭합니다. 개체가 **Selected Append FlexConfigs** 목록에 추가됩니다.
d) **Save(**저장**)**를 클릭합니다.
e) (선택 사항). **Preview Config(**구성 미리보기**)**를 클릭하고 디바이스 중 하나를 선택하여 올바른 설정인지 확인할 수 있습니다.

시스템은 다음 구축 중에 디바이스에 기록될 CLI 명령을 생성합니다. 이 명령에는 위협 탐지 통계에 필요한 명령뿐만 아니라 서비스 정책에 필요한 명령도 포함됩니다. 미리보기 하단으로 스크롤하여 추가된 CLI를 확인합니다. TCP 가로채기 통계 명령은 기본값을 사용하는 경우 다음과 유사해야 합니다 (명확성을 위해 줄바꿈이 추가됨).

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

단계 **5** 이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

단계 **6** 다음 명령을 사용하여 디바이스 CLI에서 TCP 가로채기 통계를 모니터링합니다.

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] - 공격에서 보호된 상위 10개의 서버를 확인합니다. **all** 키워드는 추적된 모든 서버의 기록 데이터를 보여줍니다. **detail** 키워드는 기록 샘플링 데이터를 보여줍니다. 이 속도 간격 중에 시스템은 공격 횟수를 30회로 샘플링하므로, 기본값인 30분 동안 60초마다 통계가 수집됩니다.

  참고 **shun** 명령을 사용하여 공격 호스트 IP 주소를 차단할 수 있습니다. 차단을 제거하려면 **no shun** 명령을 사용합니다.

- **clear threat-detection statistics tcp-intercept**- TCP 가로채기 통계를 지웁니다.

예제:

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

Firepower Threat Defense 디바이스가 트레이스라우트(traceroute)에 표시되도록 설정

기본적으로 Firepower Threat Defense 디바이스는 트레이스라우트에 홉으로 나타나지 않습니다. 디바이스를 표시하려면 디바이스를 통과하는 패킷에서 TTL(Time to Live)을 줄이고 ICMP 연결 불가 메시지의 속도 제한을 늘려야 합니다. 이를 위해 서비스 정책 규칙을 구성하고 ICMP 플랫폼 설정 정책을 조정해야 합니다.

참고 TTL(time-to-live)을 줄이면 TTL이 1인 패킷이 삭제되지만, 연결이 더 큰 TTL이 있는 패킷을 포함할 수 있다는 가정하에 세션에 대한 연결이 열립니다. OSPF Hello 패킷과 같은 일부 패킷은 TTL 이 1로 전송되어 TTL을 줄이면 예기치 않은 결과가 발생할 수 있습니다. 트래픽 클래스를 정의할 때는 다음 사항을 고려하십시오.

프로시저

단계 **1** 트레이스라우트(traceroute) 보고를 활성화할 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 OSPF 트래픽을 제외한 모든 주소에 대한 트래픽 클래스를 정의하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: traceroute-enabled).
e) OSPF를 제외하는 규칙을 추가하려면 **Add(**추가**)**를 클릭합니다.
f) 작업을 **Block(**차단**)**으로 변경하고 **Port(**포트**)**를 클릭하고 **Destination Ports(**대상 포트**)** 목록 아래의 프로토콜로 **OSPFIGP (89)**를 선택한 다음 **Add(**추가**)**를 클릭하여 선택한 목록에 프로토콜을 추가합니다.
g) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 OSPF 규칙을 ACL에 추가합니다.

h) **Add(**추가**)**를 클릭하여 다른 모든 연결을 포함하는 규칙을 추가합니다.
i) 작업에 대해 **Allow(**허용**)**를 유지하고 소스 및 대상 목록을 비워 둡니다.
j) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.

   OSPF 거부 규칙이 Allow Any(모두 허용) 규칙 위에 있는지 확인합니다. 필요한 경우 드래그 앤 드롭하여 규칙을 이동합니다.

k) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** TTL(time-to-live) 값을 감소시키는 서비스 정책 규칙을 구성합니다.

예를 들어 전역적으로 TTL(time-to-live)을 감소시키려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.
b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**에 대해 수정( )을 클릭합니다.
c) **Add Rule(**규칙 추가**)**을 클릭합니다.
d) **Apply Globally(**전역으로 적용**)**를 선택하고 **Next(**다음**)**를 클릭합니다.
e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.
f) **Enable Decrement TTL(TTL** 감소 활성화**)**을 선택합니다.
g) (선택 사항). 필요에 따라 다른 연결 옵션을 조정합니다.
h) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.
i) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.
j) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

   이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

단계 **3** ICMP 연결 불가 메시지의 속도 제한을 늘립니다.

a) **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택합니다.
b) 이미 디바이스에 정책이 할당되어 있는 경우 편집합니다. 그렇지 않으면 새 Firepower Threat Defense 플랫폼 설정 정책을 생성하고 영향을 받는 디바이스에 할당합니다.
c) 목차에서 **ICMP**를 선택합니다.
d) **Rate Limit(**속도 제한**)**를 늘립니다(예: 50). 사용되지 않는 경우 **Burst Size(**버스트 크기**)**를 무시할 수 있습니다.

   이 작업과 관련이 없는 경우 ICMP 규칙 테이블을 비워 둘 수 있습니다.

e) **Save(**저장**)**를 클릭합니다.

단계 **4** 이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

서비스 정책 모니터링

디바이스 CLI를 사용하여 서비스 정책 관련 정보를 모니터링할 수 있습니다. 다음은 몇 가지 유용한 명령입니다.

- **show conn** [**detail**]

  연결 정보를 표시합니다. 자세한 정보는 특수 연결 특성을 나타내는 플래그를 사용합니다. 예를 들어 "b" 플래그는 TCP 상태 우회의 트래픽 대상을 나타냅니다.

  detail 키워드를 사용하면 DCD(Dead Connection Detection) 검색 관련 정보를 확인할 수 있습니다. 이니시에이터와 응답자가 연결을 탐지하는 방법을 보여줍니다. 예를 들어 DCD가 활성화된 연결에 대한 상세정보는 다음과 같이 표시됩니다.

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show service-policy**

  DCD 통계를 포함하여 서비스 정책 통계를 표시합니다.

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  공격에서 보호된 상위 10개의 서버를 확인합니다. **all** 키워드는 추적된 모든 서버의 기록 데이터를 보여줍니다. **detail** 키워드는 기록 샘플링 데이터를 보여줍니다. 이 속도 간격 중에 시스템은 공격 횟수를 30회로 샘플링하므로, 기본값인 30분 동안 60초마다 통계가 수집됩니다.

Firepower Threat Defense Service 정책 기록

기능	버전	설명
Firepower Threat Defense Service 정책.	6.3	이제 액세스 제어 정책 고급 옵션의 일부로 Firepower Threat Defense Service 정책을 구성할 수 있습니다. 특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 지원되는 기능에는 TCP 상태 우회, TCP 시퀀스 번호 임의 지정, 패킷의 TTL(time-to-live) 값 감소, Dead Connection Detection, 트래픽 클래스 및 클라이언트당 최대 연결 수 및 원시 연결 수에 대한 제한 설정, 원시 연결, 절반이 닫힌 연결 및 유휴 연결에 대한 시간 초과가 포함됩니다. 새 화면: **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**, **Advanced(**고급**)** 탭, **Threat Defense Service Policy(Threat Defense Service** 정책**)**. 지원 플랫폼: Firepower Threat Defense
DCD(Dead Connection Detection)의 이니시에이터 및 응답자 정보와, 클러스터에서의 DCD 지원입니다.	6.5	DCD(Dead Connection Detection)를 활성화하면, **show conn detail** 명령을 이용해 이니시에이터 및 응답자 정보를 얻을 수 있습니다. DCD(Dead Connection Detection)를 이용하면 비활성 연결을 유지할 수 있으며, **show conn** 출력은 엔드포인트를 얼마나 자주 조사했는지 알려줍니다. 또한 이제 DCD는 클러스터에서도 지원됩니다. 신규/수정된 명령: **show conn** (출력 전용) 지원 플랫폼: Firepower Threat Defense

49 장

Firepower Threat Defense에 대한 FlexConfig 정책

다음 주제에서는 FlexConfig 정책을 구성하고 구축하는 방법을 설명합니다.

- FlexConfig 정책 개요, 1269 페이지
- FlexConfig 정책에 대한 요구 사항 및 사전 요건, 1291 페이지
- FlexConfig 가이드라인 및 제한 사항, 1291 페이지
- FlexConfig 정책을 사용한 디바이스 설정 맞춤 설정, 1291 페이지
- FlexConfig의 예시, 1306 페이지
- FlexConfig를 위한 기록, 1320 페이지

FlexConfig 정책 개요

FlexConfig 정책은 순서가 지정된 FlexConfig 개체 목록의 컨테이너입니다. 각 개체에는 일련의 Apache Velocity 스크립팅 언어 명령, ASA 소프트웨어 구성 명령 및 사용자 정의 변수가 포함됩니다. 각 FlexConfig 개체의 내용은 ASA 명령 시퀀스를 생성하는 프로그램이며, 이는 지정된 디바이스에 구축됩니다. 그런 다음 이 명령 시퀀스에 의해 FTD 디바이스에서 관련 기능이 구성됩니다.

FTD ASA 구성 명령을 사용하여 일부 기능(모든 기능이 아님)을 구현합니다. FTD 구성 명령의 고유 집합은 없습니다. 대신, FlexConfig를 사용하면 Firepower Management Center 정책 및 설정을 통해 직접 지원되지 않는 기능을 구성할 수 있습니다.

주의 ASA에 대한 강력한 배경 지식을 보유하고 있으며 사용에 대한 전적인 책임을 질 수 있는 고급 사용자인 경우에만 FlexConfig 정책을 사용하는 것이 좋습니다. 금지되지 않은 모든 명령을 구성할 수 있습니다. FlexConfig 정책을 통해 기능을 활성화하는 경우, 구성되어 있는 다른 기능과 함께 의도하지 않은 결과를 초래할 수 있습니다.

구성한 FlexConfig 정책과 관련된 지원을 받기 위해 Cisco TAC(Technical Assistance Center)에 문의할 수 있습니다. Cisco TAC(Technical Assistance Center)에서는 고객을 대신하여 맞춤형 구성을 설계하거나 작성하지 않습니다. Cisco에서는 올바른 작동이나 기타 Firepower System 기능과의 상호운용성에 대해 어떠한 보증도 명시하지 않습니다. FlexConfig 기능은 언제든지 사용이 중지될 수 있습니다. 완벽하게 보장되는 기능을 지원받으려면 Firepower Management Center의 지원을 기다려야 합니다. 의심스러운 경우에는 FlexConfig를 사용하지 마십시오.

FlexConfig 정책에 대한 추천 사용

FlexConfig에는 다음과 같이 권장되는 주요 사용 방법이 두 가지 있습니다.

- ASA에서 FTD로 변환하는 중이며 Firepower Management Center에서 직접 지원하지 않는 호환 가능한 기능을 현재 사용 중이고 계속 사용해야 하는 경우, 이 경우, ASA에서 **show running-config** 명령을 사용하여 해당 기능에 대한 구성을 확인하고 FlexConfig 개체를 생성하여 해당 기능을 구현하십시오. 적절한 설정을 가져오려면 개체의 구축 설정을 실험합니다(한 번/항상 추가 /추가). 두 디바이스에서 **show running-config** 출력을 비교하여 확인합니다.
- FTD를 사용 중이지만 구성해야 하는 설정 또는 기능이 있는 경우(예: Cisco TAC(Technical Assistance Center)에서 발생한 특정 문제를 해결하려면 특정 설정이 필요하다고 알려주는 경우), 복잡한 기능에 대해서는 랩 디바이스를 사용하여 FlexConfig를 테스트하고 정상적으로 작동하는지 확인합니다.

시스템에는 테스트된 구성을 나타내는 사전 정의된 FlexConfig 개체 집합이 포함되어 있습니다. 필요한 기능이 이러한 개체로 표시되지 않는 경우 먼저 표준 정책에서 동일한 기능을 구성할 수 있는지 확인합니다. 예를 들어, 액세스 제어 정책에 침입 탐지 및 방지, HTTP 및 기타 프로토콜 검사 유형, URL 필터링, 애플리케이션 필터링, 액세스 제어(ASA에서는 별도의 기능을 사용하여 구현함)가 포함된 경우, 많은 기능이 CLI 명령을 사용하여 컨피그레이션된 것이 아니므로 **show running-config**의 출력 내에 모든 정책이 표시되지는 않습니다.

참고 ASA와 FTD는 일대일로 중복되지 않는다는 점을 항상 기억해야 합니다. FTD 디바이스에서 ASA 컨피그레이션을 완벽하게 재생성하려고 시도하지 마십시오. FlexConfig를 사용하여 구성하는 모든 기능은 신중히 테스트해야 합니다.

FlexConfig 개체의 CLI 명령

FTD 는 ASA 구성 명령을 사용하여 일부 기능을 구성합니다. 모든 ASA 기능이 FTD에서 호환되는 것은 아니지만, FTD에서는 작업 가능하나 Firepower Management Center 정책에서는 구성할 수 없는 기

능도 일부 있습니다. FlexConfig 개체를 사용하여 이러한 기능을 구성하는 데 필요한 CLI를 지정할 수 있습니다.

FlexConfig를 사용하여 기능을 수동으로 구성하려는 경우, 적절한 구문에 따라 명령을 파악하고 구현해야 합니다. FlexConfig 정책은 CLI 명령 구문을 검증하지 않습니다. 적절한 구문 및 CLI 명령 구성에 대한 자세한 내용을 확인하려면 ASA 설명서를 참조하십시오.

- ASA CLI 컨피그레이션 가이드에서는 기능을 구성하는 방법에 대해 설명합니다. 가이드 위치: http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- ASA 명령 참조에서는 명령 이름을 기준으로 정렬된 추가 정보를 제공합니다. 참조 위치: http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

다음 주제에서는 컨피그레이션 명령에 대해 자세히 설명합니다.

ASA 소프트웨어 버전 및 현재 CLI 컨피그레이션 확인

시스템이 ASA 소프트웨어 명령을 사용하여 일부 기능을 구성하므로 FTD 디바이스에서 실행 중인 소프트웨어에서 사용되는 현재 ASA 버전을 확인해야 합니다. 이 버전 번호에 따라 기능 구성 시 어떤 ASA CLI 컨피그레이션 가이드를 참조해야 하는지 알 수 있습니다. 또한 현재 CLI 기반 컨피그레이션을 확인하고, 구현하려는 ASA 컨피그레이션과 이를 비교합니다.

모든 ASA 컨피그레이션은 FTD 컨피그레이션과 매우 다릅니다. FTD 정책은 CLI 외부에서 구성되는 경우가 많아서 명령을 보고 컨피그레이션을 확인할 수가 없습니다. ASA와 FTD 컨피그레이션 간에 일대일 대응 관계를 생성하지 마십시오.

이 정보를 확인하려면 디바이스 관리 인터페이스에 대한 SSH 연결을 설정하고 다음 명령을 실행합니다.

- **show version system** Cisco Adaptive Security Appliance 소프트웨어 버전 번호를 찾습니다. (Firepower Management Center CLI 도구를 통해 명령을 실행하는 경우 **system** 키워드를 생략합니다.)
- **show running-config** 현재 CLI 컨피그레이션을 확인합니다.
- **show running-config all** 현재 CLI 구성의 모든 기본 명령을 포함합니다.

다음 절차를 사용하여 Firepower Management Center 내에서 이 명령을 실행할 수도 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** FlexConfig 정책이 대상으로 하는 디바이스의 이름을 클릭합니다.

상태 테이블의 **Count(**개수**)** 열에서 열기/닫기 화살표를 클릭하여 모든 디바이스를 볼 수 있습니다.

단계 **3** **Advanced Troubleshooting(**고급 문제 해결**)**을 선택합니다.

단계 **4** **Threat Defense CLI**를 선택합니다.

단계 **5** 명령을 **show**로 선택하고 **version** 또는 다른 명령 중 하나를 파라미터로 입력합니다.

단계 **6** **Execute(**실행**)**를 클릭합니다.

버전의 경우 Cisco Adaptive Security Appliance 소프트웨어 버전 번호의 출력을 검색합니다.

출력을 선택하고 Ctrl+C를 누른 다음 나중에 분석할 수 있도록 텍스트 파일에 붙여 넣을 수 있습니다.

금지된 CLI 명령

FlexConfig의 목적은 Firepower Management Center를 사용하여 FTD 디바이스에서는 구성할 수 없으나 ASA 디바이스에서는 사용 가능한 기능을 구성하는 것입니다.

따라서 Firepower Management Center에서 동일한 역할을 하는 ASA 기능을 구성할 수 없습니다. 다음 표에는 이러한 금지된 명령 영역 중 일부가 나와 있습니다.

또한 일부 **clear** 명령은 관리 정책과 중복되기 때문에 금지되며, 관리 정책에 대한 구성의 일부를 삭제할 수 있습니다.

FlexConfig 개체 편집기를 사용하면 개체에 금지된 명령을 포함할 수 없습니다.

금지된 CLI 명령	설명
AAA	차단된 구성.
AAA-Server	차단된 구성.
Access-list	고급 ACL, 확장 ACL 및 표준 ACL이 차단됩니다. 이더 타입 ACL은 허용됩니다. 템플릿 내의 개체 관리자에 정의된 표준 및 확장 ACL 개체를 변수로 사용할 수 있습니다.
ARP 감시	차단된 구성.
As-path Object	차단된 구성.
배너	차단된 구성.
BGP	차단된 구성.
클럭	차단된 구성.
Community-list Object	차단된 구성.
카피	차단된 구성.
삭제	차단된 구성.
DHCP	차단된 구성.

금지된 **CLI** 명령	설명
Enable Password(활성화 비밀번호)	차단된 구성.
Erase	차단된 구성.
Fragment Setting	차단됨(**fragment reassembly** 제외).
Fsck	차단된 구성.
HTTP	차단된 구성.
ICMP	차단된 구성.
인터페이스	**nameif**, **mode**, **shutdown**, **ip address** 및 **mac-address** 명령만 차단됩니다.
멀티캐스트 라우팅	차단된 구성.
NAT	차단된 구성.
Network Object/Object-group	FlexConfig 개체에서의 네트워크 개체 생성은 차단되어 있지만, 템플릿 내부에서 개체 관리자에 정의되어 있는 네트워크 개체 및 그룹을 변수로 사용할 수는 있습니다.
NTP	차단된 구성.
OSPF/OSPFv3	차단된 구성.
비밀번호 암호화	차단된 구성.
Policy-list Object	차단된 구성.
Prefix-list Object	차단된 구성.
재로드	reload 명령은 예약할 수 없습니다. 시스템에서는 **reload** 명령이 아닌 **reboot** 명령을 사용해 재시작합니다.
RIP	차단된 구성.
Route-Map Object	FlexConfig 개체에서의 경로 맵 개체 생성은 차단되어 있지만, 템플릿 내부에서 개체 관리자에 정의되어 있는 경로 맵 개체를 변수로 사용할 수는 있습니다.
Service Object/Object-group	FlexConfig 개체에서의 서비스 개체 생성은 차단되어 있지만, 템플릿 내부에서 개체 관리자에 정의되어 있는 포트 개체를 변수로 사용할 수는 있습니다.
SNMP	차단된 구성.

금지된 **CLI** 명령	설명
SSH	차단된 구성.
고정 경로	차단된 구성.
시스템 로그	차단된 구성.
시간 동기화	차단된 구성.
시간 초과	차단된 구성.
VPN	차단된 구성.

템플릿 스크립트

스크립팅 언어를 사용하여 FlexConfig 개체 내에서 처리를 제어할 수 있습니다. 스크립팅 언어 명령어는 루프, if/else 문 및 변수를 지원하는 Java 기반 스크립팅 언어인 Apache Velocity 1.3.1 템플릿 엔진에서 지원되는 명령의 하위 집합입니다.

스크립팅 언어 사용 방법을 알아보려면 http://velocity.apache.org/engine/devel/developer-guide.html에서 *Velocity Developer Guide*를 참조하십시오.

FlexConfig 변수

명령 또는 처리 지침의 일부가 정적 정보가 아닌 실행 정보에 따라 달라지는 경우 FlexConfig 개체에서 변수를 사용할 수 있습니다. 구축하는 동안 변수는 변수 유형에 따라 디바이스의 다른 구성에서 얻은 문자열로 대체됩니다.

- 정책 개체 변수는 Firepower Management Center에 정의된 개체에서 가져온 문자열로 대체됩니다.
- 시스템 변수는 디바이스 자체 또는 디바이스에 대해 구성된 정책에서 얻은 정보로 대체됩니다.
- 스크립팅 명령이 처리될 때 처리 변수에는 정책 개체 또는 시스템 변수의 내용이 로드됩니다. 예를 들어, 루프에서 정책 개체 또는 시스템 변수에서 하나의 값을 처리 변수로 반복적으로로드한 다음 해당 처리 변수를 사용하여 명령 문자열을 구성하거나 다른 작업을 수행합니다. 이러한 처리 변수는 FlexConfig 개체의 변수 목록에 표시되지 않습니다 또한 FlexConfig 개체 편집기의 **Insert(**삽입**)** 메뉴를 사용하여 추가하지 마십시오.
- 비밀 키 변수는 FlexConfig 개체 내의 변수에 대해 정의된 단일 문자열로 대체됩니다.

변수는 @ 문자로 시작하는 비밀 키를 제외하고는 $ 문자로 시작합니다. 예를 들어 $ifname은 다음 명령에서 정책 개체 변수인 반면, @keyname은 비밀 키입니다.

```
interface $ifname
key @keyname
```

참고 정책 개체 또는 시스템 변수를 처음 삽입할 때 FlexConfig 개체 편집기의 **Insert(**삽입**)** 메뉴를 통해 정책 개체 또는 시스템 변수를 삽입해야 합니다. 이 작업은 변수를 FlexConfig 개체 편집기의 하단에 있는 **Variables(**변수**)** 목록에 추가합니다. 하지만 시스템 변수를 사용하는 경우에도 그 다음 사용 시 변수 문자열을 입력해야 합니다. 개체 또는 시스템 변수 할당이 없는 처리 변수를 추가하는 경우 **Insert(**삽입**)** 메뉴를 사용하지 마십시오. 비밀 키를 추가하는 경우 항상 **Insert(**삽입**)** 메뉴를 사용하십시오. 비밀 키 변수는 변수 목록에 표시되지 않습니다.

변수가 단일 문자열, 문자열 목록 또는 값 테이블로 확인되는지 여부는 변수에 할당한 정책 개체 또는 시스템 변수의 유형에 따라 다릅니다. (비밀 키는 항상 단일 문자열로 확인됩니다.) 변수를 올바르게 처리하기 위해 반환할 내용을 이해해야 합니다.

다음 주제는 다양한 유형의 변수와 이러한 변수를 처리하는 방법을 설명합니다.

변수 처리 방법

실행 시간에서 변수는 단일 문자열, 동일한 유형의 문자열 목록, 다른 유형의 문자열 목록 또는 이름이 지정된 값의 테이블로 확인될 수 있습니다. 또한 여러 값으로 확인되는 변수는 확실하거나 불확실한 길이일 수 있습니다. 값을 올바르게 처리하기 위해 반환할 내용을 이해해야 합니다.

다음은 기본 가능성입니다.

단일 값 변수

변수가 항상 단일 문자열로 확인되는 경우 FlexConfig 스크립트에서 변수의 수정 없이 직접 사용하십시오.

예를 들어 사전 정의된 텍스트 변수 tcpMssBytes는 항상 단일 값(숫자여야 함)으로 확인됩니다. 그런 다음 **Sysopt_basic** FlexConfig는 if/then/else 구조를 사용하여 또 다른 단일 값 텍스트 변수 tcpMssMinimum의 값을 기반으로 최대 세그먼트 크기를 설정합니다.

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

이 예에서는 FlexConfig 개체 편집기의 **Insert(**삽입**)** 메뉴를 사용하여 $tcpMssBytes의 첫 번째 사용을 추가하지만 변수를 #else 행에 직접 입력하기도 합니다.

비밀 키 변수는 단일 값 변수의 특수 유형입니다. 비밀 키의 경우 **Insert(**삽입**)** 메뉴를 사용하여 두 번째 상ㅇ 및 후속 사용을 위해 변수를 추가합니다. 이러한 변수는 FlexConfig 개체의 변수 목록에 표시되지 않습니다 예를 들어 EIGRP 구성을 위한 키를 숨기려면 **Eigrp_Interface_Configure FlexConfig**를 복사하고 $eigrpAuthKey 및 $eigrpAuthKeyId 변수를 비밀 키 @SecretEigrpAuthKey 및 @SecretEigrpAuthKeyId로 대체할 수 있습니다.

```
authentication key eirgp $eigrpAS @SecretEigrpAuthKey key-id @SecretEigrpAuthKeyId
```

참고 네트워크 개체의 정책 개체 변수는 호스트 주소, 네트워크 주소 또는 주소 범위와 같은 단일 IP 주소 사양과 동일합니다. 하지만 이 경우 ASA 명령에 특정 주소 유형이 필요하기 때문에 예상 주소 유형을 알아야 합니다. 예를 들어 명령에 호스트 주소가 필요한 경우 네트워크 주소가 포함된 개체를 가리키는 네트워크 개체 변수를 사용하면 구축 중에 오류가 발생합니다.

다중 값 변수, 모든 값이 동일한 유형

여러 정책 개체 및 시스템 변수가 동일한 유형의 여러 값으로 확인됩니다. 예를 들어 네트워크 개체 그룹을 가리키는 개체 변수는 그룹 내의 IP 주소 목록으로 확인됩니다. 마찬가지로 시스템 변수 $SYS_FW_INTERFACE_NAME_LIST는 인터페이스 이름 목록으로 확인됩니다.

동일한 유형의 여러 값에 대한 텍스트 개체를 생성할 수도 있습니다. 예를 들어 사전 정의된 텍스트 개체인 enableInspectProtocolList는 둘 이상의 프로토콜 이름을 포함할 수 있습니다.

동일한 유형의 항목 목록으로 확인되는 여러 값 변수는 종종 불확실한 길이입니다. 예를 들어 사용자는 언제든지 인터페이스를 구성 또는 구성 해제할 수 있으므로 이름이 지정된 디바이스의 인터페이스 수를 미리 알 수 없습니다.

따라서 일반적으로 루프를 사용하여 동일한 유형의 여러 값 변수를 처리합니다. 예를 들어 사전 정의된 FlexConfig **Default_Inspection_Protocol_Enable**은 #foreach 루프를 사용하여 enableInspectProtocolList 개체를 탐색하고 각 값을 처리합니다.

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

이 예에서 스크립트는 각 값을 차례대로 $protocol 변수에 할당합니다. 이 변수는 ASA **inspect** 명령에서 해당 프로토콜에 대한 검사 엔진을 활성화하는 데 사용됩니다. 이 경우 변수 이름으로 $protocol을 입력하기만 하면 됩니다. 개체 또는 시스템 값을 변수에 할당하지 않으므로 **Insert(**삽입**)** 메뉴를 사용하여 추가하지 마십시오. 하지만 $enableInspectProtocolList를 추가하려면 **Insert(**삽입**)** 메뉴를 사용해야 합니다.

시스템은 $enableInspectProtocolList에 값이 남아 있지 않을 때까지 #foreach와 #end 사이의 코드를 반복합니다.

다중 값 변수, 값이 다른 유형

여러 개의 값 텍스트 개체를 만들 수 있지만 각 값은 다른 용도로 사용됩니다. 예를 들어 사전 정의된 **netflow_Destination** 텍스트 개체는 인터페이스 이름, 대상 IP 주소 및 UDP 포트 번호 순으로 3개의 값을 가져야 합니다.

이 방법으로 정의된 개체는 확실한 수의 값을 가져야 합니다. 그렇지 않으면 처리가 어려울 수 있습니다.

이러한 개체를 처리하려면 get 메서드를 사용합니다. 개체 이름 끝에 **.get(***n***)**을 입력하여 *n*을 개체의 인덱스를 대체합니다. 텍스트 개체가 1에서 시작하는 값을 나열하더라도 0에서 계산이 시작됩니다.

예를 들어 Netflow_Add_Destination 개체는 다음 줄을 사용하여 netflow_Destination의 3가지 값을 ASA **flow-export** 명령에 추가합니다.

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

이 예에서는 FlexConfig 개체 편집기의 **Insert(**삽입**)** 메뉴를 사용하여 $netflow_Destination의 첫 번째 사용을 추가한 다음 **.get(0)**을 추가합니다. 하지만 **$netflow_Destination.get(1)** 및 **$netflow_Destination.get(2)** 사양에 대한 변수를 직접 입력해야 합니다.

값 테이블을 확인하는 다중 값 변수

일부 시스템 변수는 값의 테이블을 반환합니다. 이러한 변수에는 이름에 MAP이 포함됩니다(예: $SYS_FTD_ROUTED_INTF_MAP_LIST). 라우팅된 인터페이스 맵은 다음과 같은 데이터를 반환합니다(명확성을 위해 줄바꿈이 추가됨).

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]
```

위의 예에서는 4개의 인터페이스에 대한 정보가 반환됩니다. 각 인터페이스는 명명된 값의 테이블을 포함합니다. 예를 들어 intf_hardwarare_id는 인터페이스 하드웨어 이름 속성의 이름이고 GigabitEthernet0/0과 같은 문자열을 반환합니다.

이 유형의 변수는 일반적으로 길이가 일정하지 않으므로 루핑을 사용하여 값을 처리해야 합니다. 하지만 검색할 값을 나타내기 위해 변수 이름에 속성 이름을 추가해야 합니다.

예를 들어 IS-IS 구성에서는 인터페이스 구성 모드에서 논리적 이름이 있는 인터페이스에 ASA **isis** 명령을 추가해야 합니다. 하지만 인터페이스의 하드웨어 이름을 사용하여 해당 모드를 입력합니다. 따라서 논리적 이름이 있는 인터페이스를 확인한 다음 해당 하드웨어 이름을 사용하여 해당 인터페이스만 구성해야 합니다. 사전 정의된 ISIS_Interface_Configuration FlexConfig는 루프에 중첩된 if/then 구조를 사용하여 이 작업을 수행합니다. 다음 코드에서는 #foreach 스크립팅 명령이 각 인터페이스 맵을 $ intf 변수로 로드한 다음 #if 문이 맵($intf.intf_logical_name)의 intf_logical_name 값을 해제한다는 것을 알 수 있으며, 값이 isisIntfList사전 정의 텍스트 변수에 정의된 목록에 있으면 intf_hardwarare_id 값($intf.intf_hardwarare_id)을 사용하여 인터페이스 명령을 입력합니다. ISIS를 구성할 인터페이스의 이름을 추가하려면 isisIntfList 변수를 편집해야 합니다.

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
```

```
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

값이 디바이스에 대해 반환하는 사항을 확인하는 방법

변수가 반환할 값을 평가할 수 있는 간단한 방법은 주석이 있는 변수 목록을 처리하는 작업만 수행하는 간단한 FlexConfig 개체를 생성하는 것입니다. 그런 다음 FlexConfig 정책에 할당하고, 디바이스에 정책을 할당하고, 정책을 저장한 다음 해당 디바이스의 구성을 미리 볼 수 있습니다. 미리보기에 확인된 값이 표시됩니다. 미리보기 텍스트를 선택하고 Ctrl+C를 누른 다음 분석할 수 있도록 텍스트 파일에 출력을 붙여 넣을 수 있습니다.

참고 하지만 유효한 구성 명령이 포함되어 있지 않으므로 이 FlexConfig를 디바이스에 구축하지 마십시오. 구축 오류가 발생할 수 있습니다. 미리보기를 얻은 후 FlexConfig 정책에서 FlexConfig 개체를 삭제하고 정책을 저장합니다.

예를 들어 다음 FlexConfig 개체를 구성할 수 있습니다.

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

이 개체의 미리보기는 다음과 유사할 수 있습니다(명확성을 위해 줄바꿈이 추가됨).

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:
```

```
[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=diagnostic}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, diagnostic]
```

FlexConfig 정책 개체 변수

정책 개체 변수는 개체 관리자에 구성된 특정 정책 개체와 연결됩니다. FlexConfig 개체에 정책 개체 변수를 삽입하면 변수에 이름을 지정하고 연결된 개체를 선택합니다.

변수에 연결된 개체와 정확히 동일한 이름을 지정할 수 있지만 변수 자체는 연결된 개체와 동일한 것이 아닙니다. FlexConfig 개체 편집기의 **Insert(**삽입**)** > **Insert Policy Object(**정책 개체 삽입**)** > ***Object Type(***개체 유형***)*** 메뉴를 사용하여 FlexConfig의 스크립트에 처음으로 변수를 추가하여 개체와의 연결을 설정해야 합니다. $ 기호 앞에 개체의 이름을 입력하기만 하면 정책 개체 변수가 생성되지 않습니다.

다음 유형의 개체를 가리키는 변수를 생성할 수 있습니다. 각 변수에 대해 올바른 유형의 개체를 생성했는지 확인하십시오. 개체를 생성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)** 페이지로 이동합니다.

- **Text Objects(**텍스트 개체**)** - 텍스트 문자열의 경우 IP 주소, 숫자 및 인터페이스 또는 영역 이름과 같은 기타 자유 형식 텍스트를 포함할 수 있습니다. 목차에서 **FlexConfig** > **Text Object(**텍스트 개체**)**를 선택한 다음 **Add Text Object(**텍스트 개체 추가**)**를 클릭합니다. 단일 값 또는 다중 값을 포함하도록 이 개체를 구성할 수 있습니다. 이러한 개체는 매우 유연하며 FlexConfig 개체 내에서 사용하도록 특수하게 생성됩니다. 자세한 내용은 FlexConfig 텍스트 개체 설정, 1298 페이지의 내용을 참조하십시오.

- **Network(**네트워크**)** - IP 주소 목적입니다. 네트워크 개체 또는 그룹을 사용할 수 있습니다. 목차에서 **Network(**네트워크**)**를 선택한 다음 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)** 또는 **Add Group(**그룹 추가**)**를 선택합니다. 그룹 개체를 사용하는 경우 변수는 그룹 내의 각 IP 주소 사양 목록을 반환합니다. 주소는 개체 내용에 따라 호스트, 네트워크 또는 주소 범위가 될 수 있습니다. 네트워크 개체, 571 페이지의 내용을 참조하십시오.
- **Security Zones(**보안 영역**)** - 보안 영역 또는 인터페이스 그룹 내의 인터페이스 목적입니다. 목차에서 **Interface(**인터페이스**)**를 선택한 다음 **Add(**추가**)** > **Security Zone(**보안 영역**)** 또는 **Interface Group(**인터페이스 그룹**)**을 선택합니다. 보안 영역 변수는 구성 중인 디바이스에 대한 해당 영역 또는 그룹 내의 인터페이스 목록을 반환합니다. 보안 영역, 577 페이지의 내용을 참조하십시오.
- **Standard ACL Object(**표준 **ACL** 개체**)** - 표준 액세스 제어 목록 목적입니다. 표준 ACL 변수는 표준 ACL 개체의 이름을 반환합니다. 목차에서 **Access List(**액세스 목록**)** > **Standard(**표준**)**를 선택한 다음 **Add Standard Access List Object(**표준 액세스 목록 개체 추가**)**를 클릭합니다. 액세스 목록, 644 페이지의 내용을 참조하십시오.
- **Extended ACL Object(**확장된 **ACL** 개체**)** - 확장된 액세스 제어 목록 목적입니다. 확장된 ACL 변수는 확장된 ACL 개체의 이름을 반환합니다. 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장됨**)**를 선택한 다음 **Add Extended Access List Object(**확장된 액세스 목록 개체 추가**)**를 클릭합니다. 액세스 목록, 644 페이지의 내용을 참조하십시오.
- **Route Map(**경로 맵**)** - 경로 맵 개체 목적입니다. 경로 맵 변수는 경로 맵 개체의 이름을 반환합니다. 목차에서 **Route Map(**경로 맵**)**을 선택한 다음 **Add Route Map(**경로 맵 추가**)**를 클릭합니다. 경로 맵, 641 페이지의 내용을 참조하십시오.

FlexConfig 시스템 변수

시스템 변수는이 대 한 구성 된 정책 또는 디바이스 자체에서 얻은 정보가으로 바뀝니다.

FlexConfig 개체 편집기의 **Insert(**삽입**)** > **Insert System Variable(**시스템 변수 삽입**)** > ***Variable Name(***변수 이름**)** 메뉴를 사용하여 FlexConfig의 스크립트에 처음으로 변수를 추가하여 시스템 변수와의 연결을 설정해야 합니다. $ 기호가 앞에 오는 시스템 변수의 이름을 입력하는 것만으로는 FlexConfig 개체의 컨텍스트 내에서 시스템 변수가 생성되지 않습니다.

다음 테이블에서는 사용 가능한 시스템 변수를 설명합니다. 변수를 사용하기 전에 일반적으로 변수에 대해 반환되는 항목을 검사하십시오. 값이 디바이스에 대해 반환하는 사항을 확인하는 방법, 1278 페이지 섹션을 참조하십시오.

이름	설명
SYS_FW_OS_MODE	디바이스의 운영 체제 모드입니다. 가능한 값은 ROUTED 또는 TRANSPARENT입니다.
SYS_FW_OS_MULTIPLICITY	디바이스가 단일 또는 다중 컨텍스트 모드로 실행 중인지 여부입니다. 가능한 값은 SINGLE, MULTI 또는 NOT_APPLICABLE입니다.
SYS_FW_MANAGEMENT_IP	디바이스의 관리되는 IP 주소
SYS_FW_HOST_NAME	디바이스 호스트네임

이름	설명
SYS_FTD_INTF_POLICY_MAP	인터페이스 이름을 키로, 정책 맵을 값으로 하는 맵입니다. 이 변수는 디바이스에 정의된 인터페이스 기반 서비스 정책이 없는 경우 아무것도 반환하지 않습니다.
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	검사가 활성화되는 프로토콜 목록입니다.
SYS_FTD_ROUTED_INTF_MAP_LIST	디바이스에서 라우팅된 인터페이스 맵 목록입니다. 각 맵에는 라우팅된 인터페이스 구성과 관련된 명명된 값 집합이 포함되어 있습니다.
SYS_FTD_SWITCHED_INTF_MAP_LIST	디바이스에서 전환된 인터페이스 맵 목록입니다. 각 맵에는 전환된 인터페이스 구성과 관련된 명명된 값 집합이 포함되어 있습니다.
SYS_FTD_INLINE_INTF_MAP_LIST	디바이스의 인라인 인터페이스 맵 목록입니다. 각 맵에는 인라인 설정 인터페이스 구성과 관련된 명명된 값 집합이 포함되어 있습니다.
SYS_FTD_PASSIVE_INTF_MAP_LIST	디바이스의 수동 인터페이스 맵 목록입니다. 각 맵에는 수동 인터페이스 구성과 관련된 명명된 값 집합이 포함되어 있습니다.
SYS_FTD_INTF_BVI_MAP_LIST	디바이스의 Bridge Virtual Interface 맵 목록입니다. 각 맵에는 BVI 구성과 관련된 명명된 값 집합이 포함되어 있습니다.
SYS_FW_INTERFACE_HARDWARE_ID_LIST	디바이스의 인터페이스에 대한 하드웨어 이름 목록(예: GigabitEthernet0/0)입니다.
SYS_FW_INTERFACE_NAME_LIST	디바이스의 인터페이스에 대한 논리적 이름 목록입니다(예: inside).
SYS_FW_INLINE_INTERFACE_NAME_LIST	수동 또는 ERSPAN 수동으로 구성된 인터페이스의 논리적 이름 목록입니다.
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	모든 라우팅된 인터페이스와 같이 인라인 집합에 속하지 않은 인터페이스의 논리적 이름 목록입니다.

사전 정의된 **FlexConfig** 개체

사전 정의된 FlexConfig 개체는 선택된 기능에 대해 테스트된 구성을 제공합니다. 이러한 기능을 구성해야 하는 경우 이 개체를 사용하십시오. 그렇지 않은 경우 Firepower Management Center를 통해 구성할 수 없습니다.

다음 테이블에는 사용 가능한 개체가 나와 있습니다. 연결된 텍스트 개체를 적어 둡니다. 사전 정의된 FlexConfig 개체의 동작을 사용자 정의하려면 이러한 텍스트 개체를 편집해야 합니다. 텍스트 개체를 사용하면 네트워크 및 디바이스에 필요한 IP 주소 및 기타 속성을 사용하여 구성을 사용자 정의할 수 있습니다.

사전 정의된 FlexConfig 개체를 수정해야 할 경우 개체를 복사하고 복사본을 변경한 다음 새 이름으로 저장합니다. 사전 정의된 FlexConfig 개체를 직접 편집할 수 없습니다.

FlexConfig를 사용하여 다른 ASA 기반 기능을 구성할 수도 있지만 이러한 기능의 구성은 테스트되지 않았습니다. ASA 기능이 Firepower Management Center 정책에서 구성할 수 있는 기능과 중복되는 경우 FlexConfig를 통해 구성하지 마십시오.

예를 들어 Snort 검사에는 HTTP 프로토콜이 포함되어 있으므로 ASA 스타일 HTTP 검사를 활성화하지 마십시오. (실제로 **http**를 enableInspectProtocolList 개체에 추가할 수 없습니다. 이 경우 디바이스를 잘못 구성하는 것이 방지됩니다.) 대신, HTTP 검사 요구 사항을 구현하기 위해 필요에 따라 애플리케이션 또는 URL 필터링을 수행하도록 액세스 제어 정책을 구성합니다.

FlexConfig 개체 이름	설명	연결된 텍스트 개체
Default_DNS_Configure (사용되지 않음)	데이터 인터페이스에서 정규화된 도메인 이름을 확인할 때 사용할 수 있는 DNS 서버를 정의하는 기본 DNS 그룹을 구성합니다. 이렇게 하면 **ping**처럼 IP 주소가 아닌 호스트 이름을 사용하여 CLI에서 명령을 사용할 수 있습니다. 버전 6.3부터 Firepower Threat Defense 플랫폼 설정 정책에서 데이터 인터페이스에 대한 DNS를 구성합니다.	defaultDNSNameServerList, defaultDNSParameters
Default_Inspection_Protocol_Disable	global_policy 기본 정책 맵에서 프로토콜을 비활성화합니다.	disableInspectProtocolList
Default_Inspection_Protocol_Enable	global_policy 기본 정책 맵에서 프로토콜을 활성화합니다.	enableInspectProtocolList
DHCPv6_Prefix_Delegation_Configure	IPv6 접두사 위임을 위해 외부 인터페이스(Prefix Delegation 클라이언트) 및 내부 인터페이스(위임된 접두사의 수신자)를 하나씩 구성할 수 있습니다. 이 템플릿을 사용하려면 복사하여 변수를 수정합니다.	pdoutside, pdinside 또한 시스템 변수 SYS_FTD_ROUTED_INTF_MAP_LIST를 사용합니다.
DHCPv6_Prefix_Delegation_UnConfigure	DHCPv6 접두사 위임 구성을 제거합니다.	pdoutside, pdinside 또한 시스템 변수 SYS_FTD_ROUTED_INTF_MAP_LIST를 사용합니다.
DNS_Configure	기본값이 아닌 DNS 서버 그룹에 DNS 서버를 구성합니다. 그룹의 이름을 변경하려면 개체를 복사합니다.	dnsNameServerList, dnsParameters.

FlexConfig 개체 이름	설명	연결된 텍스트 개체
DNS_UnConfigure	Default_DNS_Configure 및 DNS_Configure가 수행하는 DNS 서버 구성을 제거합니다. DNS_Configure를 변경한 경우 개체를 복사하여 DNS 서버 그룹 이름을 변경합니다.	—
Eigrp_Configure	EIGRP 라우팅 next-hop, auto-summary, router-id, eigrp-stub을 구성합니다.	eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary
Eigrp_Interface_Configure	EIGRP 인터페이스 인증 모드, 인증 키, hello 간격, 보류 시간, split horizon을 구성합니다.	eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon 또한 시스템 변수 SYS_FTD_ROUTED_INTF_MAP_LIST를 사용합니다.
Eigrp_Unconfigure	- 5) 디바이스의 자율 시스템에 대한 EIGRP 구성을 지웁니다.	—
Eigrp_Unconfigure_all	모든 EIGRP 구성을 지웁니다.	—
Inspect_IPv6_Configure	global_policy 정책 맵에서 IPv6 검사를 구성하고 IPv6 헤더 내용을 기반으로 트래픽을 기록 및 삭제합니다.	IPv6RoutingHeaderDropLogList, IPv6RoutingHeaderLogList, IPv6RoutingHeaderDropList.
Inspect_IPv6_UnConfigure	IPv6 검사를 지우고 비활성화합니다.	—
ISIS_Configure	IS-IS 라우팅에 대한 전역 파라미터를 구성합니다.	isIsNet, isIsAddressFamily, isISType
ISIS_Interface_Configuration	인터페이스 레벨 IS-IS 구성.	isIsAddressFamily, IsIsIntfList 또한 시스템 변수 SYS_FTD_ROUTED_INTF_MAP_LIST를 사용합니다.
ISIS_Unconfigure	디바이스의 IS-IS 라우터 구성을 지웁니다.	—
ISIS_Unconfigure_All	디바이스 인터페이스의 라우터 할당을 포함하여 디바이스에서 IS-IS 라우터 구성을 지웁니다.	—

FlexConfig 개체 이름	설명	연결된 텍스트 개체
Netflow_Add_Destination	Netflow 내보내기 대상을 만들고 구성합니다.	Netflow_Destinations, netflow_Event_Types
Netflow_Clear_Parameters	Netflow 내보내기 전역 기본 설정을 복원합니다.	—
Netflow_Delete_Destination	Netflow 내보내기 대상을 삭제 합니다.	Netflow_Destinations, netflow_Event_Types
Netflow_Set_Parameters	Netflow 내보내기 전역 파라미터를 설정합니다.	netflow_Parameters
NGFW_TCP_NORMALIZATION	기본 TCP 정규화 구성을 수정합니다.	—
Policy_Based_Routing	이 예제 구성을 사용하려면 복사하고, 인터페이스 이름을 수정하고, r-map-object 텍스트 개체를 사용하여 개체 관리자에서 경로 맵 개체를 식별합니다.	—
Policy_Based_Routing_Clear	디바이스에서 정책 기반 라우팅 구성을 지웁니다.	—
Sysopt_AAA_radius	RADIUS 계정 응답에서 인증 키를 무시합니다.	—
Sysopt_AAA_radius_negate	Sysopt_AAA_radius 구성을 무효화합니다.	—
Sysopt_basic	sysopt 대기 시간, TCP 패킷의 최대 세그먼트 크기 및 자세한 트래픽 통계를 구성합니다.	tcpMssMinimum, tcpMssBytes
Sysopt_basic_negate	sysopt_basic 세부 트래픽 통계, 대기 시간 및 TCP 최대 세그먼트 크기를 지웁니다.	—
Sysopt_clear_all	디바이스에서 모든 sysopt 구성을 지웁니다.	—
Sysopt_noproxyarp	noproxy-arp CLI를 구성합니다.	시스템 변수 SYS_FW_NON_INLINE_INTF_NAME_LIST를 사용합니다.
Sysopt_noproxyarp_negate	Sysopt_noproxyarp 구성을 지웁니다.	시스템 변수 SYS_FW_NON_INLINE_INTF_NAME_LIST를 사용합니다.

FlexConfig 개체 이름	설명	연결된 텍스트 개체
Sysopt_Preserve_Vpn_Flow	syopt preserve VPN 흐름을 구성합니다.	—
Sysopt_Preserve_Vpn_Flow_negate	Sysopt_Preserve_Vpn_Flow 구성을 지웁니다.	—
Sysopt_Reclassify_Vpn	sysopt reclassify vpn을 구성합니다.	—
Sysopt_Reclassify_Vpn_Negate	sysopt reclassify vpn을 무효화합니다.	—
TCP_Embryonic_Conn_Limit (사용되지 않음)	SYN 플러드 서비스 거부(DoS) 공격으로부터 보호하기 위해 원시 연결 제한을 구성합니다. 버전 6.3부터 Firepower Threat Defense Service 정책에서 이러한 기능을 구성합니다. 해당 정책은 디바이스에 할당된 액세스 제어 정책의 Advanced(고급) 탭에서 찾을 수 있습니다.	tcp_conn_misc, tcp_conn_limit
TCP_Embryonic_Conn_Timeout (사용되지 않음)	SYN 플러드 서비스 거부(DoS) 공격으로부터 보호하기 위해 원시 연결 시간 초과를 구성합니다. 버전 6.3부터 Firepower Threat Defense Service 정책에서 이러한 기능을 구성합니다. 해당 정책은 디바이스에 할당된 액세스 제어 정책의 Advanced(고급) 탭에서 찾을 수 있습니다.	tcp_conn_misc, tcp_conn_timeout
Threat_Detection_Clear	위협 탐지 TCP 가로채기 구성을 지웁니다.	—
Threat_Detection_Configure	TCP 가로채기에 의해 가로채기된 공격에 대한 위험 탐지 통계를 구성합니다.	threat_detection_statistics
VxLAN_Clear_Nve	VxLAN_Configure_Port_And_Nve 디바이스에서 사용 하는 경우 구성 된 NVE 1을 제거 합니다.	—
VxLAN_Clear_Nve_Only	구축될 때 인터페이스에 구성된 NVE를 지웁니다.	—
VxLAN_Configure_Port_And_Nve	VLAN 포트 및 NVE 1을 구성합니다.	vxlan_Port_And_Nve

FlexConfig 개체 이름	설명	연결된 텍스트 개체
VxLAN_Make_Nve_Only	NVE 전용 인터페이스를 설정합니다.	vxlan_Nve_Only 또한 시스템 변수 SYS_FTD_ROUTED_MAP_LIST 및 SYS_FTD_SWITCHED_INTF_MAP_LIST를 사용합니다.
VxLAN_Make_Vni	VNI 인터페이스를 만듭니다. 구축한 후에는 VNI 인터페이스를 제대로 검색할 수 있도록 디바이스를 등록 취소하고 다시 등록해야 합니다.	vxlan_Vni
Wccp_Configure	이 템플릿은 WCCP를 구성하는 예제를 제공합니다.	isServiceIdentifier, serviceIdentifier, wccpPassword
Wccp_Configure_Clear	WCCP 구성을 지웁니다.	—

사전 정의된 텍스트 개체

여러 개의 사전 정의된 텍스트 개체가 있습니다. 이 개체는 사전 정의된 FlexConfig 개체에 쓰이는 변수와 관련 있습니다. 대부분의 경우 관련 FlexConfig 개체를 사용하는 경우 이 개체를 편집하여 값을 추가해야 합니다. 그렇지 않으면 구축 중에 오류가 표시됩니다. 이러한 옵션 중 일부는 기본값을 포함하고 있으나 어떤 옵션은 비어 있습니다.

텍스트 개체 편집에 대한 내용은 FlexConfig 텍스트 개체 설정, 1298 페이지 섹션을 참조하십시오.

이름	설명	관련 **FlexConfig** 개체
defaultDNSNameServerList (사용되지 않음)	기본 DNS 그룹에서 구성할 DNS 서버 IP 주소입니다. 버전 6.3부터 Firepower Threat Defense 플랫폼 설정 정책에서 데이터 인터페이스에 대한 DNS를 구성합니다.	Default_DNS_Configure
defaultDNSParameters (사용되지 않음)	기본 DNS 서버 그룹에 대한 DNS 동작을 제어하는 파라미터입니다. 개체에는 재시도, 시간 초과, expire-entry-timer, poll-timer, domain-name에 대한 개별 항목이 순서대로 포함됩니다. 버전 6.3부터 Firepower Threat Defense 플랫폼 설정 정책에서 데이터 인터페이스에 대한 DNS를 구성합니다.	Default_DNS_Configure

이름	설명	관련 **FlexConfig** 개체
disableInspectProtocolList	기본 정책 맵에서 프로토콜을 비활성화합니다(global_policy).	Disable_Default_Inspection_Protocol
dnsNameServerList	사용자 정의 DNS 그룹에서 구성할 DNS 서버 IP 주소입니다.	DNS_Configure
dnsParameters	기본값 이외의 DNS 서버 그룹에 대한 DNS 동작을 제어하는 파라미터입니다. 개체에는 재시도, 시간 초과, domain-name, name-server-interface에 대한 개별 항목이 순서대로 포함됩니다.	DNS_Configure
eigrpAS	자율 시스템 번호입니다.	Eigrp_Configure, Eigrp_Interface_Configure, Eigrp_Unconfigure
eigrpAuthKey	EIGRP 인증 키입니다.	Eigrp_Interface_Configure
eigrpAuthKeyId	인증 키와 일치하는 공유 키 ID입니다.	Eigrp_Interface_Configure
eigrpDisableAutoSummary	true일 때 자동 요약을 비활성화하는 플래그입니다.	Eigrp_Configure
eigrpDisableSplitHorizon	true일 때 split horizon을 비활성화하는 플래그입니다.	Eigrp_Interface_Configure
eigrpHelloInterval	hello 전송 간격(초)입니다.	Eigrp_Interface_Configure
eigrpHoldTime	네이버가 중단된 것으로 간주하기 전의 시간(초)입니다.	Eigrp_Interface_Configure
eigrpIntfList	EIGRP가 적용될 논리적 인터페이스 이름 목록입니다.	Eigrp_Interface_Configure
eigrpRouterId	IP 주소 형식의 라우터-Id입니다.	Eigrp_Configure
eigrpStubConnected	true일 때 **eigrp stub** 구성을 **connected**에서 사용할 수 있는 플래그입니다.	Eigrp_Configure
eigrpStubReceiveOnly	true일 때 **eigrp stub** 구성을 **receive-only**에서 사용할 수 있는 플래그입니다.	Eigrp_Configure
eigrpStubRedistributed	true일 때 **eigrp stub** 구성을 **redistributed**에서 사용할 수 있는 플래그입니다.	Eigrp_Configure
eigrpStubSummary	true일 때 **eigrp stub** 구성을 **summary**에서 사용할 수 있는 플래그입니다.	Eigrp_Configure

이름	설명	관련 **FlexConfig** 개체
enableInspectProtocolList	기본 정책 맵에서 프로토콜을 활성화합니다(global_policy). 해당 프로토콜 검사가 Snort 검사와 충돌하는 프로토콜을 추가할 수 없습니다.	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	허용하지 않으려는 IPv6 라우팅 헤더 유형의 목록입니다. IPv6 검사는 중단을 기록하지 않고 이러한 헤더가 포함된 패킷을 삭제합니다.	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	허용 및 기록하지 않으려는 IPv6 라우팅 헤더 유형의 목록입니다. IPv6 검사는 이러한 헤더가 포함된 패킷을 삭제하고 중단에 대한 시스템 로그 메시지를 보냅니다.	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	허용하지만 기록하지 않으려는 IPv6 라우팅 헤더 유형의 목록입니다. IPv6 검사는 이러한 헤더를 포함하는 패킷을 허용하지만 헤더의 존재 여부에 대한 시스템 로그 메시지를 보냅니다.	Inspect_IPv6_Configure
isIsAddressFamily	IPv4 또는 IPv6 주소군입니다.	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	논리적 인터페이스 이름 목록입니다.	ISIS_Interface_Configuration
isIsISType	IS 유형(level-1, level-2-only 또는 level-1-2)입니다.	ISIS_Configure
isIsNet	네트워크 엔티티입니다.	ISIS_Configure
isServiceIdentifier	false이면 표준 **web-cache** 서비스 식별자를 사용합니다.	Wccp_Configure
netflow_Destination	단일 Netflow 내보내기 대상의 인터페이스, 대상, UDP 포트 번호를 정의합니다.	Netflow_Add_Destination
netflow_Event_Types	대상에 대해 내보낼 이벤트 유형을 **all**, **flow-create**, **flow-defined**, **flow-teardown**, **flow-update**의 하위 집합으로 정의합니다.	Netflow_Add_Destination

이름	설명	관련 **FlexConfig** 개체
netflow_Parameters	Netflow 내보내기 전역 설정(활성 새로 고침 간격(흐름 업데이트 이벤트사이의 시간(분)), 지연(초 단위의 흐름 생성 지연, 기본값 0 = 명령이 나타나지 않음) 및 템플릿 시간 초과 비율(분)을 제공합니다.	Netflow_Set_Parameters
PrefixDelegationInside	DHCPv6 접두사 위임을 위한 내부 인터페이스를 구성합니다. 개체에는 인터페이스 이름, 프리픽스 길이가 포함된 IPv6 접미사 및 접두사 풀 이름 순서대로 여러 항목이 포함됩니다.	없음. 하지만 DHCPv6_Prefix_Delegation_Configure 사본과 함께 사용할 수 있습니다.
PrefixDelegationOutside	외부 DHCPv6 접두사 위임 클라이언트를 구성합니다. 개체에는 인터페이스 이름, 프리픽스 길이 순서대로 여러 항목이 포함됩니다.	없음. 그러나 DHCPv6_Prefix_Delegation_Configure 사본과 함께 사용할 수 있습니다.
serviceIdentifier	동적 WCCP 서비스 식별자 번호입니다.	Wccp_Configure
tcp_conn_limit (사용되지 않음)	TCP 원시 연결 제한을 구성하는 데 사용되는 파라미터입니다. 버전 6.3부터 Firepower Threat Defense Service 정책에서 이러한 기능을 구성합니다. 해당 정책은 디바이스에 할당된 액세스 제어 정책의 Advanced(고급) 탭에서 찾을 수 있습니다.	TCP_Embryonic_Conn_Limit
tcp_conn_misc (사용되지 않음)	TCP 원시 연결 설정을 구성하는 데 사용되는 파라미터입니다. 버전 6.3부터 Firepower Threat Defense Service 정책에서 이러한 기능을 구성합니다. 해당 정책은 디바이스에 할당된 액세스 제어 정책의 Advanced(고급) 탭에서 찾을 수 있습니다.	TCP_Embryonic_Conn_Limit, TCP_Embryonic_Conn_Timeout
tcp_conn_timeout (사용되지 않음)	TCP 원시 연결 시간 초과를 구성하는 데 사용되는 파라미터입니다. 버전 6.3부터 Firepower Threat Defense Service 정책에서 이러한 기능을 구성합니다. 해당 정책은 디바이스에 할당된 액세스 제어 정책의 Advanced(고급) 탭에서 찾을 수 있습니다.	TCP_Embryonic_Conn_Timeout

이름	설명	관련 **FlexConfig** 개체
tcpMssBytes	최대 세그먼트 크기(바이트)입니다.	Sysopt_basic
tcpMssMinimum	이 플래그가 true인 경우에만 설정되는 최대 세그먼트 크기(MSS)를 설정할지 여부를 확인합니다.	Sysopt_basic
threat_detection_statistics	TCP 가로채기에 대한 위협 탐지 통계에 사용되는 파라미터입니다.	Threat_Detection_Configure
vxlan_Nve_Only	인터페이스에서 NVE 전용 구성을 위한 파라미터: • 인터페이스의 논리적 이름 • IPv4 주소(라우팅된 인터페이스에 대한 선택 사항) • IPv4 넷마스크(라우팅된 인터페이스에 대한 선택 사항)	VxLAN_Make_Nve_Only
vxlan_Port_And_Nve	포트 및 VXLAN용 NVE 구성에 사용되는 파라미터: • vxlan port • 소스 인터페이스(논리적 이름) • 유형(피어 또는 mcast) • 피어 IP 주소 또는 default-mcast-grooup	VxLAN_Configure_Port_And_Nve
vxlan_Vni	VNI 생성에 사용되는 파라미터: • 인터페이스 번호(1-10000) • segment-id(1-16777215) • nameif(논리적 인터페이스 이름) • 유형(라우팅 또는 투명) • IP 주소(라우팅된 모드 디바이스의 경우 사용) 또는 브리지 그룹 번호(투명 모드 디바이스의 경우 사용) • 넷마스크(디바이스가 라우팅 모드에 있는 경우) 또는 사용되지 않음	VxLAN_Make_Vni
wccpPassword	WCCP 비밀번호.	Wccp_Configure

FlexConfig 정책에 대한 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

FlexConfig 가이드라인 및 제한 사항

- FlexConfig 정책을 잘못 수행하면 실패한 FlexConfig가 포함된 구축 시도의 모든 변경 사항이 롤백됩니다. 구축 실패로 인한 롤백에는 구성 지우기가 포함되므로 네트워크에 지장을 줄 수 있습니다. 업무 시간 외 FlexConfig 변경 사항을 포함하는 구축을 고려하십시오. 또한 FlexConfig 변경 사항만 포함되도록 구축을 격리하고 다른 정책 업데이트는 고려하지 마십시오.
- VxLAN_Make_VNI 개체를 사용하는 경우 클러스터 또는 고가용성 쌍을 구성하기 전에 동일한 FlexConfig를 클러스터 또는 고가용성 쌍의 모든 유닛에 구축해야 합니다. Management Center에서는 클러스터 또는 고가용성 쌍을 만들기 전에 모든 디바이스에서 VXLAN 인터페이스를 일치시켜야 합니다.
- 트래픽 영역을 사용하여 Equal-Cost-Multi-Path(ECMP) 라우팅을 구성하려는 경우 **zone** 명령은 ASA에서 사용되는 것과 비교하여 FTD 디바이스에 따라 다릅니다. ASA 일반 설정 가이드의 지침을 계속 수행할 수 있더라도 ASA 버전의 명령 대신 **zone** *name* **ecmp**을 사용하십시오. 그렇지 않은 경우 트래픽 영역 기능의 작동은 ASA와 FTD 간에 동일합니다.

참고 또한 일부 인터페이스를 수동으로 정의한 경우 시스템에서는 수동 영역을 구성하기 위해 **zone** *name* **passive** 명령을 구성합니다. 이는 인터페이스 구성에 따라 자동으로 처리됩니다. 수동 트래픽 영역을 생성하려면 FlexConfig를 사용하지 마십시오.

FlexConfig 정책을 사용한 디바이스 설정 맞춤 설정

FlexConfig 정책을 사용하여 FTD 디바이스 구성을 사용자 정의합니다.

FlexConfig를 사용하기 전에 Firepower Management Center의 다른 기능을 사용하여 필요한 모든 정책과 설정을 구성합니다. FlexConfig는 FTD와 호환되지만 Firepower Management Center에서는 구성할 수 없는 ASA 기반 기능을 구성하기 위한 마지막 수단입니다.

다음은 FlexConfig 정책을 구성하고 구축하기 위한 엔드 투 엔드 절차입니다.

프로시저

단계 **1** 구성하려는 CLI 명령 시퀀스를 결정합니다.

ASA 디바이스에서 작동하는 구성이 있는 경우 **show running-config**를 사용하여 필요한 명령 시퀀스를 가져옵니다. 필요에 따라 인터페이스 이름 및 IP 주소와 같은 항목을 조정합니다.

이 기능이 새로운 기능인 경우 올바른 명령 시퀀스인지 확인하기 위해 실험실 설정에서 ASA 디바이스에 구현하는 것이 가장 좋습니다.

자세한 내용은 다음 주제를 참고하십시오.

- FlexConfig 정책에 대한 추천 사용, 1270 페이지
- FlexConfig 개체의 CLI 명령, 1270 페이지

단계 **2** 목차에서 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 선택합니다.

사전 정의된 FlexConfig 개체를 검사하여 필요한 명령을 생성할 수 있는지 확인합니다. 보기 ( )을 클릭해서 개체 내용을 볼 수 있습니다. 기존 개체가 원하는 개체에 가까울 경우 해당 개체의 사본을 만든 다음 편집합니다. 사전 정의된 FlexConfig 개체, 1281 페이지의 내용을 참조하십시오.

개체를 검사하면 FlexConfig 개체의 구조, 명령 구문 및 예상되는 시퀀스에 대한 아이디어를 얻을 수 있습니다.

참고 직접 또는 사본으로 사용할 개체를 찾는 경우 개체의 맨 아래에 있는 변수 목록을 검사합니다. 시스템 변수인 SYS로 시작하는 모든 대문자를 제외한 변수 이름을 기록합니다. 이러한 변수는 특히 기본값 열에서 해당 개체에 값이 없다는 것이 표시되는 경우 편집하고 재정의해야 하는 텍스트 개체입니다.

단계 **3** 자체 FlexConfig 개체를 생성해야 하는 경우 필요한 변수를 결정하고 관련 개체를 생성합니다.

배포해야 하는 CLI에는 IP 주소, 인터페이스 이름, 포트 번호 및 시간 경과에 따라 조정할 수 있는 기타 파라미터가 포함될 수 있습니다. 이러한 변수는 필요한 값을 포함하는 개체를 가리키는 변수로 가장 잘 격리되어 있습니다. 구성의 일부이지만 시간 경과에 따라 변경될 수 있는 문자열에 대한 변수가 필요할 수도 있습니다.

또한 정책을 할당할 각 디바이스마다 다른 값이 필요한지 여부도 결정합니다. 예를 들어 세 가지 디바이스에 기능을 구성하려고 할 수 있지만 각 디바이스에 대해 지정된 명령에 다른 인터페이스 이름이나 IP 주소를 지정해야 할 수 있습니다. 각 디바이스에 대해 개체를 사용자 정의해야 하는 경우 개체를 생성할 때 재정의를 활성화하도록 설정한 다음 디바이스별로 재정의 값을 정의합니다.

다양한 유형의 변수에 대한 설명과 필요한 경우 관련 개체를 구성하는 방법에 대해서는 다음 주제를 참조하십시오.

- FlexConfig 변수, 1274 페이지
- FlexConfig 정책 개체 변수, 1279 페이지
- FlexConfig 시스템 변수, 1280 페이지
- FlexConfig 텍스트 개체 설정, 1298 페이지

단계 **4** 사전 정의된 FlexConfig 개체를 사용하는 경우 변수로 사용되는 텍스트 개체를 편집하십시오.

FlexConfig 텍스트 개체 설정, 1298 페이지의 내용을 참조하십시오.

단계 **5** (필요한 경우) FlexConfig 개체 구성, 1293 페이지.

사전 정의된 개체가 작업을 수행할 수 없는 경우에만 개체를 생성해야 합니다.

단계 **6** FlexConfig 정책 설정, 1299 페이지.

단계 **7** FlexConfig 정책에 대한 대상 디바이스 설정, 1300 페이지.

정책을 생성할 때 디바이스에 해당 정책을 할당할 수도 있습니다. 미리보기 전에 정책에 할당된 디바이스가 하나 이상 있어야 합니다.

단계 **8** FlexConfig 정책 미리보기, 1301 페이지.

정책을 미리보기 전에 변경 사항을 저장해야 합니다.

생성된 명령이 의도된 것인지, 모든 변수가 올바르게 확인되는지 확인하십시오.

단계 **9** 메뉴 모음에서 **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다.

단계 **10** 정책에 할당된 디바이스를 선택하고 **Deploy(**구축**)**를 클릭합니다.

구축이 완료될 때까지 기다립니다.

단계 **11** 구축된 설정 확인, 1302 페이지.

단계 **12** (필요한 경우) FlexConfig를 사용하여 설정된 기능 제거, 1304 페이지.

다른 유형의 정책과 달리 디바이스에서 FlexConfig를 할당 해제하면 관련 구성이 제거되지 않을 수 있습니다. FlexConfig 생성 구성을 제거하려면 언급된 절차를 따릅니다.

FlexConfig 개체 구성

FlexConfig 개체를 사용하여 디바이스에 구축할 구성을 정의합니다. 각 FlexConfig 정책은 FlexConfig 개체 목록으로 구성되므로 개체는 본질적으로 Apache Velocity 스크립팅 명령, ASA 소프트웨어 구성 명령 및 변수로 구성된 코드 모듈입니다.

직접 사용할 수 있는 사전 정의된 FlexConfig 개체가 있으며, 편집해야 할 경우 사본을 만들 수 있습니다. 처음부터 자체 개체를 생성할 수도 있습니다. FlexConfig 개체의 콘텐츠는 단순한 단일 명령 문자열에서부터 CLI 명령어 구조를 정의하는 범위까지 다양합니다. 이때 이 구조는 변수 및 스크립팅 명령을 사용하여 콘텐츠가 디바이스 간 또는 구축 간 다를 수 있는 명령을 구축합니다.

FlexConfig 정책을 정의할 때 FlexConfig 정책 개체를 생성할 수도 있습니다.

시작하기 전에

다음에 유의해야 합니다.

- FlexConfig 개체는 명령으로 변환된 다음 디바이스에 구축됩니다. 이러한 명령은 이미 전역 구성 모드에서 실행됩니다. 따라서 **enable** 및 **configure terminal** 명령을 FlexConfig 개체의 일부로 포함하지 마십시오.
- 필요한 변수 유형을 결정하고 필요한 모든 정책 개체를 생성합니다. FlexConfig 개체를 편집하는 동안 변수에 대한 개체를 생성할 수 없습니다.
- 명령이 어떤 방식으로도 VPN 또는 디바이스의 액세스 제어 구성과 충돌하지 않는지 확인합니다.
- 인터페이스에 대해 두 개 이상의 명령 집합이 있는 경우 마지막 명령 집합만 구축됩니다. 따라서 시작 및 끝 명령을 사용하여 인터페이스를 구성하지 않는 것이 좋습니다. 인터페이스 구성 예제는 사전 정의된 ISIS_Interface_Configuration FlexConfig 개체를 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 **Add FlexConfig Object(FlexConfig** 개체 추가**)**를 클릭합니다.
- 수정( )을 클릭하여 기존 개체를 편집합니다.
- 보기 ( )을 클릭하여 사전 정의된 개체 콘텐츠를 볼 수 있습니다.
- 사전 정의된 개체를 편집하려면 복사 ( )을 클릭하여 동일한 콘텐츠로 새 개체를 생성합니다.

단계 **4** 개체의 이름과 설명(선택 사항)을 입력합니다.

단계 **5** 개체 본문 영역에 명령 및 지침을 입력하여 필요한 구성을 생성합니다.

개체 콘텐츠는 올바른 ASA 소프트웨어 명령 시퀀스를 생성하는 일련의 스크립팅 명령 및 구성 명령입니다. FTD 디바이스는 ASA 소프트웨어 명령을 사용하여 일부 기능을 구성합니다. 스크립팅 및 구성 명령에 대한 자세한 내용은 다음을 참조하십시오.

- 템플릿 스크립트, 1274 페이지
- FlexConfig 개체의 CLI 명령, 1270 페이지

변수를 사용하여 실행 시간에만 알 수 있거나 디바이스 간에 다를 수 있는 정보를 제공할 수 있습니다. 처리 변수를 입력하면 되지만 **Insert(**삽입**)** 메뉴를 사용하여 정책 개체 또는 시스템 변수와 연관된 변수 또는 비밀 키인 변수를 추가해야 합니다. 변수에 대한 자세한 내용은 FlexConfig 변수, 1274 페이지 섹션을 참조하십시오.

- 시스템 변수를 삽입하려면 **Insert(**삽입**)** > **Insert System Variable(**시스템 변수 삽입**)** > ***Variable Name(***변수 이름***)***을 선택합니다. 이 변수에 대한 자세한 설명은 FlexConfig 시스템 변수, 1280 페이지 섹션을 참조하십시오.
- 정책 개체 변수를 삽입하려면 **Insert(**삽입**)** > **Insert Policy Object(**정책 개체 삽입**)** > ***Object Type(***개체 유형***)***을 선택하여 적절한 유형의 개체를 선택합니다. 그런 다음 변수에 이름(관련 정책 개체와 동일한 이름일 수 있음)을 제공하고 변수와 연결할 개체를 선택한 후 **Save(**저장**)**를 클릭합니다. 이 유형에 대한 자세한 설명은 FlexConfig 정책 개체 변수, 1279 페이지 섹션을 참조하십시오. 자세한 절차는 FlexConfig 개체에 정책 개체 변수 추가, 1296 페이지 섹션을 참조하십시오.
- 비밀 키 변수를 삽입하려면 **Insert(**삽입**)** > **Secret Key(**비밀 키**)**를 선택 하고 변수 이름 및 값을 정의합니다. 자세한 절차는 비밀 키 구성, 1297 페이지 섹션을 참조하십시오.

참고 새 정책 개체 또는 시스템 변수를 생성하려면 **Insert(**삽입**)** 메뉴를 사용해야 합니다. 하지만 해당 변수의 후속 사용을 위해 $를 포함하여 입력해야 합니다. 이는 시스템 변수에서도 마찬가지입니다. 처음 사용할 때 **Insert(**삽입**)** 메뉴에서 추가하십시오. 그런 다음 후속 사용을 위해 입력합니다. 시스템 변수에 **Insert(**삽입**)** 메뉴를 두 번 이상 사용하면 시스템 변수가 변수 목록에 여러 번 추가되고 FlexConfig가 확인하지 않으므로 변경 사항을 저장할 수 없습니다. 변수(정책 개체 또는 시스템 변수와 연관되지 않은 변수)를 처리하려면 변수를 입력합니다. 비밀 키를 추가하는 경우 항상 **Insert(**삽입**)** 메뉴를 사용하십시오. 비밀 키 변수는 변수 목록에 표시되지 않습니다.

단계 **6** 구축 빈도 및 유형을 선택합니다.

- **Deployment(**구축**)** - 개체에 명령을 한 번 또는 항상 구축할지 여부입니다. 올바른 옵션을 선택하는 유일한 방법은 구축 결과를 테스트하는 것입니다.

  Everytime(항상**)**을 선택하여 시작합니다. 그런 다음 FlexConfig 정책에 개체를 연결한 후 구성을 구축합니다. 구축이 성공적으로 완료되면 FlexConfig 정책으로 돌아가서 FlexConfig 정책 미리보기, 1301 페이지에 설명된 대로 할당된 디바이스 중 하나의 구성을 미리 봅니다. `###CLI generated from managed features ###` 섹션에 개체의 명령을 지우거나 무효화하는 명령이 포함되어 있고 `###Flex-config Appended CLI ###` 섹션에 기능을 재구성하는 명령이 포함되어 있는 경우 **Everytime(**항상**)**이 적절한 옵션입니다.

  명령 무효화가 표시되지 않더라도 디바이스 구성을 약간 변경한 다음 다른 구축을 실행합니다. 구축이 성공적으로 완료되면 구축 내역을 확인할 수 있습니다(구축된 설정 확인, 1302 페이지 참조). 오류가 발생하지 않은 상태에서 명령이 다시 실행된 것을 확인하면 **Everytime(**항상**)**을 계속 유지할 수 있습니다.

  시스템에서 개체를 다시 발급하기 전에 먼저 개체의 명령을 무효화하지 않거나 구축으로 인해 명령과 관련된 오류가 발생하는 경우에만 **Once(**한 번**)**로 변경합니다. 경우에 따라 시스템에서 이미 구성된 명령을 실행할 수 없지만 이는 예외의 경우입니다.

  몇 가지 추가 팁:

  - FlexConfig 개체가 네트워크 또는 ACL 개체와 같은 시스템 관리 개체를 가리키는 경우 **Everytime(**항상**)**을 선택합니다. 그렇지 않으면 개체에 대한 업데이트가 구축되지 않을 수 있습니다.

- 개체에서 구성을 지우는 작업만 수행하는 경우 **Once(**한 번**)**를 사용합니다. 그리고 다음 구축 이후에 FlexConfig 정책에서 개체를 제거합니다.

- **Type(**유형**)** - 다음 중 하나를 선택합니다.
  - **Append(**뒤에 추가**)** - (기본값) 개체의 명령은 Firepower Management Center 정책에서 생성된 구성의 마지막에 배치됩니다. 관리 개체에서 생성된 객체를 가리키는 정책 객체 변수를 사용하는 경우 Append(뒤에 추가)를 사용해야 합니다. 다른 정책에 대해 생성된 명령이 개체에 지정된 명령과 중복되면 이 옵션을 선택하여 명령을 덮어쓰지 않아야 합니다. 이는 가장 안전한 옵션입니다.
  - **Prepend(**앞에 추가**)** - 개체의 명령은 Firepower Management Center 정책에서 생성된 구성의 앞에 배치됩니다. 일반적으로 구성을 지우거나 무효화하는 명령에는 Prepend(앞에 추가)를 사용합니다.

단계 **7** (선택 사항). 개체 본문 위에 있는 **Validate(**확인**)**를 클릭하여 스크립트의 무결성을 확인합니다.

Save(저장**)**를 클릭하면 항상 개체가 확인됩니다. 잘못된 개체는 저장할 수 없습니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

FlexConfig 개체에 정책 개체 변수 추가

다른 유형의 정책 개체와 연결된 FlexConfig 정책 개체에 변수를 삽입할 수 있습니다. FlexConfig가 디바이스에 구축되면 이 변수는 연결된 개체의 이름이나 콘텐츠로 확인됩니다.

FlexConfig 개체에서 정책 개체 변수를 처음 사용할 때는 다음 절차를 사용합니다. 개체를 다시 참조해야 하는 경우 변수($ 기호 포함)를 입력합니다. 이러한 변수를 사용하는 방법을 알아보려면 변수 처리 방법, 1275 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **Insert(**삽입**)** > **Insert Policy Object(**정책 개체 삽입**)** > ***Object Type(***개체 유형***)***을 선택하여 적절한 유형의 개체를 선택합니다.

단계 **2** 변수의 이름과 설명(선택 사항)을 입력합니다.

이름은 FlexConfig 개체의 컨텍스트 내에서 고유해야 합니다. 공백을 포함할 수 없습니다. 변수와 연관된 개체와 정확히 동일한 이름을 사용할 수 있습니다.

단계 **3** 변수와 연결할 개체를 선택하고 **Add(**추가**)**를 클릭하여 **Selected Object(**선택한 개체**)** 목록으로 이동합니다.

변수를 단일 개체에만 연결할 수 있습니다.

참고 텍스트 개체의 경우 필요에 따라 사전 정의된 개체를 선택할 수 있습니다. 하지만 이러한 개체의 대부분에는 기본값이 없습니다. 필요한 값을 직접 추가하거나 FlexConfig 개체를 구축할 디바이스의 개체를 재정의로 업데이트해야 합니다. 이러한 개체를 업데이트하지 않고 FlexConfig를 구축하려고 하면 일반적으로 구축 오류가 발생합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

변수는 FlexConfig 개체 편집기의 하단에 있는 변수 목록에 나타납니다.

비밀 키 구성

비밀 키는 비밀번호와 같이 콘텐츠를 마스크 처리하려는 단일 문자열 변수입니다. 이 시스템은 민감한 정보의 전달을 방지하기 위해 이러한 변수에 대한 특수 취급 방식을 제공합니다.

비밀 키는 FlexConfig 개체의 변수 목록에 표시되지 않습니다

다음 절차에 따라 FlexConfig 개체에서 비밀 키 변수를 생성, 삽입 및 관리하십시오. 다른 유형의 변수와 달리 지정된 비밀 키 변수를 삽입해야 할 때마다 **Insert(**삽입**)** 명령을 사용할 수 있습니다. 처리와 관련하여 이러한 변수는 단일 값 텍스트 개체 변수처럼 동작합니다. 단일 값 변수, 1275 페이지 섹션을 참조하십시오.

참고 비밀 키 변수에 정의된 모든 데이터는 FlexConfig 정책을 미리 볼 때를 제외하고 사용자로부터 마스크 처리됩니다. 또한 FlexConfig 정책을 내 보내면 모든 비밀 키 변수의 콘텐츠가 지워집니다. 정책을 가져올 때 각 비밀 키 변수를 수동으로 편집하여 데이터를 입력해야 합니다.

프로시저

단계 **1** FlexConfig 정책 개체를 편집하는 동안 **Insert(**삽입**)** > **Secret Key(**비밀 키**)**를 선택합니다.

단계 **2** Insert Secret Key(비밀 키 삽입) 대화 상자에서 다음 중 하나를 수행합니다.

- 새 키를 생성하려면 **Add Secret Key(**비밀 키 추가**)**를 클릭한 후 다음 정보를 입력하고 **Add(**추가**)**를 클릭합니다.
  - **Secret Key Name(**비밀 키 이름**)** - 변수 이름입니다. 이 이름은 접두사가 @인 FlexConfig 개체에 나타납니다.
  - **Password(**비밀번호**)**, **Confirm Password(**비밀번호 확인**)** - 입력할 때 별표로 마스크 처리되는 비밀 문자열입니다.
- FlexConfig 개체에 비밀 키 변수를 삽입하려면 변수의 확인란을 선택합니다.
- 비밀 키 변수 값을 편집하려면 해당 변수의 수정( )을 클릭합니다. 필요에 맞게 변경하고 **Add(**추가**)**를 클릭합니다.

- 비밀 키를 삭제하려면 해당 변수의 삭제( )을 클릭합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

FlexConfig 텍스트 개체 설정

FlexConfig 개체의 텍스트 개체를 정책 개체 변수의 대상으로 사용합니다. 변수를 사용하여 실행 시간에만 알 수 있거나 디바이스 간에 다를 수 있는 정보를 제공할 수 있습니다. 구축 중에 텍스트 개체를 가리키는 변수는 텍스트 개체의 콘텐츠로 대체됩니다.

텍스트 개체에는 키워드, 인터페이스 이름, 숫자, IP 주소 등 자유 형식 문자열이 포함됩니다. 콘텐츠는 FlexConfig 스크립트 내에서 정보를 사용하는 방법에 따라 다릅니다.

텍스트 개체를 생성하거나 편집하기 전에 필요한 콘텐츠를 정확히 결정하십시오. 여기에는 개체를 처리하는 방법이 포함되어 있어 단일 문자열 또는 다중 문자열 개체를 생성할지 결정하는 데 도움이 됩니다. 다음 주제를 읽습니다.

- FlexConfig 변수, 1274 페이지
- 변수 처리 방법, 1275 페이지

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **FlexConfig** > **Text Object(**텍스트 개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 **Add Text Object(**텍스트 개체 추가**)**를 클릭합니다.
- 수정( )을 클릭하여 기존 개체를 편집합니다. 사전 정의된 텍스트 개체를 편집할 수 있으며, 이는 사전 정의된 FlexConfig 개체를 사용하려는 경우 필요합니다.

단계 **4** 개체의 이름과 설명(선택 사항)을 입력합니다.

단계 **5** (새 개체에만 해당) 드롭다운 목록에서 **Variable Type(**변수 유형**)**을 선택합니다.

- **Single(**단일**)** - 개체가 단일 텍스트 문자열을 포함해야 하는 경우
- **Multiple(**다중**)** - 개체가 텍스트 문자열 목록을 포함해야 하는 경우

개체를 저장 한 후에는 변수 유형을 변경할 수 없습니다.

단계 **6** 변수 유형이 **Multiple(**다중**)**인 경우 위쪽 및 아래쪽 화살표를 사용하여 **Count(**개수**)**를 지정합니다.

숫자를 변경하면 개체에서 행이 추가되거나 제거됩니다.

단계 **7** 개체에 콘텐츠를 추가합니다.

변수 번호 옆에 있는 텍스트 상자를 클릭하고 값을 입력하거나 텍스트 개체를 사용하는 FlexConfig 개체가 할당될 각 디바이스에 대한 디바이스 재정의를 설정할 수 있습니다. 두 가지 작업을 모두 수행할 수도 있습니다. 이 경우 기본 객체에 구성된 값은 지정된 디바이스에 대한 재정의가 없는 경우 기본값으로 사용됩니다.

사전 정의된 개체를 편집할 때는 디바이스 재정의를 사용하는 것이 좋으므로 다른 FlexConfig 정책에서 개체를 사용해야 할 수 있는 다른 사용자가 시스템 기본값을 그대로 유지해야 합니다. 접근 방식은 조직의 요구 사항에 따라 다릅니다.

팁 일부 사전 정의된 개체는 각 값이 특정 용도로 사용되는 여러 값을 필요로 합니다. 설명 텍스트를 주의깊게 읽고 개체의 예상 값을 확인하십시오. 일부 경우에 지침에는 기준 값을 변경하는 대신 재정의를 사용해야 한다고 명시되어 있습니다. enableInspectProtocolList의 경우 해당 프로토콜 검사가 Snort 검사와 호환되지 않는 프로토콜을 입력할 수 없습니다.

디바이스 재정의를 사용하려면 다음을 수행합니다.

a) **Allow Overrides(**재정의 허용**)**를 선택합니다.
b) Overrides(재정의) 영역을 확장하고(필요한 경우) **Add(**추가**)**를 클릭합니다.

   해당 디바이스에 대한 재정의가 이미 있는 경우 해당 재정의를 클릭하고 편집하여 변경합니다.

c) 개체 재정의 추가 대화 상자의 **Targets(**대상**)**에서 값을 정의할 디바이스를 선택하고 **Add(**추가**)**를 클릭하여 Selected Devices(선택한 디바이스) 목록으로 이동합니다.
d) **Override(**재정의**)**를 클릭하고 필요에 따라 **Count(**개수**)**를 조정한 다음 변수 필드를 클릭하고 디바이스에 대한 값을 입력합니다.
e) **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경사항 구축, 498 페이지를 참조하십시오.

FlexConfig 정책 설정

FlexConfig 정책에는 FlexConfig 개체의 순서가 지정된 목록이 두 개 포함되어 있습니다. 하나는 앞에 추가된 목록이고 하나는 뒤에 추가된 목록입니다. 앞에 추가/뒤에 추가에 대한 설명은 FlexConfig 개체 구성, 1293 페이지 섹션을 참조하십시오.

FlexConfig 정책은 여러 디바이스에 할당할 수 있는 공유 정책입니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **FlexConfig**을(를) 선택합니다.
단계 **2** 다음 중 하나를 수행합니다.

- **New Policy(**새 정책**)**를 클릭하여 새 FlexConfig 정책을 생성합니다. 이름을 입력하라는 메시지가 표시됩니다. 선택적으로 Available Devices(사용 가능한 디바이스) 목록에서 디바이스를 선택하고 **Add to Policy(**정책에 추가**)**를 클릭하여 디바이스를 할당합니다. **Save(**저장**)**를 클릭합니다.
- 수정( )을 클릭하여 기존 규칙을 편집합니다. 편집 모드에서 이름이나 설명을 클릭하여 변경할 수 있습니다.
- 동일한 콘텐츠의 새 정책을 만들려면 복사 ( )을 클릭합니다. 이름에 대한 메시지가 표시됩니다. 디바이스 할당은 사본에 대해 유지되지 않습니다.
- 더 이상 필요하지 않은 정책을 제거하려면 Delete(삭제)를 클릭합니다.

단계 **3** **Available FlexConfig(**사용 가능한 **FlexConfig)** 목록에서 정책에 필요한 FlexConfig 개체를 선택하고 >를 클릭하여 정책에 추가합니다.

개체는 FlexConfig 개체에 지정된 구축 유형에 따라 자동으로 목록의 앞이나 뒤에 추가됩니다.

선택한 개체를 제거하려면 개체 옆에 있는 삭제( )를 클릭합니다.

단계 **4** 선택한 각 개체에 대해 해당 개체 옆에 있는 보기 ( )를 클릭하여 개체에 사용된 변수를 식별합니다.

SYS로 시작하는 시스템 변수를 제외하고 변수와 연관된 개체가 비어 있지 않도록 해야 합니다. 빈칸이나 괄호 사이에 아무것도 없는 경우 []는 빈 개체를 나타냅니다. 정책을 구축하기 전에 이러한 개체를 편집해야 합니다.

참고 개체 재정의를 사용하면 해당 값이 이 보기에 표시되지 않습니다. 따라서 기본값이 비어 있어도 필요한 값이 있는 개체를 업데이트하지 않았다는 의미는 아닙니다. 구성을 미리 보면 지정된 디바이스에 대한 변수가 올바르게 확인되는지 여부가 표시됩니다. FlexConfig 정책 미리보기, 1301 페이지를 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 정책의 대상 디바이스를 설정합니다. FlexConfig 정책에 대한 대상 디바이스 설정, 1300 페이지 섹션을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

FlexConfig 정책에 대한 대상 디바이스 설정

FlexConfig 정책을 생성할 때 정책을 사용하는 디바이스를 선택할 수 있습니다. 이후에 아래 설명된 대로 정책에 대한 디바이스 할당을 변경할 수 있습니다.

참고 일반적으로 디바이스에서 정책 할당을 취소하면 시스템은 다음 구축 시 관련 구성을 자동으로 제거합니다. 하지만 FlexConfig 개체는 사용자 정의 명령을 구축하기 위한 스크립트이기 때문에 디바이스에서 FlexConfig 정책 할당을 해제하지 않아도 FlexConfig 개체가 구성한 명령은 제거되지 않습니다. 디바이스 구성에서 FlexConfig 생성 명령을 제거하려는 경우 FlexConfig를 사용하여 설정된 기능 제거, 1304 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **Devices** > **FlexConfig**를 선택하고 FlexConfig 정책을 편집합니다.

단계 **2** **Policy Assignments(**정책 할당**)**를 클릭합니다.

단계 **3** **Targeted Devices(**대상 디바이스**)**에 대상 목록을 만듭니다.

- Add(추가) - 하나 이상의 **Available Devices(**사용 가능한 디바이스**)**를 선택한 다음 **Add to Policy(**정책에 추가**)**를 클릭하거나 **Selected Devices(**선택한 디바이스**)** 목록으로 드래그앤 드롭합니다. 정책을 디바이스, 고가용성 쌍 및 클러스터된 디바이스에 할당할 수 있습니다.
- Delete(삭제) - 단일 디바이스 옆에 있는 삭제( )을 클릭하거나 여러 디바이스를 선택하고 오른쪽 클릭한 다음 **Delete Selection(**선택 사항 삭제**)**을 선택합니다.

단계 **4** 선택 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭하여 FlexConfig 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

FlexConfig 정책 미리보기

FlexConfig 정책을 미리 보고 FlexConfig 개체를 CLI 명령으로 변환하는 방법을 확인합니다. 미리보기는 FlexConfig 개체에 사용되는 스크립트 및 변수에서 선택한 디바이스에 대해 생성될 명령을 표시합니다. 변수는 디바이스 구성에 따라 확인되므로 구축할 대상에 대해 명확히 알 수 있습니다.

미리보기를 사용하여 FlexConfig 개체의 잠재적 문제를 찾습니다. 미리보기에서 예상 결과가 표시될 때까지 개체를 편집합니다.

변수는 디바이스 구성에 따라 다르게 확인될 수 있으므로 각 디바이스에 대한 구성을 별도로 미리 봐야 합니다.

프로시저

단계 **1** **Devices** > **FlexConfig**를 선택하고 FlexConfig 정책을 편집합니다.

단계 **2** 보류 중인 변경 내용이 있을 경우 **Save(**저장**)**를 클릭합니다.

미리보기에는 가장 최근에 저장된 정책 버전에 있던 FlexConfig 개체에 대한 결과만 표시됩니다. 새로 추가된 객체를 미리 보려면 정책을 저장해야 합니다.

단계 **3** **Preview Config(**구성 미리보기**)**를 클릭합니다.

단계 **4** **Select Device(**디바이스 선택**)** 드롭다운 목록에서 디바이스를 선택합니다.

시스템은 디바이스 및 구성된 정책에서 정보를 검색하고 다음 구축 시 디바이스에 대해 생성될 CLI 명령을 결정합니다. 출력을 선택하고 Ctrl+C를 사용하여 클립 보드에 복사할 수 있으며, 추가 분석을 위해 텍스트 파일에 붙여 넣을 수 있습니다.

미리보기에는 다음 섹션이 포함됩니다.

- Flex-config Prepended CLI - 구성에 대해 앞에 추가되는 FlexConfigs 생성 명령입니다.
- 관리되는 기능에서 생성된 CLI - Firepower Management Center에서 구성된 정책에 대해 생성된 명령입니다. 마지막으로 디바이스에 성공적으로 구축된 이후의 새 정책 또는 변경된 정책에 대해 명령이 생성됩니다. 이 명령은 할당된 정책을 구현하는 데 필요한 모든 명령을 나타내지는 않습니다. 이 섹션의 명령은 FlexConfig 개체에서 생성되지 않습니다.
- Flex-config Appended CLI - 구성에 대해 뒤에 추가되는 FlexConfigs 생성 명령입니다.

단계 **5** **Close(**닫기**)**를 클릭하여 미리보기 대화 상자를 종료합니다.

구축된 설정 확인

FlexConfig 정책을 디바이스에 구축한 후 구축이 성공적이었으며 결과 구성이 예상한 그대로인지 확인합니다. 또한 디바이스가 예상대로 작동하는지 확인합니다.

프로시저

단계 **1** 구축에 성공했는지 확인하려면 다음을 수행합니다.

a) 메뉴 모음에서 **System Status(**시스템 상태**)**를 클릭합니다. 이 메뉴는 **Deploy(**구축**)** 및 **System(**시스템**)** 사이에 이름이 지정되지 않은 메뉴입니다.

아이콘은 다음 중 하나와 같으며 오류가 있는 경우 숫자가 포함될 수 있습니다.

- **Indicates No Warnings(**경고 없음 표시**)** — 시스템에 발생한 오류 및 경고가 없음을 나타냅니다.
- Indicates **One or More Warnings(**경고가 하나 이상임을 표시**)** — 시스템에 오류 없이 하나 이상의 경고가 발생했음을 나타냅니다.
- **Indicates One or More Errors(**오류가 하나 이상임을 표시**)** — 시스템에 하나 이상의 오류 및 경고가 발생했음을 나타냅니다.

b) **Deployments(**구축**)**에서 구축에 성공했는지 확인합니다.

c) 특히 실패한 구축에 대한 세부 정보를 보려면 **Show History(**기록 표시**)**를 클릭합니다.
d) 왼쪽 열에있는 작업 목록에서 구축 작업을 선택합니다.

작업 정보는 역순으로 나열되며 가장 최근의 작업이 목록 상단에 표시됩니다.

e) 오른쪽 열의 디바이스에 대한 **Transcript(**기록**)** 열에서 다운로드를 클릭합니다.

구축 기록에는 디바이스로 전송된 명령과 디바이스에서 반환된 응답이 포함되어 있습니다. 이러한 응답은 정보 메시지 또는 오류 메시지일 수 있습니다. 장애가 발생한 구축의 경우 FlexConfig를 통해 전송한 명령 오류를 나타내는 메시지를 확인합니다. 이 오류를 확인하여 명령을 구성하려는 FlexConfig 개체의 스크립트를 수정할 수 있습니다.

참고 관리 기능에 대해 전송된 명령과 FlexConfig 정책에서 생성된 명령이 기록에서 구분되지는 않습니다.

예를 들어 다음 시퀀스에서는 Firepower Management Center(FMC)가 외부에서 논리적 이름으로 GigabitEthernet0/0을 구성하기 위해 명령을 전송했음을 확인할 수 있습니다. 디바이스에서 보안 수준을 0으로 자동 설정했다고 응답했습니다. FTD에서는 어떠한 경우에도 보안 수준을 사용하지 않습니다. FlexConfig와 관련된 메시지는 기록의 CLI Apply(CLI 적용) 섹션에 있습니다.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

단계 **2** 구축된 구성에 예상되는 명령이 포함되어 있는지 확인합니다.

디바이스의 관리 IP 주소에 SSH 연결을 설정하여 이 작업을 수행할 수 있습니다. **show running-config** 명령을 사용하여 구성을 봅니다.

또는 Firepower Management Center 내의 CLI 툴을 사용합니다.

a) **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터링**)**을 선택하고 디바이스의 이름을 클릭합니다.

상태 테이블의 **Count(**개수**)** 열에서 열기/닫기 화살표를 클릭하여 모든 디바이스를 볼 수 있습니다.

b) **Advanced Troubleshooting(**고급 문제 해결**)**을 클릭하십시오.
c) **Threat Defense CLI(**위협 방어 **CLI)**를 클릭합니다.
d) **show**를 명령으로 선택하고 **running-config**를 파라미터로 입력합니다.
e) **Execute(**실행**)**를 클릭합니다.

실행 중인 구성이 텍스트 상자에 나타납니다. 구성을 선택하고 Ctrl+C를 누른 다음 나중에 분석할 수 있도록 텍스트 파일에 붙여 넣을 수 있습니다.

단계 **3** 디바이스가 예상대로 작동하는지 확인합니다.

이 기능과 관련된 **show** 명령을 사용하여 자세한 정보와 통계를 확인합니다. 예를 들어 추가 프로토콜 검사를 활성화한 경우 **show service-policy** 명령은 이 정보를 제공합니다. 사용할 정확한 명령은 기능에 따라 다르며, ASA 설정 가이드 및 기능 구성 방법에 대해 알아보는 데 사용한 명령 참조에 나와 있습니다.

통계를 표시하는 명령에서 숫자가 변경되지 않음을 나타내면(예: 적중 횟수, 연결 수 등) 구성은 유효하지만 의미가 없습니다. 통계에 표시되어야 하는 디바이스를 통해 트래픽이 진행되고 있음을 알고 있는 경우 구성에서 누락된 부분을 찾습니다. 예를 들어 기능이 작동하기 전에 NAT 또는 액세스 규칙이 트래픽을 삭제하거나 변경했을 수 있습니다.

SSH 세션 또는 Firepower Management Center CLI 툴을 통해 **show** 명령을 사용할 수 있습니다.

하지만 사용해야 하는 **show** 명령을 FTD CLI에서 직접 사용할 수 없는 경우 디바이스에 SSH 연결을 설정해서 명령을 사용해야 합니다. CLI에서 다음 명령 시퀀스를 입력하여 진단 CLI 내의 Privileged EXEC 모드로 진입합니다. 여기에서만 지원되는 **show** 명령을 입력할 수 있어야 합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

FlexConfig를 사용하여 설정된 기능 제거

FlexConfig를 사용하여 구성한 일련의 구성 명령을 제거해야 한다고 결정한 경우 해당 구성을 수동으로 제거해야 할 수 있습니다. FlexConfig 정책을 디바이스에서 할당 해제하면 모든 구성이 제거되지 않을 수 있습니다.

구성을 수동으로 제거하려면 새 FlexConfig 개체를 생성하여 구성 명령을 지우거나 무효화합니다.

시작하기 전에

개체에 의해 생성된 구성의 일부 또는 전부를 수동으로 제거해야 하는지 확인하려면 다음을 수행합니다.

1. FlexConfig 정책 미리보기, 1301 페이지에 설명된 대로 구성 미리보기를 검사합니다. `###CLI generated from managed features ###` 섹션에 FlexConfig 개체의 모든 명령을 제거하는 clear 또는 negate 명령이 포함되어 있으면 FlexConfig 정책, 저장 및 재구축 단계에서 개체를 간단히 제거할 수 있습니다.
2. FlexConfig 정책에서 개체를 제거하고 변경 사항을 저장한 다음 구성을 다시 미리 봅니다. `###CLI generated from managed features ###` 섹션에 필요한 clear 또는 negate 명령이 여전히 포함되어 있지 않으면 이 절차에 따라 수동으로 구성을 제거해야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 FlexConfig 개체를 생성하여 구성 명령을 지우거나 무효화합니다.

기능에 모든 구성 설정을 제거할 수 있는 **clear** 명령이 있는 경우 해당 명령을 사용합니다. 예를 들어 사전 정의된 Eigrp_Unconfigure_All 개체에는 모든 EIGRP 관련 구성 명령을 제거하는 단일 명령이 포함되어 있습니다.

```
clear configure router eigrp
```

해당 기능에 대한 **clear** 명령이 없으면 제거할 각 명령의 **no** 형식을 사용해야 합니다. 예를 들어 사전 정의된 Sysopt_basic_negate 개체는 사전 정의된 Sysopt_basic 개체를 통해 구성된 명령을 제거합니다.

```
no sysopt traffic detailed-statistics
```

```
no sysopt connection timewait
```

일반적으로 구성을 prepended, deploy once 개체로 제거하는 FlexConfig 개체를 구성합니다.

단계 **2** **Devices(**디바이스**)** > **FlexConfig**를 선택하고 새 FlexConfig 정책을 생성하거나 기존 정책을 편집합니다.

구성 명령을 구축하는 FlexConfig 정책을 유지하려면 명령을 무효화하기 위한 새 정책을 생성하고 디바이스를 정책에 할당합니다. 그런 다음 새 FlexConfig 개체를 정책에 추가합니다.

FlexConfig 구성 개체를 모든 디바이스에서 완전히 제거하려면 기존 FlexConfig 정책에서 해당 명령을 삭제하고 구성을 무효화하는 개체로 간단히 대체할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭하여 FlexConfig 정책을 저장합니다.

단계 **4** **Preview Config(**구성 미리보기**)**를 클릭하고 clear 및 negation 명령이 올바르게 생성되는지 확인합니다.

단계 **5** 메뉴 모음에서 **Deploy(**구축**)** > **Deployment(**구축**)**를 클릭하고 디바이스를 선택하고 **Deploy(**구축**)**를 클릭합니다.

구축이 완료될 때까지 기다립니다.

단계 **6** 명령이 제거되었는지 확인합니다.

디바이스에서 실행 중인 구성을 보고 명령이 제거되었는지 확인합니다. 자세한 내용은 구축된 설정 확인, 1302 페이지 섹션을 참조하십시오.

단계 **7** FlexConfig 정책을 편집하는 동안 **Policy Assignments(**정책 할당**)**를 클릭하고 디바이스를 제거합니다. 선택적으로 정책에서 FlexConfig 개체를 제거합니다.

FlexConfig 정책이 원치 않는 구성 명령을 간단히 제거한다고 가정하면 제거가 완료된 후 정책을 디바이스에 할당하지 않아도 됩니다.

하지만 FlexConfig 정책이 디바이스에 구성하려는 옵션을 유지하는 경우 정책에서 무효화 개체를 제거합니다. 해당 개체는 더 이상 필요하지 않습니다.

FlexConfig의 예시

다음은 FlexConfig 사용의 몇 가지 예입니다.

Precision Time Protocol을 구성하는 방법(ISA 3000)

PTP(Precision Time Protocol)는 패킷 기반 네트워크에서 다양한 디바이스의 클록을 동기화하기 위해 개발된 시간 동기화 프로토콜입니다. 이러한 디바이스 클록은 일반적으로 정밀도와 안정성이 다양합니다. 이 프로토콜은 산업, 네트워크에 연결된 측정 및 제어 시스템을 위해 특별히 설계되었으며 최소한의 대역폭 및 적은 처리 오버헤드를 필요로 하기 때문에 분산 시스템에서 사용하기에 가장 적합합니다.

PTP 시스템은 PTP 및 비 PTP 디바이스의 조합으로 구성된 분산형, 네트워크에 연결된 시스템입니다. PTP 디바이스에는 일반 클록, 경계 클록 및 투명 클록이 있습니다. 비 PTP 디바이스에는 네트워크 스위치, 라우터 및 기타 인프라 디바이스가 있습니다.

FTD 디바이스를 투명 클록이 되도록 구성할 수 있습니다. FTD 디바이스에서는 클록을 PTP 클록과 동기화하지 않습니다. FTD 디바이스에서는 PTP 클록에 정의된 대로 PTP 기본 프로필을 사용합니다.

PTP 디바이스를 구성할 때 함께 작동할 디바이스의 도메인 번호를 정의합니다. 따라서 여러 PTP 도메인을 구성한 다음, 하나의 특정 도메인에 대해 PTP 클록을 사용하도록 비 PTP 디바이스를 각각 구성할 수 있습니다.

시작하기 전에

디바이스에서 사용해야 하는 PTP 클록에 구성된 도메인 번호를 결정합니다. 이 예에서는 PTP 도메인 번호를 10으로 가정합니다. 또한 시스템에서 도메인의 PTP 클록에 연결하기 위해 통과하는 인터페이스를 결정합니다.

다음은 PTP 구성에 대한 지침입니다.

- 이 기능은 Cisco ISA 3000 어플라이언스에서만 사용할 수 있습니다.
- Cisco PTP는 멀티캐스트 PTP 메시지만 지원합니다.
- PTP는 IPv4 네트워크용으로만 사용할 수 있으며 IPv6 네트워크용으로는 사용할 수 없습니다.
- PTP 구성은 독립형 또는 브리지 그룹 멤버에 관계없이 물리적 이더넷 데이터 인터페이스에서 지원됩니다. 이는 관리 인터페이스, 하위 인터페이스, EtherChannel, BVI(Bridge Virtual Interfaces) 또는 기타 가상 인터페이스에서 지원되지 않습니다.
- VLAN 하위 인터페이스에서 이동하는 PTP가 지원되며 이때 적절한 PTP 구성이 현재 상위 인터페이스에 있다고 가정합니다.
- PTP 패킷이 디바이스를 통해 이동할 수 있는지 확인해야 합니다. PTP 트래픽은 UDP 대상 포트 319 및 320과 대상 IP 주소 224.0.1.129로 식별되므로 이 트래픽을 허용하는 액세스 제어 규칙이 작동해야 합니다.

- 라우팅 방화벽 모드에서는 PTP 멀티캐스트 그룹에 대해 멀티캐스트 라우팅을 활성화해야 합니다. 또한 PTP를 활성화하는 인터페이스가 브리지 그룹에 없는 경우에는 IGMP 멀티캐스트 그룹인 224.0.1.129에 조인하도록 인터페이스를 구성해야 합니다. 물리적 인터페이스가 브리지 그룹 멤버인 경우에는 IGMP 멀티캐스트 그룹에 조인하도록 구성하지 마십시오.

프로시저

단계 **1** (라우팅된 모드 전용) 멀티캐스트 라우팅을 활성화하고, 인터페이스에 대 한 IGMP 그룹을 구성합니다.

라우티드 모드에서는 멀티캐스트 라우팅을 활성화해야 합니다. 또한 독립형 물리적 인터페이스, 즉 브리지 그룹 멤버가 아닌 인터페이스의 경우에는 인터페이스가 224.0.1.129 IGMP 그룹에 가입하도록 구성해야 합니다. 브리지 그룹 멤버가 IGMP 그룹에 가입하도록 구성할 수는 없지만, 브리지 그룹 멤버의 PTP 구성은 IGMP에 가입하지 않아도 정상적으로 적용됩니다.

PTP를 구성할 디바이스별로 이 절차를 수행합니다.

참고 각 디바이스의 PTP 지향 인터페이스의 하드웨어 이름(예: GigabitEthernet1/1)을 기록합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스를 수정합니다.
b) **Routing(**라우팅**)**을 클릭합니다.
c) **Multicast Routing(**멀티캐스트 라우팅**)** > **IGMP**를 선택합니다.
d) **Enable Multicast Routing(**멀티캐스트 라우팅 활성화**)** 확인란을 선택합니다.
e) **Join Group(**조인 그룹**)**을 클릭합니다.
f) **Add(**추가**)**를 클릭하고, Add IGMP Join Group Parameters(IGMP 가입 그룹 매개변수 추가) 대화상자에서 다음 옵션을 구성한 다음 **OK(**확인**)**를 클릭합니다.
   - **Interface(**인터페이스**)** - PTP 지향 독립형 인터페이스를 선택합니다.
   - **Join Group(**조인 그룹**)** - 새 네트워크 개체를 추가하려면 **+**를 클릭합니다. 주소 224.0.1.129를 사용하여 호스트 개체를 생성합니다. 추가 인터페이스를 구성할 때는 이 개체를 선택하기만 하면 됩니다.

   디바이스의 PTP 지향 독립형 인터페이스마다 이 단계를 반복합니다.
g) Routing(라우팅) 페이지에서 **Save(**저장**)**를 클릭합니다.

단계 **2** FlexConfig 개체를 생성해 PTP를 전역 및 인터페이스에서 활성화합니다.

다음 절차에서는 구성 중인 모든 디바이스에서 PTP 지향 인터페이스가 동일하다고 가정합니다. 다른 디바이스에서 다른 인터페이스를 사용한다면, 각 고유 조합에 대해 별도의 개체를 생성해야 합니다. 예를 들어 디바이스 A와 B에서 GigabitEthernet1/1을 사용하고 디바이스 C와 D에서는 GigabitEthernet1/2를 사용하며, 디바이스 E와 F에서는 GigabitEthernet1/1 및 1/2를 모두 사용한다면, 별도의 FlexConfig 개체 3개와 (다음 단계에서 설명하는) 별도의 FlexConfig 정책 3개가 필요합니다.

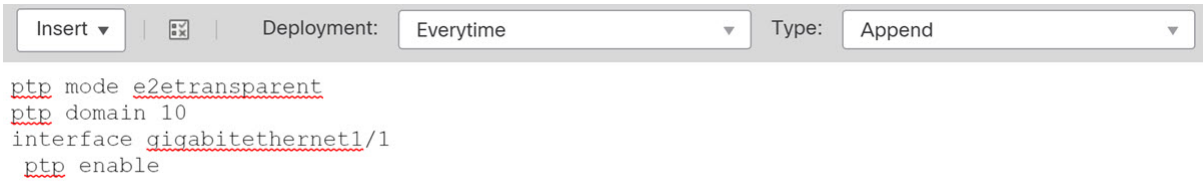
a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.

c) **Add FlexConfig Object(FlexConfig** 개체 추가**)**를 클릭하고, 다음 속성을 구성한 다음 **Save(**저장**)**를 클릭합니다.

- **Name(**이름**)** - 개체 이름입니다. 예를 들어, Enable_PTP입니다.
- **Deployment(**구축**)** - **Everytime(**항상**)**을 선택합니다. 모든 구축에 구성을 전송해 설정 상태를 유지합니다.
- **Type(**유형**)** - 기본값인 **Append(**추가**)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다. 이렇게 하면 인터페이스 구성에 대한 다른 변경 사항은 이러한 명령을 실행하기 전에 설정됩니다.
- **Object body(**개체 본문**)** - 개체 본문에는 PTP를 전역적으로 구성하고 각 PTP 지향 인터페이스에서 구성하는 데 필요한 명령을 입력합니다. 예를 들어 PTP 도메인 10의 전역 구성 및 GigabitEthernet1/1에서의 인터페이스 구성에 필요한 명령은 다음과 같습니다.

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

개체 본문은 다음과 비슷해야 합니다.



단계 **3** FlexConfig 정책을 생성하고 디바이스에 할당합니다.

다양한 PTP 지향 인터페이스 조합에 대한 여러 FlexConfig 개체를 생성했다면, 개체별로 FlexConfig 정책을 만들고 구성해야 하는 인터페이스에 맞는 올바른 디바이스에 정책을 할당해야 합니다. 디바이스 그룹별로 다음 절차를 반복합니다.

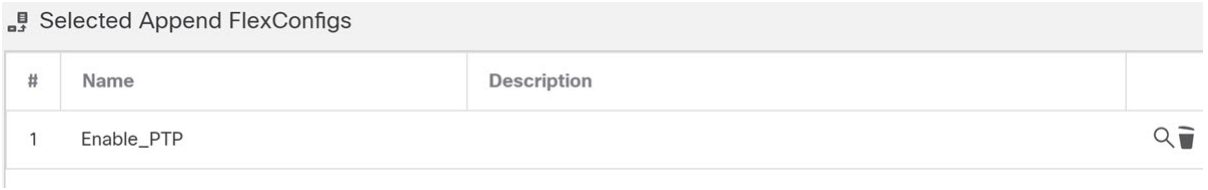
a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.

b) **New Policy(**새 정책**)**를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

c) 목차의 **User Defined(**사용자 정의**)** 폴더에서 PTP FlexConfig 개체를 선택하고 >을 클릭해 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs** 목록에 추가해야 합니다.



d) **Save(**저장**)**를 클릭합니다.

e) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 Save(저장) 아래에 있는 **Policy Assignments(**정책 할당**)** 링크를 클릭하여 할당합니다.

f) **Preview Config(**구성 미리보기**)**를 클릭하고, Preview(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. PTP FlexConfig 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. PTP 명령의 경우 다음과 유사한 내용이 표시되어야 합니다.

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

단계 **4** 변경 사항을 배포합니다.

FlexConfig 정책을 디바이스에 할당했기 때문에 항상 구축 경고가 표시됩니다. FlexConfig는 주의해서 사용해야 한다는 뜻입니다. **Proceed(**계속하기**)**를 클릭하여 구축을 계속 진행합니다.

구축이 끝나면 구축 내역과 구축 기록을 확인할 수 있습니다. 이 기능은 구축이 실패했을 때 특히 유용합니다. 구축된 설정 확인, 1302 페이지의 내용을 참조하십시오.

단계 **5** 각 디바이스의 PTP 구성을 확인합니다.

각 디바이스의 SSH 또는 콘솔 세션에서 PTP 설정을 확인합니다.

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled
```

```
PTP PORT DATASET: GigabitEthernet1/3
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 3
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 4
 PTP version: 2
 Port state: Disabled
```

정전(ISA 3000)에 대한 자동 하드웨어 우회를 구성하는 방법

정전 상태에서도 인터페이스 쌍 간에 트래픽 플로우가 계속되도록 하드웨어 바이패스를 활성화할 수 있습니다. 지원되는 인터페이스 쌍은 구리 인터페이스 GigabitEthernet 1/1과 1/2 및 GigabitEthernet 1/3과 1/4입니다. 파이버 이더넷 모델을 사용하는 경우에는 구리 이더넷 쌍(GigabitEthernet 1/1 및 1/2)만 하드웨어 바이패스를 지원합니다.

하드웨어 바이패스가 활성 상태이면 트래픽이 계층 1에서 이러한 인터페이스 쌍 간을 통과합니다. FTD CLI는 인터페이스가 중단되는 것으로 간주합니다. 방화벽 기능은 없으므로 트래픽의 디바이스 통과를 허용하는 경우의 위험을 파악해야 합니다.

CLI 콘솔 또는 SSH 세션에서 **show hardware-bypass** 명령을 사용하여 운영 상태를 모니터링합니다.

시작하기 전에

다음 조건을 충족해야 하드웨어 바이패스가 작동합니다.

- 같은 브리지 그룹에 인터페이스 쌍을 배치해야 합니다.
- 스위치의 액세스 포트에 인터페이스를 연결해야 합니다. 트렁크 포트에는 인터페이스를 연결하지 마십시오.

디바이스에 할당된 액세스 제어 정책에 연결된 Threat Defense Service 정책을 사용하여 TCP 시퀀스 번호 임의 설정을 전역적으로 비활성화하는 것이 좋습니다. 기본적으로 ISA 3000을 통과하는 TCP 연결의 ISN(초기 시퀀스 번호)는 임의의 숫자로 재작성됩니다. 하드웨어 바이패스를 활성화하면 ISA 3000은 더 이상 데이터 경로에 없으며 시퀀스 번호를 변환하지 않습니다. 수신 클라이언트는 예상치 않은 시퀀스 번호를 수신하므로 연결을 삭제합니다. 따라서 TCP 세션을 다시 설정해야 합니다. TCP 시퀀스 번호 임의 설정을 비활성화하더라도 전환 중에 일시적으로 중단되는 링크 때문에 일부 TCP 연결은 다시 설정해야 합니다.

프로시저

단계 **1** FlexConfig 개체를 생성하여 자동 우회를 활성화합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

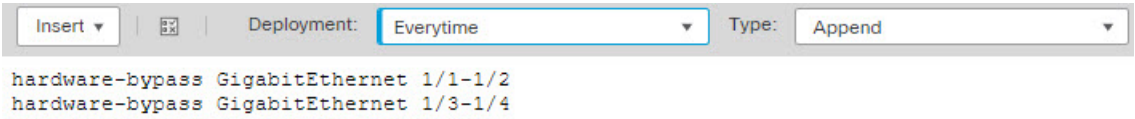
b) 목차에서 **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.

c) **Add FlexConfig Object(FlexConfig** 개체 추가**)**를 클릭하고, 다음 속성을 구성한 다음 **Save(**저장**)**를 클릭합니다.

- **Name(**이름**)** - 개체 이름입니다. 예를 들어, Enable_HW-Bypass를 입력합니다.
- **Deployment(**구축**)** - **Everytime(**항상**)**을 선택합니다. 모든 구축에 구성을 전송해 설정 상태를 유지합니다.
- **Type(**유형**)** - 기본값인 **Append(**추가**)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.
- **Object body(**개체 본문**)** - 개체 본문에서 자동 하드웨어 우회를 활성화하는 데 필요한 명령을 입력합니다. 예를 들어, 가능한 두 인터페이스 쌍에 필요한 명령은 다음과 같습니다.

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

개체 본문은 다음과 비슷해야 합니다.



단계 **2** FlexConfig 정책을 생성하고 디바이스에 할당합니다.

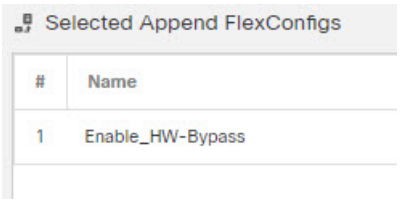
a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.

b) **New Policy(**새 정책**)**를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

c) 목차의 **User Defined(**사용자 정의**)** 폴더에서 하드웨어 우회 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs** 목록에 추가해야 합니다.



d) **Save(**저장**)**를 클릭합니다.

e) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 Save(저장) 아래에 있는 **Policy Assignments(**정책 할당**)** 링크를 클릭하여 할당합니다.

f) **Preview Config(**구성 미리보기**)**를 클릭하고, Preview(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. 하드웨어 우회 FlexConfig 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상

기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 하드웨어 우회 명령의 경우, 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

단계 **3** 변경 사항을 배포합니다.

FlexConfig 정책을 디바이스에 할당했기 때문에 항상 구축 경고가 표시됩니다. FlexConfig는 주의해서 사용해야 한다는 뜻입니다. **Proceed(**계속하기**)**를 클릭하여 구축을 계속 진행합니다.

구축이 끝나면 구축 내역과 구축 기록을 확인할 수 있습니다. 이 기능은 구축이 실패했을 때 특히 유용합니다. 구축된 설정 확인, 1302 페이지의 내용을 참조하십시오.

다음에 수행할 작업

수동으로 하드웨어 우회를 호출하거나 직접 해제하려면 FlexConfig 개체를 두 개 생성해야 합니다.

- 하나는 수동으로 우회를 시작하는 명령인데, 두 쌍에 대해 우회를 호출할지에 따라 다음 명령 중 하나 또는 둘 다를 포함합니다.

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

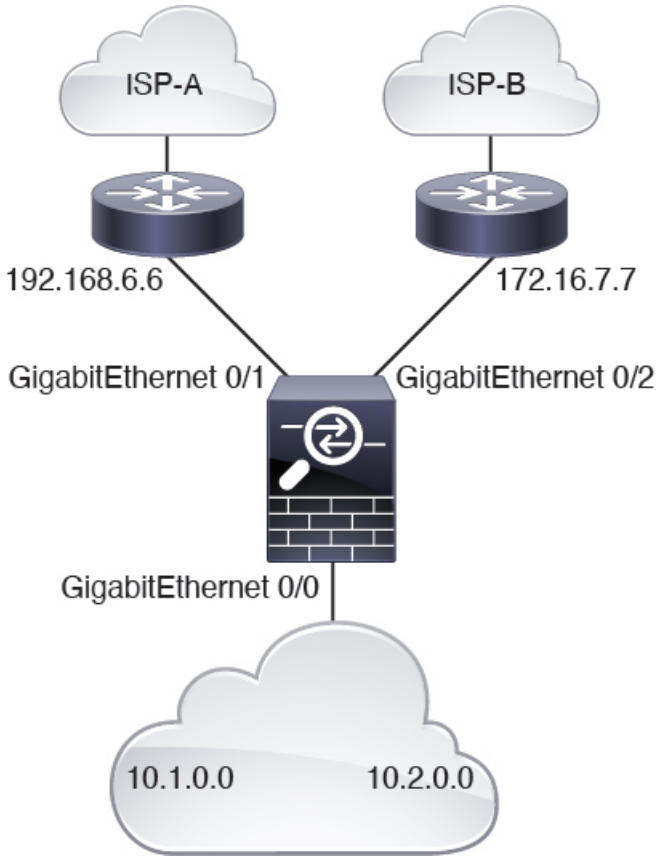
- 다른 하나는 다음 명령 중 하나 또는 둘 모두를 포함해서 우회 기능을 수동으로 해제하는 명령입니다.

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

그러고 나서 우회를 켜거나 끄려면 FlexConfig 정책에 둘 중 하나의 개체를 추가하고 변경 사항을 구축해야 합니다. 또한 구축 후 FlexConfig 정책에서 개체를 즉시 제거해야 합니다. 수동으로 우회를 호출하는 경우, 프로세스를 반복하여 우회를 다시 해제해야 합니다. 따라서 이 수동 방법을 사용하려면 FlexConfig 정책 및 추가 구축을 자주 신중하게 편집해야 합니다.

정책 기반 라우팅 구성 방법

FlexConfig를 사용하여 PBR(정책 기반 라우팅) 기능을 구현할 수 있습니다. 예를 들어 다음 그림은 소스 IP 주소를 기반으로 네트워크 간의 트래픽 로드밸런싱을 보여줍니다. 이 경우 10.1.0.0/16 네트워크가 높은 우선 순위 트래픽을 생성하고, 이 트래픽은 ISP-A에 대한 더 높은 대역폭 링크를 통과해야 하며 10.2.0.0/16은 더 낮은 우선 순위를 가져야 하며 -ISP-B에 대한 더 낮은 대역폭 링크을 통과해야 한다고 가정합니다.



시작하기 전에

이 절차에서는 다음과 같이 인터페이스를 이미 구성했다고 가정합니다.

- GigabitEthernet0/0.
  - 인터페이스 이름: inside
  - IP 주소: 10.1.1.1/24
  - 네트워크의 다른 라우터는 이 인터페이스를 10.1.0.0/16 및 10.2.0.0/16 주소 공간의 경로에 대한 게이트웨이로 사용합니다.
- GigabitEthernet0/1.
  - 인터페이스 이름: outside-1
  - IP 주소: 192.168.6.5/24
- GigabitEthernet0/2.
  - 인터페이스 이름: outside-2
  - IP 주소: 172.16.7.6/24

프로시저

단계 **1** 10.1.0.0/16 및 10.2.0.0/16 주소 공간의 트래픽과 일치하도록 확장 ACL 개체를 생성합니다. 경로 맵의 트래픽에 다른 작업을 적용하므로 별도의 ACL을 생성해야 합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다. 트래픽 소스 주소를 지정하려면 확장 액세스 목록을 구성해야 합니다.

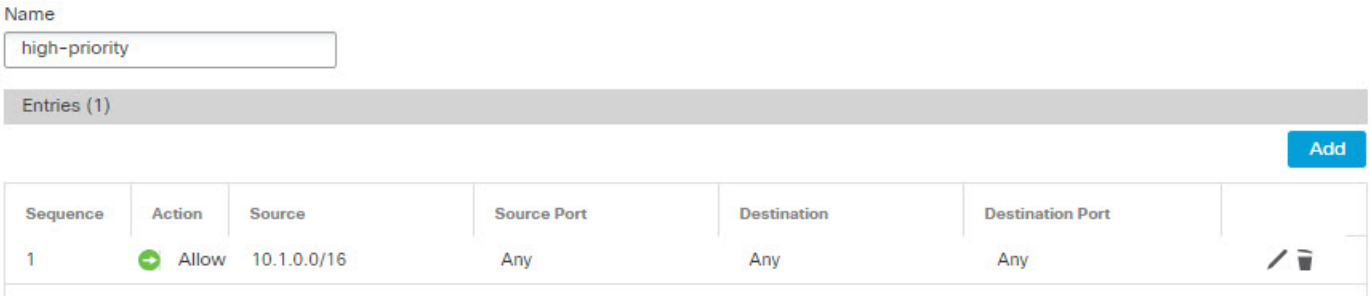
c) **Add Extended Access List(**확장된 액세스 목록 추가**)** 버튼을 클릭합니다.

d) 액세스 목록의 이름(예 : 높은 우선 순위)을 입력합니다.

e) **Add(**추가**)** 버튼을 클릭하고 우선 순위가 높은 주소 공간에 대한 규칙을 생성합니다. 주요 특징:

- **Action(**작업**) - Allow(**허용**)**.
- **Source Networks(**소스 네트워크**)**-목록 아래의 수정 상자에 10.1.0.0/16을 입력하고 **Add(**추가**)**를 클릭합니다. 또는 이 네트워크 주소에 대한 네트워크 개체를 정의할 수 있습니다.

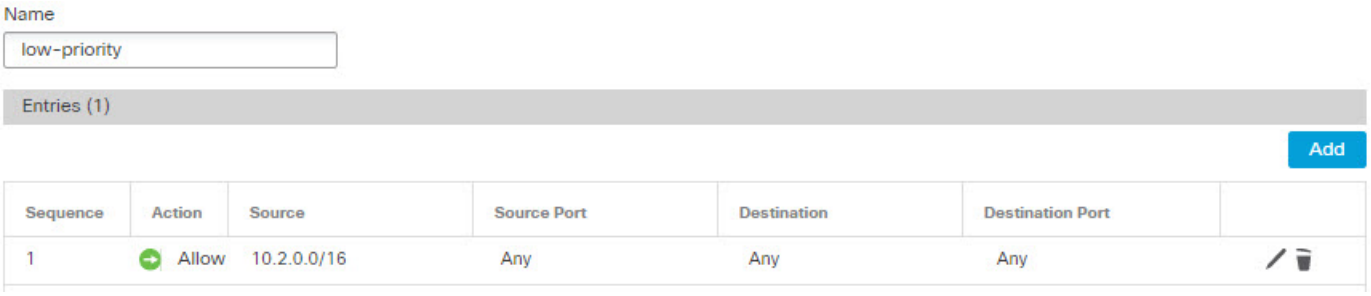
f) 대화 상자의 하단에 있는 **Add(**추가**)**를 클릭합니다. 그러면 액세스 목록에 규칙이 추가됩니다.



g) **Save(**저장**)**를 클릭합니다.

h) 이 프로세스를 반복하여 다음 속성의 두 번째 액세스 목록을 생성합니다.

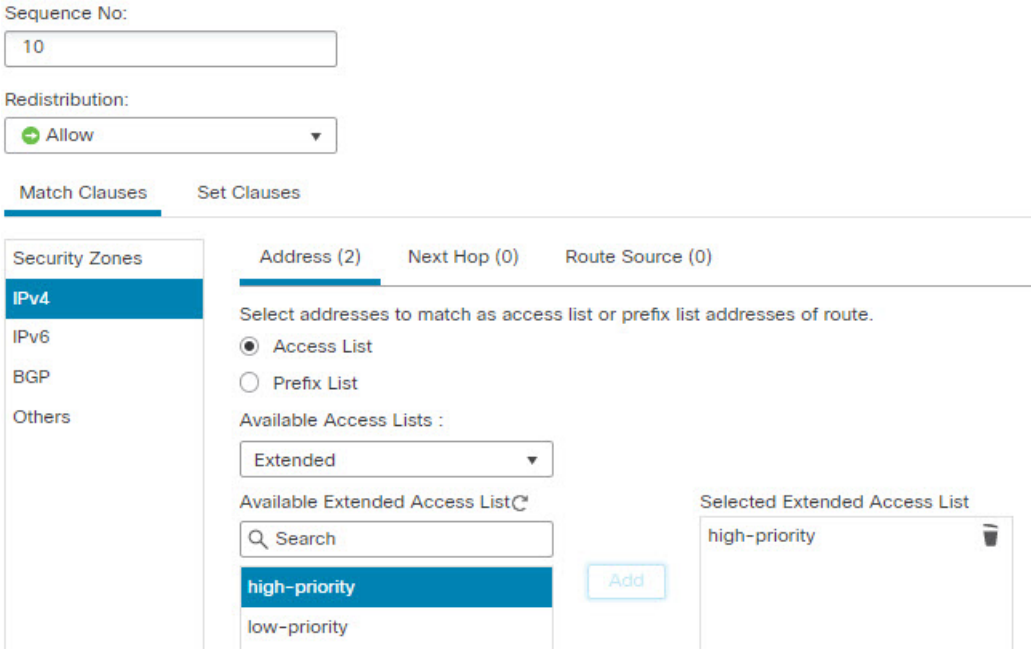
- 이름-낮은 우선 순위
- **Action(**작업**) - Allow(**허용**)**.
- **Source Networks(**소스 네트워크**)**-목록 아래의 수정 상자에 10.2.0.0/16을 입력하고 **Add(**추가**)**를 클릭합니다. 또는 이 네트워크 주소에 대한 네트워크 개체를 정의할 수 있습니다.



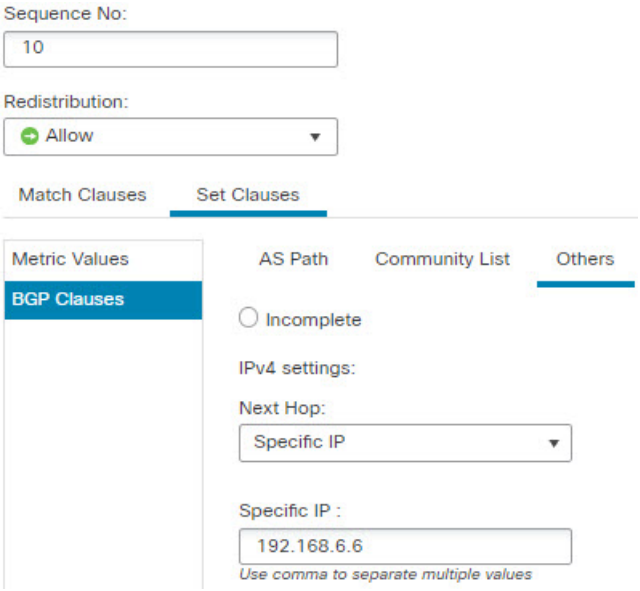
단계 **2** 이러한 주소 공간에 대한 다음 홉 주소를 정의하는 경로 맵을 만듭니다.

a) 개체 페이지에 있는 동안 목차에서 **Route Map(**경로 맵**)**을 클릭합니다.
b) **Add Route Map(**경로 맵 추가**)** 버튼을 클릭합니다.
c) 개체의 이름(예: **load-balance**)을 입력합니다.
d) **Add(**추가**)**를 클릭하고 다음 특성의 우선 순위가 높은 트래픽에 대한 규칙을 생성합니다.

- 시퀀스 번호—**10**.
- 재배포—허용.
- **Match Clauses(**일치 절**)** > **IPv4** > **Address(**주소**)-Access List(**액세스 목록**)** 라디오 버튼을 선택한 다음**Available Access Lists(**사용 가능한 액세스 목록**)** > **Extended(**확장**)**를 선택하고 우선 순위가 높은 ACL을 선택한 목록으로 이동합니다.



- **Set Clauses(**절 설정**)** > **BGP Clauses Others(BGP** 절**)** > **Others(**기타**)-IPv4 Settings(IPv4** 설정**)** > **Next Hop(**다음 홉**)**에서 **Specific IP(**특정 **IP)**를 선택한 다음 ISP-A용 게이트웨이, **192.168.6.6**을 **Specific IP(**특정 **IP)** 수정 상자에 입력합니다.



e) 경로 맵에 규칙을 추가하려면 **Add(**추가**)**를 클릭합니다.

f) **Add(**추가**)**를 클릭하고 다음 속성을 가진 낮은 우선 순위 트래픽에 대한 규칙을 생성합니다.

- 시퀀스 번호—**20**.
- 재배포—허용.
- **Match Clauses(**일치 절**)** > **IPv4** > **Address(**주소**)-Access List(**액세스 목록**)** 라디오 버튼을 선택한 다음**Available Access Lists(**사용 가능한 액세스 목록**)** > **Extended(**확장**)**를 선택하고 우선 순위가 낮은 ACL을 선택한 목록으로 이동합니다.
- **Set Clauses(**절 설정**)** > **BGP Clauses Others(BGP** 절**)** > **Others(**기타**)-IPv4 Settings(IPv4** 설정**)** > **Next Hop(**다음 홉**)**에서 **Specific IP(**특정 **IP)**를 선택한 다음 ISP-B용 게이트웨이, **172.16.7.7**을 **Specific IP(**특정 **IP)** 수정 상자에 입력합니다.

g) 경로 맵에 규칙을 추가하려면 **Add(**추가**)**를 클릭합니다.

h) **Save(**저장**)**를 클릭합니다.

단계 **3** 경로 맵을 사용하여 내부 인터페이스에서 PBR을 활성화하는 FlexConfig 개체를 생성합니다.

a) 개체 페이지에 있는 동안 목차에서 **FlexConfig** > **FlexConfig** 개체를 클릭합니다.

b) Policy_Based_Routing 개체를 찾은 다음 복사 ( )를 클릭합니다.

이 개체는 시스템 정의 개체이지만 편집하기 전까지는 사용할 수 없습니다. 경로 맵의 이름으로 간단하게 업데이트할 수 있는 텍스트 개체를 가리키지는 않습니다. 이 시스템 정의 개체에 대해 항상 사용자 지정 개체를 생성해야 합니다.

c) 복사 아이콘을 클릭하면 기본 이름이 Policy_Based_Routing_Copy인 새 개체가 포함된 대화 상자가 열립니다. 다음과 같이 기본 변경을 수행합니다.

- **Name(**이름**)**-의미 있는 이름을 입력합니다. 예를 들어 디바이스 FTD1에 대해 PBR을 구성하는 경우 **PBR_FTD1**일 수 있습니다.
- **Description(**설명**)**-설명을 삭제하거나 용도에 맞게 의미를 부여합니다.
- **Deployment(**구축**)** -한 번을 유지합니다.
- **Type(**유형**)** = **Append(**뒤에 추가**)**를 유지합니다.

d) 개체의 본문에는 다음 줄이 있습니다.

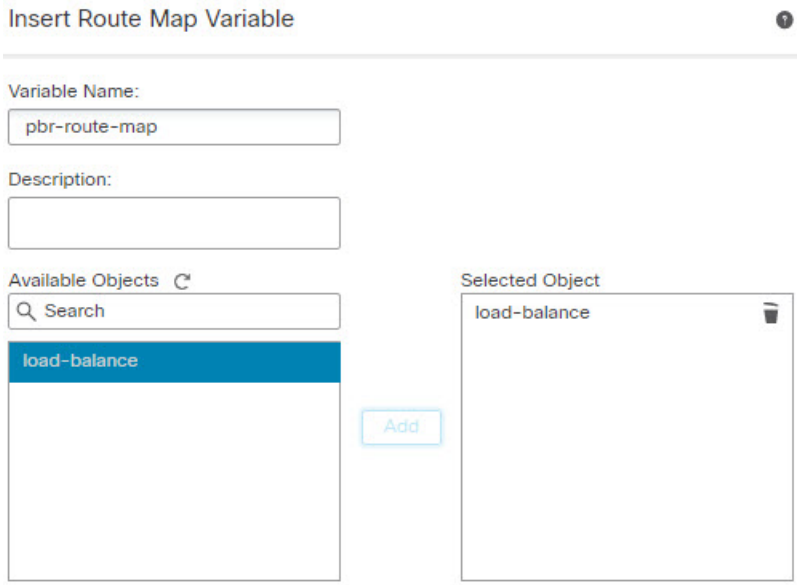
```
interface GigabitEthernet0/0
    policy-route route-map $r-map-object
```

"interface GigabitEthernet0/0" 행은 이 예에서 올바른 인터페이스를 구성하도록 이미 설정되어 있습니다. 다른 인터페이스에 PBR을 적용하려면 인터페이스 하드웨어 이름을 수정해야 합니다.

$r-map-object 문자열은 사실 실제 변수가 아니며 아무 것도 가리키지 않습니다. 이 문자열을 교체해야 합니다.

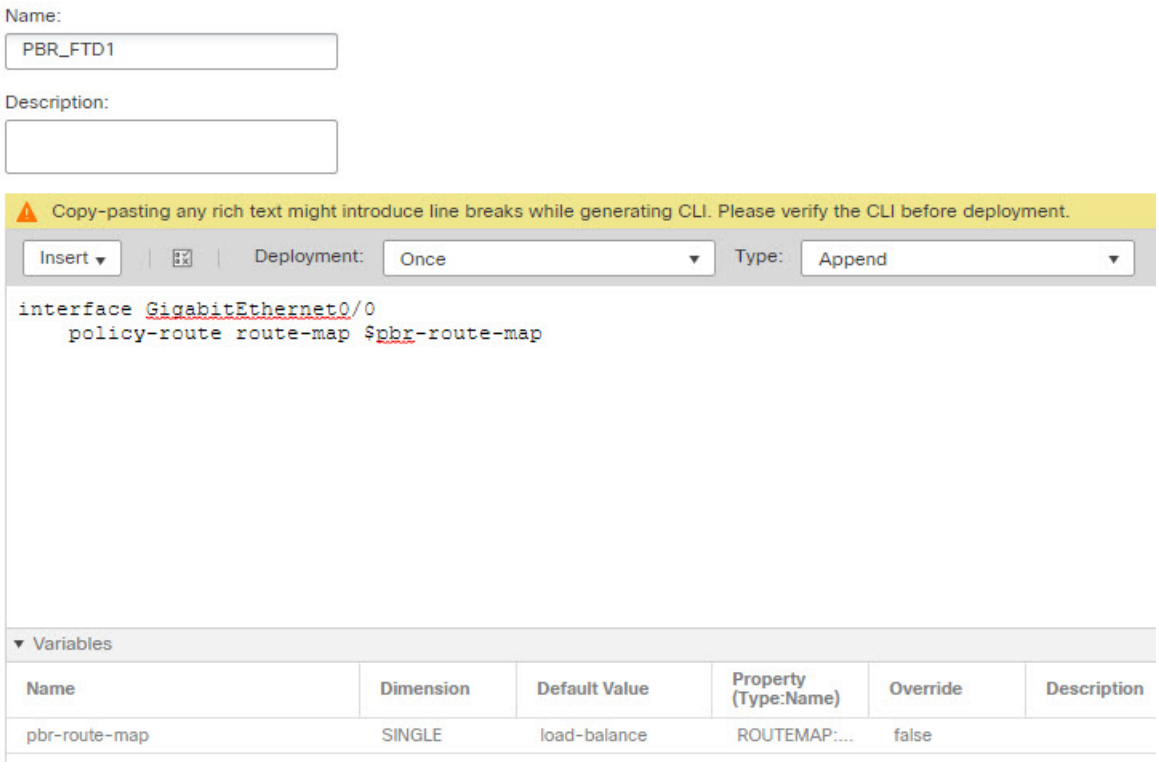
e) $r-map-object 문자열을 삭제하고 “policy-route route-map” 줄(경로 맵 뒤 공백)에 커서를 둡니다.
f) **Insert(**삽입**)** > **Insert Policy Object(**정책 개체 삽입**)** > **Route Map(**경로 맵**)**을 선택합니다.
g) Route Map Variable(경로 맵 변수) 대화 상자에서 다음을 구성합니다.

- **Variable Name(**변수 이름**)-pbr-route-map**과 같은 이름입니다.
- **Selected Object(**선택한 개체**)**-로드 밸런싱 경로 맵 개체를 사용 가능한 목록에서 선택한 목록으로 이동합니다.



h) Variable(변수) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

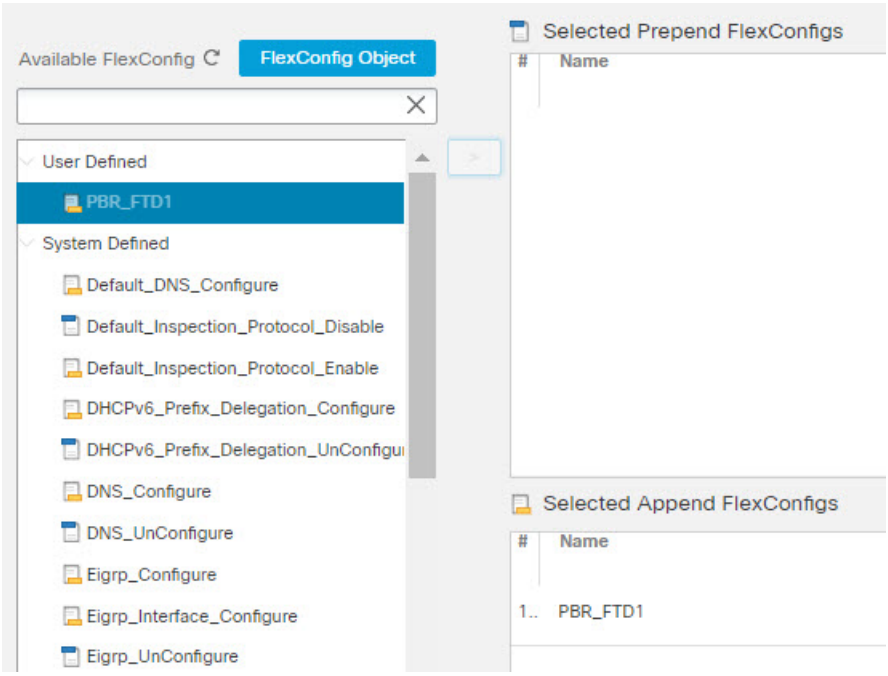
이제 FlexConfig 개체가 다음과 같이 표시됩니다. 여기서 변수는 대화 상자의 하단에 있는 변수 목록에 있습니다.



i) **Save(**저장**)**를 클릭합니다.

단계 **4** 디바이스에 할당된 FlexConfig 정책에 FlexConfig 개체를 추가합니다.

a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.
b) 이 디바이스에 아직 FlexConfig 정책이 할당되지 않았다고 가정하고 **New Policy(**새 정책**)**를 클릭하고 정책에 이름을 지정한 다음 정책에 할당할 FTD1 디바이스를 선택하고 **Save(**저장**)**를 클릭합니다.
c) 사용 가능한 개체 목록의 User Defined(사용자 정의) 폴더 아래에서 개체를 찾은 다음, >을 클릭하여 선택한 개체 목록에 추가합니다.



d) **Save**를 클릭하여 정책을 저장합니다.
e) **Preview Config(**구성 미리보기**)**를 클릭하고, Preview(미리보기) 대화 상자에서 FTD1 디바이스를 선택합니다.

미리보기에는 FlexConfig 개체와 구성 명령을 사용하여 구현된 FMC 관리 구성 부분에서 생성된 CLI가 포함되어 있습니다. 이들은 섹션으로 구분됩니다. 이 예에서 수행한 작업을 기반으로 구성할 명령은 다음과 같습니다. 이 미리보기를 사용하여 예상한 결과를 얻고 있는지 확인할 수 있습니다.

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###
configure session OBJECT
object-group service ProxySG_ExtendedACL_4294969626
 service-object ip
object-group service ProxySG_ExtendedACL_4294969648
 service-object ip
commit noconfirm revert-save
configure session FMC_SESSION_1
access-list high-priority extended permit object-group
      ProxySG_ExtendedACL_4294969626 10.1.0.0 255.255.0.0 any
access-list low-priority extended permit object-group
      ProxySG_ExtendedACL_4294969648 10.2.0.0 255.255.0.0 any
commit noconfirm revert-save
```

```
route-map load-balance permit 10
 match ip address high-priority
 set ip next-hop 192.168.6.6
route-map load-balance permit 20
 match ip address low-priority
 set ip next-hop 172.16.7.7


###Flex-config Appended CLI ###
interface GigabitEthernet0/0
    policy-route route-map load-balance
```

f) **Close(**닫기**)**를 클릭하여 미리보기 대화 상자를 종료합니다.

다음에 수행할 작업

이제 디바이스에 구성을 구축할 수 있습니다.

FlexConfig를 위한 기록

기능	버전	설명
FlexConfig.	6.2	FlexConfig 기능을 이용하면 Firepower Management Center을(를) 사용하여 ASA CLI 템플릿 기반 기능을 Firepower Threat Defense 디바이스에 구축할 수 있습니다. 이 기능을 이용하면 현재 Firepower Threat Defense 디바이스에서 지원되지 않는 가장 중요한 ASA 기능 일부를 활성화할 수 있습니다. 이 기능은 정책에서 함께 작동하는 템플릿 및 개체로 구성됩니다. 기본 템플릿은 Cisco TAC에서 공식적으로 지원됩니다. 새 화면: **Devices(**디바이스**)** > **FlexConfig**. 또한 **Objects(**개체**)** > **Object Management(**개체 관리**)**에서는 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)** 및 **FlexConfig** > **Text Object(**텍스트 개체**)**입니다. 지원되는 플랫폼: Firepower Threat Defense

기능	버전	설명
FlexConfig 업데이트	6.2 (1) 6.2 (2)	정부 인증 요구 사항에 따라 시스템 제공 또는 사용자 정의 FlexConfig 개체에 있는 모든 중요 정보(비밀번호, 공유 키 등)는 비밀 키 변수를 사용하여 마스킹해야 합니다. Firepower Management Center을(를) 이러한 릴리스로 업데이트하면, FlexConfig 개체의 모든 중요 정보가 비밀 키 변수 형식으로 변환됩니다. 또한 다음과 같은 새 FlexConfig 템플릿이 추가됩니다. • **Default_DNS_Configure** 템플릿을 이용하면 기본 DNS 그룹을 사용할 수 있습니다. 이 그룹은 데이터 인터페이스를 통해 이름을 확인하는 명령 또는 기능에 대한 호스트 이름을 확인하는 데 사용합니다. • **TCP** 초기 연결 제한 및 시간 초과 컨피그레이션 템플릿을 사용하면 SYN Flood DoSAttack을 차단하기 위한 초기 연결 제한/시간 초과 CLI를 구성할 수 있습니다. • 위협 탐지 구성 및 해제 활성화 템플릿을 사용하면 TCP 인터셉트가 적용되는 공격의 위협 탐지 통계를 구성할 수 있습니다. • **IPV6** 라우터 헤더 검사 템플릿을 사용하면 다양한 유형의 특정 헤더를 선택적으로 허용/차단하도록 IPV6 검사 헤더를 구성할 수 있습니다(예: RH Type 2,mobile 허용). • **DHCPv6** 접두사 위임 템플릿을 사용하면 IPv6 접두사 위임을 위해 외부 인터페이스(PD 클라이언트) 및 내부 인터페이스(위임된 접두사의 수신자)를 하나씩 구성할 수 있습니다. 지원되는 플랫폼: Firepower Threat Defense

기능	버전	설명
지원 중단된 FlexConfig 개체입니다.	6.3	FlexConfig를 이용해 구성한 이전 릴리스의 여러 기능을 이제 Firepower Management Center에서 바로 사용할 수 있습니다. 이러한 FlexConfig 개체를 사용하고 있다면 해당 개체를 제거하고, 새 개체를 사용할 수 있도록 구성을 변경해야 합니다. 다음은 지원 중단된 FlexConfig 개체 및 텍스트 개체입니다. • **Default_DNS_Configure**(defaultDNSNameServerList 및 defaultDNSParameters 텍스트 개체 포함). 이제 플랫폼 설정 정책을 사용하여 데이터 인터페이스에 대한 DNS를 구성하십시오. • **TCP_Embryonic_Conn_Limit** 및 tcp_conn_misc and tcp_conn_limit 텍스트 개체. 디바이스에 할당된 액세스 제어 정책의 Advanced(고급) 탭에 있는 Firepower Threat Defense 서비스 정책에서 이러한 기능을 구성합니다. • **TCP_Embryonic_Conn_Timeout** 및 the tcp_conn_misc and tcp_conn_timeout 텍스트 개체. Firepower Threat Defense 서비스 정책에서 이러한 기능을 구성합니다. 지원되는 플랫폼: Firepower Threat Defense
ISA 3000 디바이스에 대한 PTP(Precision Time Protocol) 구성	6.5	FlexConfig를 사용하여 ISA 3000 디바이스에서 PTP(Precision Time Protocol)를 구성할 수 있습니다. PTP는 패킷 기반 네트워크에서 다양한 디바이스의 클록을 동기화하기 위해 개발된 시간 동기화 프로토콜입니다. 이 프로토콜은 산업용, 네트워크 측정 및 제어 시스템용으로 특별히 설계되었습니다. 이제 **ptp**(인터페이스 모드) 명령과 글로벌 명령 **ptp mode e2etransparent** 및 **ptp domain**을(를) FlexConfig 개체에 포함할 수 있습니다. 신규/수정된 명령: **show ptp** 지원되는 플랫폼: Firepower Threat Defense

50 장

Cisco ISA 3000에 대한 알람

원치 않는 상황이 발생하면 알림을 받을 수 있도록 Cisco ISA 3000 디바이스의 알람 시스템을 구성할 수 있습니다.

- 알람 정보, 1323 페이지
- 알람 기본값, 1325 페이지
- 알람 요구 사항 및 사전 요건, 1326 페이지
- ISA 3000에 대한 알람 구성, 1326 페이지
- 알람 모니터링, 1335 페이지
- 알람에 대한 기록, 1336 페이지

알람 정보

여러 조건에 대해 알람을 생성하도록 ISA 3000을 구성할 수 있습니다. 조건이 구성된 설정과 일치하지 않으면 시스템은 알람을 트리거합니다. 이러한 알람은 LED, syslog 메시지, SNMP 트랩 및 알람 출력 인터페이스에 연결된 외부 디바이스를 통해 보고됩니다. 기본적으로 알람이 트리거되면 syslog 메시지만 발급됩니다.

다음을 모니터링하도록 알람 시스템을 구성할 수 있습니다.

- 전원 공급 장치
- 기본 및 보조 온도 센서
- 알람 입력 인터페이스

ISA 3000에는 내부 센서와 알람 입력 인터페이스 2개, 알람 출력 인터페이스 1개가 있습니다. 도어 센서와 같은 외부 센서를 알람 입력에 연결할 수 있습니다. 버저나 표시등과 같은 외부 알람 디바이스를 알람 출력 인터페이스에 연결할 수 있습니다.

알람 출력 인터페이스는 릴레이 메커니즘입니다. 알람 조건에 따라 릴레이가 활성화되거나 비활성화됩니다. 릴레이가 활성화되면 인터페이스에 연결된 디바이스가 활성화됩니다. 릴레이가 비활성화되면 연결된 디바이스가 비활성 상태가 됩니다. 알람이 트리거되는 동안에는 릴레이가 활성화된 상태로 유지됩니다.

외부 센서와 알람 릴레이 연결에 대한 자세한 정보는 Cisco ISA 3000 Industrial Security Appliance 하드웨어 설치 가이드를 참조하십시오.

알람 입력 인터페이스

도어가 열린 상태를 탐지하는 센서 등의 외부 센서에 알람 입력 인터페이스나 접촉부를 연결할 수 있습니다.

각 알람 입력 인터페이스에는 해당하는 LED가 있습니다. 이러한 LED는 각 알람 입력의 알람 상태를 전달합니다. 각 알람 입력에 대해 트리거와 심각도를 구성할 수 있습니다. LED 외에도 출력 릴레이를 트리거하여 외부 알람을 활성화하고 syslog 메시지와 SNMP 트랩을 전송하는 접촉부를 구성할 수도 있습니다.

다음 표에서는 알람 입력에 대한 알람 조건에 대응하는 LED의 상태를 설명합니다. 또한 출력 릴레이, syslog 메시지 및 SNMP 트랩(알람 입력에 대해 이러한 응답을 활성화하는 경우)의 동작도 설명합니다.

알람 상태	**LED**	출력 릴레이	**Syslog**	**SNMP** 트랩
알람이 구성되지 않음	Off	—	—	—
알람이 트리거되지 않음	녹색	—	—	—
알람 활성화됨	경미한 알람 - 빨간색으로 켜짐 중요한 알람 - 빨간색으로 깜박임	릴레이 활성화됨	Syslog 생성됨	SNMP 트랩 전송됨
알람 종료됨	녹색	릴레이 비활성화됨	Syslog 생성됨	—

알람 출력 인터페이스

버저나 표시등과 같은 외부 알람을 알람 출력 인터페이스에 연결할 수 있습니다.

알람 출력 인터페이스는 릴레이로 작동하며 해당하는 LED도 가지고 있습니다. 이러한 LED는 입력 인터페이스에 연결된 외부 센서와 듀얼 전원 공급 장치 및 온도 센서 등의 내부 센서의 알람 상태를 전달합니다. 출력 릴레이(있는 경우)를 활성화하는 알람을 구성합니다.

다음 표에서는 알람 조건에 대응하는 LED 및 출력 릴레이의 상태를 설명합니다. 또한 syslog 메시지 및 SNMP 트랩(알람에 대해 이러한 응답을 활성화하는 경우)의 동작도 설명합니다.

알람 상태	**LED**	출력 릴레이	**Syslog**	**SNMP** 트랩
알람이 구성되지 않음	Off	—	—	—

알람 상태	LED	출력 릴레이	Syslog	SNMP 트랩
알람이 트리거되지 않음	녹색	—	—	—
알람 활성화됨	빨간색으로 켜짐	릴레이 활성화됨	Syslog 생성됨	SNMP 트랩 전송됨
알람 종료됨	녹색	릴레이 비활성화됨	Syslog 생성됨	—

Syslog 알람

기본적으로 시스템은 특정 알람이 트리거될 때 syslog 메시지를 전송합니다. 메시지가 전송되지 않도록 하려는 경우 syslog 메시지를 비활성화할 수 있습니다.

시스템 로그 알람을 작동하게 하려면 진단 로깅도 활성화해야 합니다. **Device(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 디바이스에 할당된 FTD 플랫폼 설정 정책을 추가 또는 수정하고 **Syslog** 페이지에서 대상과 설정을 구성합니다. 예를 들어, 시스템 로그 서버, 콘솔 로깅 또는 내부 버퍼 로깅을 구성할 수 있습니다.

진단 로깅의 대상을 활성화하지 않으면 알람 시스템은 어떤 위치로도 syslog 메시지를 전송하지 않습니다.

SNMP 알람

SNMP 트랩을 SNMP 서버로 전송할 때의 알람을 선택적으로 구성할 수 있습니다. SNMP 트랩 알람을 작동하게 하려면 SNMP 설정도 구성해야 합니다.

Device(디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 디바이스에 할당된 FTD 플랫폼 설정 정책을 추가 또는 수정하고 **SNMP** 페이지에서 SNMP를 활성화하고 설정을 구성합니다.

알람 기본값

다음 표에는 알람 입력 인터페이스(접촉부), 예비 전원 공급 장치 및 온도의 기본값이 지정되어 있습니다.

	경보	트리거	심각도	SNMP 트랩	출력 릴레이	Syslog 메시지
알람 접촉부 1	활성화	닫힌 상태	경미	비활성화됨	비활성화	활성화
알람 접촉부 2	활성화	닫힌 상태	경미	비활성화됨	비활성화	활성화
예비 전원 공급 장치(활성화된 경우)	활성화	—	—	비활성화됨	비활성화	활성화

	경보	트리거	심각도	**SNMP** 트랩	출력 릴레이	**Syslog** 메시지
온도	기본 온도 알람에 대해 활성화됨(최고 임계값과 최저 임계값의 기본값은 각각 92°C 및 -40°C) 보조 알람에 대해 비활성화됨.	—	—	기본 온도 알람에 대해 활성화됨	기본 온도 알람에 대해 활성화됨	기본 온도 알람에 대해 활성화됨

알람 요구 사항 및 사전 요건

모델 지원

FTD ISA 3000

지원되는 도메인

모든

사용자 역할

관리자

ISA 3000에 대한 알람 구성

FlexConfig를 사용하여 ISA 3000에 대한 알람을 구성합니다. 다음 주제에서는 다양한 유형의 알람을 구성하는 방법을 설명합니다.

알람 입력 접촉부 구성

알람 입력 접촉부(인터페이스)를 외부 센서에 연결하는 경우에는 센서의 입력을 기준으로 하여 알람을 생성하도록 접촉부를 구성할 수 있습니다. 실제로 접촉부는 닫히는 경우(즉, 접촉부를 통한 전류 흐름이 중지되는 경우) 기본적으로 syslog 메시지를 전송하도록 설정됩니다. 기본값이 요구 사항을 충족하지 않는 경우에만 접촉부를 구성해야 합니다.

알람 접촉부의 번호는 1번과 2번으로 지정되므로 정확한 설정을 구성하려면 물리적 핀을 유선 연결한 방법을 파악해야 합니다. 접촉부는 개별적으로 구성합니다.

프로시저

단계 **1** FlexConfig 개체를 생성하여 알람 입력 연락처를 구성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.

c) **Add FlexConfig Object(FlexConfig** 개체 추가**)**를 클릭하고, 다음 속성을 구성한 다음 **Save(**저장**)**를 클릭합니다.

- **Name(**이름**)** - 개체 이름입니다. 예를 들어 Configure_Alarm_Contacts를 입력합니다.
- **Deployment(**구축**)** - **Everytime(**항상**)**을 선택합니다. 모든 구축에 구성을 전송해 설정 상태를 유지합니다.
- **Type(**유형**)** - 기본값인 **Append(**추가**)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.
- **Object body(**개체 본문**)** - 개체 본문에서 알람 연락처를 구성하는 데 필요한 명령을 입력합니다. 다음 단계에서는 명령에 대해 설명합니다.

d) 알람 접촉부의 설명을 구성합니다.

alarm contact {**1** | **2**} **description** *string(*문자열*)*

예를 들어 접촉부 1의 설명을 "Door Open(도어 열림)"으로 설정하려면 다음을 입력합니다.

```
alarm contact 1 description Door Open
```

e) 알람 접촉부의 심각도를 구성합니다.

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

하나의 접촉부를 컨피그레이션하는 대신 **any**를 지정하여 모든 접촉부의 심각도를 변경할 수 있습니다. 심각도는 접촉부와 연결된 LED의 동작을 제어합니다.

- **major**- LED가 빨간색으로 깜박입니다.
- **minor**- LED가 빨간색으로 켜져 있습니다. 이는 기본값입니다.
- **none**- LED가 꺼져 있습니다.

예를 들어 접촉부 1의 심각도를 Major(중대)로 설정하려면 다음을 입력합니다.

```
alarm contact 1 severity major
```

f) 알람 접촉부의 트리거를 구성합니다.

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

하나의 접촉부를 컨피그레이션하는 대신 **any**를 지정하여 모든 접촉부의 트리거를 변경할 수 있습니다. 트리거는 알림 신호를 보내는 전기적 상태를 결정합니다.

- **open**- 접촉부의 기본 상태가 닫힌 상태(즉, 전류가 접촉부를 통과하고 있음)입니다. 접촉부가 열리면(즉, 전류 흐름이 중지됨) 알림이 트리거됩니다.

- **closed**- 접촉부의 기본 상태가 열린 상태(전류가 접촉부를 통과하지 않음)입니다. 접촉부가 닫히면(즉, 전류가 접촉부를 통과하기 시작함) 알림이 트리거됩니다. 이는 기본값입니다.

도어 센서를 알람 입력 접촉부 1에 연결하고 해당 접촉부의 기본 상태가 알람 접촉부를 통한 전류 흐름이 없는 상태(접촉부가 열린 상태)인 경우를 예로 들어 보겠습니다. 도어가 열리면 접촉부는 닫히며 알람 접촉부를 통해 전류가 흐릅니다. 이 경우에는 전류 흐름이 시작되면 알람이 꺼지도록 알람 트리거를 닫힘으로 설정합니다.

```
alarm contact 1 trigger closed
```

g) 알람 접촉부가 트리거될 때 수행할 작업을 구성합니다.

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

여러 작업을 구성할 수 있습니다. 예를 들어 외부 알람을 활성화하고, syslog 메시지를 보내고, SNMP 트랩도 전송하도록 디바이스를 구성할 수 있습니다.

- **relay(**릴레이**)** - 알람 출력 릴레이를 활성화합니다. 그러면 버저, 플래쉬 등 접촉부에 부착한 외부 알람이 활성화됩니다. 또한 출력 LED가 빨간색으로 바뀝니다.
- **syslog** - syslog 메시지를 보냅니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- **notifies(**알림**)** - SNMP 트랩을 보냅니다.

예를 들어 알람 입력 접촉부 1에 대해 모든 작업을 활성화하려면 다음을 입력합니다.

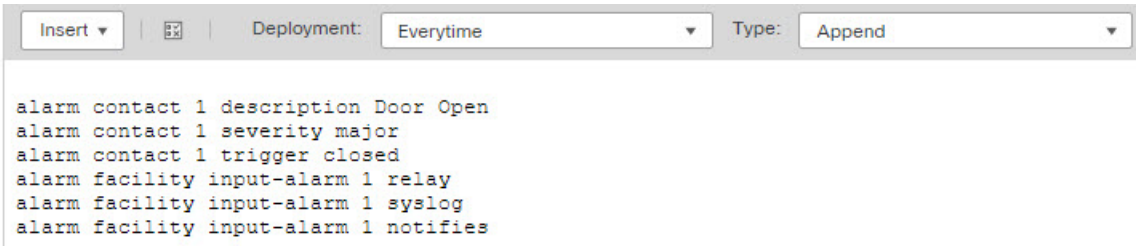
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

h) 개체 본문에 원하는 명령이 포함되어 있는지 확인합니다.

예를 들어 이 템플릿에 이 절차에 나와 있는 모든 명령 예시가 포함되어 있는 경우 개체 본문은 다음과 같은 명령을 포함하게 됩니다.

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

개체 본문은 다음과 비슷해야 합니다.



i) **Save(**저장**)**를 클릭합니다.

단계 **2** FlexConfig 정책을 생성하고 디바이스에 할당합니다.

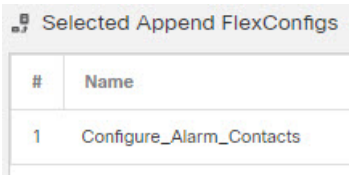
a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.

b) **New Policy(**새 정책**)**를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

c) 목차의 **User Defined(**사용자 정의**)** 폴더에서 알람 연락처 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs** 목록에 추가해야 합니다.



d) **Save(**저장**)**를 클릭합니다.

e) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 Save(저장) 아래에 있는 **Policy Assignments(**정책 할당**)** 링크를 클릭하여 할당합니다.

f) **Preview Config(**구성 미리보기**)**를 클릭하고, Preview(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. FlexConfig 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 알람 연락처 명령의 경우 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

단계 **3** 변경 사항을 배포합니다.

FlexConfig 정책을 디바이스에 할당했기 때문에 항상 구축 경고가 표시됩니다. FlexConfig는 주의해서 사용해야 한다는 뜻입니다. **Proceed(**계속하기**)**를 클릭하여 구축을 계속 진행합니다.

구축이 끝나면 구축 내역과 구축 기록을 확인할 수 있습니다. 이 기능은 구축이 실패했을 때 특히 유용합니다. 구축된 설정 확인, 1302 페이지의 내용을 참조하십시오.

전원 공급 장치 알람 구성

ISA 3000에는 전원 공급 장치 두 개가 있습니다. 기본적으로 시스템은 단일 전원 모드에서 작동합니다. 그러나 듀얼 모드로 작동하도록 시스템을 구성할 수 있습니다. 그러면 기본 전원 공급 장치에서

장애가 발생하는 경우 두 번째 전원 공급 장치가 자동으로 전원을 공급합니다. 듀얼 모드를 활성화하면 syslog 알림을 전송하도록 전원 공급 장치 알람이 자동으로 활성화됩니다. 하지만 알림을 완전히 비활성화할 수도 있고 SNMP 트랩 또는 알람 하드웨어 릴레이를 활성화할 수도 있습니다.

다음 절차에서는 듀얼 모드를 활성화하고 전원 공급 장치 알람을 구성하는 방법을 설명합니다.

프로시저

단계 **1** FlexConfig 개체를 생성하여 전원 공급 장치 알람을 구성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.

c) **Add FlexConfig Object(FlexConfig** 개체 추가**)**를 클릭하고, 다음 속성을 구성한 다음 **Save(**저장**)**를 클릭합니다.

- **Name(**이름**)** - 개체 이름입니다. 예를 들어 Power_Supply_Alarms.
- **Deployment(**구축**)** - **Everytime(**항상**)**을 선택합니다. 모든 구축에 구성을 전송해 설정 상태를 유지합니다.
- **Type(**유형**)** - 기본값인 **Append(**추가**)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.
- **Object body(**개체 본문**)**-개체 본문에서 전원 공급 장치 알람을 구성하는 데 필요한 명령을 입력합니다. 다음 단계에서는 명령에 대해 설명합니다.

d) 듀얼 전원 공급 장치 모드를 활성화합니다.

power-supply dual

예를 들면 다음과 같습니다.

```
power-supply dual
```

e) 전원 공급 장치 알람이 트리거될 때 수행할 작업을 구성합니다.

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

여러 작업을 구성할 수 있습니다. 예를 들어 외부 알람을 활성화하고, syslog 메시지를 보내고, SNMP 트랩도 전송하도록 디바이스를 구성할 수 있습니다.

- **relay(**릴레이**)** - 알람 출력 릴레이를 활성화합니다. 그러면 버저, 플래쉬 등 접촉부에 부착한 외부 알람이 활성화됩니다. 또한 출력 LED가 빨간색으로 바뀝니다.
- **syslog** - syslog 메시지를 보냅니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- **notifies(**알림**)** - SNMP 트랩을 보냅니다.
- **disable(**비활성**)** - 전원 공급 장치 알람을 비활성화합니다. 전원 공급 장치 알람에 대해 구성된 기타 모든 작업은 작동하지 않습니다.

예를 들어 전원 공급 장치 알람에 대한 모든 작업을 활성화하려면 다음 명령을 입력합니다.

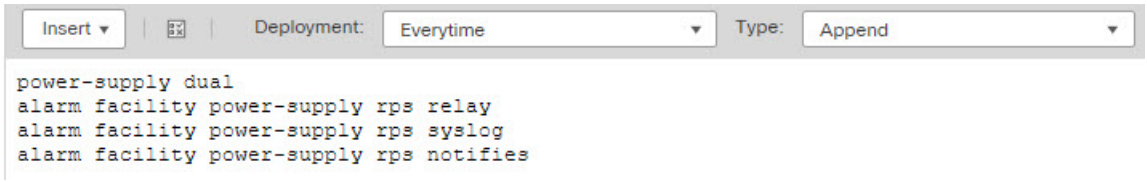
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

f) 개체 본문에 원하는 명령이 포함되어 있는지 확인합니다.

예를 들어 이 템플릿에 이 절차에 나와 있는 모든 명령 예시가 포함되어 있는 경우 개체 본문은 다음과 같은 명령을 포함하게 됩니다.

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

개체 본문은 다음과 비슷해야 합니다.



g) **Save(**저장**)**를 클릭합니다.

단계 **2** FlexConfig 정책을 생성하고 디바이스에 할당합니다.

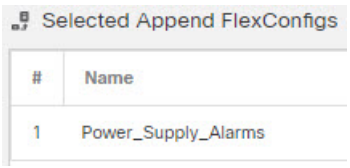
a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.

b) **New Policy(**새 정책**)**를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

c) 목차의 **User Defined(**사용자 정의**)** 폴더에서 전원 공급 장치 알람 FlexConfig 개체를 선택하고 > 을 클릭해 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs** 목록에 추가해야 합니다.



d) **Save(**저장**)**를 클릭합니다.

e) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 Save(저장) 아래에 있는 **Policy Assignments(**정책 할당**)** 링크를 클릭하여 할당합니다.

f) **Preview Config(**구성 미리보기**)**를 클릭하고, Preview(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. FlexConfig 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 전원 공급 장치 알람 명령의 경우 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

단계 **3** 변경 사항을 배포합니다.

FlexConfig 정책을 디바이스에 할당했기 때문에 항상 구축 경고가 표시됩니다. FlexConfig는 주의해서 사용해야 한다는 뜻입니다. **Proceed(**계속하기**)**를 클릭하여 구축을 계속 진행합니다.

구축이 끝나면 구축 내역과 구축 기록을 확인할 수 있습니다. 이 기능은 구축이 실패했을 때 특히 유용합니다. 구축된 설정 확인, 1302 페이지의 내용을 참조하십시오.

온도 알람 구성

디바이스의 CPU 카드 온도를 기준으로 알람을 구성할 수 있습니다.

기본 및 보조 온도 범위를 설정할 수 있습니다. 온도가 최저 임계값 아래로 떨어지거나 최고 임계값을 초과하면 알람이 트리거됩니다.

기본 온도 알람은 모든 알람 작업(출력 릴레이, syslog, SNMP)에 대해 기본적으로 활성화됩니다. 기본 온도 범위의 기본 설정은 -40°C~92°C입니다.

보조 온도 알람은 기본적으로 비활성화됩니다. 보조 온도는 -35°C~85°C 범위 내에서 설정할 수 있습니다.

보조 온도 범위는 기본 범위보다 더 제한적이므로 보조 최저 온도나 최고 온도를 설정하는 경우, 기본 설정에 대해 기본값이 아닌 값을 구성하더라도 이 설정으로 인해 해당하는 기본 설정이 비활성화됩니다. 최고 온도 알람 2개와 최저 온도 알람 2개를 각기 별도로 활성화할 수는 없습니다.

따라서 실제로는 최고 온도와 최저 온도에 대해 기본 설정이나 보조 설정만 구성해야 합니다.

프로시저

단계 **1** FlexConfig 개체를 생성하여 온도 알람을 구성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택합니다.
c) **Add FlexConfig Object(FlexConfig** 개체 추가**)**를 클릭하고, 다음 속성을 구성한 다음 **Save(**저장**)**를 클릭합니다.

- **Name(**이름**)** - 개체 이름입니다. 예를 들어 Configure_Temperature_Alarms.
- **Deployment(**구축**) - Everytime(**항상**)**을 선택합니다. 모든 구축에 구성을 전송해 설정 상태를 유지합니다.
- **Type(**유형**)** - 기본값인 **Append(**추가**)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.

- **Object body(**개체 본문**)**-개체 본문에서 온도 알람을 구성하는 데 필요한 명령을 입력합니다. 다음 단계에서는 명령에 대해 설명합니다.

d) 허용 가능한 온도 범위를 구성합니다.

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

온도는 섭씨 단위입니다. 기본 알람에 대해 허용되는 범위는 -40~92(기본 범위)입니다. 보조 알람에 대해 허용되는 범위는 -35~85입니다. 최저 온도 값은 최고 온도 값보다 작아야 합니다.

예를 들어 더 제한적인 온도 범위인 -20~80(보조 알람에 대해 허용되는 범위 내)을 설정하려면 다음과 같이 보조 알람을 구성합니다.

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

e) 온도 알람이 트리거될 때 수행할 작업을 구성합니다.

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

여러 작업을 구성할 수 있습니다. 예를 들어 외부 알람을 활성화하고, syslog 메시지를 보내고, SNMP 트랩도 전송하도록 디바이스를 구성할 수 있습니다.

- **relay(**릴레이**)** - 알람 출력 릴레이를 활성화합니다. 그러면 버저, 플래쉬 등 접촉부에 부착한 외부 알람이 활성화됩니다. 또한 출력 LED가 빨간색으로 바뀝니다.
- **syslog** - syslog 메시지를 보냅니다.
- **notifies(**알림**)** - SNMP 트랩을 보냅니다.

예를 들어 보조 온도 알람에 대해 모든 작업을 활성화하려면 다음 명령을 입력합니다.

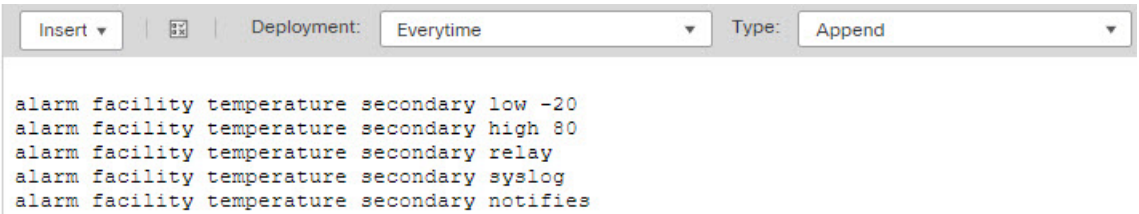
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

f) 개체 본문에 원하는 명령이 포함되어 있는지 확인합니다.

예를 들어 이 템플릿에 이 절차에 나와 있는 모든 명령 예시가 포함되어 있는 경우 개체 본문은 다음과 같은 명령을 포함하게 됩니다.

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

개체 본문은 다음과 비슷해야 합니다.



g) **Save(**저장**)**를 클릭합니다.

단계 **2** FlexConfig 정책을 생성하고 디바이스에 할당합니다.

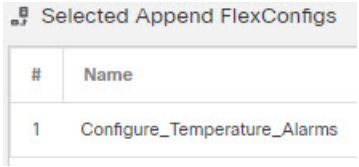
a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.

b) **New Policy(**새 정책**)**를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

c) 목차의 **User Defined(**사용자 정의**)** 폴더에서 온도 알람 FlexConfig 개체를 선택하고 >을 클릭해 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs** 목록에 추가해야 합니다.



d) **Save(**저장**)**를 클릭합니다.

e) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 Save(저장) 아래에 있는 **Policy Assignments(**정책 할당**)** 링크를 클릭하여 할당합니다.

f) **Preview Config(**구성 미리보기**)**를 클릭하고, Preview(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. FlexConfig 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 온도 알람 명령의 경우 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

단계 **3** 변경 사항을 배포합니다.

FlexConfig 정책을 디바이스에 할당했기 때문에 항상 구축 경고가 표시됩니다. FlexConfig는 주의해서 사용해야 한다는 뜻입니다. **Proceed(**계속하기**)**를 클릭하여 구축을 계속 진행합니다.

구축이 끝나면 구축 내역과 구축 기록을 확인할 수 있습니다. 이 기능은 구축이 실패했을 때 특히 유용합니다. 구축된 설정 확인, 1302 페이지의 내용을 참조하십시오.

알람 모니터링

다음 주제에서는 알람을 모니터링하고 관리하는 방법을 설명합니다.

알람 상태 모니터링

CLI에서 다음 명령을 사용하여 알람을 모니터링할 수 있습니다.

- **show alarm settings**

  가능한 각 알람의 현재 컨피그레이션을 표시합니다.

- **show environment alarm-contact**

  입력 알람 접촉부의 물리적 상태에 대한 정보를 표시합니다.

- **show facility-alarm relay**

  출력 릴레이를 트리거한 알람에 대한 정보를 표시합니다.

- **show facility-alarm status** [**info** | **major** | **minor**]

  트리거된 모든 알람에 대한 정보를 표시합니다. **major** 또는 **minor** 상태를 기준으로 필터링하여 보기를 제한할 수 있습니다. **info** 키워드를 사용하면 키워드를 사용하지 않을 때와 출력이 동일합니다.

Syslog 메시지에서 알람 모니터링

구성하는 알람 유형에 따라 다음 syslog 메시지가 표시될 수 있습니다.

듀얼 전원 공급 장치 알람

- %FTD-1-735005: Power Supply Unit Redundancy OK(전원 공급 장치 유닛 이중화 정상)
- %FTD-1-735006: Power Supply Unit Redundancy Lost(전원 공급 장치 유닛 이중화 손실)

온도 알람

이러한 알람에서 *Celsius*는 디바이스에서 탐지된 온도(섭씨)로 대체됩니다.

- %FTD-6-806001: Primary alarm CPU temperature is High(기본 알람 CPU 온도 높음) 섭씨
- %FTD-6-806002: Primary alarm for CPU high temperature is cleared(CPU 고온에 대한 기본 알람이 해제됨)
- %FTD-6-806003: Primary alarm CPU temperature is Low(기본 알람 CPU 온도 낮음) 섭씨
- %FTD-6-806004: Primary alarm for CPU Low temperature is cleared(CPU 저온에 대한 기본 알람이 해제됨)
- %FTD-6-806005: Secondary alarm CPU temperature is High(보조 알람 CPU 온도 높음) 섭씨

- %FTD-6-806006: Secondary alarm for CPU high temperature is cleared(CPU 고온에 대한 보조 알람이 해제됨)
- %FTD-6-806007: Secondary alarm CPU temperature is Low(보조 알람 CPU 온도 낮음) 섭씨
- %FTD-6-806008: Secondary alarm for CPU Low temperature is cleared(CPU 저온에 대한 보조 알람이 해제됨)

알람 입력 접촉부 알람

이러한 알람에서 *description*은 구성한 접촉부에 대한 설명입니다.

- %FTD-6-806009: Alarm asserted for ALARM_IN_1 *alarm_1_description*(ALARM_IN_1 alarm_1_description에 대해 알람 어셜션됨)
- %FTD-6-806010: Alarm cleared for ALARM_IN_1 *alarm_1_description*(ALARM_IN_1 alarm_1_description에 대한 알람 해제됨)
- %FTD-6-806011: Alarm asserted for ALARM_IN_2 *alarm_2_description*(ALARM_IN_2 alarm_2_description에 대해 알람 어셜션됨)
- %FTD-6-806012: Alarm cleared for ALARM_IN_2 *alarm_2_description*(ALARM_IN_2 alarm_2_description에 대해 알람 해제됨)

외부 알람 끄기

알람 출력에 연결된 외부 알람을 사용 중인 경우, 알람이 트리거되면 **clear facility-alarm output** 명령을 사용하여 디바이스 CLI에서 외부 알람을 끌 수 있습니다. 이 명령은 출력 PIN을 비활성화하며 출력 LED도 끕니다.

알람에 대한 기록

기능	버전	설명
Cisco ISA 3000 시리즈에 대한 알람	6.7	Cisco ISA 3000 시리즈에 대한 알람 구성은 FlexConfig를 사용하여 검증되었습니다. 듀얼 전원 공급 장치 알람을 제외하고 FlexConfig를 지원하는 이전 릴리스에서 알람을 구성할 수 있어야 합니다. 지원되는 플랫폼 : ISA 3000의 Firepower Threat Defense

XII 부

어플라이언스 플랫폼 설정

- 시스템 구성, 1339 페이지
- 플랫폼 설정 정책, 1401 페이지
- 클래식 디바이스에 대한 플랫폼 설정, 1405 페이지
- Firepower Threat Defense 플랫폼 설정, 1423 페이지
- 보안 인증 컴플라이언스, 1469 페이지

51 장

시스템 구성

다음 항목에서는 Firepower Management Center 및 매니지드 디바이스에 대한 시스템 구성 설정을 구성하는 방법에 대해 설명합니다.

- 시스템 컨피그레이션 요구 사항 및 전제 조건, 1340 페이지
- 시스템 구성 관련 정보, 1340 페이지
- 어플라이언스 정보, 1343 페이지
- HTTPS 인증서, 1344 페이지
- 외부 데이터베이스 액세스 설정, 1349 페이지
- 데이터베이스 이벤트 제한 수, 1350 페이지
- Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지
- 종료 또는 재시작, 1362 페이지
- 원격 스토리지 관리, 1363 페이지
- 검증 번경, 1367 페이지
- 정책 변경 코멘트, 1369 페이지
- 액세스 목록, 1370 페이지
- 감사 로그, 1371 페이지
- 대시보드 설정, 1373 페이지
- DNS 캐시, 1373 페이지
- 이메일 공지, 1374 페이지
- 언어 선택, 1375 페이지
- 로그인 배너, 1376 페이지
- SNMP 폴링, 1376 페이지
- STIG 컴플라이언스, 1378 페이지
- 시간 및 시간 동기화, 1379 페이지
- 전역 사용자 구성, 1385 페이지
- 세션 시간 초과, 1388 페이지
- 취약성 매핑, 1389 페이지
- 원격 콘솔 액세스 관리, 1390 페이지
- VMware Tools 및 가상 시스템, 1396 페이지
- 시스템 구성 기록, 1397 페이지

시스템 컨피그레이션 요구 사항 및 전제 조건

모델 지원

FMC

일부 설정은 7000 및 8000 Series 디바이스에도 적용됩니다.

지원되는 도메인

글로벌

사용자 역할

관리자

시스템 구성 관련 정보

Firepower Management Center 또는 클래식 매니지드 디바이스(7000 및 8000 Series, ASA FirePOWER, NGIPSv)에 적용된 시스템 구성 설정입니다.

- Firepower Management Center의 경우 이 구성 설정은 '로컬' 시스템 구성에 포함되어 있습니다. Firepower Management Center의 시스템 구성은 단일 시스템에만 해당되며 FMC의 시스템 구성 변경은 해당 시스템에만 영향을 미칩니다.
- 클래식 관리 디바이스의 경우, Firepower Management Center의 이 구성을 플랫폼 설정 정책의 일부로 적용합니다. 공유 정책을 생성하여 매니지드 디바이스에 적합한 시스템 구성 설정의 하위 집합을 구성합니다. 이 하위 집합은 구축 전반에서 유사할 수 있습니다.

팁 7000 및 8000 Series 디바이스의 경우 콘솔 구성 및 원격 관리와 같은 로컬 웹 인터페이스에서 제한된 시스템 구성 작업을 수행할 수 있습니다. 이러한 구성은 플랫폼 설정 정책을 사용하는 7000 또는 8000 Series 디바이스에 적용되는 구성과 다릅니다.

Firepower Management Center 시스템 구성 탐색

시스템 구성은 Firepower Management Center에 대한 기본적인 설정을 나타냅니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** 탐색 패널을 사용하여 변경할 구성을 선택합니다. 자세한 내용은 표 87: 시스템 구성 설정 , 1341 페이지 섹션을 참조하십시오.

시스템 구성 설정

매지니드 디바이스의 경우, 이러한 구성 대부분은 FMC에서 적용한 플랫폼 설정 정책으로 처리합니다. 자세한 내용은 플랫폼 설정 정책, 1401 페이지의 내용을 참조하십시오.7000/8000 시리즈 디바이스의 경우, 비정책 기반 시스템 구성의 로컬 웹 인터페이스에 로그인할 수 있습니다. 자세한 내용은 7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성, 1416 페이지의 내용을 참조하십시오.

표 ***87:*** 시스템 구성 설정

설정	설명
액세스 제어 환경 설정	액세스 제어 정책을 추가하거나 수정할 때 주석을 사용자에게 표시하도록 시스템을 구성합니다. 정책 변경 코멘트, 1369 페이지 섹션을 참조하십시오.
액세스 목록	특정 포트에서 어떤 컴퓨터가 시스템에 액세스할 수 있는지 제어합니다. 액세스 목록, 1370 페이지 섹션을 참조하십시오.
감사 로그	감사 로그를 외부 호스트로 보내도록 시스템을 구성합니다. 감사 로그, 1371 페이지 섹션을 참조하십시오.
검증 번경	지난 24시간 동안 시스템 변경 사항에 대한 상세한 보고서를 보내도록 시스템을 구성합니다. 검증 번경, 1367 페이지 섹션을 참조하십시오.
콘솔 구성	VGA 또는 시리얼 포트나 LOM(Lights-Out Management)을 통한 콘솔 액세스를 구성합니다. 원격 콘솔 액세스 관리, 1390 페이지 섹션을 참조하십시오.
대시보드	대시보드에서 Custom Analysis 위젯을 활성화합니다. 대시보드 설정, 1373 페이지 섹션을 참조하십시오.
데이터베이스	Firepower Management Center에서 저장할 수 있는 각 이벤트 유형의 최대 수를 지정합니다. 데이터베이스 이벤트 제한 수, 1350 페이지 섹션을 참조하십시오.
DNS 캐시	이벤트 보기 페이지에서 자동으로 IP 주소를 확인하도록 시스템을 구성합니다. DNS 캐시, 1373 페이지 섹션을 참조하십시오.
이메일 알림	메일 호스트를 구성하고, 암호화 방법을 선택하고, 이메일 기반 알림 및 보고를 위한 인증 자격 증명을 제공합니다. 이메일 공지, 1374 페이지 섹션을 참조하십시오.
External Database Access(외부 데이터베이스 액세스)	데이터베이스에 대한 외부 읽기 전용 액세스를 활성화하고, 다운로드할 클라이언트 드라이버를 제공합니다. 외부 데이터베이스 액세스 설정, 1349 페이지 섹션을 참조하십시오.
HTTPS 인증서	필요하다면 신뢰된 권한 및 업로드 인증서에서 시스템에 HTTPS 서버 인증서를 요청합니다. HTTPS 인증서, 1344 페이지 섹션을 참조하십시오.

설정	설명
정보	어플라이언스에 대한 현재 정보를 보고 표시 이름을 편집합니다. 어플라이언스 정보, 1343 페이지 섹션을 참조하십시오.
Intrusion Policy Preferences(침입 정책 환경 설정)	사용자가 침입 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성합니다 정책 변경 코멘트, 1369 페이지 섹션을 참조하십시오.
언어	웹 인터페이스에 대해 다른 언어를 지정합니다. 언어 선택, 1375 페이지 섹션을 참조하십시오.
로그인 배너	사용자가 로그인 때 나타나는 사용자 정의 로그인 배너를 만듭니다. 로그인 배너, 1376 페이지 섹션을 참조하십시오.
Management Interfaces(관리 인터페이스)	어플라이언스의 IP 주소, 호스트 이름 및 프록시 설정과 같은 옵션을 변경합니다. Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지 섹션을 참조하십시오.
네트워크 분석 정책 환경 설정	사용자가 네트워크 분석 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성합니다. 정책 변경 코멘트, 1369 페이지 섹션을 참조하십시오.
프로세스	Firepower 프로세스를 종료, 리부팅 또는 다시 시작합니다. 종료 또는 재시작, 1362 페이지 섹션을 참조하십시오.
원격 스토리지 디바이스	백업 및 보고서에 대한 원격 스토리지를 구성합니다. 원격 스토리지 관리, 1363 페이지 섹션을 참조하십시오.
셸 시간 초과	비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 분 단위로 구성합니다. 세션 시간 초과, 1388 페이지 섹션을 참조하십시오.
SNMP	SNMP(Simple Network Management Protocol) 폴링을 활성화합니다. SNMP 폴링, 1376 페이지 섹션을 참조하십시오.
STIG 컴플라이언스	미 국방부에서 정한 특정 요구 사항 준수 설정을 활성화합니다. STIG 컴플라이언스, 1378 페이지 섹션을 참조하십시오.
시간	현재 시간 설정을 확인하고 변경합니다. 시간 및 시간 동기화, 1379 페이지 섹션을 참조하십시오.
시간 동기화	시스템에 대한 시간 동기화를 관리합니다. 시간 및 시간 동기화, 1379 페이지 섹션을 참조하십시오.
사용자 구성	모든 사용자의 로그인 기록 및 비밀번호 기록을 성공적으로 추적하거나 유효하지 않은 로그인 자격 증명을 입력한 사용자에게 임시 잠금을 시행하도록 Firepower Management Center를 구성합니다. 전역 사용자 구성, 1385 페이지 섹션을 참조하십시오.
VMware Tools	Firepower Management Center Virtual에서 VMware Tools를 활성화하고 사용합니다. VMware Tools 및 가상 시스템, 1396 페이지 섹션을 참조하십시오.
취약성 매핑	해당 주소에서 수신되거나 전송된 모든 애플리케이션 프로토콜 트래픽의 취약성을 호스트 IP 주소에 매핑합니다. 취약성 매핑, 1389 페이지 섹션을 참조하십시오.

관련 항목

클래식 디바이스에 대한 플랫폼 설정 관련 정보, 1405 페이지

어플라이언스 정보

웹 인터페이스의 **System(**시스템**) > Configuration(**구성**)** 페이지에는 아래 표에 나열된 정보가 포함됩니다. 달리 명시되지 않는 한 모든 필드는 읽기 전용입니다.

참고 **Help(**도움말**) > About(**정보**(** 페이지를 참조하십시오. 비슷하지만 약간 다른 정보를 제공합니다.

필드	설명
이름	FMC어플라이언스에 할당한 설명 이름입니다. 어플라이언스 이름으로 호스트 이름을 사용할 수 있지만 이 필드에 다른 이름을 입력해도 호스트 이름은 변경되지 않습니다. 이 이름은 특정 통합에서 사용됩니다. 예를 들어 SecureX 및 Cisco SecureX Threat Response와의 통합을 위해 디바이스 목록에 표시됩니다.
제품 모델	어플라이언스의 모델 이름입니다.
일련 번호	어플라이언스의 일련 번호입니다.
Software Version(소프트웨어 버전)	어플라이언스에 현재 설치된 소프트웨어 버전입니다.
Prohibit Packet Transfer to the Firepower Management Center	매니지드 디바이스가 이벤트와 함께 패킷 데이터를 전송하여 Firepower Management Center에 데이터를 저장할 수 있는지 여부를 지정합니다. 이 설정은 7000 및 8000 Series 디바이스의 로컬 웹 인터페이스에서 사용할 수 있습니다.
운영 체제	현재 어플라이언스에서 실행되는 운영 체제입니다.
운영 체제 버전	현재 어플라이언스에서 실행되는 운영 체제의 버전입니다.
IPv4 주소	기본(`eth0`) 관리 인터페이스의 IPv4 주소입니다. IPv4 관리가 비활성화된 경우, 이 필드는 이를 나타냅니다.

필드	설명
IPv6 주소	기본(eth0) 관리 인터페이스의 IPv6 주소입니다. IPv6 관리가 비활성화된 경우, 이 필드는 이를 나타냅니다.
현재 정책	현재 구축된 시스템 레벨 정책입니다. 마지막으로 구축된 후부터 정책이 업데이트된 경우, 정책 이름은 기울임 꼴로 표시됩니다.
모델 번호	내부 플래시 드라이브에 저장된 어플라이언스별 모델 번호입니다. 이 번호는 문제 해결을 위해 중요할 수 있습니다.

어플라이언스 정보 보기

프로시저

System(시스템**)** > **Configuration(**구성**)**을 선택합니다.

기본 시스템 정보 보기

About(정보) 페이지에는 Firepower System의 모델, 일련 번호, 다양한 구성 요소에 대한 버전 정보 등 어플라이언스에 대한 정보가 표시됩니다. 또한 Cisco 저작권 정보도 포함되어 있습니다.

프로시저

단계 **1** 페이지 상단에 있는 툴바에서 **Help(**도움말**)**를 클릭합니다.

단계 **2** **About(**정보**)**를 선택합니다.

HTTPS 인증서

SSL(Secure Sockets Layer)/TLS 인증서를 사용하면 Firepower Management Center 및 7000 및 8000 Series 디바이스가 시스템과 웹 브라우저 간에 암호화된 채널을 활성화할 수 있습니다. 기본 인증서는 모든 Firepower 디바이스에 포함되어 있지만 전역적으로 알려진 CA가 신뢰할 수 있는 인증 기관 (CA)에서 생성되지는 않습니다. 따라서 전역적으로 알려졌거나 내부에서 신뢰할 수 있는 CA가 서명한 사용자 정의 인증서로 교체하는 것이 좋습니다.

기본 HTTPS 서버 인증서

어플라이언스와 함께 제공된 기본 서버 인증서를 사용하는 경우 기본 서버 인증서가 클라이언트 인증서에 서명한 CA에 의해 서명되지 않았으므로 시스템에서 웹 인터페이스 액세스에 유효한 HTTPS 클라이언트 인증서를 요구하도록 구성하지 마십시오.

기본 서버 인증서의 수명은 인증서가 생성된 시점에 따라 달라집니다. 기본 서버 인증서 만료일을 보려면 **System(**시스템**)** > **Configuration(**구성**)** > **HTTPS Certificate(HTTPS** 인증서**)**을 선택합니다.

일부 Firepower 소프트웨어 업그레이드는 인증서를 자동으로 갱신할 수 있습니다. 자세한 내용은 Cisco Firepower 릴리스 노트를 참조하십시오.

Firepower Management Center 및 7000 및 8000 Series 디바이스의 **System(**시스템**)** > **Configuration(**구성**)** > **HTTPS Certificate(HTTPS** 인증서**)** 페이지에서 기본 인증서를 갱신할 수 있습니다. 7000 및 8000 Series디바이스에서 CLI 명령 `system renew-http-cert`를 사용하여 기본 인증서를 갱신할 수도 있습니다.

맞춤형 HTTPS 서버 인증서

사용자가 제공하는 시스템 정보 및 ID 정보에 따라 Firepower Management Center 웹 인터페이스를 사용하여 서버 인증서 요청을 생성할 수 있습니다. 브라우저가 신뢰하는 설치된 내부 인증 기관(CA)이 있는 경우 요청을 사용하여 인증서에 서명할 수 있습니다. 또한 인증 기관에 서버 인증서를 요청하는 결과 요청을 보낼 수 있습니다. 인증 기관(CA)으로부터 서명된 인증서를 확보한 후, 이를 가져올 수 있습니다.

HTTPS 클라이언트 인증서

클라이언트 브라우저 인증서 확인을 사용하여 Firepower System 웹 서버에 대한 액세스를 제한할 수 있습니다. 사용자 인증서를 활성화하면, 웹 서버는 사용자의 브라우저 클라이언트가 올바른 사용자 인증서가 선택되도록 했는지 확인합니다. 해당 사용자 인증서는 반드시 서버 인증서에 사용되는 인증 기관과 동일한 신뢰 기관에서 생성된 것이어야 합니다. 브라우저는 다음과 같은 경우 웹 인터페이스를 로드할 수 없습니다.

- 사용자가 유효하지 않은 브라우저에서 인증서를 선택합니다.
- 사용자가 브라우저에서 서버 인증서에 서명한 인증 기관이 생성하지 않은 인증서를 선택합니다.
- 사용자가 브라우저에서 디바이스의 인증서 체인에 있는 인증 기관이 생성하지 않은 인증서를 선택합니다.

또한 서버에 대한 CRL(인증서 해치 목록)을 로드할 수 있습니다. CRL 목록은 인증 기관에서 해지한 모든 인증서를 나열하므로, 웹 서버는 클라이언트 브라우저 인증서가 유효한 것을 확인할 수 있습니다. 사용자가 해지된 인증서로서 CRL에 나열된 인증서를 선택한 경우, 브라우저는 웹 인터페이스를 로드할 수 없습니다.

현재 서버 인증서 보기

로그인한 어플라이언스의 서버 인증서만 볼 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

인증서 서명 요청 생성 및 제출

이 절차를 사용하여 로컬 구성 HTTPS Certificate(HTTPS 인증서) 페이지를 통해 인증서 요청을 생성할 때, 단일 시스템에 대해서만 인증서를 생성할 수 있습니다. 유사하게, 시스템에 연결할 때 전역으로 알려졌거나 내부적으로 신뢰할 수 있는 CA에서 서명되지 않은 인증서를 설정하는 경우 보안 경고가 표시됩니다.

인증서 요청에 대해 생성된 키는 Base-64로 인코딩된 PEM 형식입니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **3** **Generate New CSR(**새로운 **CSR** 생성**)**을 클릭합니다.

단계 **4** **Country Name (two-letter code)(**국가 이름**(2**글자 코드**))** 필드에 국가 번호를 입력합니다.

단계 **5** **State or Province(**주 또는 도**)** 필드에 주 또는 도에 대한 우편 약자를 입력합니다.

단계 **6** **Locality or City(**구/군/시**)**를 입력합니다.

단계 **7** **Organization(**조직**)** 이름을 입력합니다.

단계 **8** **Organizational Unit(**조직 단위**)(Department(**부서**))** 이름을 입력합니다.

단계 **9** **Common Name(**공용 이름**)** 필드에 인증서를 요청할 서버의 정규화된 도메인 이름을 올바르게 입력합니다.

참고 **Common Name(**공용 이름**)** 필드의 인증서에 나타나도록 서버의 정규화된 도메인 이름을 올바르게 입력해야 합니다. 공용 이름과 DNS 호스트 이름이 일치하지 않는 경우, 어플라이언스에 연결하면 경고를 받습니다.

단계 **10** **Generate(**생성**)**를 클릭합니다.

단계 **11** 텍스트 편집기를 엽니다.

단계 **12** `BEGIN CERTIFICATE REQUEST(`인증서 요청 시작`)` 및 `END CERTIFICATE REQUEST(`인증서 요청 끝`)`를 포함하는 인증서 요청의 전체 텍스트 블록을 복사하여 비어있는 텍스트 파일에 붙여 넣습니다.

단계 **13** 파일을 `servername.csr`로 저장합니다. 여기서 *servername*은 인증서 사용을 계획하고 있는 서버의 이름입니다.

단계 **14** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 서명된 서버 인증서를 업로드합니다. 서버 인증서 업로드, 1347 페이지 섹션을 참조하십시오.

서버 인증서 업로드

인증서를 생성한 서명 기관이 중간 CA를 신뢰하기를 요청하는 경우, 또한 인증서 체인을 제공해야 하는데, 이는 때로 인증서 경로라고 합니다. 사용자 인증서를 요청하는 경우, 중간 권한이 인증서 체인에 포함된 인증 기관에서 생성된 것이어야 합니다.

서버 인증서 업로드

인증서를 생성한 서명 기관이 중간 CA를 신뢰하기를 요청하는 경우, 또한 인증서 체인을 제공해야 하는데, 이는 때로 인증서 경로라고 합니다. 사용자 인증서를 요청하는 경우, 중간 권한이 인증서 체인에 포함된 인증 기관에서 생성된 것이어야 합니다.

시작하기 전에

- 인증서 서명 요청을 생성합니다. 인증서 서명 요청 생성 및 제출, 1346 페이지 섹션을 참조하십시오.
- 인증서를 요청할 인증 기관에 CSR 파일을 업로드하거나 CSR를 사용하여 자체 서명된 인증서를 만드십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **3** **Import HTTPS Certificate(HTTPS** 인증서 가져오기**)**를 클릭합니다.

단계 **4** 텍스트 편집기의 서버 인증서를 열어 `BEGIN CERTIFICATE` 및 `END CERTIFICATE` 문구를 포함하는 전체 텍스트 블록을 복사하여 **Server Certificate(**서버 인증서**)** 필드에 붙여 넣습니다.

단계 **5** 개인 키를 업로드하려는 경우 개인 키 파일을 열어 `BEGIN RSA PRIVATE KEY(RSA 개인 키 시작)` 및 `END RSA PRIVATE KEY(RSA 개인 키 끝)` 문구를 포함하는 전체 텍스트 블록을 복사하여 **Private Key(**개인 키**)** 필드에 붙여 넣습니다.

단계 **6** 사용자가 제공해야 하는 중간 인증서를 열어서 전체 텍스트 블록을 복사하여 각각을 **Certificate Chain(**인증서 체인**)** 필드에 붙여 넣습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

유효한 사용자 인증서 필요

시스템은 식별 부호화 규칙(DER) 형식의 CRL 업로드를 지원합니다. 한 서버에 대해 단 하나의 CRL만 로드할 수 있습니다.

해지된 인증서 목록이 통용되고 있음을 확인하기 위해, CRL을 업데이트하는 예약된 작업을 생성할 수 있습니다. 가장 최근 재생된 CRL이 인터페이스에 나열됩니다.

참고 반드시 사용자 브라우저(또는 판독기에 삽입된 CAC)에 유효한 사용자 인증서가 있어야 사용자 인증서를 활성화할 수 있고, 실행 후 웹 인터페이스에 액세스할 수 있습니다.

시작하기 전에

- 서버 인증서에 사용된 것과 동일한 인증 기관을 사용하여 사용자 인증서를 생성합니다.
- 인증서의 중간 인증서를 업로드합니다. 서버 인증서 업로드, 1347 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **3** **Enable User Certificates(**사용자 인증서 활성화**)**를 선택합니다. 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **4** CRL을 검색하려는 경우 **Enable Cetching of CRL(CRL** 가져오기**)**을 선택합니다.

단계 **5** 기존 CRL 파일에 유효한 URL을 입력하고 **Refresh CRL(CRL** 새로 복구**)**을 클릭합니다. 제공된 URL에서 현재 CRL을 서버에 로드합니다.

참고 CRL 페칭을 활성화하면 정기적으로 CRL을 업데이트하는 예약된 작업을 생성합니다. 작업을 수정하여 업데이트의 빈도를 설정합니다.

단계 **6** 가지고 있는 사용자 인증서가 서버 인증서를 만든 것과 동일한 인증 기관에서 생성한 것인지 확인합니다.

주의 활성화된 사용자 인증서로 구성을 저장하면, 브라우저 인증서 스토어에 유효한 사용자 인증서가 없는 경우, 어플라이언스에 모든 웹 서버 액세스를 비활성화합니다. 구성을 저장하기 전에 설치된 사용 가능한 인증서가 있는지 확인합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

기본 HTTPS 서버 인증서 갱신

로그인한 어플라이언스의 서버 인증서만 볼 수 있습니다.

프로시저

단계 1 **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 2 **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

이 버튼은 시스템이 기본 HTTPS 서버 인증서를 사용하도록 구성된 경우에만 나타납니다.

단계 3 **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)**을 클릭합니다. (이 옵션은 시스템이 기본 HTTPS 서버 인증서를 사용하도록 구성된 경우에만 인증서 정보 아래 화면에 나타납니다.)

단계 4 (선택 사항) **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)** 대화 상자에서 인증서에 대한 새 키를 생성하기 위한 **Generate New Key(**새 키 생성**)**를 선택합니다.

단계 5 **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)** 대화 상자에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

HTTPS Certificate(HTTPS 인증서**)** 페이지에 표시된 인증서 유효 기간이 업데이트되었는지 확인하여 인증서가 갱신되었는지 확인할 수 있습니다.

외부 데이터베이스 액세스 설정

서드파티 클라이언트에 데이터베이스에 대한 읽기 전용 액세스를 허용하도록 Firepower Management Center를 구성할 수 있습니다. 그러면 다음 중 하나를 사용하여 SQL로 데이터베이스에 쿼리할 수 있습니다.

- Actuate BIRT, JasperSoft iReport 또는 Crystal Reports와 같은 산업 표준 보고 툴
- JDBC SSL 연결을 지원하는 기타 보고 애플리케이션(사용자 지정 애플리케이션 포함)
- 인터랙티브 방식으로 실행하거나 단일 쿼리에 대해 쉼표로 구분된 결과를 얻기 위해 사용할 수 있는 RunQuery라는 Cisco 제공 명령줄 Java 애플리케이션

Firepower Management Center의 시스템 구성을 사용하여 데이터베이스 액세스를 활성화하고 선택한 호스트가 데이터베이스를 쿼리할 수 있도록 액세스 목록을 만듭니다. 이 액세스 목록은 어플라이언스 액세스를 제어하지 않습니다.

다음이 포함된 패키지를 다운로드할 수도 있습니다.

- RunQuery - Cisco 제공 데이터베이스 쿼리 툴
- InstallCert - 액세스하려는 Firepower Management Center에서 SSL 인증서를 검색하고 승인하기 위해 사용할 수 있는 툴

- 데이터베이스에 연결하기 위해 사용해야 하는 JDBC 드라이버

데이터베이스 액세스를 구성하기 위해 다운로드한 패키지의 툴 사용에 대한 내용은 *Firepower System* 데이터베이스 액세스 설명서 섹션을 참조하십시오.

데이터베이스에 대한 외부 액세스 활성화

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **External Database Access(**외부 데이터베이스 액세스**)**를 클릭합니다.

단계 **3** **Allow External Database Access**(외부 데이터베이스 액세스 허용) 확인란을 선택합니다.

단계 **4** **Server Hostname(**서버 호스트네임**)** 필드에 적절한 값을 입력합니다. 서드파티 애플리케이션 요건에 따라 이 값은 Firepower Management Center의 QDN(정규화된 도메인 이름), IPv4 주소 또는 IPv6 주소일 수 있습니다.

단계 **5** **Client JDBC Driver**(클라이언트 JDBC 드라이버) 옆에 있는 **Download**(다운로드)를 클릭하고 브라우저의 지시에 따라 `client.zip` 패키지를 다운로드합니다.

단계 **6** 하나 이상의 IP 주소에 대한 데이터베이스 액세스를 추가하려면 **Add Hosts**(호스트 추가)를 클릭합니다. **Access List**(액세스 목록) 필드에 **IP Address**(IP 주소) 필드가 나타납니다.

단계 **7** **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 `모두`를 입력하십시오.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

팁 마지막으로 저장된 데이터베이스 설정으로 되돌리려면 **Refresh(**새로 고침**)**를 클릭합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

데이터베이스 이벤트 제한 수

디스크 공간을 관리하기 위해서 FMC은 이벤트 데이터베이스에서 가장 오래된 침입 이벤트, 감사 기록, 보안 인텔리전스 데이터 또는 URL 필터링 데이터를 자동으로 제거합니다. 각 이벤트 유형에 대해 정리 후 FMC가 보유할 레코드 수를 지정할 수 있습니다. 해당 유형에 대해 구성된 보유 제한보다 많은 유형의 레코드를 포함하는 이벤트 데이터베이스에도 의존하지 않습니다. 성능을 높이려면 정기적으로 작업하는 이벤트 수에 대한 이벤트 제한을 조정해야 합니다. 선택적으로 정리가 발생할 때 이메일 알림을 수신하도록 선택할 수 있습니다. 일부 이벤트 유형의 경우 스토리지를 비활성화할 수 있습니다.

개별 이벤트를 수동으로 삭제하려면 이벤트 뷰어를 사용합니다. (버전 6.6.0 이상에서는 이러한 방식으로 연결 또는 보안 인텔리전스 이벤트를 수동으로 삭제할 수 없습니다.) 데이터베이스를 수동으로 제거할 수도 있습니다. 데이터 스토리지, 269 페이지의 내용을 참조하십시오.

데이터베이스 이벤트 제한 구성

시작하기 전에

- 이벤트가 Firepower Management Center 데이터베이스에서 정리될 때 이메일 알림을 받으려면 이메일 서버를 구성해야 합니다. 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Database(**데이터베이스**)**를 선택합니다.

단계 **3** 각 데이터베이스에 대해 저장할 레코드의 수를 입력합니다.

각 데이터베이스가 유지 관리할 레코드 수에 대한 정보는 데이터베이스 이벤트 제한 수, 1351 페이지 섹션을 참조하십시오.

단계 **4** 선택적으로 **Data Pruning Notification Address(**데이터 제거 알림 주소**)** 필드에 제거 알림을 수신할 이메일 주소를 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

데이터베이스 이벤트 제한 수

다음 표에는 Firepower Management Center에 저장할 수 있는 각 이벤트 유형의 최소 및 최대 레코드 수가 나열되어 있습니다.

표 ***88:*** 데이터베이스 이벤트 제한 수

이벤트 유형	상한 제한	하한 제한
침입 이벤트	1,000만(FMC Virtual) 3,000만(FMC1000, FMC1600) 6,000만(FMC2500, FMC2600, FMCv 300) 3억(FMC4500, FMC4600)	10,000
검색 이벤트	1,000만(FMC Virtual) 2,000만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	0(스토리지 비활성화)

이벤트 유형	상한 제한	하한 제한
연결 이벤트 보안 인텔리전스 이벤트	5,000만(FMC Virtual) 1억(FMC1000, FMC1600) 3억(FMC2500, FMC2600, FMCv 300) 10억(FMC4500, FMC4600) 제한은 연결 이벤트와 보안 인텔리전스 이벤트 간에 공유됩니다. 구성된 최대 값의 합은 이 제한을 초과할 수 없습니다.	0(스토리지 비활성화) 이러한 설정은 연결 요약에 영향을 주지 않습니다.
연결 요약(취합된 연결 이벤트)	5,000만(FMC Virtual) 1억(FMC1000, FMC1600) 3억(FMC2500, FMC2600, FMCv 300) 10억(FMC4500, FMC4600)	0(스토리지 비활성화)
상관관계 이벤트 및 컴플라이언스 화이트 목록 이벤트	100만(FMC Virtual) 200만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	1개
악성코드 이벤트	1,000만(FMC Virtual) 2,000만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	10,000
파일 이벤트	1,000만(FMC Virtual) 2,000만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	0(스토리지 비활성화)
상태 이벤트	100만	0(스토리지 비활성화)
감사 기록	100,000	1개
복원 상태 이벤트	1,000만	1개
화이트 리스트 위반 기록	30일 위반 기록	일일 이력
사용자 활동(사용자 이벤트)	1,000만	1개
사용자 로그인(사용자 이력)	1,000만	1개
침입 규칙 업데이트 가져오기 로그 기록	1백만	1개
VPN 문제 해결 데이터베이스	1,000만	0(스토리지 비활성화)

Management Interfaces(관리 인터페이스)관리 인터페이스

설정 후 FMC에 관리 인터페이스, 호스트 이름, 검색 도메인, DNS 서버 및 HTTP 프록시를 추가하는 것을 포함하여 관리 네트워크 설정을 변경할 수 있습니다.

FMC 관리 인터페이스 정보

기본적으로 FMC는 모든 디바이스를 단일 관리 인터페이스에서 관리합니다. 또한 관리 인터페이스에 대한 초기 설정을 수행하고 이 인터페이스에서 관리자로 FMC에 로그인할 수도 있습니다. 관리 인터페이스는 Smart Licensing 서버와 통신하고, 업데이트를 다운로드하고, 기타 관리 기능을 수행하는 작업에도 사용됩니다.

디바이스 관리 인터페이스에 대한 자세한 내용은 디바이스 관리 인터페이스, 299 페이지의 내용을 참조하십시오.

FMC의 관리 인터페이스

FMC는 초기 설정, 관리자를 위한 HTTP 액세스, 디바이스 관리, 라이선스 및 업데이트와 같은 기타 관리 기능을 위해 eth0 인터페이스를 사용합니다.

동일한 네트워크 또는 다른 네트워크에서 추가 관리 인터페이스를 구성할 수도 있습니다. FMC에서 많은 수의 디바이스를 관리할 때 관리 인터페이스를 추가하면 처리량과 성능이 향상될 수 있습니다. 다른 모든 관리 기능에 대해 이 인터페이스를 사용할 수도 있습니다. 특정 기능을 위해 각 관리 인터페이스를 사용할 수도 있습니다. 예를 들어 HTTP 관리자 액세스용으로 하나의 인터페이스를 사용하고 디바이스 관리용으로 하나의 인터페이스를 사용할 수 있습니다.

디바이스 관리의 경우 관리 인터페이스에는 두 개의 별도 트래픽 채널이 있습니다. 즉, 관리 트래픽 채널은 모든 내부 트래픽(예: 디바이스 관리와 관련된 디바이스 간 트래픽)을 전달하고, 이벤트 트래픽 채널은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다. 선택적으로 이벤트 트래픽을 처리하기 위해 FMC에 별도의 이벤트 전용 인터페이스를 구성할 수 있습니다. 하나의 이벤트 인터페이스만 구성할 수 있습니다. 이벤트 트래픽은 많은 양의 대역폭을 사용할 수 있으므로 관리 트래픽에서 이벤트 트래픽을 분리하면 FMC의 성능이 향상될 수 있습니다. 예를 들어 관리를 위해 1GigabitEthernet 인터페이스를 사용하는 경우 10GigabitEthernet 인터페이스를 이벤트 인터페이스로 할당할 수 있습니다. 예를 들어 인터넷 액세스가 포함된 네트워크의 일반 관리 인터페이스를 사용하는 동안 완전히 안전한 프라이빗 네트워크에 이벤트 전용 인터페이스를 구성할 수 있습니다. 또한 증가된 처리량만 활용하는 것이 목표인 경우 동일한 네트워크에서 관리 및 이벤트 인터페이스를 모두 사용할 수 있습니다. 매니지드 디바이스는 관리 트래픽을 FMC 관리 인터페이스로 보내고 이벤트 트래픽을 FMC 이벤트 전용 인터페이스로 보냅니다. 매니지드 디바이스가 이벤트 전용 인터페이스에 연결할 수 없는 경우 관리 인터페이스로 이벤트를 전송합니다.

참고 모든 관리 인터페이스는 액세스 목록 구성 (액세스 목록 구성, 1370 페이지)에 의해 제어되는 HTTP 관리자 액세스를 지원합니다. 반대로 인터페이스를 HTTP 액세스 전용으로 제한할 수는 없습니다. 관리 인터페이스는 항상 디바이스 관리(관리 트래픽, 이벤트 트래픽 또는 둘 다)를 지원합니다.

참고 eth0 인터페이스만 DHCP IP 주소를 지원합니다. 다른 관리 인터페이스는 고정 IP 주소만 지원합니다.

FMC 모델별 관리 인터페이스 지원

관리 인터페이스 위치에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.

각 FMC 모델에서 지원되는 관리 인터페이스는 다음 표를 참조하십시오.

표 ***89: FMC***의 관리 인터페이스 지원

모델	**Management Interfaces(**관리 인터페이스**)**관리 인터페이스
MC1000	eth0(기본값) eth1
MC2500, MC4500	eth0(기본값) eth1 eth2 eth3
MC1600, MC2600, MC4600	eth0(기본값) eth1 eth2 eth3 CIMC(Lights-Out 관리에만 지원됨)
Firepower Management Center Virtual	eth0(기본값)

FMC 관리 인터페이스의 네트워크 라우트

관리 인터페이스(이벤트 전용 인터페이스 포함)는 정적 경로만 지원하여 원격 네트워크에 연결할 수 있습니다. FMC를 설정하면 설정 과정에서 지정한 게이트웨이 IP 주소에 대한 기본 경로가 생성됩니다. 이 경로는 삭제할 수 없으며 게이트웨이 주소만 수정할 수 있습니다.

기본 경로는 항상 가장 낮은 번호의 관리 인터페이스(예: eth0)를 사용합니다.

원격 네트워크에 액세스하기 위해서는 관리 인터페이스당 최소 1개의 정적 경로가 권장됩니다. 다른 디바이스에서 FMC로의 라우팅 문제를 비롯하여 잠재적인 라우팅 문제를 방지하려면 각 인터페이스를 별도의 네트워크에 배치하는 것이 좋습니다. 동일한 네트워크의 인터페이스에서 문제가 발생하지 않으면 고정 경로를 올바르게 설정해야 합니다. 예를 들어 FMC에서 eth0 및 eth1은 모두 동일한 네트워크에 있지만 각 인터페이스에서 서로 다른 디바이스 그룹을 관리하려고 합니다. 기본 게이트웨이는 192.168.45.1입니다. eth1이 원격 10.6.6.0/24 대상 네트워크에서 디바이스를 관리하도록 하려면 동일한 게이트웨이 192.168.45.1을 사용하여 eth1을 통해 10.6.6.0/24에 대한 정적 경로를 만들 수 있습

니다. 10.6.6.0/24 트래픽은 기본 경로에 도달하기 전에 이 경로에 도달하므로 eth1이 예상대로 사용됩니다.

2개의 FMC 인터페이스를 사용하여 동일한 네트워크에 있는 원격 디바이스를 관리하려는 경우 디바이스 IP 주소별로 별도의 정적 경로가 필요하기 때문에 FMC의 정적 라우팅이 제대로 확장되지 않을 수 있습니다.

또 다른 예는 FMC 및 매니지드 디바이스에 별도의 관리 및 이벤트 전용 인터페이스를 포함합니다. 이벤트 전용 인터페이스는 관리 인터페이스와 별도의 네트워크에 있습니다. 이 경우 원격 이벤트 전용 네트워크를 대상으로 하는 트래픽에 대해 이벤트 전용 인터페이스를 통해 정적 경로를 추가할 수 있으며, 그 반대의 경우도 마찬가지입니다.

NAT 환경

NAT(Network Address Translation)는 소스 또는 대상 IP 주소를 재할당하는 작업에 관여하는 라우터를 통해 네트워크 트래픽을 보내고 받는 방법입니다. NAT는 일반적으로 프라이빗 네트워크와 인터넷이 통신하는 데 사용됩니다. 정적 NAT는 1:1 변환을 수행하여 디바이스와 FMC의 통신에 문제를 일으키지 않지만 포트 주소 변환(PAT)이 더욱 일반적입니다. PAT를 사용하면 단일 공용 IP 주소에 고유한 포트를 사용해 공용 네트워크에 접속할 수 있습니다. 이러한 포트는 필요에 따라 동적으로 할당되므로 PAT 라우터 뒤에 있는 디바이스에 연결을 시작할 수 없습니다.

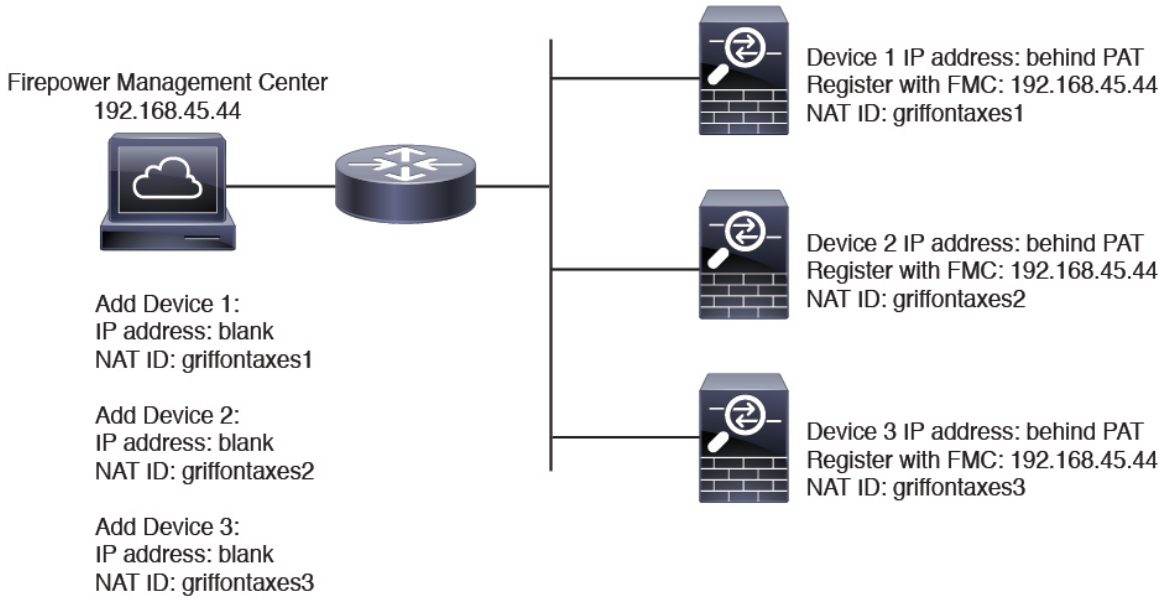
일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

예를 들어 FMC에 디바이스를 추가하지만 디바이스 IP 주소를 모르는 경우(디바이스가 PAT 라우터 뒤에 있는 경우) FMC에 NAT ID와 등록 키만 지정하고 IP 주소는 공백으로 둡니다. 디바이스에 FMC IP 주소, 동일한 NAT ID와 동일한 등록 키를 지정합니다. FMC의 IP 주소에 디바이스를 등록합니다. 이때 FMC은 IP 주소 대신 NAT ID를 사용해 디바이스를 인증합니다.

NAT 환경에서 NAT ID 사용은 일반적이지만 FMC에 많은 디바이스를 추가하려고 할 때에도 NAT ID를 선택할 수 있습니다. FMC에는 추가하려는 각 디바이스에 고유한 NAT ID를 지정하고 IP 주소를 공백으로 두고, 각 디바이스에서 FMC IP 주소 및 NAT ID를 지정하십시오. 주의: NAT ID는 디바이스별로 고유해야 합니다.

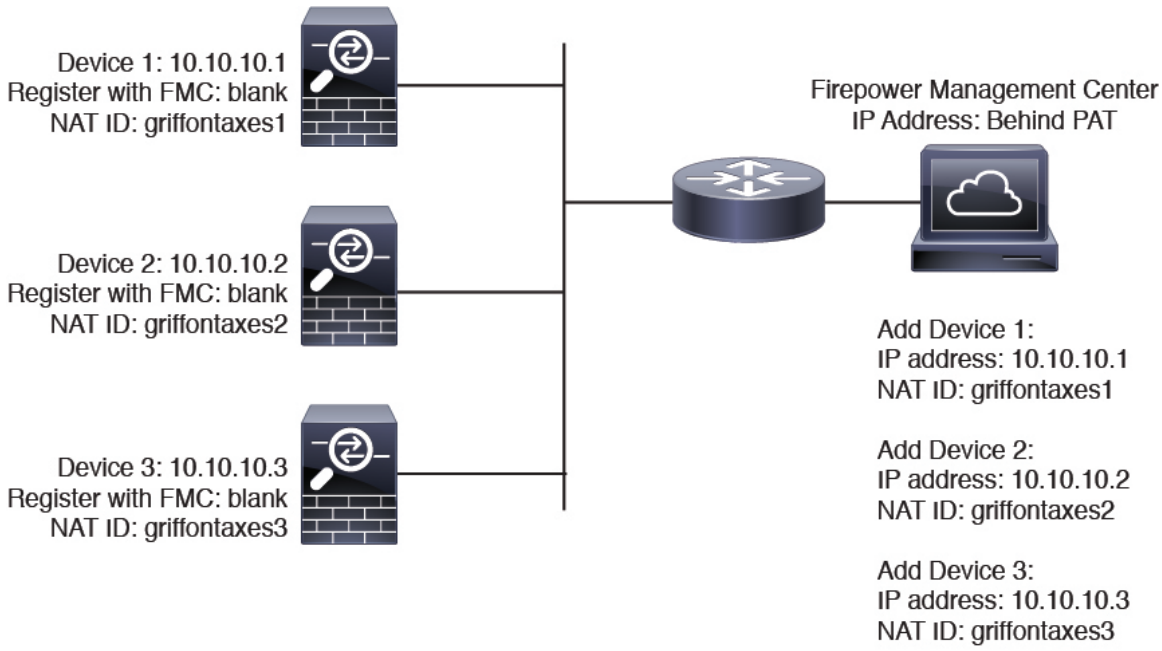
다음 예에서는 PAT IP 주소 뒤에 3개의 장치가 있음을 보여줍니다. 이 경우 FMC 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 디바이스에 FMC IP 주소를 지정하십시오.

그림 *41: PAT* 뒤의 관리되는 디바이스의 *NAT ID*



다음 예는 PAT ID 주소 뒤의 FMC을 보여줍니다. 이 경우 FMC 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 FMC에 디바이스 IP 주소를 지정하십시오.

그림 *42: PAT* 뒤의 *FMC*에 대한 *NAT ID*

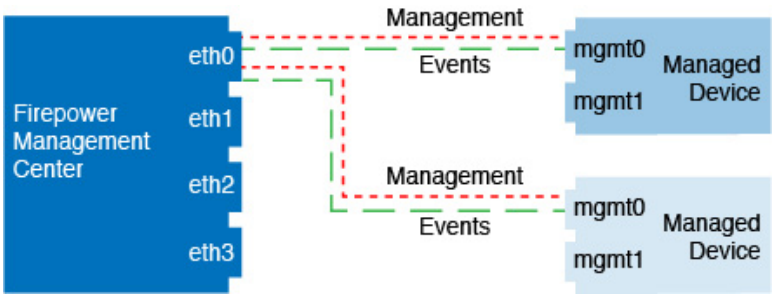


관리 및 이벤트 트래픽 채널 예시

참고 FTD에서 관리를 위해 데이터 인터페이스를 사용하는 경우 해당 디바이스에 대해 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다.

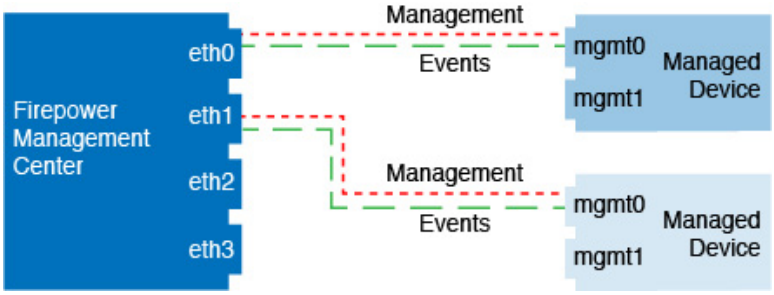
다음 예에서는 기본 관리 인터페이스만 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

그림 **43:** 단일 관리 인터페이스**: *Firepower Management Center***



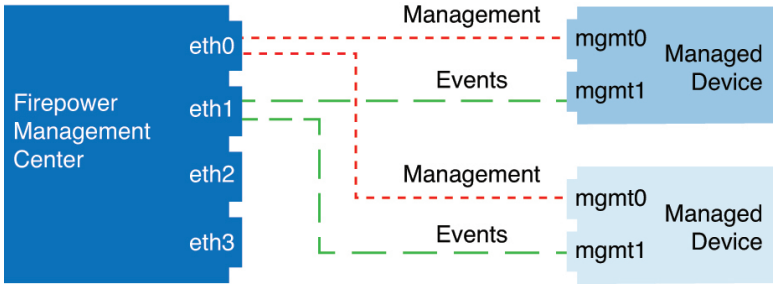
다음 예는 디바이스에 별도의 관리 인터페이스를 사용하는 Firepower Management Center를 보여 줍니다. 관리되는 각 디바이스는 1개의 관리 인터페이스를 사용합니다.

그림 **44:** 다중 관리 인터페이스**: *Firepower Management Center***



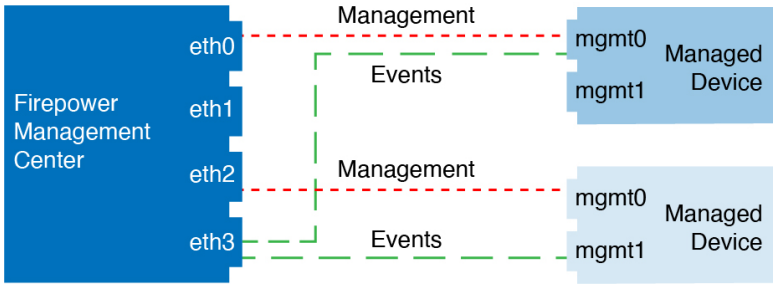
다음 예에서는 별도의 이벤트 인터페이스를 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

그림 ***45: Firepower Management Center*** 및 매니지드 디바이스에 대한 별도의 이벤트 인터페이스



다음 예는 별도의 이벤트 인터페이스를 사용하거나 단일 관리 인터페이스를 사용하는 Firepower Management Center 및 여러 매니지드 디바이스에 대한 다중 관리 인터페이스 및 별도의 이벤트 인터페이스를 보여 줍니다.

그림 *46:* 혼합 관리 및 이벤트 인터페이스 사용



FMC 관리 인터페이스 수정

Firepower Management Center에서 관리 인터페이스 설정을 수정합니다. 필요에 따라 추가 관리 인터페이스를 활성화하거나 이벤트 전용 인터페이스를 구성할 수 있습니다.

주의 연결된 관리 인터페이스를 변경할 때 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 FMC 콘솔 포트에 액세스하여 Linux 셸의 네트워크 설정을 다시 구성해야 합니다. 이 작업에 대한 안내를 받으려면 Cisco TAC에 문의해야 합니다.

참고 FMC IP 주소를 변경하는 경우, 디바이스에서 FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다., 351 페이지의 내용을 참조하십시오. FMC IP 주소 또는 호스트네임을 변경하는 경우, 설정이 일치하도록 디바이스 CLI의 값도 변경해야 합니다. 대부분 디바이스에서 FMC IP 주소 또는 호스트네임을 변경하지 않고 관리 연결이 다시 설정되지만, 적어도 FMC에 디바이스를 추가하고 NAT ID만 지정한 경우 연결을 다시 설정하려면 이 작업을 수행해야 합니다. 다른 경우에도 네트워크의 복원력을 높이려면 FMC IP 주소 또는 호스트네임을 최신 상태로 유지하는 것이 좋습니다.

참고 고가용성 설정에서 등록된 Firepower 디바이스의 관리 IP 주소를 디바이스 CLI 또는 Firepower Management Center에서 수정할 때 보조 Firepower Management Center는 HA 동기화 후에도 변경 내용을 반영하지 않습니다. 보조 Firepower Management Center도 업데이트되도록 하려면 두 Firepower Management Center 간에 역할을 전환하여 보조 Firepower Management Center를 활성 유닛으로 설정합니다. 현재 활성 Firepower Management Center의 Device Management(디바이스 관리) 페이지에 등록된 Firepower 디바이스의 관리 IP 주소를 수정합니다.

시작하기 전에

- 디바이스 관리의 작동 방식에 대한 자세한 내용은 디바이스 관리 인터페이스, 299 페이지의 내용을 참조하십시오.
- 프록시를 사용하는 경우:
  - NTLM(NT LAN Manager) 인증을 사용하는 프록시는 지원되지 않습니다.
  - 스마트 라이선스를 사용하거나 사용할 예정인 경우 프록시 FQDN은 64자를 초과할 수 없습니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을 선택한 다음 **Management Interface(**관리 인터페이스**)**를 선택합니다.

단계 **2** **Interfaces(**인터페이스**)** 영역에서 구성하려는 인터페이스 옆에 있는 **Edit(**편집**)**를 클릭합니다.

이 섹션에는 사용 가능한 모든 인터페이스가 나열되어 있습니다. 다른 인터페이스를 추가할 수 없습니다.

각 관리 인터페이스에서 다음 옵션을 구성할 수 있습니다.

- **Enabled(**활성화됨**)** - 관리 인터페이스를 활성화합니다. 기본 eth0 관리 인터페이스를 비활성화하지 마십시오. 일부 프로세스에는 eth0 인터페이스가 필요합니다.
- **Channels(**채널**)** - 이벤트 전용 인터페이스를 구성합니다. FMC에 하나의 이벤트 인터페이스만 구성할 수 있습니다. 이렇게 하려면 **Management Traffic(**관리 트래픽**)** 확인란을 선택 취소하고 **Event Traffic(**이벤트 트래픽**)** 확인란을 선택한 상태로 유지합니다. 관리 인터페이스에 대한 **Event Traffic(**이벤트 트래픽**)**을 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다. 인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.
- **Mode(**모드**)** - 연결 모드를 지정합니다. GigabitEthernet 인터페이스의 경우 자동 협상에 대한 변경 사항은 무시됩니다.
- **MDI/MDIX** - **Auto-MDIX**를 설정합니다.
- **MTU** - 최대 전송 단위(MTU)를 설정합니다. 기본값은 1500입니다. MTU 설정 가능 범위는 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

  시스템은 구성된 MTU 값에서 자동으로 18바이트를 잘라내므로 1298 아래의 값은 최소 IPv6 MTU 설정인 1280을 준수하지 못하며 594 아래의 값은 최소 IPv4 MTU 설정인 576을 준수하지 못합니다. 예를 들면 시스템은 구성된 값 576을 자동으로 558로 자릅니다.
- **IPv4 Configuration(IPv4** 구성**)** - IPv4 IP 주소를 설정합니다. 선택:
  - **Static(**정적**)** - 수동으로 **IPv4 Management IP(IPv4** 관리 **IP)** 주소 및 **IPv4 Netmask(IPv4** 넷마스크**)**를 입력합니다.

- **DHCP** - DHCP를 사용하도록 인터페이스를 설정합니다(eth0 전용).
- **Disabled(**비활성화됨**)** - IPv4를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.

- **IPv6 Configuration(IPv6** 구성**)** - IPv6 IP 주소를 설정합니다. 선택:
  - **Static(**정적**)** - 수동으로 **IPv6 Management IP(IPv6** 관리 **IP)** 주소 및 **IPv6 Prefix Length(IPv6** 프리픽스 길이**)**를 입력합니다.
  - **DHCP** - DHCPv6를 사용하도록 인터페이스를 설정합니다(eth0 전용).
  - **Router Assigned(**라우터 할당**)** - 상태 비저장 자동 구성을 활성화합니다.
  - **Disabled(**비활성화됨**)** - IPv6를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
  - **IPv6 DAD** - IPv6을 활성화할 때 DAD(Duplicate Address Detection)를 활성화 또는 비활성화합니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다.

단계 **3** **Routes(**경로**)** 영역에서 수정( )을 클릭하여 정적 경로를 편집하거나 추가( )를 클릭하여 경로를 추가합니다.

을 클릭하여 경로 테이블을 확인합니다.

각 추가 인터페이스가 원격 네트워크에 도달할 수 있는 정적 경로가 필요합니다. 새 경로가 필요한 시점에 대한 자세한 내용은 FMC 관리 인터페이스의 네트워크 라우트, 1354 페이지 섹션을 참조하십시오.

참고 기본 경로의 경우 게이트웨이 IP 주소만 변경할 수 있습니다. 기본 경로는 항상 eth0 인터페이스를 사용합니다.

정적 경로에 대해 다음 설정을 구성할 수 있습니다.

- **Destination(**대상**)** - 경로를 생성할 네트워크의 대상 주소를 설정합니다.
- **Netmask(**넷마스크**)** 또는 **Prefix Length(**프리픽스 길이**)** - 네트워크의 넷마스크(IPv4) 또는 프리픽스 길이(IPv6)를 설정합니다.
- **Interface(**인터페이스**)** - 이그레스 관리 인터페이스를 설정합니다.
- **Gateway(**게이트웨이**)** - 게이트웨이 IP 주소를 설정합니다.

단계 **4** **Shared Settings(**공유 설정**)** 영역의 모든 인터페이스에서 공유하는 네트워크 파라미터를 설정합니다.

참고 eth0 인터페이스에 **DHCP**를 선택한 경우 DHCP 서버에서 파생된 일부 공유 설정을 수동으로 지정할 수 없습니다.

다음 공유 설정을 구성할 수 있습니다.

- **Hostname(**호스트네임**)** - FMC 호스트네임을 설정합니다. 호스트 이름은 문자 또는 숫자로 시작하고 끝나야 하며 문자, 숫자 또는 하이픈만 사용할 수 있습니다. 호스트네임을 변경하는 경우 새 호스트네임을 시스템 로그 메시지에 반영하려면 FMC를 리부팅합니다. 시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.
- **Domains(**도메인**)** - FMC에 대한 검색 도메인을 쉼표로 구분하여 설정합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.
- **Primary DNS Server(**기본 **DNS** 서버**)**, **Secondary DNS Server(**보조 **DNS** 서버**)Tertiary DNS Server(3**차 **DNS** 서버**)** - 환경설정 순서대로 사용할 DNS 서버를 설정합니다.
- **Remote Management Port(**원격 관리 포트**)** - 매니지드 디바이스와의 통신을 위한 원격 관리 포트를 설정합니다. FMC 및 매니지드 디바이스는 기본적으로 포트 8305에 있는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

  참고 Cisco에서는 원격 관리 포트에 대해 기본 설정을 유지할 것을 적극 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 디바이스의 설정을 변경해야 합니다.

단계 **5** **ICMPv6** 영역에서 ICMPv6 설정을 구성합니다.

- **Allow Sending Echo Reply Packets(**에코 응답 패킷 전송 허용**)** - 에코 응답 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 FMC 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.
- **Allow Sending Destination Unreachable Packets(**대상에 연결할 수 없는 패킷 전송 허용**)** - 대상에 연결할 수 없는 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다.

단계 **6** **Proxy(**프록시**)** 영역에서 HTTP 프록시 설정을 구성합니다.

FMC는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다.

이 주제의 사전 요구 사항에서 프록시 요구 사항을 참조하십시오.

a) **Enable(**활성화**)** 확인란을 선택합니다.
b) 프록시 서버의 IP 주소 또는 정규화된 도메인 이름을 **HTTP Proxy(HTTP** 프록시**)** 필드에 입력합니다.

   이 주제의 사전 요구 사항에서 해당 요구 사항을 참조하십시오.

c) **Port(**포트**)** 필드에서 포트 번호를 입력합니다.
d) **Use Proxy Authentication(**프록시 인증 사용**)**을 선택하여 인증 자격 증명을 제공하고 **User Name(**사용자 이름**)** 및 **Password(**비밀번호**)**를 제공합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** FMC IP 주소를 변경하는 경우, 'FMC IP 주소를 변경하는 경우'와 디바이스에서 FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다., 351 페이지의 내용을 참조하십시오.

FMC IP 주소 또는 호스트네임을 변경하는 경우, 설정이 일치하도록 디바이스 CLI의 값도 변경해야 합니다. 대부분 디바이스에서 FMC IP 주소 또는 호스트네임을 변경하지 않고 관리 연결이 다시 설정되지만, 적어도 FMC에 디바이스를 추가하고 NAT ID만 지정한 경우 연결을 다시 설정하려면 이 작업을 수행해야 합니다. 다른 경우에도 네트워크의 복원력을 높이려면 FMC IP 주소 또는 호스트네임을 최신 상태로 유지하는 것이 좋습니다

종료 또는 재시작

웹 인터페이스를 사용하여 FMC의 프로세스 종료 및 재시작을 제어합니다. 다음 작업을 수행할 수 있습니다.

- 종료: 어플라이언스의 정상 종료를 시작합니다.

  주의 전원 버튼을 사용하여 Firepower 어플라이언스를 종료하지 마십시오. 데이터가 손실될 수 있습니다. 웹 인터페이스(또는 CLI)를 사용하여 구성 데이터 손실 없이 시스템의 전원을 안전하게 끄고 재시작할 수 있도록 준비합니다.

- 재부팅: 종료한 다음 정상적으로 재시작합니다.
- 콘솔 재시작: 통신, 데이터베이스 및 HTTP 서버 프로세스를 다시 시작합니다. 이는 일반적으로 문제 해결 중에 사용됩니다.

팁 Snort 프로세스 재시작을 포함한 7000/8000 시리즈 디바이스 종료/재시작 관련 정보는 7000/8000 시리즈 디바이스 종료 또는 재시작, 1421 페이지 섹션을 참조하십시오. 가상 디바이스의 경우에는 가상 플랫폼 설명서를 참조하십시오. 특히 VMware의 경우 사용자 지정 전원 옵션을 VMware 도구로 제공합니다.

FMC를 종료하거나 재시작합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Process(**프로세스**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

종료	**Shutdown Management Center(Management Center** 종료**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다.
재부팅	**Reboot Management Center(Management Center** 재부팅**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 참고 리부팅하면 로그아웃되며, 완료하는 데 최대 1시간이 소요될 수 있는 데이터베이스 검사가 실행됩니다.
콘솔 재시작	**Restart Management Center Console(Management Center** 콘솔 재시작**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 참고 재시작하면 삭제된 호스트가 네트워크 맵에 다시 나타날 수 있습니다.

관련 항목

Snort® 재시작 시나리오, 505 페이지

원격 스토리지 관리

Firepower Management Center에서 백업 및 보고를 위해 로컬 또는 원격 스토리지 다음을 사용할 수 있습니다.

- NFS(Network File System)
- Server Message Block (SMB)/Common Internet File System (CIFS)
- SSH(Secure Shell)

백업은 한 원격 시스템으로 전송하고 보고서는 다른 원격 시스템으로 전송할 수는 없습니다. 그러나 둘 중 하나는 원격 시스템으로 전송하고 나머지는 Firepower Management Center에 저장할 수는 있습니다.

팁 원격 스토리지를 구성 및 선택한 경우, 오직 연결 데이터베이스 한도를 높이지 않은 경우에만 로컬 스토리지로 다시 전환할 수 있습니다.

로컬 스토리지 설정

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Remote Storage Device(**원격 스토리지 디바이스**)**를 선택합니다.

단계 **3** **Storage Type(**스토리지 유형**)** 드롭다운 목록에서 **Local (No Remote Storage)(**로컬**(**원격 스토리지 아님**))**을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

원격 스토리지에 대한 **NFS** 설정

시작하기 전에

- 외부 원격 스토리지 시스템이 정상적으로 작동하는지와 FMC에서 액세스할 수 있는지를 확인합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Remote Storage Device(**원격 스토리지 디바이스**)**를 클릭합니다.

단계 **3** **Storage Type(**스토리지 유형**)** 드롭다운 목록에서 **NFS**를 선택합니다.

단계 **4** 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host(**호스트**)** 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory(**디렉터리**)** 필드에 입력합니다.

단계 **5** 선택적으로 **Use Advanced Options(**고급 옵션 사용**)** 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. 원격 스토리지 관리 고급 옵션, 1366 페이지 섹션을 참조하십시오.

단계 **6** **System Usage(**시스템 사용**)**에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups(**백업용으로 사용**)**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports(**보고서용으로 사용**)**를 선택합니다.
- 원격 스토리지용 백업에 대해 **Disk Space Threshold**를 입력합니다. 기본값은 90%입니다.

단계 **7** 설정을 테스트하려면 **Test(**테스트**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

원격 스토리지에 대한 SMB 설정

시작하기 전에

외부 원격 스토리지 시스템이 정상적으로 작동하는지 그리고 FMC에서 액세스할 수 있는지를 확인합니다.

- 시스템에서는 전체 파일 경로가 아니라 상위 레벨의 공유만 인식합니다. 사용하려는 정확한 디렉토리를 공유하려면 Windows를 사용해야 합니다.
- FMC에서 SMB 공유에 액세스하는 데 사용할 Windows 사용자에게 공유 위치에 대한 소유권과 읽기/변경 액세스 권한이 있는지 확인합니다.
- 보안을 유지하려면 SMB 2.0 이상을 설치해야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Remote Storage Device(**원격 스토리지 디바이스**)**를 클릭합니다.

단계 **3** **Storage Type(**스토리지 유형**)** 드롭다운 목록에서 **SMB**를 선택합니다.

단계 **4** 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host(**호스트**)** 필드에 입력합니다.
- 스토리지 영역의 공유를 **Share(**공유**)** 필드에 입력합니다.
- 선택적으로, 원격 스토리지 시스템의 도메인 이름을 **Domain(**도메인**)** 필드에 입력합니다.
- **Username(**사용자 이름**)** 필드에 스토리지 시스템의 사용자 이름을 입력하고 **Password(**비밀번호**)** 필드에 해당 사용자의 비밀번호를 입력합니다.

단계 **5** 선택적으로 **Use Advanced Options(**고급 옵션 사용**)** 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. 원격 스토리지 관리 고급 옵션, 1366 페이지 섹션을 참조하십시오.

단계 **6** **System Usage(**시스템 사용**)**에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups(**백업용으로 사용**)**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports(**보고서용으로 사용**)**를 선택합니다.

단계 **7** 설정을 테스트하려면 **Test(**테스트**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

원격 스토리지에 대한 SSH 설정

주의 어플라이언스에서 STIG 규정 준수를 활성화한 경우 해당 어플라이언스의 원격 스토리지에 SSH를 사용할 수 없습니다.

시작하기 전에

- 외부 원격 스토리지 시스템이 정상적으로 작동하는지와 Firepower Management Center에서 액세스할 수 있는지를 확인합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Remote Storage Device(**원격 스토리지 디바이스**)**를 클릭합니다.

단계 **3** **Storage Type(**스토리지 유형**)** 드롭다운 목록에서 **SSH**를 선택합니다.

단계 **4** 연결 정보를 추가합니다.

- 스토리지 시스템의 IP 주소 또는 호스트네임을 **Host(**호스트**)** 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory(**디렉터리**)** 필드에 입력합니다.
- **Username(**사용자 이름**)** 필드에 스토리지 시스템의 사용자 이름을 입력하고 **Password(**비밀번호**)** 필드에 해당 사용자의 비밀번호를 입력합니다. 연결 사용자 이름의 일부로 네트워크 도메인을 지정하려면 사용자 이름 앞에 슬래시(/)가 오는 도메인을 지정합니다.
- SSH 키를 사용하려면 **SSH Public Key** 필드의 내용을 복사하여 authorized_keys 파일에 붙여넣습니다.

단계 **5** 선택적으로 **Use Advanced Options(**고급 옵션 사용**)** 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. 원격 스토리지 관리 고급 옵션, 1366 페이지 섹션을 참조하십시오.

단계 **6** System Usage(시스템 사용)에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups(**백업용으로 사용**)**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports(**보고서용으로 사용**)**를 선택합니다.

단계 **7** 설정을 테스트하려면 **Test(**테스트**)**를 클릭해야 합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

원격 스토리지 관리 고급 옵션

SFMB(보안 파일 전송 프로토콜)를 사용하여 보고서 및 백업을 저장하기 위해 NFS(Network File System) 프로토콜, SMB(Server Message Block) 프로토콜 또는 SSH를 선택하는 경우 **Use Advanced Options(**고

급 옵션 사용**)** 확인란을 선택하여 NFS, SMB 또는 SSH 마운트 매뉴얼 페이지에 설명된 마운트 바이너리 옵션 중 하나를 사용할 수 있습니다

SMB를 선택할 경우 다음 형식을 사용하여 **Command Line Options(**명령줄 옵션**)** 필드에서 보안 모드를 입력할 수 있습니다.

`sec=mode`

여기서 `mode`는 원격 스토리지에 사용할 보안 모드입니다.

표 ***90: SMB*** 보안 모드 설정

모드	설명
[없음]	Null 사용자(이름 없음)로서 연결을 시도합니다.
`krb5`	Kerberos 버전 5 인증을 사용합니다.
`krb5i`	Kerberos 인증 및 패킷 서명을 사용합니다.
`ntlm`	NTLM 비밀번호 해싱을 사용합니다. (기본값)
`ntlmi`	서명과 함께 NTLM 비밀번호 해싱을 사용합니다 (서버에서 서명을 요구하는 경우 `/proc/fs/cifs/PacketSigningEnabled`가 On이면 기본값).
`ntlmv2`	NTLMv2 비밀번호 해싱을 사용합니다.
`ntlmv2i`	패킷 서명과 함께 NTLMv2 비밀번호 해싱을 사용합니다.

검증 번경

사용자가 변경하는 내용을 모니터링하고 그러한 변경이 회사의 기본 표준을 따르는지 확인하려면 지난 24시간 동안 변경 사항의 자세한 보고서를 이메일로 전송하도록 시스템을 구성할 수 있습니다. 사용자가 시스템 구성에 변경 사항을 저장할 때마다 변경에 대한 스냅샷이 생성됩니다. 변경 조정 보고서는 이러한 스냅샷의 정보를 결합하여 최신 시스템 변경 사항에 대한 명확한 요약을 제공합니다.

다음 샘플 그림에는 예제 변경 조정 보고서의 User 페이지가 표시되며, 각 구성의 이전 값과 변경 이후의 값이 모두 나열되어 있습니다. 여러 사용자가 동일한 구성을 여러 번 변경하면 보고서에는 최근 것부터 시간순으로 각 변경 사항의 요약이 나열됩니다.

지난 24시간 동안 변경된 내용을 볼 수 있습니다.

검증 변경 구성

시작하기 전에

- 이메일 서버가 24시간 동안 시스템 변경 사항에 대한 이메일 보고서를 수신하도록 구성합니다. 자세한 내용은 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Change Reconciliation(**검증 변경**)**을 클릭합니다.

단계 **3** **Enable(**사용**)** 확인란을 선택합니다.

단계 **4** 시스템에서 변경 검증 보고서를 전송하도록 할 시간을 **Time to Run(**실행 시간**)** 드롭다운 목록에서 선택합니다.

단계 **5** **Email to(**수신자**)** 필드에 이메일 주소를 입력합니다.

팁 이메일 주소를 추가한 후 **Resend Last Report(**마지막 보고서 다시 보내기**)**를 클릭하여 받는 사람에게 최신 변경 검증 보고서 사본을 전송합니다.

단계 **6** 정책 변경 사항을 포함하려면 **Include Policy Configuration(**정책 구성 포함**)** 확인란을 선택합니다.

단계 **7** 지난 24시간 동안 모든 변경 사항을 포함하려는 경우 **Show Full Change History(**전체 변경 기록 표시**)** 확인란을 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

감사 로그를 사용하여 변경 검사, 454 페이지

검증 변경 옵션

Include Policy Configuration(정책 구성 포함**)** 옵션은 시스템에 정책 변경 기록이 변경 검증 보고서에 포함되는지 여부를 제어합니다. 여기에는 액세스 제어, 침입, 시스템, 상태 및 네트워크 검색 정책에 대한 변경 사항이 포함됩니다. 이 옵션을 선택하지 않으면 정책에 대한 변경 사항이 보고서에 표시되지 않습니다. 이 옵션은 Firepower Management Center에서만 사용할 수 있습니다.

Show Full Change History(전체 변경 기록 표시**)** 옵션은 시스템이 변경 검증 보고서에 지난 24시간 동안 발생한 모든 변경 사항의 기록을 포함할지 여부를 제어합니다. 이 옵션을 선택하지 않으면 보고서에는 각 카테고리에 대한 변경 사항의 통합된 보기만 포함됩니다.

참고 변경 조정 보고서에는 Firepower Threat Defense 인터페이스 및 라우팅 설정에 대한 변경 사항이 포함되지 않습니다.

정책 변경 코멘트

사용자가 액세스 제어, 침입 또는 네트워크 분석 정책을 수정할 때 코멘트 기능을 사용하여 여러 정책 관련 변경 사항을 추적하도록 Firepower 시스템을 구성할 수 있습니다.

정책 변경 코멘트를 활성화하면 관리자는 배포의 중요한 정책이 수정된 이유를 신속하게 평가할 수 있습니다. 선택적으로 감사 로그에 작성된 침입 및 네트워크 분석 정책을 변경할 수 있습니다.

정책 변경 추적 코멘트 구성

액세스 제어 정책, 침입 정책 또는 네트워크 분석 정책을 수정할 때 사용자에게 코멘트를 요구하도록 Firepower 시스템을 구성할 수 있습니다. 코멘트를 사용하여 사용자가 정책을 변경한 이유를 추적할 수 있습니다. 정책 변경에 대한 코멘트를 활성화하는 경우, 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 정책에 대한 새로운 변경 사항이 저장될 때마다 시스템은 사용자에게 코멘트를 입력하라는 메시지를 표시합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

왼쪽된 탐색 패널에서 시스템 구성 옵션이 나타납니다.

단계 **2** 다음 중 하나에 대한 정책 설명 환경설정을 구성합니다.

- 액세스 제어 정책에 대한 설명 환경설정을 보려면 **Access Control Preferences(**액세스 제어 환경설정**)**를 클릭합니다.
- 침입 정책에 대한 설명 환경설정을 보려면 **Intrusion Policy Preferences(**침입 정책 환경설정**)**를 클릭합니다.
- 네트워크 분석 정책에 대한 설명 환경설정을 보려면 **Network Analysis Policy Preferences(**네트워크 분석 정책 환경설정**)**를 클릭합니다.

단계 **3** 각 정책 유형에 대해 다음과 같은 옵션을 선택할 수 있습니다.

- **Disabled(**비활성화**)** - 변경 코멘트를 비활성화합니다.
- **Optional(**선택 사항**)** - 코멘트에서 변경 사항을 설명할 수 있는 옵션을 사용자에게 제공합니다.
- **Required(**필수**)** - 사용자는 저장 전에 코멘트에서 변경 사항을 설명해야 합니다.

단계 **4** 선택적 침입 또는 네트워크 분석 정책 코멘트:

- 모든 침입 정책 변경 사항을 감사 로그에 기록하려면 **Write changes in Intrusion Policy to audit log(**침입 정책의 변경 사항을 감사 로그에 쓰기**)**를 선택합니다.
- 모든 네트워크 분석 정책 변경 사항을 감사 로그에 기록하려면 **Write changes in Network Analysis Policy to audit log(**네트워크 분석 정책의 변경 사항을 감사 로그에 쓰기**)**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

액세스 목록

IP 주소 및 포트를 기준으로 FMC에 대한 액세스를 제한할 수 있습니다. 기본적으로 모든 IP 주소에 대해 다음과 같은 포트가 활성화됩니다.

- 웹 인터페이스 액세스용 443(HTTPS)
- CLI 액세스용 22(SSH)

포트 161을 통해 SNMP 정보를 폴링할 수 있는 액세스 권한을 추가할 수도 있습니다. SNMP는 기본적으로 비활성화되며, 따라서 먼저 SNMP를 활성화해야 SNMP 액세스 규칙을 추가할 수 있습니다. 자세한 내용은 SNMP 폴링 구성, 1377 페이지의 내용을 참고하십시오.

주의 기본적으로 액세스는 제한되지 않습니다. 더 안전한 환경에서 작동하려면 특정 IP 주소의 액세스를 추가한 후 기본 **any** 옵션을 삭제하는 것을 고려하십시오.

액세스 목록 구성

이 액세스 목록은 외부 데이터베이스 액세스를 제어하지 않습니다. 데이터베이스에 대한 외부 액세스 활성화, 1350 페이지의 내용을 참조하십시오.

주의 FMC에 연결하기 위해 현재 사용 중인 IP 주소에 대한 액세스를 삭제하면, '`IP=any port=443`'에 대한 항목은 존재하지 않으며, 저장할 때 액세스 권한을 잃게 됩니다.

클래식 디바이스에 액세스 목록을 구성하려면, 디바이스 플랫폼 설정을 사용합니다. 클래식 디바이스에 대한 액세스 목록 구성, 1407 페이지의 내용을 참조하십시오.

시작하기 전에

기본적으로 액세스 목록에는 HTTPS 및 SSH에 대한 규칙이 포함됩니다. SNMP 규칙을 액세스 목록에 추가하려면 먼저 SNMP를 활성화해야 합니다. 자세한 내용은 SNMP 폴링 구성, 1377 페이지를 참고하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** (선택 사항) SNMP 규칙을 액세스 목록에 추가하려면 **SNMP**를 클릭해 SNMP를 구성합니다. 기본적으로 SNMP는 비활성화되어 있습니다. 자세한 내용은 SNMP 폴링 구성, 1377 페이지을 참조하십시오.

단계 **3** 액세스 목록을 클릭합니다.

단계 **4** 하나 이상의 IP 주소에 대한 액세스를 추가하려면 **Add Rules(**규칙 추가**)**를 클릭합니다.

단계 **5** **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 모두를 입력하세요.

단계 **6** **SSH**, **HTTPS**, **SNMP** 또는 이 옵션의 조합을 선택하여 이 IP 주소에 활성화할 포트를 지정합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

감사 로그

Firepower Management Center는 사용자 활동을 읽기 전용 감사 로그로 기록합니다. 여러 가지 방법으로 감사 로그 데이터를 검토할 수 있습니다.

- 웹 인터페이스인 시스템 감사, 449 페이지를 사용합니다.

  감사 로그는 감사 보기의 항목을 기준으로 감사 로그 메시지를 보고, 정렬하고, 필터링할 수 있는 표준 이벤트 보기에서 제공됩니다. 감사 정보를 손쉽게 삭제하고 보고할 수 있으며, 사용자가 변경한 내용에 대한 자세한 보고서를 볼 수 있습니다.

- 시스템 로그.

- HTTP 서버인에 감사 로그 메시지를 스트리밍합니다.

외부 서버로 감사 로그 메시지를 스트리밍하면 FMC의 공간을 절약할 수 있습니다. 감사 로그 스트리밍 구성, 1371 페이지 섹션을 참조하십시오.

여러 시스템 로그 서버로 스트리밍

감사 로그 데이터를 최대 5개의 시스템 로그 서버로 스트리밍할 수 있습니다. 그러나 보안 감사 로그 스트리밍에 대해 TLS를 활성화한 경우, 단일 시스템 로그 서버로만 스트리밍할 수 있습니다.

또한 클래식 디바이스의 감사 로그를 유지합니다. 클래식 디바이스에서 감사 로그를 스트리밍하는 방법은 클래식 디바이스에서의 감사 로그 스트리밍, 1408 페이지 섹션을 참조하십시오.

감사 로그 스트리밍 구성

다음은 출력 구조의 예입니다.

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

로컬 날짜, 시간 및 호스트 이름이 괄호로 묶인 선택적 태그 앞에 오는 경우, 그리고 발신 디바이스 이름이 감사 로그 메시지 앞에 오는 경우

예를 들면 다음과 같습니다.

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3500: admin@10.1.1.2, Operations > Monitoring, Page
View
```

시작하기 전에

- 외부 호스트가 작동해야 하며 감사 로그를 보내는 시스템에서 액세스할 수 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Audit Log(**로그 감사**)**를 클릭합니다.

단계 **3** **Enabled(**활성화**)**를 **Send Audit Log to Syslog(**감사 로그를 시스템 로그로 전송**)** 드롭다운 메뉴에서 선택합니다.

단계 **4** IP 주소를 사용하여 감사 정보에 대한 대상 호스트를 지정하거나 **Host(**호스트**)** 필드에 호스트의 FQDN(Fully Qualified Domain Name)을 지정합니다. 기본 포트(514)가 사용됩니다.

주의 감사 로그를 수신하도록 구성한 컴퓨터가 원격 메시지를 수락하도록 설정되지 않은 경우, 호스트에서 감사 로그를 허용하지 않습니다.

단계 **5** 시스템 로그 **Facility(**시설**)**를 선택합니다.

단계 **6** **Severity(**심각도**)**를 선택합니다.

단계 **7** 또는, **Tag(**태그**)**(선택 사항) 필드에 참조 태그를 삽입합니다.

단계 **8** 외부 HTTP 서버에 정기 감사 로그 업데이트를 전송하려면 **Enabled(**활성화**)**를 **Send Audit Log to HTTP Server(HTTP** 서버에 감사 로그 전송**)** 드롭다운 메뉴에서 선택합니다.

단계 **9** **URL to Post Audit(**사후 감사 **URL)** 필드에서 감사 정보를 전송할 URL을 지정합니다. 다음과 같이 나열된 대로 HPPT POST 변수를 기대하는 listener 프로그램에 해당하는 URL을 입력해야 합니다.

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- `result`
- 시간
- `tag`(위와 같이 정의된 경우)

주의 암호화된 게시물을 허용하려면, HTTPS URL을 사용해야 합니다. 외부 URL에 감사 정보를 보내면 시스템 성능에 영향을 미칠 수 있음에 유의하십시오.

단계 **10** **Save(**저장**)**를 클릭합니다.

대시보드 설정

대시보드는 Firepower System의 여러 부분에 대한 통찰력을 제공하는 소규모의 자족적 구성 요소인 위젯을 사용하여 현재 시스템 상태에 대한 간략한 보기를 제공합니다. Firepower System은 여러 대시보드 위젯이 사전 정의된 상태로 제공됩니다.

맞춤형 분석 위젯이 대시보드에서 활성화되도록 Firepower Management Center를 구성할 수 있습니다.

관련 항목

대시보드 정보, 363 페이지

대시보드에 대한 맞춤형 분석 위젯 활성화

맞춤형 분석 대시보드 위젯을 사용하여 유연하고 사용자가 구성할 수 있는 쿼리를 기반으로 이벤트를 시각적으로 표현할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Dashboard(**대시보드**)**를 클릭합니다.

단계 **3** 사용자가 Custom Analysis 위젯을 대시보드에 추가하도록 허용하려면 **Enable Custom Analysis Widgets(**맞춤형 분석 위젯 활성화**)** 확인란을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

DNS 캐시

이벤트 보기 페이지에서 자동으로 IP 주소를 확인하도록 시스템을 구성할 수 있습니다. 어플라이언스가 수행하는 DNS 캐싱의 기본 등록 정보를 구성할 수도 있습니다. DNS 캐싱을 구성하면 추가 조회를 수행하지 않고도 전에 확인한 IP 주소를 식별할 수 있습니다. 이렇게 하면 네트워크의 트래픽 양을 줄이고, IP 주소 확인이 활성화된 경우 이벤트 페이지의 표시 속도를 높일 수 있습니다.

DNS 캐시 속성 설정

DNS 확인 캐싱은 전에 확인된 DNS 조회의 캐싱을 허용하는 시스템 전체의 설정입니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **DNS Cache(DNS** 캐시**)**를 선택합니다.

단계 **3** **DNS Resolution Caching(DNS** 확인 캐싱**)** 드롭다운 목록에서 다음 중 하나를 선택합니다.

- **Enabled(**활성화**)** - 캐싱을 활성화합니다.
- **Disabled(**비활성화**)** - 캐싱을 비활성화합니다.

단계 **4** DNS 항목이 제거되어 비활성화되기 전 메모리에 캐시되어 머무는 시간(분)을 **DNS Cache Timeout (in minutes)** 필드에 입력합니다.

기본 설정은 300분(5시간)입니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관련 항목

이벤트 보기 구성, 41 페이지

이메일 공지

다음을 수행하려는 경우 메일 호스트를 구성합니다.

- 이벤트 기반 보고서 이메일 전송
- 예약 작업에 대한 상태 보고서 이메일 전송
- 변경 검증 보고서 이메일 전송
- 데이터 정리 알림 이메일 전송
- 검색 이벤트, 영향 플래그, 상관 이벤트 알림, 침입 이벤트 알림 및 상태 이벤트 알림에 이메일 사용

이메일 알림을 구성할 때 시스템과 메일 릴레이 호스트 간 통신을 위한 암호화 방법을 선택할 수 있고 필요한 경우 메일 서버의 인증 자격 증명을 제공할 수 있습니다. 구성한 후 연결을 테스트할 수 있습니다.

메일 릴레이 호스트 및 알림 주소 구성

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을 선택합니다.

단계 **2** **Email Notification(**이메일 알림**)**을 클릭합니다.

단계 **3** **Mail Relay Host(**메일 릴레이 호스트**)** 필드에서 사용할 메일 서버의 호스트 이름 또는 IP 주소를 입력합니다. 입력한 메일 호스트는 어플라이언스의 액세스를 허용해야 합니다.

단계 **4** **Port Number(**포트 번호**)** 필드에 이메일 서버에서 사용할 포트 번호를 입력합니다.

일반적인 포트는 다음과 같습니다.

- 25: 암호화를 사용하지 않는 경우
- 465: SSLv3를 사용하는 경우
- 587: TLS를 사용하는 경우

단계 **5** **Encryption(**암호화**)** 방법을 선택합니다.

- **TLS**-전송 계층 보안을 사용하여 통신을 암호화합니다
- **SSLv3**-Secure Socket Layer을 사용 하 여 통신을 암호화 합니다.
- **None (**없음**)**-암호화 되지 않은 통신을 허용 합니다.

참고 Certificate validation is not required for encrypted communication between the appliance and mail server.

단계 **6** In the **From Address** field, enter the valid email address you want to use as the source email address for messages sent by the appliance.

단계 **7** Optionally, to supply a user name and password when connecting to the mail server, choose **Use Authentication**. **Username(**사용자 이름**)** 필드에 사용자 이름을 입력합니다. **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다.

단계 **8** 구성된 메일 서버를 사용하는 테스트 이메일을 전송하려면 **Test Mail Server Settings(**메일 서버 설정 테스트**)**를 클릭합니다.

테스트의 성공 또는 실패를 나타내는 메시지가 버튼 옆에 나타납니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

언어 선택

웹 인터페이스에 대해 다른 언어를 지정하려면 Language 페이지를 사용할 수 있습니다.

웹 인터페이스의 언어 설정

여기서 지정하는 언어는 모든 사용자에 대한 웹 인터페이스에 사용됩니다. 다음 항목을 선택할 수 있습니다.

- 영어
- 일본어

7000/8000 시리즈 디바이스의 언어를 설정하려면 디바이스 플랫폼 설정인 7000/8000 시리즈 웹 인터페이스 언어 설정, 1412 페이지을(를) 사용합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Language**를 클릭합니다.

단계 **3** 사용하려는 언어를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

로그인 배너

Login Banner(로그인 배너) 페이지를 사용하여 보안 어플라이언스 또는 공유 정책에 대한 세션, 로그인 또는 사용자 정의 메시지 배너를 지정할 수 있습니다.

ASCII 문자와 캐리지 리턴을 사용하여 사용자 정의 로그인 배너를 만들 수 있습니다. 시스템은 탭 간격을 유지하지 않습니다. 로그인 배너가 너무 크거나 오류가 발생하면 시스템에서 배너를 표시하려고 시도할 때 텔넷 또는 SSH 세션이 실패할 수 있습니다.

로그인 배너 사용자 지정

클래식 디바이스의 로그인 배너를 사용자 정의하려면, 디바이스 플랫폼 설정을 사용합니다. 클래식 디바이스에 대한 로그인 배너 맞춤 설정 , 1412 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Login Banner(**로그인 배너**)**를 선택합니다.

단계 **3** **Custom Login Banner(**사용자 정의 로그인 배너_ 필드에서 사용하려는 로그인 배너 텍스트를 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

SNMP 폴링

SNMP(Simple Network Management Protocol) 폴링을 활성화할 수 있습니다. 이 기능은 SNMP 프로토콜의 1, 2, 3 버전 사용을 지원합니다. 이 기능을 이용하면 연락처, 관리, 위치, 서비스 정보, IP 주소 지정 및 라우팅 정보, 전송 프로토콜 사용 통계 등의 시스템 세부사항을 포함하는 표준 MIB(management information base)에 액세스할 수 있습니다.

참고 SNMP 프로토콜을 위한 SNMP 버전을 선택하는 경우, SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3는 읽기 전용 사용자만 지원한다는 사실을 유념하십시오. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

SNMP 폴링을 활성화한다고 해서 시스템에서 SNMP 트랩을 전송하지는 않습니다. MIB의 정보를 네트워크 관리 시스템을 통한 폴링에 사용할 수 있도록 지원할 뿐입니다.

SNMP 폴링 구성

클래식 매니지드 디바이스에서 SNMP 폴링을 구성하려면, 디바이스 플랫폼 설정을 사용합니다. 클래식 디바이스에서의 SNMP 폴링 구성, 1415 페이지의 내용을 참조하십시오.

시작하기 전에

시스템 폴링에 사용할 각 컴퓨터에 대해 SNMP 액세스를 추가합니다. 액세스 목록 구성, 1370 페이지의 내용을 참조하십시오.

참고 SNMP MIB에는 구축을 공격하는 데 사용할 수 있는 정보가 있습니다. Cisco에서는 MIB를 폴링하는 데 사용하는 특정 호스트에 대한 SNMP 액세스용 액세스 목록을 제한할 것을 권장합니다. 또한 SNMPv3을 사용하고 네트워크 관리 액세스에 강력한 비밀번호를 사용할 것도 권장합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **SNMP**를 클릭합니다.

단계 **3** **SNMP Version(SNMP** 버전**)** 드롭다운 목록에서, 사용할 SNMP 버전을 선택합니다.

- **Version(**버전**) 1** 또는 **Version(**버전**) 2**: 커뮤니티 문자열 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뜁니다.

  참고 SNMP 커뮤니티 문자열 이름에는 특수문자(< > / % # & ? ', 등)를 포함하지 않습니다.

- **Version 3(**버전 **3)**: **Add User(**사용자 추가**)**를 클릭하여 사용자 정의 페이지를 표시합니다. SNMPv3는 읽기 전용 사용자 및 AES128 암호화만 지원합니다.

단계 **4** 사용자 이름을 입력합니다.

단계 **5** **Authentication Protocol(**인증 프로토콜**)** 드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.

단계 **6** **Authentication Password(**인증 비밀번호**)** 필드에 SNMP 서버와 함께 인증에 필요한 비밀번호를 입력합니다.

단계 **7** **Verify Password(**비밀번호 확인**)** 필드에 인증 비밀번호를 다시 입력합니다.

단계 **8** 사용할 비공개 프로토콜을 **Privacy Protocol** 목록에서 선택하거나, 비공개 프로토콜을 사용하지 않으려면 **None**을 선택합니다.

단계 **9** **Privacy Password(**프라이버시 비밀번호**)** 필드에 SNMP 서버에 필요한 SNMP 프라이버시 키를 입력합니다.

단계 **10** **Verify Password(**비밀번호 확인**)** 필드에 프라이버시 비밀번호를 다시 입력합니다.

단계 **11** **Add(**추가**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

STIG 컴플라이언스

미국 연방 정부 내 기구는 경우에 따라 Security Technical Implementation Guides(보안 기술 구현 가이드, STIG)에 정리된 일련의 보안 검사 목록을 준수해야 합니다. Firepower는 미국 국방부가 수립한 STIG 요구 사항을 준수하도록 지원합니다.

구축의 어플라이언스에서 STIG 컴플라이언스를 활성화하는 경우 모든 어플라이언스에서 활성화해야 합니다. 비준수 매니지드 디바이스는 STIG 준수 Firepower Management Center에 등록할 수 없으며 STIG 준수 디바이스는 비준수 FMC에 등록할 수 없습니다.

STIG 규정 준수를 활성화해도 적용 가능한 모든 STIG에 대한 엄격한 규정 준수가 보장되지는 않습니다.

STIG 규정 준수를 활성화할 경우, 로컬 셸 액세스 계정의 비밀번호 복잡성 및 보관 규칙이 변경됩니다. 또한, STIG 준수 모드에서는 SSH 원격 스토리지를 사용할 수 없습니다.

⚠

주의 Cisco TAC의 도움 없이 이 설정을 비활성화해선 안 됩니다. 또한, 이 설정은 사용자 시스템의 성능에 상당한 영향을 줄 수 있습니다. Cisco에서는 국방부 보안 요구 사항 준수 이외에는 STIG 준수의 활성화를 권장하지 않습니다.

STIG 컴플라이언스 활성화

이 구성은 Firepower Management Center 또는 기본 매니지드 디바이스(7000 및 8000 Series, ASA FirePOWER 및 NGIPSv)에 적용됩니다.

- Firepower Management Center의 경우 이 구성은 시스템 구성에 포함되어 있습니다.
- 기본 매니지드 디바이스의 경우, Firepower Management Center의 이 구성을 플랫폼 설정 정책의 일부로 적용합니다.

두 경우 모두, 시스템 구성 변경 사항을 저장하거나 공유 플랫폼 설정 정책을 구축할 때까지 구성이 적용되지 않습니다.

주의 구축의 어플라이언스에서 STIG 컴플라이언스를 활성화하는 경우 모든 어플라이언스에서 활성화해야 합니다. Support(지원팀)의 도움 없이는 이 설정을 비활성화할 수 없습니다. 또한, 이 설정은 사용자 시스템의 성능에 상당한 영향을 줄 수 있습니다. Cisco에서는 국방부 보안 요구 사항을 준수하는 경우 외에는 STIG 컴플라이언스를 활성화하지 않을 것을 권장합니다.

프로시저

단계 **1** Firepower Management Center 또는 기존 매니지드 디바이스를 구성하는지 여부에 따라 다음 작업을 수행합니다.

- FMC - **System(**시스템**)** > **Configuration(**구성**)**을 선택합니다.
- 매니지드 디바이스 - **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **STIG Compliance(STIG** 준수**)**를 클릭합니다.

참고 STIG 컴플라이언스를 활성화하는 경우 어플라이언스가 재부팅됩니다. 시스템 구성을 저장할 때 Firepower Management Center가 재부팅됩니다. 매니지드 디바이스는 구성 변경 사항을 구축할 때 재부팅됩니다.

단계 **3** 어플라이언스에서 STIG 컴플라이언스를 영구적으로 활성화하려는 경우, **Enable STIG Compliance(STIG** 컴플라이언스 활성화**)**를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- 어플라이언스가 5.2.0 이전 버전에서 업데이트된 경우, STIG 컴플라이언스를 활성화하면 어플라이언스 인증서가 다시 생성됩니다. 구축 전체에서 STIG 컴플라이언스를 활성화한 후 매니지드 디바이스를 Firepower Management Center에 다시 등록합니다.

시간 및 시간 동기화

Firepower Management Center(FMC)와 매니지드 디바이스에서 시스템 시간을 동기하하는 작업은 Firepower System의 성공적인 작업을 위해 반드시 필요합니다. Cisco에서는 FMC 초기 구성 중에 NTP 서버를 지정할 것을 권장하지만, 초기 구성이 끝난 후 이 섹션의 정보를 이용해 시간 동기화 설정을 구성하거나 변경할 수 있습니다.

FMC 및 모든 디바이스에서 시스템 시간을 동기화하려면 NTP(Network Time Protocol) 서버를 사용합니다. FMC는 MD5 또는 SHA-1 대칭 키 인증을 통해 NTP 서버와의 안전한 통신을 지원합니다. Cisco에서는 시스템 보안을 위해 이 기능을 사용하도록 권장합니다.

또한 인증된 NTP 서버에만 연결하도록 FMC를 구성할 수도 있습니다. 혼합 인증 환경을 이용 중이거나 시스템을 다른 NTP 서버로 마이그레이션할 때 이 옵션을 이용하면 보안을 강화할 수 있습니다. 연결 가능한 모든 NTP 서버가 인증된 환경에서 이 설정을 사용하는 것은 중복 행위입니다.

참고 초기 구성 중에 FMC에 NTP 서버를 지정하면, 해당 NTP 서버와의 연결은 보호되지 않습니다. 연결이 MD5 또는 SHA-1 키를 지정하도록 설정을 편집해야 합니다.

주의 시간이 FMC 및 매니지드 디바이스 간에 동기화되지 않으면 의도하지 않은 결과가 발생할 수 있습니다.

FMC 및 매니지드 디바이스의 시간을 동기화하는 방법은 다음을 참조하십시오.

- 권장: FMC의 시간을 NTP 서버와 동기화, 1380 페이지

  이 주제에서는 FMC를 NTP 서버 또는 서버와 동기화하도록 설정하는 데 필요한 지침을 제공하며, 동일한 NTP 서버와 동기화하도록 매니지드 디바이스를 설정하는 방법을 안내하는 링크를 제공합니다.

- 그렇지 않을 경우, 네트워크 NTP 서버에 액세스하지 않고 시간 동기화, 1382 페이지

  이 주제에서는 FMC에서 시간을 설정하고 NTP 서버 역할을 하도록 FMC를 설정하는 방법에 대한 지침과 FMC NTP 서버와 동기화하도록 매니지드 디바이스를 설정하는 지침으로 연결되는 링크를 제공합니다.

FMC의 시간을 NTP 서버와 동기화

시스템의 모든 구성 요소 간의 시간 동기화는 매우 중요합니다.

Firepower Management Center 및 모든 매니지드 디바이스 간의 적절한 시간 동기화를 보장하는 가장 좋은 방법은 네트워크에서 NTP 서버를 사용하는 것입니다.

FMC은(는) NTPv4를 지원합니다.

이 절차를 수행하려면 관리자 또는 네트워크 관리자 권한이 있어야 합니다.

시작하기 전에

다음에 유의하십시오.

- FMC 및 매니지드 디바이스가 네트워크 NTP 서버에 액세스할 수 없다면 이 절차를 사용하지 마십시오. 대신 네트워크 NTP 서버에 액세스하지 않고 시간 동기화, 1382 페이지 섹션을 참조하십시오.
- 신뢰할 수 없는 NTP 서버를 지정하지 마십시오.
- (시스템 보안 상 권장되는) NTP 서버와의 보안 연결을 설정하려면, 해당 NTP 서버에 설정된 SHA-1 또는 MD5 키 번호 및 값을 얻어야 합니다.

- NTP 서버에 대한 연결에는 구성된 프록시 설정이 사용되지 않습니다.
- Firepower 4100 시리즈 디바이스 및 Firepower 9300 디바이스는 이 절차를 사용하여 시스템 시간을 설정할 수 없습니다. 대신 이 절차를 사용하여 설정한 것과 동일한 NTP 서버를 사용하도록 해당 디바이스를 설정합니다. 자세한 내용은 하드웨어 모델의 설명서를 참조하십시오.

⚠

주의 Firepower Management Center가 재부팅되고 DHCP 서버가 NTP 서버 레코드를 여기에 지정된 것과 다르게 설정하는 경우 DHCP 제공 NTP 서버가 대신 사용됩니다. 이 상황을 피하려면 DHCP 서버를 동일한 NTP 서버를 사용하게 설정하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Time Synchronization(**시간 동기화**)**을 클릭합니다.

단계 **3** **Serve Time via NTP(NTP**를 통해 시간 제공**)**가 **Enabled(**활성화됨**)**인 경우라면, **Disabled(**비활성화됨**)**를 선택해 FMC을(를) NTP 서버로 비활성화합니다.

단계 **4** **Set My Clock(**내 시계 설정**)** 옵션에서 **Via NTP(NTP**를 통해**)**를 선택합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Add NTP Server(NTP** 서버 추가**)** 대화상자에 NTP 서버의 호스트 이름, IPv4 또는 IPv6 주소를 입력합니다.

단계 **7** (선택 사항) FMC 및 NTP 서버 간의 통신을 보호하려면 다음을 수행합니다.

a) **Key Type(**키 유형**)** 드롭다운 목록에서 **MD5** 또는 **SHA-1**을 선택합니다.

b) 지정된 NTP 서버에서 해당 MD5 또는 SHA-1 키 번호와 키 값을 입력합니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** 다른 NTP 서버를 추가하려면 5~8 단계를 반복합니다.

단계 **10** (선택 사항) FMC에서 인증에 성공한 NTP 서버만 사용하게 하려면, **Use the authenticated NTP server only(**인증된 **NTP** 서버만 사용**)** 확인란을 선택합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

다음과 같이 매니지드 디바이스를 동일한 NTP 서버나 서버 모음과 동기화되도록 설정합니다.

- 디바이스 플랫폼 설정인 Threat Defense를 위한 NTP 시간 동기화 구성, 1463 페이지및 NTP 서버와 클래식 디바이스의 시간 동기화, 1413 페이지을(를) 구성합니다.

  FMC가 NTP 서버와 보안 연결을 구성하도록 강제하더라도(인증된 **NTP** 서버만 사용), 해당 서버에 대한 디바이스 연결은 인증을 사용하지 않습니다.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 NTP 서버에 액세스하지 않고 시간 동기화

디바이스에서 네트워크 NTP 서버에 직접 연결할 수 없는 경우 또는 조직에 네트워크 NTP 서버가 없는 경우, 물리적 하드웨어 Firepower Management Center가 NTP 서버 역할을 수행할 수 있습니다.

중요

- 다른 NTP 서버가 없는 경우가 아니면 이 절차를 사용하지 마십시오. 대신 FMC의 시간을 NTP 서버와 동기화, 1380 페이지의 절차를 사용하십시오.
- 가상 Firepower Management Center를 NTP 서버로 사용하지 마십시오.

Firepower Management Center를 NTP 서버로 설정한 후 수동으로 시간을 변경하려면 NTP 옵션을 비활성화하고 수동으로 시간을 변경한 다음 NTP 옵션을 다시 활성화해야 합니다.

프로시저

단계 **1** 다음과 같이 Firepower Management Center에서 시스템 시간을 수동으로 설정합니다.

a) **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.
b) **Time Synchronization(**시간 동기화**)**을 클릭합니다.
c) **Serve Time via NTP(NTP**를 통해 시간 제공**)**가 **Enabled(**활성화됨**)**인 경우 **Disabled(**비활성화됨**)**를 선택합니다.
d) **Save(**저장**)**를 클릭합니다.
e) **Set My Clock(**내 클럭 설정**)**에서 **Manually in Local Configuration(**로컬 구성에서 수동으로**)**을 선택합니다.
f) **Save(**저장**)**를 클릭합니다.
g) 화면 왼쪽 탐색 패널에서 **Time(**시간**)**을 클릭합니다.
h) **Set Time(**시간 설정**)** 드롭다운 목록을 사용하여 시간을 설정합니다.
i) 표시된 표준 시간대가 UTC가 아닌 경우, 이를 클릭하고 표준 시간대를 **UTC**로 설정합니다.
j) **Save(**저장**)**를 클릭합니다.
k) **Done(**완료**)**을 클릭합니다.
l) **Apply(**적용**)**를 클릭합니다.

단계 **2** 다음과 같이 Firepower Management Center가 NTP 서버 역할을 하도록 설정합니다.

a) 화면 왼쪽 탐색 패널에서 **Time Synchronization(**시간 동기화**)**을 클릭합니다.
b) **Serve Time via NTP(NTP**를 통해 시간 제공**)**에 대해 **Enabled(**활성화됨**)**를 선택합니다.
c) **Save(**저장**)**를 클릭합니다.

단계 **3** 다음과 같이 매니지드 디바이스를 Firepower Management Center NTP 서버와 동기화되도록 설정합니다.

a) 매니지드 디바이스에 할당된 플랫폼 설정 정책에 대한 Time Synchronization(시간 동기화) 설정에서 **Via NTP from Management Center(Management Center**에서 **NTP**를 통해**)**를 사용하여 동기화하도록 클럭을 설정합니다.
b) 매니지드 디바이스에 변경 사항을 구축합니다.

지침은 다음 내용을 참조하십시오.

NTP 서버와 클래식 디바이스의 시간 동기화, 1413 페이지의 내용을 참조하십시오.

시간 동기화 설정 변경 정보

- Firepower Management Center 및 매니지드 디바이스는 주로 정확한 시간에 의존합니다. 시스템 시계는 Firepower System의 시간을 유지하는 시스템 기능입니다. 시스템 시계는 전 세계가 시계와 시간을 규제하는 기본 시간 기준인 UTC(Universal Coordinated Time)로 설정됩니다.

  시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 변경할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.

- NTP를 사용하여 시간을 서비스하도록 FMC를 구성한 다음 나중에 이를 비활성화하면, 매니지드 디바이스의 NTP 서비스는 계속해서 FMC와 시간을 동기화하려고 시도합니다. 새 시간 소스를 설정하려면 해당 플랫폼 설정 정책을 업데이트하고 다시 구축해야 합니다.

- Firepower Management Center를 NTP 서버로 설정한 후 수동으로 시간을 변경하려면 NTP 옵션을 비활성화하고 수동으로 시간을 변경한 다음 NTP 옵션을 다시 활성화해야 합니다.

현재 시스템 시간, 소스 및 NTP 서버 연결 상태 보기

시간 설정이 대부분의 페이지에서 로컬 시간으로 표시됩니다. 여기서 사용되는 시간대는 User Preferences(사용자 환경 설정)의 Time Zone(표준 시간대) 페이지에서 설정하며(기본값은 미국/뉴욕), UTC 시간을 사용해 어플라이언스에 저장합니다.

제한 Time Zone(표준 시간대) 기능(User Preferences(사용자 환경 설정))에서는 기본 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 그러할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.

참고 7000 및 8000 하드웨어 디바이스에 대한 시간 및 시간 소스 정보를 보는 방법은 7000/8000 시리즈 디바이스의 시스템 시간 보기, 1422 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Time(**시간**)**을 클릭합니다.

현재 시간은 사용자 기본 설정에서 계정에 지정된 표준 시간대를 사용하여 표시됩니다.

어플라이언스에서 NTP 서버를 사용하는 경우: 테이블 항목에 대한 자세한 내용은 NTP 서버 상태, 1384 페이지 섹션을 참조하십시오.

NTP 서버 상태

NTP 서버에서 시간을 동기화한다면, **Time(**시간**)** 페이지에서 연결 상태를 볼 수 있습니다**(System(**시스템**) > Configuration(**구성**)**선택).

표 ***91: NTP*** 상태

열	설명
NTP 서버	구성된 NTP 서버의 IP 주소 및 이름.
상태	NTP 서버 시간 동기화의 상태: • **Being Used(**사용 중**)** - 어플라이언스가 NTP 서버와 동기화됨을 나타냅니다. • **Available(**사용 가능**)** - NTP 서버를 사용할 수 있지만 시간이 아직 동기화되지 않았음을 나타냅니다. • **Not Available(**사용 불가**)** - NTP 서버가 설정에 있지만 NTP 디먼이 이를 사용할 수 없음을 나타냅니다. • **Pending(**보류 중**)** - NTP 서버가 새로운 것이거나 NTP 디먼이 최근에 다시 시작되었음을 나타냅니다. 시간 경과에 따라 값이 **Being Used(**사용 중**)**, **Available(**사용 가능**)** 또는 **Not Available(**사용 불가**)**로 변경됩니다. • **Unknown(**알 수 없음**)** - NTP 서버의 상태를 알 수 없음을 나타냅니다.
인증	FMC 및 NTP 서버 간의 통신에 대한 인증 상태입니다. • **none(**없음**)**은 인증을 구성하지 않았다는 뜻입니다. • **bad(**불량**)**은 인증을 구성했지만 실패했다는 뜻입니다. • **ok(**양호**)**는 인증에 성공했다는 뜻입니다. 인증을 구성했다면, 시스템은 상태 값 다음에 키 번호와 키 유형(SHA-1 또는 MD5)을 표시합니다. 예: **bad, key 2, MD5**.
Offset(오프셋)	어플라이언스 및 구성된 NTP 서버 간 밀리초 단위의 시간 차이. 음수 값은 어플라이언스가 NTP 서버 뒤에 있음을 나타내고, 양수 값은 그 반대를 나타냅니다.
마지막 업데이트	시간이 NTP 서버와 마지막으로 동기화된 후 경과한 기간(초). NTP 디먼은 몇 가지 조건을 기반으로 동기화 시간을 자동으로 조정합니다. 예를 들어 300초와 같이 업데이트 시간이 좀 더 긴 경우, 이는 시간이 비교적 안정적이며 NTP 디먼이 더 낮은 업데이트 증분을 사용할 필요가 없다고 결정했음을 나타냅니다.

전역 사용자 구성

전역 사용자 구성 설정은 Firepower Management Center에 있는 모든 사용자에게 영향을 줍니다. User Configuration(사용자 구성) 페이지(**System(**시스템**)** > **Configuration(**설정**)** > **User Configuration(**사용자 설정**)**)에서 이러한 설정을 구성합니다.

- **Password Reuse Limit(**비밀번호 재사용 한도**)**: 재사용할 수 없는 사용자의 최근 기록에 있는 비밀번호 수입니다. 이 제한은 모든 사용자의 웹 인터페이스 액세스에 적용됩니다. 관리자 사용자의 경우 이는 CLI 액세스에도 적용됩니다. 시스템은 각 액세스 형식에 대해 별도의 비밀번호 목록을 유지합니다. 한도를 0(기본값)으로 설정하면 비밀번호 재사용에 대한 제한이 없습니다. 비밀번호 재사용 한도 설정, 1386 페이지의 내용을 참조하십시오.
- **Track Successful Logins(**성공적인 로그인 추적**)**: 시스템이 사용자별, 액세스 방법별(웹 인터페이스 또는 CLI)로 Firepower Management Center에 대한 성공적인 로그인을 추적하는 일수입니다. 사용자가 로그인하면 사용 중인 인터페이스에 대한 로그인 성공 횟수가 표시됩니다. **Track Successful Logins(**성공적인 로그인 추적**)**가 가 0으로 설정되면(기본값) 시스템은 로그인 활동을 추적하거나 보고하지 않습니다. 성공적인 로그인 추적, 1386 페이지의 내용을 참조하십시오.
- **Max Number of Login Failures(**최대 로그인 실패 횟수**)**: 시스템이 구성 가능한 시간 동안 계정 액세스를 일시적으로 차단하기 전에 사용자가 잘못된 웹 인터페이스 로그인 자격 증명을 연속적으로 입력할 수 있는 횟수입니다. 임시 잠금이 적용되는 동안 사용자가 로그인 시도를 계속하는 경우:
  - 시스템은 사용자에게 임시 잠금이 적용되었음을 알리지 않고 해당 계정에 대한 액세스(유효한 비밀번호 포함)를 거부합니다.
  - 시스템은 로그인 시도가 있을 때마다 해당 계정의 로그인 실패 횟수를 계속 누적합니다.
  - 사용자가 개별 User Configuration(사용자 구성) 페이지에서 해당 계정에 대해 구성된 **Maximum Number of Failed Logins(**최대 실패 로그인 횟수**)**를 초과하면 관리자 사용자가 다시 활성화할 때까지 계정이 잠깁니다.
- **Set Time in Minutes to Temporarily Lockout Users(**사용자에 대한 임시 잠금 시간**(**분**)** 설정**)**: **Maximum Number of Failed Logins(**최대 실패 로그인 횟수**)**가 0이 아닌 경우 임시 웹 인터페이스 사용자 잠금 기간(분)입니다.
- **Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션 수**)**: 동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 세션 수입니다. 세션 유형은 사용자에게 할당된 역할을 기준으로 결정됩니다. 사용자에게 읽기 전용 역할만 할당되었다면, 해당 사용자의 세션은 **(**읽기 전용**)** 세션 제한 수에 적용됩니다. 사용자에게 쓰기 권한을 제공하는 역할이 있다면, 세션은 읽기/쓰기 세션 제한 수에 적용됩니다. 예를 들어 사용자에게 관리자 역할이 할당되고 **Maximum sessions for users with Read/Write privileges/CLI users(**읽기/쓰기 권한이 있는 사용자**/CLI** 사용자의 최대 세션 수**)**를 5로 설정했다면, 사용자는 읽기/쓰기 권한이 있는 다른 사용자 5명이 로그인한 상태에서는 로그인할 수 없습니다.

참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할과 맞춤형 사용자 역할은 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)** 및 **System(**시스템**)** > **Users(**사용자**)** > **User Roles(**사용자 역할**)**의 역할 이름에 **(**읽기 전용**)**이라고 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 시스템은 **(**읽기 전용**)**을 필수 기준을 충족하는 역할에 자동으로 적용합니다. 텍스트 문자열을 역할 이름에 수동으로 추가하는 방법으로는 역할을 읽기 전용을 만들 수 없습니다.

각 세션 유형에 대해 1~1024 범위의 최대 제한을 설정할 수 있습니다. **Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션**)**을 0(기본값)으로 설정하면, 동시 세션 수는 무제한이 됩니다.

동시 세션 제한을 더 제한적인 값으로 변경하면, 시스템은 현재 열린 세션을 닫지는 않습니다. 대신 지정된 숫자 이상의 신규 세션이 열리지 않게 합니다.

비밀번호 재사용 한도 설정

Password Reuse Limit(비밀번호 재사용 한도**)**을 활성화하면 시스템은 FMC 사용자에 대한 암호화된 비밀번호 기록을 유지합니다. 사용자는 기록에 있는 비밀번호는 다시 사용할 수 없습니다. 액세스 방법(웹 인터페이스 또는 CLI)별로 각 사용자에 대해 저장된 비밀번호 수를 지정할 수 있습니다. 사용자의 현재 비밀번호도 이 숫자에 적용됩니다. 한도를 낮추면 시스템은 기록에서 이전 비밀번호를 삭제합니다. 한도를 늘려도 삭제된 비밀번호는 복원되지 않습니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** **Password Reuse Limit(**비밀번호 재사용 한도**)**을 기록에서 유지할 비밀번호 수(최대 256)로 설정합니다.

비밀번호 재사용 검사를 비활성화하려면 0을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

성공적인 로그인 추적

이 절차를 사용하면 지정된 일수 동안 각 사용자에 대해 성공적인 로그인을 추적할 수 있습니다. 이 추적을 활성화하면 사용자가 웹 인터페이스 또는 CLI에 로그인할 때 로그인 성공 횟수가 표시됩니다.

참고 일수를 낮추면 시스템은 이전 로그인 기록을 삭제합니다. 그런 다음 한도를 늘리면 시스템은 해당 일수의 계산을 복원하지 않습니다. 이 경우 보고된 로그인 성공 횟수가 실제 수보다 일시적으로 낮을 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** **Track Successful Login Days(**성공적인 로그인 일수 추적**):**를 성공한 로그인을 추적하는 일수로 설정합니다(최대 365일).

로그인 추적을 비활성화하려면 0을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

임시 잠금 활성화

잠금이 적용되기 전에 시스템에서 허용하는 연속적인 로그인 시도 횟수를 지정하여 임시 시간 지정 잠금 기능을 활성화합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** 사용자가 일시적으로 잠금 처리되기 전에 **Max Number of Login Failures(**최대 로그인 실패 횟수**)**를 연속 로그인 실패 시도의 최대 횟수로 설정합니다.

임시 잠금을 비활성화하려면 0을 입력합니다.

단계 **4** **Time in Minutes to Temporarily Lockout Users(**사용자에 대한 임시 잠금 시간**(**분**))**를 임시 잠금을 트리거한 사용자를 잠금 처리하는 시간(분)으로 설정합니다.

이 값이 0이면 **Max Number of Login Failures(**최대 로그인 실패 횟수**)**가 0이 아니더라도 사용자가 로그인을 다시 시도할 때까지 기다릴 필요가 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

최대 동시 세션 수 설정

동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 최대 세션 수를 지정할 수 있습니다. 세션 유형은 사용자에게 할당된 역할을 기준으로 결정됩니다. 사용자에게 읽기 전용 역할만 할당되었다면, 해당 사용자의 세션은 읽기 전용 세션 제한 수에 적용됩니다. 사용자에게 쓰기 권한을 제공하는 역할이 있다면, 세션은 읽기/쓰기 세션 제한 수에 적용됩니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** 각 세션 유형(읽기 전용 및 읽기/쓰기)에 대해, **Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션**)**를 해당 유형에 대해 동시에 열 수 있는 최대 세션 수로 설정합니다.

세션 유형별 동시 사용자 수를 제한하지 않으려면 0을 입력합니다.

참고 동시 세션 제한을 더 제한적인 값으로 변경하면, 시스템은 현재 열린 세션을 닫지는 않습니다. 대신 지정된 숫자 이상의 신규 세션이 열리지 않게 합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

세션 시간 초과

무인 로그인 세션은 보안 위험이 될 수 있습니다. 비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 구성할 수 있습니다.

시스템을 오랫동안 패시브 방식으로 안전하게 모니터링하려는 상황이라면, 특정 웹 인터페이스 사용자를 시간 제한에서 제외할 수 있습니다. 메뉴 옵션에 완전히 액세스할 수 있으므로 손상 시 더 큰 위험을 초래하는 Administrator 역할의 사용자는 세션 시간 초과에서 제외할 수 없습니다.

세션 시간 제한 구성

클래식 디바이스에 세션 시간 제한을 구성하려면, 디바이스 플랫폼 설정을 사용합니다. 클래식 디바이스에 대한 세션 시간 초과 구성, 1414 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Shell Timeout(**셸 시간 초과**)**를 클릭합니다.

단계 **3** 세션 시간 제한 구성

- 웹 인터페이스(FMC에만 해당): 브라우저 세션 시간 제한(분)을 구성합니다. 기본값은 60이고 최대값은 1440(24시간)입니다.

  이 세션 시간 제한에서 사용자를 제외하는 방법은 사용자 어카운트 로그인 옵션의 내용을 참조하십시오.

- CLI: 셸 시간 제한(분) 필드를 구성합니다. 기본값은 0이고 최대값은 1440(24시간)입니다.

단계 **4** **Save**(저장)를 클릭합니다.

취약성 매핑

서버의 검색 이벤트 데이터베이스에 애플리케이션 ID가 있고 트래픽에 대한 패킷 헤더에 공급업체 및 버전이 포함된 경우, 호스트 IP 주소에서 주고받는 모든 애플리케이션 프로토콜 트래픽에 대해 Firepower System은 해당 주소에 취약성을 자동으로 매핑합니다.

패킷에 공급업체 또는 버전 정보가 포함되어 있지 않은 서버의 경우 시스템이 취약성을 해당 공급업체 및 버전 없는 서버의 서버 트래픽과 연결할지 여부를 구성할 수 있습니다.

예를 들어, 호스트가 헤더에 공급업체 또는 버전을 가지고 있지 않은 SMTP 트래픽을 서비스할 수 있습니다. 시스템 구성의 Vulnerability Mapping 페이지에서 SMTP 서버를 활성화한 다음 트래픽을 탐지하는 디바이스를 관리하는 Firepower Management Center에 해당 구성을 저장하면, SMTP 서버와 관련된 모든 취약성이 호스트의 호스트 프로파일에 추가됩니다.

탐지기는 서버 정보를 수집하여 호스트 프로파일에 추가하지만, 애플리케이션 프로토콜 탐지기는 취약성 매핑에 사용되지 않습니다. 사용자 지정 애플리케이션 프로토콜 탐지기에 대해 공급업체 및 버전을 지정할 수 없으며 취약성 매핑을 위해 서버를 선택할 수 없기 때문입니다.

서버의 취약성 매핑

이 절차를 수행하려면 스마트 라이선스 또는 보호 클래식 라이선스가 필요합니다.

프로시저

단계 **1** **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 **2** **Vulnerability Mapping**(취약성 매핑)을 선택합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되지 않도록 하려면 해당 서버의 확인란을 선택 취소합니다.
- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되도록 하려면 해당 서버의 확인란을 선택합니다.

팁 **Enabled**(활성화됨) 옆에 있는 확인란을 사용하여 모든 확인란을 동시에 선택하거나 선택 취소할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

원격 콘솔 액세스 관리

VGA 포트(기본값) 또는 물리적 어플라이언스의 시리얼 포트를 통해 지원되는 시스템에 원격으로 액세스하도록 하려면 Linux 시스템 콘솔을 사용할 수 있습니다. Console Configuration(콘솔 구성) 페이지를 사용하여 조직 내 Firepower 구축의 실제 레이아웃에 가장 적합한 옵션을 선택합니다.

지원되는 물리적 하드웨어 기반 Firepower 시스템에서는 기본(`eth0`)) 관리 인터페이스의 SOL(Serial Over LAN) 연결에서 LOM(Lights-Out Management)을 사용하여 시스템의 관리 인터페이스에 로그인하지 않고 시스템을 원격으로 모니터링하거나 관리할 수 있습니다. OOB(Out of Band) 관리 연결에서 명령줄 인터페이스를 사용하여 섀시 일련 번호 보기, 팬 속도와 온도 등의 조건 모니터링 등 제한적인 작업을 수행할 수 있습니다. LOM을 지원하기 위한 케이블 연결은 FMC 모델에 따라 다릅니다.

- FMC 모델 MC1600, MC2600 및 MC4600의 경우, CIMC 포트와의 연결을 사용하여 LOM을 지원합니다. 자세한 내용은 *Cisco Firepower Managemenet Center 1600, 2600 및 4600 시작 가이드*를 참조하십시오.
- 다른 모든 FMC 하드웨어 모델의 경우, 기본(eth0) 관리 포트가 있는 연결을 사용하여 LOM을 지원합니다. 해당 하드웨어 모델의 *Cisco Firepower Management Center 시작 가이드*를 참조하십시오.

시스템을 관리하려는 사용자와 시스템 모두에 대해 LOM을 활성화해야 합니다. 시스템 및 사용자를 활성화한 후 시스템에 대한 액세스 및 관리를 위해 서드파티 IPMI(Intelligent Platform Management Interface) 유틸리티를 사용합니다.

시스템에서 원격 콘솔 설정

이 절차를 수행하려면 관리자 사용자여야 합니다.

시작하기 전에

- 디바이스의 관리 인터페이스에 연결된 모든 서드파티 스위칭 장비에서 STP(Spanning Tree Protocol)를 비활성화해야 합니다.
- Lights-Out 관리를 활성화하려는 경우 IPMI(Intelligent Platform Management Interface) 유틸리티 설치 및 사용에 대한 정보는 어플라이언스의 시작하기 가이드를 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.
단계 **2** **Console Configuration(**콘솔 구성**)**을 클릭합니다.
단계 **3** 원격 콘솔 액세스 옵션을 선택합니다.

- 어플라이언스의 VAG 포트를 사용하려면 **VGA**를 선택합니다.
- **Physical Serial Port(**물리적 시리얼 포트**)**를 선택해 어플라이언스의 시리얼 포트를 사용합니다.
- FMC의 기본 관리 포트에서 SOL 연결을 사용하려면 **Lights-Out** 관리를 선택합니다.

단계 **4** SOL을 통해 LOM을 구성하려면:

- 시스템(**DHCP** 또는 **Manual(**수동**)**)에 대한 주소 **Configuration(**구성**)**을 선택합니다.
- 수동 구성을 선택한 경우 필요한 IPv4 설정을 입력합니다.
  - LOM에 사용될 **IP Address(IP** 주소**)**를 입력합니다.

    참고 LOM IP 주소는 FMC 관리 인터페이스 IP 주소와 달라야 합니다.

  - 시스템에 대한 **Netmask(**넷마스크**)**를 입력합니다.
  - 시스템에 대한 **Default Gateway(**기본 게이트웨이**)**를 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** "다음 변경 사항을 적용하려면 시스템을 재부팅해야합니다."라는 경고가 표시됩니다. 지금 재부팅하려면 **OK(**확인**)**를 클릭하고 나중에 재부팅하려면 **Cancel(**취소**)**을 클릭합니다.

다음에 수행할 작업

- 직렬 액세스를 구성한 경우, FMC 모델용 시작 가이드에 설명된 대로 이더넷을 통한 원격 직렬 액세스를 지원할 수있는 로컬 컴퓨터, 터미널 서버 또는 기타 디바이스에 후면 패널 직렬 포트가 연결되어 있는지 확인합니다.
- Lights-Out Management를 구성한 경우 Lights-Out Management 사용자를 활성화합니다. LOM(Lights-Out Management) 사용자 액세스 구성, 1391 페이지 섹션을 참조하십시오.

LOM(Lights-Out Management) 사용자 액세스 구성

또한 기능을 사용할 사용자에게 Lights-Out Management 권한을 명시적으로 부여해야 합니다. 또한 LOM 사용자에는 다음과 같은 제한이 있습니다.

- 사용자에게 관리자 역할을 할당해야 합니다.
- 사용자 이름은 최대 16자의 영숫자로 지정할 수 있습니다. LOM 사용자는 16자보다 긴 사용자 이름과 하이픈을 사용할 수 없습니다.
- 사용자의 LOM 비밀번호는 해당 사용자의 시스템 비밀번호와 동일합니다. 비밀번호는 사용자 암호, 52 페이지에 설명된 요구 사항을 준수해야 합니다. 어플라이언스에서 지원되는 최대 길이로 사전에 없는 복잡한 암호를 사용하고 3개월마다 변경하는 것이 좋습니다.

- LOM이 Firepower 7110, 7115, 7120 또는 7125 디바이스에서 활성화되면 비밀번호는 최대 영숫자 16자로 구성할 수 있습니다.
- 물리적 Firepower Management Center 및 8000 Series 디바이스에는 최대 13명의 LOM 사용자가 있을 수 있습니다. 7000 시리즈 디바이스에는 최대 8명의 LOM 사용자가 있을 수 있습니다.

그러한 사용자가 로그인한 상태에서 LOM으로 해당 사용자를 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자를 복원할 경우, 해당 사용자가 다시 웹 인터페이스에 로그인해야 `impitool` 명령에 다시 액세스할 수 있습니다.

LOM(Lights-Out Management) 사용자 액세스 활성화

이 절차를 수행하려면 관리자 사용자여야 합니다.

이 작업을 통해 기존 사용자에게 LOM 액세스 권한을 부여할 수 있습니다. 새 사용자에게 LOM 액세스 권한을 부여하려면 내부 사용자 추가, 55 페이지의 내용을 참조하십시오.

각 시스템의 로컬 웹 인터페이스를 사용하여 시스템별로 LOM 및 LOM 사용자를 구성합니다. Firepower Management Center를 사용하여 매니지드 디바이스에서 LOM을 구성할 수 없습니다. 마찬가지로, 사용자는 어플라이언스별로 독립적으로 관리되므로 Firepower Management Center에서 LOM 지원 사용자를 생성할 경우 해당 기능이 매니지드 디바이스의 사용자로 전달되지 않습니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** 기존 사용자에 대해 LOM 사용자 액세스 권한을 부여하려면 목록의 사용자 이름 옆에 있는 수정( )을 클릭합니다.

단계 **3** **User Configuration(**사용자 구성**)** 아래에서 Administrator 역할을 활성화합니다.

단계 **4** **Allow Lights-Out Management Access(Lights-Out Management** 액세스 허용**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

SoL(Serial over LAN) 연결 구성

컴퓨터에서 타사 IPMI 유틸리티를 사용하여 어플라이언스에 대한 Serial Over LAN 연결을 만듭니다. Linux와 유사한 컴퓨터 환경 또는 Mac 환경에서는 IPMItool을 사용하고, Windows 환경에서는 Windows 버전에 따라 IPMIutil 또는 IPMItool을 사용할 수 있습니다.

참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

Linux

IPMItool은 많은 배포의 표준이며 곧바로 사용 가능합니다.

Mac

Mac에는 IPMItool을 설치해야 합니다. 먼저 Mac에 Apple의 XCode Developer 툴이 설치되었는지 확인하고, 명령줄 개발을 위한 선택적인 구성 요소가 설치되었는지 확인합니다(새 버전에서는 UNIX Development 및 System Tools, 이전 버전에서는 Command Line Support). 그런 다음 macports 및 IPMItool을 설치할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

Windows

Linux용 Windows 하위 시스템(WSL)이 활성화된 Windows 버전 10 이상 및 일부 이전 버전의 Windows Server의 경우 IPMItool을 사용할 수 있습니다. 그렇지 않으면 Windows 시스템에서 IPMIutil을 컴파일해야 합니다. IPMIutil 자체를 사용하여 컴파일 할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

IPMI 유틸리티 명령 이해

IPMI 유틸리티에 사용되는 명령은 Mac에서 다음 IPMItool 예와 같은 세그먼트로 구성됩니다.

```
ipmitool -I lanplus -H IP_address -U user_name command
```

여기서 각 항목은 다음을 나타냅니다.

- `ipmitool`은 유틸리티를 호출합니다.
- `-I lanplus`는 세션에 대해 암호화된 IPMI v2.0 RMCP + LAN 인터페이스를 사용하도록 지정합니다.
- `-H IP_address`는 액세스하려는 어플라이언스의 LOM(Lights-Out Management)을 위해 구성한 IP 주소를 나타냅니다.
- `-U user_name`는 권한 있는 원격 세션 사용자의 이름입니다.
- *command*는 사용할 명령의 이름입니다.

참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

Windows의 IMPIutil에서는 동일한 명령이 다음과 같이 표시됩니다.

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

이 명령은 어플라이언스에서 실제로 존재 하는 것 처럼 로그인 할 수 있는 기기의 명령행에 연결 합니다. 비밀번호를 입력하라는 프롬프트가 표시될 수 있습니다.

IPMItool을 사용한 SoL(Serial over LAN) 설정

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMItool을 사용하여 다음 명령을 입력하고 메시지가 표시되면 암호를 입력합니다.

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

IPMIutil을 사용한 SoL(Serial over LAN) 설정

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMIutil을 사용하여 다음 명령을 입력하고 메시지가 표시되면 암호를 입력합니다.

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

LOM(Lights-Out Management) 개요

Lights-Out Management(LOM)를 사용하면 시스템에 로그인하지 않고도 기본(`eth0`) 관리 인터페이스에서 SOL 연결을 통해 제한된 작업을 수행할 수 있습니다. 이 명령을 사용하여 SOL 연결을 생성한 후 LOM 명령 중 하나를 사용합니다. 명령이 완료되면 연결이 종료됩니다. 일부 전원 제어 명령은 70xx 제품군 디바이스에서 유효합니다.

참고 Firepower 71xx, Firepower 82xx 또는 Firepower 83xx 디바이스에 대한 BMC(baseboard management controller)는 호스트 전원이 켜져 있을 때 1Gbps 링크 속도를 통해서만 액세스할 수 있습니다. 디바이스 전원이 꺼져 있으면 BMC는 10 및 100Mbps의 이더넷 링크만 설정할 수 있습니다. 따라서 LOM을 사용하여 디바이스 전원을 원격으로 제어하는 경우 10 및 100Mbps 링크 속도만을 사용하여 디바이스를 네트워크에 연결하십시오.

주의 드물긴 하지만, 시스템의 관리 인터페이스와 다른 서브넷에 있으며 시스템이 DHCP로 구성되어 있는 경우 LOM 기능에 액세스하려고 시도하면 실패할 수 있습니다. 이런 일이 발생하면 시스템에서 LOM을 비활성화한 후 다시 활성화하거나, 동일한 서브넷의 컴퓨터를 시스템으로 사용하여 관리 인터페이스를 ping할 수 있습니다. 이렇게 하면 LOM을 사용할 수 있게 됩니다.

주의 Cisco에서는 IPMI(Intelligent Platform Management Interface) 표준(CVE-2013-4786)에 내재된 취약성에 대해 잘 알고 있습니다. 시스템에서 LOM(Lights-Out Management)을 활성화하면 이 취약성이 노출됩니다. 이 취약성을 완화하려면 신뢰할 수 있는 사용자만 액세스할 수 있는 안전한 관리 네트워크에 시스템을 구축하고, 시스템에서 지원되는 최대 길이로 사전에 없는 복잡한 비밀번호를 사용하고 3개월에 한 번씩 변경하십시오. 이 취약성이 노출되지 않도록 하려면 LOM을 활성화하지 마십시오.

시스템에 대한 모든 액세스 시도가 실패한 경우 LOM을 사용하여 시스템을 원격으로 재시작할 수 있습니다. SOL 연결이 활성화된 상태에서 시스템을 다시 시작하면 LOM 세션이 끊어지거나 시간이 초과될 수 있습니다.

주의 다시 시작하려는 다른 시도에 응답하지 않는 상황이 아니면 시스템을 다시 시작하지 마십시오. 원격으로 다시 시작하는 경우 시스템이 정상적으로 재부팅되지 않으며, 데이터가 손실될 수 있습니다.

표 ***92: Lights-Out Management*** 명령

IPMItool	**IPMIutil**	설명
(해당 없음)	`-V 4`	IPMI 세션의 관리자 권한을 활성화합니다.
`-I lanplus`	`-J 3`	IPMI 세션의 암호화를 활성화합니다.
`-H 호스트 이름/IP 주소`	`-N 노드 이름/IP 주소`	다음에 대한 LOM IP 주소 또는 호스트 이름을 나타냅니다. FMC
`-U`	`-U`	권한이 있는 LOM 계정의 사용자 이름을 나타냅니다.
`sol activate`	`sol -a`	SOL 세션을 시작합니다.
`sol deactivate`	`sol -d`	SOL 세션을 종료합니다.
`chassis power cycle`	`power -c`	어플라이언스를 다시 시작합니다(70xx 제품군 디바이스에서는 유효하지 않음).
`chassis power on`	`power -u`	어플라이언스 전원을 켭니다.
`chassis power off`	`power -d`	어플라이언스 전원을 끕니다(70xx 제품군 디바이스에서는 유효하지 않음).
`sdr`	`sensor`	팬 속도와 온도 등 어플라이언스 정보를 표시합니다.

예를 들어 어플라이언스 정보 목록을 표시하려면 다음 IPMItool 명령을 사용합니다.

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

IPMIutil 유틸리티에서는 동일한 명령이 다음과 같습니다.

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

IPMItool을 사용한 LOM(Lights-Out Management) 구성

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMItool에 대해 다음 명령을 입력하고 메시지가 표시되면 비밀번호를 입력합니다.

```
ipmitool -I lanplus -H IP_address -U user_name command
```

IPMIutil을 사용한 LOM(Lights-Out Management) 구성

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMIutil에 대해 다음 명령을 입력하고 메시지가 표시되면 비밀번호를 입력합니다.

```
ipmiutil -J 3 -N IP_address -U username command
```

VMware Tools 및 가상 시스템

VMware Tools는 가상 머신용 성능 향상 유틸리티 모음입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. VMware에서 실행되는 Firepower 가상 어플라이언스는 다음 플러그인을 지원합니다.

- guestInfo
- powerOps

- timeSync
- vmbackup

또한 모든 지원되는 ESXi 버전에서 VMware Tools를 활성화할 수 있습니다. 지원되는 버전 목록을 보려면 VMware용 Cisco Firepower NGIPSv 빠른 시작 가이드 섹션을 참조하십시오. VMware Tools의 전체 기능에 대한 자세한 내용은 VMware 웹 사이트(http://www.vmware.com/)를 참조하십시오.

VMware용 Firepower Management Center의 VMWare Tools 활성화

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	Any(모든)	Firepower Management Center	전역만 해당	Admin(관리자)

NGIPSv에는 웹 인터페이스가 없으므로 CLI를 사용하여 해당 플랫폼에서 VMware Tools를 활성화해야 합니다. VMware용 Cisco Firepower NGIPSv 빠른 시작 가이드 섹션을 참조하십시오.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **VMware Tools**를 클릭합니다.

단계 **3** **Enable VMware Tools(VMware Tools** 활성화**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

시스템 구성 기록

기능	버전	세부 사항
SAN(Subject Alternative Name)	6.6	FMC의 HTTPS 인증서를 생성할 때 SAN 필드를 지정할 수 있습니다. 인증서가 여러 도메인 이름 또는 IP 주소를 보호하는 경우, SAN을 사용하는 것이 좋습니다. SAN에 대한 자세한 내용은 RFC 5280, 섹션 4.2.1.6을 참조하십시오. 신규/수정된 화면: **System(**시스템**)** > **Configuration(**구성**)** > **HTTPS Certificate(HTTPS** 인증서**)** 지원되는 플랫폼: FMC

기능	버전	세부 사항
HTTPS 인증서	6.6	시스템과 함께 제공되는 기본 HTTPS 서버 인증서는 이제 800일 후에 만료됩니다. 어플라이언스가 버전 6.6으로 업그레이드되기 전에 생성된 기본 인증서를 사용하는 경우, 인증서 수명은 인증서 생성 시 사용되던 Firepower 버전에 따라 달라집니다. 자세한 내용은 기본 HTTPS 서버 인증서, 1345 페이지를 참조하십시오. 신규/수정된 화면: 없음 지원되는 플랫폼: 하드웨어 FMC
보안 NTP	6.5	FMC은(는) SHA1 또는 MD5 대칭 키 인증을 이용해 NTP 서버와의 안전 연결을 지원합니다. 신규/수정된 화면: **System(**시스템**)** > **Configuration(**설정**)** > **Time Synchronization(**시간 동기화**)** 지원되는 플랫폼: FMC
웹 분석	6.5	EULA에 동의하면 웹 분석 데이터 수집이 시작됩니다. 예전처럼, 데이터 공유를 계속하지 않도록 선택할 수 있습니다. (선택 사항) 웹 분석 추적 선택 취소의 내용을 참조하십시오.
다음에 대한 자동 CLI 액세스 FMC	6.5	SSH를 이용해 FMC에 로그인하면, CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI `expert` 명령을 사용하면 Linux 셸에 액세스할 수 있습니다. 참고 이 기능을 이용하면 버전 6.3 기능인 FMC에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 FMC에서는 **System(**시스템**)** > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)** 페이지가 표시되지 않습니다. 물리적 FMC에서는 계속 표시됩니다.
읽기 전용 및 읽기/쓰기 액세스에 구성 가능한 세션 제한	6.5	**Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션**)** 설정을 추가했습니다. 이 설정을 이용하면 관리자는 동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 최대 세션 수를 지정할 수 있습니다. 참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할과 맞춤형 사용자 역할은 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)**와 **System(**시스템**)** > **Users(**사용자**)** > **User Roles(**사용자 역할**)**의 역할 이름에 **(**읽기 전용**)**이라고 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 신규/수정된 화면: **System(**시스템**)** > **Configuration(**구성**)** > **User Configuration(**사용자 구성**)** **System(**시스템**)** > **Users(**사용자**)** > **User Roles(**사용자 역할**)** 지원되는 플랫폼: FMC

기능	버전	세부 사항
관리 인터페이스에서 DAD(Duplicate Address Detection)를 비활성화하는 기능	6.4	IPv6를 활성화하면 DAD를 비활성화할 수 있습니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다. 신규/수정된 화면: **System(**시스템**)** > **Configuration(**구성**)** > **Management Interfaces(**관리 인터페이스**)** > **Interfaces(**인터페이스**)** > **Edit Interface(**인터페이스 편집**)** 대화 상자 > **IPv6 DAD** 확인란 지원되는 플랫폼: FMC, 7000 및 8000 Series 디바이스
관리 인터페이스에서 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 비활성화하는 기능	6.4	IPv6를 활성화할 때 이제 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 비활성화할 수 있습니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 디바이스 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다. 신규/수정된 화면: **System(**시스템**)** > **Configuration(**구성**)** > **Management Interfaces(**관리 인터페이스**)** > **ICMPv6** 신규/수정된 명령: **configure network ipv6 destination-unreachable**, **configure network ipv6 echo-reply** 지원되는 플랫폼: FMC(웹 인터페이스에만 해당), 7000 및 8000 Series, FTD(CLI에만 해당), ASA FirePOWER 모듈(CLI에만 해당), NGIPSv(CLI에만 해당)
전역 사용자 구성	6.3	**Track Successful Logins(**성공적인 로그인 추적**)** 설정을 추가했습니다. 시스템은 선택한 일수 이내에 각 FMC 계정이 수행한 성공적인 로그인 수를 추적할 수 있습니다. 이 기능을 활성화하면 로그인 사용자는 구성된 일수 전에 시스템에 성공적으로 로그인한 횟수를 나타내는 메시지를 볼 수 있습니다. (셸/CLI 액세스뿐만 아니라 웹 인터페이스에도 적용됩니다.) **Password Reuse Limit(**비밀번호 재사용 한도**)** 설정을 추가했습니다. 시스템은 구성 가능한 수의 이전 비밀번호에 대해 각 계정의 비밀번호 기록을 추적할 수 있습니다. 시스템은 모든 사용자가 해당 기록에 나타나는 비밀번호를 다시 사용할 수 없게 방지합니다. (셸/CLI 액세스뿐만 아니라 웹 인터페이스에도 적용됩니다.) **Max Number of Login Failures(**최대 로그인 실패 횟수**)** 및 **Set Time in Minutes to Temporarily Lockout Users(**사용자에 대한 임시 잠금 시간**(**분**)** 설정**)** 설정을 추가했습니다. 이는 시스템이 구성 가능한 시간 동안 계정을 일시적으로 차단하기 전에 사용자가 잘못된 웹 인터페이스 로그인 자격 증명을 연속적으로 입력할 수 있는 횟수를 제한하는 기능을 관리자에게 제공합니다. 신규 화면: **System(**시스템**)** > **Configuration(**설정**)** > **User Configuration(**사용자 설정**)** 지원되는 플랫폼: FMC

기능	버전	세부 사항
HTTPS 인증서	6.3	시스템과 함께 제공되는 기본 HTTPS 서버 인증서는 이제 3년 후에 자동으로 만료됩니다. 어플라이언스가 버전 6.3으로 업그레이드하기 전에 생성된 기본 서버인증서를 사용하는 경우 해당 서버 인증서는 처음 생성된 시점에서 20년 후에 만료됩니다. 기본 HTTPS 서버 인증서를 사용하는 경우 시스템은 이제 이 인증서를 갱신할 수 있는 기능을 제공합니다. 신규/수정된 화면: **System(**시스템**)** > **Configuration(**설정**)** > **HTTPS Certificate(HTTPS** 인증서**)** 페이지 > **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)** 지원되는 플랫폼: FMC, 7000 및 8000 Series 디바이스
CLI 액세스를 활성화 및 비활성화 하는 기능 FMC	6.3	신규/수정된 화면: FMC 웹 인터페이스 관리자가 사용할 수 있는 새 체크박스: **Enable CLI Access(CLI** 액세스 활성화**)**(**System(**시스템**)** > **Configuration(**구성**)**에 위치) > (**Console Configuration(**콘솔 구성**)**) 페이지 • 선택: SSH를 사용하여 FMC에 로그인하면 CLI에 액세스할 수 있습니다. • 선택 취소: SSH를 사용하여 FMC에 로그인하면 Linux 셸에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다. 버전 6.3 이전에는 **Console Configuration(**콘솔 구성**)** 페이지에 하나의 설정만 있었으며 물리적 디바이스에만 적용되었습니다. 따라서 가상 FMC에서는 **Console Configuration(**콘솔 구성**)** 페이지를 사용할 수 없었습니다. 이제 이 새로운 옵션의 추가를 통해 **Console Configuration(**콘솔 구성**)** 페이지가 물리적 디바이스 및 가상 FMC 모두에 나타납니다. 하지만 가상 FMC의 경우 이 확인란만 페이지에 나타납니다. 지원되는 플랫폼: FMC

52 장

플랫폼 설정 정책

다음 주제에서는 플랫폼 설정 정책 및 매니지드 디바이스에 이 정책을 구축하는 방법을 설명합니다.

- 플랫폼 설정 소개, 1401 페이지
- 플랫폼 설정 정책을 위한 요구 사항 및 사전 요건, 1402 페이지
- 플랫폼 설정 정책 관리, 1402 페이지
- 플랫폼 설정 정책 생성, 1403 페이지
- 플랫폼 설정 정책에 대한 대상 디바이스 설정, 1403 페이지

플랫폼 설정 소개

플랫폼 설정 정책은 시간 설정 및 외부 인증과 같이 구축의 다른 매니지드 디바이스와 유사할 가능성이 있는 매니지드 디바이스의 측면을 정의하는 기능 또는 파라미터의 공유 집합입니다.

공유 정책을 사용하면 여러 매니지드 디바이스를 한 번에 구성할 수 있으므로 구축 일관성을 유지하고 관리 작업을 간소화할 수 있습니다. 플랫폼 설정 정책을 변경하면 정책을 적용한 모든 매니지드 디바이스에 영향을 줍니다. 디바이스마다 다른 설정을 원한다고 해도 공유 정책을 생성하고 원하는 디바이스에 적용해야 합니다.

예를 들어, 조직의 보안 정책을 이용하려면 사용자가 로그인하는 경우 사용자 어플라이언스에 "무단 사용 금지" 메시지가 표시되어야 할 수 있습니다. 플랫폼 설정을 통해 플랫폼 설정 정책에서 로그인 배너를 한 번 설정할 수 있습니다.

또한 Firepower Management Center의 플랫폼 설정 정책이 유용할 수도 있습니다. 예를 들어, 다양한 상황에서 사용하는 서로 다른 메일 릴레이 호스트가 있거나 다양한 액세스 목록을 테스트하려는 경우, 단일 정책을 수정하는 대신 여러 플랫폼 설정을 생성하여 전환할 수 있습니다.

관련 항목

클래식 디바이스에 대한 플랫폼 설정 구성, 1407 페이지

시스템 구성 설정, 1341 페이지

플랫폼 설정 정책을 위한 요구 사항 및 사전 요건

모델 지원

모두, 그러나 대상 디바이스에 대해 올바른 유형의 정책을 생성해야 합니다.

- **Firepower Settings(Firepower** 설정**)**를 선택하여 클래식 관리 디바이스(ASA FirePOWER, NGIPSv, 7000 및 8000 Series)에 대한 공유 정책을 만듭니다.
- **Threat Defense Settings(Threat Defense** 설정**)**를 선택하여 Firepower Threat Defense 매니지드 디바이스에 대한 공유 정책을 만듭니다.

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

플랫폼 설정 정책 관리

플랫폼 설정 정책을 관리하려면 Platform Settings(플랫폼 설정) 페이지(**Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**)를 사용합니다. 이 페이지는 각 정책에 대한 디바이스 유형을 나타냅니다. Status(상태) 열에는 정책에 대한 장치 대상이 표시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택합니다.

단계 **2** 다음과 같이 플랫폼 설정 정책을 관리합니다.

- 생성 - 새 플랫폼 설정 정책을 생성하려면 **New Policy(**새 정책**)**를 클릭합니다. 플랫폼 설정 정책 생성, 1403 페이지 섹션을 참조하십시오.
- 복사 - 플랫폼 설정 정책을 복사하려면 복사 아이콘(복사 ( ))을 클릭합니다.
- 편집 - 기존 플랫폼 설정 정책의 설정을 수정하려면 편집 아이콘(수정( ))을 클릭합니다.
- 삭제 - 사용하지 않는 정책을 삭제하려면 삭제 아이콘(삭제( ))을 클릭하고 선택을 확인합니다.

주의 대상 디바이스에 마지막으로 구축한 정책은 최신 상태가 아니더라도 삭제할 수 없습니다. 정책을 완전히 삭제하기 전에 다른 정책을 해당 대상에 구축하는 것이 좋습니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

플랫폼 설정 정책 생성

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택합니다.

단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** 드롭다운 목록에서 디바이스 유형을 선택합니다.

- **Firepower Settings(Firepower** 설정**)**를 선택하여 클래식 관리 디바이스에 대한 공유 정책을 만듭니다.

단계 **4** 새 정책의 이름을 입력하고 선택적으로 설명을 입력합니다.

단계 **5** 선택적으로 정책을 적용할 **Available Devices(**사용 가능한 디바이스**)**를 선택하고 **Add to Policy(**정책에 추가**)**(또는 드래그 앤 드롭)를 클릭하여 선택한 디바이스를 추가합니다. **Search(**검색**)** 필드에 검색 문자열을 입력하여 디바이스 목록을 좁힐 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.
시스템이 정책을 생성하고 편집을 위해 엽니다.

단계 **7** 디바이스 플랫폼 유형에 따라 플랫폼 설정을 구성합니다.

- Firepower 설정은 클래식 디바이스에 대한 플랫폼 설정, 1405 페이지 섹션을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

플랫폼 설정 정책에 대한 대상 디바이스 설정

새 정책을 생성할 때 동시에 대상 디바이스를 추가하거나 나중에 변경할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택합니다.

단계 **2** 편집하려는 플랫폼 설정 정책 옆에 있는 수정( )을 클릭합니다.

단계 **3** **Policy Assignment(**정책 할당**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹을 정책에 할당하려면 **Available Devices(**사용 가능한 디바이스**)** 목록에서 이를 선택하고 **Add to Policy(**정책에 추가**)**를 클릭합니다. 아니면 끌어서 놓을 수도 있습니다.
- 디바이스 할당을 제거하려면 **Selected Devices(**선택한 디바이스**)** 목록의 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹 옆에 있는 삭제( )를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

53 장

클래식 디바이스에 대한 플랫폼 설정

다음 주제에서는 Firepower 플랫폼 설정 및 클래식 디바이스에서 설정하는 방법에 대해 설명합니다.

- 클래식 디바이스에 대한 플랫폼 설정 관련 정보, 1405 페이지
- 클래식 디바이스에 대한 플랫폼 설정 요구 사항, 1406 페이지
- 클래식 디바이스에 대한 플랫폼 설정 구성, 1407 페이지
- 7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성, 1416 페이지

클래식 디바이스에 대한 플랫폼 설정 관련 정보

매니지드 디바이스용 플랫폼 설정은 정책 기반이며, 따라서 같은 구성을 여러 디바이스에 적용할 수 있습니다. *Firepower* 플랫폼 설정 정책을 클래식 디바이스와 함께 사용:

- 7000/8000 시리즈 디바이스
- ASA FirePOWER 모듈
- NGIPSv

FMC의 경우에는 이러한 설정 중 상당수가 시스템 구성에서 처리됩니다. 시스템 구성, 1339 페이지 섹션을 참조하십시오.

표 ***93:*** 클래식 디바이스에 대한 ***Firepower*** 플랫폼 설정

플랫폼 설정	설명	확인
액세스 목록	특정 포트에서 시스템에 액세스할 수 있는 컴퓨터를 제어합니다.	클래식 디바이스에 대한 액세스 목록 구성, 1407 페이지
감사 로그	감사 로그를 외부 호스트로 보내도록 시스템을 구성합니다.	클래식 디바이스에서의 감사 로그 스트리밍, 1408 페이지

플랫폼 설정	설명	확인
외부 인증	외부 RADIUS, LDAP 또는 Microsoft Active Directory 저장소에 의해 인증된 7000/8000 시리즈 디바이스 사용자의 기본 사용자 권한을 설정합니다.	7000/8000 시리즈 디바이스에 대한 외부 인증 활성화, 1410 페이지
언어	7000/8000 시리즈 디바이스의 웹 인터페이스에 다른 언어를 지정합니다.	7000/8000 시리즈 웹 인터페이스 언어 설정, 1412 페이지
로그인 배너	사용자가 로그인 때 나타나는 사용자 정의 로그인 배너를 만듭니다.	클래식 디바이스에 대한 로그인 배너 맞춤 설정, 1412 페이지
셸 시간 초과	비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 분 단위로 구성합니다.	클래식 디바이스에 대한 세션 시간 초과 구성, 1414 페이지
SNMP	SNMP(Simple Network Management Protocol) 폴링을 활성화합니다.	클래식 디바이스에서의 SNMP 폴링 구성, 1415 페이지
STIG 컴플라이언스	미 국방부에서 정한 특정 요구 사항 준수 설정을 활성화합니다.	STIG 컴플라이언스, 1378 페이지
시간 동기화	시스템에 대한 시간 동기화를 관리합니다.	NTP 서버와 클래식 디바이스의 시간 동기화, 1413 페이지

클래식 디바이스에 대한 플랫폼 설정 요구 사항

라이선스 요건

없음

모델 요구 사항

모든 클래식 디바이스에 Firepower 플랫폼 설정 정책을 적용할 수 있습니다.

일부 플랫폼 설정은 7000/8000 시리즈 디바이스에만 적용되는데, 외부 인증 설정, 표시 언어, 세션 시간 초과 등의 웹 인터페이스가 있는 디바이스이기 때문입니다. 이 설정을 ASA FirePOWER나 NGIPSv에 적용하면 아무런 효과도 발생하지 않습니다.

7000/8000 시리즈 디바이스의 로컬 웹 인터페이스에 로그인해 비정책 기반 시스템 구성을 이용할 수도 있습니다. 7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성, 1416 페이지의 내용을 참조하십시오.

도메인 요구 사항

없음

모든 도메인 레벨에 Firepower 플랫폼 설정 정책을 적용할 수 있습니다.

클래식 디바이스에 대한 플랫폼 설정 구성

매니지드 디바이스용 플랫폼 설정은 정책 기반이며, 따라서 같은 구성을 여러 디바이스에 적용할 수 있습니다. Firepower 플랫폼 설정 정책을 클래식 디바이스와 함께 사용:

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

클래식 디바이스에 대한 플랫폼 설정 관련 정보, 1405 페이지 및 플랫폼 설정 정책 생성, 1403 페이지를 참조하십시오.

단계 **2** **Policy Assignment(**정책 할당**)**를 클릭하여 정책을 구축할 **Available Devices(**사용 가능한 디바이스**)**를 선택합니다.

단계 **3** 정책에 추가를 클릭(또는 끌어서 놓기)하여 선택한 디바이스를 추가합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

클래식 디바이스에 대한 액세스 목록 구성

기본적으로 Firepower 디바이스에 대한 액세스는 제한되지 않습니다. 포트 22(SSH)는 CLI 액세스를 지원합니다. 7000/8000 시리즈 디바이스의 경우, 포트 443(HTTPS)은 웹 인터페이스 액세스도 지원합니다.

더 안전한 환경에서 작동하려면, 특정 IP 주소의 액세스를 추가하는 방법을 고려하십시오. 포트 161을 통해 SNMP 정보를 폴링할 수 있는 액세스 권한을 추가할 수도 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** 액세스 목록을 클릭합니다.

단계 **3** 하나 이상의 IP 주소에 대한 액세스를 추가하려면 **Add Rules(**규칙 추가**)**를 클릭합니다.

단계 **4** **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 모두를 입력하세요.

단계 **5** **SSH**, **HTTPS**, **SNMP** 또는 이 옵션의 조합을 선택하여 이 IP 주소에 활성화할 포트를 지정합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

클래식 디바이스에서의 감사 로그 스트리밍

Firepower 어플라이언스는 사용자 상호작용의 기록(또는 감사 로그)을 생성합니다. 이러한 감사 로그를 시스템 로그나 HTTP 서버에 스트리밍할 수 있습니다. 외부 URL에 감사 정보를 보내면 시스템 성능에 영향을 미칠 수 있음에 유의하십시오.

팁 7000/8000 시리즈 디바이스에서는 디바이스의 웹 인터페이스인 시스템 감사, 449 페이지에서 감사 로그를 검토할 수도 있습니다.

감사 로그의 형식은 다음과 같습니다.

```
timestamp host [tag] appliance_name: username@ip_address, subsystem, action
```

예를 들면 다음과 같습니다.

```
Mar 01 14:45:24 localhost [FIREPOWER] MyFirepowerAppliance: admin@10.1.1.2, System >
Configuration, Page View
```

태그는 선택 사항이며 사용자가 구성할 수 있습니다. 또한 시스템 로그 이벤트에는 선택적인 기능 및 심각도가 있습니다..

시작하기 전에

감사 로그를 스트림할 서버 또는 서버 모음과 디바이스가 통신할 수 있는지 확인합니다. 시스템 로그 스트리밍의 경우, 구성을 저장할 때 시스템은 시스템 로그 서버에 연결할 수 있는지를 포트 7/UDP를 사용하여 확인합니다. 그런 다음 시스템은 포트 514/UDP를 사용 하 여 감사 로그를 스트리밍합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Audit Log(**감사 로그**)**를 클릭하여 감사 로그 스트리밍을 구성합니다.

시스템 로그 스트리밍:

a) **Send Audit Log To** 시스템 로그 를 사용으로 설정 합니다.

b) 시스템 로그 서버에 대 한 호스트 정보 (IPv4 주소 또는 정규화된 이름)를 제공 합니다.

c) **Facility(**시설**)**(시스템 로그 알림 시설, 2685 페이지) 및**Severity(**심각도**)**(Syslog 심각도 레벨, 2686 페이지)를 선택합니다.

주의 **Send Audit Log to Syslog(**시스템 로그에 감사 로그 보내기**)**를 활성화하고 호스트 정보를 제공할 경우, 시스템 로그 메시지는 감사 로그 외에 설정된 호스트로도 전송됩니다. 감사 로그에서 시스템 로그 필터링, 1409 페이지의 내용을 참조하십시오.

HTTP 스트리밍:

a) **Send Audit Log to HTTP Server(**감사 로그를 **HTTP** 서버로 전송**)**를 **Enabled(**활성화**)**로 설정합니다.

b) 감사 로그를 전송할 **URL to Post Audit(**사후 감사를 위한 **URL)**를 입력합니다. HTTPS가 지원됩니다.

URL은 다음과 같은 HTTP POST 변수를 기대하는 리스너 프로그램에 해당해야 합니다. `subsystem`, `actor`, `event_type`, `message`, `action_source_ip`, `action_destination_ip`, `result`, `time`, `tag`(제공되는 경우)

단계 **3** (선택 사항) 각 메시지에 포함할 **Tag(**태그**)**를 입력합니다. 예를 들어 Firepower 감사 로그에 **`FIREPOWER`** 라는 태그를 지정할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.
시스템 로그 스트리밍을 구성했다면, 시스템은 시스템 로그 서버에 연결할 수 있는지를 확인합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

- (선택 사항) 시스템 로그 서버로의 감사 로그 스트리밍을 활성화하고 감사 로그에서 시스템 로그 메시지를 필터링하려는 경우: 감사 로그에서 시스템 로그 필터링, 1409 페이지.

감사 로그에서 시스템 로그 필터링

Send Audit Log to Syslog(Syslog에 감사 로그 보내기**)**를 활성화하고 호스트 정보를 제공할 경우, 시스템 로그 메시지는 감사 로그 외에 설정된 호스트로도 전송됩니다. 이 동작은 Firepower 플랫폼 설정 정책을 구축할 때 `/etc/syslog-ng.d/syslog-tls.conf`가 생성되어 감사 로그만 전송하는 대신 시스템 로그 메시지가 설정된 호스트로 전달/전송됩니다.

감사 정책에 이러한 시스템 로그 레코드가 필요하지 않은 경우 해당 시스템 로그가 설정된 호스트로 스트리밍되지 않도록 할 수 있습니다. 감사 로그에서 시스템 로그를 필터링하려면 어플라이언스의 **admin** 사용자 계정에 대한 액세스 권한이 있어야 하며, 어플라이언스의 콘솔에 액세스하거나 SSH(Secure Shell)를 열 수 있어야 합니다.

⚠

주의 권한이 있는 사용자만 어플라이언스 및 **admin** 계정에 액세스할 수 있습니다.

프로시저

단계 1 `/etc/syslog-ng.conf` 파일에서 `@include "/etc/syslog-ng.d/*.conf"` 줄을 주석 처리합니다.

예제:

```
#@include "/etc/syslog-ng.d/*.conf"
```

단계 2 시스템 로그 설정 파일을 다시 로드합니다. `syslog-ng-ctl reload` 명령을 사용하여 애플리케이션을 재시작하지 않고 설정 파일을 다시 로드합니다.

예제:

```
syslog-ng-ctl reload
```

7000/8000 시리즈 디바이스에 대한 외부 인증 활성화

디바이스 플랫폼 설정을 사용하여 7000/8000 시리즈 디바이스 사용자가 로컬 데이터베이스를 사용하는 대신 LDAP 또는 RADIUS 서버에 인증하게 합니다.

시작하기 전에

외부 인증 개체를 구성합니다. 외부 인증의 내용을 참조하십시오.

프로시저

단계 1 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 2 **External Authentication(**외부 인증**)**을 클릭합니다.

단계 3 **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 4 외부에서 인증된 사용자에게 허용할 기본 권한을 정의하기 위한 사용자 역할을 **Default User Role(**기본 사용자 역할**)** 드롭다운 목록에서 선택합니다.

단계 5 외부 서버를 사용하여 CLI 또는 셸 액세스 계정도 인증하려면 **Shell Authentication(**셸 인증**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 6 CAC 인증 및 권한 부여를 활성화하려면 **CAC Authentication(CAC** 인증**)** 드롭다운 목록에서 사용 가능한 CAC 인증 개체를 선택합니다.

자세한 내용은 CAC 인증을 참고하십시오.

단계 7 사용할 각 외부 인증 개체 옆의 확인란을 선택합니다. 객체를 1개 이상 활성화하는 경우, 사용자가 지정된 순서대로 서버에 대해 확인됩니다. 다음 단계를 참조하고 서버를 재정렬합니다.

셸 인증을 활성화 하는 경우에 셸 액세스 필터를 포함 하는 외부 인증 개체를 활성화 해야 합니다. CLI/셸 액세스 사용자는 인증 객체가 목록에서 순위가 가장 높은 서버에 대해 인증할 수 있습니다.

CLI 및 CAC 인증이 모두 필요한 경우 각 용도별로 별도의 인증 개체를 사용해야 합니다.

단계 **8** (선택 사항) 위쪽 및 아래쪽 화살표를 사용해 인증 요청이 발생할 때 인증 서버에 액세스하는 순서를 변경합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

7000/8000 시리즈 디바이스에 대한 외부 인증 관련 정보

외부 인증 서버를 참조하는 인증 객체를 생성하는 경우, 매니지드 디바이스에 로그인한 사용자가 해당 서버에 대해 인증을 받도록(로컬 데이터베이스를 사용하는 대신) 외부 인증서를 활성화할 수 있습니다.

외부 인증을 활성화하면 시스템이 LDAP 또는 RADIUS 서버의 사용자에 대해 사용자 자격 증명을 확인합니다. 또한 사용자의 로컬 내부 인증이 활성화되었는데 내부 데이터베이스에 사용자 자격 증명이 없으면, 시스템은 일치하는 자격 증명 집합을 외부 서버에서 확인합니다. 여러 시스템에서 사용자의 사용자 이름이 동일하면 모든 서버에서 모든 비밀번호가 작동합니다. 그러나 사용 가능한 외부 인증 서버에서 인증이 실패하면 시스템은 로컬 데이터베이스를 다시 확인하지 않습니다.

외부 인증을 활성화하는 경우, 외부에서 계정이 인증되는 사용자에 대해 기본 사용자 역할을 설정할 수 있습니다. 역할을 결합할 수 있는 한 여러 역할을 선택할 수 있습니다. 예를 들어 회사의 Network Security 그룹의 사용자만 검색하는 외부 인증을 활성화하는 경우, Security Analyst 역할을 포함하도록 기본 사용자 역할을 설정할 수 있습니다. 그러면 추가 사용자 구성 없이도 사용자가 수집된 이벤트 데이터에 액세스할 수 있습니다. 그러나 외부 인증에서 보안 그룹 외에 다른 직원의 레코드를 검색하는 경우에는 기본 역할을 선택하지 않은 상태로 둘 수 있습니다.

액세스 역할을 선택하지 않으면 사용자는 로그인할 수 있지만 어떤 기능에도 액세스할 수 없습니다. 사용자가 로그인을 시도하면 해당 계정이 User Management 페이지**(System(**시스템**)** > **Users(**사용자**))**에 나열됩니다. 여기에서 추가 권한을 허용하도록 계정 설정을 수정할 수 있습니다.

팁 하나의 사용자 역할을 사용하도록 시스템을 구성하고 적용한 다음 나중에 다른 기본 사용자 역할을 사용하도록 구성을 수정하면, 계정을 수정하거나 삭제하고 다시 생성하기 전에는 수정 전에 생성된 사용자 계정에 첫 번째 사용자 역할이 그대로 유지됩니다.

CLI 액세스 또는 CAC 인증 및 권한 부여를 위해 LDAP 서버에 대해 인증할 수 있는 사용자 집합을 지정하려면 각각에 대해 별도의 인증 개체를 생성하여 개체를 개별적으로 활성화해야 합니다.

내부에서 인증되는 사용자가 로그인을 시도하면 시스템은 해당 사용자가 로컬 사용자 데이터베이스에 있는지를 우선 확인합니다. 사용자가 있으면 시스템은 로컬 데이터베이스에서 사용자 이름과 비밀번호를 확인합니다. 일치가 확인되면 로그인이 성공합니다. 그러나 로그인이 실패하고 외부 인증이 활성화되면 시스템은 구성에 명시된 인증 순서에 따라 각 외부 인증 서버에서 사용자를 확인합니다. 사용자 이름 및 비밀번호가 외부 서버의 결과와 일치하면 시스템은 사용자를 해당 인증 객체에 대한 기본 권한이 있는 외부 사용자로 변경합니다.

외부 사용자가 로그인을 시도하면 시스템은 외부 인증 서버에 대해 사용자 이름과 비밀번호를 확인합니다. 일치가 확인되면 로그인이 성공합니다. 로그인이 실패하면 사용자 로그인 시도가 거절됩니다. 외부 사용자는 로컬 데이터베이스의 사용자 목록을 기준으로 인증할 수 없습니다. 사용자가 새로운 외부 사용자이면 외부 인증 객체로부터의 기본 권한과 함께 로컬 데이터베이스에 외부 사용자 계정이 생성됩니다.

7000/8000 시리즈 웹 인터페이스 언어 설정

여기서 지정하는 언어는 로그인하는 모든 사용자에 대한 웹 인터페이스에 사용됩니다. 다음 언어를 선택할 수 있습니다.

- 영어
- 일본어

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Language**를 클릭합니다.

단계 **3** 사용하려는 언어를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

클래식 디바이스에 대한 로그인 배너 맞춤 설정

클래식 디바이스의 CLI 로그인 배너를 사용자 지정할 수 있습니다. 7000/8000 시리즈 디바이스의 경우 로그인 배너는 웹 인터페이스에도 표시됩니다. 로그인 배너가 너무 크거나 오류가 발생하면, 시스템에서 배너를 표시하려고 시도할 때 CLI 세션이 실패할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Login Banner(**로그인 배너**)**를 선택합니다.

단계 **3** **Custom Login Banner(**사용자 정의 로그인 배너_ 필드에서 사용하려는 로그인 배너 텍스트를 입력합니다.

시스템은 탭 간격을 유지하지 않습니다.

단계 4 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

NTP 서버와 클래식 디바이스의 시간 동기화

Firepower Management Center 및 매니지드 디바이스에서 시스템 시간을 동기화하는 작업은 성공적인 작업을 위해 반드시 필요합니다.구축에 FTD 디바이스가 포함된다면 Threat Defense를 위한 NTP 시간 동기화 구성, 1463 페이지의 내용을 참조하십시오.

디바이스는 NTPv4를 지원합니다.

⚠

주의 시간이 FMC 및 매니지드 디바이스 간에 동기화되지 않으면 의도하지 않은 결과가 발생할 수 있습니다.

구축이 끝나면, 매니지드 디바이스를 구성된 NTP 서버와 동기화하는 데 몇 분 정도 걸릴 수 있습니다.

시작하기 전에

사용하려는 NTP 서버 또는 서버 모음과 통신할 수 있는지 확인합니다. 다음 중 하나를 수행할 수 있습니다.

- (권장) FMC와 동일한 NTP 서버인 FMC의 시간을 NTP 서버와 동기화, 1380 페이지을(를) 사용합니다.

  FMC와 NTP 서버 간의 보안 연결을 구성하더라도(인증된 **NTP** 서버만 사용), 해당 서버에 대한 디바이스 연결은 인증을 사용하지 않습니다.

  이 옵션을 선택하면 디바이스가 설정된 NTP 서버에서 직접 시간을 가져옵니다. 어떤 이유로든 디바이스의 설정된 NTP 서버에 연결할 수 없는 경우, 시간을 FMC와 동기화합니다.

- 디바이스가 NTP 서버에 연결할 수 없거나 조직에 NTP 서버가 없는 경우에는 다음 절차에 설명된 대로 **Via NTP from Management Center(**관리 센터에서 **NTP**를 통해**)** 옵션을 사용해야 합니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 2 **Time Synchronization(**시간 동기화**)**을 클릭합니다.

단계 3 시간이 동기화되는 방법을 지정합니다.

- **Via NTP from(NTP**를 통해**)** - Firepower Management Center가 네트워크에서 NTP 서버를 사용 중인 경우, 이 옵션을 선택하고 정규화된 DNS 이름(예: ntp.example.com) 또는 FMC의 **System(**시스템**) > Configuration(**구성**) > Time Synchronization(**시간 동기화**)**에서 지정한 동일한 NTP 서버의 IPv4 또는 IPv6 주소를 입력합니다. NTP 서버에 연결할 수 없는 경우, Firepower Management Center는 NTP 서버로 작동합니다.
- **Via NTP from Management Center(**관리 센터에서 **NTP**를 통해**)**: (기본값) 매니지드 디바이스는 Firepower Management Center에 대해 설정한 NTP 서버에서 시간을 가져오고 (인증된 NTP 서버 제외) 시간을 해당 서버와 직접 동기화합니다. 그러나 다음 중 하나라도 해당하는 경우, 매니지드 디바이스는 Firepower Management Center에서 시간을 동기화합니다.
  - 디바이스에서 Firepower Management Center의 NTP 서버에 연결할 수 없습니다.
  - Firepower Management Center에 인증되지 않은 서버가 없습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

클래식 디바이스에 대한 세션 시간 초과 구성

무인 로그인 세션은 보안 위험이 될 수 있습니다. 비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 구성할 수 있습니다. 최대값은 24시간 또는 1440분입니다.

프로시저

단계 **1** **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **Shell Timeout(**셸 시간 초과**)**를 클릭합니다.

단계 **3** 셸 시간 제한**(**분**)**을 입력합니다.

단계 **4** 세션 시간 제한 구성

- 웹 인터페이스(7000/8000 시리즈에만 해당): 브라우저 세션 시간 제한**(**분**)**을 입력합니다.

  시스템을 오랫동안 패시브 방식으로 안전하게 모니터링하려는 상황이라면, 특정 웹 인터페이스 사용자를 시간 제한에서 제외할 수 있습니다. 자세한 내용은 사용자 어카운트 로그인 옵션를 참고하십시오.

- CLI: 셸 시간 제한**(**분**)**을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

클래식 디바이스에서의 **SNMP** 폴링 구성

단순 네트워크 관리 프로토콜(SNMP) 폴링을 이용하면 연락처, 관리, 위치, 서비스 정보, IP 주소 지정 및 라우팅 정보, 전송 프로토콜 사용 통계 등의 시스템 세부 사항을 포함하는, Firepower 디바이스의 표준 MIB(management information base)에 액세스할 수 있습니다. 7000/8000 시리즈 디바이스에 대한 추가 MIB는 물리적 인터페이스, 논리적 인터페이스, 가상 인터페이스, ARP, NDP, 가상 브리지, 가상 라우터 등을 통과하는 트래픽에 대한 통계를 포함합니다. SNMP 폴링을 활성화한다고 해서 시스템에서 SNMP 트랩을 전송하지는 않습니다. MIB의 정보를 네트워크 관리 시스템을 통한 폴링에 사용할 수 있도록 지원할 뿐입니다.

시스템은 SNMPv1, v2 및 v3을 지원합니다. SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3은 읽기 전용 사용자만 지원합니다. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

시작하기 전에

시스템 폴링에 사용할 각 컴퓨터에 대해 SNMP 액세스를 추가합니다. 클래식 디바이스에 대한 액세스 목록 구성, 1407 페이지의 내용을 참조하십시오.

참고 SNMP MIB에는 구축을 공격하는 데 사용할 수 있는 정보가 있습니다. Cisco에서는 MIB를 폴링하는 데 사용하는 특정 호스트에 대한 SNMP 액세스용 액세스 목록을 제한할 것을 권장합니다. 또한 SNMPv3을 사용하고 네트워크 관리 액세스에 강력한 비밀번호를 사용할 것도 권장합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 **2** **SNMP**를 클릭합니다.

단계 **3** **SNMP Version(SNMP** 버전**)** 드롭다운 목록에서, 사용할 SNMP 버전을 선택합니다.

- **Version(**버전**) 1** 또는 **Version(**버전**) 2**: 커뮤니티 문자열 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뜁니다.

  참고 SNMP 커뮤니티 문자열 이름에는 특수문자(< > / % # & ? ', 등)를 포함하지 않습니다.

- **Version 3(**버전 **3)**: **Add User(**사용자 추가**)**를 클릭하여 사용자 정의 페이지를 표시합니다. SNMPv3는 읽기 전용 사용자 및 AES128 암호화만 지원합니다.

단계 **4** 사용자 이름을 입력합니다.

단계 **5** **Authentication Protocol(**인증 프로토콜**)** 드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.

단계 **6** **Authentication Password(**인증 비밀번호**)** 필드에 SNMP 서버와 함께 인증에 필요한 비밀번호를 입력합니다.

단계 **7** **Verify Password(**비밀번호 확인**)** 필드에 인증 비밀번호를 다시 입력합니다.

단계 **8** 사용할 비공개 프로토콜을 **Privacy Protocol** 목록에서 선택하거나, 비공개 프로토콜을 사용하지 않으려면 **None**을 선택합니다.

단계 **9** **Privacy Password(**프라이버시 비밀번호**)** 필드에 SNMP 서버에 필요한 SNMP 프라이버시 키를 입력합니다.

단계 **10** **Verify Password(**비밀번호 확인**)** 필드에 프라이버시 비밀번호를 다시 입력합니다.

단계 **11** **Add(**추가**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성

7000/8000 시리즈 디바이스의 로컬 웹 인터페이스에 로그인해 비정책 기반 시스템 구성을 이용할 수 있습니다. 이러한 구성은 대부분 병렬 FMC 시스템 구성으로, FMC 시스템 구성 장인 시스템 구성, 1339 페이지에서 설명합니다.

표 ***94: 7000/8000*** 시리즈 디바이스에 대한 로컬 시스템 구성

시스템 구성	설명	확인
검증 번경	지난 24시간 동안의 시스템 변경 사항에 대한 상세한 보고서를 전송합니다.	검증 번경, 1367 페이지
콘솔 구성	VGA 또는 시리얼 포트나 LOM(Lights-Out Management)을 통한 콘솔 액세스를 구성합니다.	원격 콘솔 액세스 관리, 1390 페이지
HTTPS 인증서	필요하다면 신뢰된 권한 및 업로드 인증서에서 시스템에 HTTPS 서버 인증서를 요청합니다.	HTTPS 인증서, 1344 페이지
정보	어플라이언스에 대한 현재 정보를 보고 표시 이름을 편집합니다.	어플라이언스 정보, 1343 페이지
Management Interfaces(관리 인터페이스)	어플라이언스의 IP 주소, 호스트 이름 및 프록시 설정과 같은 옵션을 변경합니다.	7000/8000 시리즈 디바이스의 관리 인터페이스 구성, 1417 페이지
프로세스	Firepower 프로세스를 종료, 리부팅 또는 다시 시작합니다.	7000/8000 시리즈 디바이스 종료 또는 재시작, 1421 페이지

시스템 구성	설명	확인
패킷 전송 금지	낮은 대역폭 구축에서 7000/8000 시리즈 디바이스의 패킷 데이터를 FMC로 전송하지 않도록 설정합니다.	FMC로의 패킷 전송 금지, 1417 페이지
시간	현재 시간 설정을 봅니다.	7000/8000 시리즈 디바이스의 시스템 시간 보기, 1422 페이지

FMC로의 패킷 전송 금지

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
해당 없음	Any(모든)	7000 및 8000 Series	해당 없음	Admin(관리자)

침입 정책 위반을 유발한 패킷의 특정 콘텐츠를 염려하지 않는다면, 저대역폭 구축에서는 7000 또는 8000 Series 디바이스에서 Firepower Management Center(으)로의 패킷 데이터 전송을 해제하는 것이 좋습니다.

프로시저

단계 **1** 7000 또는 8000 Series 디바이스의 로컬 웹 인터페이스에서 **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Information(**정보**)**을 클릭합니다.

단계 **3** **Prohibit Packet Transfer to the Management Center(Management Center**에 대한 패킷 전송 금지**)**를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

7000/8000 시리즈 디바이스의 관리 인터페이스 구성

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
해당 없음	Any(모든)	7000 및 8000 Series	전역만 해당	Admin(관리자)

웹 인터페이스를 사용하여 매니지드 디바이스의 관리 인터페이스 설정을 수정합니다. 모델에서 지원하는 경우 이벤트 인터페이스를 선택적으로 활성화할 수 있습니다. 관리 인터페이스에 대한 자세한 내용은 디바이스 관리 인터페이스, 299 페이지 섹션을 참조하십시오.

⚠

주의 관리 인터페이스를 변경할 때는 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 디바이스 콘솔 포트에 액세스하여 CLI에서 설정을 재구성해야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Configuration(**구성**)**을 선택한 다음 **Management Interface(**관리 인터페이스**)**를 선택합니다.

단계 **2** **Interfaces(**인터페이스**)** 영역에서 구성하려는 인터페이스 옆에 있는 **Edit(**편집**)**를 클릭합니다.

이 섹션에는 사용 가능한 모든 인터페이스가 나열되어 있습니다. 다른 인터페이스를 추가할 수 없습니다.

각 관리 인터페이스에서 다음 옵션을 구성할 수 있습니다.

- **Enabled(**활성화됨**)** - 관리 인터페이스를 활성화합니다. 기본 eth0 관리 인터페이스를 비활성화하지 마십시오. 일부 프로세스에는 eth0 인터페이스가 필요합니다.
- **Channels(**채널**)** - (8000 Series에만 해당) 이벤트 전용 인터페이스를 구성합니다. 8000 Series의 eth1 관리 인터페이스를 이벤트 인터페이스로 사용하도록 활성화할 수 있습니다. 이렇게 하려면 **Management Traffic(**관리 트래픽**)** 확인란을 선택 취소하고 **Event Traffic(**이벤트 트래픽**)** 확인란을 선택한 상태로 유지합니다. eth0 관리 인터페이스의 경우 두 확인란을 모두 선택 상태로 둡니다.

  Firepower Management Center 이벤트 전용 인터페이스는 관리 채널 트래픽을 허용할 수 없으므로 디바이스 이벤트 인터페이스에서 관리 채널을 비활성화해야 합니다.

  관리 인터페이스에 대한 **Event Traffic(**이벤트 트래픽**)**을 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다.

  인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.
- **Mode(**모드**)** - 연결 모드를 지정합니다. GigabitEthernet 인터페이스의 경우 자동 협상에 대한 변경 사항은 무시됩니다.
- **MTU** - 최대 전송 단위(MTU)를 설정합니다. 기본값은 1500입니다. MTU 설정 가능 범위는 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

  시스템은 구성된 MTU 값에서 자동으로 18바이트를 잘라내므로 1298 아래의 값은 최소 IPv6 MTU 설정인 1280을 준수하지 못하며 594 아래의 값은 최소 IPv4 MTU 설정인 576을 준수하지 못합니다. 예를 들면 시스템은 구성된 값 576을 자동으로 558로 자릅니다.
- **MDI/MDIX** - **Auto-MDIX**를 설정합니다.
- **IPv4 Configuration(IPv4** 구성**)** - IPv4 IP 주소를 설정합니다. 선택:
  - **Static(**정적**)** - 수동으로 **IPv4 Management IP(IPv4** 관리 **IP)** 주소 및 **IPv4 Netmask(IPv4** 넷마스크**)**를 입력합니다.
  - **DHCP** - DHCP를 사용하도록 인터페이스를 설정합니다(eth0 전용).
  - **Disabled(**비활성화됨**)** - IPv4를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
- **IPv6 Configuration(IPv6** 구성**)** - IPv6 IP 주소를 설정합니다. 선택:

- **Static(**정적**)** - 수동으로 **IPv6 Management IP(IPv6** 관리 **IP)** 주소 및 **IPv6 Prefix Length(IPv6** 프리픽스 길이**)**를 입력합니다.
- **DHCP** - DHCPv6를 사용하도록 인터페이스를 설정합니다(eth0 전용).
- **Router Assigned(**라우터 할당**)** - 상태 비저장 자동 구성을 활성화합니다.
- **Disabled(**비활성화됨**)** - IPv6를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
- **IPv6 DAD** - IPv6을 활성화할 때 DAD(Duplicate Address Detection)를 활성화 또는 비활성화합니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다.

단계 **3** **Routes(**경로**)** 영역에서 수정( )을 클릭하여 정적 경로를 편집하거나 추가( )를 클릭하여 경로를 추가합니다. 보기 ( )를 클릭하여 경로 통계를 봅니다.

참고 Firepower Management Center가 원격 네트워크에 있는 경우 이벤트 전용 인터페이스에 정적 경로를 추가해야 합니다. 그렇지 않으면 모든 트래픽이 관리 인터페이스를 통해 기본 경로와 일치하게 됩니다. 기본 경로의 경우 게이트웨이 IP 주소만 변경할 수 있습니다. 기본 경로는 항상 eth0 인터페이스를 사용합니다. 라우팅에 대한 내용은 디바이스 관리 인터페이스의 네트워크 라우트, 301 페이지 섹션을 참조하십시오.

정적 경로에 대해 다음 설정을 구성할 수 있습니다.

- **Destination(**대상**)** - 경로를 생성할 네트워크의 대상 주소를 설정합니다.
- **Netmask(**넷마스크**)** 또는 **Prefix Length(**프리픽스 길이**)** - 네트워크의 넷마스크(IPv4) 또는 프리픽스 길이(IPv6)를 설정합니다.
- **Interface(**인터페이스**)** - 이그레스 관리 인터페이스를 설정합니다.
- **Gateway(**게이트웨이**)** - 게이트웨이 IP 주소를 설정합니다.

단계 **4** **Shared Settings(**공유 설정**)** 영역의 모든 인터페이스에서 공유하는 네트워크 파라미터를 설정합니다.

참고 eth0 인터페이스에 **DHCP**를 선택한 경우 DHCP 서버에서 파생된 일부 공유 설정을 수동으로 지정할 수 없습니다.

다음 공유 설정을 구성할 수 있습니다.

- **Hostname(**호스트네임**)** - 디바이스 호스트네임을 설정합니다. 호스트네임을 변경하는 경우 새 호스트네임을 시스템 로그 메시지에 반영하려면 디바이스를 리부팅합니다. 시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.
- **Domains(**도메인**)** - 디바이스에 대한 검색 도메인을 쉼표로 구분하여 설정합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.

- **Primary DNS Server(**기본 **DNS** 서버**)**, **Secondary DNS Server(**보조 **DNS** 서버**)Tertiary DNS Server(3**차 **DNS** 서버**)** - 환경설정 순서대로 사용할 DNS 서버를 설정합니다.
- **Remote Management Port(**원격 관리 포트**)** - FMC와의 통신을 위한 원격 관리 포트를 설정합니다. FMC 및 매니지드 디바이스는 기본적으로 포트 8305에 있는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

  참고 Cisco에서는 원격 관리 포트에 대해 기본 설정을 유지할 것을 적극 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 디바이스의 설정을 변경해야 합니다.

단계 **5** **ICMPv6** 영역에서 ICMPv6 설정을 구성합니다.

- **Allow Sending Echo Reply Packets(**에코 응답 패킷 전송 허용**)** - 에코 응답 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 디바이스 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.
- **Allow Sending Destination Unreachable Packets(**대상에 연결할 수 없는 패킷 전송 허용**)** - 대상에 연결할 수 없는 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다.

단계 **6** **LCD Panel(LCD** 패널**)** 영역에서 **Allow reconfiguration of network settings(**네트워크 설정의 재구성 허용**)** 확인란을 선택하여 디바이스의 LCD 패널을 통해 네트워크 설정 변경을 활성화합니다.

디바이스에 대한 IP 주소를 편집하려면 LCD 패널을 사용할 수 있습니다. 변경 사항이 관리되는 Firepower Management Center에 반영되었는지 확인합니다. 경우에 따라 Firepower Management Center에서 수동으로 데이터를 업데이트해야 할 수도 있습니다.

주의 LCD 패널을 사용한 재구성을 허용할 경우 보안 위험에 노출될 수 있습니다. LCD 패널을 사용하여 네트워크 설정을 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다. 이 옵션을 활성화하면 보안 문제가 발생할 수 있다는 경고 메시지가 표시됩니다.

단계 **7** **Proxy(**프록시**)** 영역에서 HTTP 프록시 설정을 구성합니다.

디바이스는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다.

참고 NTLM(NT LAN Manager) 인증을 사용하는 프록시는 지원되지 않습니다.

a) **Enable(**활성화**)** 확인란을 선택합니다.
b) 프록시 서버의 IP 주소 또는 정규화된 도메인 이름을 **HTTP Proxy(HTTP** 프록시**)** 필드에 입력합니다.
c) **Port(**포트**)** 필드에서 포트 번호를 입력합니다.
d) **Use Proxy Authentication(**프록시 인증 사용**)**을 선택하여 인증 자격 증명을 제공하고 **User Name(**사용자 이름**)** 및 **Password(**비밀번호**)**를 제공합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** 관리 IP 주소를 변경하는 경우 FMC 및 매니지드 디바이스 간의 통신에 영향을 미칠 수 있습니다.

IP 주소를 변경해도 현재 연결에는 영향을 주지 않습니다. 하지만 디바이스 또는 FMC가 다시 로드되면 연결을 다시 설정해야 합니다. 피어의 올바른 IP 주소를 사용하려면 적어도 하나의 디바이스(FMC 또는 매니지드 디바이스)가 필요합니다. 예를 들어 디바이스 설정 중 IP 주소 대신 FMC에 대한 NAT ID를 지정했고 디바이스에 추가할 때 FMC에 정의한 디바이스 IP 주소가 잘못되는 경우 FMC가 통신을 다시 설정할 수 없게 됩니다 . 이 경우 FMC에서 디바이스의 관리 IP 주소를 변경해야 합니다. FMC에서 호스트 이름 또는 IP 주소 업데이트 , 317 페이지 섹션을 참조하십시오.

7000/8000 시리즈 디바이스 종료 또는 재시작

프로시저

단계 **1** 디바이스의 웹 인터페이스에서 **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Process(**프로세스**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

종료	**Shutdown Appliance(**어플라이언스 종료**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 주의 전원 버튼을 사용하여 Firepower 어플라이언스를 종료하지 마십시오. 데이터가 손실될 수 있습니다. 웹 인터페이스(또는 CLI)를 사용하여 구성 데이터 손실 없이 시스템의 전원을 안전하게 끄고 재시작할 수 있도록 준비합니다.
재부팅	**Reboot Appliance(**어플라이언스 리부팅**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 참고 리부팅하면 로그아웃되며, 완료하는 데 최대 1시간이 소요될 수 있는 데이터베이스 검사가 실행됩니다.
콘솔 재시작	**Restart Appliance Console(**어플라이언스 콘솔 재시작**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다.
Snort 프로세스 다시 시작	**Restart Snort(Snort** 다시 시작**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 주의 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 디바이스의 구성 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지를 참조하십시오.

7000/8000 시리즈 디바이스의 시스템 시간 보기

시간 설정이 대부분의 페이지에서 로컬 시간으로 표시됩니다. 여기서 사용되는 시간대는 User Preferences(사용자 환경 설정)의 Time Zone(표준 시간대) 페이지에서 설정하며, UTC 시간을 사용해 어플라이언스에 저장합니다. 또한 현재 시간은 Time Synchronization(시간 동기화) 페이지 상단에 UTC로 표시됩니다(로컬 시간은 활성화한 경우 Manual(수동) 시계 설정 옵션으로 표시됨).

제한

Time Zone(표준 시간대) 기능(User Preferences(사용자 환경 설정))에서는 기본 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 이 설정은 변경하지 마십시오**.** 시스템 시간을 UTC 이외로 변경하는 것은 지원되지 않으며, 디바이스를 이미지로 다시 설치해야 합니다.

7000 및 8000 Series 디바이스의 시스템 시간 정보를 확인하려면 이 절차를 사용합니다.

프로시저

단계 **1** 디바이스의 웹 인터페이스에 로그인하고 **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Time(**시간**)**을 클릭합니다.

NTP를 사용한다면 NTP 서버 상태, 1384 페이지 섹션을 참조하십시오.

54 장

Firepower Threat Defense 플랫폼 설정

FTD 디바이스의 플랫폼 설정은 값을 여러 디바이스 간에 공유하려고 할 수 있는 비 관련 기능을 구성합니다. 디바이스마다 다른 설정을 원한다고 해도 공유 정책을 생성하고 원하는 디바이스에 적용해야 합니다.

- ARP 검사 설정, 1423 페이지
- 배너 설정, 1425 페이지
- DNS 구성, 1425 페이지
- 프래그먼트 처리 설정, 1427 페이지
- HTTP 설정, 1428 페이지
- ICMP 액세스 규칙 구성, 1429 페이지
- SSL 설정 , 1431 페이지
- 에서 SSH(Secure Shell) 설정, 1435 페이지
- SMTP 설정, 1437 페이지
- Threat Defense에 대한 SNMP 설정, 1437 페이지
- 시스템 로그 구성 관련 정보, 1445 페이지
- 전역 시간 제한 구성, 1461 페이지
- Threat Defense를 위한 NTP 시간 동기화 구성, 1463 페이지
- 정책 애플리케이션에 대한 디바이스 표준 시간대 구성, 1464 페이지
- Firepower Threat Defense 플랫폼 설정 기록, 1465 페이지

ARP 검사 설정

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 간에 허용됩니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다.

ARP 감시 기능은 악의적인 사용자가 다른 호스트 또는 라우터로 위장(ARP 스푸핑이라고도 함)하는 것을 방지합니다. ARP 스푸핑은 "끼어들기" 공격을 활성화할 수 있습니다. 예를 들어, 호스트에서 ARP 요청을 게이트웨이 라우터에 전송할 경우 해당 게이트웨이 라우터는 게이트웨이 라우터 MAC 주소에 응답합니다. 그러나 공격자는 라우터 MAC 주소가 아닌 공격자 MAC 주소가 포함된 다른 ARP 응답을 호스트에 전송합니다. 이제 공격자는 라우터에 트래픽이 전달되기 전에 모든 호스트 트래픽을 가로챌 수 있게 됩니다.

ARP 감시 기능은 고정 ARP 테이블에 올바른 MAC 주소와 관련 IP 주소를 입력하기만 하면 공격자가 공격자 MAC 주소가 포함된 ARP 응답을 보낼 수 없도록 합니다.

ARP 감시를 활성화할 경우 Firepower Threat Defense 디바이스에서는 MAC 주소, IP 주소, 모든 ARP 패킷의 소스 인터페이스를 ARP 테이블의 고정 항목과 비교하고 다음과 같은 조치를 취합니다.

- IP 주소, MAC 주소, 소스 인터페이스가 ARP 항목과 일치하면 패킷이 통과됩니다.
- MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 Firepower Threat Defense 디바이스에서는 패킷을 누락시킵니다.
- ARP 패킷이 고정 ARP 테이블의 어느 항목과도 일치하지 않으면 Firepower Threat Defense 디바이스를 설정하여 패킷을 모든 인터페이스로 전달(플러딩)하거나 패킷이 누락되도록 합니다.

참고 전용 진단 인터페이스는 이 파라미터가 플러딩을 실행하도록 설정된 경우에도 패킷을 플러딩하지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **ARP Inspection(ARP** 검사**)**을 선택합니다.

단계 **3** ARP 검사 테이블에 항목을 추가합니다.

a) **Add(**추가**)**를 클릭하여 새 항목을 만들거나 항목이 이미 있는 경우 **Edit(**편집**)**를 클릭합니다.

b) 원하는 옵션을 선택합니다.

- **Inspect Enabled(**검사 활성화**)** - 선택한 인터페이스 및 영역에서 ARP 검사를 수행할 수 있습니다.
- **Flood Enabled(**플러드 활성화**)** - 정적 ARP 항목과 일치하지 않는 ARP 요청이 원래 인터페이스 또는 전용 관리 인터페이스 이외의 모든 인터페이스로 플러딩될지 여부입니다. 이는 기본 동작입니다.

  ARP 요청을 플러딩하도록 선택하지 않으면 정적 ARP 항목과 정확히 일치하는 요청만 허용됩니다.
- **Security Zones(**보안 영역**)** - 선택한 작업을 수행하는 인터페이스를 포함하는 영역을 추가합니다. 영역은 전환된 영역이어야 합니다. 영역에 없는 인터페이스의 경우 선택한 Selected Security Zone(보안 영역 목록) 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** 고정 ARP 항목 추가, 839 페이지에 따라 고정 ARP 항목을 추가합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

배너 설정

사용자가 장치 명령줄 인터페이스(CLI)에 연결할 때 이를 표시하도록 메시지를 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Banner(**배너**)**를 선택합니다.

단계 **3** 배너를 구성합니다.

다음은 배너에 대한 몇 가지 팁과 요구 사항입니다.

- ASCII 문자만 허용됩니다. 줄바꿈(Enter를 누름)을 사용할 수 있지만 탭은 사용할 수 없습니다.
- 변수 **$(hostname)** 또는 **$(domain)**를 포함하여 디바이스의 호스트네임 또는 도메인 이름을 동적으로 추가할 수 있습니다.
- 배너에 대한 절대적인 길이 제한은 없지만 배너 메시지를 처리할 수 있는 시스템 메모리가 충분하지 않으면 텔넷 또는 SSH 세션이 닫힙니다.
- 보안의 관점에서는 배너에서 무단 액세스를 방지하는 것이 중요합니다. 침입자를 초대하는 것처럼 보이는 "환영" 또는 "부탁"에 해당하는 단어를 사용하지 마십시오. 다음 배너는 무단 액세스에 대해 올바른 톤을 설정합니다.

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

DNS 구성

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. 서로 다른 트래픽 유형에 적용되는 두 가지 DNS 서버 설정(데이터 및 특수 관리 트래픽)이 있습니다. 데이터 트래픽에는 액세스 제어 규칙 및 원격 액세스 VPN과 같이 DNS 조회가 필요한 FQDN을 사용하는 모든 서비

스가 포함됩니다. 특수 관리 트래픽에는 FMC 관리 및 데이터베이스 업데이트와 같은 관리 인터페이스에서 발생하는 트래픽이 포함됩니다. 이 절차는 데이터 DNS 서버에만 적용됩니다. 관리 DNS 설정은 CLI **configure network dns servers** 및 **configure network dns searchdomains** 명령을 참조하십시오.

DNS 서버 통신에 대한 올바른 인터페이스를 결정하기 위해 FTD는 라우팅 조회를 사용하지만, 사용되는 라우팅 테이블은 DNS를 활성화하는 인터페이스에 따라 다릅니다. 자세한 내용은 아래 인터페이스 설정을 참조하십시오.

시작하기 전에

- DNS 서버 그룹을 만들었는지 확인합니다. 자세한 내용은 DNS 서버 그룹 개체 생성, 637 페이지 섹션을 참조해 주십시오.
- FTD에 DNS 서버에 액세스하기 위한 적절한 정적 또는 동적 경로가 있는지 확인합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Threat Defense 정책을 생성하거나 수정합니다.

단계 **2** **DNS**를 클릭합니다.

단계 **3** **Enable DNS name resolution by device(**디바이스로 **DNS** 이름 확인 활성화**)**를 선택합니다.

단계 **4** 이미 생성한 **DNS Server Group(DNS** 서버 그룹**)**을 선택합니다.

단계 **5** (선택 사항) **Expiry Entry Timer(**만료 입력 타이머**)** 및 **Poll Timer(**폴링 타이머**)** 값을 분 단위로 입력합니다.

- 만료 입력 타이머는 TTL(Time-To-Live)이 만료된 후 DNS 조회 테이블에서 확인된 FQDN의 IP 주소를 제거하는 시간 제한을 지정합니다. 항목 제거 시 테이블을 다시 컴파일해야 하므로 자주 제거하면 디바이스의 처리 부하가 증가할 수 있습니다. 이 설정은 가상으로 TTL을 확장합니다.
- 폴링 타이머는 네트워크 개체 그룹에 정의된 FQDN을 확인하기 위해 디바이스가 DNS 서버를 쿼리한 후 시간 제한을 지정합니다. FQDN은 폴링 타이머가 만료된 때와 확인된 IP 엔트리의 TTL이 만료된 때 중 더 빠른 시점에 정기적으로 확인됩니다.

참고 FQDN 확인의 첫 번째 인스턴스는 FQDN 개체가 액세스 제어 정책에 배포될 때 발생합니다.

단계 **6** 모든 인터페이스 또는 특정 인터페이스에서 DNS 조회를 활성화합니다. 이러한 선택은 사용되는 라우팅 테이블에도 영향을 미칩니다.

인터페이스에서 DNS 조회를 활성화하는 것은 조회를 위해 소스 인터페이스를 지정하는 것과 다릅니다. FTD는 항상 경로 조회를 사용하여 소스 인터페이스를 결정합니다.

- 인터페이스를 선택하지 않음 - 관리 및 관리 전용 인터페이스를 포함하여 모든 인터페이스에서 DNS 조회를 활성화합니다. FTD는 데이터 라우팅 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- 특정 인터페이스 선택 진단 인터페이스를 통한 **DNS** 조회 활성화 옵션 - 지정된 인터페이스에서 DNS 조회를 활성화합니다. FTD는 데이터 라우팅 테이블만 확인합니다.

- 특정 인터페이스 선택 진단 인터페이스를 통한 **DNS** 조회 활성화 옵션 - 지정된 인터페이스 및 진단 인터페이스에서 DNS 조회를 활성화합니다. FTD는 데이터 라우팅 테이블을 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- 진단 인터페이스를 통한 **DNS** 활성화 옵션만 - 진단에서 DNS 조회를 활성화합니다. FTD는 관리 전용 라우팅 테이블만 확인합니다.**Devices(**디바이스**)Device Management(**디바이스 관리**) edit device(**디바이스 수정**)Interfaces(**인터페이스**)** 페이지에서 진단 인터페이스의 IP 주소를 설정해야 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

액세스 제어 규칙에 FQDN 개체를 사용하려면 액세스 제어 규칙에 할당할 수 있는 FQDN 네트워크 개체를 만듭니다. 자세한 내용은 네트워크 개체 생성, 571 페이지 섹션을 참조하십시오.

프래그먼트 처리 설정

기본적으로 FTD 디바이스는 IP 패킷당 최대 24개의 프래그먼트를 허용하고 재조립 작업에 대기 중인 최대 200개의 프래그먼트를 허용합니다. UDP를 통한 NFS와 같이 일상적으로 패킷을 프래그먼트하는 애플리케이션이 있는 경우 네트워크에 프래그먼트가 필요할 수도 있습니다. 그러나 트래픽을 단편화하는 애플리케이션이 없으면 **Chain(**체인**)**을 1로 설정하여 프래그먼트를 허용하지 않는 것이 좋습니다. 단편화된 패킷은 종종 서비스 거부(DoS) 공격으로 사용됩니다.

참고 이 설정은 이 정책에 할당된 디바이스의 기본값을 설정합니다. 인터페이스 구성에서 **Override Default Fragment Setting(**기본 프래그먼트 설정 재정의**)**을 선택하여 디바이스의 특정 인터페이스에 대해 이 설정을 재정의할 수 있습니다. 인터페이스를 편집할 때 **Advanced(**고급**)** > **Security Configuration(**보안 구성**)**에서 옵션을 찾을 수 있습니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 편집한 다음 **Interfaces(**인터페이스**)**를 선택하여 인터페이스 속성을 편집합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Fragment Settings(**프래그먼트 설정**)**를 선택합니다.

단계 **3** 다음 옵션을 구성합니다. 기본 설정을 사용하려면 **Reset to Defaults(**기본값으로 재설정**)**를 클릭합니다.

- **Size(Block)(**크기**(**블록**))** - 재조립에 대해 대기할 수 있는 모든 연결에서 패킷 프래그먼트의 최대 수입니다. 기본값은 200 프래그먼트입니다.

- **Chain (Fragment)(**체인**(**프래그먼트**))** - 전체 IP 패킷을 단편화할 수 있는 최대 패킷 수입니다. 기본값은 24패킷입니다. 프래그먼트를 허용하지 않으려면 이 옵션을 1로 설정합니다.
- **Timeout (Sec)(**시간 초과**(**초**))** - 단편화된 전체 패킷이 도착할 때까지 기다리는 최대 시간(초)입니다. 기본값은 5일입니다. 이 시간 내에 모든 프래그먼트가 수신되지 않으면 모든 프래그먼트가 삭제됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

HTTP 설정

FTD 디바이스의 하나 이상의 인터페이스에 HTTPS 연결을 허용하려면 HTTPS 설정을 구성합니다. HTTPS를 사용하여 문제 해결을 위해 패킷 캡처를 다운로드할 수 있습니다.

시작하기 전에

- Firepower Management Center를 사용하여 FTD를 관리하면 FTD에 대한 HTTPS 액세스는 패킷 캡처 파일을 보는 용도로만 사용됩니다. FTD에는 이 관리 모드에서 구성할 웹 인터페이스가 없습니다.
- HTTPS 로컬 사용자는 **configure user add** 명령을 사용하여 CLI에서만 구성할 수 있습니다. 기본적으로 초기 설정 중에 비밀번호를 구성한 관리자 사용자가 있습니다. AAA 외부 인증은 지원되지 않습니다.
- 물리적 관리 인터페이스는 논리적 진단 인터페이스와 논리적 관리 인터페이스 간에 공유됩니다. 이 구성은 논리적 진단 인터페이스(사용 된 경우) 또는 다른 데이터 인터페이스에만 적용됩니다. 논리적 관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 Firepower Management Center에 설치하고 등록하는 데 사용됩니다. 별도의 IP 주소와 정적 라우팅을 가지고 있습니다.
- HTTPS를 사용하려면 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 HTTPS 액세스를 구성하면 됩니다.
- 연결할 수 있는 인터페이스에만 HTTPS를 사용할 수 있습니다. HTTPS 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다.
- 동일한 TCP 포트에 대한 동일한 인터페이스에서 HTTPS 액세스와 AnyConnect 원격 액세스 SSL VPN을 모두 구성할 수는 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. 동일한 인터페이스에서 두 기능을 구성해야 하는 경우 다른 포트를 사용합니다. 예를 들어 포트 4443에서 HTTPS를 엽니다.
- 디바이스는 최대 5개의 동시 HTTPS 연결을 허용합니다.

- 디바이스에 HTTPS 연결을 허용할 호스트 또는 네트워크를 정의하는 네트워크 개체가 필요합니다. 이 절차의 일부로 개체를 추가할 수 있지만 개체 그룹을 사용하여 IP 주소 그룹을 식별하려면 규칙에 필요한 그룹이 이미 있는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 구성합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **HTTP**를 선택합니다.

단계 **3** **Enable HTTP server(HTTP** 서버 활성화**)**를 클릭하여 HTTPS 서버를 활성화합니다.

단계 **4** (선택 사항) HTTPS 포트를 변경합니다. 기본값은 443입니다.

단계 **5** HTTPS 연결을 허용하는 인터페이스와 IP 주소를 확인합니다.

이 테이블을 사용하여 HTTPS 연결을 허용할 인터페이스와 이러한 연결을 허용할 수 있는 클라이언트의 IP 주소를 제한합니다. 개별 IP 주소가 아닌 네트워크 주소를 사용할 수 있습니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **IP Address(IP** 주소**)** - HTTPS 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체입니다. 드롭다운 메뉴에서 개체를 선택하거나 +를 클릭하여 새 네트워크 개체를 추가합니다.
- **Security Zones(**보안 영역**)** - HTTPS 연결을 허용할 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 선택한 Selected Security Zone(보안 영역 목록) 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

ICMP 액세스 규칙 구성

기본적으로 IPv4 또는 IPv6을 사용하여 ICMP 패킷을 모든 인터페이스로 전송할 수 있습니다.

- Firepower Threat Defense 디바이스는 브로드캐스트 주소로 전달되는 ICMP 에코 요청에 응답하지 않습니다.
- Firepower Threat Defense 디바이스는 트래픽이 들어오는 인터페이스로 전송되는 ICMP 트래픽에만 응답합니다. 인터페이스를 통해 먼 인터페이스로 ICMP 트래픽을 전송할 수 없습니다.

디바이스를 공격으로부터 보호하려면 ICMP 규칙을 사용하여 인터페이스에 대한 ICMP 액세스를 특정 호스트, 네트워크 또는 ICMP 유형으로 제한할 수 있습니다. ICMP 규칙은 액세스 규칙과 같은 방식으로 작동합니다. 규칙의 순서가 정해지고, 패킷과 일치하는 첫 번째 규칙이 작업을 정의합니다.

인터페이스에 대해 ICMP 규칙을 구성하면 ICMP 규칙 목록의 끝에 암시적 거부 ICMP 규칙이 추가되어 기본 동작이 변경됩니다. 따라서 단지 몇 가지 메시지 유형만 거부하려면 ICMP 규칙 목록의 끝에 나머지 메시지 유형을 허용하는 허용 규칙을 포함해야 합니다.

ICMP Unreachable 메시지 유형(type 3)은 항상 허용하는 것이 좋습니다. ICMP Unreachable 메시지를 거부하면 ICMP 경로 MTU 검색이 비활성화되고, 그 결과 IPsec 및 PPTP 트래픽이 정지할 수 있습니다. 또한 IPv6 인접 디바이스 검색 프로세스에서 IPv6의 ICMP 패킷이 사용됩니다.

시작하기 전에

규칙에 필요한 개체가 이미 존재하는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 구성합니다. 원하는 호스트 또는 네트워크를 정의하는 네트워크 개체 또는 그룹 및 제어하려는 ICMP 메시지 유형을 정의하는 포트 개체가 필요합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **ICMP**를 선택합니다.

단계 **3** ICMP 규칙을 구성합니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **Action(**작업**)** - 일치하는 트래픽을 허용 또는 거할지 여부입니다.
- **ICMP Service(ICMP** 서비스**)** - ICMP 메시지를 식별하는 포트 개체 유형입니다.
- **Network(**네트워크**)** - 액세스를 제어하는 호스트 또는 네트워크를 식별하는 네트워크 개체 또는 그룹입니다.
- **Security Zones(**보안 영역**)** - 보호하려는 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 선택한 Selected Security Zone(보안 영역 목록) 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** (선택 사항). ICMPv4 연결 불가 메시지의 속도 제한을 설정합니다.

- **Rate Limit(**속도 제한**)** - Unreachable 메시지의 속도 제한을 설정합니다(초당 메시지 1~100개). 기본값은 초당 메시지 1개입니다.
- **Burst Size(**버스트 크기**)** - 버스트 속도를 설정합니다(1~10). 이 값은 현재 시스템에서 사용되지 않습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SSL 설정

참고 이 작업을 수행하려면 관리자 권한이 있어야 하며 리프 도메인에 있어야 합니다.

Firepower Management Center의 완전한 라이선스 버전을 실행하는지 확인해야 합니다. 평가 모드에서 Firepower Management Center를 실행 중인 경우 SSL 설정을 사용할 수 없습니다. 또한 라이선스가 있는 Firepower Management Center 버전이 export-compliance기준을 충족하지 않으면 SSL 설정이 비활성화됩니다. SSL과 함께 원격 액세스 VPN을 사용하는 경우 스마트 계정에 강력한 암호화 기능이 활성화되어 있어야 합니다. 자세한 내용은 FTD 라이선스 유형 및 제한 사항를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firepower Threat Defense 정책을 생성하거나 수정합니다.

단계 **2** **SSL**을 선택합니다.

단계 **3** **Add SSL Configuration(SSL** 구성 추가**)** 테이블에 항목을 추가합니다.

a) **Add(**추가**)**를 클릭하여 새 항목을 만들거나 항목이 이미 있는 경우 **Edit(**편집**)**을 클릭합니다.

b) 드롭다운 목록에서 필수 보안 설정을 선택합니다.

- **Protocol Version(**프로토콜 버전**)** - Remote Access VPN 세션을 설정하는 동안 사용할 TLS 프로토콜을 지정합니다.
- **Security Level(**보안 수준**)** - SSL에 대해 설정하려는 보안 위치 지정의 종류를 나타냅니다.

단계 **4** 선택한 프로토콜 버전에 따라 **Available Algorithms(**사용 가능한 알고리즘**)**를 선택하고 **Add(**추가**)**를 클릭하여 선택한 프로토콜에 대해 포함합니다. 자세한 내용은 SSL 설정 정보, 1432 페이지을 참조해 주십시오.

알고리즘은 선택한 프로토콜 버전에 따라 나열됩니다. 각 보안 프로토콜은 보안 수준을 설정하는 고유한 알고리즘을 식별합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

Deploy(구축**)** > **Deployment(**구축**)**을 선택하고 **Deploy(**구축**)**를 클릭하여 할당된 디바이스에 정책을 구축합니다.

SSL 설정 정보

Firepower Threat Defense 디바이스 SSL(Secure Sockets Layer) (SSL) 프로토콜 및 전송 레이어 보안(TLS)을 사용 하 여 원격 클라이언트에서 Remote Access VPN 연결에 대 한 보안 메시지 전송을 지원합니다. SSL 설정 창을 사용하면 SSL을 통한 원격 VPN 액세스 중 메시지 전송을 위해 협상되고 사용되는 SSL 버전 및 암호화 알고리즘을 구성할 수 있습니다.

다음 위치에 SSL 설정을 구성합니다.

Devices(디바이스**) > Platform Settings(**플랫폼 설정**) > SSL**

필드

Minimum SSL Version as Server(최소 **SSL** 버전**(**서버**))** - Firepower Threat Defense 디바이스가 서버 역할을 할 때 사용하는 최소 SSL/TLS 프로토콜 버전을 지정합니다. 예를 들어 Remote Access VPN 게이트웨이로 작동할 경우입니다.

TLS Version(TLS 버전**)** - 드롭다운 목록에서 다음 TLS 버전 중 하나를 선택합니다.

TLS V1	SSLv2 클라이언트 Hello를 수락하고 TLSv1 이상을 협상합니다.
TLSv1.1	SSLv2 클라이언트 Hello를 수락하고 TLSv1.1 이상을 협상합니다.
TLSV1.2	SSLv2 클라이언트 Hello를 수락하고 TLSv1.2 이상을 협상합니다.

DTLS Version(DTLS 버전**)** - 선택한 TLS 버전을 기준으로 드롭다운 목록에서 DTLS 버전을 선택합니다. 기본적으로 DTLSv1은 FTD 디바이스에 설정됩니다. 요구 사항에 따라 DTLS 버전을 선택할 수 있습니다.

참고 TLS 프로토콜 버전이 선택한 DTLS 프로토콜 버전과 같거나 그 이상인지 확인합니다. TLS 프로토콜 버전은 다음 DTLS 버전을 지원합니다.

TLS V1	DTLSv1
TLSv1.1	DTLSv1
TLSV1.2	DTLSv1, DTLSv1.2

Diffie-Hellman Group(Diffie-Hellman그룹**)** - 드롭다운 목록에서 그룹을 선택합니다. 사용 가능한 옵션은 Group1 - 768-bit modulus(그룹 1 - 768비트 모듈러스), Group2 - 1024-bit modulus(그룹 2 - 1024비

트 모듈러스), Group5 - 1536-bit modulus(그룹 5 - 1536비트 모듈러스), Group14 - 2048-bit modulus, 224-bit prime order(그룹 14 - 2048비트 모듈러스, 224비트 소수 위수) 및 Group24 - 2048-bit modulus, 256-bit prime order(그룹 24 - 2048비트 모듈러스, 256비트 소수 위수)입니다. 기본값은 Group1입니다.

Elliptical Curve Diffie-Hellman Group(Elliptical Curve Diffie-Hellman 그룹) - 드롭다운 목록에서 그룹을 선택합니다. 사용 가능한 옵션은 Group19 - 256-bit EC(그룹 19 - 256비트 EC), Group20 - 384-bit EC(그룹 20 - 384비트 EC) 및 Group21 - 521-bit EC(그룹 21 - 521비트 EC)입니다. 기본값은 Group19입니다.

TLSv1.2는 다음과 같은 암호화에 대한 지원을 추가합니다.

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

참고 ECDSA 및 DHE 암호가 우선 순위가 가장 높습니다.

SSL 구성 테이블을 사용하여 Firepower Threat Defense 디바이스에서 지원하려는 프로토콜 버전, 보안 수준 및 비밀번호 알고리즘을 지정할 수 있습니다.

Protocol Version(프로토콜 버전) - Firepower Threat Defense 디바이스에서 지원하고 SSL 연결에 사용하는 프로토콜 버전을 나열합니다. 사용 가능한 프로토콜 버전은 다음과 같습니다.

- 기본
- TLSV1
- TLSv1.1
- TLSV1.2
- DTLSv1

- DTLSv1.2

Security Level(보안 수준**)** - Firepower Threat Defense 디바이스에서 지원하고 SSL 연결에 사용하는 암호화 보안 수준을 나열합니다.

평가 라이선스가 있는 Firepower Threat Defense 디바이스를 사용하는 경우 기본적으로 보안 레벨은 Low(낮음)입니다. Firepower Threat Defense 스마트 라이선스의 경우 기본 보안 레벨은 High(높음)입니다. 다음 옵션 중 하나를 선택하여 필요한 보안 레벨을 설정할 수 있습니다.

- **All(**모두**)** - NULL-SHA를 비롯한 모든 암호화를 포함합니다.
- **Low(**낮음**)** - NULL-SHA를 제외한 모든 암호화를 포함합니다.
- **Medium(**보통**)**은 NULL-SHA, DES-CBC-SHA, RC4-SHA 및 RC4-MD5를 제외한 모든 암호화를 포함합니다(기본값).
- **Fips** - 모든 FIPS 호환 암호화(NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA 및 DES-CBC3-SHA 제외)를 포함합니다.
- **High(**높음**)**는 AES-256 SHA-2 암호화만 포함하며, TLS 버전 1.2 및 기본 버전에 적용됩니다.
- **Custom(**사용자 지정**)**은 Cipher algorithms/custom string(암호화 알고리즘/사용자 지정 문자열) 상자에서 지정한 하나 이상의 암호화를 포함합니다. 이 옵션은 OpenSSL 암호화 정의 문자열을 사용하는 암호 그룹에 대한 모든 권한을 제공합니다.

Cipher Algorithms/Custom String(암호화 알고리즘/사용자 지정 문자열**)** - Firepower Threat Defense 디바이스에서 지원하고 SSL 연결에 사용하는 암호화 알고리즘을 나열합니다. OpenSSL을 사용하는 암호화에 대한 자세한 내용은 다음 섹션을 참고하십시오. https://www.openssl.org/docs/apps/ciphers.html

Firepower Threat Defense 디바이스에서는 지원되는 암호화에 대한 우선순위를 다음과 같이 지정합니다.

TLSv1.2에서만 지원되는 암호화

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256

DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

TLSv1.1 또는 TLSv1.2에서 지원되지 않는 암호화

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

에서 SSH(Secure Shell) 설정

외부와 같은 데이터 인터페이스에서 FMC 액세스를 활성화한 경우 이 절차를 사용하여 해당 인터페이스에서 SSH를 활성화해야 합니다. 이 섹션에서는 FTD에서 하나 이상의 데이터 인터페이스에 대한 SSH 연결을 활성화하는 방법을 설명합니다. SSH는 논리적 진단 인터페이스에서 지원되지 않습니다.

참고 SSH는 관리 인터페이스에서 기본적으로 활성화됩니다. 하지만 이 화면은 관리 SSH 액세스에 영향을 미치지 않습니다.

관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 Firepower Management Center에 설치하고 등록하는 데 사용됩니다. 데이터 인터페이스용 SSH는 관리 인터페이스용 SSH로 내부 사용자 목록을 공유합니다. 다른 설정은 별도로 구성됩니다. 데이터 인터페이스의 경우 이 화면을 사용하여 SSH 및 액세스 목록을 활성화합니다. 데이터 인터페이스용 SSH 트래픽은 일반 라우팅 구성을 사용하며 설치 또는 CLI에서 구성된 정적 경로는 사용하지 않습니다.

관리 인터페이스의 경우 SSH 액세스 목록을 구성하려면 Firepower Threat Defense 명령 참조의 **configure ssh-access-list** 명령을 참조하십시오. 정적 경로를 구성하려면 **configure network static-routes** 명령을 참조하십시오. 기본적으로 초기 설정 시 관리 인터페이스를 통해 기본 경로를 구성합니다.

SSH를 사용하려면 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 SSH 액세스를 구성하면 됩니다.

연결할 수 있는 인터페이스에만 SSH를 사용할 수 있습니다. SSH 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다.

디바이스는 최대 5개의 동시 SSH 연결을 허용합니다.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면, 시스템이 SSH 연결을 종료합니다.

시작하기 전에

- SSH 로컬 사용자는 **configure user add** 명령을 사용하여 CLI에서만 구성할 수 있습니다. FTD CLI용 로컬 사용자 계정 생성 섹션을 참조하십시오. 기본적으로 초기 설정 중에 비밀번호를 구성한 관리자 사용자가 있습니다. AAA 외부 인증은 지원되지 않습니다.
- 디바이스에 SSH 연결을 허용할 호스트 또는 네트워크를 정의하는 네트워크 개체가 필요합니다. 이 절차의 일부로 개체를 추가할 수 있지만 개체 그룹을 사용하여 IP 주소 그룹을 식별하려면 규칙에 필요한 그룹이 이미 있는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 설정합니다.

  참고 시스템에서 제공하는 **any** 네트워크 개체를 사용할 수 없습니다. 대신 **any-ipv4** 또는 **any-ipv6**를 사용합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Secure Shell**을 선택합니다.

단계 **3** SSH 연결을 허용하는 인터페이스와 IP 주소를 확인합니다.

이 테이블을 사용하여 SSH 연결을 허용할 인터페이스와 이러한 연결을 허용할 수 있는 클라이언트의 IP 주소를 제한합니다. 개별 IP 주소가 아닌 네트워크 주소를 사용할 수 있습니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **IP Address(IP** 주소**)** - SSH 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체입니다. 드롭다운 메뉴에서 개체를 선택하거나 +를 클릭하여 새 네트워크 개체를 추가합니다.
- **Security Zones(**보안 영역**)** - SSH 연결을 허용할 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 선택한 Selected Security Zone(보안 영역 목록) 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SMTP 설정

Syslog 설정에서 이메일 알림을 구성하는 경우 SMTP 서버를 식별해야 합니다. Syslog에 대해 구성하는 소스 이메일 주소는 SMTP 서버의 유효한 계정이어야 합니다.

시작하기 전에

기본 및 보조 SMTP 서버의 호스트 주소를 정의하는 네트워크 개체가 존재하는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 정의합니다. 정책을 편집하면서 개체를 생성할 수도 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **SMTP Server(SMTP** 서버**)**를 클릭합니다.

단계 **3** **Primary Server IP Address(**기본 서버 **IP** 주소**)** 및 선택적으로 **Secondary Server IP Address(**보조 서버 **IP** 주소**)**를 식별하는 네트워크 개체를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Threat Defense에 대한 SNMP 설정

단순 네트워크 관리 프로토콜(SNMP)은 PC 또는 워크스테이션에서 실행되는 네트워크 관리 스테이션을 위한 표준 방식을 정의하여 스위치, 라우터 및 보안 어플라이언스를 포함한 여러 유형의 디바이스 상태를 모니터링합니다. SNMP 페이지를 사용하여 SNMP 관리 스테이션의 모니터링을 위해 방화벽 디바이스를 구성할 수 있습니다.

단순 네트워크 관리 프로토콜(SNMP)을 활성화하면 중앙 위치에서 네트워크 디바이스를 모니터링할 수 있습니다. Cisco 보안 어플라이언스는 SNMP 버전 1, 2c 및 3은 물론 트랩 및 SNMP 읽기 액세스를 사용하는 네트워크 모니터링을 지원합니다. SNMP 쓰기 액세스는 지원되지 않습니다.

SNMPv3는 읽기 전용 사용자 및 DES(더 이상 사용되지 않음), 3DES, AES256, AES192 및 AES128을 통한 암호화를 지원합니다.

참고 DES 암호화는 향후 릴리스에서 더 이상 사용되지 않습니다. 플랫폼 정책 설정에서 암호화 유형으로 DES를 사용하지 않는 것이 좋습니다.

참고 외부 SNMP 서버에 알림을 생성하려면 **Policies(**정책**)** > **Action(**작업**)** > **Alerts(**알림**)**에 액세스합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **SNMP**를 선택합니다.

단계 **3** SNMP를 활성화하고 기본 옵션을 구성합니다.

- **Enable SNMP Servers(SNMP** 서버 활성화**)** - SNMP 정보를 구성된 SNMP 호스트에 제공할지 여부입니다. 구성 정보를 유지하는 동안 SNMP 모니터링을 비활성화하려면 이 옵션의 선택을 취소할 수 있습니다.
- **Read Community String(**읽기 커뮤니티 문자열**)**, **Confirm(**확인**)** - FTD 디바이스에 요청을 보낼 때 SNMP 관리 스테이션에서 사용하는 암호를 입력합니다. SNMP 커뮤니티 문자열은 SNMP 관리 스테이션과 관리 대상 네트워크 노드 사이에서 비밀로 공유됩니다. 보안 디바이스는 이 비밀번호를 사용하여 수신 SNMP 요청이 유효한지 판단합니다. 비밀번호는 대/소문자를 구분하며 최대 32자의 영숫자 문자열입니다. 공백과 특수 문자는 허용되지 않습니다.
- **System Administrator Name(**시스템 관리자 이름**)** - 디바이스 관리자 또는 다른 담당자의 이름을 입력합니다. 이 문자열은 대/소문자를 구분하며 최대 127자까지 가능합니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.
- **Location(**위치**)** - 이 보안 디바이스의 위치를 입력합니다(예: Building 42, Sector 54). 이 문자열은 대/소문자를 구분하며 최대 127자까지 가능합니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.
- **Port(**포트**)** - 수신 요청을 수락할 UDP 포트를 입력합니다. 기본값은 161입니다.

단계 **4** (SNMPv3만 해당) SNMPv3 사용자 추가, 1439 페이지.

단계 **5** SNMP 호스트 추가, 1441 페이지.

단계 **6** SNMP 트랩 구성, 1442 페이지.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SNMPv3 사용자 추가

참고 SNMPv3에 대해서만 사용자를 생성합니다. 이러한 단계는 SNMPv1 또는 SNMPv2c에 적용할 수 없습니다.

SNMPv3는 읽기 전용 사용자만 지원합니다.

SNMP 사용자는 지정된 사용자 이름, 인증 비밀번호, 암호화 비밀번호 및 승인, 그리고 사용할 암호화 알고리즘을 가져야 합니다.

인증 알고리즘 옵션은 MD5(사용되지 않음), SHA 및 SHA256입니다.

참고 MD5 인증 알고리즘은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 수 있습니다. 플랫폼 정책 설정에서 MD5 인증 알고리즘 유형을 사용하지 않는 것이 좋습니다.

암호화 알고리즘 옵션은 DES(더 이상 사용되지 않음), 3DES, AES256, AES192 및 AES128입니다.

참고 DES 암호화는 향후 릴리스에서 더 이상 사용되지 않습니다. 플랫폼 정책 설정에서 암호화 유형으로 DES를 사용하지 않는 것이 좋습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **SNMP** > **Users(**사용자**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** **Security Level(**보안 수준**)** 드롭다운 목록에서 사용자의 보안 수준을 선택합니다.

- **Auth** - Authentication but No Privacy(인증 있음 및 개인정보 보호 없음)로 메시지가 인증을 받음을 의미합니다.
- **No Auth** - No Authentication and No Privacy(인증 없음 및 개인정보 보호 없음)로 메시지에 보안이 적용되지 않음을 의미합니다.
- **Priv** - Authentication and Privacy(인증 있음 및 개인정보 보호 있음)로 메시지가 인증을 받고 암호화됨을 의미합니다.

단계 **5** **Username(**사용자 이름**)** 필드에 SNMP 사용자 이름을 입력합니다. 사용자 이름은 32자 이하여야 합니다.

단계 **6** **Encryption Password Type(**비밀번호 유형 암호화**)** 드롭다운 목록에서 사용할 비밀번호 유형을 선택합니다.

- **Clear text(**일반 텍스트**)** - FTD 디바이스는 구축할 때 비밀번호를 계속 암호화합니다.
- **Encrypted(**암호화됨**)** - FTD 디바이스는 암호화된 비밀번호를 직접 구축합니다.

단계 **7** **Auth Algorithm Type(**인증 알고리즘 유형**)** 드롭다운 목록에서 사용할 인증 유형(MD5, SHA, or SHA256)을 선택합니다.

참고 MD5 인증 알고리즘은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 수 있습니다. 플랫폼 정책 설정에서 MD5 인증 알고리즘 유형을 사용하지 않는 것이 좋습니다.

단계 **8** **Authentication Password(**인증 비밀번호**)** 필드에 인증에 사용할 비밀번호를 입력합니다. Encryption Password Type(비밀번호 유형 암호화)으로 Encrypted(암호화됨)를 선택하면 비밀번호는 xx:xx:xx... 형식이어야 합니다. 여기서 xx는 16진수 값입니다.

참고 비밀번호의 길이는 선택한 인증 알고리즘에 따라 다릅니다. 모든 비밀번호의 길이는 256자 이하여야 합니다.

Encrypt Password Type(비밀번호 유형 암호화)로 Clear Text(일반 텍스트)를 선택한 경우, **Confirm(**확인**)** 필드에 암호를 반복합니다.

단계 **9** **Encryption Type(**암호화 유형**)** 드롭다운 목록에서 사용할 암호화 유형을 선택합니다(AES128, AES192, AES256, 3DES 또는 DES).

참고 AES 또는 3DES 암호화를 사용하려면 디바이스에 적절한 라이선스가 설치되어 있어야 합니다.

참고 DES 암호화는 향후 릴리스에서 더 이상 사용되지 않습니다. 플랫폼 정책 설정에서 암호화 유형으로 DES를 사용하지 않는 것이 좋습니다.

단계 **10** **Encryption Password(**암호화 비밀번호**)** 필드에 암호화에 사용할 비밀번호를 입력합니다. Encryption Password Type(암호화 비밀번호 유형)으로 Encrypted(암호화됨)를 선택하면 비밀번호는 xx:xx:xx... 형식이어야 합니다. 여기서 xx는 16진수 값입니다. 암호화된 비밀번호의 경우 길이는 선택한 암호화 유형에 따라 다릅니다. 비밀번호 크기는 다음과 같습니다(각 xx는 8진법).

- AES 128에는 16 8진수 필요
- AES 192에는 24 8진수 필요
- AES 25에는 32 8진수 필요
- 3DES에는 32 8진수 필요
- DES는 모든 크기일 수 있음

참고 모든 비밀번호의 길이는 256자 이하여야 합니다.

Encrypt Password Type(비밀번호 유형 암호화)로 Clear Text(일반 텍스트)를 선택한 경우, **Confirm(**확인**)** 필드에 암호를 반복합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SNMP 호스트 추가

Host(호스트)를 사용하여 SNMP 페이지의 SNMP 호스트 테이블에 항목을 추가하거나 편집합니다. 이 항목은 FTD 디바이스에 액세스할 수 있는 SNMP 관리 스테이션을 나타냅니다.

최대 4000개의 호스트를 추가할 수 있습니다. 하지만 이 중 128개만 트랩에 사용할 수 있습니다.

시작하기 전에

SNMP 관리 스테이션을 정의하는 네트워크 개체가 존재하는지 확인합니다. **Device(**디바이스**)** > **Object Management(**개체 관리**)**를 선택하여 네트워크 개체를 구성합니다.

참고 지원되는 네트워크 개체에는 IPv6 호스트, IPv4 호스트, IPv4 범위 및 IPv4 서브넷 주소가 포함됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **SNMP** > **Hosts(**호스트**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** **IP Address(IP** 주소**)**필드에 유효한 IPv6 또는 IPv4 호스트를 입력하거나 SNMP 관리 스테이션의 호스트 주소를 정의하는 네트워크 개체를 선택합니다.

IP 주소는 IPv6 호스트, IPv4 호스트, IPv4 범위 또는 IPv4 서브넷일 수 있습니다.

단계 **5** **SNMP version(SNMP** 버전**)** 드롭다운 목록에서 적절한 SNMP 버전을 선택합니다.

단계 **6** (SNMPv3만 해당) **User Name(**사용자 이름**)** 드롭다운 목록에서 구성한 SNMP 사용자의 사용자 이름을 선택합니다.

참고 SNMP 호스트당 최대 23명의 SNMP 사용자를 연결할 수 있습니다.

단계 **7** (SNMPv1, 2c만 해당) **Read Community String(**읽기 커뮤니티 문자열**)** 필드에 디바이스에 대한 읽기 액세스용으로 이미 구성한 커뮤니티 문자열을 입력합니다. 문자열을 다시 입력하여 확인합니다.

참고 이 문자열은 이 SNMP 스테이션에서 사용된 문자열이 **Enable SNMP Server(SNMP** 서버 활성화**)** 섹션에서 사전 정의된 문자열과 다른 경우에만 필요합니다.

단계 **8** 디바이스 및 SNMP 관리 스테이션 간의 통신 유형을 선택합니다. 두 유형을 선택할 수 있습니다.

- **Poll** - 관리 스테이션이 주기적으로 디바이스의 정보를 요청합니다.
- **Trap** - 디바이스가 트랩 이벤트를 발생하면 관리 스테이션으로 전송합니다.

참고 SNMP 호스트 IP 주소가 IPv4 범위 또는 IPv4 서브넷일 때 **Poll** 또는 **Trap** 중 하나만 구성할 수 있으며 둘 다를 구성할 수는 없습니다.

단계 **9** **Port(**포트**)** 필드에 SNMP 호스트에 대한 포트 번호를 입력합니다. 기본값은 162입니다. 유효한 범위는 1 ~65535입니다.

단계 **10** **Reachable By(**연결 방법**)** 옵션 아래에서 디바이스 및 SNMP 관리 스테이션 간의 통신을 위한 인터페이스 유형을 선택합니다. 디바이스의 관리 인터페이스 또는 사용 가능한 보안 영역/명명된 인터페이스를 선택할 수 있습니다.

- 디바이스 관리 인터페이스 - 디바이스와 SNMP 관리 스테이션 간의 통신은 관리 인터페이스를 통해 수행됩니다.
  - SNMPv3 폴링에 대해 이 인터페이스를 선택하면 구성된 모든 SNMPv3 사용자가 폴링할 수 있으며 단계 6, 1441 페이지 단계에서 선택한 사용자로 제한되지 않습니다. 여기서 SNMPv1 및 SNMPv2c는 SNMPv3 호스트에서 허용되지 않습니다.
  - SNMPv1 및 SNMPv2c 폴링에 대해 이 인터페이스를 선택하면 폴링이 단계 5, 1441 페이지 단계에서 선택한 버전으로 제한되지 않습니다.
- 보안 영역 또는 명명된 인터페이스 - 디바이스와 SNMP 관리 스테이션 간의 통신은 보안 영역 또는 인터페이스를 통해 수행됩니다.
  - **Available Zones(**사용 가능한 영역**)** 필드에서 영역을 검색합니다.
  - **Selected Zones/Interfaces(**선택된 영역/인터페이스**)** 필드에서 디바이스가 관리 스테이션과 통신하는 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Zone/Interface(**선택한 영역/ 인터페이스**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 선택한 인터페이스 또는 영역이 디바이스에 포함되어 있는 경우에만 디바이스에서 호스트가 구성됩니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SNMP 트랩 구성

SNMP Traps(SNMP 트랩)을 사용하여 FTD 디바이스에 대한 SNMP 트랩(이벤트 알림)을 구성합니다. 트랩은 찾아보기와 다릅니다. 이는 linkup, linkdown 및 syslog 이벤트 생성과 같은 특정 이벤트에 대해 FTD 디바이스에서 관리 스테이션으로의 요청되지 않은 "코멘트"입니다. 디바이스 SNMP 개체 ID(OID)가 디바이스에서 보낸 SNMP 이벤트 트랩에 나타납니다.

일부 트랩은 특정 하드웨어 모델에 적용됩니다. 이러한 모델 중 하나에 정책을 적용하면 이러한 트랩은 무시됩니다. 예를 들어 모든 모델에 현장 교체 가능한 디바이스가 있는 것은 아니므로 해당 모델에 **Field Replaceable Unit Insert/Delete** 트랩이 구성되지 않습니다.

SNMP 트랩은 표준 또는 기업별 MIB로 정의됩니다. 표준 트랩은 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. SNMP 트랩은 FTD 소프트웨어로 컴파일됩니다.

필요한 경우 다음 위치에서 RFC, 표준 MIB 및 표준 트랩을 다운로드할 수 있습니다.

http://www.ietf.org/

다음 위치에서 Cisco MIB, 트랩 및 OID의 전체 목록을 검색하십시오.

SNMP Object Navigator

또한 다음 위치에서 FTP를 통해 Cisco OID를 다운로드할 수 있습니다.

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **SNMP** > **SNMP Traps(SNMP** 트랩**)**을 클릭하여 FTD 디바이스에 대한 SNMP 트랩(이벤트 알림)을 구성합니다.

단계 **3** 적절한 Enable Traps(트랩 활성화) 옵션을 선택합니다. 옵션 중 하나 또는 두 가지를 선택할 수 있습니다.

a) 이후의 네 섹션에서 모든 트랩을 빠르게 선택하려면 **Enable All SNMP Traps(**모든 **SNMP** 트랩 활성화**)**를 선택합니다.

b) 트랩 관련 syslog 메시지 전송을 활성화하려면 **Enable All Syslog Traps(**모든 **Syslog** 트랩 활성화**)**를 선택합니다.

참고 SNMP 트랩은 실시간에 가까울 것으로 예상되는 FTD의 다른 알림 메시지보다 우선 순위가 높습니다. 모든 SNMP 또는 syslog 트랩을 활성화하면 SNMP 프로세스가 에이전트 및 네트워크에서 초과 리소스를 소비하여 시스템이 중단될 수 있습니다. 시스템 지연, 완료되지 않은 요청 또는 시간 초과가 있는 경우 SNMP 및 syslog 트랩을 선택적으로 활성화할 수 있습니다. 심각도 수준 또는 메시지 ID별로 syslog 메시지가 생성되는 속도를 제한할 수도 있습니다. 예를 들어 212로 시작하는 모든 syslog 메시지 ID는 SNMP 클래스와 연결되어 있습니다. Syslog 메시지 생성 속도 제한, 1457 페이지 섹션을 참조하십시오.

단계 **4** **Standard(**표준**)** 섹션의 이벤트 알림 트랩은 기본적으로 기존 정책에 대해 활성화됩니다.

- **Authentication(**인증**)** - 무단 SNMP 액세스입니다. 이 인증 실패는 잘못된 커뮤니티 문자열이 있는 패킷에 대해 발생합니다.
- **Link Up(**링크업**)** - 알림에 표시된 대로 디바이스의 통신 링크 중 하나를 사용할 수 있습니다.
- **Link Down(**링크다운**)** - 알림에 표시된 대로 디바이스의 통신 링크 중 하나가 실패했습니다.
- **Cold Start(**콜드 스타트**)** - 디바이스가 다시 초기화하고 있거나, 프로토콜 엔티티 구현이 변경될 수 있습니다.
- **Warm Start(**웜 스타트**)** - 디바이스 자체 구성 또는 프로토콜 엔티티 구현이 변경될 수 있도록 다시 초기화하고 있습니다.

단계 **5** **Entity MIB** 섹션에서 원하는 이벤트 알림 트랩을 선택합니다.

- **Field Replaceable Unit Insert(**현장 교체 가능 디바이스 삽입**)** - 현장 교체 가능 디바이스(FRU)가 표시된 대로 삽입되었습니다. (FRU에는 전원 공급 장치, 팬, 프로세서 모듈, 인터페이스 모듈 등과 같은 어셈블리가 포함됩니다.)
- **Field Replaceable Unit Delete(**현장 교체 가능 디바이스 삭제**)** - 현장 교체 가능 디바이스(FRU)가 알림에 표시된 대로 제거되었습니다.
- **Configuration Change(**구성 변경**)** - 알림에 표시된 대로 하드웨어가 변경되었습니다.

단계 **6** **Resource(**리소스**)** 섹션에서 원하는 이벤트 알림 트랩을 선택합니다.

- **Connection Limit Reached(**연결 제한 도달**)** - 이 트랩은 구성된 연결 제한에 도달했기 때문에 연결 시도가 거부되었음을 나타냅니다.

단계 **7** **Other(**기타**)** 섹션에서 원하는 이벤트 알림 트랩을 선택합니다.

- **NAT Packet Discard(NAT** 패킷 폐기**)** - 이 알림은 IP 패킷이 NAT 기능에 의해 폐기될 때 생성됩니다. 사용 가능한 네트워크 주소 변환 주소 또는 포트가 구성된 임계값 아래로 하락함
- **CPU Rising Threshold(CPU** 상승 임계값**)**-이 알림은 CPU 사용률 상승이 구성된 기간 동안 사전 정의된 임계값을 초과할 때 생성됩니다. CPU 상승 임계값 알림을 활성화하려면 이 옵션을 선택합니다.
  - **Percentage(**백분율**)**-높은 임계값 알림의 기본값은 70%입니다. 범위는 10% ~ 94%입니다. 중요 임계값은 95%로 하드 코딩됩니다.
  - **(Period)**기간-기본 모니터링 기간은 1분입니다. 범위는 1 ~ 60분입니다.
- **Memory Rising Threshold(**메모리 상승 임계값**)**-이 알림은 메모리 사용률이 미리 정의된 임계값을 초과하여 사용 가능한 메모리가 감소하면 생성됩니다. 메모리 상승 임계값 알림을 활성화하려면 이 옵션을 선택합니다.
  - **Percentage(**백분율**)**-높은 임계값 알림의 기본값은 70%입니다. 범위는 50% ~ 95%입니다.
- **Failover(**페일 오버**)** –이 알림은 CISCO-UNIFIED-FIREWALL-MIB에서 보고한 페일오버 상태가 변경되면 생성됩니다.
- **Cluster(**클러스터**)**-이 알림은 CISCO-UNIFIED-FIREWALL-MIB에서 보고한 대로 클러스터 상태가 변경되면 생성됩니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

시스템 로그 구성 관련 정보

FTD 디바이스에 대한 시스템 로그를 활성화할 수 있습니다. 기록 정보는 네트워크 또는 디바이스 구성 관련 문제를 식별하고 격리하는 데 도움이 됩니다. 일부 보안 이벤트를 시스템 로그 서버에 전송할 수도 있습니다. 다음 주제에서는 기록 및 기록을 구성하는 방법에 대해 설명합니다.

Syslog 정보

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다. Cisco 디바이스는 로그 메시지를 UNIX 스타일 syslog 서비스로 전송할 수 있습니다. syslog 서비스는 메시지를 수신하고 파일로 저장하거나 간단한 구성 파일에 따라 인쇄합니다. 이 로깅 양식을 통해 로그를 안전하게 장기 보관할 수 있습니다. 로그는 일상적인 문제 해결과 사고 처리에 모두 유용합니다.

표 ***95:*** 시스템 로그 ***Firepower Threat Defense***

관련 로그	세부 사항	구성
디바이스 및 시스템 상태, 네트워크 구성	이 syslog 구성에서는 데이터 플레인에서 실행되는 기능, 즉 **show running-config** 명령으로 볼 수 있는 CLI 구성에 정의된 기능에 대해 메시지를 생성합니다. 여기에는 라우팅, VPN, 데이터 인터페이스, DHCP 서버, NAT 등과 같은 기능이 포함됩니다. 데이터 플레인 syslog 메시지는 번호가 매겨지며 ASA 소프트웨어를 실행하는 디바이스에서 생성된 메시지와 동일합니다. 하지만 Firepower Threat Defense는 ASA 소프트웨어에 사용할 수 있는 모든 메시지 유형을 생성하지는 않습니다. 이 메시지에 대한 정보는 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html의 *Cisco Firepower Threat Defense Syslog* 메시지를 참조하십시오. 이 구성은 다음 주제에서 설명됩니다.	플랫폼 설정
보안 이벤트	이 syslog 구성은 파일 및 악성코드, 연결, 보안 인텔리전스 및 침입 이벤트에 대한 알림을 생성합니다. 자세한 내용은 Security Events(보안 이벤트)에 대한 시스템 로그 메시지 전송 정보, 2755 페이지 및 하위 주제를 참조하십시오.	액세스 제어 정책의 **Platform Settings(**플랫폼 설정**)** 및 **Logging(**로깅**)**
(모든 디바이스) 정책, 규칙 및 이벤트	이 syslog 구성은 알림 응답 지원 설정, 2682 페이지에서 설명한 대로 액세스 제어 규칙, 침입 규칙 및 기타 고급 서비스에 대한 알림을 생성합니다. 이러한 메시지에 번호가 매겨지지는 않습니다. 이 유형의 syslog 구성에 대한 자세한 내용은 Syslog 알림 응답 생성, 2684 페이지 섹션을 참조하십시오.	액세스 제어 정책의 **Alert Responses(**알림 응답**)** 및 **Logging(**로깅**)**

두 개 이상의 syslog 서버를 구성하고 각 서버로 전송되는 메시지 및 이벤트를 제어할 수 있습니다. 콘솔, 이메일, 내부 버퍼 등과 같은 다른 대상을 구성할 수도 있습니다.

심각도 레벨

다음 표는 syslog 메시지 심각도 수준을 나열합니다.

표 ***96: Syslog*** 메시지 심각도 레벨

레벨 번호	심각도 레벨	설명
0	**emergencies(**비상**)**	시스템을 사용할 수 없습니다.
1	**Alert(**긴급 경고**)**	즉각적인 행동이 필요합니다.
2	**critical(**심각**)**	심각한 상태입니다.
3	**error(**오류**)**	오류 상태입니다.
4	**warning(**경고**)**	경고 상태입니다.
5	**notification(**알림**)**	일반적이지만 중요한 상태입니다.
6	**informational(**정보**)**	정보 메시지만 해당됩니다.
7	**debugging(**디버깅**)**	디버깅 메시지만 해당됩니다.

참고 Firepower Threat Defense 심각도 레벨이 0(응급)인 syslog 메시지를 생성하지 않습니다.

Syslog 메시지 필터링

특정 syslog 메시지만 특정 출력 대상에 전송되도록 생성된 syslog 메시지를 필터링할 수 있습니다. 예를 들어 모든 syslog 메시지를 하나의 출력 대상으로 전송하고 이 syslog 메시지의 하위 집합을 다른 출력 대상으로 보내도록 Firepower Threat Defense 디바이스를 구성할 수 있습니다.

구체적으로 syslog 메시지가 다음 기준에 따라 출력 대상으로 전송되도록 지시할 수 있습니다.

- Syslog 메시지 ID 번호

  (이 번호는 연결 및 침입 이벤트 같은 보안 이벤트에 대한 syslog 메시지에 적용되지 않습니다.)

- Syslog 메시지 심각도 레벨
- Syslog 메시지 클래스(기능 영역에 해당)

  (이 번호는 연결 및 침입 이벤트 같은 보안 이벤트에 대한 syslog 메시지에 적용되지 않습니다.)

출력 대상을 설정할 때 지정할 수 있는 메시지 목록을 생성함으로써 이 기준을 사용자 정의할 수 있습니다. 또는 특정 메시지 클래스를 메시지 목록과는 별개로 각 출력 대상 유형으로 전송하도록 Firepower Threat Defense 디바이스를 구성할 수도 있습니다.

(메시지 목록은 연결 및 침입 이벤트 같은 보안 이벤트에 대한 syslog 메시지에 적용되지 않습니다.)

Syslog 메시지 클래스

참고 이 주제는 보안 이벤트(예: 연결, 침입 등)에 대한 메시지에 적용되지 않습니다.

syslog 메시지 클래스를 2가지 방법으로 사용할 수 있습니다.

- 전체 syslog 메시지 카테고리에 대한 출력 위치를 지정합니다.
- 메시지 클래스를 지정하는 메시지 목록을 생성합니다.

syslog 메시지 클래스는 디바이스의 기능에 해당하는 유형에 따라 syslog 메시지를 분류하는 방식을 제공합니다. 예를 들어 rip 클래스는 RIP 라우팅을 나타냅니다.

특정 클래스의 모든 syslog 메시지는 syslog 메시지 ID 번호의 첫 3자리가 같습니다. 예를 들어 611로 시작하는 모든 syslog 메시지 ID는 vpnc(VPN 클라이언트)와 연결되어 있습니다. VPN 클라이언트 기능에 연결된 syslog 메시지는 611101부터 611323까지입니다.

또한 대부분의 ISAKMP syslog 메시지는 터널 식별을 돕는 공통의 접두사가 있는 객체 세트를 갖습니다. 이러한 객체가 있는 경우 syslog 메시지의 설명 텍스트 앞에 위치합니다. syslog 메시지가 생성되는 시점에 객체를 알 수 없는 경우 구체적인 heading = value 조합은 표시되지 않습니다.

객체는 다음과 같이 접두사가 붙습니다.

그룹 = *groupname*, 사용자 이름 = *user*, IP = *IP_address*

그룹이 터널-그룹인 경우 사용자 이름은 로컬 데이터베이스 또는 AAA 서버의 사용자 이름이고 IP 주소는 원격 액세스 클라이언트 또는 레이어 2 피어의 공용 IP 주소입니다.

다음 표에는 메시지 클래스와 각 클래스의 메시지 ID 범위가 나와 있습니다.

표 ***97: Syslog*** 메시지 클래스와 연결된 메시지 ***ID*** 번호

클래스	정의	**Syslog** 메시지 **ID** 번호
auth	사용자 인증	109, 113
—	액세스 목록	106
—	애플리케이션 방화벽	415
bridge	투명한 방화벽	110, 220
ca	PKI 인증 기관	717
citrix	Citrix 클라이언트	723
—	클러스터링	747

클래스	정의	**Syslog** 메시지 **ID** 번호
—	카드 관리	323
config	CLI(Command Line Interface)	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	동적 액세스 정책	734
eap, eapoudp	Network Admission Control용 EAPoUDP 또는 EAP	333, 334
eigrp	EIGRP 라우팅	336
email	이메일 프록시	719
—	환경 모니터링	735
HA	페일오버	101, 102, 103, 104, 105, 210, 311, 709
—	ID 기반 방화벽	746
ids	Intrusion Detection System(침입 탐지 시스템)	400, 733
—	IKEv2 툴킷	750, 751, 752
ip	IP 스택	209, 215, 313, 317, 408
ipaa	IP 주소 할당	735
ips	Intrusion Protection System(침입 방지 시스템)	400, 401, 420
—	IPv6	325
—	봇넷 트래픽 필터링	338
—	라이선싱	444
mdm-proxy	MDM 프록시	802
nac	NAC(Network Admission Control)	731, 732
nacpolicy	NAC 정책	731
nacsettings	NAC 정책을 적용할 NAC 설정	732
—	네트워크 액세스 포인트	713
np	네트워크 프로세서	319
—	NP SSL	725

클래스	정의	**Syslog** 메시지 **ID** 번호
ospf	OSPF 라우팅	318, 409, 503, 613
—	비밀번호 암호화	742
—	전화 프록시	337
rip	RIP 라우팅	107, 312
rm	리소스 관리자	321
—	Smart Call Home	120
session	사용자 세션	204, 302, 303, 304, 202 305, 314 및 405, 108, 201, 406 및/또는/또는//407/106
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL 스택	725
svc	SSL VPN 클라이언트	722
sys	시스템	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	위협 탐지	733
tre	트랜잭션 규칙 엔진	780
—	UC-IME	339
tag-switching	서비스 태그 스위칭	779
VM	VLAN 매핑	730
vpdn	PPTP 및 L2TP 세션	213, 403, 603
vpn	IKE 및 IPSEC	316, 320, 404, 501, 602, 402
vpnc	VPN 클라이언트	611
vpnfo	VPN 페일오버	720
vpnlb	VPN 로드 밸런싱	718
—	VXLAN	778
webfo	WebVPN 페일오버	721

클래스	정의	**Syslog** 메시지 **ID** 번호
webvpn	WebVPN 및 AnyConnect Client	716
—	NAT 및 PAT	305

로깅 지침

이 섹션에는 로깅을 구성하기 전에 검토해야 할 지침 및 제한사항이 포함되어 있습니다.

IPv6 지침

- IPv6가 지원됩니다. TCP 또는 UDP를 사용하여 Syslog를 전송할 수 있습니다.
- Syslogs 전송에 대해 구성된 인터페이스가 활성화되어 있으며 IPv6를 지원 가능하며 syslog 서버에 지정된 인터페이스를 통해 연결할 수 있는지 확인합니다.
- IPv6를 통한 보안 로깅은 지원되지 않습니다.

추가 지침

- syslog 서버는 syslogd라는 서버 프로그램을 실행해야 합니다. Windows 운영 체제에는 syslog 서버가 포함되어 있습니다.
- Firepower Threat Defense 디바이스에서 생성된 로그를 보려면 로깅 출력 대상을 지정해야 합니다. 로깅 출력 대상을 지정하지 않고 로깅을 활성화하면 Firepower Threat Defense 디바이스는 메시지를 생성하지만 메시지를 볼 수 있는 위치에 저장하지 않습니다. 각 다른 로깅 출력 대상을 별도로 지정해야 합니다.
- 두 개의 서로 다른 목록 또는 다른 syslog 서버 또는 동일한 위치에 할당 중인 클래스를 갖는 것은 불가능합니다.
- 최대 16개의 syslog 서버를 구성할 수 있습니다.
- syslog 서버는 Firepower Threat Defense 디바이스를 통해 연결할 수 있습니다. syslog 서버가 연결할 수 없는 인터페이스의 ICMP 연결 불가 메시지를 거부하고 syslog를 동일한 서버로 전송하도록 디바이스를 구성할 수 있습니다. 모든 심각도 레벨에 대해 로깅을 활성화했는지 확인합니다. syslog 서버가 충돌하지 않게 하려면 syslogs 313001, 313004 및 313005의 생성을 억제합니다.
- syslog에 대한 UDP 연결 수는 하드웨어 플랫폼의 CPU 수 및 구성한 syslog 서버 수와 직접 관련이 있습니다. 어느 시점이든 CPU에는 구성된 syslog 서버의 수와 동일한 수의 UDP syslog 연결이 있을 수 있습니다. 예를 들어, 각 syslog 서버에 대해서는 다음 연결이 가능합니다.
  - ASA 5585-SSP-10에는 최대 4개의 UDP syslog 연결이 있을 수 있습니다.
  - Firepower 4110에는 최대 22개의 UDP syslog 연결이 있을 수 있습니다.
  - Firepower 4120에는 최대 46개의 UDP syslog 연결이 있을 수 있습니다.

이는 정상적인 동작입니다. 전역 UDP 연결 유휴 시간 초과가 이 세션에 적용되며 기본값은 2분입니다. 이러한 세션을 더욱 신속하게 종료하려면 설정을 조정할 수 있지만 시간 초과는 syslog뿐만 아니라 모든 UDP 연결에 적용됩니다.

- TCP를 통해 Firepower Threat Defense 디바이스가 syslogs를 전송할 때 syslogd 서비스가 재시작된 후에 연결을 초기화하는 데 약 1분 이상이 걸릴 수 있습니다.

FTD 디바이스에 대한 Syslog 로깅 구성

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용을 참조하십시오.

syslog 설정을 구성하려면 다음 단계를 수행합니다.

시작하기 전에

로깅 지침, 1450 페이지의 요구 사항을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** 목차에서 **Syslog**를 클릭합니다.

단계 **3** 로깅을 활성화하고 FTP 서버 설정을 지정하고 플래시 사용을 지정하려면 **Logging Setup(**로깅 설정**)**을 클릭합니다. 자세한 내용은 로깅 활성화 및 기본 설정, 1452 페이지을 참조해 주십시오.

단계 **4** 특정 대상에 대한 로깅을 활성화하고 메시지 심각도 레벨, 이벤트 클래스 또는 사용자 지정 이벤트 목록에 대한 필터링을 지정하려면 **Logging Destinations(**로깅 대상**)**를 클릭합니다. 자세한 내용은 로깅 대상 활성화, 1454 페이지을 참조해 주십시오.

로깅 대상을 활성화하여 해당 대상에서 메시지를 볼 수 있도록 해야 합니다.

단계 **5** 이메일 메시지로 전송되는 시스템 로그 메시지의 소스 주소로 사용할 이메일 주소를 지정하려면 **E-mail Setup(**이메일 설정**)**을 클릭합니다. 자세한 내용은 이메일 주소로 Syslog 메시지 전송, 1455 페이지을 참조해 주십시오.

단계 **6** **Events List(**이벤트 목록**)**를 클릭하여 이벤트 클래스, 심각도 레벨 및 이벤트 ID를 포함하는 사용자 지정 이벤트 목록을 정의합니다. 자세한 내용은 사용자 지정 이벤트 목록 생성, 1456 페이지을 참조해 주십시오.

단계 **7** **Rate Limit(**속도 제한**)**을 클릭하여 구성된 모든 대상에 전송되는 메시지의 양을 지정하고 속도 제한을 할당할 메시지 심각도 레벨을 정의합니다. 자세한 내용은 Syslog 메시지 생성 속도 제한, 1457 페이지을 참조해 주십시오.

단계 **8** **Syslog Settings(**시스템 로그 설정**)**를 클릭하여 로깅 기능을 지정하고 타임스탬프 추가를 활성화하며, 다른 설정을 활성화하여 서버를 시스템 로그 대상으로 설정합니다. 자세한 내용은 Syslog 설정, 1458 페이지을 참조해 주십시오.

단계 **9** **Syslog Servers(**시스템 로그 서버**)**를 클릭하여 로깅 대상으로 지정된 시스템 로그 서버의 IP 주소, 사용된 프로토콜, 형식 및 보안 영역을 지정합니다. 자세한 내용은 Syslog 서버 설정, 1459 페이지을 참조해 주십시오.

보안 이벤트 **Syslog** 메시지에 적용되는 **FTD** 플랫폼 설정

'보안 이벤트'에는 연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트가 포함됩니다.

Devices(디바이스**) > Platform Settings(**플랫폼 설정**) > Threat Defense Settings(Threat Defense** 설정**) > Syslog(**시스템 로그**)** 페이지 및 해당 탭의 일부 시스템 로그 설정은 보안 이벤트에 대한 시스템 로그 메시지에 적용되지만, 대부분은 시스템 상태 및 네트워킹 관련 이벤트용 메시지에만 적용됩니다.

보안 이벤트에 대한 시스템 로그 메시지에는 다음 설정이 적용됩니다.

- **Logging Setup(**로깅 설정**)** 탭:
  - **EMBLEM** 형식으로 **syslog** 전송
- **Syslog Settings(Syslog** 설정**)** 탭:
  - **Syslog** 메시지에서 타임스탬프 활성화
  - 타임스탬프 형식
  - **Syslog** 디바이스 **ID** 활성화
- **Syslog Servers(Syslog** 서버**)** 탭:
  - **Add Syslog Server(Syslog** 서버 추가**)** 양식(및 구성된 서버 목록)의 모든 옵션

보안 이벤트 시스템 로그 메시지 구성 모범 사례, 2755 페이지도 참조하십시오.

로깅 활성화 및 기본 설정

시스템에서 데이터 플레인 이벤트에 대한 syslog 메시지를 생성하려면 로깅을 활성화해야 합니다.

또한 로컬 버퍼가 가득 차면 플래시 또는 FTP 서버를 스토리지 위치로 설정할 수 있습니다. 로깅 데이터를 저장한 후에 조작할 수 있습니다. 예를 들어 특정 유형의 syslog 메시지가 기록될 때 실행할 작업을 지정하고, 로그에서 데이터를 추출하고 보고를 위해 기록을 다른 파일에 저장하거나, 사이트별 스크립트를 사용하여 통계를 추적할 수 있습니다.

다음 절차에서는 몇 가지 기본 syslog 설정에 관해 설명합니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Syslog** > **Logging Setup(**로깅 설정**)**을 선택합니다.

단계 **3** 로깅을 활성화하고 기본 로깅 설정을 구성합니다.

- **Enable Logging(**로깅 활성화**)** - Firepower Threat Defense 디바이스의 데이터 플레인 시스템 로깅을 켭니다.
- **Enable Logging on the Failover Standby Unit(**장애 조치 대기 유닛에서 로깅 활성화**)** - 가능한 경우 Firepower Threat Defense 디바이스에 대한 대기 로깅을 켭니다.
- **Send syslogs in EMBLEM format(EMBLEM** 형식으로 **syslog** 전송**)** - 모든 로깅 대상에 대해 EMBLEM 형식 로깅을 활성화합니다. EMBLEM을 활성화하면 UDP 프로토콜을 사용하여 syslog 메시지를 게시해야 합니다. EMBLEM은 TCP와 호환되지 않습니다.

  참고 RFC5424 형식의 시스템 로그 메시지는 일반적으로 우선순위 값(PRI)을 표시합니다. 그러나 FMC에서 관리되는 FTD의 syslog 메시지에 PRI 값을 표시하려면 EMBLEM 형식을 활성화해야 합니다. PRI에 대한 자세한 내용은 RFC5424를 참조하십시오.

- **Send debug messages as syslogs(**디버그 메시지를 **syslog**로 전송**)** - 모든 디버그 추적 출력을 syslog로 리디렉션합니다. 이 옵션이 활성화되어 있으면 syslog 메시지가 콘솔에 표시되지 않습니다. 따라서 디버그 메시지를 보려면 콘솔에서 로깅을 활성화하고 디버그 syslog 메시지 번호 및 로깅 레벨에 대한 대상으로 구성해야 합니다. 사용할 syslog 메시지 번호는 711011입니다. 이 syslog의 기본 로깅 레벨은 디버그입니다.
- **Memory Size of Internal Buffer(**내부 버퍼의 메모리 크기**)** - 버퍼를 활성화한 경우 syslog 메시지가 저장되는 내부 로그 버퍼의 크기를 지정합니다. 버퍼는 가득 차면 덮어쓰기됩니다. 기본값은 4096바이트입니다. 범위는 4096~52428800입니다.

단계 **4** (선택 사항) **Enable Logging to FMC(FMC**에 로깅 활성화**)** 확인란을 선택하여 VPN 로깅을 활성화합니다. **Logging level(**로깅 레벨**)** 드롭다운 목록에서 VPN 메시지의 syslog 심각도 레벨을 선택합니다.

레벨에 대한 자세한 내용은 심각도 레벨, 1446 페이지 섹션을 참조하십시오.

단계 **5** (선택 사항) 버퍼를 덮어쓰기 전에 로그 버퍼 내용을 서버에 저장하려면 FTP 서버를 구성합니다. FTP 서버 정보를 지정합니다.

- **FTP Server Buffer Wrap(FTP** 서버 버퍼 랩**)** - 덮어쓰기 전에 버퍼 내용을 FTP 서버에 저장하려면 이 확인란을 선택하고 다음 필드에 필요한 대상 정보를 입력합니다. FTP 구성을 제거하려면 이 옵션의 선택을 취소합니다.
- **IP Address(IP** 주소**)** - FTP 서버의 IP 주소를 포함하는 호스트 네트워크 개체를 선택합니다.
- **User Name(**사용자 이름**)** - FTP 서버에 연결할 때 사용할 사용자 이름을 입력합니다.

- **Path(**경로**)** - 버퍼 내용을 저장해야 하는 FTP 루트에 상대적인 경로를 입력합니다.
- **Password/ Confirm(**비밀번호/확인**)** - FTP 서버에 대한 사용자 이름을 인증하는 데 사용되는 비밀번호를 입력하고 확인합니다.

단계 **6** (선택 사항) 버퍼를 덮어쓰기 전에 로그 버퍼 내용을 플래시에 저장하려면 플래시 크기를 지정합니다.

- **Flash(**플래시**)** - 덮어쓰기 전에 버퍼 내용을 플래시 메모리에 저장하려면 이 확인란을 선택합니다.
- **Maximum flash to be used by logging (KB)(**로깅에 사용할 최대 플래시**(KB))** - 로깅에 사용할 플래시 메모리의 최대 공간을 KB 단위로 지정합니다. 범위는 4-8044176 킬로바이트입니다.
- **Minimum free space to be preserved(KB)(**유지할 최소 여유 공간**(KB))** - 플래시 메모리에 유지할 최소 여유 공간을 KB 단위로 지정합니다. 범위는 0-8044176 킬로바이트입니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

로깅 대상 활성화

로깅 대상을 활성화하여 해당 대상에서 메시지를 볼 수 있도록 해야 합니다. 대상을 활성화할 때 대상에 대한 메시지 필터도 지정해야 합니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Syslog** > **Logging Destinations(**로깅 대상**)**을 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 대상을 활성화하고 로깅 필터를 적용하거나 기존 대상을 편집합니다.

단계 **4** **Logging Destinations(**로깅 대상**)** 대화 상자에서 대상을 선택하고 대상에 사용할 필터를 구성합니다.

a) **Logging Destination(**로깅 대상**)** 드롭다운 목록에서 활성화하려는 대상을 선택합니다. 대상 당 하나의 필터(콘솔, 이메일, 내부 버퍼, SNMP 트랩, SSH 세션 및 Syslog 서버)를 만들 수 있습니다.

참고 콘솔 및 SSH 세션 로깅은 진단 CLI에서만 작동합니다. **system support diagnostic-cli**을 입력합니다.

b) **Event Class(**이벤트 클래스**)**에서 테이블에 없는 모든 클래스에 적용할 필터를 선택합니다.

이러한 필터를 구성할 수 있습니다.

- **Filter on severity(**심각도 필터**)** - 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 대상으로 전송됩니다.
- **Use Event List(**이벤트 목록 사용**)** - 필터를 정의하는 이벤트 목록에서 선택합니다. **Event Lists(**이벤트 목록**)** 페이지에서 이러한 목록을 생성합니다.
- **Disable Logging(**로깅 비활성화**)** - 이 대상으로 메시지가 전송되지 않도록 합니다.

c) 이벤트 클래스당 필터를 작성하려면 **Add(**추가**)**를 클리하여 새 필터를 생성하거나 기존 필터를 편집하고 이벤트 클래스 및 심각도 레벨을 선택하여 해당 클래스의 메시지를 제한합니다. 필터를 저장하려면 **OK(**확인**)**를 클릭합니다.

이벤트 클래스에 대한 설명은 Syslog 메시지 클래스, 1447 페이지의 내용을 참조하십시오.

d) **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

이메일 주소로 **Syslog** 메시지 전송

Syslog 메시지가 이메일로 전송되도록 수신자 목록을 설정할 수 있습니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용을 참조하십시오.

시작하기 전에

- SMTP 서버 플랫폼 설정 페이지에서 SMTP 서버 구성
- 로깅 활성화 및 기본 설정, 1452 페이지
- 로깅 대상 활성화

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Syslog** > **Email Setup(**이메일 설정**)**을 선택합니다.

단계 **3** 이메일 메시지로 전송되는 syslog 메시지의 소스 주소로 사용할 이메일 주소를 지정합니다.

단계 **4** 지정된 syslog 메시지의 새로운 이메일 주소 수신자를 입력하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** 드롭다운 목록에서 수신자에게 전송되는 syslog 메시지의 심각도 레벨을 선택합니다.

대상 이메일 주소에 사용되는 syslog 메시지 심각도 필터는 지정된 심각도 레벨 이상의 메시지가 전송되도록 만듭니다. 레벨에 대한 자세한 내용은 심각도 레벨, 1446 페이지 섹션을 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

사용자 지정 이벤트 목록 생성

이벤트 목록은 어떤 메시지를 대상으로 전송할지 제어하기 위해 기록 대상에 적용할 수 있는 맞춤형 필터입니다. 일반적으로 심각도만을 기준으로 대상에 대한 메시지를 필터링하지만, 이벤트 목록을 사용하여 이벤트 클래스, 심각도 및 메시지 식별자(ID)의 조합을 기준으로 어떤 메시지를 전송할지 세부 조정할 수 있습니다.

사용자 정의 이벤트 목록을 만드는 과정은 두 단계로 이루어집니다. **Event Lists(**이벤트 목록**)**에서 사용자 정의 목록을 만든 다음 이벤트 목록을 사용하여 다양한 대상 유형에 대한 로깅 필터를 **Logging Destinations(**로깅 대상**)**에서 정의할 수 있습니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Syslog** > **Events List(**이벤트 목록**)**를 선택합니다.

단계 **3** 이벤트 목록을 구성합니다.

a) **Add(**추가**)**를 클릭하여 새 목록을 추가하거나 기존 목록을 편집합니다.

b) **Name(**이름**)**필드에 이벤트 이름을 입력합니다. 공백은 허용되지 않습니다.

c) 심각도 또는 이벤트 클래스를 기반으로 메시지를 식별하려면 **Severity/Event Class(**심각도/이벤트 클래스**)** 탭을 선택하고 항목을 추가하거나 편집합니다.

사용 가능한 클래스에 대한 내용은 Syslog 메시지 클래스, 1447 페이지 섹션을 참조하십시오.

레벨에 대한 자세한 내용은 심각도 레벨, 1446 페이지 섹션을 참조하십시오.

특정 이벤트 클래스는 투명 모드에서 해당 디바이스에 적용할 수 없습니다. 이러한 옵션이 구성되면 무시되며 구축되지 않습니다.

d) 메시지 ID별로 메시지를 식별하려면 **Message ID(**메시지 **ID)**를 선택하고 ID를 추가하거나 편집합니다.

하이픈을 사용하여 ID 범위를 입력할 수 있습니다(예: 100000-200000). ID는 6자리입니다. 처음 세 자리를 기능에 매핑하는 방법에 대한 내용은 Syslog 메시지 클래스, 1447 페이지 섹션을 참조하십시오.

특정 메시지 번호는 Cisco ASA Series Syslog Messages(Cisco ASA Series Syslog 메시지)를 참조하십시오.

e) 이벤트 목록을 저장하려면 **OK(**확인**)**를 클릭합니다.

단계 **4** **Logging Destinations(**로깅 대상**)**를 클릭하고 필터를 사용해야 하는 대상을 추가하거나 편집합니다.

로깅 대상 활성화, 1454 페이지의 내용을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**) > Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Syslog 메시지 생성 속도 제한

심각도 수준 또는 메시지 ID별로 syslog 메시지가 생성되는 속도를 제한할 수 있습니다. 각 로깅 수준 및 각 Syslog 메시지 ID에 대해 개별적인 제한을 지정할 수 있습니다. 설정이 충돌하면 Syslog 메시지 ID 제한이 우선 적용됩니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Syslog > Rate Limit(**속도 제한**)**을 선택합니다.

단계 **3** 심각도 레벨별로 메시지 생성을 제한하려면 **Logging Level(**로깅 레벨**) > Add(**추가**)**를 클릭하고 다음 옵션을 구성합니다.

- **Logging Level** - 속도를 제한하는 심각도 레벨입니다. 레벨에 대한 자세한 내용은 심각도 레벨, 1446 페이지 섹션을 참조하십시오.
- **Number of messages** - 지정된 기간에 허용된 지정된 유형의 최대 메시지 수입니다.
- **Interval** - 속도 제한 카운터가 재설정되기 전의 시간(초)입니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** syslog 메시지 ID별로 메시지 생성을 제한하려면 **Syslog Level(Syslog** 레벨**) > Add(**추가**)**를 클릭하고 다음 옵션을 구성합니다.

- **Syslog ID** - 속도를 제한하는 syslog 메시지 ID입니다. 특정 메시지 번호는 Cisco ASA Series Syslog Messages(Cisco ASA Series Syslog 메시지)를 참조하십시오.
- **Number of messages** - 지정된 기간에 허용된 지정된 유형의 최대 메시지 수입니다.
- **Interval** - 속도 제한 카운터가 재설정되기 전의 시간(초)입니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Syslog 설정

syslog 서버로 전송되는 syslog 메시지에 포함될 기능 코드를 설정하고, 각 메시지에 타임스탬프가 포함되는지 여부를 지정하고, 메시지에 포함할 디바이스 ID를 지정하고, 메시지의 심각도 레벨을 보고 수정하도록 일반 syslog 설정을 구성하고, 특정 메시지의 생성을 비활성화할 수 있습니다.

보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 이 페이지의 일부 설정은 이러한 메시지에 적용되지 않습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Syslog** > **Syslog Settings(Syslog** 설정**)**를 선택합니다.

단계 **3** **Facility(**시설**)** 드롭다운 목록에서 파일 메시지의 기반으로 사용할 syslog 서버에 대한 시스템 로그를 선택합니다.

기본값은 대부분의 UNIX 시스템이 기대하는 LOCAL4(20)입니다. 하지만 네트워크 디바이스가 이용 가능한 시설을 공유하기 때문에 시스템 로그에 대한 이 값을 변경해야 할 수 있습니다.

일반적으로 시설 값은 보안 이벤트의 메시지와는 무관합니다. 메시지에 시설 값을 포함해야 하는 경우 보안 이벤트 시스템 로그 메시지의 시설, 2767 페이지 섹션을 참조하십시오.

단계 **4** syslog 메시지에 메시지가 생성된 날짜와 시간을 포함하려면 **Enable timestamp on each syslog message(**각 **Syslog** 메시지에서 타임스탬프 활성화**)** 확인란을 선택합니다.

단계 **5** syslog 메시지에 대한 **Timestamp Format(**타임스탬프 형식**)**을 선택합니다.

- 레거시(MMM dd yyyy HH:mm:ss) 형식은 syslog 메시지의 기본 형식입니다.

  이 타임스탬프 형식을 선택하면 메시지에 시간대가 표시되지 않으며 항상 UTC입니다.

- RFC 5424(yyyy-MM-ddTHH:mm:ssZ)는 RFC 5424 syslog 형식에 지정된 대로 ISO 8601 타임스탬프 형식을 사용합니다.

  RFC 5424 형식을 선택하는 경우 각 타임스탬프 끝에 "Z"가 추가되어 타임스탬프가 UTC 시간대를 사용함을 나타냅니다.

단계 **6** 메시지의 시작 부분에 있는 syslog 메시지에 디바이스 식별자를 추가하려면 **Enable Syslog Device ID(Syslog** 디바이스 **ID** 활성화**)** 확인란을 선택한 다음 ID 유형을 선택합니다.

- **Interface(**인터페이스**)** - 어플라이언스가 메시지를 보내는 인터페이스와 상관없이 선택한 인터페이스의 IP 주소를 사용합니다. 인터페이스를 식별하는 보안 영역을 선택합니다. 영역은 단일 인터페이스로 매핑되어야 합니다.
- **User Defined ID(**사용자 정의 **ID)** - 선택한 텍스트 문자열(최대 16자)을 사용합니다.
- **Host Name(**호스트 이름**)** - 디바이스의 호스트 이름을 사용합니다.

단계 **7** Syslog Message 테이블을 사용하여 특정 syslog 메시지의 기본 설정을 변경합니다. 기본 설정을 변경하려는 경우에만 이 테이블에서 규칙을 구성해야 합니다. 메시지에 할당된 심각도를 변경하거나 메시지 생성을 비활성화할 수 있습니다.

기본적으로 Netflow가 활성화되고 항목이 테이블에 표시됩니다.

a) Netflow로 인해 중복되는 syslog 메시지를 표시하지 않으려면 **Netflow Equivalent Syslogs**를 선택합니다.

이렇게 하면 메시지가 억제된 메시지로 테이블에 추가됩니다.

참고 이러한 syslog 항목 중 하나라도 이미 테이블에 있으면 기존 규칙을 덮어쓰지 않습니다.

b) 새 규칙을 추가하려면 **Add(**추가**)**를 클릭합니다.

c) **Syslog ID** 드롭다운 목록에서 구성을 변경하려는 메시지 번호를 선택한 다음 **Logging Level(**로깅 레벨**)** 드롭다운 목록에서 새 심각도 레벨을 선택하거나 **Suppressed(**억제**)**를 선택하여 메시지 생성을 비활성화합니다. 일반적으로 심각도 레벨을 변경하지 않고 메시지를 비활성화하지 않지만 원하는 경우 두 필드를 모두 변경할 수 있습니다.

d) 테이블에 규칙을 추가하려면 **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지

Syslog 서버 설정

시스템에서 생성한 메시지를 처리하는 시스템 로그 서버를 구성하려면 다음 단계를 수행합니다.

이 시스템 로그 서버가 연결 및 침입 이벤트와 같은 보안 이벤트를 수신하도록 하려는 경우 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지의 내용도 참조하십시오.

시작하기 전에

- 로깅 지침, 1450 페이지의 요구 사항을 참조하십시오.
- 디바이스가 네트워크의 시스템 로그 수집기에 연결할 수 있는지 확인합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Syslog** > **Syslog Server(Syslog** 서버**)**를 선택합니다.

단계 **3** TCP 프로토콜을 사용하는 syslog 서버가 다운된 경우 트래픽을 허용하려면 **Allow user traffic to pass when TCP syslog server is down(TCP syslog** 서버가 중단되었을 때 사용자 트래픽이 전달되도록 허용**)** 확인란을 선택합니다.

단계 **4** syslog 서버가 **Message queue size (messages)(**메시지 대기열 크기**(**메시지**))** 필드에서 사용 중일 때 보안 어플라이언스에 syslog 메시지를 저장하기 위한 대기열의 크기를 입력 최소값은 메시지 1개입니다. 기본값은 512입니다. 무제한 메시지 수가 대기열에 포함되도록 허용하려면 0을 지정합니다(사용 가능한 블록 메모리가 있는 경우).

단계 **5** **Add(**추가**)**를 클릭하여 새 syslog 서버를 추가합니다.

a) **IP Address(IP** 주소**)** 드롭다운 목록에서 syslog 서버의 IP 주소를 포함하는 호스트 네트워크 개체를 선택합니다.

b) 프로토콜(TCP 또는 UDP)을 선택하고 Firepower Threat Defense 디바이스와 syslog 서버 간의 통신 포트 번호를 입력합니다.

UDP는 TCP에 비해 속도가 빠르고 디바이스의 리소스를 적게 사용합니다.

기본 포트는 UDP의 경우 514, TCP의 경우 1470입니다. 각 프로토콜에 대한 유효한 비 기본 포트 값은 1025부터 65535입니다.

c) **Log messages in Cisco EMBLEM format (UDP only)(Cisco EMBLEM** 형식 로그 메시지**(UDP** 전용**))** 확인란을 선택하여 Cisco EMBLEM 형식의 메시지 로깅 여부를 지정합니다(프로토콜로 UDP가 선택된 경우만 사용 가능).

참고 RFC5424 형식의 시스템 로그 메시지는 일반적으로 우선순위 값(PRI)을 표시합니다. 그러나 FMC에서는 Cisco EMBLEM 형식으로 로깅을 활성화하는 경우에만 관리되는 FTD의 시스템 로그 메시지에 있는 PRI 값이 표시됩니다. PRI에 대한 자세한 내용은 RFC5424를 참조하십시오.

d) TCP를 통한 SSL/TLS를 사용하여 디바이스와 서버 간의 연결을 암호화하려면 Enable Secure Syslog(보안 Syslog 활성화) 확인란을 선택합니다.

참고 이 옵션을 사용하려면 TCP를 프로토콜로 선택해야 합니다. 또한 **Devices(**디바이스**)** > **Certificates(**인증서**)** 페이지에서 시스템 로그 서버와 통신하는 데 필요한 인증서를 업로드해야 합니다. 마지막으로, Firepower Threat Defense 디바이스에서 syslog 서버로 인증서를 업로드하여 보안 관계를 완료하고 트래픽의 비밀번호를 해독하도록 허용합니다. **Enable Secure Syslog(**보안 시스템 로그 활성화**)** 옵션은 디바이스 관리 인터페이스에서 지원되지 않습니다.

e) syslog 서버와 통신하려면 **Device Management Interface(**디바이스 관리 인터페이스**)** 또는 **Security Zones or Named Interfaces(**보안 영역 또는 이름이 지정된 인터페이스**)**를 선택합니다.

- **Device Management Interface(**디바이스 관리 인터페이스**)**: 관리 인터페이스에서 시스템 로그를 전송합니다. Snort 이벤트에서 시스템 로그를 설정할 때 이 옵션을 사용하는 것이 좋습니다.

  참고 디바이스 관리 인터페이스 옵션은 **Enable Secure Syslog(**보안 시스템 로그 활성화**)** 옵션을 지원하지 않습니다.

- **Security Zones or Named Interfaces(**보안 영역 또는 이름이 지정된 인터페이스**)**: **Available Zones(**사용 가능한 영역**)** 목록에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭합니다.진단 인터페이스 이름을 입력하는 경우, 진단 인터페이스(**Device Management(**디바이스 관리**)** 페이지에서 디바이스 설정을 편집하고 **Interfaces(**인터페이스**)** 탭 선택)에 대한 IP 주소를 설정해야 합니다. 관리/진단 인터페이스에 대한 자세한 내용은 진단 인터페이스, 783 페이지의 내용을 참조하십시오.

f) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

전역 시간 제한 구성

다양한 프로토콜의 연결 및 변환 슬롯에 대해 전역 유휴 타임아웃 시간을 설정할 수 있습니다. 지정한 유휴 시간 동안 슬롯이 사용되지 않은 경우 리소스가 해제 풀로 반환됩니다.

디바이스와 콘솔 세션에 대한 시간 제한을 설정할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Timeouts(**시간 제한**)**를 선택합니다.

단계 **3** 변경하려는 시간 제한을 구성합니다.

지정된 설정에 대해 **Custom(**사용자 정의**)**을 선택하여 고유 값을 정의하고, **Default(**기본값**)**를 선택하여 시스템 기본값으로 되돌립니다. 대부분의 경우 최대 시간 제한은 1193시간입니다.

Disable(비활성화**)**을 선택하여 일부 시간 제한을 비활성화할 수 있습니다.

- **Console Timeout(**콘솔 시간 초과**)** - 콘솔 연결이 끊어질 때까지의 유휴 시간이며, 범위는 0 또는 5~1440분입니다. 기본값은 0입니다. 즉 세션에 시간 제한이 없습니다. 값을 변경하면 기존 콘솔 세션에서 이전 시간 제한 값을 사용합니다. 새 값은 새 연결에만 적용됩니다.
- **Translation Slot (xlate)**—변환 슬롯이 해제될 때까지의 유휴 시간입니다. 이 기간은 1분 이상이어야 합니다. 기본값은 3시간입니다.
- **Connection (Conn)**—연결 슬롯이 해제되기 전에 경과해야 하는 유휴 시간입니다. 이 시간은 5분 이상이어야 합니다. 기본값은 1시간입니다.
- **Half-Closed**—절반이 닫힌 TCP 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 최소값은 30초입니다. 기본값은 10분입니다.
- **UDP**—UDP 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 이 시간은 1분 이상이어야 합니다. 기본값은 2분입니다.
- **ICMP**—UDP 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 기본값 및 최소값은 2초입니다.
- **RPC/Sun RPC**—SunRPC 슬롯이 해제될 때까지의 유휴 시간입니다. 이 시간은 1분 이상이어야 합니다. 기본값은 10분입니다.

  Sun RPC 기반 연결에서 상위 연결이 삭제되거나 시간 초과되면, 새로운 하위 연결은 상위-하위 연결의 일부로 간주되지 않을 수도 있으며 시스템의 정책 또는 규칙 모음에 따라 평가될 수 있습니다. 상위 연결의 시간이 초과되면 기존 하위 연결은 설정한 시간 제한 값에 도달할 때까지만 사용할 수 있습니다.
- **H. 225**—H.225 신호 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 기본값은 1시간입니다. 모든 호출이 지원진 직후 연결을 닫으려면 타임아웃은 1초(0:0:1)가 좋습니다.
- **H. 323**—H.245(TCP) 및 H.323(UDP) 미디어 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 기본값 및 최소값은 5분입니다. H.245 및 H.323 미디어 연결 모두에 동일한 연결 플래그가 설정되어 있으므로 H.245(TCP) 연결에서 H.323(RTP 및 RTCP) 미디어 연결과 유휴 타임아웃을 공유합니다.
- **SIP**—SIP 신호 포트 연결이 닫힐 때까지의 유휴 시간입니다. 이 시간은 5분 이상이어야 합니다. 기본값은 30분입니다.
- **SIP Media**—SIP 미디어 포트 연결이 닫힐 때까지의 유휴 시간입니다. 이 시간은 1분 이상이어야 합니다. 기본값은 2분입니다. SIP 미디어 타이머는 UDP 비활성 타임아웃 대신 SIP UDP 미디어 패킷이 있는 SIP RTP/RTCP에 사용됩니다.
- **SIP Disconnect**—CANCEL 또는 BYE 메시지에 대해 200 OK를 수신하지 못한 경우 SIP 세션이 삭제되기까지의 유휴 시간(0:0:1~0:10:0)입니다. 기본값은 2분(0:2:0)입니다.
- **SIP Invite**—PROVISIONAL 응답 및 미디어 xlate에 대한 핀홀이 닫히기 전까지 경과해야 하는 유휴 시간(0:1:0~00:30:0)입니다. 기본값은 3분(0:3:0)입니다.
- **SIP Provisional Media**—SIP 프로비전 미디어 연결에 대한 타임아웃 값(1~30분)입니다. 기본은 2분입니다.

- **Floating Connection**—여러 경로가 서로 다른 메트릭으로 네트워크에 존재하는 경우 ASA는 연결 생성 시 최상의 메트릭이 있는 경로를 사용합니다. 더 나은 경로를 사용할 수 있게 되면 연결을 다시 설정하여 해당 경로를 사용할 수 있도록 이 시간 제한을 통해 연결을 닫을 수 있습니다. 기본값은 0(연결이 시간 초과되지 않음)입니다. 더 나은 경로를 사용하려면 타임아웃 값을 0:0:30~1193:0:0로 설정합니다.
- **PAT Xlate**—PAT 변환 슬롯이 해제될 때까지의 유휴 시간(0:0:30~0:5:0)입니다. 기본값은 30초입니다. 이전 연결이 업스트림 디바이스에서 여전히 열려 있을 수 있기 때문에 업스트림 라우터가 확보된 PAT 포트를 사용하는 새 연결을 거부하는 경우 시간 제한을 늘릴 수 있습니다.
- **TCP Proxy Reassembly**—리어셈블리를 기다리는 버퍼링된 패킷이 삭제되기 전에 경과해야 하는 유휴 타임아웃(0:0:10~1193:0:0)입니다. 기본값은 1분(0:1:0)입니다.
- **ARP Timeout**—(투명 모드에만 해당) ARP 테이블 재작성 간격(초)이며 범위는 60초~4294967초입니다. 기본값은 14,400초(4시간)입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Threat Defense를 위한 NTP 시간 동기화 구성

디바이스에서 클럭 설정을 동기화하려면 NTP(Network Time Protocol) 서버를 사용합니다. FMC에서 관리하는 모든 FTD을(를) FMC과(와) 동일한 NTP 서버를 사용하도록 설정하는 것이 좋습니다. FTD은(는) 설정된 NTP 서버에서 직접 시간을 가져옵니다. FTD의 설정된 NTP 서버에 연결할 수 없는 경우와 시간을 FMC과(와) 동기화합니다.

디바이스는 NTPv4를 지원합니다.

참고 Firepower 4100/9300 섀시에 FTD를 구축 중인 경우, Smart Licensing의 올바른 작동 및 디바이스 등록 시 올바른 타임스탬프를 보장하려면 Firepower 4100/9300 섀시에서 NTP를 구성해야 합니다. Firepower 4100/9300 섀시 및 Firepower Management Center에 대해 동일한 NTP 서버를 사용해야 합니다.

시작하기 전에

- 조직에 FTD가 연결할 수 있는 하나 이상의 NTP 서버가 있는 경우, FMC의 **System(**시스템**)** > **Configuration(**구성**)** 페이지에서 시간 동기화를 위해 구성한 디바이스용으로 동일한 하나 이상의 NTP 서버를 사용합니다.
- FMC에 대한 NTP 서버 또는 서버 모음을 구성할 때 **Use the authenticated NTP server only(**인증된 **NTP** 서버만 사용**)**를 선택했다면, 디바이스는 FMC(으)로 인증하도록 구성된 NTP 서버 또는 서버 모음만 사용합니다. (매니지드 디바이스는 FMC와 동일한 NTP 서버를 사용하지만, NTP 연결에서는 인증을 사용하지 않습니다.)

- 디바이스가 NTP 서버에 연결할 수 없거나 조직에 NTP 서버가 없는 경우에는 다음 절차에 설명된 대로 **Via NTP from Defense Center(**방어 센터에서 **NTP**를 통해**)** 옵션을 사용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

단계 **2** **Time Synchronization(**시간 동기화**)**을 선택합니다.

단계 **3** 다음 클릭 옵션 중 하나를 구성합니다.

- **Via NTP from Defense Center(**방어 센터에서 **NTP**를 통해**)**—(기본값). 매니지드 디바이스는 Firepower Management Center에 대해 설정한 NTP 서버에서 시간을 가져오고 (인증된 NTP 서버 제외) 시간을 해당 서버와 직접 동기화합니다. 그러나 다음 중 하나라도 해당하는 경우 매니지드 디바이스는 Firepower Management Center에서 시간을 동기화합니다.
  - Firepower Management Center의 NTP 서버는 디바이스에서 연결할 수 없습니다.
  - Firepower Management Center에 인증되지 않은 서버가 없습니다.
- **Via NTP from(NTP**를 통해**)** - Firepower Management Center가 네트워크에서 NTP 서버를 사용 중인 경우, 이 옵션을 선택하고 정규화된 DNS 이름(예: ntp.example.com) 또는 FMC의 **System(**시스템**)** > **Configuration(**구성**)** > **Time Synchronization(**시간 동기화**)**에서 지정한 동일한 NTP 서버의 IPv4 또는 IPv6 주소를 입력합니다. NTP 서버에 연결할 수없는 경우 Firepower Management Center는 NTP 서버로 작동합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 정책이 디바이스에 할당되었는지 확인합니다. 플랫폼 설정 정책에 대한 대상 디바이스 설정, 1403 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- Firepower System이 기본 디바이스를 포함하는 경우, 해당 디바이스에 대해 시간 동기화를 설정합니다. NTP 서버와 클래식 디바이스의 시간 동기화, 1413 페이지의 내용을 참조하십시오.

정책 애플리케이션에 대한 디바이스 표준 시간대 구성

기본적으로 시스템은 UTC 표준 시간대를 사용합니다. 디바이스에 대해 다른 표준 시간대를 지정하려면 이 절차를 사용합니다.

지정하는 표준 시간대는 이 기능을 지원하는 정책의 시간 기반 정책 애플리케이션에만 사용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 FTD 정책을 생성하거나 수정합니다.

Objects(개체**)** > **Object Management(**개체 관리**)** > **Time Zone(**표준 시간대**)** 페이지에서 표준 시간대 개체를 생성 할 수도 있습니다.

단계 **2** +를 클릭하여 새 표준 시간대 개체를 생성합니다.

단계 **3** 표준 시간대를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 정책이 디바이스에 할당되었는지 확인합니다. 플랫폼 설정 정책에 대한 대상 디바이스 설정, 1403 페이지의 내용을 참조하십시오.
- 시간 범위 개체를 생성하고, 액세스 제어 및 사전 필터 규칙에서 적용 가능한 시간 범위를 선택하고, 올바른 시간대와 연결된 디바이스에 상위 정책을 할당합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

Firepower Threat Defense 플랫폼 설정 기록

기능	버전	세부 사항
디바이스의 표준 시간대 지정	6.6	시간 기반 정책 애플리케이션에 사용할 매니지드 디바이스의 로컬 표준 시간대를 지정합니다. 새 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Time Zone(**시간대**)** 지원 플랫폼: Firepower Threat Defense
SNMP 통신용 관리 인터페이스 지정	6.6	이제 디바이스와 SNMP 관리 스테이션 간의 통신에 관리 인터페이스를 선택할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SNMP** > **Hosts(**호스트**)** 지원 플랫폼: Firepower Threat Defense

기능	버전	세부 사항
SNMPv3 사용자의 권한 부여 알고리즘에 SHA256 지정	6.6	이제 SNMPv3 사용자의 권한 부여 알고리즘에 대해 SHA256을 선택할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SNMP** > **Users(**사용자**)** 지원 플랫폼: Firepower Threat Defense
Threat Defense에서 SNMPv3 사용자에 대한 DES 암호화 및 MD5 인증 알고리즘은 더 이상 사용되지 않습니다.	6.5	Firepower Threat Defense 디바이스의 SSNMPv3 사용자에 대해서는 MD5 인증 알고리즘 또는 DES 암호화를 사용하지 않는 것이 좋습니다. 이는 더 이상 사용되지 않으며 향후 Firepower 버전에서 제거될 가능성이 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SNMP** > **Users(**사용자**)** 지원 플랫폼: Firepower Threat Defense
Threat Defense의 SNMPv3 사용자에 대한 DES 암호화 및 MD5 인증 알고리즘은 곧 사용이 중단됩니다.	6.4	Firepower Threat Defense 디바이스의 SNMPv3 사용자에 대해서는 MD5 인증 알고리즘 또는 DES 암호화를 사용하지 않는 것이 좋습니다. 향후 Firepower 버전에서 곧 사용이 중단됩니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SNMP** > **Users(**사용자**)** 지원 플랫폼: Firepower Threat Defense
SSH 로그인 실패 횟수를 제한합니다.	6.3	사용자가 SSH를 통해 디바이스에 액세스하고 3회 연속 로그인 시도가 실패한 경우, 해당 디바이스가 SSH 세션을 종료합니다.
UC/APPL 컴플라이언스 모드에 대한 지원	6.2.1	CC 모드 또는 UCAPL 모드에서 보안 인증서 컴플라이언스를 활성화할 수 있습니다. 보안 인증 컴플라이언스를 활성화한다고 해서 선택한 보안 모드의 모든 요구 사항이 반드시 엄격하게 준수되는 것은 아닙니다. 강화 절차에 대한 자세한 내용은 엔티티 인증을 통해 제공된 이 제품에 대한 지침을 참조하십시오. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **UC/APPL Compliance(UC/APPL** 컴플라이언스**)** 지원되는 플랫폼: 모든 디바이스

기능	버전	세부 사항
Remote Access VPN에 대한 SSL 설정	6.2.1	Firepower Threat Defense 디바이스는 SSL(Secure Sockets Layer) 프로토콜과 TLS(Transport Layer Security)를 사용하여 원격 클라이언트에서 Remote Access VPN 연결을 위한 보안 메시지 전송을 지원합니다. SSL을 통한 원격 VPN 액세스 중 메시지 전송을 위해 협상되고 사용되는 SSL 버전 및 암호화 알고리즘을 구성할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **SSL** 지원 플랫폼: Firepower Threat Defense
Firepower Threat Defense 지원	6.0.1	이 기능을 도입했습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** 지원 플랫폼: Firepower Threat Defense

55 장

보안 인증 컴플라이언스

다음 주제에서는 보안 인증 표준을 준수하도록 시스템을 구성하는 방법에 대해 설명합니다.

- 보안 인증 컴플라이언스 모드, 1469 페이지
- 보안 인증서 컴플라이언스 특성, 1470 페이지
- 보안 인증서 컴플라이언스 추천, 1472 페이지
- 보안 인증서 컴플라이언스 활성화, 1475 페이지

보안 인증 컴플라이언스 모드

조직에서는 미국국방부 및 글로벌 인증 기관이 마련한 보안 표준을 준수하는 장비 및 소프트웨어만 사용해야 할 수 있습니다. Firepower에서는 다음 보안 인증 표준에 대한 컴플라이언스를 지원합니다.

- CC(Common Criteria): 국제상호인정협정(Common Criteria Recognition Arrangement)에서 마련한 글로벌 표준으로, 보안 제품의 속성이 정의되어 있음
- UCAPL(Unified Capabilities Approved Products List): 미국국방부 정보시스템 계획국(U.S. Defense Information Systems Agency, DISA)이 마련한 보안 요구 사항을 충족하는 제품의 목록

참고 미국 정부에서 UCAPL(Unified Capabilities Approved Products List)의 이름을 DODIN APL(국방부 정보 네트워크 승인 제품 목록)로 변경했습니다. Firepower Management Center 웹 인터페이스 및 이 문서의 UCAPL에 대한 참조를 DODIN APL에 대한 참조로 해석할 수 있습니다.

- FIPS(Federal Information Processing Standard) 140: 암호화 모듈에 대한 요구 사항 사양

CC 모드 또는 UCAPL 모드에서 보안 인증서 컴플라이언스를 활성화할 수 있습니다. 보안 인증 컴플라이언스를 활성화한다고 해서 선택한 보안 모드의 모든 요구 사항이 반드시 엄격하게 준수되는 것은 아닙니다. 강화 절차에 대한 자세한 내용은 엔티티 인증을 통해 제공된 이 제품에 대한 지침을 참조하십시오.

주의 이 설정을 활성화한 후에는 비활성화할 수 없습니다. 어플라이언스를 CC 또는 UCAPL 모드에서 해제해야 한다면, 이미지로 다시 설치해야 합니다.

보안 인증서 컴플라이언스 특성

다음 표에서는 CC 또는 UCAPL 모드를 활성화하는 경우 동작 변경에 대해 설명합니다. (로그인 계정에 대한 제한은 웹 인터페이스 액세스가 아닌 명령줄 액세스를 의미합니다.)

시스템 변경	**CC** 모드	**UCAPL** 모드
FIPS 컴플라이언스 활성화됨	예	예
시스템에서 백업 또는 보고서를 위한 원격 스토리지를 허용하지 않습니다.	예	예
시스템이 추가 시스템 감사 데몬을 시작합니다.	아니요	예
시스템 부트 로더가 보호됩니다.	아니요	예
시스템은 로그인 계정에 추가 보안을 적용합니다.	아니요	예
시스템은 재부팅 키 시퀀스 Ctrl-Alt-Del을 비활성화합니다.	아니요	예
시스템은 최대 10개의 동시 로그인 세션을 시행합니다.	아니요	예
시스템이 eStreamer를 사용하여 이벤트 데이터 내보내기를 지원하지 않습니다.	예	예
시스템은 로그인 계정에 대해 더 엄격한 보호 장치를 적용합니다. • 비밀번호는 대/소문자가 혼합된 영숫자 15자 이상이고 숫자를 하나 이상 포함해야 합니다. • 비밀번호는 사전에 나와 있는 단어를 사용할 수 없고 연속적으로 반복되는 문자를 포함할 수 없습니다. • 세 번 연속으로 로그인 시도에 실패한 후 시스템이 사용자를 잠금 처리합니다. 이 경우 관리자가 비밀번호를 재설정해야 합니다. • 시스템은 비밀번호 기록을 저장합니다.	아니요	예

시스템 변경	**Firepower Management Center**		클래식 관리 디바이스		**Firepower Threat Defense**	
	CC 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드
FIPS 컴플라이언스 활성화됨	예	예	예	예	예	예
시스템에서 백업 또는 보고서를 위한 원격 스토리지를 허용하지 않습니다.	예	예	—	—	—	—
시스템은 버전 6.2.2.1 및 이후 6.2.2.x 패치에 대해서만 eStreamer를 사용하여 이벤트 데이터 내보내기를 지원합니다.	예	예	예	예	—	—
시스템이 추가 시스템 감사 데몬을 시작합니다.	아니요	예	아니요	예	아니요	아니요
시스템 부트 로더가 보호됩니다.	아니요	예	아니요	예	아니요	아니요
시스템은 로그인 계정에 추가 보안을 적용합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 재부팅 키 시퀀스 Ctrl+Alt+Del을 비활성화합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 최대 10개의 동시 로그인 세션을 시행합니다.	아니요	예	아니요	예	아니요	아니요
비밀번호는 대/소문자가 혼합된 영숫자 15자 이상이고 숫자를 하나 이상 포함해야 합니다.	아니요	예	아니요	예	아니요	아니요
로컬 관리자 CLI의 최소 필수 암호 길이는 로컬 장치 CLI를 사용하여 구성할 수 있습니다.	아니요	아니요	아니요	아니요	예	예
비밀번호는 사전에 나와 있는 단어를 사용할 수 없고 연속적으로 반복되는 문자를 포함할 수 없습니다.	아니요	예	아니요	예	아니요	아니요
세 번 연속으로 로그인 시도에 실패한 후 시스템이 관리자가 아닌 사용자를 잠금 처리합니다. 이 경우 관리자가 비밀번호를 재설정해야 합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 기본적으로 비밀번호 기록을 저장합니다.	아니요	예	아니요	예	아니요	아니요
관리자는 웹 인터페이스를 통해 구성할 수 있는 최대 로그인 시도 실패 횟수가 초과된 후에 잠금 처리될 수 있습니다.	예	예	예	예	—	—

시스템 변경	**Firepower Management Center**		클래식 관리 디바이스		**Firepower Threat Defense**	
	CC 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드
관리자는 로컬 어플라이언스 CLI를 통해 구성할 수 있는 최대 로그인 시도 실패 횟수가 초과된 후에 잠금 처리될 수 있습니다.	아니요	아니요	예, 보안 인증서 컴플라이언스 활성화 여부와 관계없습니다.	예, 보안 인증서 컴플라이언스 활성화 여부와 관계없습니다.	예	예
다음의 경우 시스템이 어플라이언스와 함께 SSH 세션을 자동으로 재설정합니다. • 세션 활동 1시간 동안 키가 사용된 후 • 연결을 통해 1GB의 데이터를 전송하는 데 키가 사용된 후	예	예	예	예	예	예
시스템은 부팅 시 FSIC(파일 시스템 무결성 검사)를 수행합니다. FSIC가 실패하면 Firepower 소프트웨어가 시작되지 않고 원격 SSH 액세스가 비활성화되며 로컬 콘솔을 통해서만 어플라이언스에 액세스할 수 있습니다. 이러한 현상이 발생하는 경우 Cisco TAC에 문의하십시오.	예	예	예	예	예	예

보안 인증서 컴플라이언스 추천

보안 인증서 컴플라이언스가 설정된 시스템을 사용하는 경우 다음 모범 사례를 준수하는 것이 좋습니다.

- 구축에서 보안 인증서 컴플라이언스를 활성화하려면 먼저 Firepower Management Center에서 보안 인증을 활성화한 다음 모든 매니지드 디바이스에서 동일한 모드로 활성화합니다.

  ⚠

  주의 Firepower Management Center는 둘 다 동일한 보안 인증서 컴플라이언스 모드에서 작동하지 않는 한 매니지드 디바이스에서 이벤트 데이터를 수신하지 않습니다.

- 모든 사용자에 대해 비밀번호 강도 검사를 활성화하고 인증 기관에 요구하는 값으로 최소 비밀번호 길이를 설정합니다.
- 고가용성 구성에서 Firepower Management Center를 사용하는 경우 동일한 보안 인증서 컴플라이언스 모드를 사용하도록 구성합니다.

- Firepower 4100/9300 섀시에서 Firepower Threat Defense가 CC 또는 UCAPL 모드에서 작동하도록 구성하는 경우 CC 모드에서 작동하도록 Firepower 4100/9300 섀시도 구성해야 합니다. 자세한 내용은 *Cisco FXOS Firepower Chassis Manager* 환경 설정 가이드를 참조하십시오.
- 다음 기능 중 하나를 사용하도록 시스템을 구성하지 마십시오.
  - 이메일 보고서, 알림 또는 데이터 정리 알림.
  - Nmap 스캔, Cisco IOS Null Route, 속성 값 설정 또는 ISE EPS 재조정
  - 백업 또는 보고서를 위한 원격 스토리지
  - 시스템 데이터베이스에 대한 타사 클라이언트 액세스
  - 이메일(SMTP), SNMP 트랩 또는 시스템 로그를 통해 전송되는 외부 알림 또는 경고
  - 어플라이언스와 서버 사이의 채널을 보호하기 위해 SSL 인증서를 사용하지 않고 HTTP 서버 또는 시스템 로그 서버로 전송된 감사 로그 메시지
  - eStreamer를 사용하여 이벤트 데이터를 외부 클라이언트로 내보내기
- 버전 6.1.0.6 및 후속 6.1.0.x 패치에 대해서만 eStreamer를 사용하여 이벤트 데이터를 외부 클라이언트로 내보내도록 시스템을 구성할 수 있습니다.
- 버전 6.2.2.1 및 후속 6.2.2.x 패치에 대해서만 eStreamer를 사용하여 이벤트 데이터를 외부 클라이언트로 내보내도록 시스템을 구성할 수 있습니다.
- CC 모드를 이용하는 구축에서는 LDAP 또는 RADIUS를 사용하여 외부 인증을 활성화하지 마십시오.
- CC 모드를 사용하는 구축에서는 CAC를 활성화하지 마십시오.
- CC 또는 UCAPL 모드를 사용하는 구축에서는 Firepower REST API를 통해 Firepower Management Center 및 매니지드 디바이스에 대한 액세스를 비활성화합니다.
- UCAPL 모드를 사용하는 구축에서 CAC를 활성화합니다.
- CC 모드를 사용하는 구축에서는 SSO를 설정하지 마십시오.
- 디바이스가 모두 동일한 보안 인증서 컴플라이언스 모드를 사용하지 않는 한 고가용성 쌍으로 Firepower Threat Defense 디바이스를 구성하지 마십시오.

참고 Firepower System은 스택 또는 고가용성 쌍의

- 스택 및 고가용성 쌍의 클래식 디바이스
- Firepower Threat Defense 클러스터의 디바이스
- Firepower Threat Defense 컨테이너 인스턴스: Firepower 4100/9300

어플라이언스 강화

Firepower 시스템을 더욱 강화할 수 있는 기능 관련 정보는 최신 버전 *Cisco Firepower Mangement Center* 강화 가이드와 *Cisco Firepower Threat Defense* 강화 가이드 및 이 문서의 다음 주제에서 확인할 수 있습니다.

- Firepower System 라이선싱, 157 페이지
- Firepower System 사용자 인증FMC의 사용자 계정, 49 페이지
- Firepower System에 로그인, 25 페이지
- 감사 로그, 1371 페이지
- 감사 로그 인증서
- 시간 및 시간 동기화, 1379 페이지
- Threat Defense를 위한 NTP 시간 동기화 구성, 1463 페이지
- 이메일 알림 응답 생성, 2687 페이지
- 침입 이벤트에 대한 이메일 알림 설정, 2696 페이지
- SMTP 설정, 1437 페이지
- Firepower 1000/2100 시리즈용 SNMP 정보, 873 페이지
- Threat Defense에 대한 SNMP 설정, 1437 페이지
- SNMP 알림 응답 생성, 2683 페이지
- 동적 DNS 구성, 865 페이지
- DNS 캐시, 1373 페이지
- 시스템 감사, 449 페이지
- 액세스 목록, 1370 페이지
- 보안 인증 컴플라이언스, 1469 페이지
- 원격 스토리지에 대한 SSH 설정, 1366 페이지
- 감사 로그 인증서
- HTTPS 인증서, 1344 페이지
- 사용자 역할웹 인터페이스의 사용자 역할 맞춤화, 127 페이지
- 사용자 계정내부 사용자 추가, 55 페이지
- 세션 시간 초과, 1388 페이지
- 시스템 로그 구성 관련 정보, 1445 페이지
- FMC 백업 예약, 248 페이지

- Site-to-Site VPN Firepower Threat Defense, 1133 페이지
- Remote Access VPN Firepower Threat Defense, 1155 페이지
- Firepower Threat Defense에 대한 FlexConfig 정책, 1269 페이지

네트워크 보호

네트워크 보호를 위해 구성 할 수 있는 Firepower System 기능에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 액세스 제어 정책, 1625 페이지
- 보안 인텔리전스 차단 목록, 1695 페이지
- 침입 정책 시작하기, 1995 페이지
- 규칙을 사용하여 침입 정책 조정, 2007 페이지
- 침입 규칙 편집기, 2063 페이지
- 침입 규칙 업데이트, 186 페이지
- 침입 이벤트 로깅 글로벌 제한, 2057 페이지
- 전송 및 네트워크 계층 전처리기, 2311 페이지
- 특정 위협 탐지, 2349 페이지
- 애플리케이션 레이어 프리프로세서, 2227 페이지
- IPS 디바이스 구축 및 구성, 697 페이지
- 시스템 감사, 449 페이지
- 침입 이벤트 작업, 2909 페이지
- 이벤트 검색, 2825 페이지
- 워크플로, 2781 페이지
- 디바이스 관리 기본 사항, 297 페이지
- 로그인 배너, 1376 페이지
- 시스템 업데이트, 179 페이지

보안 인증서 컴플라이언스 활성화

이 구성은 Firepower Management Center 또는 매니지드 디바이스에 적용됩니다.

- Firepower Management Center의 경우 이 구성은 시스템 구성에 포함되어 있습니다.

• 매니지드 디바이스의 경우, FMC의 이 구성을 플랫폼 설정 정책의 일부로 적용합니다.

두 경우 모두, 시스템 구성 변경 사항을 저장하거나 공유 플랫폼 설정 정책을 구축할 때까지 구성이 적용되지 않습니다.

⚠

주의 이 설정을 활성화한 후에는 비활성화할 수 없습니다. 어플라이언스를 CC 또는 UCAPL 모드에서 해제해야 한다면, 이미지로 다시 설치해야 합니다.

시작하기 전에

- Cisco에서는 모든 어플라이언스에서 보안 인증서 컴플라이언스를 활성화하기 전에 구축에 포함할 모든 디바이스를 FMC에 등록하는 방법을 권장합니다.
- Firepower Threat Defense 디바이스는 평가 라이선스를 사용할 수 없습니다. Cisco Smart Software Manager 계정에서 내보내기 제어 기능을 활성화해야 합니다.
- Firepower Threat Defense 디바이스는 라우팅 모드에서 구축해야 합니다.
- 이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** FMC 또는 매니지드 디바이스 중 무엇을 구성하는지에 따라 다음 작업을 수행합니다.

- FMC: **System(**시스템**)** > **Configuration(**구성**)**을(를) 선택합니다.
- 클래식 디바이스: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택하고 Firepower 정책을 생성하거나 수정합니다.
- FTD 디바이스: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택하고 Firepower Threat Defense 정책을 생성하거나 수정합니다.

단계 **2** **UCAPL/CC Compliance(UCAPL/CC** 규정준수**)**를 클릭합니다.

참고 UCAPL 또는 CC 컴플라이언스를 활성화하면 어플라이언스가 재부팅됩니다. 시스템 구성을 저장할 때 FMC가 재부팅됩니다. 매니지드 디바이스는 구성 변경 사항을 구축할 때 재부팅됩니다.

단계 **3** 어플라이언스에서 보안 인증서 컴플라이언스를 영구적으로 활성화하려면 다음 두 가지 중에서 선택할 수 있습니다.

- Common Criteria 모드에서 보안 인증서 컴플라이언스를 활성화하려면 드롭다운 목록에서 **CC**를 선택합니다.
- Unified Capabilities Approved Products List 모드에서 보안 인증서 컴플라이언스를 활성화하려면 드롭다운 목록에서 **UCAPL**을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 아직 수행하지 않았다면 구축의 모든 클래식 디바이스에 제어 및 보호 라이선스를 적용합니다.
- 인증 엔티티가 제공한 이 제품의 지침에 설명된 대로 추가 구성 변경을 설정합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

XIII 부

NAT(네트워크 주소 변환)

- NAT 정책 관리, 1481 페이지
- Firepower Threat Defense용 NAT(네트워크 주소 변환), 1487 페이지

56 장

NAT 정책 관리

다음 주제에서는 Firepower System의 NAT 정책을 관리하는 방법에 대해 설명합니다.

- NAT 정책 요구 사항 및 사전 요건, 1481 페이지
- NAT 정책 관리, 1482 페이지
- NAT 정책 생성, 1482 페이지
- NAT 정책 설정, 1483 페이지
- NAT 정책 대상 설정, 1485 페이지
- NAT 정책 복사, 1486 페이지

NAT 정책 요구 사항 및 사전 요건

모델 지원

모두, 그러나 디바이스 모델에 대해 올바른 유형의 정책을 선택해야 합니다.

- 7000 및 8000 Series 시리즈 디바이스용 **Firepower NAT**
- FTD 디바이스용 **Threat Defense NAT**

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

NAT 정책 관리

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인의 관리자는 하위 도메인에서 사용자 정의된 로컬 정책을 사용하거나 대체할 수 있는 상위 도메인의 디바이스에 NAT 정책을 지정할 수 있습니다. NAT 정책이 다른 하위 도메인의 디바이스를 대상으로 하는 경우 하위 도메인의 관리자는 자신의 도메인에 속한 대상 디바이스의 정보만 볼 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT** 을(를) 선택합니다.

단계 **2** 다음과 같이 NAT 정책을 관리합니다.

- 복사 - 복사할 정책 옆의 복사( )을 클릭합니다. NAT 정책 복사, 1486 페이지의 내용을 참조하십시오.
- 생성 - 새 정책을 클릭합니다. NAT 정책 생성, 1482 페이지를 참조하십시오.
- 삭제 - 삭제하려는 정책 옆의 삭제( )을 클릭하고 **OK(**확인**)**를 클릭합니다. 계속할지 여부를 물을 때 다른 사용자가 정책을 변경했고 저장하지 않았으면 알려줍니다.

  주의 관리되는 디바이스에 NAT 정책을 구축한 후에는 디바이스에서 정책을 삭제할 수 없습니다. 그러나 관리되는 디바이스에 이미 있는 NAT 규칙을 제거하려면 규칙이 없는 NAT 정책을 구축해야 합니다. 대상 디바이스에 마지막으로 구축한 정책은 최신 상태가 아니더라도 삭제할 수 없습니다. 정책을 완전히 삭제할 수 있으려면 해당 대상에 다른 정책을 구축해야 합니다.

- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- 편집 - 수정( )을 클릭합니다. NAT 정책 설정, 1483 페이지의 내용을 참조하십시오.
- 보고서- 보고서( )를 클릭합니다. 현재 정책 보고서 생성, 515 페이지를 참조하십시오.

NAT 정책 생성

새 NAT 정책을 생성할 때 최소한 고유한 이름을 지정해야 합니다. 사용자가 정책 생성 시간에 정책 대상을 확인해야 하는 것은 아니지만, 정책을 구축하기 전에 반드시 이 단계를 먼저 수행해야 합니다.

규칙 없는 NAT 정책을 디바이스에 적용하는 경우 시스템은 해당 디바이스에서 모든 NAT 규칙을 제거합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인의 관리자는 하위 도메인에서 사용자 정의된 로컬 정책을 사용하거나 대체할 수 있는 상위 도메인의 디바이스에 NAT 정책을 지정할 수 있습니다. NAT 정책이 다른 하위 도메인의 디바이스를 대상으로 하는 경우 하위 도메인의 관리자는 자신의 도메인에 속한 대상 디바이스의 정보만 볼 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT** 을(를) 선택합니다.

단계 **2** **New Policy(**새 정책**)** 드롭다운 목록에서 **Threat Defense NAT**를 선택합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 정책 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 정책 이름과의 충돌을 식별할 수 있습니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** 정책을 구축하려는 디바이스를 선택합니다.

- **Available Devices(**사용 가능한 디바이스**)** 목록에서 디바이스를 선택하고 **Add to Policy(**정책에 추가**)**를 클릭합니다.
- **Available Devices(**사용 가능한 디바이스**)** 목록의 디바이스를 클릭하여 **Selected Devices(**선택한 디바이스**)** 목록으로 끌어옵니다.
- 디바이스 옆에 있는 삭제( )을 클릭하여 **Selected Devices(**선택한 디바이스**)** 목록에서 디바이스를 제거합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

NAT 정책 설정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인의 관리자는 하위 도메인에서 사용자 정의된 로컬 정책을 사용하거나 대체할 수 있는 상위 도메인의 디바이스에 NAT 정책을 지정할 수 있습니다. NAT 정책이 다른 하위 도메인의 디바이스

를 대상으로 하는 경우 하위 도메인의 관리자는 자신의 도메인에 속한 대상 디바이스의 정보만 볼 수 있습니다.

인터페이스 유형을 해당 인터페이스가 있는 디바이스를 대상으로 하는 NAT 정책과 함께 사용하기에 적절하지 않은 유형으로 변경하면, 정책에는 해당 인터페이스가 삭제된 것으로 표시됩니다. 정책에서 인터페이스를 자동으로 제거하려면 NAT 정책에서 **Save(**저장**)**를 클릭합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT** 을(를) 선택합니다.

단계 **2** 수정하려는 NAT 정책 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** NAT 정책을 구성합니다.

- 정책 이름이나 설명을 수정하려면 **Name(**이름**)** 또는 **Description(**설명**)** 필드를 클릭하고 필요에 따라 문자를 삭제한 다음 새 이름이나 설명을 입력합니다. 다중 도메인 구축에서 정책 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 정책 이름과의 충돌을 식별할 수 있습니다.
- 정책 목표를 관리하려면 NAT 정책 대상 설정, 1485 페이지 섹션을 참조하십시오.
- 정책 변경 사항을 저장하려면 **Save(**저장**)**를 클릭합니다.
- 정책에 규칙을 추가하려면 **Add Rule(**규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙 옆의 수정( )을 클릭합니다.
- 규칙을 삭제하려면 규칙 옆의 삭제( )을 클릭한 다음 **OK(**확인**)**를 클릭합니다.
- 기존 규칙을 비활성화하려면 규칙을 마우스 오른쪽 버튼으로 클릭하고 **State(**상태**)**를 선택한 다음 **Disable(**비활성화**)** 또는 **Enable(**활성화**)**을 선택합니다.
- (Firepower NAT에만 해당) 특정 규칙 속성의 구성 페이지를 표시하려면 규칙 행의 조건 열에서 이름 또는 값을 클릭합니다. 이를테면 **Source Networks** 열의 이름이나 값을 클릭하여 선택한 규칙의 Source Network 페이지를 표시합니다.
- 정책의 경고나 오류를 보려면 **Show Warnings(**경고 표시**)**를 클릭하고 **Device(**디바이스**)**를 선택합니다. 경고 및 오류는 트래픽 흐름에 악영향을 미치거나 정책 배포를 방해할 수 있는 구성을 표시합니다.
- 페이지에 표시되는 규칙 수를 변경하려면 **Rows Per Page(**페이지당 행**)** 드롭다운 목록을 사용합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

NAT 정책 대상 설정

정책을 생성하거나 수정하는 동안 정책의 대상이 될 매니지드 디바이스를 식별할 수 있습니다. 사용 가능한 디바이스, 7000 또는 8000 Series 스택 및 고가용성 쌍의 목록을 검색하고, 이들을 선택한 디바이스 목록에 추가할 수 있습니다.

서로 다른 버전의 Firepower System을 실행하는 누적형 디바이스를 대상으로 할 수 없습니다(예를 들어, 디바이스 중 하나의 업그레이드가 실패할 경우).

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인의 관리자는 하위 도메인에서 사용자 정의된 로컬 정책을 사용하거나 대체할 수 있는 상위 도메인의 디바이스에 NAT 정책을 지정할 수 있습니다. NAT 정책이 다른 하위 도메인의 디바이스를 대상으로 하는 경우 하위 도메인의 관리자는 자신의 도메인에 속한 대상 디바이스의 정보만 볼 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT** 을(를) 선택합니다.

단계 **2** 수정하려는 NAT 정책 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** **Policy Assignments(**정책 할당**)**를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹을 정책에 할당하려면 **Available Devices(**사용 가능한 디바이스**)** 목록에서 이를 선택하고 **Add to Policy(**정책에 추가**)**를 클릭합니다. 아니면 끌어서 놓을 수도 있습니다.
- 디바이스 할당을 제거하려면 **Selected Devices(**선택한 디바이스**)** 목록의 디바이스, 스택, 고가용성 쌍 또는 디바이스 그룹 옆에 있는 삭제( )를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

NAT 정책 복사

NAT 정책의 사본을 만들 수 있습니다. 사본에는 모든 정책 규칙 및 구성이 포함됩니다.

다중 도메인 구축에서는 현재 도메인과 상위 도메인의 정책을 복사할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT** 을(를) 선택합니다.

단계 **2** 복사하려는 NAT 정책 옆의 복사 ( )을 클릭합니다.

단계 **3** 정책의 고유한 이름을 입력합니다.

다중 도메인 구축에서 정책 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 정책 이름과의 충돌을 식별할 수 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

57 장

Firepower Threat Defense용 NAT(네트워크 주소 변환)

다음 주제에서는 NAT(네트워크 주소 변환)에 대한 내용 및 Firepower Threat Defense 디바이스에 NAT를 구성하는 방법을 설명합니다.

- NAT를 사용해야 하는 이유, 1487 페이지
- NAT 기본 사항, 1488 페이지
- NAT용 지침, 1497 페이지
- Threat Defense NAT 구성, 1502 페이지
- IPv6 네트워크 변환, 1544 페이지
- NAT 모니터링, 1556 페이지
- NAT의 예, 1557 페이지
- FTD NAT 기록, 1604 페이지

NAT를 사용해야 하는 이유

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지 않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0~192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.
- IP 라우팅 솔루션 - NAT를 사용하는 경우 중첩 IP 주소 문제가 발생하지 않습니다.
- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

참고 NAT는 필수 항목이 아닙니다. 특정 트래픽에 대해 NAT를 구성하지 않으면 해당 트래픽은 변환되지 않지만, 모든 보안 정책은 정상적으로 적용됩니다.

NAT 기본 사항

다음 주제에서는 NAT의 기본 사항 일부를 설명합니다.

NAT 용어

이 설명서는 다음과 같은 용어를 사용합니다.

- 실제 주소/호스트/네트워크/인터페이스 - 실제 주소는 변환되기 전 호스트에서 정의된 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 내부 네트워크가 "실제" 네트워크일 수 있습니다. 내부 네트워크뿐 아니라 디바이스에 연결된 모든 네트워크를 변환할 수 있습니다. 따라서 외부 주소를 변환하도록 NAT를 구성하는 경우 "실제"는 내부 네트워크에 액세스하는 외부 네트워크를 지칭할 수 있습니다.
- 매핑된 주소/호스트/네트워크/인터페이스 - 매핑된 주소는 실제 주소가 변환되는 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 외부 네트워크가 "매핑된" 네트워크일 수 있습니다.

  참고 주소 변환 중에 디바이스 인터페이스용으로 구성된 IP 주소는 변환되지 않습니다.

- 양방향 시작 - 고정 NAT에서는 연결이 양방향으로 시작될 수 있습니다(호스트에서 나가기도 하고 호스트로 들어오기도 함).
- 소스 및 대상 NAT - 모든 패킷에 대해 소스 및 대상 IP 주소를 NAT 규칙과 비교하며, 하나 또는 둘 모두를 변환하거나 변환하지 않을 수 있습니다. 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "source(소스)"와 "destination(대상)"이 사용됩니다. 특정 연결이 "destination(대상)" 주소에서 시작되는 경우에도 마찬가지입니다.

NAT 유형

다음 방법을 사용하여 NAT를 구현할 수 있습니다.

- 동적 NAT - 실제 IP 주소의 그룹이 매핑된 IP 주소의 그룹(대개 더 작음)에 선착순으로 매핑됩니다. 실제 호스트만 트래픽을 시작할 수 있습니다. 동적 NAT, 1507 페이지의 내용을 참조하십시오.
- 동적 PAT(동적 포트 주소 변환) - 실제 IP 주소의 그룹이 해당 IP 주소의 고유한 소스 포트를 사용하여 단일 IP 주소로 매핑됩니다. 동적 PAT, 1513 페이지의 내용을 참조하십시오.
- 고정 NAT - 실제 IP 주소와 매핑된 IP 주소 간의 일관된 매핑입니다. 양방향 트래픽 시작이 허용됩니다. 고정 NAT, 1524 페이지의 내용을 참조하십시오.
- ID NAT - 실제 주소가 기본적으로 NAT를 우회하여 자신에게 고정으로 변환됩니다. 대규모 주소 그룹을 변환하되 좀 더 작은 규모의 주소 하위 집합을 제외하고자 할 경우 이 방법으로 NAT를 구성할 수 있습니다. ID NAT, 1533 페이지의 내용을 참조하십시오.

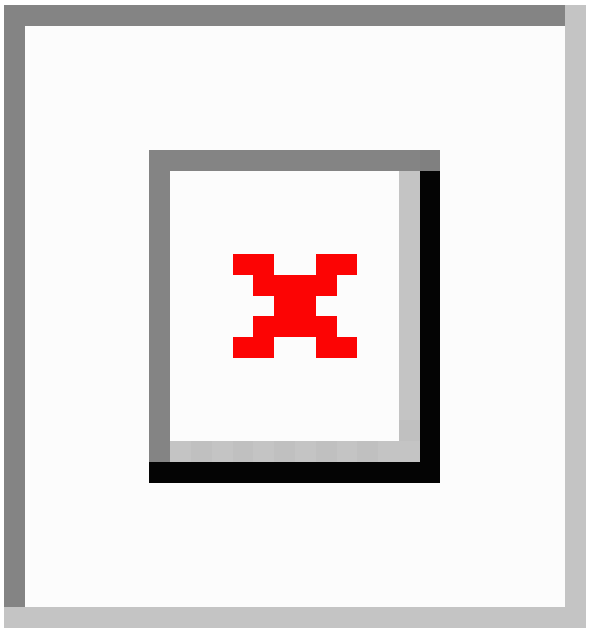
라우팅된 모드 및 투명 모드의 NAT

라우팅된 방화벽 모드와 투명 방화벽 모드에서 모두 NAT를 구성할 수 있습니다. 인라인, 인라인 탭 또는 수동 모드로 작동하는 인터페이스에 대해서는 NAT를 구성할 수 없습니다. 다음 섹션에서는 각 방화벽 모드의 일반적인 사용법에 대해 설명합니다.

라우팅 모드의 NAT

다음 그림은 내부에 사설 네트워크가 있는 라우팅된 모드의 일반적인 NAT 예를 보여줍니다.

그림 *47: NAT* 예*:* 라우팅된 모드



1. 10.1.2.27의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.2.27이 매핑된 주소 209.165.201.10으로 변환됩니다.
2. 서버가 응답하면 해당 호스트는 응답을 매핑된 주소 209.165.201.10으로 전송하며 Firepower Threat Defense 디바이스에서 패킷을 수신합니다. 이는 Firepower Threat Defense 디바이스에서 프록시 ARP를 수행하여 패킷을 신청하기 때문입니다.
3. 그런 다음 Firepower Threat Defense 디바이스에서는 호스트로 전송하기 전에, 매핑된 주소 209.165.201.10에서 다시 실제 주소 10.1.2.27로의 변환을 변경합니다.

투명 모드 또는 브리지 그룹 내 NAT

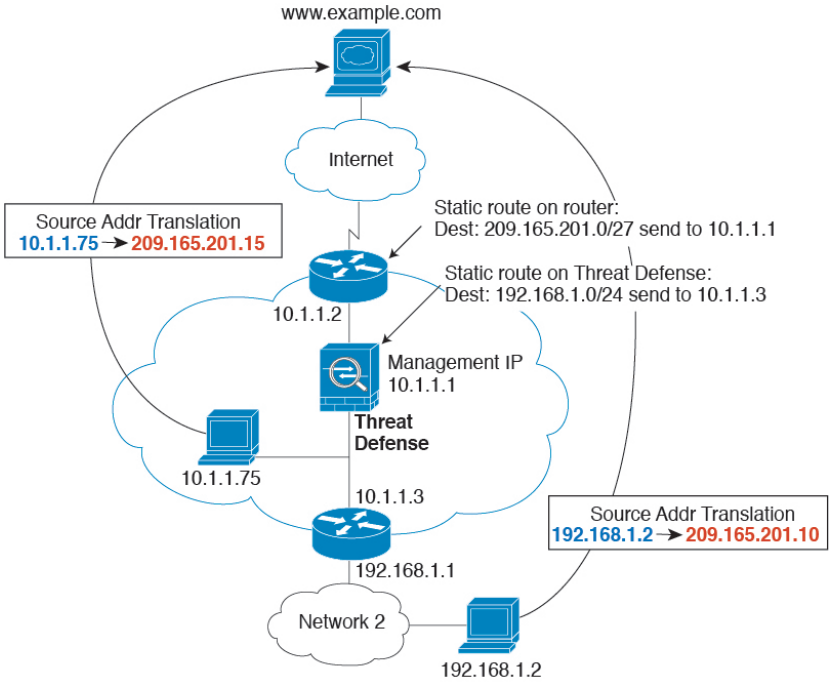
투명 모드에서 NAT를 사용하면 업스트림 또는 다운스트림 라우터가 네트워크에 대해 NAT를 수행할 필요가 없습니다. 라우팅 모드에서 브리지 그룹 내에 유사한 기능을 수행할 수 있습니다.

투명 모드의 NAT 또는 동일한 브리지 그룹의 멤버 간 라우팅 모드에서의 NAT에는 다음과 같은 요구사항과 제한 사항이 있습니다.

- 매핑된 주소가 브리지 그룹 멤버 인터페이스일 때는 인터페이스 PAT를 구성할 수 없습니다. 인터페이스에 연결된 IP 주소가 없기 때문입니다.
- ARP 검사는 지원되지 않습니다. 또한 Firepower Threat Defense 디바이스의 한 쪽에 있는 호스트가 어떤 이유로든 Firepower Threat Defense 디바이스의 다른 쪽에 있는 호스트로 ARP 요청을 전송하고, 시작한 호스트의 실제 주소가 동일한 서브넷의 다른 주소로 매핑되면, ARP 요청에 실제 주소가 가시적으로 남게 됩니다.
- IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 두 IPv6 네트워크 간 변환 또는 두 IPv4 네트워크 간 변환은 지원됩니다.

다음 그림은 내부 인터페이스와 외부 인터페이스의 네트워크가 동일한 투명 모드의 일반적인 NAT 시나리오를 보여줍니다. 이 시나리오의 투명 방화벽은 NAT 서비스를 수행하므로 업스트림 라우터가 NAT를 수행할 필요가 없습니다.

그림 *48: NAT* 예: 투명 모드



1. 10.1.1.75의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.1.75가 매핑된 주소 209.165.201.15로 변경됩니다.
2. 서버가 응답하며 매핑된 주소 209.165.201.15로 응답을 전송하면, Firepower Threat Defense 디바이스에서 패킷을 수신합니다. 업스트림 라우터는 Firepower Threat Defense 디바이스 관리 IP 주소로 연결되는 고정 경로에 이 매핑된 주소를 포함하기 때문입니다.
3. 그런 다음 Firepower Threat Defense 디바이스에서는 매핑된 주소 209.165.201.15에서 다시 실제 주소 10.1.1.1.75로의 변환을 취소합니다. 실제 주소는 직접 연결되어 있으므로 Firepower Threat Defense 디바이스는 호스트로 주소를 직접 전송합니다.
4. 호스트 192.168.1.2에서도 반환 트래픽을 제외하고는 동일한 프로세스가 발생합니다. Firepower Threat Defense 디바이스는 라우팅 테이블에서 경로를 조회하고, 192.168.1.0/24에 대한 Firepower Threat Defense 디바이스 고정 경로를 기반으로 10.1.1.3의 다운스트림 라우터로 패킷을 전송합니다.

자동 NAT 및 수동 NAT

자동 *NAT* 및 수동 *NAT* 두 가지 방법으로 주소 변환을 구현할 수 있습니다.

수동 NAT에서 제공하는 추가 기능이 필요한 경우가 아니면 자동 NAT를 사용하는 것이 좋습니다. 자동 NAT가 컨피그레이션이 더 쉽고, VoIP(Voice over IP) 등의 애플리케이션에서 좀 더 안정적일 수 있습니다. VoIP의 경우 규칙에서 사용되는 개체 중 하나에 속하지 않는 간접 주소를 변환할 때 오류가 발생할 수 있습니다.

자동 NAT

네트워크 개체의 파라미터로 컨피그레이션되는 모든 NAT 규칙은 자동 *NAT* 규칙으로 간주됩니다. NAT 규칙을 사용하면 네트워크 개체에 대해 NAT를 빠르고 쉽게 구성할 수 있습니다. 그러나 그룹 개체에 대해서는 이러한 규칙을 생성할 수 없습니다.

이러한 규칙은 개체 자체의 일부분으로 구성되지만, 개체 관리자를 통해 개체 정의에서 NAT 컨피그레이션을 확인할 수는 없습니다.

패킷이 인터페이스로 들어가면 소스 및 대상 IP 주소 둘 다에서 자동 NAT 규칙을 확인합니다. 별도의 일치를 만든 경우 별도의 규칙을 통해 패킷의 소스 및 대상 주소를 변환할 수 있습니다. 이러한 규칙은 서로 연결되어 있지 않습니다. 트래픽에 따라 규칙의 서로 다른 조합을 사용할 수 있습니다.

규칙은 쌍을 이루지 않으므로 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 없습니다. 이러한 종류의 기능이 필요한 경우 수동 NAT를 사용하십시오. 그러면 한 가지 규칙에서 소스 및 대상 주소를 식별할 수 있습니다.

수동 NAT

수동 NAT 한 가지 규칙에서 소스 및 대상 주소를 모두 식별할 수 있습니다. 소스 주소와 대상 주소를 모두 지정하면 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 있습니다.

참고 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "source(소스)"와 "destination(대상)"이 사용됩니다. 특정 연결이 "destination(대상)" 주소에서 시작되는 경우에도 마찬가지입니다. 예를 들어 포트 주소 변환 고정 NAT를 구성하고, 소스 주소를 텔넷 서버로 지정하며, 텔넷 서버로 이동하는 모든 트래픽에 대해 포트를 2323에서 23으로 변환하려면 소스 포트가 변환되도록 지정해야 합니다(실제 포트: 23, 매핑된 포트: 2323). 텔넷 서버 주소를 소스 주소로 지정했기 때문에 소스 포트를 지정하는 것입니다.

대상 주소는 선택 사항입니다. 대상 주소를 지정하는 경우 이를 대상 주소 자신에게 매핑할 수도 있고(ID NAT) 다른 주소에 매핑할 수도 있습니다. 대상 주소 매핑은 항상 고정 매핑입니다.

자동 NAT와 수동 NAT 비교

이 두 NAT 유형의 주요 차이점은 다음과 같습니다.

- 실제 주소를 정의하는 방법
  - 자동 NAT - NAT 규칙은 네트워크 개체의 파라미터가 됩니다. 네트워크 개체 IP 주소는 원래(실제) 주소 역할을 합니다.
  - 수동 NAT- 실제 주소와 매핑된 주소 모두에서 네트워크 개체 또는 네트워크 개체 그룹을 식별합니다. 이 경우 NAT는 네트워크 개체의 매개변수가 아닙니다. 네트워크 개체 또는 그룹은 NAT 컨피그레이션의 매개변수입니다. 실제 주소에 네트워크 개체 그룹을 사용할 수 있으므로 수동 NAT의 확장성이 더 뛰어납니다.
- 소스 및 대상 NAT의 구현 방법

- 자동 NAT- 각 규칙을 패킷의 소스 또는 대상에 적용할 수 있습니다. 따라서 소스 IP 주소와 대상 IP 주소에 각각 하나씩 두 개의 규칙이 사용될 수 있습니다. 소스/대상조합에 특정 변환을 적용하기 위해 이러한 두 규칙을 결합할 수 없습니다.
- 수동 NAT단일 규칙에서 소스와 대상을 모두 변환합니다. 패킷은 하나의 규칙에서만 일치하며, 더 이상 규칙이 점검되지 않습니다. 선택적 대상 주소를 컨피그레이션하지 않더라도 일치하는 패킷은 여전히 하나의 수동 NAT 규칙과만 일치합니다. 소스와 대상이 결합되어 있으므로, 소스/대상조합에 따라 서로 다른 변환을 적용할 수 있습니다. 예를 들어 소스A/대상A의 변환은 소스A/대상B의 변환과 다를 수 있습니다.

- NAT 규칙의 순서
  - 자동 NAT- NAT 테이블에서 자동으로 순서가 지정됩니다.
  - 수동 NAT - NAT 테이블에서 수동으로 순서가 지정됩니다(자동 NAT 규칙 앞이나 뒤).

NAT 규칙 순서

자동 NAT 및 수동 NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예를 들어 섹션 1에서 일치가 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

표 ***98: NAT*** 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	수동 NAT	첫 번째 일치부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 수동 NAT 규칙은 섹션 1에 추가됩니다. "특정 규칙 우선"이라는 의미는 다음과 같습니다. • 정적 규칙이 동적 규칙 앞에 와야 합니다. • 대상 변환을 포함한 규칙은 소스 변환만을 포함한 규칙보다 앞에 와야 합니다. 소스 또는 대상 주소를 기반으로 둘 이상의 규칙이 적용될 수 있는 중복 규칙을 제거할 수 없는 경우에는 특히 주의하여 이러한 권장 사항을 따르십시오.

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 2	자동 NAT	섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다. **1.** 고정 규칙 **2.** 동적 규칙 각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다. **1.** 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다. **2.** 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다. **3.** IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들면 abracadabra가 catwoman보다 먼저 평가됩니다.
섹션 3	수동 NAT	아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다.

예를 들어 섹션 2 규칙의 경우 네트워크 개체 내에서 다음 IP 주소를 정의합니다.

- 192.168.1.0/24(고정)
- 192.168.1.0/24(동적)
- 10.1.1.0/24(고정)
- 192.168.1.1/32(고정)
- 172.16.1.0/24(동적)(개체 def)
- 172.16.1.0/24(동적)(개체 abc)

결과 순서는 다음과 같습니다.

- 192.168.1.1/32(고정)
- 10.1.1.0/24(고정)
- 192.168.1.0/24(고정)
- 172.16.1.0/24(동적)(개체 abc)
- 172.16.1.0/24(동적)(개체 def)

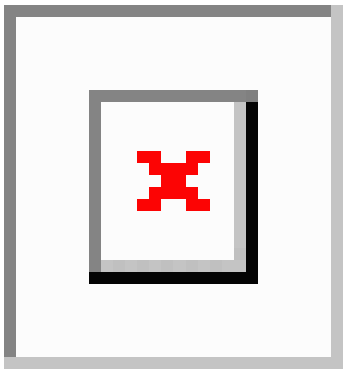
- 192.168.1.0/24(동적)

NAT 인터페이스

브리지 그룹 멤버 인터페이스를 제외한 임의의 인터페이스(즉, 모든 인터페이스)에 적용할 NAT 규칙을 구성할 수도 있고, 특정 실제 및 매핑된 인터페이스를 지정할 수도 있습니다. 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 특정 인터페이스를 지정하거나, 그 반대로 지정할 수도 있습니다.

예를 들어, 여러 인터페이스에서 동일한 사설 주소를 사용하며, 외부에 액세스할 때 이들을 모두 동일한 전역 풀로 변환하려는 경우 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 외부 인터페이스를 지정할 수 있습니다.

그림 ***49:*** 임의의 인터페이스 지정



그러나 브리지 그룹 멤버 인터페이스에는 "any" 인터페이스라는 개념이 적용되지 않습니다. "any" 인터페이스를 지정하면 모든 브리지 그룹 멤버 인터페이스는 제외됩니다. 따라서 브리지 그룹 멤버에 NAT를 적용하려면 멤버 인터페이스를 지정해야 합니다. 이렇게 하면 유사한 여러 규칙에서 인터페이스 하나만 다른 현상이 발생할 수 있습니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT를 구성할 수 없으며 멤버 인터페이스에 대해서만 NAT를 구성할 수 있습니다.

참고 인라인, 인라인 탭 또는 수동 모드로 작동하는 인터페이스에 대해서는 NAT를 구성할 수 없습니다. 인터페이스를 지정할 때는 인터페이스가 포함된 인터페이스 개체를 선택하여 간접적으로 지정합니다.

NAT 라우팅 구성

FTD 디바이스는 변환(매핑)된 주소로 전송되는 모든 패킷의 대상이어야 합니다.

패킷을 전송할 때 디바이스는 대상 인터페이스를 지정한 경우 해당 인터페이스를 사용하고, 그렇지 않으면 라우팅 테이블 조회를 사용하여 이그레스 인터페이스를 결정합니다. ID NAT의 경우에는 대상 인터페이스를 지정하더라도 경로 조회를 사용하는 옵션이 있습니다.

필요한 라우팅 컨피그레이션의 유형은 다음 항목에서 설명하는 것처럼 매핑된 주소의 유형에 따라 다릅니다.

매핑된 인터페이스와 동일한 네트워크의 주소

대상(매핑된) 인터페이스와 동일한 네트워크의 주소를 사용하는 경우, Firepower Threat Defense 디바이스에서는 매핑된 주소에 대한 ARP 요청에 응답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. Firepower Threat Defense 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 이 솔루션은 외부 네트워크에 적절한 수의 여유 주소가 있는 경우 이상적이며, 동적 NAT 또는 고정 NAT 등 1:1 변환을 사용하는 경우 고려해볼 수 있습니다. 동적 PAT는 소수의 주소로 사용 가능한 변환의 수를 크게 확장합니다. 따라서 외부 네트워크에 사용 가능한 주소가 적어도 이 방법을 사용할 수 있습니다. PAT의 경우 매핑된 인터페이스의 IP 주소를 사용할 수도 있습니다.

참고 매핑된 인터페이스를 임의의(any) 인터페이스로 구성하고 동일한 네트워크의 매핑된 주소를 매핑된 인터페이스 중 하나로 지정하면, 해당 매핑된 주소에 대한 ARP 요청이 다른 인터페이스에서 오는 경우 인그레스 인터페이스에서 해당 네트워크에 대한 ARP 항목을 수동으로 구성하여 해당 MAC 주소를 지정해야 합니다. 일반적으로 매핑된 인터페이스에 대해 임의의 인터페이스를 지정하면 매핑된 주소에 대해 고유한 네트워크를 사용하게 되므로 이러한 상황이 발생하지 않습니다. 인그레스 인터페이스의 **Advanced(**고급**)** 설정에서 ARP 테이블을 컨피그레이션합니다.

고유한 네트워크의 주소

대상(매핑된) 인터페이스 네트워크에서 사용할 수 있는 것보다 더 많은 주소가 필요한 경우 별도의 서브넷에서 주소를 지정할 수 있습니다. 업스트림 라우터에는 Firepower Threat Defense 디바이스를 가리키는, 매핑된 주소에 대한 고정 경로가 필요합니다.

라우팅된 모드에 대한 대안으로, 대상 네트워크의 IP 주소를 게이트웨이로 사용하여 Firepower Threat Defense 디바이스에서 매핑된 주소에 대해 고정 경로를 구성한 다음 라우팅 프로토콜을 사용하여 경로를 재배포할 수 있습니다. 예를 들어 내부 네트워크(10.1.1.0/24)에 대해 NAT를 사용하고 매핑된 IP 주소 209.165.201.5를 사용하는 경우 209.165.201.5 255.255.255.255(호스트 주소)에 대한 고정 경로를 재배포 가능한 10.1.1.99 게이트웨이로 구성할 수 있습니다.

투명 모드에서 실제 호스트가 직접 연결된 경우 8.3에서는 업스트림 라우터의 고정 경로가 Firepower Threat Defense 디바이스를 가리키도록 구성하고 합니다. 투명 모드의 원격 호스트에 대해서는 업스트림 라우터의 고정 경로에서 다운스트림 라우터 IP 주소를 대신 지정할 수 있습니다.

실제 주소와 동일한 주소**(ID NAT)**

ID NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 사용 해제할 수 있습니다. 원하는 경우 정기적인 고정 NAT에 대해 프록시 ARP를 사용 해제할 수도 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다.

일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다. 예를 들어 "any" IP 주소에 대해 광범위한 ID NAT 규칙을 구성하고 프록시 ARP를 사용하는 상태로 두면 매핑된 인터페이스에 직접 연결된 네트워크에서 호스트 문제가 발생할 수

있습니다. 이 경우 매핑된 네트워크의 호스트가 동일한 네트워크의 다른 호스트와 통신하려면 ARP 요청의 주소가 NAT 규칙과 일치해야 합니다("any" 주소와 일치). 패킷이 실제로 Firepower Threat Defense 디바이스로 이동하도록 지정되지 않아도 Firepower Threat Defense 디바이스에서는 주소에 대해 프록시 ARP를 수행합니다. (이 문제는 수동 NAT 규칙이 있는 경우에도 발생합니다. NAT 규칙은 소스 주소 및 대상 주소와 모두 일치해야 하지만 프록시 ARP 결정은 "소스" 주소에 대해서만 내려집니다.) 실제 호스트 ARP 응답 전에 Firepower Threat Defense 디바이스 ARP 응답을 수신하는 경우, 트래픽이 Firepower Threat Defense 디바이스로 잘못 전송됩니다.

NAT용 지침

다음 주제에서는 NAT 구현에 대한 자세한 지침을 제공합니다.

NAT용 방화벽 모드 지침

NAT는 라우팅된 모드 및 투명 방화벽 모드에서 지원됩니다.

그러나 브리지 그룹 멤버 인터페이스, 즉 BVI(브리지 그룹 가상 인터페이스)에 속하는 인터페이스에 대해 NAT를 구성할 때는 다음과 같은 제한이 있습니다.

- 브리지 그룹 멤버에 대해 NAT를 구성할 때는 멤버 인터페이스를 지정합니다. BVI(브리지 그룹 인터페이스) 자체에 대해서는 NAT를 구성할 수 없습니다.
- 브리지 그룹 멤버 인터페이스 간에 NAT를 수행할 때는 실제 및 매핑된 주소를 지정해야 합니다. 인터페이스로 "임의"를 지정할 수는 없습니다.
- 매핑된 주소가 브리지 그룹 멤버 인터페이스일 때는 인터페이스 PAT를 구성할 수 없습니다. 인터페이스에 연결된 IP 주소가 없기 때문입니다.
- 소스 및 대상 인터페이스가 동일한 브리지 그룹의 멤버이면 IPv4 및 IPv6 네트워크(NAT64/46) 간을 변환할 수 없습니다. 지원되는 방법은 고정 NAT/PAT 44/66, 동적 NAT44/66 및 동적 PAT44뿐이며 동적 PAT66은 지원되지 않습니다. 그러나 다른 브리지 그룹의 멤버나 브리지 그룹 멤버(소스)와 표준 라우팅 인터페이스(대상) 간에는 NAT64/46을 수행할 수 있습니다.

참고 인라인, 인라인 탭 또는 수동 모드로 작동하는 인터페이스에 대해서는 NAT를 구성할 수 없습니다.

IPv6 NAT 지침

NAT는 다음 지침 및 제약 사항과 함께 IPv6를 지원합니다.

- 표준 라우팅 모드 인터페이스에서는 IPv4와 IPv6 간을 변환할 수도 있습니다.
- 고정 NAT에서는 IPv6 서브넷을 최대 /64까지 지정할 수 있습니다. 더 큰 서브넷은 지원되지 않습니다.

- FTP with NAT46을 사용할 때, IPv4 FTP 클라이언트가 IPv6 FTP 서버에 연결될 때 클라이언트는 확장 패시브 모드(EPSV) 또는 확장 포트 모드(EPRT)를 사용해야 하며, PASV 및 PORT 명령은 IPv6에서 지원되지 않습니다.

IPv6 NAT 모범 사례

IPv6 네트워크 간 변환 및 IPv4와 IPv6 네트워크 간 변환(라우팅된 모드 전용)을 위해 NAT를 사용할 수 있습니다. 다음의 모범 사례를 권장합니다.

- NAT66(IPv6-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다. 반환 트래픽을 허용하지 않으려면 정적 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함).
- NAT46(IPv4-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. IPv6 주소 공간이 IPv4 주소 공간보다 훨씬 크기 때문에 고정 변환을 손쉽게 수용할 수 있습니다. 반환 트래픽을 허용하지 않으려면 정적 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함). IPv6 서브넷(/96 이하)으로 변환하면 결과로 나타나는 매핑된 주소는 기본적으로 IPv4가 포함된 IPv6 주소입니다. 이 경우 IPv6 접두사 뒤에 IPv4 주소의 32비트가 포함됩니다. 예를 들어 IPv6 접두사가 /96 접두사이면, 주소의 마지막 32비트에 IPv4 주소가 첨부됩니다. 예를 들어 192.168.1.0/24를 201b::0/96에 매핑하면 192.168.1.4는 201b::0.192.168.1.4(혼합된 표기로 표시됨)에 매핑됩니다. 접두사가 더 작으면(예: /64) IPv4 주소가 접두사 뒤에 첨부되고, 접미사 0이 IPv4 주소 뒤에 첨부됩니다. 선택적으로 주소를 net-to-net으로 변환할 수도 있습니다. 이 경우 첫 번째 IPv4 주소가 첫 번째 IPv6 주소로, 두 번째가 두 번째로 등과 같이 매핑됩니다.
- NAT64(IPv6-to-IPv4) - IPv6 주소의 수를 수용할 만큼 IPv4 주소가 충분하지 않을 수 있습니다. 대량의 IPv4 변환을 제공하려면 동적 PAT 풀을 사용하는 것이 좋습니다.

검사된 프로토콜에 대한 NAT 지원

보조 연결을 열거나 패킷에 IP 주소를 포함한 일부 애플리케이션 레이어 프로토콜을 검사하여 다음 서비스를 제공합니다.

- 핀홀 생성 - 일부 애플리케이션 프로토콜은 표준 포트 또는 협상된 포트에서 보조 TCP 또는 UDP 연결을 엽니다. 검사에서는 이러한 보조 포트를 허용하기 위한 액세스 제어 규칙을 생성할 필요가 없도록 해당 포트에 대해 핀홀을 엽니다.
- NAT 재작성 - FTP 등의 프로토콜은 프로토콜의 일부분으로 패킷 데이터에 보조 연결용 IP 주소 및 포트를 포함합니다. 엔드포인트 중 하나에서 NAT 변환이 수행되는 경우 검사 엔진은 포함된 주소와 포트의 NAT 변환을 반영하기 위해 패킷 데이터를 재작성합니다. NAT 재작성이 수행되지 않으면 보조 연결은 작동하지 않습니다.
- 프로토콜 적용 - 일부 검사에서는 검사된 프로토콜에 대해 특정 수준의 RFC 적합성을 적용합니다.

다음 표에는 NAT 재작성을 적용하는 검사된 프로토콜 및 이러한 프로토콜의 NAT 제한이 나와 있습니다. 이러한 프로토콜을 포함하는 NAT 규칙을 작성할 때는 이와 같은 제한에 주의해야 합니다. 여

기에 나와 있지 않은 검사된 프로토콜은 NAT 재작성을 적용하지 않습니다. 이러한 검사에는 GTP, HTTP, IMAP, POP, SMTP, SSH 및 SSL이 포함됩니다.

참고 NAT 재작성은 여기에 나와 있는 포트에서만 지원됩니다. 이러한 프로토콜 중 일부의 경우에는 네트워크 분석 정책을 사용하여 다른 포트로 검사를 확장할 수 있지만, NAT 재작성은 해당 포트로 확장되지 않습니다. 여기에는 DCERPC, DNS, FTP 및 Sun RPC 검사가 포함됩니다. 비표준 포트에서 이러한 프로토콜을 사용하는 경우에는 연결에 NAT를 사용하지 마십시오.

표 ***99: NAT***가 지원되는 애플리케이션 검사

애플리케이션	검사된 프로토콜, 포트	**NAT** 제한	핀홀 생성 여부
DCERPC	TCP/135	NAT64 없음	예
DNS over UDP	UDP/53	WINS를 통한 이름 확인에 NAT 지원을 이용할 수 없음	아니요
ESMTP	TCP/25	NAT64 없음	아니요
FTP	TCP/21	제한 없음 (클러스터링) 고정 PAT 없음.	예
H.323 H.225(호출 신호) H.323 RAS	TCP/1720 UDP/1718 RAS의 경우 UDP/1718-1719	(클러스터링) 고정 PAT 없음 확장 PAT 없음 NAT64 없음	예
ICMP ICMP Error	ICMP (디바이스 인터페이스로 전달된 ICMP 트래픽은 검사되지 않음)	제한 없음	아니요
IP Options	RSVP	NAT64 없음	아니요
NetBIOS Name Server over IP	UDP/137, 138(소스 포트)	확장 PAT 없음 NAT64 없음	아니요
RSH	TCP/514	PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예

애플리케이션	검사된 프로토콜, 포트	NAT 제한	핀홀 생성 여부
RTSP	TCP/554 (HTTP 클로킹을 처리하지 않음)	확장 PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예
SIP	TCP/5060 UDP/5060	확장 PAT 없음 NAT64 또는 NAT46 없음 (클러스터링) 고정 PAT 없음.	예
Skinny(SCCP)	TCP/2000	확장 PAT 없음 NAT64, NAT46 또는 NAT66 없음 (클러스터링) 고정 PAT 없음.	예
SQL*Net (버전 1, 2)	TCP/1521	확장 PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예
Sun RPC	TCP/111 UDP/111	확장 PAT 없음 NAT64 없음	예
TFTP	UDP/69	NAT64 없음 (클러스터링) 고정 PAT 없음. 페이로드 IP 주소는 변환되지 않습니다.	예
XDMCP	UDP/177	확장 PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예

NAT 추가 지침

- 브리지 그룹 멤버인 인터페이스의 경우 멤버 인터페이스용 NAT 규칙을 작성합니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT 규칙을 작성할 수 없습니다.
- 사이트 대 사이트 VPN에서 사용되는 VTI(Virtual Tunnel Interface)에 대해서는 NAT 규칙을 작성할 수 없습니다. VTI의 소스 인터페이스에 대해 규칙을 작성하면 VPN 터널에 NAT가 적용되지 않습니다. VTI에서 터널링된 VPN 트래픽에 적용할 NAT 규칙을 작성하려면 "any"를 인터페이스로 사용해야 합니다. 인터페이스 이름을 명시적으로 지정할 수 없습니다.

- (자동 NAT에만 해당함.) 한 개체에는 단일 NAT 규칙만 정의할 수 있습니다. 한 개체에 대해 여러 NAT 규칙을 구성하려면 동일한 IP 주소를 지정하는 서로 다른 이름의 여러 개체를 생성해야 합니다.
- 인터페이스에 VPN이 정의되어 있으면 인터페이스의 인바운드 ESP 트래픽에는 NAT 규칙이 적용되지 않습니다. 시스템은 설정된 VPN 터널에 대해서만 ESP 트래픽을 허용하며 기존 터널과 연결되지 않은 트래픽은 삭제합니다. 이러한 제한은 ESP 및 UDP 포트 500과 4500에 적용됩니다.
- UDP 포트 500 및 4500이 실제로 사용되지 않도록 동적 PAT를 적용하는 디바이스 뒤에 있는 디바이스에서 사이트 대 사이트 VPN을 정의하는 경우에는 PAT 디바이스 뒤의 디바이스에서 연결을 시작해야 합니다. 응답자는 정확한 포트 번호를 모르므로 SA(보안 연결)를 시작할 수 없습니다.
- NAT 컨피그레이션을 변경할 때 새 NAT 컨피그레이션이 사용되기 전에 기존 변환이 시간 초과되기까지 기다리지 않으려면 디바이스 CLI에서 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 변환을 사용하는 현재의 모든 연결이 해제됩니다.

참고 동적 NAT 또는 PAT 규칙을 제거한 후 제거된 규칙의 주소와 중복되는 매핑된 주소가 포함된 새 규칙을 추가하는 경우, 새 규칙을 사용하려면 제거된 규칙과 관련된 모든 연결이 시간 초과되기까지 기다리거나 **clear xlate** 명령으로 해당 연결을 지워야 합니다. 이러한 안전 조치는 동일한 주소가 여러 호스트에 할당되는 것을 방지합니다.

- IPv4 및 IPv6 주소를 모두 포함하는 개체 그룹은 사용할 수 없습니다. 개체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
- NAT에서 사용되는 네트워크 개체는 주소 범위 또는 서브넷에서 명시적으로 또는 묵시적으로 131,838개 이상의 IP 주소를 포함할 수 없습니다. 주소 공간을 더 작은 범위로 분할하고 더 작은 개체에 대해 별도의 규칙을 작성합니다.
- (수동 NAT에만 해당함.) NAT 규칙에서 **any**를 소스 주소로 사용하는 경우 "any" 트래픽의 정의(IPv4 대 IPv6)는 규칙에 따라 다릅니다. Firepower Threat Defense 디바이스가 패킷에 대해 NAT를 수행하기 전에 패킷은 IPv6-IPv6 또는 IPv4-IPv4여야 합니다. 이 전제 조건하에 Firepower Threat Defense 디바이스는 NAT 규칙에서 **any**의 값을 결정할 수 있습니다. 예를 들어 **any**에서 IPv6 서버로 규칙을 구성하며 해당 서버가 IPv4 주소에서 매핑된 것이면 any는 "모든 IPv6 트래픽"을 의미합니다. “any” 에서 “any”로 규칙을 구성하며 소스를 인터페이스 IPv4 주소로 매핑하면 **any**는 “모든 IPv4 트래픽”을 의미합니다. 매핑된 인터페이스 주소는 대상 주소도 IPv4임을 암시하기 때문입니다.
- 여러 NAT 규칙에서 동일한 매핑된 개체 또는 그룹을 사용할 수 있습니다.
- 매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.
  - 매핑된 인터페이스 IP 주소. 규칙에 대해 "any" 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅 모드만 해당함)의 경우 인터페이스 주소 대신 인터페이스 이름을 사용합니다.
  - 페일오버 인터페이스 IP 주소

  - (투명 모드) 관리 IP 주소.
  - (동적 NAT) VPN이 활성화된 경우의 스탠바이 인터페이스 IP 주소

- 고정 및 동적 NAT 정책에서는 겹치는 주소 사용을 피해야 합니다. 예를 들어, PPTP의 보조 연결이 동적 xlate 대신 고정 상태인 경우 겹치는 주소를 사용하면 PPTP 연결 설정에 실패할 수 있습니다.
- NAT 규칙의 소스 주소와 원격 액세스 VPN 주소 풀에서는 겹치는 주소를 사용할 수 없습니다.
- 규칙에서 대상 인터페이스를 지정하는 경우에는 라우팅 테이블에서 경로를 조회하지 않고 해당 인터페이스를 이그레스 인터페이스로 사용합니다. 그러나 ID NAT의 경우에는 경로 조회를 대신 사용할 수 있는 옵션이 제공됩니다.
- NFS 서버에 연결하는 데 사용되는 Sun RPC 트래픽에서 PAT를 사용하는 경우, PAT'ed 포트가 1024 이상인 경우 NFS 서버가 연결을 거부할 수 있다는 점에 유의하십시오. NFS 서버의 기본 구성은 1024보다 상위 포트로부터의 연결을 거부하는 것입니다. 오류는 일반적으로 "권한 거부"입니다. PAT 풀의 포트 범위에 예약된 포트(1~1023)를 포함하는 옵션을 선택하지 않으면 1024 이상의 포트 매핑이 발생합니다. 모든 포트 번호를 허용하도록 NFS 서버 구성을 변경하여 이 문제를 방지할 수 있습니다.
- NAT는 통과 트래픽에만 적용됩니다. 시스템에서 생성된 트래픽에는 NAT가 적용되지 않습니다.
- 대문자 또는 소문자 조합을 사용하여 네트워크 개체 또는 그룹 pat-pool의 이름을 지정하지 마십시오.
- 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

Threat Defense NAT 구성

네트워크 주소 변환은 매우 복잡해질 수 있습니다. 따라서 변환 문제와 까다로운 트러블슈팅 상황을 방지하기 위해 규칙을 최대한 단순하게 유지하는 것이 좋습니다. 그리고 NAT를 구현하기 전에 면밀한 계획을 세워야 합니다. 다음 절차에서는 기본적인 구성 방식에 대해 설명합니다.

NAT 정책은 공유 정책입니다. 디바이스에 NAT 규칙과 유사한 정책을 할당합니다.

할당된 디바이스에 정책의 규칙이 적용되는지 여부는 규칙에서 사용되는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)에 의해 결정됩니다. 인터페이스 개체가 디바이스에 하나 이상의 인터페이스를 포함하는 경우 규칙이 디바이스에 구축됩니다. 따라서 인터페이스 개체로 신중하게 구성된 단일 공유 정책 내에서 디바이스의 하위 집합에 적용되는 규칙을 구성할 수 있습니다. "Any" 인터페이스 개체에 적용되는 규칙은 모든 디바이스에 구축됩니다.

디바이스 그룹에 현저히 다른 규칙이 요구되는 경우 복수의 NAT 정책을 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**을 선택합니다.

- 새 정책을 생성하려면 **New Policy(**새 정책**)** > **Threat Defense NAT(**위협 방어 **NAT)**을 클릭합니다. 정책에 이름과 선택적으로 디바이스를 할당하고 **Save(**저장**)**을 클릭합니다.

  정책을 편집하고 정책 할당을 클릭하여 나중에 디바이스 할당을 변경할 수 있습니다.

- 수정( )을 클릭하여 기존 위협 방어 NAT 정책을 편집합니다. 해당 페이지는 FTD 디바이스에서 사용되지 않는 Firepower NAT 정책도 표시합니다.

단계 **2** 필요한 규칙의 종류를 결정합니다.

동적 NAT, 동적 PAT, 고정 NAT 및 ID NAT 규칙을 생성할 수 있습니다. 이와 관련된 개요는 NAT 유형, 1489 페이지를 참조하십시오.

단계 **3** 수동 또는 자동 NAT로 구현할 규칙을 결정합니다.

이 두 가지 구현 옵션을 비교한 내용은 자동 NAT 및 수동 NAT, 1491 페이지를 참조하십시오.

단계 **4** 디바이스에 따라 사용자 정의되어야 하는 규칙을 결정합니다.

여러 디바이스에 NAT 정책을 할당할 수 있으므로 여러 장치에 단일 규칙을 구성할 수 있습니다. 그러나 각 디바이스에 따라 다르게 해석되어야 하는 규칙 또는 디바이스의 하위 집합에만 적용되어야 하는 일부 규칙이 따로 있을 수 있습니다.

규칙이 구성될 디바이스를 제어할 때는 인터페이스 개체를 사용합니다. 디바이스당 주소를 사용자 정의하려면 네트워크 개체의 개체 오버라이드를 사용합니다.

자세한 내용은 여러 디바이스에 대한 NAT 규칙 맞춤 설정, 1504 페이지를 참조하십시오.

단계 **5** 다음 섹션에서 설명하는 대로 규칙을 생성합니다.

- 동적 NAT, 1507 페이지
- 동적 PAT, 1513 페이지
- 고정 NAT, 1524 페이지
- ID NAT, 1533 페이지

단계 **6** NAT 정책 및 규칙을 관리합니다.

다음을 수행하여 정책과 해당 규칙을 관리할 수 있습니다.

- 정책 이름 또는 설명을 편집하려면 해당 필드를 클릭하고 변경 내용을 입력한 다음 필드 바깥쪽을 클릭합니다.
- 특정 디바이스에만 적용되는 규칙을 보려면 **Filter by Device(**디바이스별 필터**)**를 클릭하고 원하는 디바이스를 선택합니다. 디바이스의 인터페이스를 포함하는 인터페이스 개체를 사용하는 경우 규칙이 디바이스에 적용됩니다.

- 정책이 할당될 디바이스를 변경하려면 **Policy Assignment(**정책 할당**)** 링크를 클릭하고 선택한 디바이스 목록을 수정합니다.
- 규칙의 활성화 또는 비활성화 여부를 변경하려면 규칙을 오른쪽 클릭하고 **State(**상태**)** 명령에서 원하는 옵션을 선택합니다. 이런 제어를 사용해 규칙을 삭제하지 않고도 일시적으로 비활성화할 수 있습니다.
- 규칙을 수정하려면 해당 규칙의 수정( )을 클릭합니다.
- 규칙을 삭제하려면 해당 규칙의 삭제( )을 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

여러 디바이스에 대한 NAT 규칙 맞춤 설정

NAT 정책이 공유되기 때문에 두 개 이상의 디바이스에 특정 정책을 할당할 수 있습니다. 지정된 개체에 대해 최대 하나의 자동 NAT 규칙을 구성할 수 있습니다. 따라서 변환을 수행하는 특정 디바이스를 기반으로 개체에 대해 다른 변환을 구성하려는 경우 인터페이스 개체(보안 영역 또는 인터페이스 그룹)를 신중하게 구성하고 변환된 주소에 대한 네트워크 개체를 재정의해야 합니다.

인터페이스 개체는 규칙이 구성되는 디바이스를 결정합니다. 네트워크 개체 재정의는 해당 디바이스에서 해당 개체에 사용되는 IP 주소를 결정합니다.

다음 시나리오를 고려하십시오.

- FTD-A와 FTD-B에는 "inside"라는 인터페이스에 연결된 내부 네트워크 192.168.1.0/24가 있습니다.
- FTD-A에서는 "outside" 인터페이스로 이동할 때 모든 192.168.1.0/24 주소를 10.100.10.10 - 10.100.10.200 범위의 NAT 풀로 변환하려고 합니다.
- FTD-B에서는 "outside" 인터페이스로 이동할 때 모든 192.168.1.0/24 주소를 10.200.10.10 - 10.200.10.200 범위의 NAT 풀로 변환하려고 합니다.

위의 작업을 수행하려면 다음을 수행합니다. 이 예제 규칙은 동적 자동 NAT를 위한 것이지만 모든 유형의 NAT 규칙에 대한 기술을 일반화할 수 있습니다.

프로시저

단계 **1** 내부 및 외부 인터페이스용 보안 영역을 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Interface Objects(**인터페이스 개체**)**를 선택하고 **Add(**추가**)** > **Security Zone(**보안 영역**)**을 선택합니다. (영역 대신 인터페이스 그룹을 사용할 수 있습니다.)

c) 내부 영역 속성을 구성합니다.

- **Name(**이름**)** - 예를 들어 **inside-zone**이라는 이름을 입력합니다.
- **Type(**유형**)** - 라우팅된 모드 디바이스에 대해 **Routed(**라우팅됨**)**을 선택하고, 투명 모드로 전환합니다.
- **Selected Interfaces(**선택한 인터페이스**)** - 선택된 목록에 FTD-A/inside 및 FTD-B/inside 인터페이스를 추가합니다.

d) **Save(**저장**)**를 클릭합니다.

e) **Add(**추가**)** > **Security Zone(**보안 영역**)**을 클릭하고 외부 영역 속성을 정의합니다.

- **Name(**이름**)** - 예를 들어 **outside-zone**이라는 이름을 입력합니다.
- **Interface Type(**인터페이스 유형**)** - 라우팅된 모드 디바이스에 대해 **Routed(**라우팅됨**)**을 선택하고, 투명 모드로 전환합니다.
- **Selected Interfaces(**선택한 인터페이스**)** - 선택된 목록에 FTD-A/outside 및 FTD-B/outside 인터페이스를 추가합니다.

f) **Save(**저장**)**를 클릭합니다.

단계 **2** 개체 관리 페이지에서 원래의 내부 네트워크에 대한 네트워크 개체를 만듭니다.

a) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 내부 네트워크 속성을 구성합니다.

- **Name(**이름**)** - 예를 들어 **inside-network**라는 이름을 입력합니다.
- **Network(**네트워크**)** - 네트워크 주소를 입력합니다(예: **192.168.1.0/24**).

c) **Save(**저장**)**를 클릭합니다.

단계 **3** 변환된 NAT 풀에 대한 네트워크 개체를 만들고 재정의를 정의합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) FTD-A에 대한 NAT 풀 등록 정보를 구성합니다.

- **Name(**이름**)** - 예를 들어 **NAT-pool**이라는 이름을 입력합니다.
- **Network(**네트워크**)** - FTD-A용 풀에 포함할 주소 범위를 입력합니다(예: **10.100.10.10-10.100.10.200**).

c) **Allow Overrides(**재정의 허용**)**를 선택합니다.

d) **Overrides** 제목을 클릭하여 개체 재정의 목록을 엽니다.

e) **Add(**추가**)**를 클릭하여 Add Object Override(개체 재정의 추가) 대화 상자를 엽니다.

f) FTD-B를 선택하고 Selected Devices(선택한 디바이스) 목록에 추가합니다.

g) **Override(**재정의**)**를 클릭하고 **Network(**네트워크**)**를 **10.200.10.10-10.200.10.200**으로 변경합니다.

h) **Add(**추가**)**를 클릭하여 디바이스에 재정의를 추가합니다.

FTD-B에 대한 재정의를 정의하면 시스템이 FTD-B에서 이 개체를 구성할 때마다 원래 개체에 정의된 값 대신 대체 값을 사용합니다.

i) **Save(**저장**)**를 클릭합니다.

단계 **4** NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside-zone.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside-zone.

참고 인터페이스 개체는 규칙이 구성되는 디바이스를 제어합니다. 이 예제에서는 영역에 FTD-A 및 FTD-B에 대한 인터페이스만 포함되어 있기 때문에 NAT 정책이 추가 디바이스에 할당된 경우에도 해당 규칙은 이 두 디바이스에만 배포됩니다.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside-network 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = NAT-pool 개체.

f) **Save(**저장**)**를 클릭합니다.

이제 FTD-A 및 FTD-B에 대해 다르게 해석될 단일 규칙이 있으며 각 방화벽으로 보호되는 내부 네트워크에 대한 고유한 변환을 제공합니다.

NAT 규칙 테이블 검색 및 필터링

NAT 규칙 테이블을 검색하고 필터링하여 수정하거나 확인해야 하는 규칙을 찾을 수 있습니다. 테이블을 필터링하면 일치하는 규칙만 표시됩니다. 규칙 번호는 1, 2 등으로 순차적으로 변경되지만 필터링에서는 숨겨진 규칙을 기준으로 실제 규칙 번호 또는 테이블의 규칙 위치가 변경되지 않습니다. 필터링은 사용자가 관심 있는 규칙을 찾는 데 도움이 될 수 있는 항목만 변경합니다.

NAT 정책을 수정할 때 테이블 위의 필드를 사용하여 다음 유형의 검색/필터를 수행할 수 있습니다.

- **Filter by Device(**디바이스로 필터링**)**-**Filter by Device(**디바이스로 필터링**)**를 클릭한 다음 규칙을 보려는 디바이스를 선택하고 **OK(**확인**)**를 클릭합니다. 규칙이 디바이스에 적용되는지 여부는 규칙의 인터페이스 제약 조건에 따라 결정됩니다. 소스 또는 대상 인터페이스에 대해 보안 영역 또는 인터페이스 그룹을 지정하는 경우 최소 하나의 디바이스 인터페이스가 해당 영역 또는 그

룹에 있어도 규칙이 디바이스에 적용됩니다. NAT 규칙이 모든 소스 및 대상 인터페이스에 적용되는 경우 모든 디바이스에 적용됩니다.

텍스트 또는 다중 속성 검색도 수행하는 경우 결과는 선택한 디바이스로 제한됩니다.

이 필터를 제거하려면 **Filter by Device(**디바이스 기준 필터링**)**를 클릭하고 디바이스를 선택 취소하거나 **All(**모두**)**을 선택하고 **OK(**확인**)**를 클릭합니다.

- **Simple Text Search(**단순 텍스트 검색**)-Filter(**필터**)** 상자에 문자열을 입력하고 Enter를 누릅니다. 문자열은 규칙의 모든 값과 비교됩니다. 예를 들어 네트워크 개체의 이름 인 "network-object-1"을 입력하면 소스, 대상 및 PAT 풀 속성에서 개체를 사용하는 규칙을 가져옵니다.

  네트워크 및 포트 개체의 경우 문자열은 규칙에 사용된 개체의 내용과도 비교됩니다. 예를 들어 PAT 풀 개체에 10.100.10.3-10.100.10.100 범위가 포함된 경우 10.100.10.3 또는 10.100.10.100(또는 부분 10.100.10)을 검색하면 해당 PAT 풀 개체를 사용하는 규칙이 포함됩니다. 그러나 정확히 일치해야 합니다. IP 주소가 개체의 IP 주소 범위 내에 있더라도 10.100.10.5를 검색하면 이 PAT 풀 개체와 일치하지 않습니다.

  필터를 제거하려면 Filter(필터) 상자의 오른쪽에 있는 **x**를 클릭합니다.

- **Multiple-Attribute Search(**다중 속성 검색**)**-단순 텍스트 검색에서 너무 많은 적중 횟수를 제공하는 경우 검색에 대해 여러 값을 구성할 수 있습니다. **Filter(**필터**)** 상자를 클릭하여 속성 목록을 연 다음 검색하려는 속성의 문자열을 선택하거나 입력하고 **Filter(**필터**)** 버튼을 클릭합니다. 이러한 속성은 NAT 규칙 내에서 구성하는 속성과 동일합니다. 속성에는 AND가 적용되므로 필터링된 결과에는 사용자가 구성한 모든 속성과 일치하는 규칙만 포함됩니다.

  - 규칙 상태(활성화됨/비활성화됨), 즉 PAT 풀의 구성 여부(활성화/비활성화), 규칙 방향(일방/쌍방) 또는 규칙 유형(고정/동적)과 같은 이진 속성의 경우 간단히 적절한 확인란을 선택 또는 선택 취소합니다. 속성 값이 중요하지 않은 경우 두 확인란을 모두 선택합니다. 두 확인란을 모두 선택 취소하면 필터와 일치하는 규칙이 없게 됩니다.
  - 문자열 속성의 경우 해당 속성과 관련된 전체 또는 부분 문자열을 입력합니다. 이는 보안 영역/인터페이스 그룹, 네트워크 개체 또는 포트 개체의 개체 이름입니다. 또한 간단한 텍스트 검색과 동일한 방식으로 일치하는 네트워크 또는 포트 개체 콘텐츠 일 수도 있습니다.

  필터를 제거하려면 Filter(필터) 상자 오른쪽의 **x**를 클릭하거나 Filter(필터) 상자를 클릭하여 드롭다운 목록을 열고 Clear(지우기) 버튼을 클릭합니다.

동적 NAT

다음 주제에서는 동적 NAT 및 동적 NAT를 구성하는 방법에 대해 설명합니다.

동적 NAT 정보

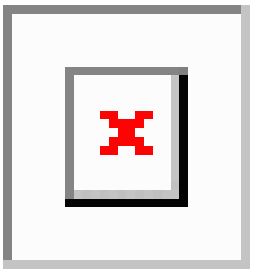
동적 NAT는 실제 주소의 그룹을 대상 네트워크에서 라우팅 가능한 매핑된 주소의 풀로 변환합니다. 매핑된 풀에는 일반적으로 실제 그룹보다 더 적은 수의 주소가 포함되어 있습니다. 변환하려는 호스트가 대상 네트워크에 액세스하면 NAT에서는 매핑된 풀의 IP 주소를 호스트에 할당합니다. 실제 호스트가 연결을 시작하는 경우에만 변환이 생성됩니다. 변환은 연결되어 있는 동안에만 이루어지며, 변환 시간이 초과된 후에는 사용자의 IP 주소가 동일하게 유지되지 않습니다. 따라서 액세스 규칙에

서 연결을 허용하더라도, 대상 네트워크의 사용자는 동적 NAT를 사용하는 호스트에 대해 안정적인 연결을 시작할 수 없습니다.

참고 액세스 규칙에서 허용하는 경우, 변환 기간 동안 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 주소는 예측할 수 없으므로 호스트로의 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

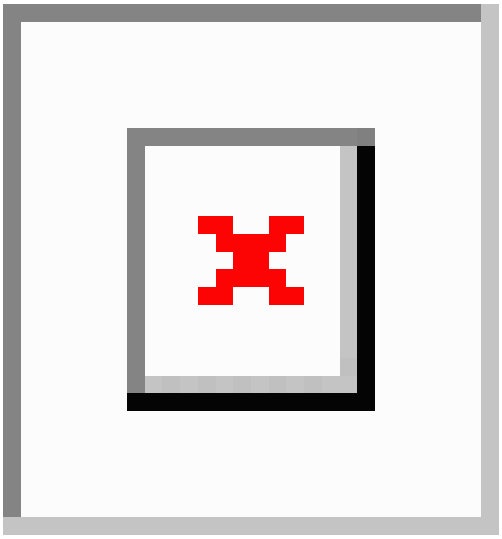
다음 그림은 일반적인 동적 NAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다.

그림 ***50:*** 동적 ***NAT***



다음 그림은 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트를 보여줍니다. 이 주소는 현재 변환 테이블에 있지 않으므로 패킷이 삭제됩니다.

그림 ***51:*** 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트



동적 NAT의 단점 및 장점

동적 NAT의 단점은 다음과 같습니다.

- 매핑된 풀의 주소 수가 실제 그룹의 주소 수보다 적은 경우, 트래픽의 양이 예상보다 많아지면 주소가 부족해질 수 있습니다.

PAT는 단일 주소의 포트를 사용하여 64,000이 넘는 변환을 제공하므로, 이러한 상황이 발생하면 PAT 또는 PAT 대안을 사용하십시오.

- 매핑된 풀에서 대량의 라우팅 가능한 주소를 사용해야 하는데, 라우팅 가능한 주소는 대량으로 사용 가능하지 않을 수 있습니다.

동적 NAT의 장점은 일부 프로토콜이 PAT를 사용할 수 없다는 것입니다. PAT는 다음과 작동하지 않습니다.

- GRE 버전 0과 같이 오버로드할 포트가 없는 IP 프로토콜
- 한 포트에 데이터 스트림이 있고 다른 포트에 제어 경로가 있으며 개방형 표준이 아닌 일부 멀티미디어 애플리케이션

동적 자동 NAT 구성

동적 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- **Translated Source(**변환된 소스**)** - 이는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 동적을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- **Translated Source(**변환된 소스**)** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.

단계 **6** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 - DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 1590 페이지을 참조하십시오.
- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **8** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

동적 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 동적 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.

- **Translated Source(**변환된 소스**)** - 이는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 NAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

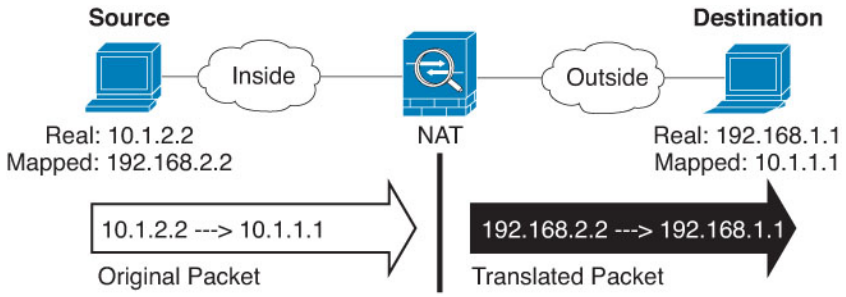
- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 동적을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.
- **Enable(**활성화**)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(**삽입**)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.
- 소스 인터페이스, 대상 인터페이스 - 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**).

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** (변환 페이지에서) 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Source Interface IP(소스 인터페이스 **IP)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- **Translated Source(**변환된 소스**)** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.
- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트(**Original Destination Port(**원본 대상 포트**)**, **Translated Destination Port(**변환된 대상 포트**)**)를 식별합니다.

동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port(**원본 대상 포트**)** 및 **Translated Destination Port(**변환된 대상 포트**)** 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- (소스 변환만 해당) 이 규칙과 일치하는 **DNS** 회신 변환 - DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 1590 페이지을 참조하십시오.

- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **9** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **10** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

동적 **PAT**

다음 주제에서는 동적 PAT에 대해 설명합니다.

동적 **PAT** 정보

동적 PAT는 실제 주소 및 소스 포트를 매핑된 주소 및 고유한 포트로 변환함으로써 여러 실제 주소를 단일 매핑된 IP 주소로 변환합니다.

소스 포트는 각 연결에 대해 다르므로 연결마다 별도의 변환 세션이 필요합니다. 예를 들어 10.1.1.1:1025를 사용하려면 10.1.1.1:1026에서 별도로 변환해야 합니다.

다음 그림은 일반적인 동적 PAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다. 매핑된 주소는 각 변환에 대해 동일하지만 포트는 동적으로 할당됩니다.

그림 ***52:*** 동적 ***PAT***

액세스 규칙에서 허용하는 경우, 변환 기간 동안 대상 네트워크의 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 포트 주소(실제 및 매핑된 주소 모두)는 예측할 수 없으므로 호스트에 대한 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

연결이 만료되면 포트 변환도 만료됩니다.

참고 각 인터페이스에 각기 다른 PAT 풀을 사용하는 것이 좋습니다. 여러 인터페이스에 동일한 풀을 사용하는 경우, 특히 "any" 인터페이스에 동일한 풀을 사용하는 경우에 풀이 빠르게 소진될 수 있어 새 변환에 포트를 사용할 수 없게 됩니다.

동적 PAT의 단점 및 장점

동적 PAT에서는 단일 매핑된 주소를 사용하여 라우팅 가능한 주소를 아낄 수 있습니다. Firepower Threat Defense 디바이스 인터페이스 IP 주소를 PAT 주소로서 사용할 수도 있습니다.

데이터 스트림이 제어 경로와 다른 일부 멀티미디어 애플리케이션에서는 동적 PAT가 작동하지 않습니다. 자세한 내용은 검사된 프로토콜에 대한 NAT 지원, 1498 페이지를 참조하십시오.

동적 PAT는 단일 IP 주소에서 오는 것처럼 보이는 대량의 연결을 생성할 수 있으며, 서버는 이 트래픽을 DoS 공격으로 해석할 수 있습니다. 주소의 PAT 풀을 구성하고 PAT 주소를 라운드 로빈 방식으로 할당하여 이 상황을 완화할 수 있습니다.

PAT 풀 개체 지침

PAT의 네트워크 개체를 만드는 경우 다음 지침을 따르십시오.

PAT 풀의 경우

- 포트는 1024~65535 범위의 사용 가능한 포트에 매핑됩니다. 경우에 따라 예약된 포트(1024 미만)를 포함하여 전체 포트 범위를 변환에 사용할 수 있습니다.

  클러스터에서 작동하는 경우, 주소당 512개 포트의 블록이 클러스터의 멤버에 할당되며 이러한 포트 블록 내에서 매핑이 이루어집니다. 블록 할당도 활성화할 경우, 포트는 블록 할당 크기에 따라 분산되며 기본값은 512입니다.

- PAT 풀에 대한 블록 할당을 활성화하면 포트 블록은 1024-65535 범위로만 할당됩니다. 따라서 애플리케이션에 낮은 포트 번호(1-1023)가 필요한 경우 작동하지 않을 수 있습니다. 예를 들어 포트 22(SSH)를 요청하는 애플리케이션은 1024-65535 범위 내에서 호스트에 할당된 블록 내에서 매핑된 포트를 가져옵니다.

- 별개의 두 규칙에서 동일한 PAT 풀 개체를 사용하는 경우 각 규칙에 대해 동일한 옵션을 지정해야 합니다. 예를 들어, 한 규칙에서 확장 PAT를 지정하는 경우, 다른 규칙에서도 확장 PAT를 지정해야 합니다.

PAT 풀용 확장 PAT의 경우

- 확장 PAT를 지원하지 않는 애플리케이션 검사가 많습니다.
- 동적 PAT 규칙에 대해 확장 PAT를 활성화하면, PAT 풀의 주소를 별도의 포트 변환 고정 NAT 규칙에서 PAT 주소로서 사용할 수 없습니다. 예를 들어 PAT 풀이 10.1.1.1을 포함하면, 10.1.1.1을 PAT 주소로 사용하는 포트 변환 고정 NAT 규칙을 만들 수 없습니다.
- PAT 풀을 사용하고 대안용 인터페이스를 지정하는 경우 확장 PAT를 지정할 수 없습니다.
- ICE 또는 TURN을 사용하는 VoIP 구축에는 확장 PAT를 사용할 수 없습니다. ICE 및 TURN은 모든 대상에 대해 PAT 바인딩이 동일할 것으로 신뢰합니다.
- 클러스터의 유닛에서는 확장 PAT를 사용할 수 없습니다.

PAT 풀용 라운드 로빈의 경우

- 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. 장애 조치 이후에는 "동질성"이 해제됩니다. 디바이스에서 장애 조치를 수행하면 호스트의 후속 연결에는 초기 IP 주소가 사용되지 않을 수 있습니다.
- 동일한 인터페이스에서 PAT 풀/라운드 로빈 규칙과 인터페이스 PAT 규칙을 혼합하면 IP 주소 "동질성"도 영향을 받습니다. 특정 인터페이스에 대해 PAT 풀 또는 인터페이스 PAT를 선택합니다. 경쟁적인 PAT 규칙을 만들지 마십시오.
- 라운드 로빈은 특히 확장 PAT와 함께 사용할 경우 대량의 메모리를 소모할 수 있습니다. NAT 풀은 모든 매핑된 프로토콜/IP 주소/포트 범위에 대해 생성되므로, 라운드 로빈에서 대량의 동시 NAT 풀이 생성되며 여기에서 메모리를 사용합니다. 확장 PAT를 사용하면 동시 NAT 풀의 수가 더 많아집니다.

동적 자동 **PAT** 구성

동적 자동 PAT 규칙을 사용하여 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환하거나 PAT 주소 풀을 사용하여 가능한 많은 수의 변환을 제공할 수 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- 변환된 소스 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.
  - **PAT** 풀 - 범위가 포함된 네트워크 개체를 만들거나 호스트, 범위 또는 둘 다를 포함하는 네트워크 개체 그룹을 만듭니다. 서브넷을 포함할 수 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 동적을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀 구성 단계를 건너뜁니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀 구성 단계를 건너뜁니다.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다.

단계 **6** PAT 풀을 사용하는 경우 **PAT Pool(PAT** 풀**)** 페이지를 선택하고 다음을 수행합니다.

a) **Enable PAT pool(PAT** 풀 활성화**)**을 선택합니다.

b) **PAT** > **Address(**주소**)** 필드에서 풀의 주소를 포함하는 네트워크 개체 그룹을 선택합니다.

Destination Interface IP(대상 인터페이스 **IP)**를 선택하여 인터페이스 PAT를 구현할 수도 있습니다.

c) (선택 사항) 필요한 경우 다음 옵션을 선택합니다.

- **Use Round Robin Allocation(**라운드 로빈 할당 사용**)** - 라운드 로빈 방식으로 주소/포트를 할당하려는 경우 선택합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.
- **Extended PAT Table(**확장 **PAT** 테이블**)** - 확장 PAT를 사용하려는 경우 선택합니다. 확장 PAT는 변환 정보의 대상 주소 및 포트를 포함하여 서비스당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 대상 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이

동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. 이 옵션은 인터페이스 PAT 또는 인터페이스 PAT 대체와 함께 사용할 수 없습니다.

- **Flat Port Range(**균일 포트 범위**)**, **Include Reserved Ports(**예약된 포트 포함**)** - TCP/UDP 포트를 할당할 때 단일 균일 범위로 1024~65535 포트 범위를 사용하려는 경우 선택합니다. (6.7 버전 이전) 변환할 매핑된 포트 번호를 선택하면 PAT에서는 실제 소스 포트 번호(사용 가능한 경우)를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 없는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **Include Reserved Ports(**예약된 포트 포함**)** 옵션도 선택합니다. 버전 6.7 이상을 실행하는 FTD 디바이스의 경우 옵션 선택 여부에 관계없이 플랫 포트 범위가 항상 구성됩니다. 이러한 시스템에 대해 **Include Reserved Ports(**예약 포트 포함**)** 옵션을 여전히 선택할 수 있으며 해당 설정이 적용됩니다.
- **Block Allocation(**블록 할당**)**- 포트 블록 할당을 활성화하려는 경우 선택합니다. 캐리어급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다. 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한 활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 포트 블록은 1024~65535 범위에서만 할당됩니다. 포트 블록 할당은 라운드 로빈과는 호환되지만 확장 PAT 또는 플랫 포트 범위 옵션과 함께 사용할 수는 없습니다. 또한 인터페이스 PAT 대체를 사용할 수 없습니다.

단계 **7** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- **Fallthrough to Interface PAT (Destination Interface)(**인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**)** - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다. 인터페이스 PAT를 변환된 주소 또는 PAT 풀로 이미 구성한 경우에는 이 옵션을 선택할 수 없습니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **9** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

동적 수동 **PAT** 구성

자동 PAT가 요구를 충족하지 않을 때는 동적 수동 PAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 PAT는 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환하거나 PAT 주소 풀을 사용하여 가능한 많은 수의 변환을 제공할 수 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- 변환된 소스 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.
  - **PAT** 풀 - 범위가 포함된 네트워크 개체를 만들거나 호스트, 범위 또는 둘 다를 포함하는 네트워크 개체 그룹을 만듭니다. 서브넷을 포함할 수 없습니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 NAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

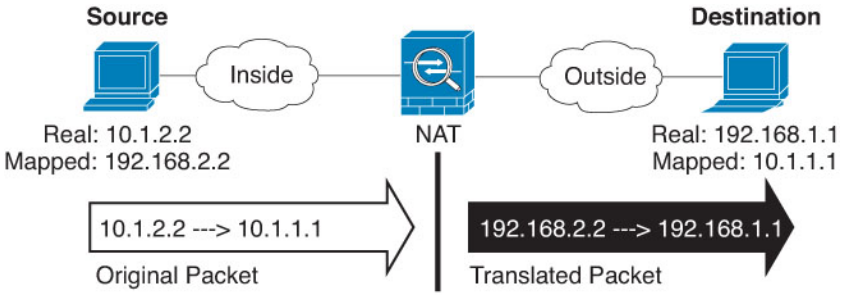
- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 동적을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.
- **Enable(**활성화**)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(**삽입**)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** (변환 페이지에서) 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Source Interface IP(소스 인터페이스 **IP)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀 구성 단계를 건너뜁니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀 구성 단계를 건너뜁니다.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다.
- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트(**Original Destination Port(**원본 대상 포트**)**, **Translated Destination Port(**변환된 대상 포트**)**)를 식별합니다.

동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port(**원본 대상 포트**)** 및 **Translated Destination Port(**변환된 대상 포트**)** 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** PAT 풀을 사용하는 경우 **PAT Pool(PAT** 풀**)** 페이지를 선택하고 다음을 수행합니다.

a) **Enable PAT pool(PAT** 풀 활성화**)**을 선택합니다.

b) **PAT** > **Address(**주소**)** 필드에서 풀의 주소를 포함하는 네트워크 개체 그룹을 선택합니다.

Destination Interface IP(대상 인터페이스 **IP)**를 선택하여 인터페이스 PAT를 구현할 수도 있습니다.

c) (선택 사항) 필요한 경우 다음 옵션을 선택합니다.

- **Use Round Robin Allocation(**라운드 로빈 할당 사용**)** - 라운드 로빈 방식으로 주소/포트를 할당하려는 경우 선택합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.

- **Extended PAT Table(**확장 **PAT** 테이블**)** - 확장 PAT를 사용하려는 경우 선택합니다. 확장 PAT는 변환 정보의 대상 주소 및 포트를 포함하여 서비스당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 대상 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. 이 옵션은 인터페이스 PAT 또는 인터페이스 PAT 대체와 함께 사용할 수 없습니다.

- **Flat Port Range(**균일 포트 범위**)**, **Include Reserved Ports(**예약된 포트 포함**)** - TCP/UDP 포트를 할당할 때 단일 균일 범위로 1024~65535 포트 범위를 사용하려는 경우 선택합니다. (6.7 버전 이전) 변환할 매핑된 포트 번호를 선택하면 PAT에서는 실제 소스 포트 번호(사용 가능한 경우)를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 없는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **Include Reserved Ports(**예약된 포트 포함**)** 옵션도 선택합니다. 버전 6.7 이상을 실행하는 FTD 디바이스의 경우 옵션 선택 여부에 관계없이 플랫 포트 범위가 항상 구성됩니다. 이러한 시스템에 대해 **Include Reserved Ports(**예약 포트 포함**)** 옵션을 여전히 선택할 수 있으며 해당 설정이 적용됩니다.

- **Block Allocation(**블록 할당**)**- 포트 블록 할당을 활성화하려는 경우 선택합니다. 캐리어급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다. 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한

활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 포트 블록은 1024~65535 범위에서만 할당됩니다. 포트 블록 할당은 라운드 로빈과는 호환되지만 확장 PAT 또는 플랫 포트 범위 옵션과 함께 사용할 수는 없습니다. 또한 인터페이스 PAT 대체를 사용할 수 없습니다.

단계 **9** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **10** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **11** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

포트 블록 할당으로 **PAT** 설정

통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한 활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 블록에서 포트를 사용하는 마지막 xlate가 제거되면 블록이 해제됩니다.

포트 블록을 할당하는 주된 이유는 로깅을 줄이는 것입니다. 포트 블록 할당이 기록되고 연결은 기록되지만 포트 블록 내에서 생성된 xlate는 기록되지 않습니다. 반면에, 이렇게 하면 로그 분석이 더 어려워집니다.

포트 블록은 1024~65535 범위에서만 할당됩니다. 따라서 애플리케이션에 낮은 포트 번호(1-1023)가 필요한 경우 작동하지 않을 수 있습니다. 예를 들어 포트 22(SSH)를 요청하는 애플리케이션은 1024-65535 범위 내에서 호스트에 할당된 블록 내에서 매핑된 포트를 가져옵니다. 낮은 포트 번호를 사용하는 애플리케이션에 대해 블록 할당을 사용하지 않는 별도의 NAT 규칙을 만들 수 있습니다. 2회 NAT를 사용하려면 규칙이 블록 할당 규칙보다 먼저 적용되는지 확인하십시오.

시작하기 전에

NAT 규칙에 대한 사용 참고 사항:

- **Use Round Robin Allocation(**라운드 로빈 할당 사용**)** 옵션을 포함할 수 있지만 PAT 고유성 확장, 플랫 범위 사용, 예비 포트 포함, 또는 PAT 인터페이스로 폴스루할 수 있는 옵션은 포함할 수 없습니다. 다른 소스/대상 주소 및 포트 정보도 허용됩니다.
- 모든 NAT 변경 사항과 마찬가지로 기존 규칙을 바꿀 경우 교체된 규칙과 관련된 xlate를 지워야 새 규칙이 적용됩니다. 명시적으로 지우거나 시간 초과될 때까지 기다릴 수 있습니다. 클러스터에서 작업할 때는 클러스터 전체에서 xlate를 전역적으로 지워야 합니다.

참고 개체 NAT에 대해 일반 PAT와 블록 할당 PAT 규칙 간에 전환하는 경우 먼저 규칙을 삭제한 다음 xlate를 지워야 합니다. 그런 다음 새 개체 NAT 규칙을 생성할 수 있습니다. 그렇지 않으면, **show asp drop** 출력에서 pat-port-block-state-mismatch 삭제가 발생합니다.

- 지정된 PAT 풀의 경우 풀을 사용하는 모든 규칙에 대해 블록 할당을 지정하거나 지정하지 않아야 합니다. 하나의 규칙에는 블록을 할당할 수 없고 다른 규칙에는 블록을 할당할 수 있습니다. 중복되는 PAT 풀도 블록 할당 설정을 혼합할 수 없습니다. 또한 정적 NAT는 풀의 포트 변환 규칙과 중복될 수 없습니다.

프로시저

단계 **1** (선택 사항). 전역 PAT 포트 블록 할당 설정을 구성합니다.

포트 블록 할당을 제어하는 몇 가지 전역 설정이 있습니다. 이 옵션의 기본값을 변경하려면 FlexConfig 개체를 구성하여 FlexConfig 정책에 추가해야 합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택하고 새 개체를 만듭니다.

b) 각 블록의 포트 수인 블록 할당 크기를 구성합니다.

xlate block-allocation size 값

범위는 32~4096입니다. 기본값은 512입니다. 기본값으로 되돌리려면 "no" 양식을 사용합니다.

기본값을 사용하지 않는 경우 선택한 크기가 64,512(1024-65535 범위의 포트 수)로 균등하게 나뉘어 있는지 확인합니다. 그렇지 않으면 사용할 수 없는 포트가 있게 됩니다. 예를 들어 100을 지정하는 경우 사용되지 않는 포트가 12개 있습니다.

c) 호스트당 할당할 수 있는 최대 블록을 구성합니다.

xlate block-allocation maximum-per-host *number*

제한은 프로토콜에 따라 다르기 때문에 4개의 제한은 호스트당 최대 4개의 UDP 블록, 4개의 TCP 블록 및 4개의 ICMP 블록을 의미합니다. 범위는 1-8이며, 기본값은 4입니다. 기본값으로 되돌리려면 "no" 양식을 사용합니다.

d) (선택 사항). 임시 syslog 생성을 활성화합니다.

xlate block-allocation pba-interim-logging *seconds*

기본적으로 시스템이 포트 블록 생성 및 삭제를 수행하는 동안 syslog 메시지를 생성합니다. 중간 로깅을 활성화하면 시스템은 지정하는 간격으로 다음 메시지를 생성합니다. 메시지는 이때 프로토콜(ICMP, TCP, UDP), 소스 및 대상 인터페이스, IP 주소, 포트 블록을 포함하여 할당된 모든 활성 포트 블록을 보고합니다. 21600-604800초(6시간~7일) 사이의 간격을 지정할 수 있습니다.

%ASA-6-305017: Pba-interim-logging: *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*의 변환에 대한 활성 포트 프로토콜 블록

예제:

다음 예제는 블록 할당 크기를 64로 설정하고 호스트당 최대 값을 8로 설정하고 6시간마다 임시 로깅을 활성화합니다.

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) FlexConfig 개체에서 다음 옵션을 선택합니다.

- **Deployment(**구축**)** = **Everytime(**항상**)**
- **Type(**유형**)** = **Append(**뒤에 추가**)**

f) **Save(**저장**)**를 클릭하여 FlexConfig 개체를 생성합니다.

g) **Devices(**디바이스**)** > **FlexConfig**를 선택하고 이러한 설정을 조정해야 하는 디바이스에 할당된 FlexConfig 정책을 만들거나 편집합니다.

h) 사용 가능한 개체 목록에서 개체를 선택하고 >를 클릭하여 선택한 개체 목록으로 이동합니다.

i) **Save(**저장**)**를 클릭합니다.

Preview Config(구성 미리보기**)**를 클릭하고 대상 디바이스 중 하나를 선택한 다음 xlate 명령이 올바르게 나타나는지 확인할 수 있습니다.

단계 **2** PAT 풀 포트 블록 할당을 사용하는 NAT 규칙을 추가합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 Threat Defense NAT 정책을 생성하거나 편집합니다.

b) NAT 규칙을 추가 또는 편집하고 다음 옵션을 구성합니다.

- **Type(**유형**)** = **Dynamic(**동적**)**.
- **Translation(**변환**)** > **Original Source(**원본 소스**)**에서 원본 주소를 정의하는 개체를 선택합니다.
- **PAT** 풀에서 다음 옵션을 구성합니다.
  - **Enable PAT Pool(PAT** 풀 활성화**)**을 선택합니다.
  - **PAT** > **Address(**주소**)**에서 pat 풀을 정의하는 네트워크 개체를 선택합니다.
  - **Block Allocation(**블록 할당**)** 옵션을 선택합니다.

c) 변경 사항을 규칙 및 NAT 정책에 저장합니다.

고정 NAT

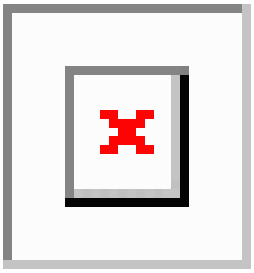
다음 주제에서는 고정 NAT 및 고정 NAT를 구현하는 방법에 대해 설명합니다.

고정 NAT 정보

고정 NAT는 실제 주소에서 매핑된 주소로의 고정된 변환을 생성합니다. 매핑된 주소는 각각의 연속 연결에 대해 동일하므로 NAT는 양방향 연결 시작을 허용합니다. 이를 허용하는 액세스 규칙이 있는 경우 호스트에서 나가기도 하고 호스트로 들어오기도 합니다. 반면 동적 NAT 및 PAT의 경우, 각 호스트는 각 후속 변환에 대해 서로 다른 주소 또는 포트를 사용하므로 양방향 시작이 지원되지 않습니다.

다음 그림은 일반적인 고정 NAT 시나리오를 보여줍니다. 변환이 항상 활성 상태이므로 실제 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 ***53:*** 고정 ***NAT***



참고 원하는 경우 양방향을 비활성화할 수 있습니다.

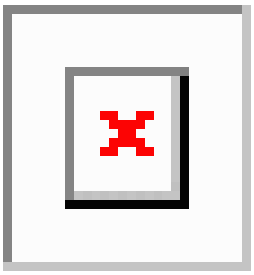
포트 변환 고정 NAT

포트 변환 고정 NAT를 사용하면 실제 및 매핑된 프로토콜과 포트를 지정할 수 있습니다.

고정 NAT로 포트를 지정하는 경우 포트 및/또는 IP 주소를 동일한 값으로 매핑할지 아니면 다른 값으로 매핑할지를 선택할 수 있습니다.

다음 그림은 자신에게 매핑되는 포트와 다른 값으로 매핑되는 포트 모두를 보여주는 포트 변환 시나리오의 일반적인 고정 NAT를 보여줍니다. 두 경우 모두 IP 주소는 다른 값으로 매핑됩니다. 변환이 항상 활성 상태이므로 변환된 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 ***54:*** 일반적인 포트 변환 고정 ***NAT*** 시나리오



포트 변환 고정 NAT 규칙은 지정된 포트에 대해서만 대상 IP 주소 액세스를 제한합니다. NAT 규칙이 적용되지 않는 다른 포트에서 대상 IP 주소에 액세스를 시도하면 연결은 차단됩니다. 또한 수동 NAT의 경우 NAT 규칙의 소스 IP 주소와 일치하지 않는 트래픽은 대상 포트와 관계없이 대상 IP 주소와 일치하는 경우 삭제됩니다. 그러므로 대상 IP 주소에 대해 허용되는 기타 모든 트래픽을 위한 규칙을 더 추가해야 합니다. 예를 들어 포트 사양 없이 IP 주소용 고정 NAT 규칙을 구성하여 포트 변환 규칙 뒤에 배치할 수 있습니다.

참고 보조 채널(예: FTP 및 VoIP)에 대해 애플리케이션 검사를 요구하는 애플리케이션의 경우 NAT에서는 자동으로 보조 포트를 변환합니다.

포트 변환 고정 NAT의 몇 가지 다른 사용 방식은 다음과 같습니다.

ID 포트 변환 고정 **NAT**

내부 리소스에 대한 외부 액세스를 간소화할 수 있습니다. 예를 들어, FTP, HTTP, SMTP 등 각기 다른 포트에서 서비스를 제공하는 개별 서버 3개가 있는 경우 외부 사용자에게 해당 서비스 액세스를 위한 단일 IP 주소를 제공할 수 있습니다. 그런 후에 외부 사용자들이 액세스하려는 포트를 기준으로 하여 실제 서버의 올바른 IP 주소에 단일 외부 IP 주소를 매핑하도록 ID 포트 변환 고정 NAT를 구성할 수 있습니다. 이러한 서버는 표준 포트(각각 21, 80, 25)를 사용하므로 포트를 변경할 필요는 없습니다.

비표준 포트에 대한 포트 변환 고정 **NAT**

잘 알려진 포트를 비표준 포트로 또는 그 반대로 변환하려는 경우에도 포트 변환 고정 NAT를 사용할 수 있습니다. 예를 들어 내부 웹 서버가 포트 8080을 사용하는 경우 외부 사용자가 포트 80에 연결하도록 허용한 다음 원본 포트 8080으로의 변환을 취소할 수 있습니다. 마찬가지로, 보안을 강화하려면 웹 사용자에게 비표준 포트 6785로 연결하도록 안내한 다음 포트 80으로의 변환을 취소할 수 있습니다.

포트 변환 고정 인터페이스 **NAT**

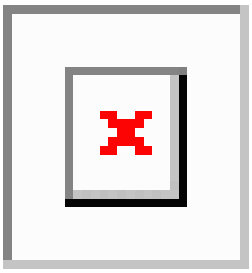
실제 주소를 인터페이스 주소/포트 조합으로 매핑하도록 고정 NAT를 구성할 수 있습니다. 예를 들어 디바이스의 외부 인터페이스에 대한 텔넷 액세스를 내부 호스트로 리디렉션하려는 경우 내부 호스트 IP 주소/포트 23을 외부 인터페이스 주소/포트 23에 매핑할 수 있습니다.

일대다 고정 **NAT**

일반적으로 NAT는 일대일 매핑으로 구성합니다. 그러나 경우에 따라 여러 매핑된 주소에 대해 단일 실제 주소를 구성해야 할 수도 있습니다(일대다). 일대다 고정 NAT를 구성할 경우, 실제 호스트가 트래픽을 시작하면 항상 첫 번째 매핑된 주소를 사용합니다. 그러나 호스트에 대해 시작된 트래픽의 경우, 매핑된 주소 중 하나에 대해 트래픽을 시작할 수 있습니다. 이러한 주소는 단일 실제 주소로 변환되지 않습니다.

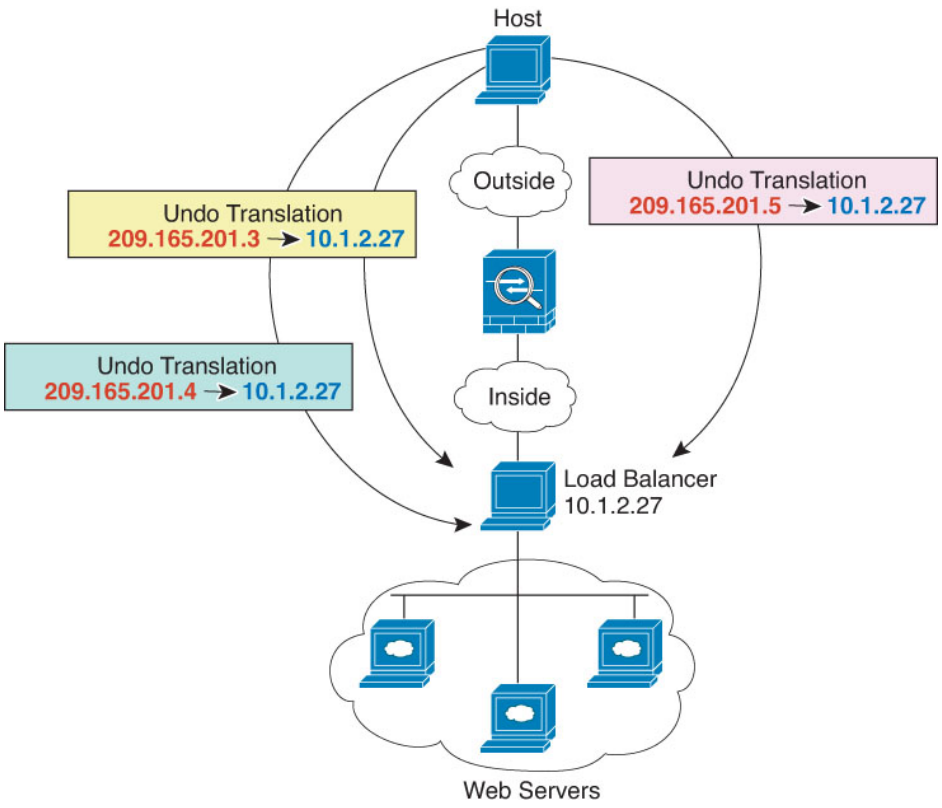
다음 그림은 일반적인 일대다 고정 NAT 시나리오를 보여줍니다. 실제 호스트에 의한 시작은 항상 첫 번째 매핑된 주소를 사용하므로, 실제 호스트 IP/첫 번째 매핑된 IP의 변환이 기술적으로 유일한 양방향 변환입니다.

그림 *55:* 일대다 고정 ***NAT***



예를 들어 10.1.2.27에 로드 밸런서가 있으면, 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다.

그림 *56:* 일대다 고정 ***NAT*** 예



기타 매핑 시나리오(권장되지 않음)

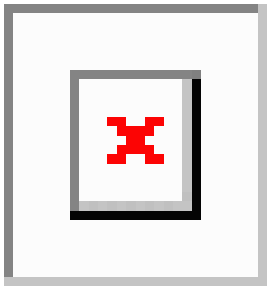
NAT에서는 일대일, 일대다, 소수대다수, 다수대소수, 다대일 등 모든 종류의 고정 매핑 시나리오를 유연하게 허용합니다. 그러나 일대일 또는 일대다 매핑만 사용하는 것이 좋습니다. 다른 매핑 옵션을 사용할 경우 예기치 않은 결과가 발생할 수 있습니다.

소수대다수는 기능상 일대다와 같지만, 구성이 좀 더 복잡하고 실제 매핑이 한눈에 명확히 파악되지 않을 수 있으므로 필요한 경우 각 실제 주소에 대해 일대다 구성을 만드는 것이 좋습니다. 소수대다수 시나리오에서는 소수의 실제 주소가 다수의 매핑된 주소로 순서대로 매핑됩니다(A-1, B-2, C-3).

모든 실제 주소가 매핑되면 다음의 매핑된 주소는 첫 번째 실제 주소로 매핑되며, 모든 매핑된 주소가 매핑될 때까지 같은 방식이 반복됩니다(A-4, B-5, C-6). 그 결과 각 실제 주소에 다수의 매핑된 주소가 연결됩니다. 일대다 구성의 경우와 마찬가지로 첫 번째 매핑만 양방향이고 이후 매핑에서는 실제 호스트로만 트래픽이 시작되고, 실제 호스트로부터의 모든 트래픽은 소스에 대해 첫 번째 매핑된 주소만 사용합니다.

다음 그림은 일반적인 소수대다수 고정 NAT 시나리오를 보여줍니다.

그림 ***57:*** 소수대다수 고정 ***NAT***

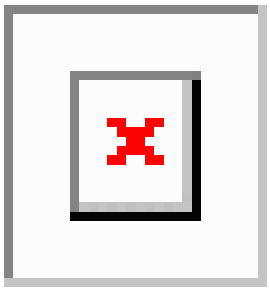


매핑된 주소보다 실제 주소가 더 많은 다수대소수 또는 다대일 컨피그레이션의 경우, 실제 주소가 소진되기 전에 매핑된 주소가 소진됩니다. 가장 낮은 실제 IP 주소와 매핑된 풀 간의 매핑만 양방향 시작이 가능합니다. 나머지 더 높은 실제 주소는 트래픽을 시작할 수 있지만 이러한 주소로 트래픽이 시작될 수는 없습니다. 연결에 대한 고유한 5튜플(소스/대상 IP 주소, 소스/대상 포트 및 프로토콜) 때문에 연결에 대한 반환 트래픽은 정확한 실제 주소로 전달됩니다.

참고 다수대소수 또는 다대일 NAT는 PAT가 아닙니다. 두 개의 실제 호스트가 동일한 소스 포트 번호를 사용하고 동일한 외부 서버 및 동일한 TCP 대상 포트로 이동하며 두 호스트가 동일한 IP 주소로 변환되면, 주소 충돌 때문에(5튜플이 고유하지 않음) 두 연결이 재설정됩니다.

다음 그림은 일반적인 다수대소수 고정 NAT 시나리오를 보여줍니다.

그림 ***58:*** 다수대소수 고정 ***NAT***



고정 규칙을 이 방식으로 사용하는 대신, 양방향 시작이 필요한 트래픽에 대해 일대일 규칙을 만든 다음 나머지 주소에 대해 동적 규칙을 만드는 방식을 권장합니다.

고정 자동 NAT 구성

고정 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- **Translated Source(**변환된 소스**)** - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
  - 주소 - 호스트, 범위 또는 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**)** - **Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 고정을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(**주소**)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
- (선택 사항). **Original Port(**원래 포트**)**, Translated Port(변환된 포트) - TCP 또는 UDP 포트를 변환해야 하는 경우 **Original Port(**원래 포트**)**에서 프로토콜을 선택하고 원래 및 변환된 포트 번호를 입력합니다. 예를 들어, 필요에 따라 TCP/80을 8080으로 변환할 수 있습니다.

단계 **6** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 -DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 1590 페이지을 참조하십시오. 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.
- **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**—NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째 IPv4 주소를 두 번째 IPv6 주소로 변환하는 방식을 사용하려면 이 옵션을 선택합니다. 이 옵션이 없으면 IPv4 포함 메서드가 사용됩니다. 일대일 변환에는 이 옵션을 사용해야 합니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **8** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

고정 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 고정 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- **Translated Source(**변환된 소스**)** - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
  - 주소 - 호스트, 범위 또는 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 및 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.

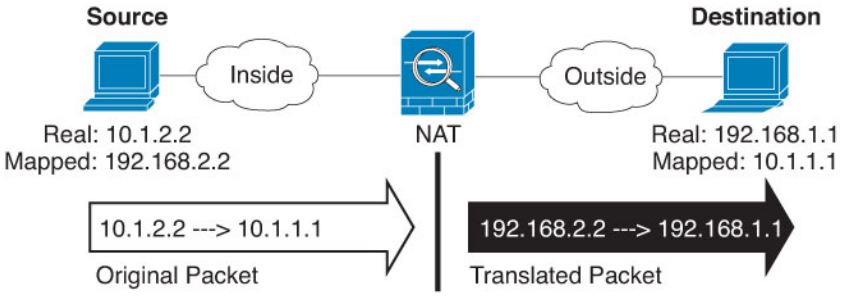
- **Enable(**활성화**)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(**삽입**)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** (변환 페이지에서) 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Source Interface IP(소스 인터페이스 **IP)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(**주소**)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인

터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.

- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환의 원본 또는 대상 서비스 포트를 식별합니다.

포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 -DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 1590 페이지을 참조하십시오. 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.
- **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**—NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째 IPv4 주소를 두 번째 IPv6 주소로 변환하는 방식을 사용하려면 이 옵션을 선택합니다. 이 옵션이 없으면 IPv4 포함 메서드가 사용됩니다. 일대일 변환에는 이 옵션을 사용해야 합니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- **Unidirectional(**단방향**)**—대상 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 이 옵션을 선택합니다. 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

단계 **9** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

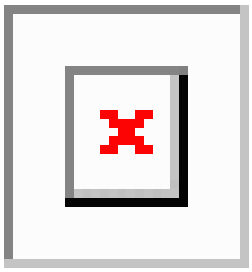
단계 **10** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

ID NAT

IP 주소를 자신으로 변환해야 하는 NAT 구성이 있을 수 있습니다. 예를 들어 NAT를 모든 네트워크에 적용하는 광범위한 규칙을 만들되 NAT에서 하나의 네트워크만 제외하고 싶은 경우, 주소를 자신으로 변환하는 고정 NAT 규칙을 만들 수 있습니다.

다음 그림은 일반적인 ID NAT 시나리오를 보여줍니다.

그림 ***59: ID NAT***



다음 주제에서는 ID NAT를 구성하는 방법을 설명합니다.

ID 자동 NAT 구성

주소 변환을 방지하려면 고정 ID 자동 NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- **Translated Source(**변환된 소스**)** - 원본 소스 개체와 내용이 정확히 동일한 네트워크 개체 또는 그룹입니다. 동일한 개체를 사용할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 고정을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- **Translated Source(**변환된 소스**)** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

ID NAT의 경우에는 원본 포트 및 변환된 포트 옵션을 구성하지 마십시오.

단계 **6** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- **IPv6** - ID NAT에 이 옵션을 구성하지 마십시오.
- **Net to Net Mapping(**네트워크 대 네트워크 매핑**)** - ID NAT에 이 옵션을 구성하지 마십시오.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- 대상 인터페이스에 대해 경로 조회 수행 - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **8** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

ID 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 ID 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 주소 변환을 방지하려면 고정 ID NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- **Translated Source(**변환된 소스**)** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 및 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. ID NAT에 대해 동일한 개체를 사용할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

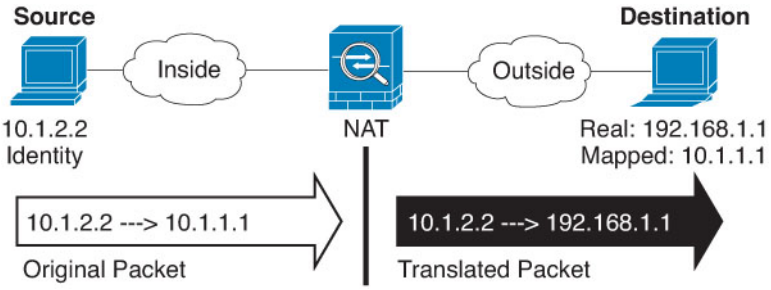
- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.
- **Enable(**활성화**)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(**삽입**)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오. 여기서 내부 호스트에 대해서는 ID NAT를 수행하지만 외부 호스트는 변환합니다.



- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination(**원본 대상**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Interface Object(인터페이스 개체**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- **Translated Source(**변환된 소스**)** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.
- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환의 원본 또는 대상 서비스 포트를 식별합니다.

포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- 대상 인터페이스에 대해 경로 조회 수행 - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.
- **Unidirectional(**단방향**)**—대상 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 이 옵션을 선택합니다. 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

단계 **9** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **10** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

Firepower Threat Defense의 NAT 규칙 속성

NAT(네트워크 주소 변환) 규칙을 사용하여 IP 주소를 다른 IP 주소로 변환합니다. 일반적으로는 NAT 규칙을 사용하여 전용 어드레스를 공개적으로 라우팅 가능한 주소로 변환합니다. 변환을 주소 간에 수행할 수도 있고, PAT(포트 주소 변환)를 사용해 여러 주소를 하나 또는 소수의 주소로 변환하고 포트 번호를 사용해 각 소스 주소를 구분할 수도 있습니다.

NAT 규칙은 다음 기본 속성을 포함합니다. 이러한 속성은 별도로 명시된 경우를 제외하면 자동 NAT 및 수동 NAT 규칙에 대해 동일합니다.

NAT 유형

수동 **NAT** 규칙 또는 자동 **NAT** 규칙을 구성할 것인지 여부입니다. 자동 NAT는 원본 주소만 변환하므로 대상 주소를 기반으로 다른 번환을 수행할 수 없습니다. 자동 NAT는 구성하기가 더 쉽기 때문에 수동 NAT의 추가 기능이 필요하지 않는 한 자동 NAT를 사용하십시오. 차이점에 대한 자세한 내용은 자동 NAT 및 수동 NAT, 1491 페이지 섹션을 참고하십시오.

유형

변환 규칙이 동적인지 아니면 정적인지를 나타냅니다. 동적 변환에서는 주소 풀에서 매핑된 주소를 자동으로 선택하며, PAT를 구현할 때는 주소/포트 조합을 선택합니다. 매핑된 주소/포트를 정확하게 정의하려면 정적 변환을 사용하십시오.

Enable(활성화**)(**수동 **NAT**만 해당**)**

규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다. 자동 NAT 규칙을 비활성화할 수 없습니다.

Insert(삽입**)(**수동 **NAT**만 해당**)**

규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

Description(설명**)(**선택 사항**,** 수동 **NAT**만 해당**)**

규칙의 목적에 대한 설명입니다.

다음 주제에서는 나머지 NAT 규칙 속성 탭에 대해 설명합니다.

인터페이스 개체 **NAT** 속성

NAT 규칙이 적용되는 인터페이스를 정의하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. 라우팅된 모드에서는 소스와 대상 모두에 대해 기본 "임의" 개념을 사용하여 할당된 모든 디바이스의 모든 인터페이스에 적용할 수 있습니다. 하지만 일반적으로 특정 소스 및 대상 인터페이스를 선택하고자 합니다.

참고 브리지 그룹 멤버 인터페이스에는 "임의" 인터페이스라는 개념이 적용되지 않습니다. "any" 인터페이스를 지정하면 모든 브리지 그룹 멤버 인터페이스는 제외됩니다. 따라서 브리지 그룹 멤버에 NAT를 적용하려면 멤버 인터페이스를 지정해야 합니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT를 구성할 수 없으며 멤버 인터페이스에 대해서만 NAT를 구성할 수 있습니다.

인터페이스 개체를 선택한 경우 디바이스에 선택한 모든 개체에 인터페이스가 있는 경우에만 할당된 디바이스에 NAT 규칙이 구성됩니다. 예를 들어 원본 및 대상 보안 영역을 모두 선택하면 두 영역 모두 특정 디바이스에 대한 하나 이상의 인터페이스를 포함해야 합니다.

Source Interface Objects(소스 인터페이스 개체**), Destination Interface Objects(**대상 인터페이스 개체**)**

(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

자동 NAT에 대한 Translation 속성

Translation(변환**)**의 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 자동 NAT에만 적용됩니다.

원본 소스**(**항상 필수**)**

변환 중인 주소를 포함하는 네트워크 개체입니다. 그룹이 아닌 네트워크 개체여야 하며, 호스트, 범위 또는 서브넷일 수 있습니다.

시스템 정의 any-ipv4 또는 any-ipv6 개체에 대해서는 자동 NAT 규칙을 생성할 수 없습니다.

변환된 소스**(**대개 필수**)**

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.
- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀을 구성하지 마십시오.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀을 구성하지 마십시오.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다. **PAT Pool(PAT** 풀**)**에서 PAT 풀 개체를 선택합니다.
- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(**주소**)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 개체 또는 그룹은 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)** 탭에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
- **ID NAT** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

원본 포트, 변환된 포트(고정 NAT에만 해당됨)

TCP 또는 UDP 포트를 변환해야 하는 경우 **Original Port(**원래 포트**)**에서 프로토콜을 선택하고 원래 및 변환된 포트 번호를 입력합니다. 예를 들어, 필요에 따라 TCP/80을 8080으로 변환할 수 있습니다. ID NAT에 이 옵션을 구성하지 마십시오.

수동 NAT에 대한 Translation 속성

Translation(변환**)**의 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 수동 NAT에만 적용됩니다. 별도로 표시된 항목을 제외한 모든 항목은 선택 사항입니다.

원본 소스(항상 필수)

변환 중인 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있으며, 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 규칙에서 임의를 지정하면 됩니다.

변환된 소스(대개 필수)

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.
- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀을 구성하지 마십시오.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀을 구성하지 마십시오.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다. **PAT Pool(PAT** 풀**)**에서 PAT 풀 개체를 선택합니다.
- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(**주소**)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 개체 또는 그룹은 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)** 탭에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페

이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.

- **ID NAT** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

Original Destination(원본 대상**)**

대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

Source Interface IP(소스 인터페이스 **IP)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

Translated Destination(변환된 대상**)**

변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

원본 소스 포트**,** 변환된 소스 포트**,** 원본 대상 포트**,** 변환된 대상 포트

원본 및 변환된 패킷의 소스 및 대상 서비스를 정의하는 포트 개체입니다. 포트를 변환할 수도 있고, 동일한 개체를 선택하여 포트를 변환하지 않고 규칙이 서비스에 따라 달라지도록 설정할 수도 있습니다. 서비스를 구성할 때는 다음 규칙에 유의하십시오.

- (동적 NAT 또는 PAT) 원본 소스 포트 및 변환된 소스 포트에 대해서는 변환을 수행할 수 없습니다. 대상 포트에 대해서만 변환을 수행할 수 있습니다.
- NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

PAT 풀 NAT 속성

동적 NAT를 구성할 때 **PAT Pool(PAT** 풀**)** 탭의 등록 정보를 사용하여 포트 주소 변환에 사용할 주소 풀을 정의할 수 있습니다.

Enable PAT Pool(PAT 풀 활성화**)**

Pat 풀의 주소를 구성하려면 이 옵션을 선택합니다.

PAT

PAT 풀에 사용할 주소이며 다음 중 하나입니다.

- **Address(**주소**)** - 범위를 포함하는 네트워크 개체 또는 호스트, 범위 또는 둘 다를 포함하는 네트워크 개체 그룹 중 하나인 PAT 풀 주소를 정의하는 개체입니다 서브넷을 포함할 수 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.

- **Destination Interface IP(**대상 인터페이스 **IP)** - 대상 인터페이스를 PAT 주소로 사용하려고 하는 것을 나타냅니다. 이 옵션의 경우 특정 **Destination Interface Object(**대상 인터페이스 개체**)** 인터페이스 개체를 선택해야 합니다. 대상 인터페이스로 **Any**를 사용할 수 없습니다. 이는 인터페이스 PAT를 구현하는 또 다른 방법입니다.

라운드 로빈

라운드 로빈 방식으로 주소/포트를 할당하려는 경우 선택합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.

확장된 **PAT** 테이블

확장 PAT를 사용하려는 경우 선택합니다. 확장 PAT는 변환 정보의 대상 주소 및 포트를 포함하여 서비스당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 대상 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. 이 옵션은 인터페이스 PAT 또는 인터페이스 PAT 대체와 함께 사용할 수 없습니다.

Flat Port Range, Include Reserved Ports

TCP/UDP 포트를 할당할 때 단일 균일 범위로 1024~65535 포트 범위를 사용하려는 경우 선택합니다. (6.7 버전 이전) 변환할 매핑된 포트 번호를 선택하면 PAT에서는 실제 소스 포트 번호(사용 가능한 경우)를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 없는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **Include Reserved Ports(**예약된 포트 포함**)** 옵션도 선택합니다. 버전 6.7 이상을 실행하는 FTD 디바이스의 경우 옵션 선택 여부에 관계없이 플랫 포트 범위가 항상 구성됩니다. 이러한 시스템에 대해 **Include Reserved Ports(**예약 포트 포함**)** 옵션을 여전히 선택할 수 있으며 해당 설정이 적용됩니다.

할당 차단

포트 블록 할당을 활성화하려는 경우 선택합니다. 캐리어급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다. 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한 활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 포트 블록은 1024~65535 범위에서만 할당됩니다. 포트 블록 할당은 라운드 로빈과는 호환되지만 확장 PAT 또는 플랫 포트 범위 옵션과 함께 사용할 수는 없습니다. 또한 인터페이스 PAT 대체를 사용할 수 없습니다.

고급 **NAT** 속성

NAT를 구성할 때는 고급 옵션에서 특수 서비스를 제공하는 속성을 구성할 수 있습니다. 이러한 모든 속성은 선택 사항이므로 서비스가 필요할 때만 구성하면 됩니다.

이 규칙과 일치하는 **DNS** 응답 변환

DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 1590 페이지을 참조하십시오. 정적 NAT 규칙에서 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.

인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**(**동적 **NAT**만 해당됨**)**

다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다. 인터페이스 PAT를 변환된 주소로 이미 컨피그레이션한 경우에는 이 옵션을 선택할 수 없습니다. 또한, PAT 풀을 구성하는 경우 이 옵션을 선택할 수 없습니다.

IPv6

인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

네트워크 대 네트워크 매핑**(**고정 **NAT**만 해당됨**)**

NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째 IPv4 주소를 두 번째 IPv6 주소로 변환하는 방식을 사용하려면 이 옵션을 선택합니다. 이 옵션이 없으면 IPv4 포함 메서드가 사용됩니다. 일대일 변환에는 이 옵션을 사용해야 합니다.

대상 인터페이스에서 **ARP** 프록시 설정 안 함**(**고정 **NAT**만 해당됨**)**

매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

대상 인터페이스에 대해 경로 조회 수행**(**고정 **ID NAT** 및 라우팅 모드만 해당됨**)**

원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단방향**(**수동 **NAT** 및 고정 **NAT**만 해당됨**)**

대상 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 이 옵션을 선택합니다. 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

IPv6 네트워크 변환

IPv6 전용 및 IPv4 전용 네트워크 간에 트래픽을 전달해야 하는 경우에는 NAT를 사용해 주소 유형을 변환해야 합니다. 두 IPv6 네트워크 간에 트래픽을 전달할 때도 외부 네트워크에서 내부 네트워크를 숨기려는 경우가 있습니다.

IPv6 네트워크에서는 다음 변환 유형을 사용할 수 있습니다.

- NAT64, NAT46 - IPv6 패킷에서 IPv4 패킷으로, 또는 그 반대로 변환합니다. 이 경우 두 개의 정책(IPv6에서 IPv4로의 변환 정책과 IPv4에서 IPv6으로의 변환 정책)을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있는 경우에는 DNS 응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로 자동 NAT 규칙 2개를 생성하는 것이 더 나은 해결책입니다.

  참고 NAT46은 정적 매핑만 지원합니다.

- NAT66 - IPv6 패킷을 다른 IPv6 주소로 변환합니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

참고 NAT64 및 NAT 46은 표준 라우팅 인터페이스에서만 사용할 수 있습니다. NAT66은 라우팅 인터페이스 및 브리지 그룹 멤버 인터페이스에서 모두 사용 가능합니다.

NAT64/46: IPv6 주소를 IPv4로 변환

트래픽이 IPv6 네트워크에서 IPv4 전용 네트워크로 이동하는 경우에는 IPv6 주소를 IPv4로 변환해야 하며, 반환 트래픽은 IPv4에서 IPv6으로 변환해야 합니다. 따라서 주소 풀 2개(IPv4 네트워크에서 IPv6 주소를 바인딩하기 위한 IPv4 주소 풀과 IPv6 네트워크에서 IPv4 주소를 바인딩하기 위한 IPv6 주소 풀)를 정의해야 합니다.

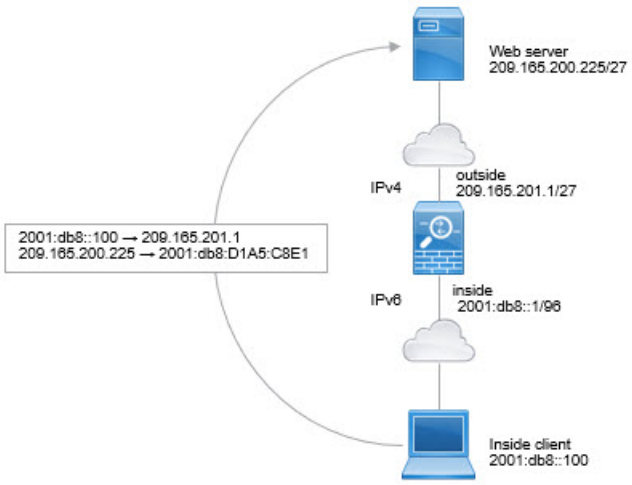
- NAT64 규칙용 IPv4 주소 풀은 일반적으로 크기가 작으므로 대개 IPv6 클라이언트 주소와 일대일로 매핑할 주소를 충분히 포함하지 않을 수 있습니다. 동적 PAT의 경우 동적 또는 고정 NAT에 비해 더 쉽게 많은 IPv6 클라이언트 주소를 포함할 수 있습니다.
- NAT46 규칙용 IPv6 주소 풀은 매핑할 IPv4 주소보다 많은 수의 주소를 포함할 수 있습니다. 따라서 각 IPv4 주소를 서로 다른 IPv6 주소에 매핑할 수 있습니다. NAT46은 고정 매핑만 지원하므로 동적 PAT는 사용할 수 없습니다.

소스 IPv6 네트워크와 대상 IPv4 네트워크 중에 하나씩 2개의 정책을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있는 경우에는 DNS

응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로 자동 NAT 규칙 2개를 생성하는 것이 더 나은 해결책입니다.

NAT64/46 예: 내부 IPv6 네트워크 및 외부 IPv4 인터넷

다음은 내부 IPv6 전용 네트워크를 보유하고 있으며 인터넷으로 전송된 트래픽에 대해 IPv4로 변환하려는 경우의 간단한 예입니다. 이 예에서는 DNS 변환이 필요하지 않다고 가정하므로 단일 수동 NAT 규칙에서 NAT64 및 NAT46 변환을 모두 수행할 수 있습니다.



이 예에서는 외부 인터페이스의 IP 주소가 포함된 동적 인터페이스 PAT를 사용하여 내부 IPv6 네트워크를 IPv4로 변환합니다. 외부 IPv4 트래픽은 2001:db8::/96 네트워크의 주소로 정적 변환되어 내부 네트워크에서 전송을 허용합니다.

프로시저

단계 **1** 내부 IPv6 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

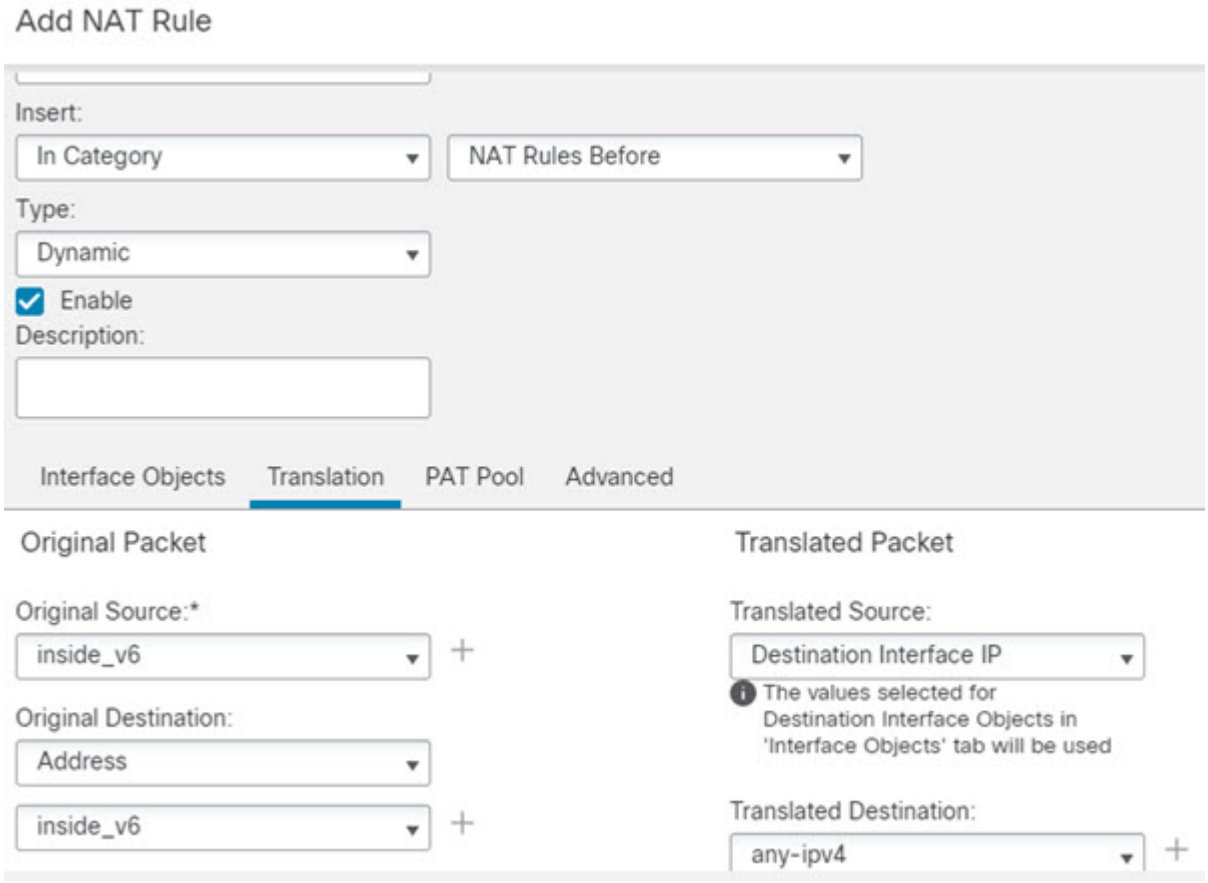
c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8::/96을 입력합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** 수동 NAT 규칙을 생성하여 IPv6 네트워크를 IPv4로 변환한 후 다시 되돌립니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.
b) **Add Rule(**규칙 추가**)**을 클릭합니다.
c) 다음 속성을 구성합니다.
   - **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
   - 유형 = 동적
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.
   - **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
   - **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.
e) **Translation(**변환**)**에서 다음을 구성합니다.
   - **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
   - **Translated Source(**변환된 소스**)** = **Destination Interface IP(**대상 인터페이스 **IP)**
   - **Original Destination(**원본 대상**)** = inside_v6 네트워크 개체
   - **Translated Destination(**변환된 대상**)** = any-ipv4 네트워크 개체



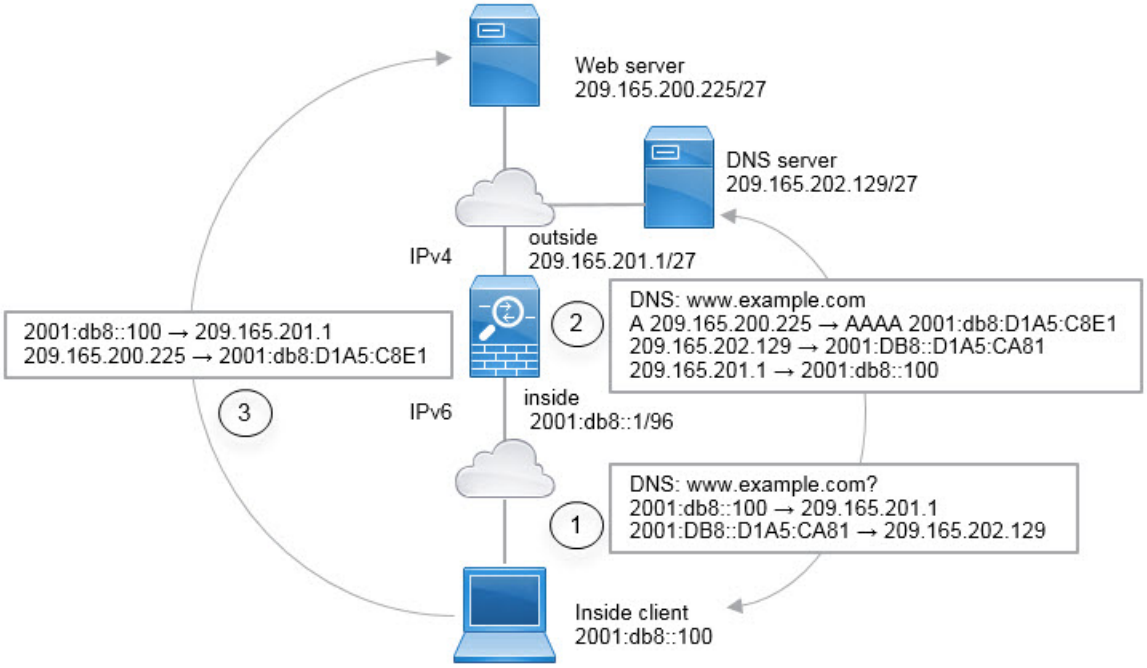
f) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 외부 인터페이스의 IPv4 주소를 사용하여 NAT64 PAT로 변환됩니다. 반대로 외부 네트워크에서 내부 인터페이스로 들어오는 모든 IPv4 주소는 임베디드 IPv4 주소 메서드를 사용하여 2001:db8::/96 네트워크의 주소로 변환됩니다.

g) NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

NAT64/46 예: 내부 IPv6 네트워크와 외부 IPv4 인터넷 및 DNS 변환

아래에는 내부 IPv6 전용 네트워크가 있는데 내부 사용자에게 필요한 일부 IPv4 전용 서비스는 외부 인터넷에 있는 일반적인 예가 나와 있습니다.



이 예에서는 외부 인터페이스의 IP 주소가 포함된 동적 인터페이스 PAT를 사용하여 내부 IPv6 네트워크를 IPv4로 변환합니다. 외부 IPv4 트래픽은 2001:db8::/96 네트워크의 주소로 정적 변환되어 내부 네트워크에서 전송을 허용합니다. 외부 DNS 서버의 회신을 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환하고 주소를 IPv4에서 IPv6으로 변환할 수 있도록 NAT46 규칙에 대해 DNS 재작성을 활성화합니다.

내부 IPv6 네트워크의 2001:DB8::100에 있는 클라이언트가 www.example.com을 열려고 하는 웹 요청의 일반적인 순서는 다음과 같습니다.

1. 클라이언트의 컴퓨터가 2001:DB8::D1A5:CA81에 있는 DNS 서버에 DNS 요청을 보냅니다. NAT 규칙이 DNS 요청에서 소스 및 대상을 다음과 같이 변환합니다.
   - 2001:DB8::100을 209.165.201.1의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
   - 2001:DB8::D1A5:CA81을 209.165.202.129로 변환합니다(NAT46 규칙. D1A5:CA81은 209.165.202.129에 해당하는 IPv6 주소입니다.).
2. DNS 서버가 www.example.com이 209.165.200.225에 있음을 나타내는 A 레코드로 응답합니다. DNS 재작성이 활성화된 NAT46 규칙이 A 레코드를 IPv6의 동일 AAAA 레코드로 변환하고 AAAA 레코드의 209.165.200.225를 2001:db8:D1A5:C8E1로 변환합니다. 또한 DNS 응답의 소스 및 대상 주소는 변환되지 않은 상태입니다.
   - 209.165.202.129 -> 2001:DB8::D1A5:CA81
   - 209.165.201.1 -> 2001:db8::100
3. 이제 IPv6 클라이언트는 웹 서버의 IP 주소를 포함하며 2001:db8:D1A5:C8E1의 www.example.com에 대한 HTTP 요청을 수행합니다. D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소입니다. 그리고 HTTP 요청의 소스 및 대상이 변환됩니다.

- 2001:DB8::100을 209.156.101.54의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
- 2001:db8:D1A5:C8E1을 209.165.200.225로 변환합니다(NAT46 규칙).

다음 절차에서는 이 예를 구성하는 방법을 설명합니다.

시작하기 전에

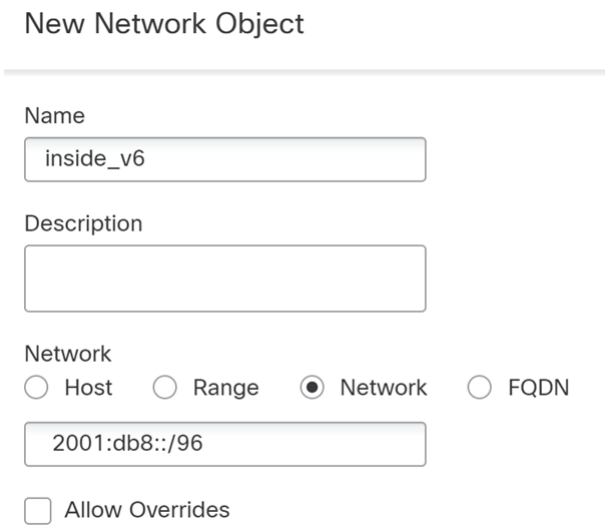
디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 내부 IPv6 및 외부 IPv4 네트워크를 정의하는 네트워크 개체를 생성합니다.

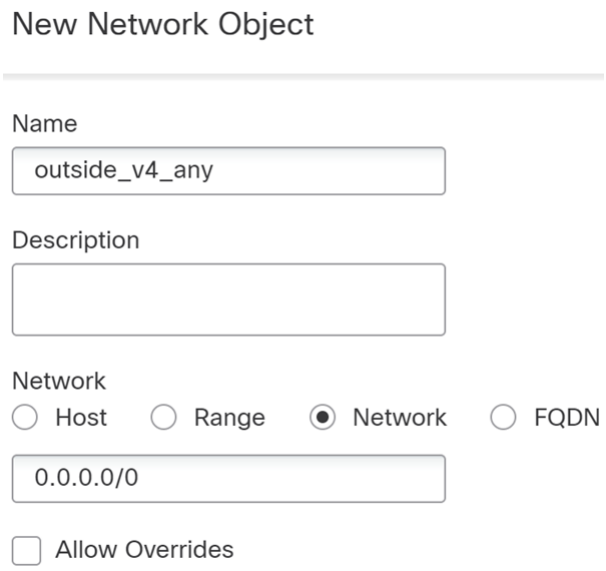
a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8::/96을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.
e) **Add Network(**추가 네트워크**)** > **Add Object(**개체 추가**)**를 클릭하고 외부 IPv4 네트워크를 정의합니다.

네트워크 개체의 이름을 outside_v4_any와 같이 지정하고 네트워크 주소 0.0.0.0/0을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 IPv6 네트워크용 NAT64 동적 PAT 규칙을 구성합니다.

단계 **3** 외부 IPv4 네트워크용 고정 NAT46 규칙을 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

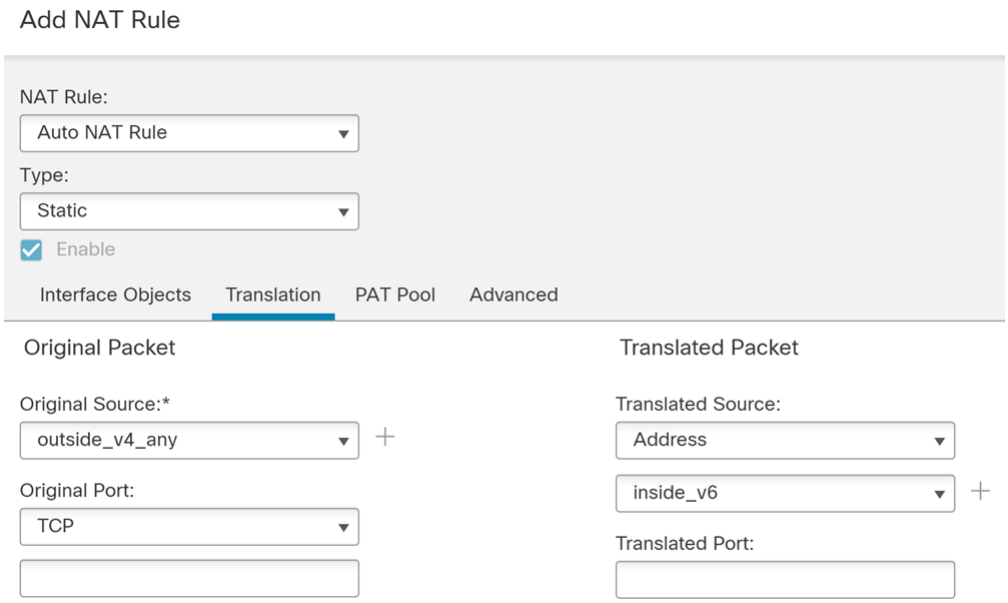
c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = outside_v4_any 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = inside_v6 네트워크 개체.

e) **Advanced(**고급**)**에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



f) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 외부 네트워크에서 내부 인터페이스로 들어오는 모든 IPv4 주소는 임베디드 IPv4 주소 방법을 사용하여 2001:db8::/96 네트워크의 주소로 변환됩니다. 또한 DNS 응답은 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환되며 주소는 IPv4에서 IPv6으로 변환됩니다.

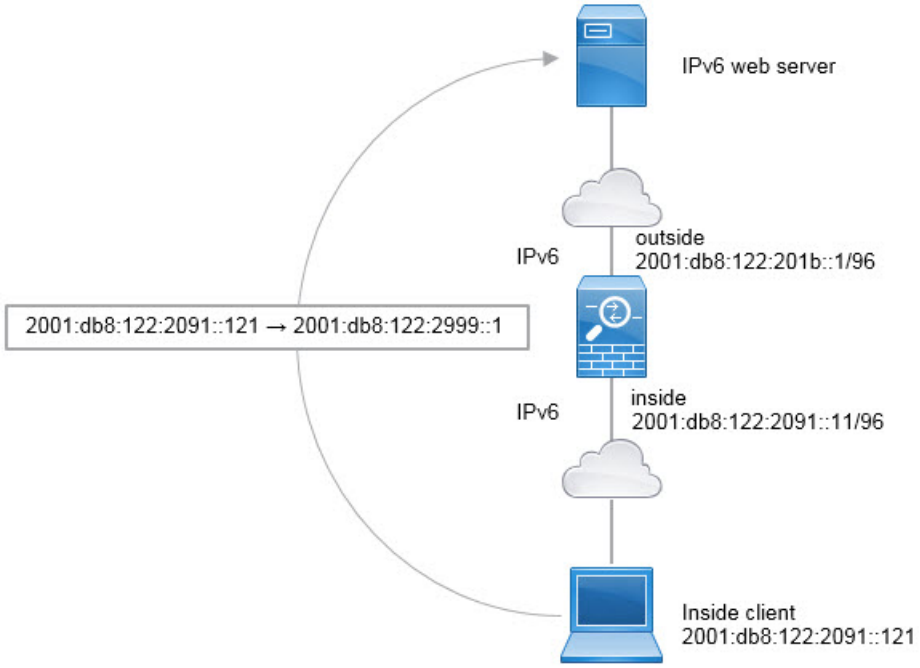
NAT66: IPv6 주소를 다른 IPv6 주소로 변환

IPv6 네트워크 간을 이동할 때는 주소를 외부 네트워크의 다른 IPv6 주소로 변환할 수 있습니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

서로 다른 주소 유형 간을 변환하는 것이 아니므로 NAT66 변환을 위한 규칙 하나만 있으면 됩니다. 자동 NAT를 사용하면 이러한 규칙을 쉽게 모델링할 수 있습니다. 그러나 반환 트래픽을 허용하지 않으려면 수동 NAT만 사용해 정적 NAT 규칙을 단방향으로 설정할 수 있습니다.

NAT66 예, 네트워크 간의 고정 변환

자동 NAT를 사용하여 IPv6 주소 풀 간의 고정 변환을 컨피그레이션할 수 있습니다. 다음 예에서는 2001:db8:122:2091::/96 네트워크의 내부 주소를 2001:db8:122:2999::/96 네트워크의 외부 주소로 변환하는 방법을 설명합니다.



시작하기 전에

디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

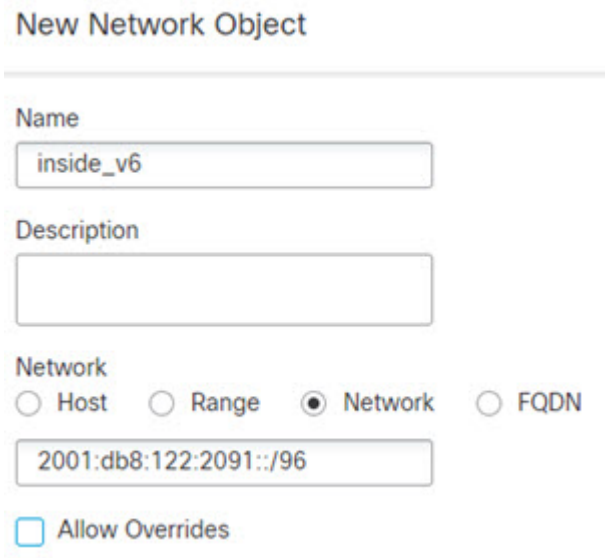
단계 **1** 내부 IPv6 및 외부 IPv6 NAT 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.

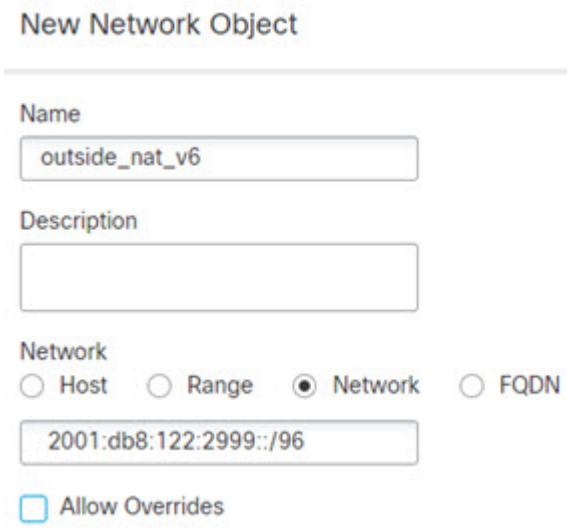
네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 외부 IPv6 NAT 네트워크를 정의합니다.

네트워크 개체의 이름을 outside_nat_v6과 같이 지정하고 네트워크 주소 2001:db8:122:2999::/96을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 IPv6 네트워크용 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.

- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = outside_nat_v6 네트워크 개체.

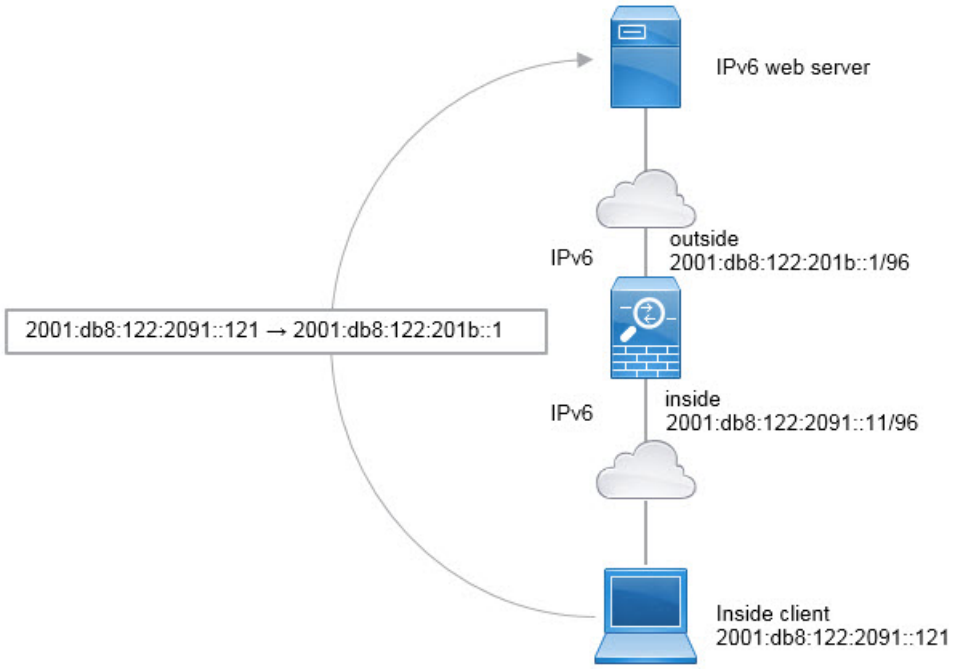
f) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 2001:db8:122:2999::/96 네트워크의 주소로 고정 NAT66 변환됩니다.

NAT66 예, 간단한 IPv6 인터페이스 PAT

NAT66을 구현하는 단순한 방식은 내부 주소를 외부 인터페이스 IPv6 주소의 각기 다른 포트에 동적으로 할당하는 것입니다.

NAT66용 인터페이스 PAT 규칙을 구성할 때는 해당 인터페이스에 구성되어 있는 모든 글로벌 주소가 PAT 매핑에 사용됩니다. 인터페이스에 대한 링크-로컬 또는 사이트-로컬 주소는 PAT에 사용되지 않습니다.



시작하기 전에

디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

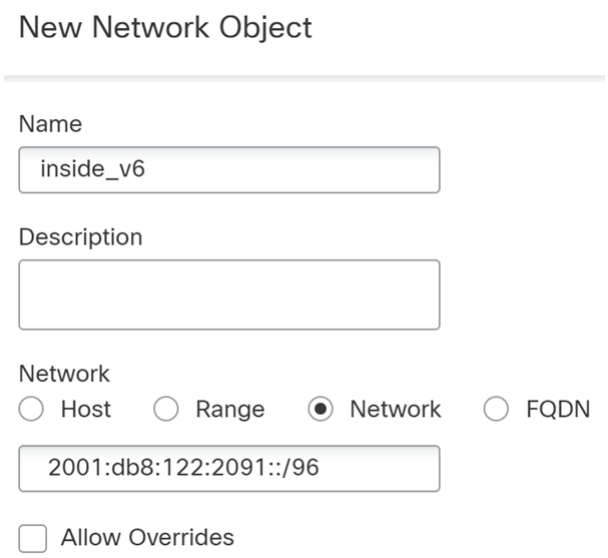
단계 **1** 내부 IPv6 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 IPv6 네트워크용 동적 PAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

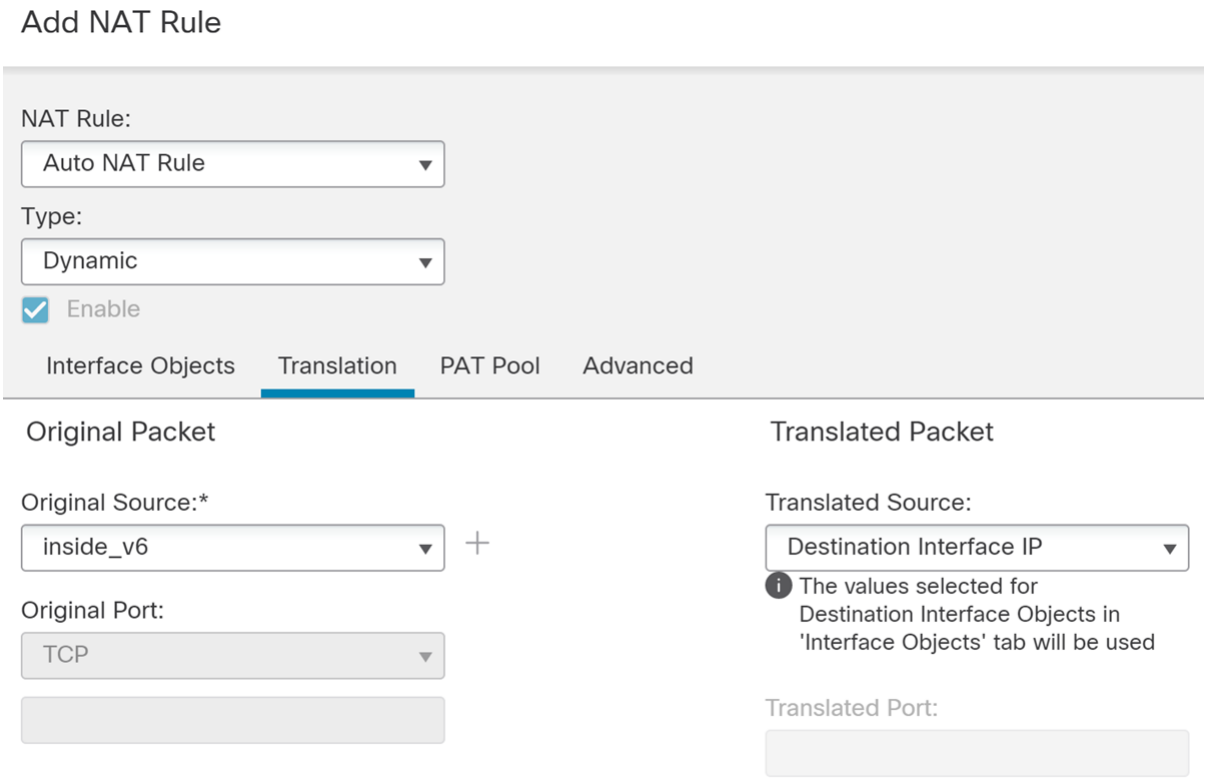
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
- **Translated Source(**변환된 소스**)** = **Destination Interface IP(**대상 인터페이스 **IP)**

f) **Advanced(**고급**)**에서 대상 인터페이스의 IPv6 주소가 사용되어야 함을 나타내는 **IPv6**를 선택합니다.



g) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 외부 인터페이스에 대해 구성된 IPv6 전역 주소를 사용하여 NAT66 PAT로 변환됩니다.

NAT 모니터링

NAT 연결을 모니터링하고 트러블슈팅하려면 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show nat** NAT 규칙 및 규칙별 적중 횟수를 표시합니다. NAT의 다른 측면을 표시하는 추가 키워드도 있습니다.
- **show xlate** 현재 활성 상태인 활성 NAT 변환을 표시합니다.
- **clear xlate** 활성 NAT 변환을 제거할 수 있습니다. NAT 규칙을 변경하는 경우에는 활성 변환을 제거해야 할 수 있습니다. 기존 연결은 종료될 때까지 이전 변환 슬롯을 계속 사용하기 때문입니다. 변환을 지우면 시스템에서 새 규칙을 기반으로 하여 클라이언트의 다음 연결 시도 시 클라이언트에 대한 새 변환을 작성할 수 있습니다.

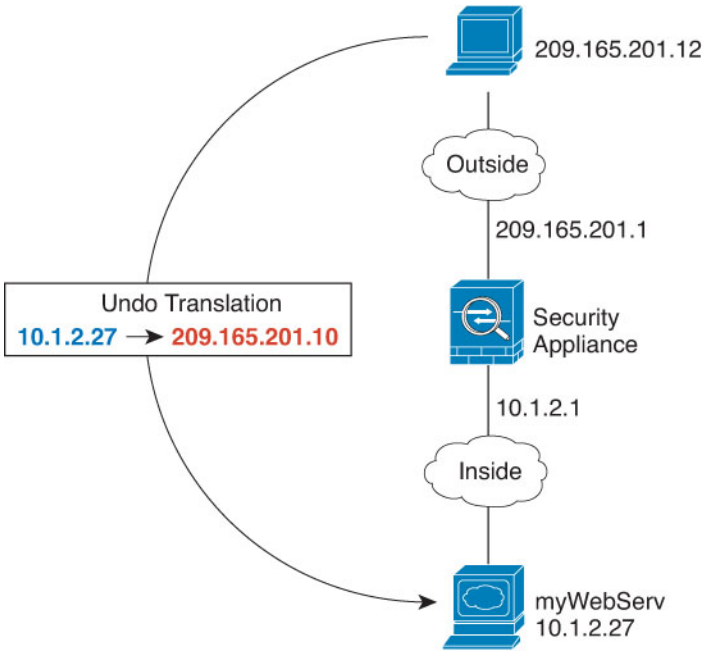
NAT의 예

다음 항목에서는 Threat Defense 디바이스에서 NAT를 구성하는 예를 제공합니다.

내부 웹 서버에 대한 액세스 제공(고정 자동 NAT)

다음 예는 내부 웹 서버에 대해 고정 NAT를 수행합니다. 실제 주소는 사설 네트워크에 있으므로 공용 주소가 필요합니다. 호스트가 고정된 주소에서 웹 서버에 대한 트래픽을 시작할 수 있으려면 고정 NAT가 필요합니다.

그림 ***60:*** 내부 웹 서버에 대한 고정 ***NAT***



시작하기 전에

웹 서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보

안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

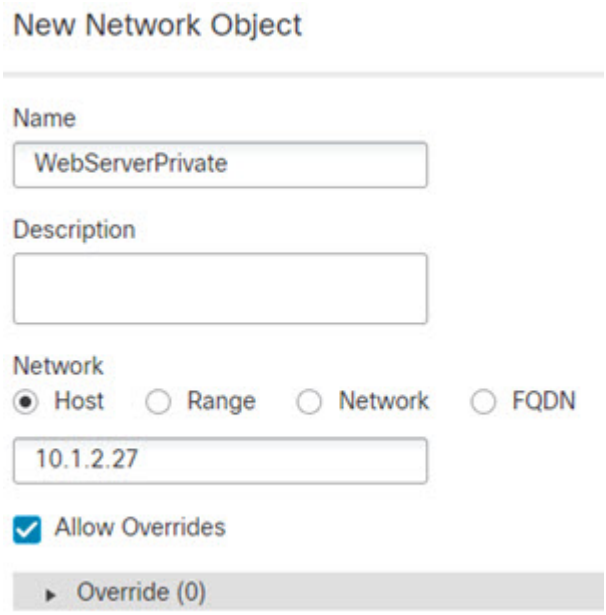
단계 **1** 서버의 전용 및 공용 호스트 주소를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 웹 서버의 전용 어드레스를 정의합니다.

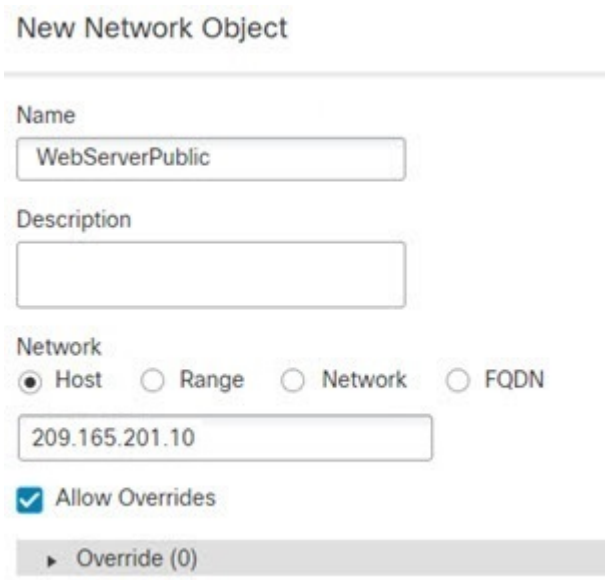
네트워크 개체의 이름을 WebServerPrivate과 같이 지정하고 실제 호스트 IP 주소 10.1.2.27을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 공용 주소를 정의합니다.

네트워크 개체의 이름을 WebServerPublic과 같이 지정하고 호스트 주소 209.165.201.10을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 개체용 고정 NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

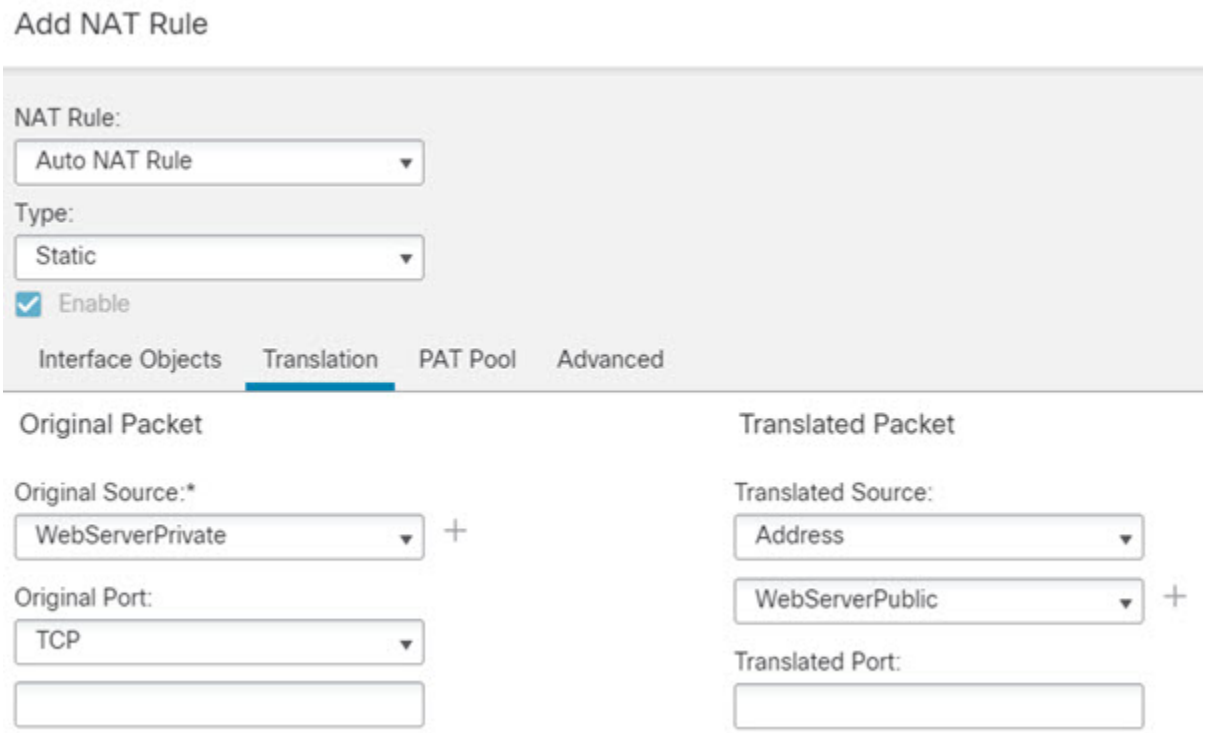
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- 원본 소스 = WebServerPrivate 네트워크 개체
- 변환된 소스 > 주소 = WebServerPublic 네트워크 개체



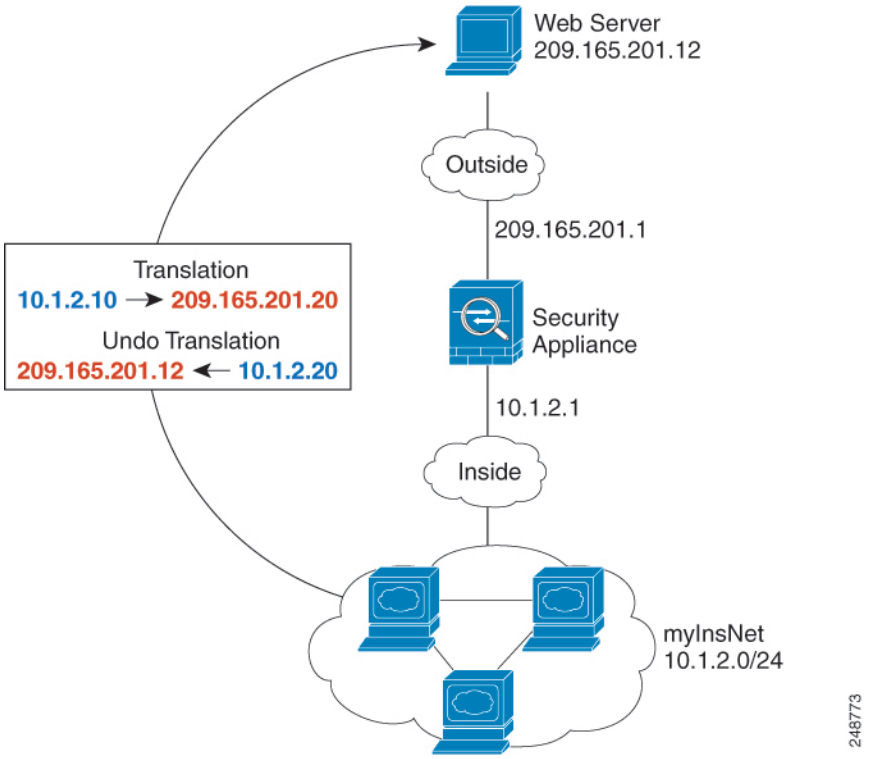
f) **Save(**저장**)**를 클릭합니다.

단계 **3** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

외부 웹 서버의 내부 호스트 및 고정 **NAT**에 대한 동적 자동 **NAT**

다음 예는 사설 네트워크의 내부 사용자가 외부에서 액세스하는 경우를 위한 동적 NAT를 구성합니다. 내부 사용자가 외부 웹 서버에 연결하는 경우도 포함됩니다. 이 경우 웹 서버 주소가 내부 네트워크에 있는 것처럼 보이는 주소로 변환됩니다.

그림 61: 내부용 동적 NAT, 외부 웹 서버용 고정 NAT



시작하기 전에

웹 서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

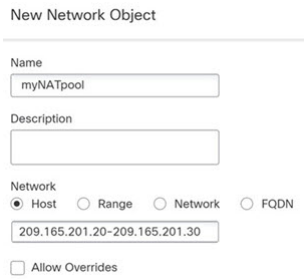
단계 **1** 내부 주소를 변환할 동적 NAT 풀용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 동적 NAT 풀을 정의합니다.

네트워크 개체의 이름을 지정하고(예: myNATpool) 네트워크 범위 209.165.201.20-209.165.201.30을 입력합니다.

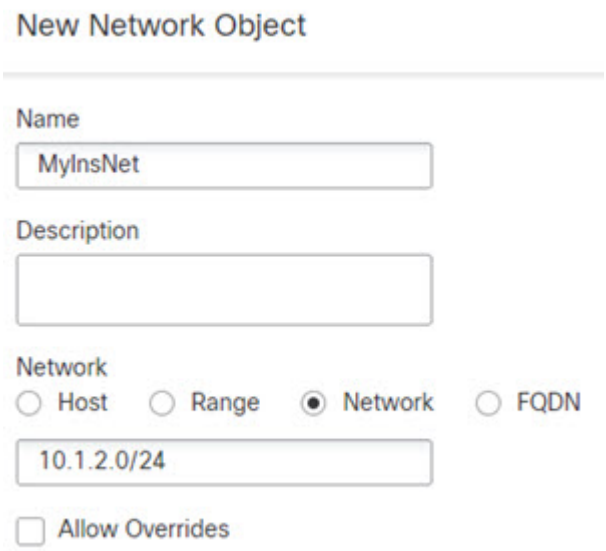


d) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 MyInsNet과 같이 지정하고 네트워크 주소 10.1.2.0/24를 입력합니다.

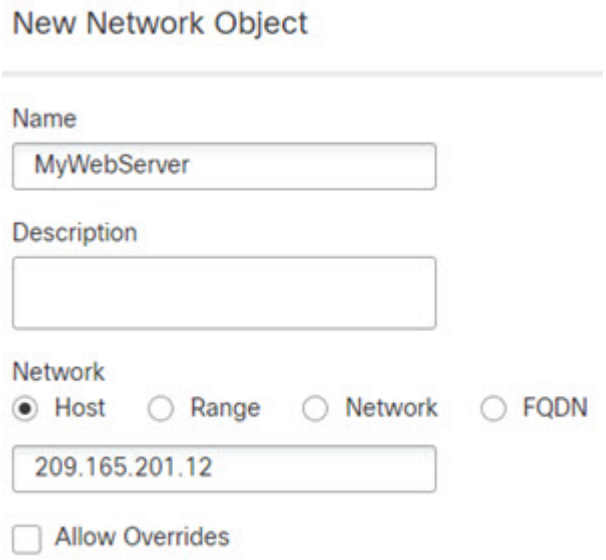


c) **Save(**저장**)**를 클릭합니다.

단계 **3** 외부 웹 서버용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 MyWebServer와 같이 지정하고 호스트 주소 209.165.201.12를 입력합니다.

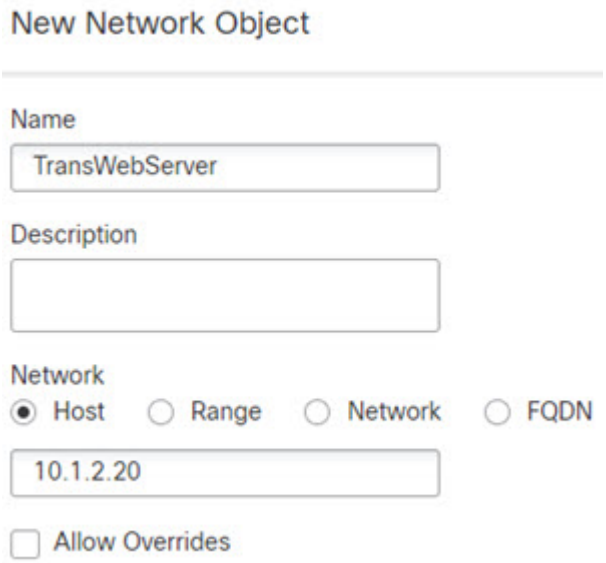


c) **Save(**저장**)**를 클릭합니다.

단계 **4** 변환된 웹 서버 주소용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 TransWebServer와 같이 지정하고 호스트 주소 10.1.2.20을 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **5** 동적 NAT 풀 개체를 사용하여 내부 네트워크용 동적 NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

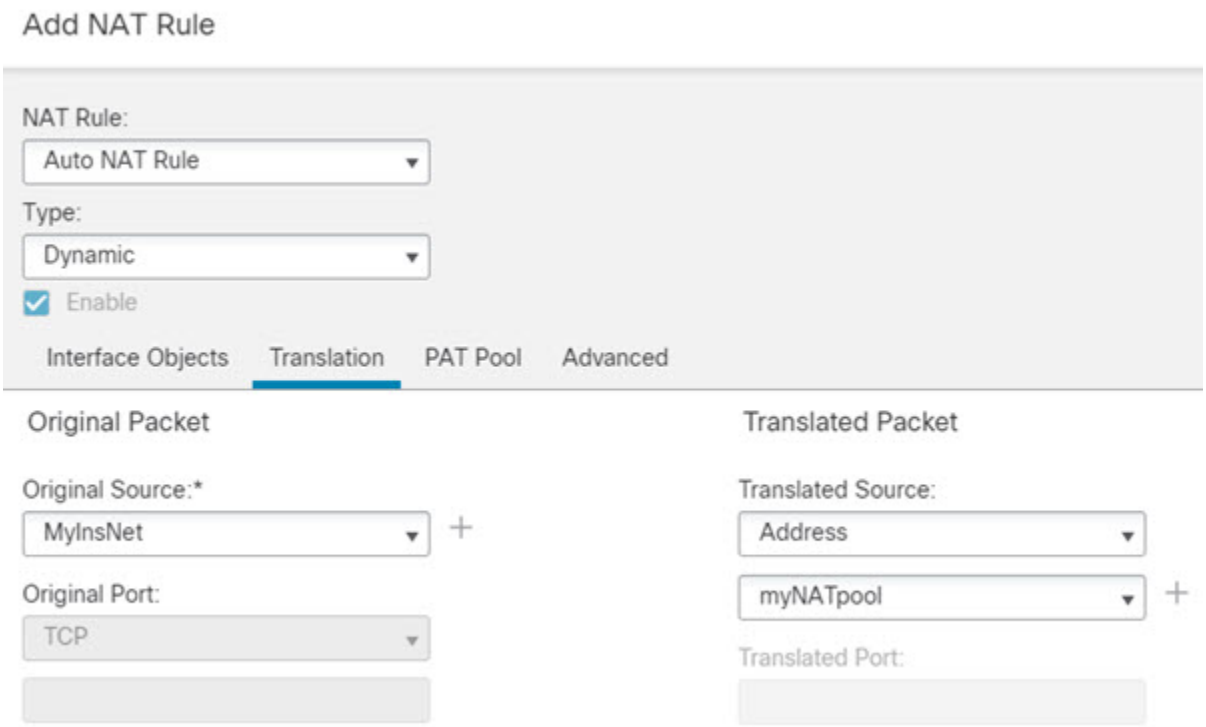
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsNet 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = myNATpool 네트워크 그룹입니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **6** 웹 서버용 고정 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

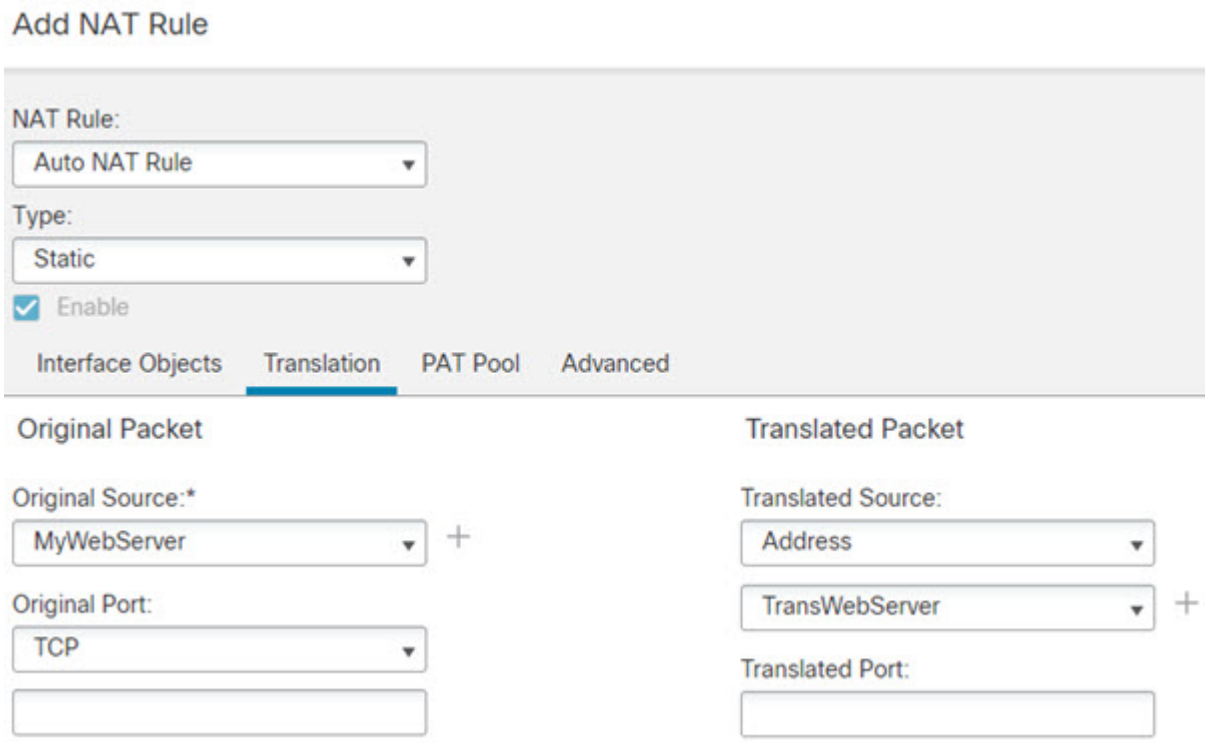
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myWebServer 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = TransWebServer 네트워크 개체.



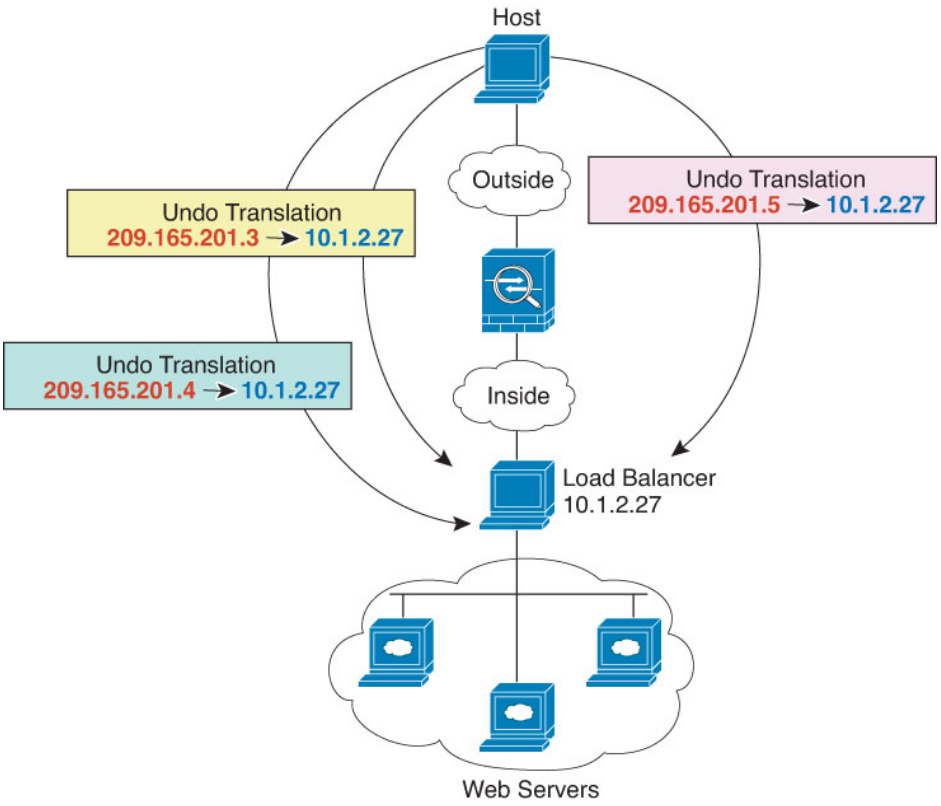
e) **Save(**저장**)**를 클릭합니다.

단계 **7** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

여러 매핑된 주소가 있는 내부 로드 밸런서(고정 자동 NAT, 일대다)

다음 예는 여러 IP 주소로 변환되는 내부 로드 밸런서를 보여줍니다. 외부 호스트가 매핑된 IP 주소 중 하나에 액세스하는 경우 단일 로드 밸런서 주소로 변환되지 않습니다. 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다.

그림 62: 내부 로드 밸런서용 일대다 고정 NAT



시작하기 전에

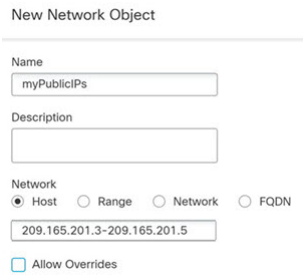
웹 서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 로드 밸런서를 매핑하려는 주소용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) Define the addresses.

네트워크 개체의 이름을 지정하고(예: myPublicIPs) 네트워크 범위 209.165.201.3-209.165.201.5를 입력합니다.

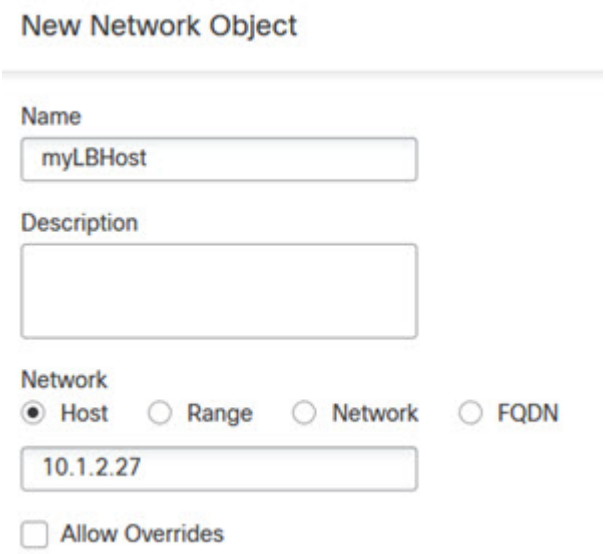


d) **Save(**저장**)**를 클릭합니다.

단계 **2** 로드 밸런서용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 myLBHost와 같이 지정하고 호스트 주소 10.1.2.27을 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **3** 로드 밸런서용 고정(static) NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

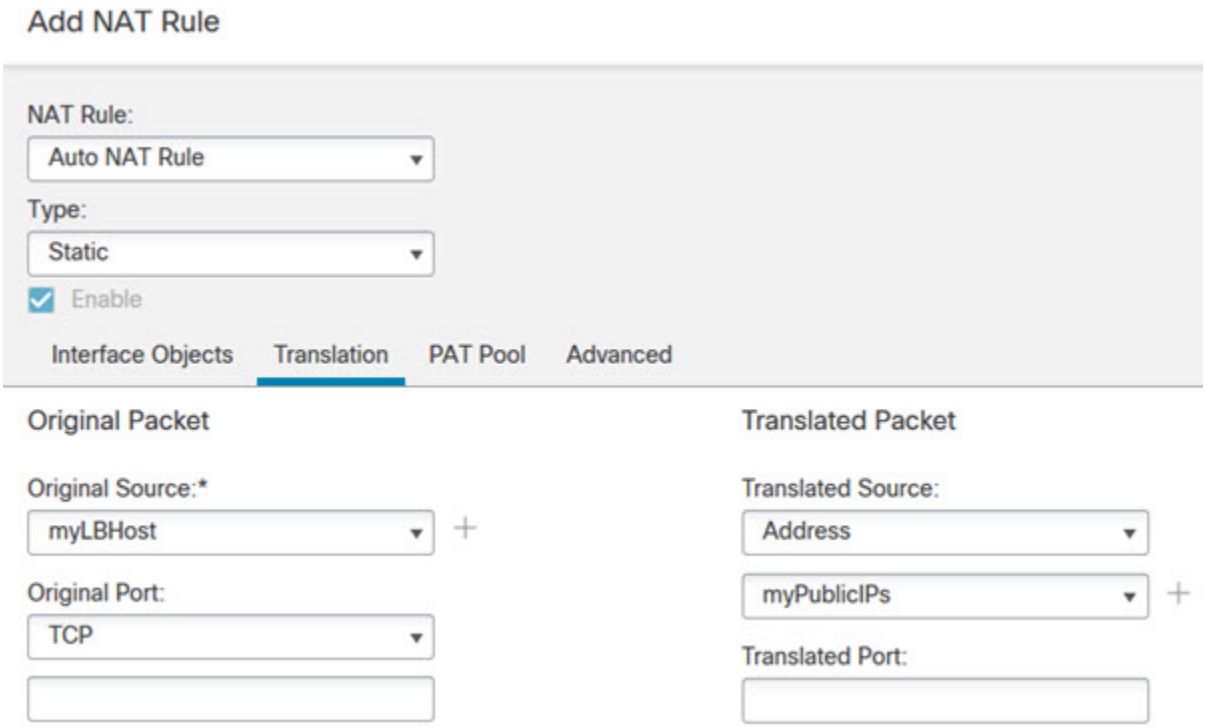
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myLBHost 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = myPublicIPs 네트워크 그룹.



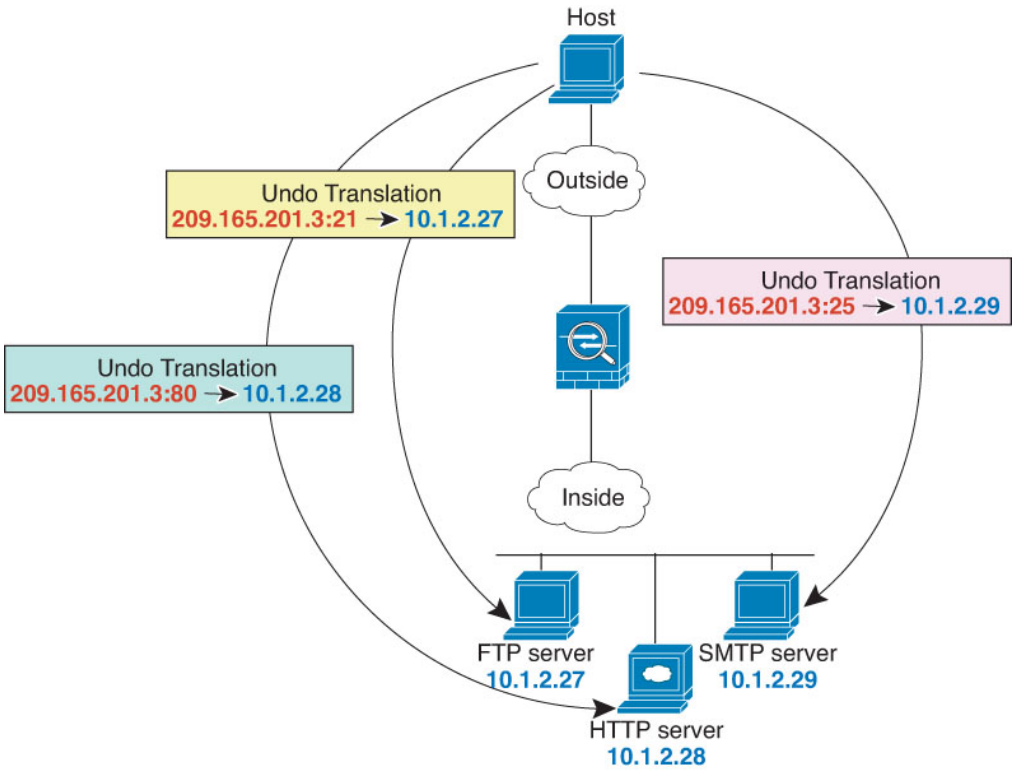
f) **Save(**저장**)**를 클릭합니다.

단계 **4** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

FTP, HTTP 및 SMTP용 단일 주소(포트 변환 고정 자동 NAT)

다음과 같은 포트 변환 고정 NAT의 예는 원격 사용자가 FTP, HTTP 및 SMTP에 액세스하기 위해 사용할 단일 주소를 제공합니다. 이러한 서버는 실제 네트워크에서 실제로 서로 다른 디바이스이지만, 각 서버에 대해 동일하게 매핑된 IP 주소를 사용하되 포트는 다른 포트 변환 고정 NAT 규칙을 지정할 수 있습니다.

그림 *63:* 포트 변환 고정 *NAT*



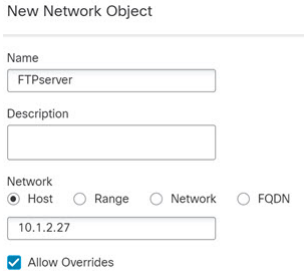
시작하기 전에

서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** FTP 서버용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 네트워크 개체의 이름을 FTPserver와 같이 지정하고 FTP 서버의 실제 IP 주소 10.1.2.27을 입력합니다.

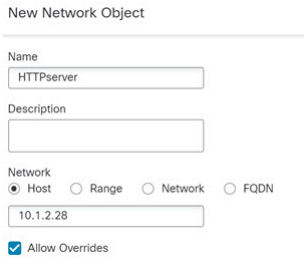


d) **Save(**저장**)**를 클릭합니다.

단계 **2** HTTP 서버용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 HTTPserver와 같이 지정하고 호스트 주소 10.1.2.28을 입력합니다.

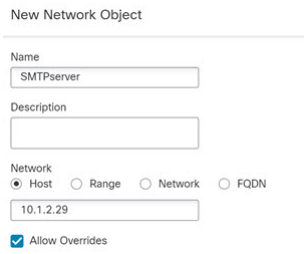


c) **Save(**저장**)**를 클릭합니다.

단계 **3** SMTP 서버용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 SMTPserver와 같이 지정하고 호스트 주소 10.1.2.29를 입력합니다.

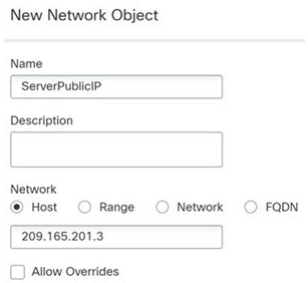


c) **Save(**저장**)**를 클릭합니다.

단계 **4** 서버 3대에 사용되는 공용 IP 주소용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 ServerPublicIP와 같이 지정하고 호스트 주소 209.165.201.3을 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **5** FTP 포트를 자기 자신에 매핑하는 FTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

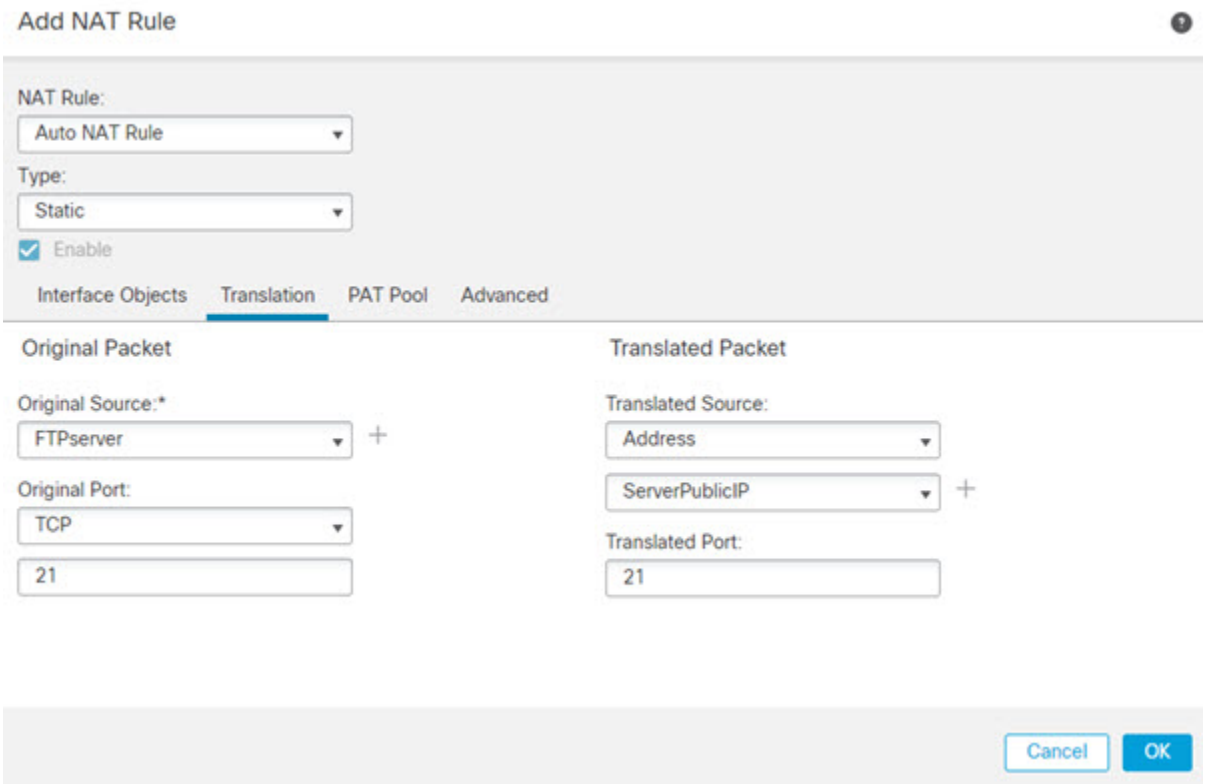
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = FTPserver 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ServerPublicIP 네트워크 개체.
- **Original Port(**원본 포트**)** > **TCP** = 21.
- **Translated Port(**변환된 포트**)** = 21.



f) **Save(**저장**)**를 클릭합니다.

단계 **6** HTTP 포트를 자기 자신에 매핑하는 HTTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

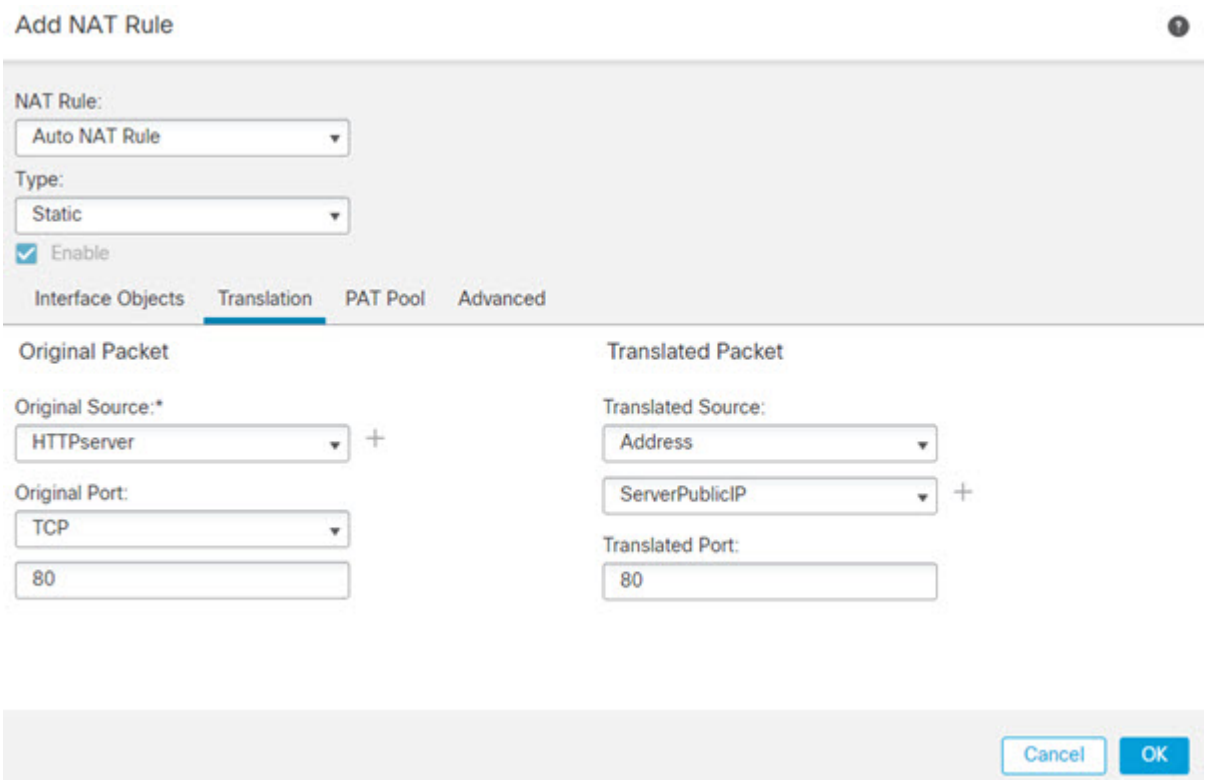
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = HTTPserver 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ServerPublicIP 네트워크 개체.
- **Original Port(**원본 포트**)** > **TCP** = 80.
- **Translated Port(**변환된 포트**)** = 80.



e) **Save(**저장**)**를 클릭합니다.

단계 **7** SMTP 포트를 자기 자신에 매핑하는 SMTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

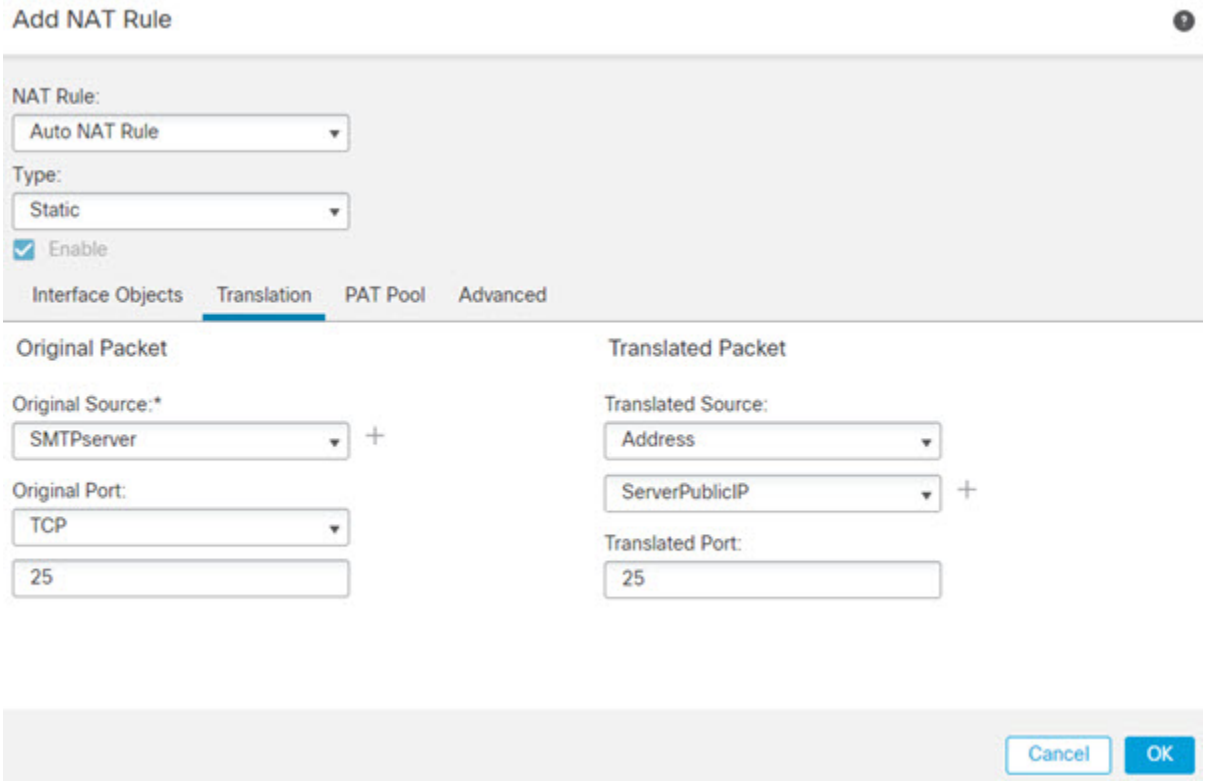
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = SMTPserver 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ServerPublicIP 네트워크 개체.
- **Original Port(**원본 포트**)** > **TCP** = 25.
- **Translated Port(**변환된 포트**)** = 25.



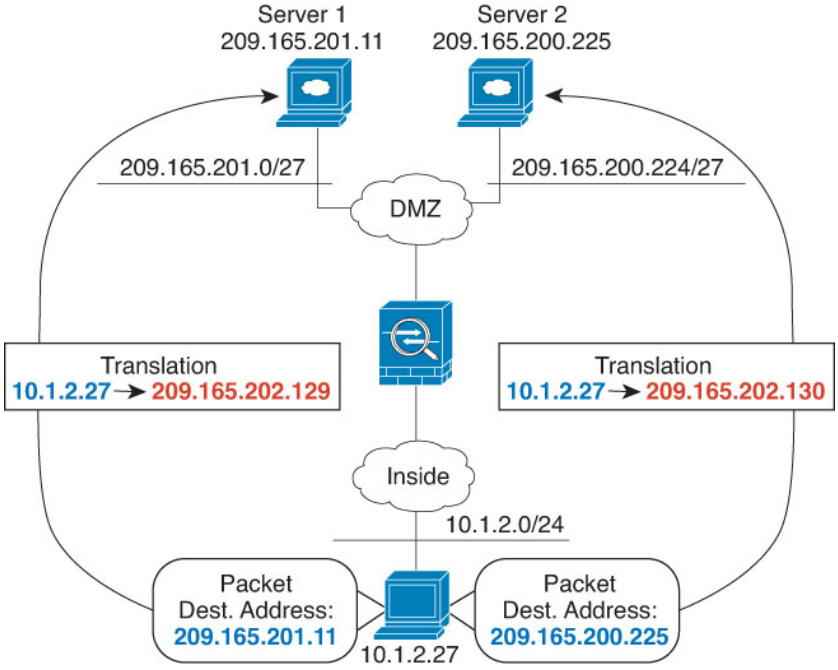
e) **Save(**저장**)**를 클릭합니다.

단계 **8** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

대상에 따라 다른 변환(동적 수동 **PAT)**

다음 그림은 두 개의 서로 다른 서버에 액세스하는 10.1.2.0/24 네트워크의 호스트를 보여줍니다. 호스트가 209.165.201.11의 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 209.165.200.225의 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

그림 *64:* 서로 다른 대상 주소를 사용하는 수동 *NAT*



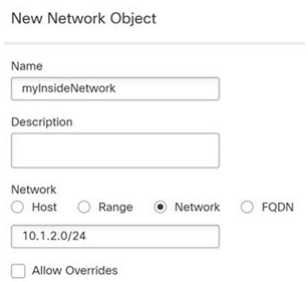
시작하기 전에

서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **dmz**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 실제 네트워크 주소 10.1.2.0/24를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

단계 **2** DMZ 네트워크 1용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

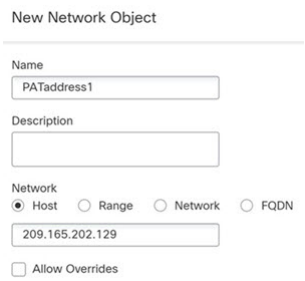
b) 네트워크 개체의 이름을 DMZnetwork1과 같이 지정하고 네트워크 주소 209.165.201.0/27(서브넷 마스크 255.255.255.224)을 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **3** DMZ 네트워크 1용 PAT 주소의 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 호스트 주소 209.165.202.129를 입력합니다.

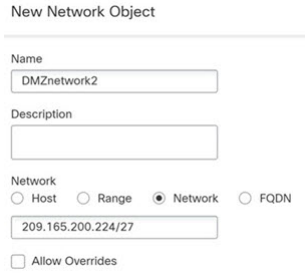


c) **Save(**저장**)**를 클릭합니다.

단계 **4** DMZ 네트워크 2용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 DMZnetwork2와 같이 지정하고 네트워크 주소 209.165.200.224/27(서브넷 마스크 255.255.255.224)을 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **5** DMZ 네트워크 2용 PAT 주소의 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 호스트 주소 209.165.202.130을 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **6** DMZ 네트워크 1용 동적 수동 PAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

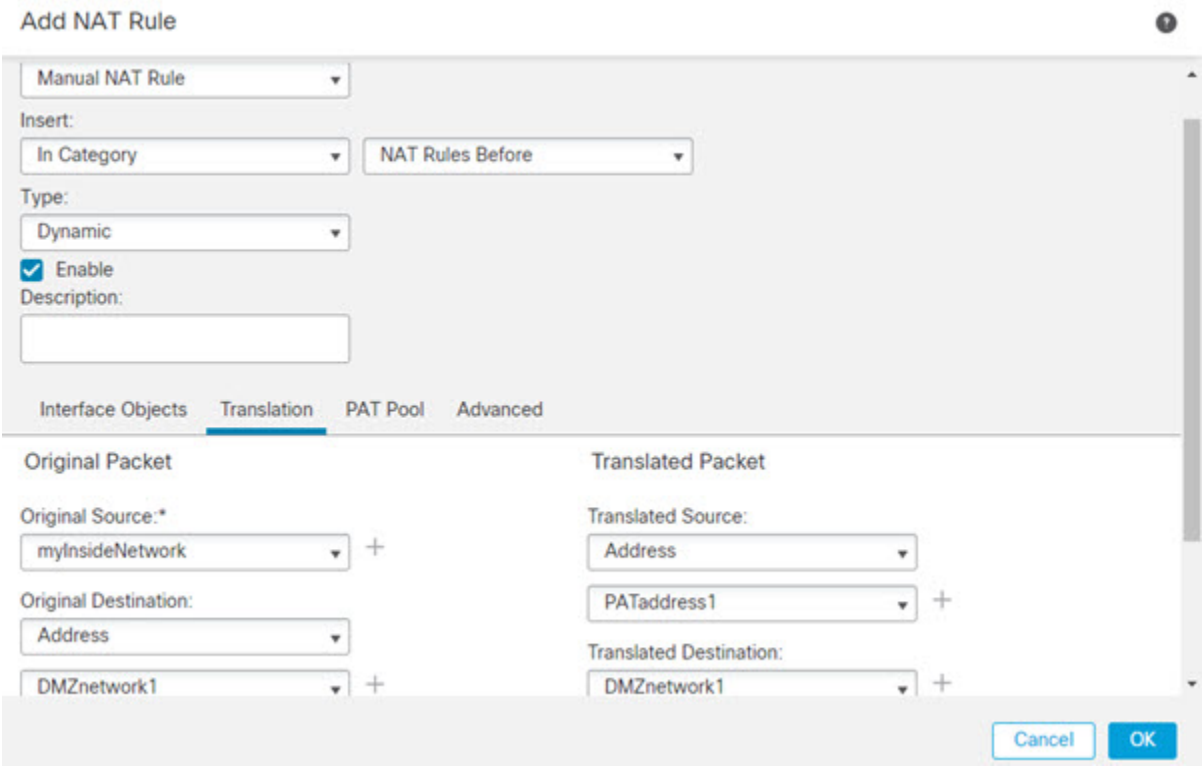
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress1 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = DMZnetwork1 네트워크 개체.
- **Translated Destination(**변환된 대상**)** = DMZnetwork1 네트워크 개체.

참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **7** DMZ 네트워크 2용 동적 수동 PAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

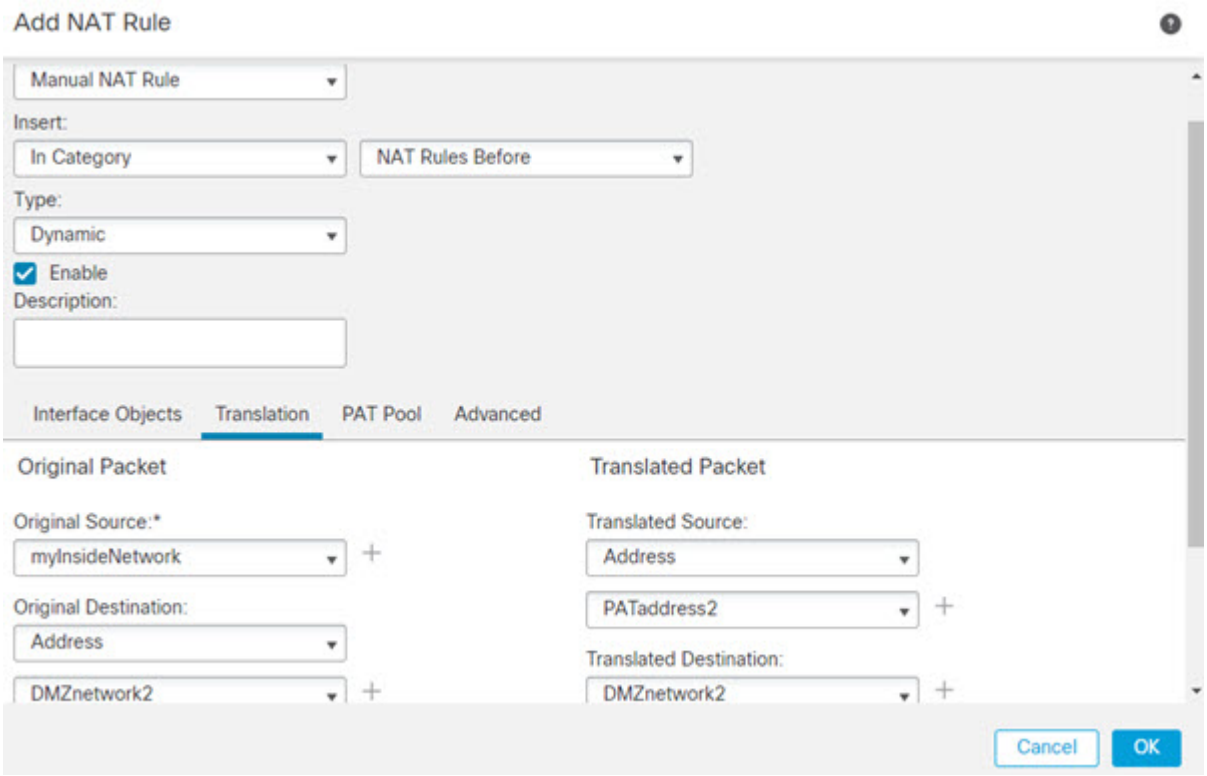
c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress2 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = DMZnetwork2 네트워크 개체.

• **Translated Destination(**변환된 대상**)** = DMZnetwork2 네트워크 개체.



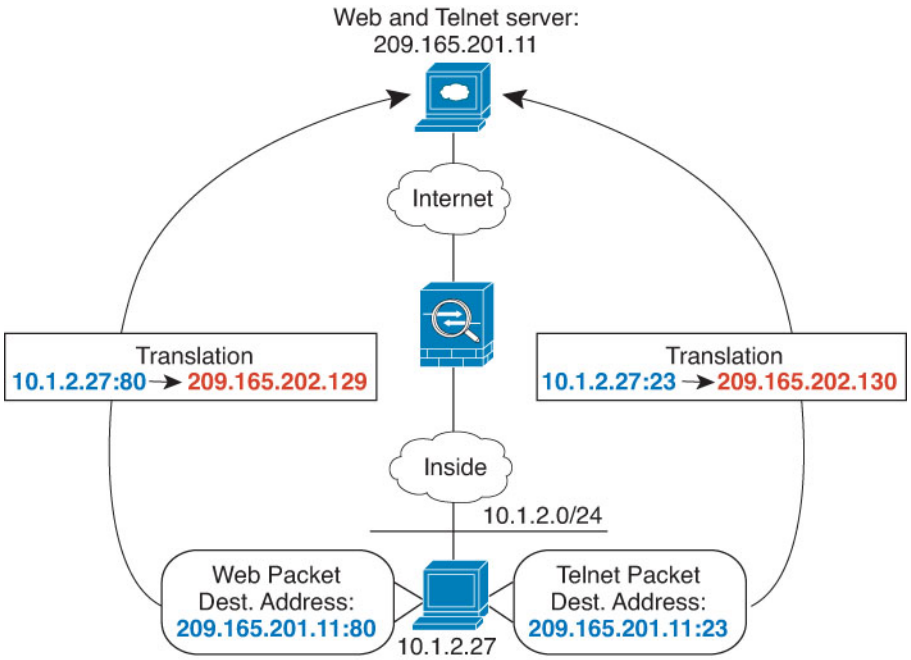
e) **Save(**저장**)**를 클릭합니다.

단계 **8** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

대상 주소 및 포트에 따라 다른 변환(동적 수동 **PAT)**

다음 그림은 소스 포트와 대상 포트의 사용법을 보여줍니다. 10.1.2.0/24 네트워크의 호스트가 웹 서비스와 텔넷 서비스를 모두 제공하는 단일 호스트에 액세스합니다. 호스트가 텔넷 서비스용 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 동일한 웹 서비스용 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

그림 *65:* 서로 다른 대상 포트를 사용하는 수동 *NAT*



시작하기 전에

서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **dmz**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

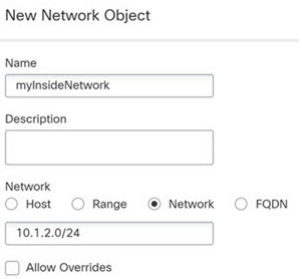
프로시저

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 실제 네트워크 주소 10.1.2.0/24를 입력합니다.

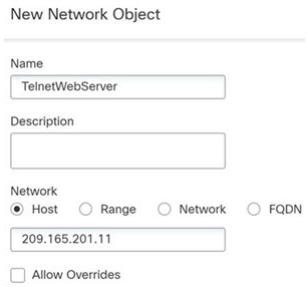


d) **Save(**저장**)**를 클릭합니다.

단계 **2** 텔넷/웹 서버용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 TelnetWebServer와 같이 지정하고 호스트 주소 209.165.201.11을 입력합니다.

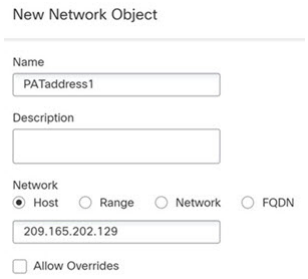


c) **Save(**저장**)**를 클릭합니다.

단계 **3** 텔넷 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 호스트 주소 209.165.202.129를 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **4** HTTP 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 호스트 주소 209.165.202.130을 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **5** 텔넷 액세스용 동적 수동 PAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.
b) **Add Rule(**규칙 추가**)**을 클릭합니다.
c) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

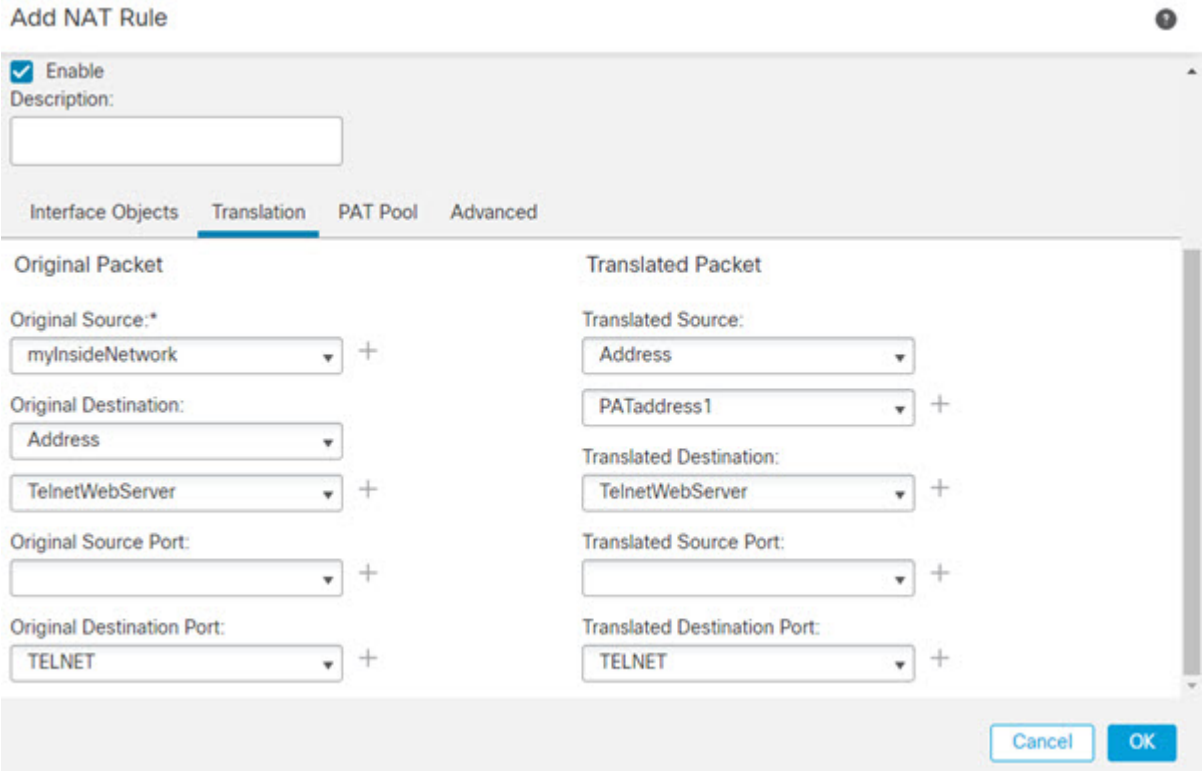
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress1 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = TelnetWebServer 네트워크 개체.
- **Translated Destination(**변환된 대상**)** = TelnetWebServer 네트워크 개체.
- **Original Destination Port(**원본 대상 포트**)** = TELNET 포트 개체(시스템 정의)
- **Translated Destination Port(**변환된 대상 포트**)** = TELNET 포트 개체(시스템 정의)

참고 대상 주소 또는 포트를 변환하지 않을 것이기 때문에 원본 및 변환된 대상 주소에 대해 동일한 주소를 지정하고 원본 및 변환된 포트에 대해 동일한 포트를 지정하여, 대상 주소 또는 포트에 대한 ID NAT를 구성해야 합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **6** 웹 액세스용 동적 수동 PAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

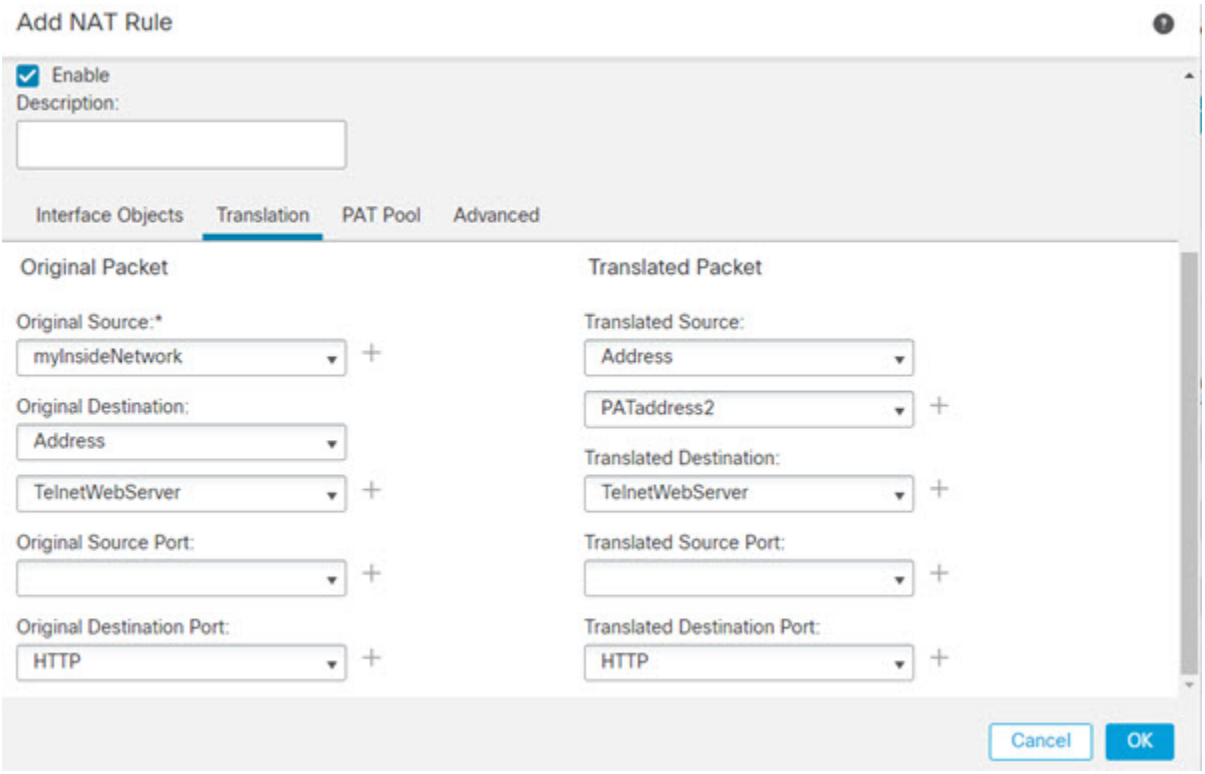
c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress2 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = TelnetWebServer 네트워크 개체.
- **Translated Destination(**변환된 대상**)** = TelnetWebServer 네트워크 개체.
- **Original Destination Port(**원본 대상 포트**)** = HTTP 포트 개체(시스템 정의)

• **Translated Destination Port(**변환된 대상 포트**)** = HTTP 포트 개체(시스템 정의)



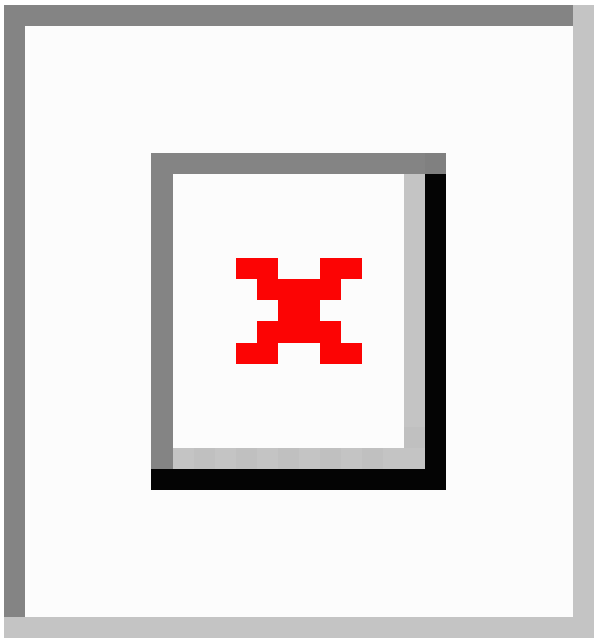
e) **Save(**저장**)**를 클릭합니다.

단계 **7** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

NAT 및 사이트 대 사이트 VPN

다음 그림은 볼더 사무실과 산호세 사무실을 연결하는 사이트 대 사이트 터널을 보여줍니다. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래의 예에서는 인터페이스 PAT 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 단순히 주소를 동일한 주소로 변환합니다.

그림 *66:* 사이트 대 사이트 *VPN*을 위한 인터페이스 *PAT* 및 *ID NAT*



다음 예에서는 방화벽1(볼더)의 구성에 대해 설명합니다.

시작하기 전에

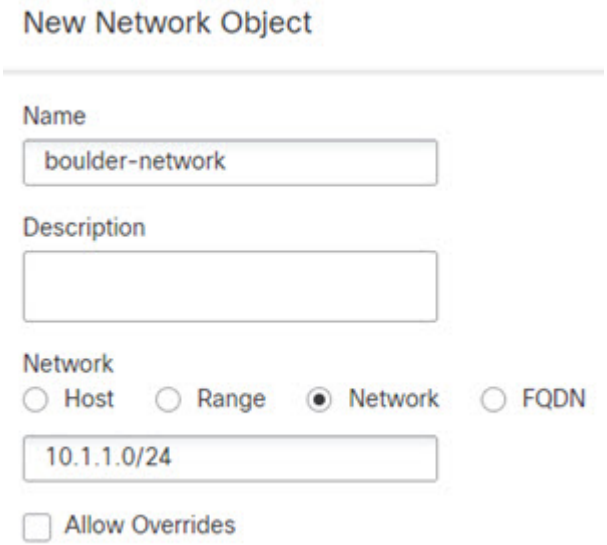
VPN의 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 Firewall1(Boulder) 인터페이스에 대한 **inside-boulder** 및 **outside-boulder**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interfaces(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 볼더 내부 네트워크를 확인합니다.

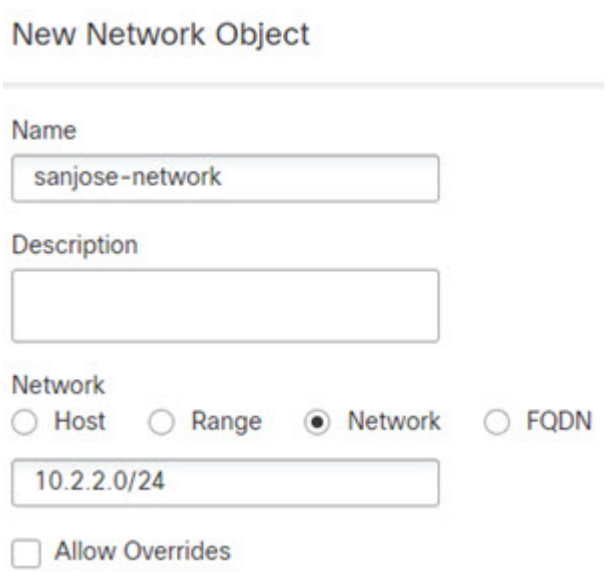
네트워크 개체의 이름을 boulder-network와 같이 지정하고 네트워크 주소 10.1.1.0/24를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 내부 San Jose 네트워크를 정의합니다.

네트워크 개체의 이름을 sanjose-network와 같이 지정하고 네트워크 주소 10.2.2.0/24를 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

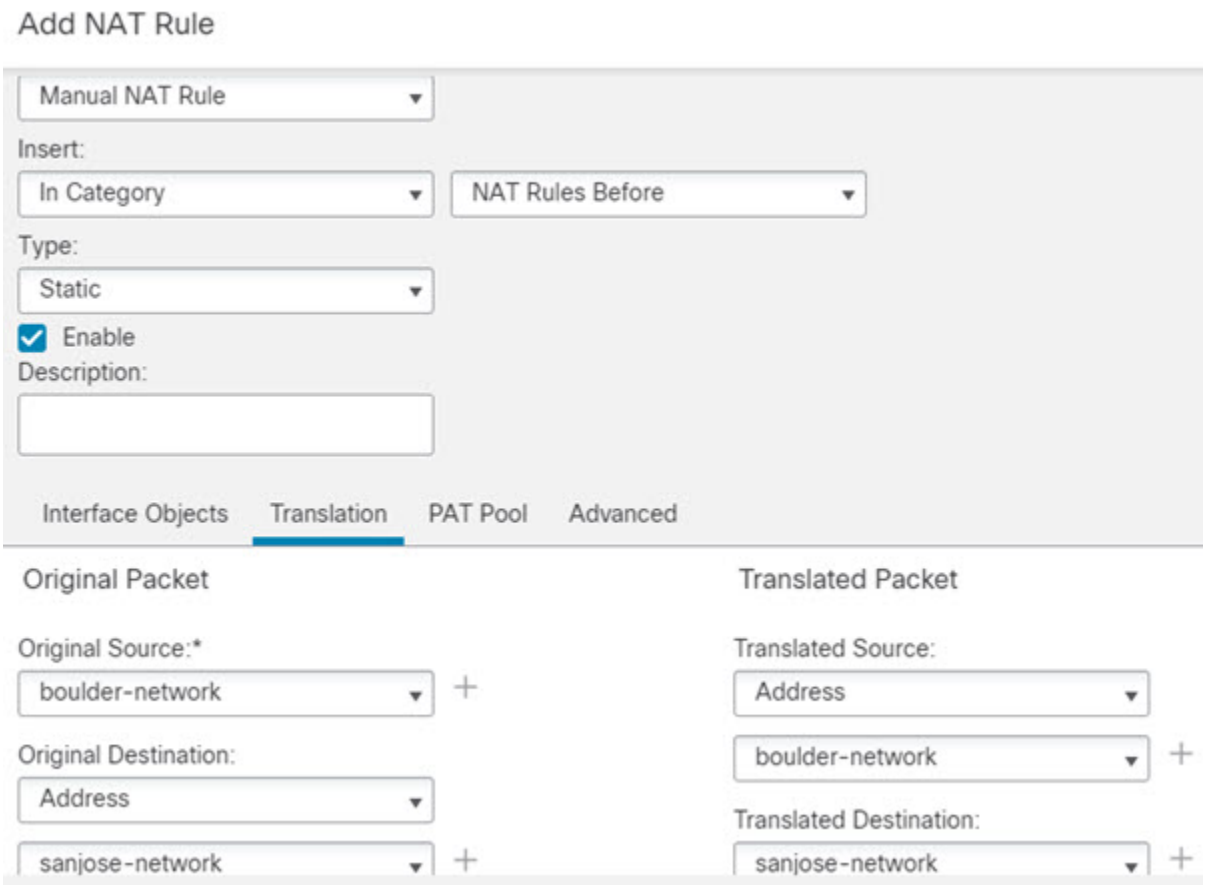
- **Source Interface Objects(**소스 인터페이스 개체**)** = inside-boulder.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside-boulder.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = boulder-network 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = boulder-network 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = sanjose-network 개체.
- **Translated Destination(**변환된 대상**)** = sanjose-network 개체.

  참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.

f) **Advanced(**고급**)**에서 **Do not proxy ARP on Destination interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)**를 선택합니다.



g) **Save(**저장**)**를 클릭합니다.

단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

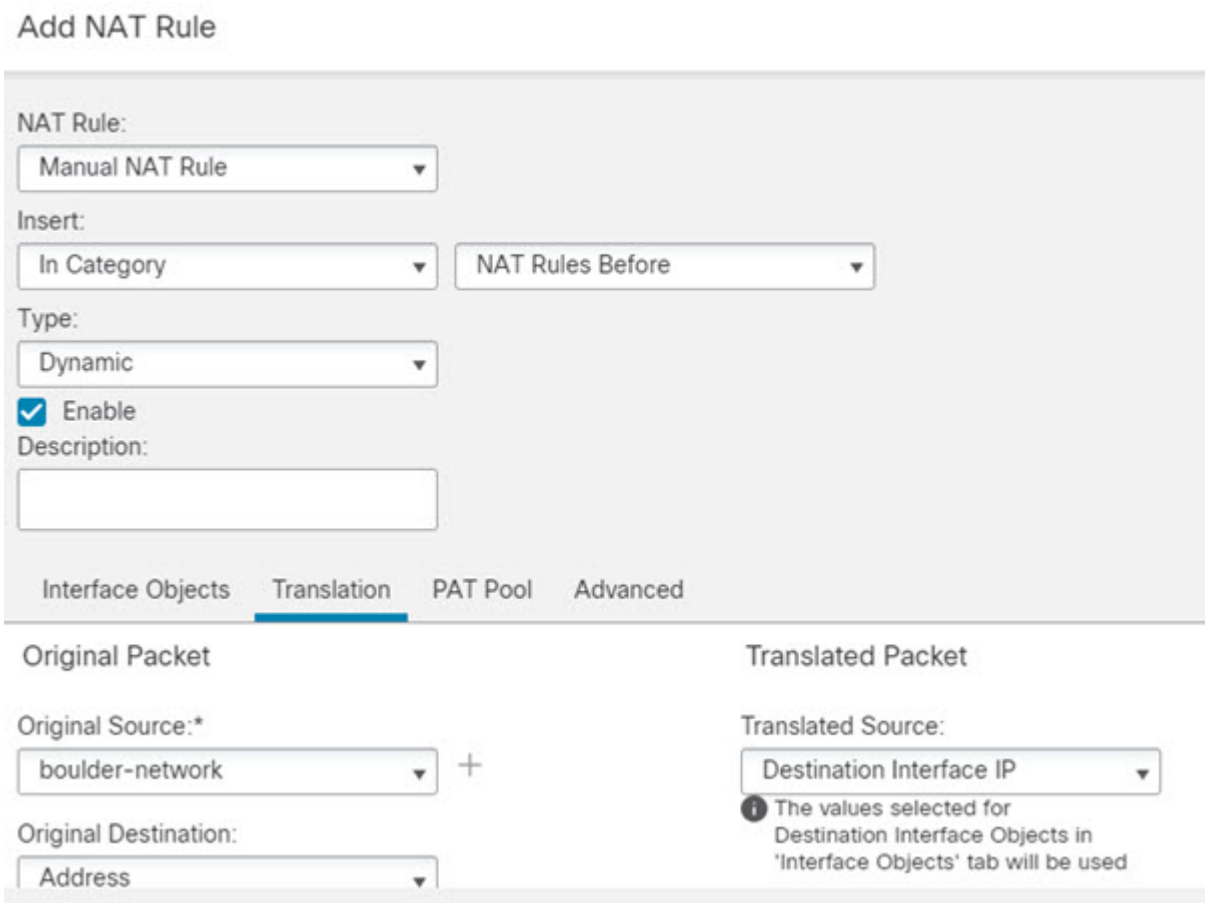
- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적
- **Insert Rule(**규칙 삽입**)** = 첫 번째 규칙 뒤의 모든 위치. 이 규칙은 모든 대상 주소에 적용되므로 sanjose-network를 대상으로 사용하는 규칙이 이 규칙 앞에 와야 합니다. 그렇지 않으면 sanjose-network 규칙은 어떤 주소와도 일치하지 않게 됩니다. 기본적으로는 "자동 NAT 앞의 NAT 규칙" 섹션 끝에 새 수동 NAT 규칙을 배치합니다.

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside-boulder.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside-boulder.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = boulder-network 개체.
- **Translated Source(**변환된 소스**)** = **Destination Interface IP(**대상 인터페이스 **IP)** 이 옵션은 대상 인터페이스 개체에 포함된 인터페이스를 사용하여 인터페이스 PAT를 구성합니다.
- **Original Destination(**원본 대상**)** > **Address** = 임의(빈 상태로 유지).
- **Translated Destination(**변환된 대상**)** = 임의(빈 상태로 유지).



e) **Save(**저장**)**를 클릭합니다.

단계 **4** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

NAT를 사용하여 DNS 쿼리 및 응답 재작성

회신의 주소를 NAT 구성과 일치하는 주소로 교체하여 DNS 회신을 수정하도록 Firepower Threat Defense 디바이스를 구성해야 할 수 있습니다. 각 변환 규칙을 구성할 때 DNS 수정을 구성할 수 있습니다. DNS 수정은 DNS Doctoring이라고도 합니다.

이 기능은 NAT 규칙과 일치하는 DNS 쿼리 및 회신의 주소를 재작성합니다(예: IPv4의 A 레코드, IPv6의 AAAA 레코드 또는 역방향 DNS 쿼리의 PTR 레코드). 매핑된 인터페이스에서 다른 임의의 인터페이스로 이동하는 DNS 회신의 경우 매핑된 값에서 실제 값으로 레코드가 재작성됩니다. 반대로, 임의의 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 회신의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 기능은 NAT44, NAT 66, NAT46 및 NAT64에서 작동합니다.

다음은 NAT 규칙에 DNS 재작성을 구성해야 하는 몇 가지 주요 상황입니다.

- 규칙이 NAT64 또는 NAT46이며 DNS 서버가 외부 네트워크에 있는 경우. DNS A 레코드(IPv4의 경우)를 AAAA 레코드(IPv6의 경우)로 변환하려면 DNS 재작성이 필요합니다.
- DNS 서버가 외부에 있고 클라이언트는 내부에 있으며 클라이언트가 사용하는 일부 FQDN(Fully Qualified Domain Name)이 다른 내부 호스트로 확인되는 경우.
- DNS 서버가 내부에 있고 프라이빗 IP 어드레스로 응답하며, 클라이언트는 외부에 있고 내부에서 호스팅되는 서버를 가리키는 FQDN(Fully Qualified Domain Name)에 액세스하는 경우.

DNS 재작성 제한

다음은 DNS 재작성의 몇 가지 제한 사항입니다.

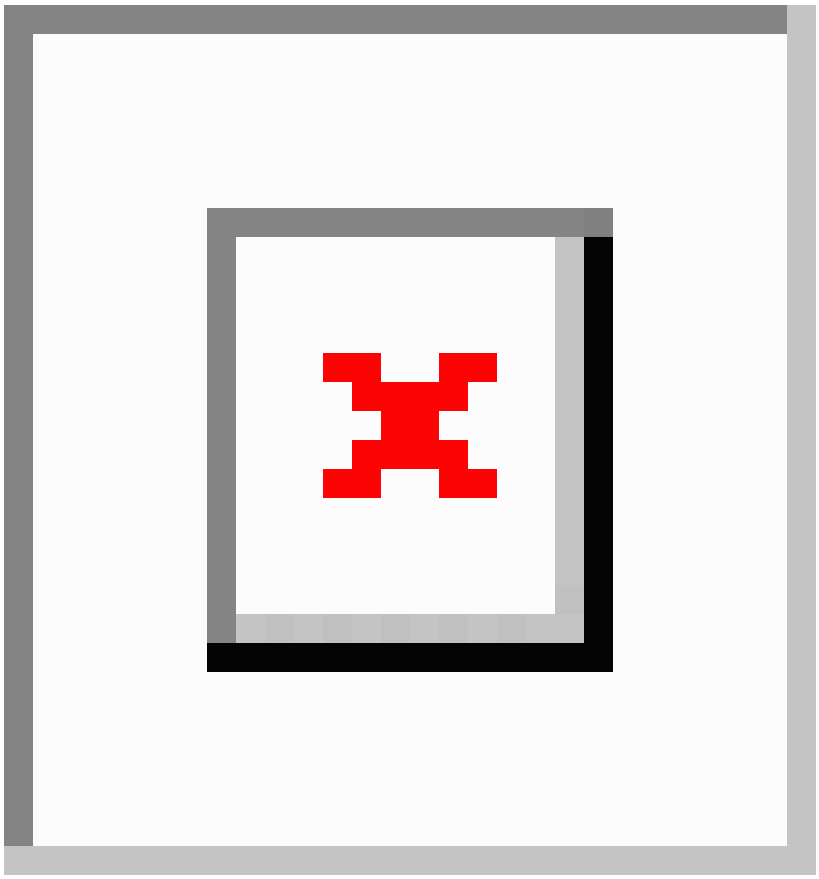
- 각 A 또는 AAAA 레코드에 여러 PAT 규칙을 적용할 수 있으며 사용할 PAT 규칙이 모호하므로 PAT에는 DNS 재작성이 적용되지 않습니다.
- 수동 NAT 규칙을 구성할 때 소스 주소와 대상 주소를 모두 지정하는 경우에는 DNS 수정을 구성할 수 없습니다. A와 B를 비교하여 전송하는 경우 이러한 종류의 규칙에는 잠재적으로 단일 주소에 다른 변환이 있을 수 있습니다. 따라서 이는 DNS 회신 내부의 IP 주소를 정확한 2회 NAT 규칙에 대해 올바르게 확인할 수 없습니다. DNS 회신에는 DNS 요청을 표시한 패킷에 어떤 source/destination 주소 조합이 있었는지에 대한 정보가 포함되어 있지 않습니다.
- DNS 쿼리 및 응답을 재작성하려면 NAT 규칙에 대해 DNS NAT 재작성을 활성화하여 DNS 애플리케이션 검사를 활성화해야 합니다. 기본적으로 DNS NAT 재작성이 활성화된 DNS 검사는 글로벌로 적용되므로 검사 구성을 변경하지 않아도 됩니다.
- DNS 재작성은 실제로 NAT 규칙이 아니라 xlate 항목에서 수행됩니다. 따라서 동적 규칙에 대한 xlate가 없으면 재작성을 정확히 수행할 수 없습니다. 고정 NAT에 대해서는 동일한 문제가 발생하지 않습니다.
- DNS 재작성에서는 DNS 동적 업데이트 메시지(opcode 5)를 재작성하지 않습니다.

다음 항목에서는 NAT 규칙의 DNS 재작성 예를 제공합니다.

DNS64 회신 수정

다음 그림은 외부 IPv4 네트워크의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 IPv6 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.200.225로 응답합니다.

내부 사용자가 ftp.cisco.com(2001:DB8::D1A5:C8E1, 여기서 D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다. 이 예에는 DNS 서버용 고정 NAT 변환 및 내부 IPv6 호스트용 PAT 규칙도 포함되어 있습니다.



시작하기 전에

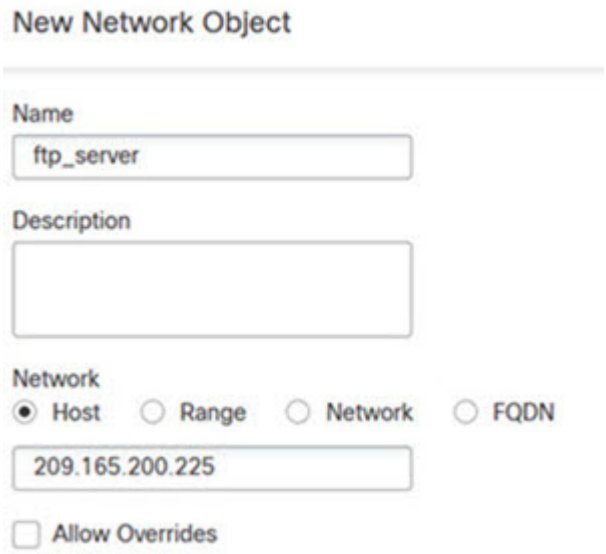
디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** FTP 서버, DNS 서버, 내부 네트워크 및 PAT 풀용 네트워크 개체를 생성합니다.

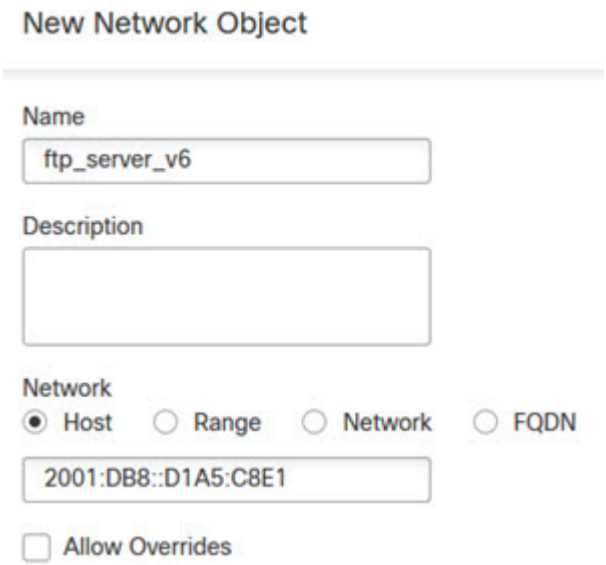
a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 실제 FTP 서버 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server와 같이 지정하고 호스트 주소 209.165.200.225를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.
e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 FTP 서버의 변환된 IPv6 주소를 정의합니다.

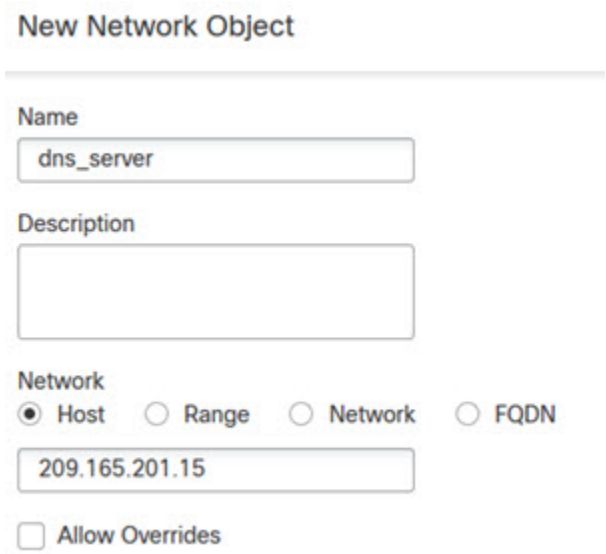
네트워크 개체의 이름을 ftp_server_v6와 같이 지정하고 호스트 주소 2001:DB8::D1A5:C8E1을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

g) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 DNS 서버의 실제 주소를 정의합니다.

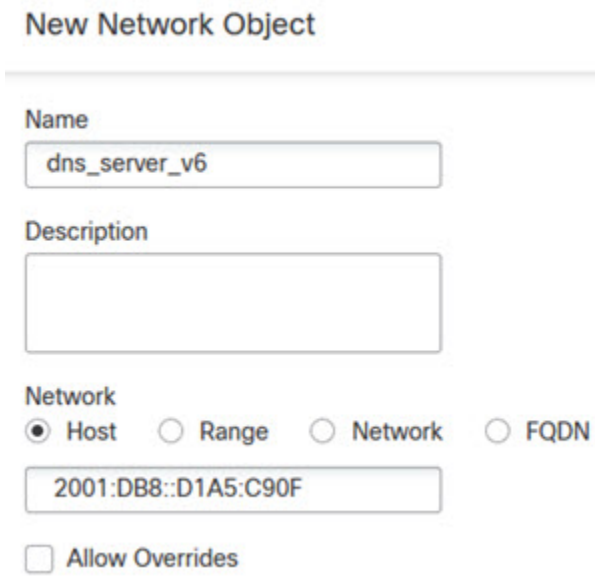
네트워크 개체의 이름을 dns_server와 같이 지정하고 호스트 주소 209.165.201.15를 입력합니다.



h) **Save(**저장**)**를 클릭합니다.

i) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 DNS 서버의 변환된 IPv6 주소를 정의합니다.

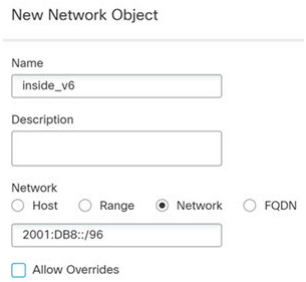
네트워크 개체의 이름을 dns_server_v6와 같이 지정하고 호스트 주소 2001:DB8::D1A5:C90F(D1A5:C90F는 209.165.201.15에 해당하는 IPv6)를 입력합니다.



j) **Save(**저장**)**를 클릭합니다.

k) **Add Network(**추가 네트워크**)** > **Add Object(**개체 추가**)**를 클릭하고 내부 IPv6 네트워크를 정의합니다.

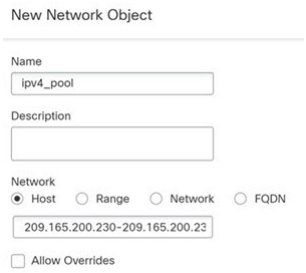
네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:DB8::/96을 입력합니다.



l) **Save(**저장**)**를 클릭합니다.

m) **Add Network(**추가 네트워크**)** > **Add Object(**개체 추가**)**를 클릭하고 내부 IPv6 네트워크에 대한 IPv4 PAT 풀을 정의합니다.

네트워크 개체의 이름을 지정하고(예: ipv4_pool) 네트워크 범위 209.165.200.230-209.165.200.235를 입력합니다.



n) **Save(**저장**)**를 클릭합니다.

단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

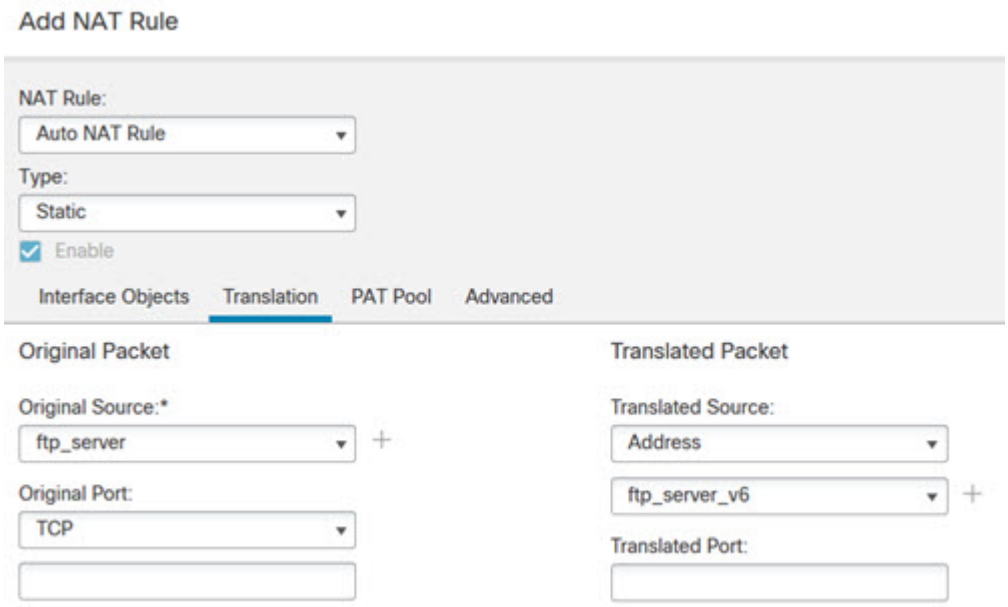
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = ftp_server 네트워크 개체.

• 번역 된 원본 > 주소 = ftp_server_v6 네트워크 개체.



f) **Advanced(**고급**)**에서 다음 옵션을 선택합니다.

- **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 회신 변환**)**.
- **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**(일대일 NAT46 변환이므로).

g) **OK(**확인**)**를 클릭합니다.

단계 **3** DNS 서버용 고정 NAT 규칙을 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

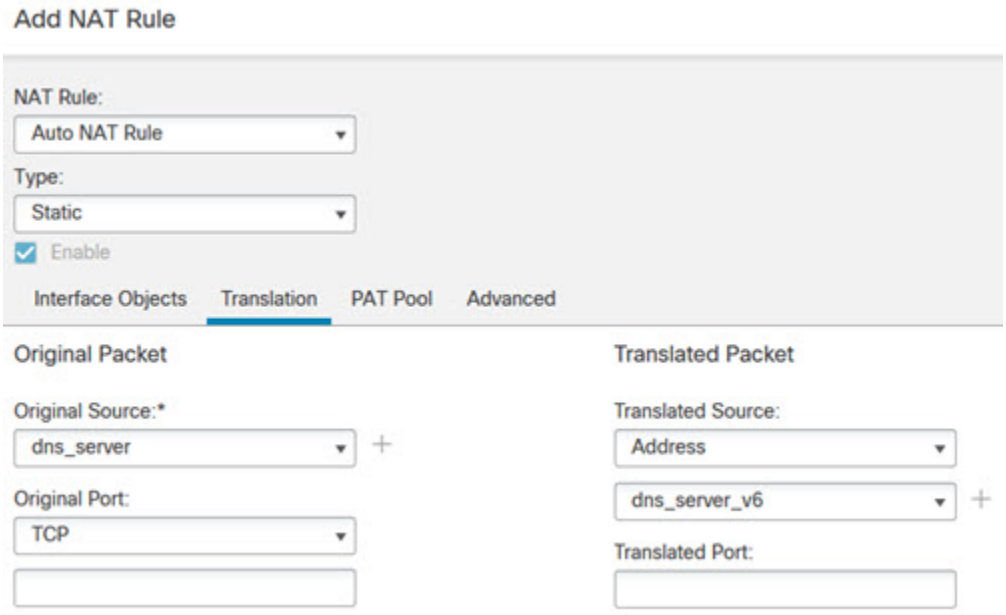
c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- 원본 소스 = dns_server 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = dns_server_v6 네트워크 개체.

e) **Advanced(**고급**)**에서 **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**을 선택합니다. 일대일 NAT46 변환이기 때문입니다.



f) **OK(**확인**)**를 클릭합니다.

단계 **4** 내부 IPv6 네트워크용 PAT 풀 규칙을 통해 동적 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

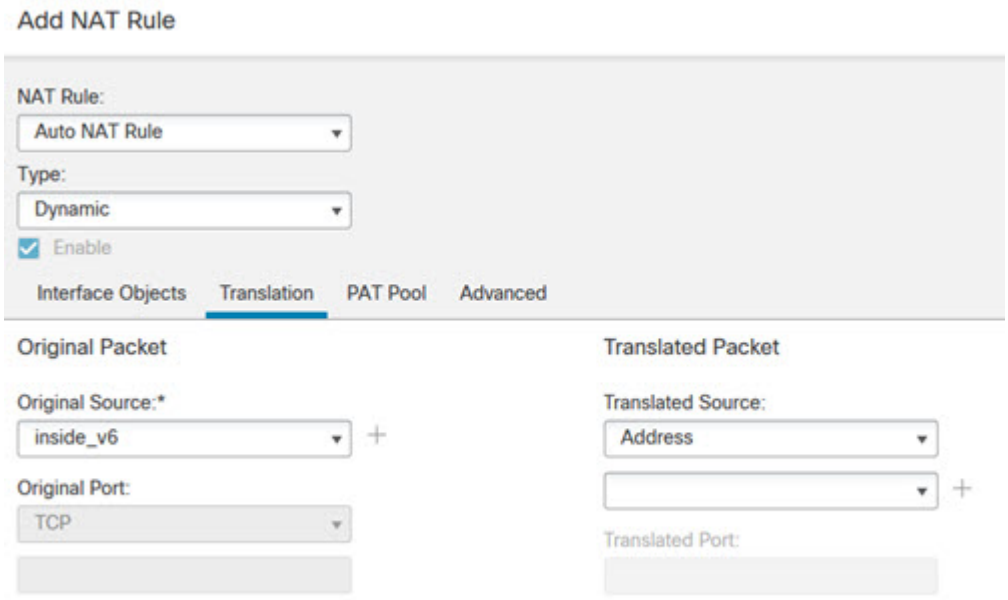
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

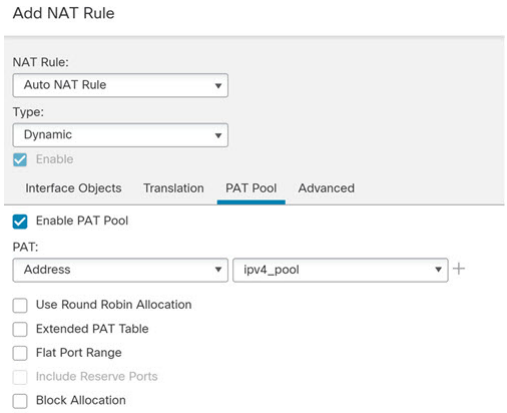
d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = 이 필드를 비워 둡니다.



e) **PAT Pool(PAT** 풀**)**에서 다음을 구성합니다.

- **Enable PAT Pool(PAT** 풀 활성화**)** = 이 옵션을 선택합니다.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ipv4_pool 네트워크 개체.



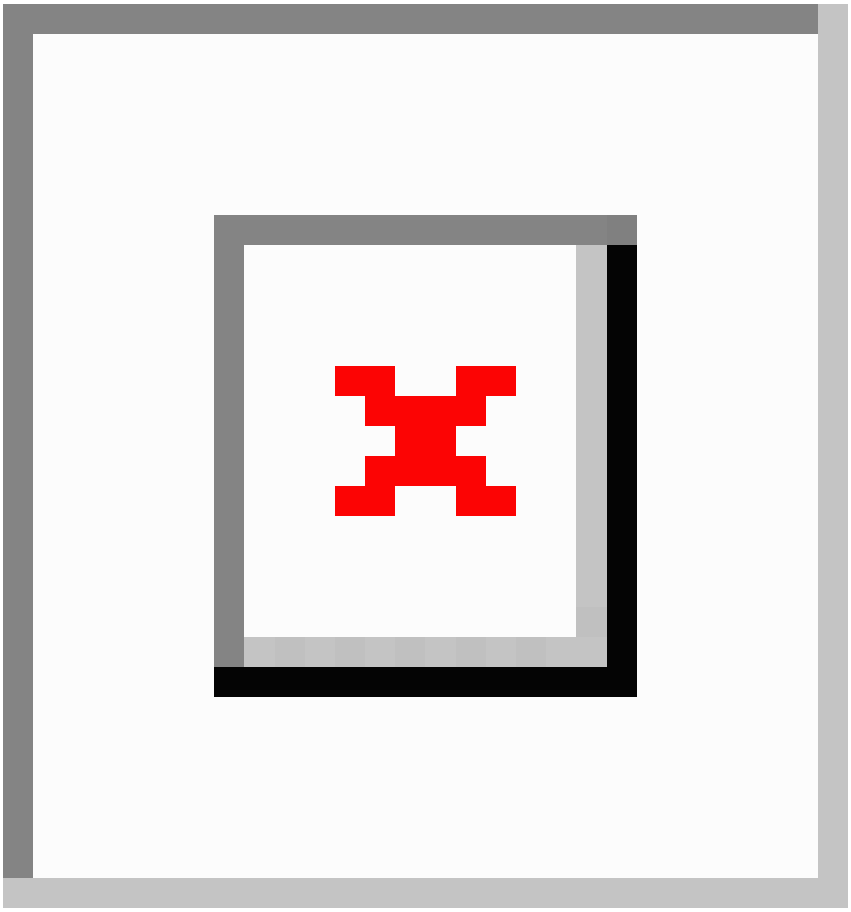
f) **OK(**확인**)**를 클릭합니다.

DNS 회신 수정, 외부의 DNS 서버

다음 그림은 인터페이스 외부에서 액세스할 수 있는 DNS 서버를 보여줍니다. ftp.cisco.com 서버는 내부 인터페이스에 있습니다. ftp.cisco.com 실제 주소(10.1.3.14)를 외부 네트워크에서 보이는 매핑된 주소(209.165.201.10)로 고정 변환하도록 NAT를 구성하십시오.

이 경우, 실제 주소를 사용하여 ftp.cisco.com에 액세스할 수 있는 내부 사용자가 DNS 서버에서 실제 주소(매핑된 주소가 아님)를 받을 수 있도록 고정 규칙에 대한 DNS 회신 수정을 사용할 수 있습니다.

내부 호스트가 ftp.cisco.com 주소에 DNS 요청을 전송하면, DNS 서버는 매핑된 주소(209.165.201.10)로 회신합니다. 시스템은 내부 서버에 대한 고정 규칙을 참조하여 DNS 회신에 있는 주소를 10.1.3.14로 변환합니다. DNS 회신 수정을 활성화하지 않으면 내부 호스트는 ftp.cisco.com에 직접 액세스하는 대신 트래픽을 209.165.201.10으로 전송하려고 시도하게 됩니다.



시작하기 전에

디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

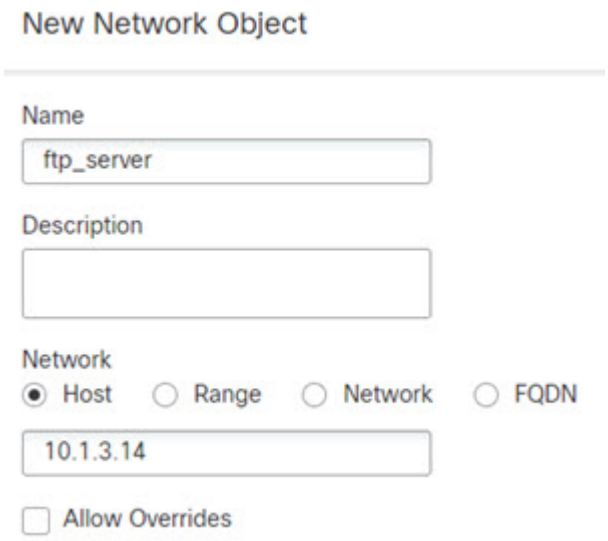
단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.

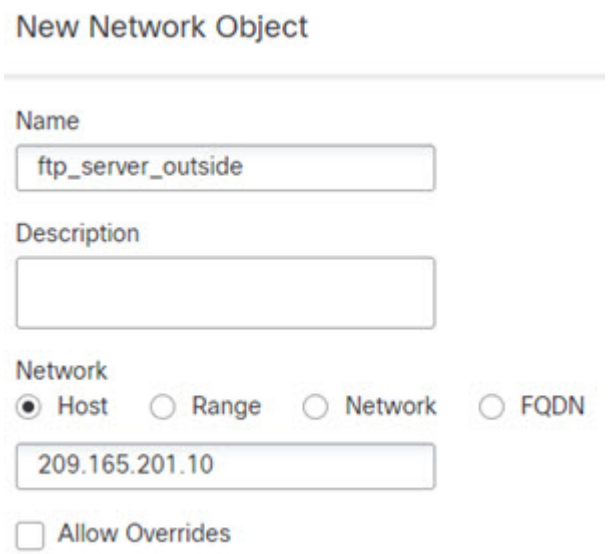
네트워크 개체의 이름을 ftp_server와 같이 지정하고 호스트 주소 10.1.3.14를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 FTP 서버의 변환된 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server_outside와 같이 지정하고 호스트 주소 209.165.201.10을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

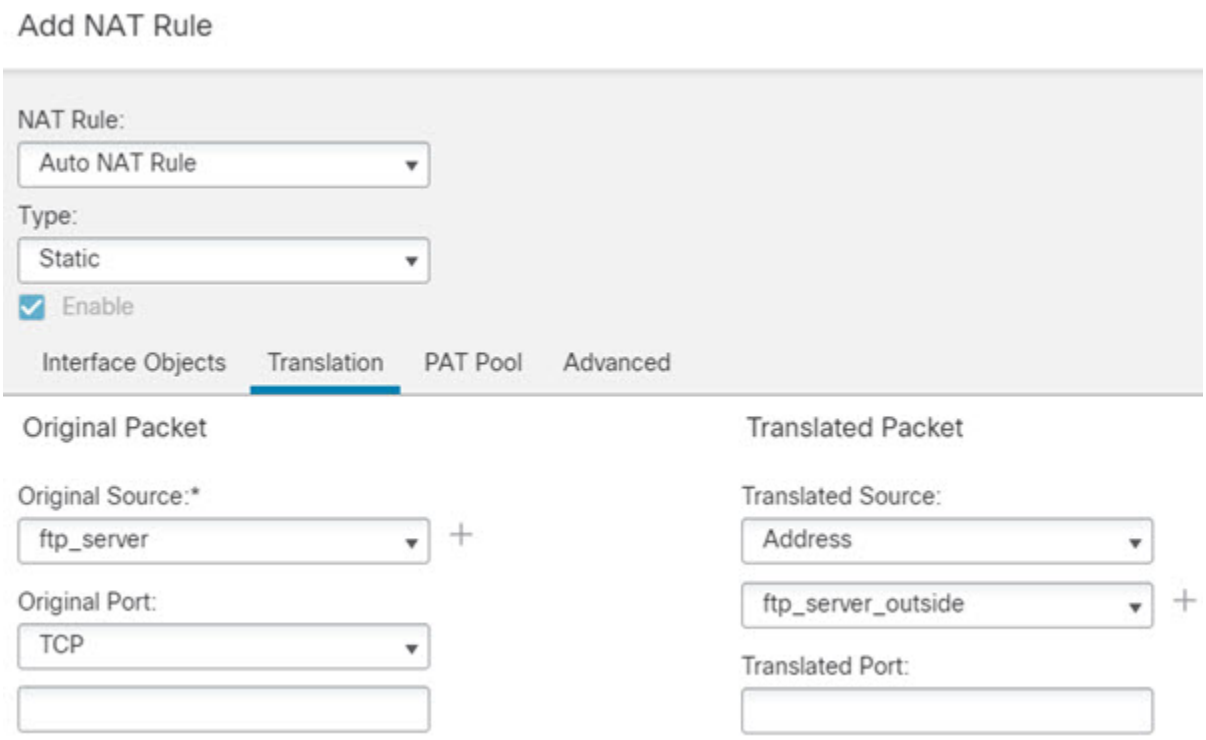
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = ftp_server 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ftp_server_outside 네트워크 개체.

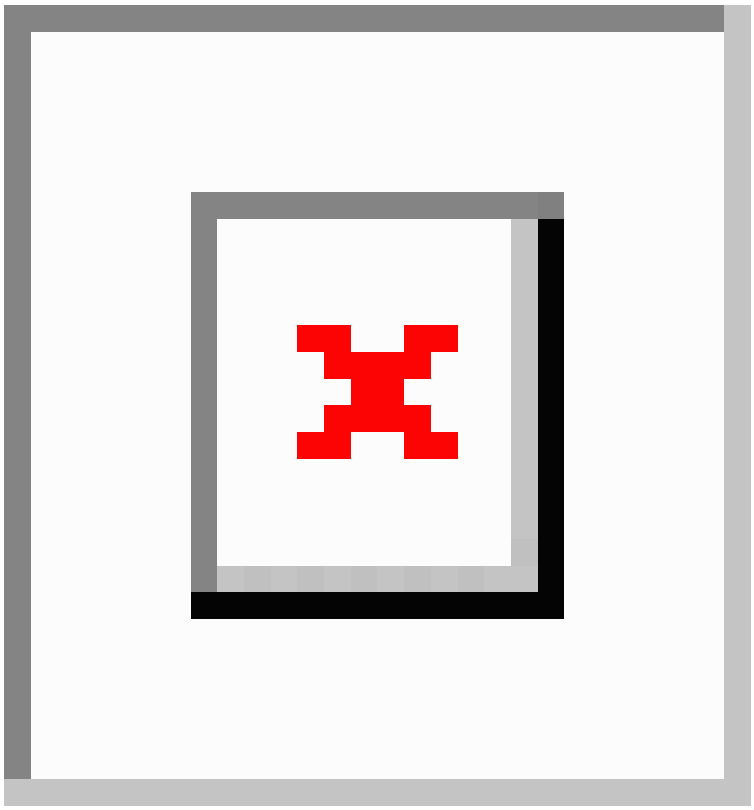
f) **Advanced(**고급**)**에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



g) **OK(**확인**)**를 클릭합니다.

DNS 회신 수정, 호스트 네트워크의 DNS 서버

다음 그림은 외부의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.20.10으로 응답합니다. 내부 사용자가 ftp.cisco.com(10.1.2.56)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다.



시작하기 전에

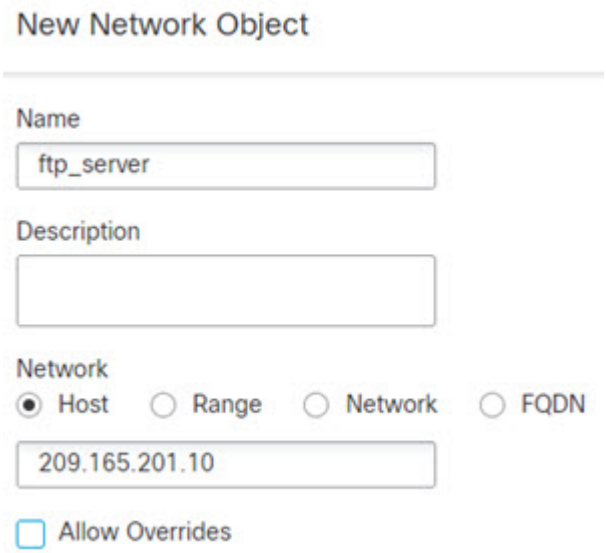
디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 실제 FTP 서버 주소를 정의합니다.

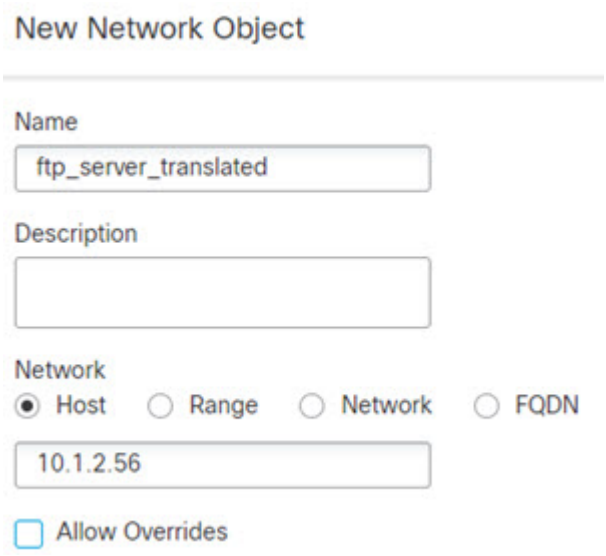
네트워크 개체의 이름을 ftp_server와 같이 지정하고 호스트 주소 209.165.201.10를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 FTP 서버의 변환된 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server_translated와 같이 지정하고 호스트 주소 10.1.2.56을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT 규칙)** = Auto NAT Rule.
- 유형 = 고정

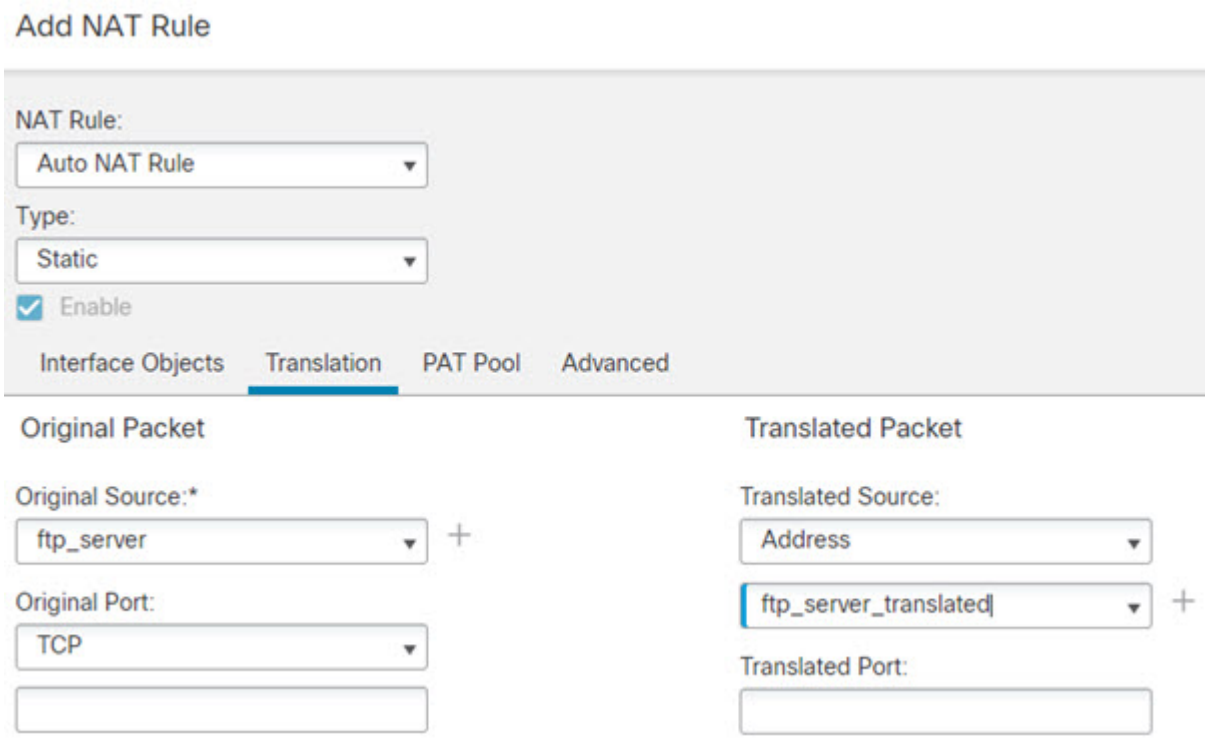
d) **Interface Objects(인터페이스 개체)**에서 다음을 구성합니다.

- **Source Interface Objects(소스 인터페이스 개체)** = outside.
- **Destination Interface Objects(대상 인터페이스 개체)** = inside.

e) **Translation(변환)**에서 다음을 구성합니다.

- **Original Source(원본 소스)** = ftp_server 네트워크 개체.
- **Translated Source(변환된 소스)** > **Address(주소)** = ftp_server_translated 네트워크 개체.

f) **Advanced(고급)**에서 **Translate DNS replies that match this rule(이 규칙과 일치하는 DNS 응답 변환)**을 선택합니다.



g) **OK(확인)**를 클릭합니다.

FTD NAT 기록

기능	버전	세부 사항
Firepower Threat Defense에 대한 NAT(Network Address Translation).	6.0.1	Firepower Threat Defense에 대한 NAT 정책이 추가되었습니다. 신규/수정된 화면: Threat Defense가 **Devices(**디바이스**)** > **NAT** 페이지에 NAT 정책 유형으로 추가되었습니다. 지원되는 플랫폼: Firepower Threat Defense
Firepower Threat Defense용 NAT에서 네트워크 범위 개체에 대해 지원합니다.	6.1.0	해당되는 경우 Firepower Threat Defense NAT 규칙에서 네트워크 범위 개체를 사용할 수 있습니다.
통신 사업자급 NAT 개선 사항	6.5	통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 신규/수정된 화면: Firepower Threat Defense NAT 규칙의 NAT PAT Pool 탭에 **Block Allocation(**블록 할당**)** 옵션을 추가했습니다. 지원되는 플랫폼: Firepower Threat Defense
FTD NAT 규칙 테이블을 검색하고 필터링하는 기능.	6.7	이제 FTD NAT 정책에서 규칙을 검색하여 IP 주소, 포트, 개체 이름 등을 기준으로 규칙을 찾을 수 있습니다. 검색 결과에는 부분 일치 항목이 포함됩니다. 기준을 검색하면 규칙 테이블이 필터링되므로 일치하는 규칙만 표시됩니다. FTD NAT 정책을 편집할 때 규칙 테이블 위에 검색 필드를 추가했습니다.

기능	버전	세부 사항
클러스터링에서 PAT 주소 할당을 변경합니다. PAT 풀 **Flat Port Range(**플랫 포트 범위**)** 옵션은 이제 기본적으로 활성화되어 있으며 구성할 수 없습니다.	6.7	PAT 주소가 클러스터 멤버에 배포되는 방식이 변경되었습니다. 이전에는 주소가 클러스터의 멤버에 분산되었으므로 PAT 풀에는 클러스터 멤버당 최소 1개의 주소가 필요했습니다. 이제 제어 유닛은 각 PAT 풀 주소를 동일한 크기의 포트 블록으로 분할하여 클러스터 멤버에 분산시킵니다. 각 멤버에는 동일한 PAT 주소에 대한 포트 블록이 있습니다. 따라서 일반적으로 PAT에 필요한 연결의 양에 따라 PAT 풀의 크기를 하나의 IP 주소로 줄일 수 있습니다. 포트 블록은 1024~65535 범위에서 512 포트 블록에 할당됩니다. PAT 풀 규칙을 구성할 때 이 블록 할당에 예약된 포트 1 ~ 1023을 선택적으로 포함할 수 있습니다. 예를 들어, 4 노드 클러스터에서 각 노드는 PAT 풀 IP 주소당 16,384 개의 연결을 처리할 수 있는 32개 블록을 가져오며, PAT 풀 IP 주소당 모든 65535 연결을 처리하는 단일 노드와 비교됩니다. 이러한 변경의 일환으로, 독립형이든 클러스터에서 작동 중인지에 관계 없이 모든 시스템의 PAT 풀은 이제 1023 ~ 65535의 플랫 포트 범위를 사용합니다. 이전에는 PAT 풀 규칙에 **Flat Port Range(**플랫 포트 범위**)** 옵션을 포함하여 플랫 범위를 선택적으로 사용할 수 있었습니다. 이제 **Flat Port Range(**플랫 포트 범위**)** 옵션이 무시됩니다. PAT 풀이 항상 플랫 상태입니다. 선택적으로 **Include Reserved Ports(**예약된 포트 포함**)** 옵션을 선택하여 PAT 풀에 1 ~ 1023 포트 범위를 포함할 수 있습니다. 포트 블록 할당(**Block Allocation(**블록 할당**)** PAT 풀 옵션)을 구성하면 기본 512 포트 블록이 아닌 블록 할당 크기가 사용됩니다. 또한 클러스터의 시스템에 대한 PAT 풀에 대해 확장 PAT를 구성할 수 없습니다.

XIV 부

액세스 제어

- 액세스 제어의 이해, 1609 페이지
- 액세스 제어의 모범 사례, 1617 페이지
- 액세스 제어 정책, 1625 페이지
- 액세스 제어 규칙, 1645 페이지
- URL 필터링, on page 1665
- HTTP 응답 페이지 및 인터랙티브 차단, 1689 페이지
- 보안 인텔리전스 차단 목록, 1695 페이지
- DNS 정책, 1709 페이지
- 사전 필터링 및 사전 필터 정책 , 1723 페이지
- IAB(Intelligent Application Bypass), 1745 페이지
- 콘텐츠 제한을 사용하는 액세스 제어, 1755 페이지

58 장

액세스 제어의 이해

- 액세스 제어 소개, 1609 페이지
- Access Control Policy Default Action(액세스 제어 정책 기본 작업), 1610 페이지
- 파일 및 침입 정책을 사용한 심층 검사, 1612 페이지
- 액세스 제어 정책 상속, 1615 페이지

액세스 제어 소개

액세스 제어는 빠른 경로가 아닌 네트워크 트래픽을 지정하고, 검사하고 로깅할 수 있는 정책 기반 기능입니다.

각 매니지드 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 네트워크 트래픽에 대한 정책의 대상 디바이스가 수집하는 정보를 사용하여 다음을 기반으로 트래픽을 필터링 및 제어할 수 있습니다.

- 소스와 목적지, 포트, 프로토콜 등 간단하고 쉽게 결정되는 전송 및 네트워크 레이어 특성
- 평판, 위험, 비즈니스 관련성, 사용된 애플리케이션 또는 방문한 URL 등의 특성을 비롯하여 트래픽에 대한 최신 상황 정보
- 영역, 사용자, 사용자 그룹 또는 ISE 속성
- 암호화된 트래픽의 특성(추가 분석을 위해 이 트래픽을 해독할 수도 있음)
- 암호화되지 않은 또는 해독된 트래픽에 금지된 파일, 탐지된 악성코드 또는 침입 시도가 포함되었는지 여부
- 시간 및 요일(지원되는 디바이스)

각 유형의 트래픽 검사와 제어는 유연성과 성능을 최대화할 수 있는 방식으로 발생합니다. 예를 들어, 평판에 기반한 차단은 단순한 소스 및 대상 데이터를 사용하므로 프로세스 초기에 금지된 트래픽을 차단할 수 있습니다. 반면, 침입과 익스플로잇의 탐지 및 차단은 최후의 방어 수단입니다.

Access Control Policy Default Action(액세스 제어 정책 기본 작업)

새로 생성된 액세스 제어 정책은 기본 작업을 사용하여 모든 트래픽을 처리하도록 대상 디바이스에 지시합니다.

간단한 액세스 제어 정책에서 기본 작업은 대상 디바이스가 모든 트래픽을 처리하는 방법을 지정합니다. 보다 복잡한 정책에서 기본 작업은 다음과 같은 트래픽을 처리합니다.

- IAB(Intelligent Application Bypass)가 신뢰하지 않는 트래픽
- 보안 인텔리전스 차단 목록 제외
- SSL 검사에서 차단되지 않은 트래픽(암호화된 트래픽만 해당)
- 정책 내 규칙 중 어느 것과도 일치하지 않는 것입니다(트래픽에 일치시키거나 트래픽을 로깅하지만 처리하거나 검사하지는 않는 모니터링 규칙은 제외).

액세스 제어 정책 기본 작업을 사용하여 추가 검사 없이 트래픽을 차단하거나 신뢰할 수 있고, 침입 및 검색 데이터 트래픽을 검사할 수 있습니다.

참고 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다. 기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화되어 있지만 활성화할 수는 있습니다.

정책 상속을 사용하는 경우 가장 낮은 수준의 하위 항목에 대한 기본 작업에 따라 최종 트래픽 처리가 결정됩니다. 액세스 제어 정책은 기본 정책에서 기본 작업을 상속할 수 있지만 이 상속을 적용할 수는 없습니다.

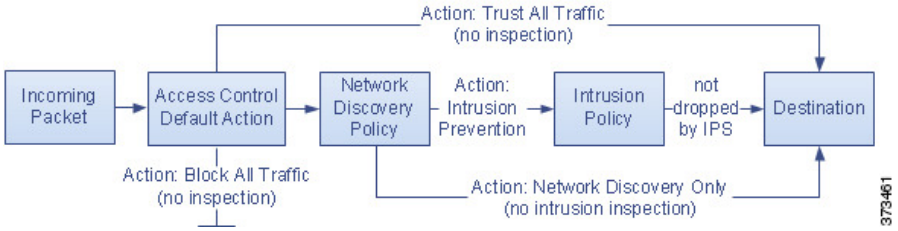
다음 표는 각 기본 작업에 의해 처리된 트래픽에서 수행할 수 있는 검사 유형을 나열합니다.

표 ***100:*** 액세스 제어 정책 기본 작업

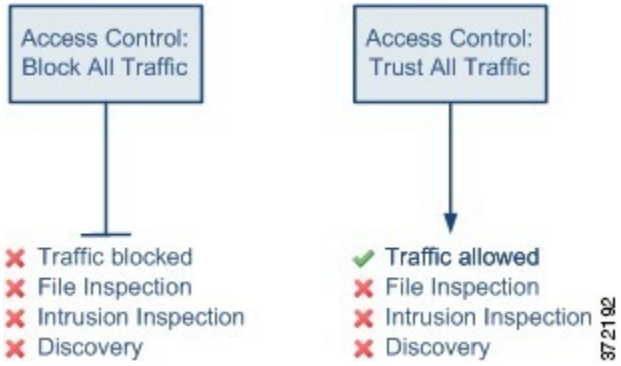
기본 작업	트래픽에 미치는 영향	검사 유형 및 정책
액세스 제어: 모든 트래픽 차단	추가 검사 없이 차단	없음
액세스 제어: 모든 트래픽 신뢰	신뢰(추가 검사 없이 최종 대상에서 허용)	없음
침입 방지	허용. 사용자가 지정한 침입 정책에 의해 통과된 경우	지정된 침입 정책 및 관련 변수 집합을 사용한 침입 및 네트워크 검색 정책을 사용한 검색
네트워크 검색 한정	허용	네트워크 검색 정책을 사용한 검색만 해당

기본 작업	트래픽에 미치는 영향	검사 유형 및 정책
기본 정책에서 상속	기본 정책에 정의됨	기본 정책에 정의됨

다음 다이어그램은 테이블을 보여 줍니다.



다음 다이어그램은 **Block All Traffic(**모든 트래픽 차단**)** 및 **Trust All Traffic(**모든 트래픽 신뢰**)** 기본 작업을 설명합니다.



다음 다이어그램은 **Intrusion Prevention(**침입 방지**)** 및 **Network Discovery Only(**네트워크 검색 한정**)** 기본 작업을 설명합니다.

팁 **Network Discovery Only**의 목적은 검색 전용 구축 작업의 성능을 향상하는 것입니다. 침입 탐지 및 방지만 사용하려는 경우 다른 구성으로 검색을 비활성화할 수 있습니다.

관련 항목

제한된 구축에 대한 성능 고려 사항, 516 페이지

정책 기본 작업으로 연결 로깅, 2873 페이지

파일 및 침입 정책을 사용한 심층 검사

심층 검사는 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로서 침입 및 파일 정책을 사용합니다.

- 침입 정책은 시스템의 침입 방지 기능을 제어합니다.

  자세한 내용은 침입 탐지 및 방지, 1959 페이지를 참조하십시오.

- 파일 정책은 시스템의 파일 제어 및 AMP for Networks 기능을 제어합니다.

  자세한 내용은 파일 정책 및 악성코드 보호, 1861 페이지를 참조하십시오.

액세스 제어는 심층 검사 전에 이루어집니다. 액세스 제어 규칙 및 액세스 제어 기본 작업은 정책 및 파일 정책으로 어떤 트래픽을 검사할지 결정합니다.

침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽이 통과하기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 우선 트래픽을 검사하도록 할 수 있습니다.

액세스 제어 정책에서는 하나의 침입 정책을 각 허용 및 인터랙티브 차단 규칙 및 기본 작업과 연결할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다.

침입 및 파일 정책을 액세스 제어 규칙과 결합하려면 다음을 확인합니다.

- 침입 방지를 수행하는 액세스 제어 규칙 설정, 2001 페이지
- 악성코드 보호를 수행하는 액세스 제어 규칙 구성, 1869 페이지

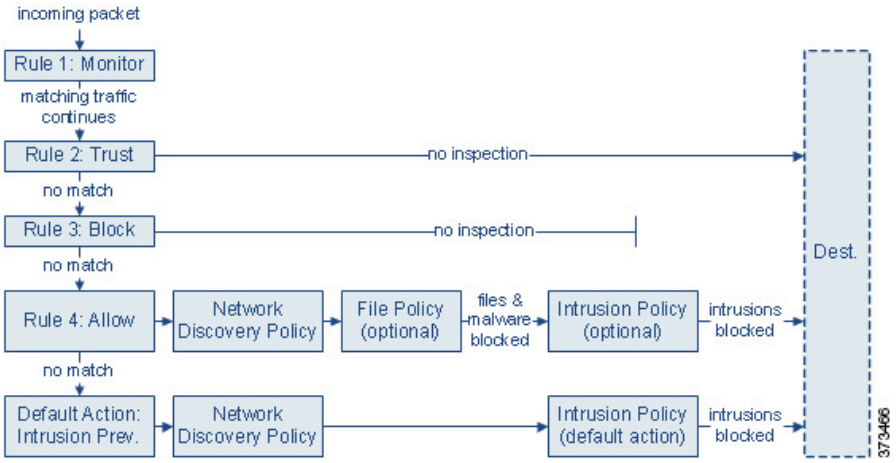
참고 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

관련 항목

정책이 트래픽에서 침입을 검토하는 방법, 1962 페이지
파일 정책, 1862 페이지

침입 정책 및 파일 정책을 사용한 액세스 제어 트래픽 처리

다음 다이어그램에는 네 가지 다른 유형의 액세스 제어 규칙 및 기본 작업이 포함된 액세스 제어 정책으로 제어되는 인라인 침입 방지 및 AMP for Networks 구축 시 트래픽의 흐름이 나와 있습니다.



위 시나리오에서 정책의 처음 세 액세스 제어 규칙(모니터, 신뢰, 차단)은 일치하는 트래픽을 검사할 수 없습니다. 모니터 규칙은 네트워크 트래픽을 추적하고 로깅하지만 검사하지는 않으므로 시스템은 트래픽을 추가 규칙과 계속 대조하여 트래픽을 허용할지 거부할지 결정합니다. (액세스 제어 규칙 모니터 작업, 1658 페이지에서 중요 예외 및 주의 사항을 확인하십시오.) 신뢰 및 차단 규칙은 어떠한 종류의 추가 검사 없이도 일치하는 트래픽을 처리하지만 일치하지 않는 트래픽은 다음 액세스 제어 규칙으로 계속 진행합니다.

정책의 네 번째이자 마지막 규칙인 허용 규칙은 다양한 다른 정책을 호출하여 다음과 같은 순서로 일치하는 트래픽을 검사하고 처리합니다.

- 검색**:** 네트워크 검색 정책 - 우선 네트워크 검색 정책은 검색 데이터에 대해 트래픽을 검사합니다. 검색은 수동 분석이며 트래픽 흐름에 영향을 미치지 않습니다. 검색을 명시적으로 활성화하지 않더라도 검색을 강화하거나 비활성화할 수 있습니다. 그러나 트래픽을 허용한다고 해서 자동으로 검색 데이터 수집이 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에서 명시적으로 모니터링하는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다.
- **AMP for Networks** 및 파일 제어**:** 파일 정책 - 검색에 의해 트래픽이 검사된 후 시스템은 트래픽에서 금지된 파일과 악성코드를 검사할 수 있습니다. AMP for Networks 는 PDF, Microsoft Office 문서 등을 포함한 여러 파일 형식에서 악성코드를 탐지하고 선택적으로 차단할 수 있습니다. 조직에서 악성코드 파일의 전송뿐만 아니라 특정 유형의 모든 파일(해당 파일의 악성코드 포함 여부에 상관없이)을 차단하려는 경우, 파일 제어를 사용하면 특정 파일 유형의 전송에 대해 네트워크 트래픽을 모니터링한 다음 해당 파일을 차단하거나 허용할 수 있습니다.
- 침입 방지**:** 침입 정책 - 파일 검사 후 시스템에서는 침입 및 익스플로잇에 대해 트래픽을 검사할 수 있습니다. 침입 정책은 패턴을 기반으로 디코딩된 패킷에서 공격을 검사하며 악의적인 트래픽을 차단하거나 변경할 수 있습니다. 침입 정책은 변수 집합과 페어링되는데, 이를 통해 네트워크 환경을 올바르게 반영하는 지정된 값을 사용할 수 있습니다.
- 대상 - 위에 설명된 모든 확인을 통과하는 트래픽은 대상에 도달합니다.

인터랙티브 차단 규칙(다이어그램에 표시되지 않음)에는 허용 규칙과 동일한 검사 옵션이 있습니다. 이를 사용하면 사용자가 경고 페이지를 클릭하여 차단된 웹 페이지를 우회할 경우 악의적인 콘텐츠에 대해 트래픽을 검사할 수 있습니다.

모니터링을 제외한 작업을 이용하는 정책의 액세스 제어 규칙과 일치하지 않는 트래픽은 기본 작업에 의해 처리됩니다. 이 시나리오에서 기본 작업은 사용자가 지정한 침입 정책에서 통과시키는 트래픽이 최종 대상에 도달하도록 허용하는 침입 방지 작업입니다. 다른 구축에는 추가 검사 없이 모든 트래픽을 신뢰하거나 차단하는 기본 작업이 있을 수 있습니다. 시스템은 기본 작업에서 허용하는 트래픽에 대해 검색 데이터 및 침입 여부를 검사할 수 있으나, 금지된 파일 또는 악성코드 여부는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 없습니다.

참고 액세스 제어 정책으로 연결을 분석할 경우, 시스템에서는 어떤 액세스 제어 규칙(있는 경우)으로 트래픽을 처리할 것인지 결정하기 전에 해당 연결의 처음 몇 가지 패킷을 처리하여, 통과되도록 허용해야 합니다. 그러나 이러한 패킷이 검사되지 않은 상태로 대상에 도달하지 않도록 침입 정책(액세스 제어 정책의 고급 설정)을 지정하여 해당 패킷을 검사하고 침입 이벤트를 생성할 수 있습니다.

파일 및 침입 검사 순서

액세스 제어 정책에서 여러 허용 및 인터랙티브 차단 규칙을 다양한 침입 및 파일 정책에 연결하여 검사 프로파일과 다양한 트래픽 유형을 대조할 수 있습니다.

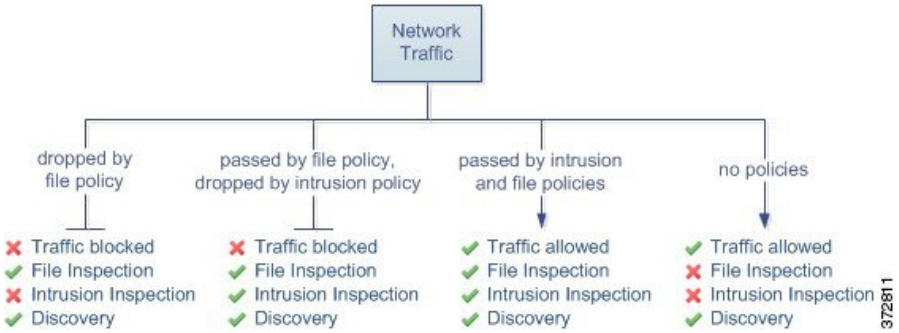
참고 트래픽이 침입 방지 또는 네트워크 검색 한정 기본 작업에 의해 허용된 경우 검색 데이터 및 침입은 검사할 수 있지만, 금지된 파일 또는 악성코드는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 없습니다.

동일한 규칙에서 파일 및 침입 검사를 모두 수행할 필요는 없습니다. Allow or Interactive Block(허용 또는 인터랙티브 차단) 규칙과 일치하는 연결의 경우:

- 파일 정책이 없는 경우, 트래픽 흐름은 침입 정책에 의해 결정됨
- 침입 정책이 없는 경우, 트래픽 흐름은 파일 정책에 의해 결정됨
- 두 가지 정책이 모두 없는 경우, 허용되는 트래픽은 네트워크 검색 한정에 의해 검사됨

팁 시스템은 신뢰할 수 있는 트래픽에는 검사를 수행하지 않습니다. 침입 또는 파일 정책 없이 허용 규칙을 구성하면 트래픽을 신뢰 규칙처럼 통과시키지만 허용 규칙을 통해 일치하는 트래픽에서 검색을 수행할 수 있습니다.

아래 다이어그램은 허용 규칙 또는 사용자가 우회한 인터랙티브 차단 규칙의 조건을 충족하는 트래픽에서 수행할 수 있는 검사 유형을 보여줍니다. 간단한 설명을 위해 다이어그램에는 침입 정책과 파일 정책 모두 단일 액세스 제어 규칙에 연결되거나 모두 연결되지 않은 상황의 트래픽 흐름을 보여줍니다.



액세스 제어 규칙으로 처리되는 단일한 연결의 경우, 침입 검사 전에 파일 검사가 이루어집니다. 즉, 시스템에서는 파일 정책 또는 침입에 의해 차단된 파일은 검사하지 않습니다. 파일 검사 내에서 유형을 기준으로 한 간단한 차단은 악성코드 검사 및 차단보다 우선합니다.

예를 들어, 액세스 제어 규칙에 정의된 대로 특정 네트워크 트래픽을 일반적으로 허용하고자 하는 시나리오를 가정해보겠습니다. 그러나 일종의 예방 조치로서 실행 파일의 다운로드를 차단하고, 다운로드된 PDF의 악성코드 여부를 검사하고 검색된 모든 인스턴스를 차단하며, 트래픽에 침입 검사를 수행하고자 합니다.

일시적으로 허용하고자 하는 트래픽의 특성과 일치하는 규칙으로 액세스 제어 정책을 생성하고 이를 침입 정책과 파일 정책에 모두 연결합니다. 파일 정책은 모든 실행 파일의 다운로드를 차단하며, 검사를 수행하고 악성코드가 포함된 PDF를 차단합니다.

- 우선 시스템에서는 파일 정책에 지정된 것과 일치하는 간단한 유형을 기준으로 모든 실행 파일의 다운로드를 차단합니다. 이러한 파일은 즉시 차단되기 때문에 악성코드 또는 침입 검사 대상에서 제외됩니다.
- 그다음, 시스템에서는 네트워크의 호스트에 다운로드된 PDF에 악성코드 클라우드 조회를 수행합니다. 악성코드 속성이 포함된 모든 PDF 파일은 차단되며 침입 검사 대상에서 제외됩니다.
- 마지막으로, 시스템에서는 액세스 제어 규칙과 연결된 침입 정책을 사용하여 모든 나머지 트래픽을 검사하며 여기에는 파일 정책으로 차단되지 않은 파일이 포함됩니다.

참고 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 수 있습니다.

액세스 제어 정책 상속

다중 도메인 구축에서 특히 유용하며 액세스 제어 정책을 중복할 수 있습니다. 각 정책은 상위(또는 기본) 정책의 규칙 및 설정을 상속합니다. 이 상속을 적용하거나 하위 정책을 허용하여 해당 상위 항목을 재정의할 수 있습니다.

액세스 컨트롤은 계층적 정책 기반 실행을 사용합니다. 도메인 계층을 생성하는 것처럼 액세스 제어 정책의 해당 계층을 생성할 수 있습니다. 하위 항목 또는 차일드, 액세스 제어 정책은 직속 부모 또는 기본 정책으로부터 규칙과 설정을 상속합니다. 기본 정책은 다른 부모 정책으로부터 규칙과 설정을 상속 받았을 수 있습니다.

액세스 제어 정책의 규칙은 상위 정책의 Mandatory(필수) 및 Default(기본값) 규칙 섹션 사이에 중첩됩니다. 이 구현은 상위 정책의 필수 규칙을 적용하지만 현재 정책이 상위 정책의 기본 규칙을 선점하는 규칙을 작성하도록 허용합니다.

다음 설정을 잠금 처리하여 모든 하위 정책에서 적용할 수 있습니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

- 보안 인텔리전스 - IP 주소, URL 및 도메인 이름에 대한 최신 평판 인텔리전스를 기반으로 연결을 허용하거나 차단합니다.
- HTTP 응답 페이지 - 사용자의 웹 사이트 요청을 차단할 때 사용자 정의 또는 시스템 제공 응답 페이지를 표시합니다.
- 고급 설정 - 관련 하위 정책, 네트워크 분석 설정, 성능 설정 및 기타 일반 옵션을 지정합니다.

정책 상속을 사용하는 경우, 가장 낮은 수준의 하위 항목에 대한 기본 작업에 따라 최종 트래픽 처리가 결정됩니다. 액세스 제어 정책은 상위 정책에서 기본 작업을 상속할 수 있지만 이 상속을 적용할 수는 없습니다.

정책 상속 및 멀티 테넌시

액세스 컨트롤의 계층적 정책 기반 실행은 멀티 테넌시를 보완합니다.

일반적인 다중 도메인 구축에서 액세스 제어 정책 계층은 도메인 구조에 해당하며, 매니지드 디바이스에 최하위 수준 액세스 제어 정책을 적용합니다. 이 구현은 상위 도메인 수준에서 선택적 액세스 제어 적용을 허용하고 하위 도메인 관리자는 구축별 설정을 조정할 수 있습니다. (하위 도메인의 관리자를 제한하려면 정책 상속 및 적용을 단독으로 수행하지 말고 역할을 사용해야 합니다.)

예를 들어 조직의 전역 도메인 관리자는 전역 수준에서 액세스 제어 정책을 만들 수 있습니다. 그런 다음 기능별로 하위 도메인으로 구분된 모든 디바이스가 해당 전역 수준 정책을 기본 정책으로 사용하도록 요구할 수 있습니다.

하위 도메인 관리자가 Firepower Management Center에 액세스하여 액세스 제어를 구성하면 전역 수준의 정책을 있는 그대로 배포할 수 있습니다. 또는 전역 수준 정책의 범위 내에서 하위 수준의 액세스 제어 정책을 만들고 구축할 수 있습니다.

참고 액세스 제어 상속 및 적용의 가장 유용한 구현이 멀티 테넌시를 보완하지만 단일 도메인 내에서 액세스 제어 정책의 계층 구조를 생성할 수 있습니다. 또한 모든 수준에서 액세스 제어 정책을 지정하고 구축할 수도 있습니다.

관련 항목

액세스 제어 정책 상속 관리, 1632 페이지
보안 인텔리전스 차단 목록, 1695 페이지
HTTP 응답 페이지 및 인터랙티브 차단, 1689 페이지
액세스 제어 정책 고급 설정, 1637 페이지
액세스 제어 정책용 로깅 설정, 1636 페이지

59 장

액세스 제어의 모범 사례

- 액세스 제어의 모범 사례, 1617 페이지
- 액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

액세스 제어의 모범 사례

다음 요구 사항 및 일반적인 모범 사례를 검토합니다.

- 구축에 라이선스를 부여하지 않고 시스템을 구성할 수는 있지만, 대부분의 기능을 사용하려면 구축 전에 적절한 라이선스를 활성화해야 합니다.
- 시스템이 트래픽에 영향을 미치려면 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 관련 구성을 매니지드 디바이스에 구축해야 합니다.

  경우에 따라 시스템에서는 탭 모드의 인라인 디바이스를 비롯하여 수동으로 구축된 디바이스에 인라인 구성을 구축하지 못하도록 할 수 있습니다.

  다른 경우에는 정책이 성공적으로 구축될 수 있지만 수동 구축된 디바이스를 사용하여 트래픽을 차단하거나 변경하려고 하면 예상치 못한 결과가 발생할 수 있습니다. 예를 들어, 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에 시스템은 각 차단된 연결에 대한 여러 초기 연결 이벤트를 보고할 수 있습니다.
- URL 필터링, 애플리케이션 탐지, 지능형 애플리케이션 우회를 비롯한 특정 기능은 시스템에서 트래픽을 식별하기 위해 일부 패킷이 통과하도록 허용해야 합니다.

  이러한 패킷이 검사되지 않은 대상에 도달하지 못하도록하려면 트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례, 2202 페이지 및 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정, 2203 페이지의 내용을 참조하십시오.
- 액세스 제어 정책의 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.
- 일부 기능은 특정 디바이스 모델에서만 사용할 수 있습니다. 경고 아이콘 및 확정 대화 상자는 지원되지 않는 기능을 지정합니다.

- 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.
- 기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화되어 있지만 활성화할 수는 있습니다.
- 액세스 제어 규칙 생성, 순서 지정 및 구현에 대한 모범 사례는 액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지 및 하위 주제에 자세히 설명되어 있습니다.

액세스 제어 규칙 순서에 대한 모범 사례

효과적인 구축을 위해서는 규칙을 올바르게 구성하고 그 순서를 지정해야 합니다. 다음 주제는 규칙 성능 지침을 요약합니다.

참고 컨피그레이션 변경 사항을 구축할 때 시스템은 모든 규칙을 함께 평가하며, 타겟 디바이스가 네트워크 트래픽을 평가하는 데 사용하는 확장된 기준 집합을 생성합니다. 이러한 기준이 타겟 디바이스의 리소스(물리적 메모리, 프로세서 등)를 초과할 경우, 해당 디바이스에 구축할 수 없습니다.

관련 항목

애플리케이션 제어 모범 사례, 539 페이지
URL 필터링 모범 사례, 1667 페이지

규칙 순서 지정 모범 사례

일반 지침:

- 일반적으로 정책 상단에서 모든 트래픽에 적용되는 최우선 규칙을 지정합니다.
- 구체적인 규칙은 일반적인 규칙보다 먼저 배치해야 합니다(특히, 구체적인 규칙이 일반적인 규칙에 대한 예외인 경우).

  그렇지 않으면 트래픽이 일반 규칙과 먼저 일치하며 적용 가능한 특정 규칙에 도달하지 않습니다.
- 구체적인 삭제 규칙은 가능한 경우 항상 정책 상위에 둡니다. 이렇게 하면 부적절한 트래픽에 대해 가능한 한 빠른 결정을 내릴 수 있습니다.
- IP 주소, 보안 영역, 포트 번호 등 레이어-3/4 기준만을 기반으로 하여 트래픽을 삭제하는 규칙은 가능한 한 먼저 배치해야 합니다.
- URL 필터링 규칙, 애플리케이션 규칙 및 검사가 필요한 기타 규칙은 레이어 3/4 기준(예: IP 주소, 보안 영역, 포트 번호)만을 바탕으로 트래픽을 삭제하는 규칙 뒤에 와야 하며, 파일 및 침입 정책을 지정하는 규칙 앞에 와야 합니다.

- URL 필터링 규칙을 애플리케이션 규칙 위에 두고, 마이크로 애플리케이션 규칙 및 CIP(Common Industrial Protocol) 하위 분류 애플리케이션 필터링 규칙을 사용하여 애플리케이션 규칙을 따릅니다.
- 파일 정책 및 침입 정책을 지정하는 규칙은 규칙 순서의 맨 아래에 와야 합니다. 이러한 규칙에는 리소스를 많이 사용하는 심층 검사가 필요하며, 심층 검사가 필요한 잠재적인 위협 수를 최소화하려면 성능상의 이유로 먼저 덜 집중적인 방법을 사용하여 최대한 많은 위협을 제거해야 합니다.
- 항상 조직의 요구 사항에 맞게 규칙의 순서를 지정해야 합니다.

위의 지침에 대한 예외 및 추가 사항은 아래 섹션에 나와 있습니다.

규칙 선점

평가 순서에서 앞서는 규칙이 트래픽에 우선 일치하기 때문에 규칙이 트래픽과 일치하지 않는 경우 규칙 선점이 발생합니다. 규칙의 조건은 다른 규칙의 선점 여부를 제어합니다. 다음 예에서는 첫 번째 규칙이 관리 트래픽을 허용하기 때문에 두 번째 규칙이 차단할 수 없습니다.

액세스 제어 규칙 1: 관리자 사용자 허용
액세스 제어 규칙 2: 관리자 사용자 차단

모든 유형의 규칙 조건은 후속 규칙에 사전 대응할 수 있습니다. 첫 번째 SSL 규칙의 VLAN 범위는 VLAN을 두 번째 규칙으로 포함하므로 첫 번째 규칙이 두 번째 규칙보다 사전에 대응합니다.

SSL 규칙 1: VLAN 22-33을 암호화하지 않음
SSL 규칙 2: VLAN 27 차단

다음 예에서는 VLAN이 설정되지 않아 규칙 1이 모든 VLAN과 일치하므로 규칙 1이 VLAN 2에 일치시키려는 규칙 2를 선점합니다.

액세스 제어 규칙 1: 소스 네트워크 10.4.0.0/16 허용
액세스 제어 규칙 2: 소스 네트워크 10.4.0.0/16, VLAN 2 허용

규칙은 또한 선점합니다.

액세스 제어 규칙 1: VLAN 1 URL www.example.com 허용
액세스 제어 규칙 2: VLAN 1 URL www.example.com 허용

후속 규칙은 조건이 다른 경우 사전 대응되지 않습니다.

액세스 제어 규칙 1: VLAN 1 URL www.example.com 허용
액세스 제어 규칙 2: VLAN 2 URL www.example.com 허용

규칙은 모든 설정 조건이 동일한 후속 규칙을 선점합니다.

QoS 규칙 1: VLAN 1 URL www.netflix.com 속도 제한
QoS 규칙 2: VLAN 1 URL www.netflix.com 속도 제한

조건이 다른 경우 후속 규칙의 선점이 발생하지 않습니다.

QoS 규칙 1: VLAN 1 URL www.netflix.com 속도 제한
QoS 규칙 2: VLAN 2 URL www.netflix.com 속도 제한

예: 사전 대응을 방지하기 위해 **SSL** 규칙 순서 지정

예를 들어 신뢰받는 CA(Good CA)에서 악성 엔티티(Bad CA)에 CA 인증서를 잘못 발급했지만 아직 그 인증서를 폐기하지 않았습니다. 신뢰할 수 없는 CA에서 발행한 인증서로 암호화된 트래픽을 차단하지만 신뢰할 수 있는 CA의 신뢰 체인의 트래픽은 허용하는 SSL 정책을 사용하려 합니다. CA 인증서 및 모든 중간 CA 인증서를 업로드한 후 다음 순서에 따라 규칙이 포함된 SSL 정책을 구성합니다.

SSL 규칙 1: 발급자 차단 CN=www.badca.com
SSL 규칙 2: 발급자 암호 해독 안 함 CN=www.goodca.com

규칙을 반대로 설정할 경우 불량 CA가 신뢰하는 트래픽을 포함해 우수한 CA가 신뢰하는 모든 트래픽을 우선 일치시킵니다. 어떤 트래픽도 이후의 불량 CA 규칙에 일치시키지 않으므로 악성 트래픽이 차단되지 않고 허용될 수 있습니다.

규칙 작업 및 규칙 순서

규칙의 작업은 시스템에서 일치하는 트래픽을 처리하는 방법을 결정합니다. 추가로 트래픽 처리를 수행하거나 확인하여 리소스를 많이 소모하는 규칙 앞에 그렇지 않은 규칙을 배치하면 성능이 향상됩니다. 시스템은 검사 대상이었던 트래픽으로 전환할 수 있습니다.

다음 예는 여러 정책에서 중요 규칙이 없고 사전 대응이 문제가 되지 않는 규칙 집합 중 규칙 순서를 정하는 방법을 나타냅니다.

규칙이 애플리케이션 조건을 포함하는 경우에도 애플리케이션 제어 구성 모범 사례, 541 페이지의 내용을 참조하십시오.

최적의 순서: **SSL** 규칙

암호 해독뿐 아니라 암호 해독된 트래픽의 추가 분석에도 리소스를 필요로 합니다. 트래픽의 암호를 해독하는 SSL 규칙을 나중에 배치하십시오.

1. 모니터링 - 일치하는 연결을 기록하지만 트래픽에 다른 작업을 수행하지 않는 규칙
2. 차단, 재설정과 함께 차단 - 추가 검사 없이 트래픽을 차단하는 규칙입니다.
3. 암호 해독 안 함 - 암호화된 트래픽의 암호를 해독하지 않고 암호화된 세션을 액세스 제어 규칙에 전달하는 규칙 이런 세션의 페이로드는 심층 검사 대상이 아닙니다.
4. 암호 해독 - 알려진 키 - 확인된 개인 키로 수신 트래픽을 암호 해독하는 규칙
5. 암호 해독 - 다시 서명 - 서버 인증서에 다시 서명을 하여 발신 트래픽을 암호 해독하는 규칙

최적의 순서: 액세스 제어 규칙

특히 여러 사용자 정의 침입 정책과 변수 집합을 사용하는 경우 침입, 파일, 악성코드 검사 시 리소스를 사용합니다. 심층 검사를 마지막으로 호출하는 액세스 제어 규칙을 배치합니다.

1. 모니터링 - 일치하는 연결을 기록하지만 트래픽에 다른 작업을 수행하지 않는 규칙 (액세스 제어 규칙 모니터 작업, 1658 페이지에서 중요 예외 및 주의 사항을 확인하십시오.)

2. 신뢰, 차단, 재설정과 함께 차단 - 추가 검사 없이 트래픽을 처리하는 규칙 신뢰할 수 있는 트래픽에는 ID 정책에 적용된 인증 요건 및 속도 제한이 적용됩니다.
3. 허용, 상호 작용 차단(심층 검사 없음) - 트래픽을 추가로 검사하지 않지만 검색을 허용하는 규칙 허용된 트래픽에는 ID 정책에 적용된 인증 요건 및 속도 제한이 적용됩니다.
4. 허용, 상호 작용 차단(심층 검사) - 금지된 파일, 악성코드, 익스플로잇에 대해 심층 검사를 수행하는 파일 또는 침입 정책과 관련된 규칙

콘텐츠 제한 규칙 순서

SSL 및 액세스 제어 정책 둘 다에서 규칙 사전 대응을 방지하려면 YouTube 제한 관리 규칙을 안전 검색 제한 관리 규칙 위에 배치합니다.

액세스 제어 규칙에 대해 Safe Search를 활성화하면 시스템은 선택된 애플리케이션 및 필터 목록에 검색 엔진 카테고리를 추가합니다. 이 애플리케이션 카테고리에는 YouTube가 포함됩니다. 그러므로 평가 우선 순위가 더 높은 규칙에서 YouTube EDU를 활성화하는 경우가 아니면 YouTube 트래픽은 안전 검색 규칙과 일치하게 됩니다.

`safesearch supported` 필터가 포함된 SSL 규칙을 평가 순서에서 특정 YouTube 애플리케이션 조건이 포함된 SSL 규칙보다 상위 위치에 배치하는 경우 이와 유사한 규칙 사전 대응이 수행됩니다.

애플리케이션 규칙 순서

애플리케이션 조건이 포함된 규칙은 목록에서 낮은 순서로 이동할 경우 트래픽과 일치할 가능성이 높습니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

자세한 정보와 예시는 애플리케이션 제어 구성 모범 사례, 541 페이지 및 애플리케이션 제어 모범 사례, 539 페이지의 내용을 참조하십시오.

SSL 규칙 순서

일반적으로 특정 조건(IP 주소 및 네트워크 등)을 사용하는 규칙은 일반 조건(애플리케이션 등)을 사용하는 규칙 앞에 배치합니다.

인증서 고정 사이트의 트래픽을 허용

일부 애플리케이션이 *TLS/SSL* 피닝또는 인증서 피닝이라는 기법을 사용하는데 이 기법에서는 원본 서버 인증서 지문이 애플리케이션 자체에 내장됩니다. 따라서 TLS/SSL 규칙을 **Decrypt - Resign(**암호 해독 - 재서명**)** 작업으로 구성하는 경우, 애플리케이션이 매니지드 디바이스로부터 재서명된 인증서를 수신할 때 확인이 실패하고 연결이 중단됩니다.

TLS/SSL 피닝이 발생하고 있는지 확인하려면, Facebook 같은 모바일 애플리케이션에 로그인을 시도합니다. 네트워크 연결 오류가 표시되는 경우, 웹 브라우저를 사용하여 로그인 합니다. (예를 들어, Facebook 모바일 애플리케이션에는 로그인이 불가능하더라도 Safari나 Chrome을 사용하여 Facebook에 로그인할 수 있습니다.) Firepower Management Center 연결 이벤트를 TLS/SSL 피닝의 추가 증거로 사용할 수 있습니다.

참고 TLS/SSL 피닝은 모바일 애플리케이션에 국한되지 않습니다.

이 트래픽을 허용하려면 암호 해독 안 함 작업을 사용해 SSL 규칙이 서버 인증서 공통 이름 또는 고유 이름과 일치하도록 설정합니다. SSL 정책에서 트래픽과 일치하는 모든 암호 해독 - 다시 서명 규칙 앞에 배치합니다. 웹사이트에 정상적으로 연결한 후 클라이언트 브라우저에서 고정된 인증서를 검색할 수 있습니다. 연결의 성공/실패 여부와 관계없이 기록된 연결 이벤트에서도 인증서를 확인할 수 있습니다.

SSL 정책이 우회되는 상황

액세스 컨트롤 규칙이 신뢰, 차단 또는 리셋과 함께 차단 동작과 일치하는 연결인 경우 SSL 정책이 우회됩니다.

- 보안 영역, 네트워크, 지리위치 및 포트를 트래픽 일치 기준으로만 사용하는 경우.
- 검사가 필요한 다른 규칙(예: 애플리케이션이나 URL을 기준으로 하는 연결과 일치하는 규칙) 앞에 오거나 침입 또는 파일 검사를 적용하는 규칙을 허용하는 경우.

URL 규칙 순서

가장 효과적인 URL 일치를 위해 특히 URL 규칙이 차단 규칙이고 다른 규칙이 다음 조건을 모두 만족하는 경우 다른 규칙 전에 URL 조건을 포함하는 규칙을 배치합니다.

- 애플리케이션 조건을 포함합니다.
- 검사할 트래픽은 암호화되어야 합니다.

규칙에 대해 예외를 설정하는 경우 다른 규칙 위에 예외를 배치합니다.

규칙 간소화 및 집중모범 사례

간소화: 과잉 구성하지 않습니다.

하나의 조건이 처리하려는 트래픽과 일치시키는 데 충분하다면 두 조건을 사용하지 마십시오.

개별 규칙 기준을 최소화합니다. 규칙 조건에 최소한의 개별 요소를 사용합니다. 예를 들어 네트워크 조건에서 개별 IP 주소 대신 IP 주소 블록을 사용합니다.

요소를 개체에 결합하는 것은 성능을 개선하지 않습니다. 예를 들어, 50개의 개별적인 IP 주소를 포함하는 네트워크 개체를 사용하면 사용자가 얻을 수 있는 이점은 성능에 관한 것이 아닌 구성적인 것에 한정되며, 조건에 해당 IP 주소를 개별적으로 포함하는 것입니다.

애플리케이션 탐지와 관련한 권장 사항은 애플리케이션 제어 구성 모범 사례, 541 페이지을 참조하십시오.

집중: 특히 인터페이스에서 리소스를 많이 사용하는 규칙을 구체적으로 제한

규칙 조건을 최대한 사용하여 리소스를 많이 사용하는 규칙을 트래픽을 구체적으로 정의합니다. 폭넓은 조건을 가진 규칙이 여러 유형의 트래픽에 일치하며 추후 더 많은 특정 규칙에 사전 정의될 수 있기 때문에 집중 규칙이 중요합니다. 리소스를 많이 사용하는 규칙은 다음과 같습니다.

- 트래픽의 암호를 해독하는 SSL 규칙 - 암호 해독뿐 아니라 암호 해독된 트래픽의 추가 분석에도 리소스가 필요합니다. 집중하여 가능한 곳에서 암호화된 트래픽을 해독하지 않도록 선택 또는 차단합니다.
- 심화 검사를 호출하는 액세스 제어 규칙 - 특히 여러 사용자 정의 침입 정책 및 변수 세트를 사용하는 경우 침입, 파일, 악성코드 검사에 리소스를 사용합니다. 필요한 경우에만 심화 검사를 호출합니다.

최대 성능 향상을 위해 인터페이스로 규칙을 제한합니다. 규칙이 모든 디바이스의 인터페이스를 제외할 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

최대 액세스 제어 규칙 및 침입 정책 개수

대상 디바이스에서 지원하는 최대 액세스 제어 규칙 또는 침입 정책 수는 정책 복잡성, 물리적 메모리 및 디바이스의 프로세서 수 등 여러 요인에 따라 달라집니다.

장치에서 지원되는 최대 한도를 초과하면 액세스 제어 정책을 구축할 수 없으며 재평가가 필요합니다.

침입 정책에 대한 지침:

액세스 제어 정책에서는 하나의 침입 정책을 각 허용 및 인터랙티브 차단 규칙 및 기본 작업과 연결할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다.

침입 정책 또는 변수 집합을 통합하여 단일한 침입 정책 변수 집합 쌍을 여러 개의 액세스 제어 규칙과 연결할 수 있습니다. 일부 디바이스에서 모든 침입 정책에 단일 변수 집합만 사용할 수 있거나 전체 디바이스에 단일 침입 정책-변수 집합 쌍을 사용할 수 있습니다.

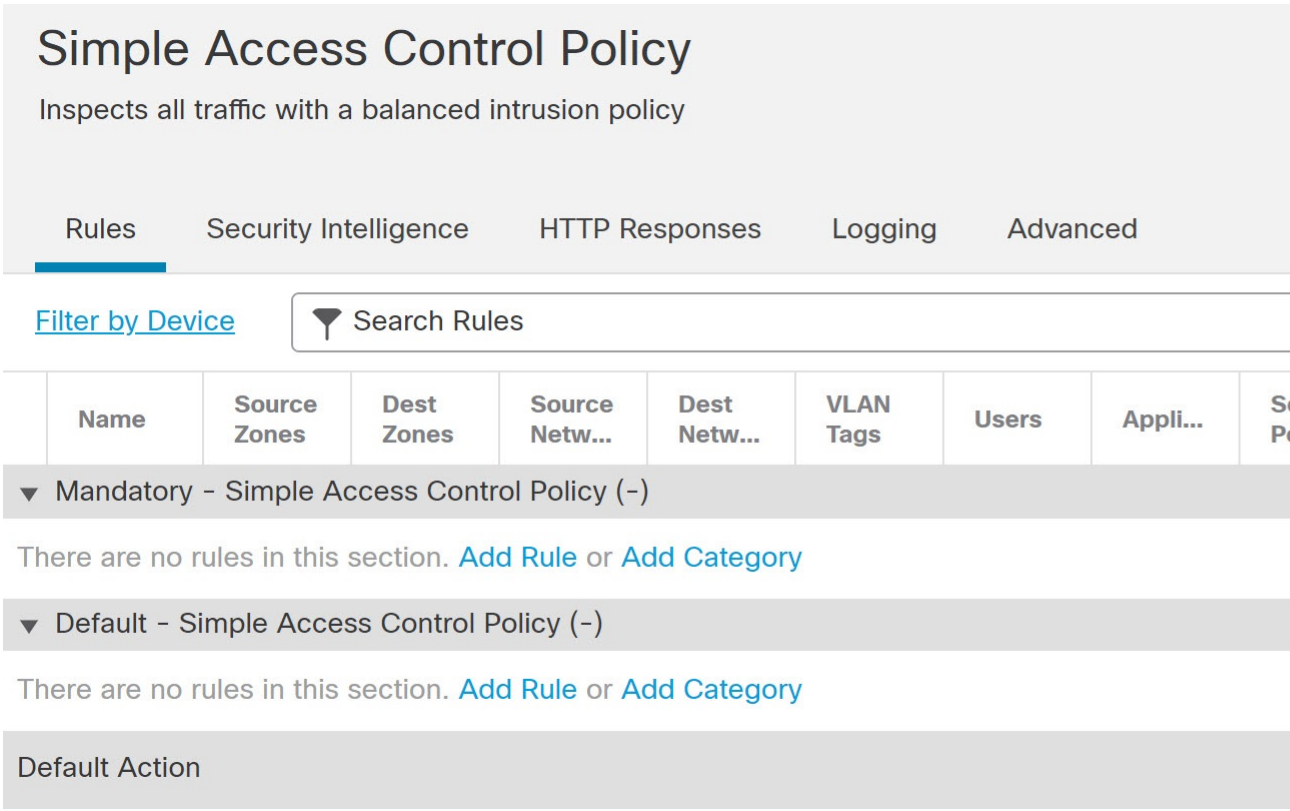
60 장

액세스 제어 정책

다음 주제에서는 액세스 제어 정책을 사용하는 방법에 대해 설명합니다.

- 액세스 제어 정책 구성 요소, 1626 페이지
- 액세스 제어 정책 요구 사항 및 사전 요건, 1628 페이지
- 액세스 제어 정책 관리, 1628 페이지
- 시스템 생성 액세스 제어 정책, 1629 페이지
- 기본 액세스 제어 정책 만들기, 1629 페이지
- 액세스 제어 정책 수정, 1630 페이지
- 액세스 제어 정책 상속 관리, 1632 페이지
- 액세스 제어 정책에 대한 대상 디바이스 설정, 1635 페이지
- 액세스 제어 정책용 로깅 설정, 1636 페이지
- 액세스 제어 정책 고급 설정, 1637 페이지
- 정책 적중 횟수 보기, 1642 페이지
- 액세스 제어 정책 히스토리, 1643 페이지

액세스 제어 정책 구성 요소



이름 및 설명

각 액세스 제어 정책에는 고유한 이름이 있어야 합니다. 설명은 선택 사항입니다.

Inheritance Settings(상속 설정**)**

정책 상속을 사용하면 액세스 계층 제어 정책을 생성할 수 있습니다. 상위(또는 기본) 정책은 하위 항목에 대한 기본 설정을 정의하고 시행하며, 이는 특히 다중 도메인 구축에서 유용합니다.

정책 상속 설정을 통해 기본 정책을 선택할 수 있습니다. 현재 정책의 설정을 잠금 처리하여 하위 항목이 강제로 상속하도록 설정할 수도 있습니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

Policy Assignment(정책 할당**)**

각 액세스 제어 정책은 이를 사용하는 디바이스를 식별합니다. 각 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 다중 도메인 구축에서는 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다.

규칙

액세스 제어 규칙은 네트워크 트래픽 처리에 대한 세분화된 방법을 제공합니다. 액세스 제어 정책의 규칙은 상위 정책에서 상속된 규칙을 포함하여 1부터 번호가 매겨집니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 액세스 제어 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 모든 규칙의 조건이 트래픽과 일치하는 첫 번째 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 조건은 단순하거나 복잡할 수 있으며, 조건의 사용은 특정 라이선스에 따라 달라지는 경우가 많습니다.

기본 작업

기본 작업은 시스템이 다른 액세스 제어 구성에 의해 처리되지 않는 트래픽을 처리하고 기록하는 방법을 결정합니다. 기본 작업을 사용하여 추가 검사 없이 모든 트래픽을 차단하거나 신뢰할 수 있고, 침입 및 검색 데이터 트래픽을 검사할 수 있습니다.

액세스 제어 정책은 상위 정책에서 기본 작업을 상속할 수 있지만 이 상속을 적용할 수는 없습니다.

보안 인텔리전스

보안 인텔리전스는 악성 인터넷 콘텐츠에 대한 1차 방어선입니다. 이 기능을 사용하여 최신 IP 주소, URL, 도메인 이름 평판 인텔리전스에 따라 연결을 차단할 수 있습니다. 중요 리소스로 지속적으로 액세스할 수 있도록 차단 목록 항목을 사용자 지정 차단 안 함 목록 항목으로 재정의할 수 있습니다.

HTTP 응답

시스템이 사용자의 웹 사이트 요청을 차단하면 일반 시스템 제공 응답 페이지 또는 사용자 정의 페이지를 표시할 수 있습니다. 또한 사용자에게 경고하는 페이지를 표시할 수도 있지만 원래 요청한 사이트를 계속 진행할 수 있습니다.

로깅

액세스 제어 정책 로깅에 대한 설정을 통해 현재 액세스 제어 정책에 대한 기본 syslog 대상을 구성할 수 있습니다. 포함된 규칙 및 정책의 syslog 대상 설정이 사용자 정의 설정으로 명시적으로 무시되지 않는 한 설정은 액세스 제어 정책 및 포함된 모든 SSL, 사전 필터 및 침입 정책에 적용됩니다.

고급 액세스 제어 옵션

고급 액세스 제어 정책 설정은 일반적으로 약간의 변경이 필요하거나 변경이 필요하지 않습니다. 종종 기본 설정이 적합합니다. 수정할 수있는 고급 설정에는 트래픽 사전 처리, SSL 검사, ID 및 다양한 성능 옵션이 포함됩니다.

관련 항목

규칙 관리: 일반 특성, 523 페이지

액세스 제어 정책 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

액세스 제어 정책 관리

Firepower System을 사용하면 시스템에서 제공한 액세스 제어 정책을 편집하고 사용자 정의 액세스 제어 정책을 생성할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** 을(를) 선택합니다.

단계 **2** 액세스 제어 정책 관리

- 복사- 복사 ( )를 클릭합니다.
- 생성 - **New Policy(**새 정책**)**을 클릭합니다(기본 액세스 제어 정책 만들기, 1629 페이지 참조).
- 삭제- 삭제( )를 클릭합니다.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- 수정-수정( )를 클릭합니다. 액세스 제어 정책 수정, 1630 페이지의 내용을 참조하십시오.
- 상속 - 정책의 계층 보기를 확장하기 위해 하위 계층이 포함된 정책 옆의 더하기 아이콘을 클릭합니다.

- 가져오기/내보내기 - **Import/Explort(**가져오기/내보내기**)**를 클릭합니다. 구성 가져오기 및 내보내기, 237 페이지를 참조하십시오.
- 보고서- 보고서( )를 클릭합니다. 현재 정책 보고서 생성, 515 페이지의 내용을 참조하십시오.

관련 항목

만료된 정책, 516 페이지

시스템 생성 액세스 제어 정책

사용자 디바이스의 초기 설정에 따라 시스템 제공 정책에 다음이 포함될 수 있습니다.

- 기본 액세스 제어 - 추가 검사 없이 모든 트래픽을 차단합니다.
- 기본 침입 예방 - 모든 트래픽을 허용하지만 균형 보안 및 연결성 침입 정책과 기본 침입 변수 집합을 검사합니다.
- 기본 네트워크 검색 - 검색 데이터를 검사하는 동안 모든 트래픽을 허용하지만 침입과 익스플로잇은 허용하지 않습니다.

기본 액세스 제어 정책 만들기

신규 액세스 제어 정책을 만들 때 적어도 하나의 기본 작업을 선택해야 합니다.

대부분의 경우 기본 작업이 처리한 연결 기록은 처음으로 비활성화됩니다. 다중 도메인 구축 시 하위 정책을 생성하는 경우 예외가 발생합니다. 이 경우 시스템은 상속된 기본 작업의 기록 설정에 따라 연결 기록을 활성화합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** 을(를) 선택합니다.

단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력하고, 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **4** 필요한 경우 기본 정책 선택 드롭다운 목록에서 기본 정책을 선택합니다.

도메인에 액세스 제어 정책이 강제 적용되는 경우 이 단계는 선택 사항이 아닙니다. 기본 정책으로는 강제 적용된 정책 또는 그 하위 정책 중 하나를 선택해야 합니다.

단계 **5** 초기 **Default Action(**기본 작업**)**을 지정합니다.

- 기본 정책을 선택한 경우 새 정책은 기본 작업을 상속합니다. 여기에서 변경할 수 없습니다.
- **Block all traffic(**모든 트래픽을 차단**)**은 **Access Control: Block All Traffic(**액세스 제어**:** 모든 트래픽을 차단**)** 기본 작업을 통해 정책을 생성합니다.

- **Intrusion Prevention(**침입 방지**)**은 기본 침입 변수 집합과 연결된 **Intrusion Prevention: Balanced Security and Connectivity(**침입 방지**:** 균형 잡힌 보안 및 연결성**)** 기본 작업을 통해 정책을 생성합니다.
- **Network Discovery(**네트워크 검색**)**을 선택하면 **Network Discovery Only(**네트워크 검색 전용**)** 기본 작업이 포함된 정책을 생성합니다.

팁 기본적으로 모든 트래픽을 신뢰하거나 기본 정책을 선택하지만 기본 작업을 상속하지 않을 경우 기본 작업을 나중에 변경할 수 있습니다.

단계 **6** 필요에 따라 정책을 구축할 **Available Devices(**사용 가능한 디바이스**)**를 선택하고 **Add to Policy(**정책에 추가**)**(또는 드래그 앤 드롭)을 클릭하여 선택한 디바이스를 추가합니다. 표시되는 디바이스의 범위를 좁히려면 **Search(**검색**)** 필드에 검색 문자열을 입력합니다.

이 정책을 즉시 구축하려는 경우 이 단계를 수행해야 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 필요한 경우, 액세스 제어 정책 수정, 1630 페이지의 설명에 따라 새 정책을 설정합니다.
- 선택적으로, 애플리케이션 및 URL 필터링이 TLS 1.3 지원 세션에서 예상대로 수행할 수 있도록 액세스 제어 정책의 고급 설정에서 TLS 서버 ID를 구성합니다. 자세한 내용은 액세스 제어 정책 고급 설정, 1637 페이지을 참조해 주십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Access Control Policy Default Action(액세스 제어 정책 기본 작업), 1610 페이지
액세스 제어 정책에 대한 대상 디바이스 설정, 1635 페이지

액세스 제어 정책 수정

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장한 변경사항이 유지됩니다. 편의상 시스템에는 현재 각 정책을 수정하고 있는 사용자(있는 경우)에 대한 정보가 표시됩니다. 세션의 개인 정보를 보호하기 위해 정책 편집기에서 30분 동안 아무런 작업을 하지 않으면 경고가 표시됩니다. 60분이 지나면 시스템에서 변경사항을 삭제합니다.

참고 현재 도메인에서 생성된 액세스 제어 정책만 편집할 수 있습니다. 또한 상위 액세스 제어 정책에 의해 잠긴 설정은 편집할 수 없습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** 를 선택합니다.

단계 **2** 편집하려는 액세스 제어 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 기존 액세스 제어 정책을 편집합니다.

팁 여러 규칙을 Shift-클릭하거나 Control-클릭한 다음 마우스 오른쪽 버튼을 클릭하고 Edit(편집)을 선택하여 여러 규칙을 한 번에 편집할 수 있습니다. 대량 편집을 통해 규칙을 활성화 및 비활성화하고, 규칙 작업을 선택하고, 대부분의 검사 및 로깅 설정을 설정할 수 있습니다.

설정:

- 이름 및 설명 - 필드를 클릭하고 새 정보를 입력합니다.
- Default Action - **Default Action(**기본 작업**)** 드롭다운 목록에서 값을 선택합니다.
- Default Action Variable Set - **Intrusion Prevention(**침입 방지**)** 기본 작업과 관련된 변수 집합을 변경하려면 변수( )를 클릭합니다. 이때 나타나는 팝업 창에서 새로운 변수 집합을 선택하고 **OK(**확인**)**를 클릭합니다. 사용자는 또한 수정( )을 클릭하여 선택한 변수 집합을 새 창에서 수정할 수 있습니다. 자세한 내용은 변수 관리, 593 페이지를 참고하십시오.
- Default Action Logging - 기본 작업에 의해 처리된 연결에 대한 로깅을 설정하려면 로깅( )을 클릭합니다. 정책 기본 작업으로 연결 로깅, 2873 페이지 섹션을 참조하십시오.
- HTTP Responses - 시스템이 웹사이트 요청을 차단할 때 브라우저에 표시되는 내용을 지정하려면 **HTTP Responses(HTTP** 응답**)**를 클릭합니다. HTTP 응답 페이지 선택, 1691 페이지 섹션을 참조하십시오.
- Inheritance: Change Base Policy - 이 정책에 대한 기본 액세스 제어 정책을 변경하려면 **Inheritance Settings(**상속 설정**)**를 클릭합니다. 기본 액세스 제어 정책 선택, 1633 페이지 섹션을 참조하십시오.
- Inheritance: Lock Settings in Descendants - 이 정책의 설정을 하위 정책에 적용하려면 **Inheritance Settings(**상속 설정**)**를 클릭합니다. 하위 액세스 제어 정책의 설정 잠금, 1634 페이지 섹션을 참조하십시오.
- Policy Assignment: Targets - 이 정책의 대상이 되는 매니지드 디바이스를 식별하려면 **Policy Assignment(**정책 할당**)**를 클릭합니다. 액세스 제어 정책에 대한 대상 디바이스 설정, 1635 페이지 섹션을 참조하십시오.
- Policy Assignment: Required in Domains - 이 정책을 하위 도메인에 적용하려면 **Policy Assignment(**정책 할당**)**를 클릭합니다. 도메인에 액세스 제어 정책 필요, 1635 페이지 섹션을 참조하십시오.
- Rules - 액세스 제어 규칙을 관리하고 침입 및 파일 정책을 사용하여 악의적인 트래픽을 검사 및 차단하려면 **Rules(**규칙**)**를 클릭합니다. 액세스 제어 규칙 생성 및 수정, 1651 페이지 섹션을 참조하십시오.

- Rule Conflicts - 규칙 충돌 경고를 표시하려면 **Show rule conflicts(**규칙 충돌 표시**)**를 활성화합니다. 이전 규칙이 항상 트래픽과 먼저 일치하므로 특정 규칙이 트래픽과 일치하지 않으면 충돌이 발생합니다. 규칙 충돌을 판별하는 것은 리소스가 많이 사용될 수 있기 때문에 표시하는 데 시간이 걸릴 수 있습니다. 자세한 내용은 규칙 순서 지정 모범 사례, 1618 페이지를 참고하십시오.
- Security Intelligence - 최신 평판 인텔리전스에 따라 즉시 연결을 차단하려면 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다. 보안 인텔리전스 설정, 1698 페이지 섹션을 참조하십시오.
- Advanced Options - 사전 처리, SSL 검사, ID, 성능 및 기타 고급 옵션을 설정하려면 **Advanced(**고급**)**를 클릭합니다. 액세스 제어 정책 고급 설정, 1637 페이지 섹션을 참조하십시오.
- Warnings - 액세스 제어 정책(및 해당 하위 항목 및 관련 정책)의 경고 또는 오류 목록을 보려면 **Show Warnings(**경고 표시**)**를 클릭합니다. 경고 및 오류는 트래픽 분석 및 흐름에 악영향을 미치거나 정책 배포를 방해할 수 있는 구성을 표시합니다. 경고가 없는 경우, 경고 표시가 나타나지 않습니다. 규칙 충돌 경고를 표시하려면 **Show rule conflicts(**규칙 충돌 표시**)**를 활성화합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

규칙 및 기타 정책 경고, 554 페이지
파일 및 침입 정책을 사용한 심층 검사, 1612 페이지

액세스 제어 정책 상속 관리

시작하기 전에

상속이 어떻게 작동하는지 이해합니다. 액세스 제어 정책 상속, 1615 페이지 및 하위 항목을 참조하십시오.

프로시저

단계 **1** 상속 설정을 변경하려는 액세스 제어 정책을 편집합니다. 액세스 제어 정책 수정, 1630 페이지 섹션을 참조하십시오.

단계 **2** 정책 상속 관리:

- Change Base Policy - 이 정책에 대한 기본 액세스 제어 정책을 변경하려면 기본 액세스 제어 정책 선택, 1633 페이지에 설명된 대로 **Inheritance Settings(**상속 설정**)**를 클릭합니다.
- Lock Settings in Descendants - 이 정책의 설정을 하위 정책에 적용하려면 하위 액세스 제어 정책의 설정 잠금, 1634 페이지에 설명된 대로 **Inheritance Settings(**상속 설정**)**를 클릭합니다.

- Required in Domains - 이 정책을 하위 도메인에 적용하려면 도메인에 액세스 제어 정책 필요, 1635 페이지에 설명된 대로 **Policy Assignment(**정책 할당**)**를 클릭합니다.
- Inherit Settings from Base Policy - 기본 액세스 제어 정책에서 설정을 상속하려면 **Security Intelligence(**보안 인텔리전스**)**, **HTTP Responses(HTTP** 응답**)** 또는 **Advanced(**고급**)**을 클릭하고 기본 정책에서 액세스 제어 정책 설정 상속, 1633 페이지의 지침에 따라 진행합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

기본 액세스 제어 정책 선택

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	Any(모든)	Any(모든)	Any(모든)	관리자/액세스 관리자/네트워크 관리자

하나의 액세스 제어 정책을 다른 정책에 대한 기본(상위)으로 사용할 수 있습니다. 잠금 해제된 설정을 변경할 수 있지만 기본적으로 하위 정책은 기본 정책에서 설정을 상속받습니다.

현재 액세스 제어 정책에 대한 기본 정책을 변경하면 시스템은 새 기본 정책에서 잠긴 설정으로 현재 정책을 갱신합니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Inheritance Settings(**상속 설정**)**를 클릭합니다.

단계 **2** **Select Base Policy(**기본 정책 선택**)** 드롭다운 목록에서 정책을 선택합니다.

다중 도메인 구축의 경우 현재 도메인에서 액세스 제어 정책이 필요할 수 있습니다. 기본 정책으로 시행된 정책 또는 그 하위 항목 중 하나만 선택할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

기본 정책에서 액세스 제어 정책 설정 상속

새 하위 정책은 기본 정책에서 많은 설정을 상속받습니다. 이 설정이 기본 정책에서 잠금 해제되어 있으면 재정의할 수 있습니다.

나중에 기본 정책의 설정을 다시 상속하면 시스템은 기본 정책의 설정을 표시하고 컨트롤을 흐릿하게 표시합니다. 하지만 시스템은 사용자가 변경한 내용을 저장하고 상속을 다시 사용하지 않도록 설정하면 복원합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**, **HTTP Responses(HTTP** 응답**)** 또는 **Advanced(**고급**)**을 클릭합니다.

단계 **2** 상속할 각 설정에 대해 **Inherit from base policy(**상속 정책에서 상속**)** 확인란을 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

하위 액세스 제어 정책의 설정 잠금

모든 하위 정책에 설정을 적용하려면 액세스 제어 정책에서 설정을 잠급니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

설정을 잠그면 시스템은 하위 정책에서 이미 적용된 재정의를 저장하므로 설정을 다시 해제하면 재정의를 복원할 수 있습니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Inheritance Settings(**상속 설정**)**를 클릭합니다.

단계 **2** Child Policy Inheritance Settings(하위 정책 상속 설정) 영역에서 잠그려는 설정을 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **3** **OK(**확인**)**를 클릭하여 상속 설정을 저장합니다.

단계 **4** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

도메인에 액세스 제어 정책 필요

도메인의 모든 디바이스가 동일한 기본 액세스 제어 정책 또는 그 하위 정책 중 하나를 사용하도록 요구할 수 있습니다.

시작하기 전에

- 전역 도메인 이외 하나 이상의 도메인을 구성합니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Policy Assignments(**정책 할당**)**를 클릭합니다.

단계 **2** **Required on Domains(**도메인에 대한 필수 요소**)**를 클릭합니다.

단계 **3** 도메인 목록을 구축합니다.

- Add(추가) - 현재 액세스 제어 정책을 적용할 도메인을 선택한 다음 **Add(**추가**)**를 클릭하거나 선택한 도메인 목록으로 끌어다 놓습니다.
- Delete(삭제) - 리프 도메인 옆에 있는 삭제( )을 클릭하거나 상위 도메인을 오른쪽 클릭하고 **Delete Selected(**선택 항목 삭제**)**를 선택합니다.
- Search(검색) - 검색 필드에 검색 문자열을 입력합니다. 지우기( )을 클릭하여 검색 내용을 삭제합니다.

단계 **4** **OK(**확인**)**를 클릭하여 도메인 적용 설정을 저장합니다.

단계 **5** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 제어 정책에 대한 대상 디바이스 설정

액세스 제어 정책은 이를 사용하는 디바이스를 지정합니다. 각 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 다중 도메인 구축에서는 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Policy Assignments(**정책 할당**)**를 클릭합니다.

단계 **2** **Targeted Devices(**대상 디바이스**)**에 대상 목록을 만듭니다.

- Add(추가) - 하나 이상의 **Available Devices(**사용 가능한 디바이스**)**를 선택한 다음 **Add to Policy(**정책에 추가**)**를 클릭하거나 **Selected Devices(**선택한 디바이스**)** 목록으로 드래그앤 드롭합니다.
- Delete(삭제) - 단일 디바이스 옆에 있는 삭제( )을 클릭하거나 여러 디바이스를 선택하고 오른쪽 클릭한 다음 **Delete Selected(**선택 항목 삭제**)**를 선택합니다.
- Search(검색) - 검색 필드에 검색 문자열을 입력합니다. 지우기( )을 클릭하여 검색 내용을 삭제합니다.

Impacted Devices(영향을 받는 디바이스**)**에서 시스템은 할당된 액세스 제어 정책이 현재 정책의 하위 디바이스를 나열합니다. 현재 정책의 변경 사항은 이러한 디바이스에 영향을 줍니다.

단계 **3** 필요에 따라 **Required on Domains(**도메인에 대한 필수 요소**)**를 클릭하여 선택한 하위 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다. 도메인에 액세스 제어 정책 필요, 1635 페이지의 내용을 참조하십시오.

단계 **4** **OK(**확인**)**를 클릭하여 대상 디바이스 설정을 저장합니다.

단계 **5** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 제어 정책용 로깅 설정

액세스 제어 정책 로깅에 대한 설정을 통해 현재 액세스 제어 정책에 대한 기본 syslog 대상 및 syslog 알림을 구성할 수 있습니다. 포함된 규칙 및 정책의 syslog 대상 설정이 사용자 정의 설정으로 명시적으로 무시되지 않는 한 설정은 액세스 제어 정책 및 포함된 모든 SSL, 사전 필터 및 침입 정책에 적용됩니다.

기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화됩니다.

기본 **Syslog** 설정

Send using specific syslog alert(특정 **syslog** 알림을 사용하여 전송**)**: 이 옵션을 선택하면 Syslog 알림 응답 생성, 2684 페이지의 지침에 따라 구성된 대로 선택한 syslog 알림을 기반으로 이벤트가 전송됩니다. 목록에서 syslog 알림을 선택하거나 이름, 로깅 호스트, 포트, 기능 및 심각도를 지정하여 syslog 알림을 추가할 수 있습니다. 자세한 내용은 침입 시스템 로그 알림에 대한 시설 및 Severities(심각도), 2695 페이지를 참고하십시오. 이 옵션은 모든 디바이스에 적용할 수 있습니다.

FTD 6.3 이상**:** 디바이스에 구축된 **FTD Platform Settings** 정책에 구성된 **syslog** 설정 사용: 이 옵션을 선택하고 심각도를 선택하면 선택한 심각도와 함께 연결 또는 침입 이벤트가 플랫폼 설정에서 구성된 syslog 수집기로 전송됩니다. 이 옵션을 사용하면 플랫폼 설정에서 구성하고 액세스 제어 정책의 설정을 다시 사용하여 syslog 구성을 통합할 수 있습니다. 이 섹션에서 선택한 심각도는 모든 연결 및 침입 이벤트에 적용됩니다. 기본 심각도는 ALERT입니다.

이 옵션은 Firepower Threat Defense 디바이스 6.3 이상에만 적용됩니다.

참고 두 옵션을 선택하는 경우 옵션의 동작이 변경됩니다. 동적 요약 섹션에는 선택 결과가 표시됩니다.

File and Malware Settings(파일 및 악성코드 설정**)**는 일반적으로 syslog 메시지를 보내는 페이지 위쪽의 옵션을 선택한 후에만 적용됩니다.

액세스 제어 정책 고급 설정

고급 액세스 제어 정책 설정은 일반적으로 약간의 변경이 필요하거나 변경이 필요하지 않습니다. 기본 설정은 대부분의 배포에 적합합니다. 액세스 제어 정책의 여러 고급 사전 처리 및 성능 옵션은 침입 규칙 업데이트, 186 페이지에 설명된 규칙 업데이트에 의해 수정될 수 있습니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

주의 트래픽 검사를 일시적으로 중단하는 Snort 프로세스를 재시작하는 고급 설정 수정 목록은 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 510 페이지을 확인하세요. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

일반 설정

옵션	설명
연결 이벤트에 저장하고자 하는 최대 **URL** 문자	사용자가 요청한 각 URL에 저장하는 문자 수를 사용자 정의하려면 긴 URL의 로깅 제한, 2874 페이지을 참고하십시오. 사용자가 최초 차단을 건너뛴 후 웹사이트를 다시 차단하기 전에 걸린 시간을 맞춤화하려면, 차단된 웹사이트의 사용자 우회 시간 제한 설정, 1693 페이지를 참고하십시오.
인터랙티브 차단을 허용하여 다음 시간**(**초**)** 동안 차단 바이패스	차단된 웹사이트의 사용자 우회 시간 제한 설정, 1693 페이지의 내용을 참조하십시오.

옵션	설명
DNS 트래픽에 대한 평판 시행 활성화	이 기능은 릴리스 **6.7**에서 실험적으로 제공됩니다**.** 따라서 예상대로 작동하지 않을 수 있습니다**.** 프로덕션 환경에서는 사용하지 마십시오**.** Enable this option(이 옵션 활성화) 활성화됩니다. 자세한 내용 및 추가 지침은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타), 1678 페이지 및 하위 주제를 참조하십시오.
정책 적용 중에 트래픽 검사	특정 설정이 Snort 프로세스 재시작을 필요로 하지 않는 경우 구축 설정을 변경할 때 트래픽을 검사하려면 정책 적용 중 트래픽 검사가 기본 값(활성화)로 설정되어 있는지 확인해야 합니다. 이 옵션이 활성화된 경우 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 시나리오, 505 페이지를 참조하십시오.

관련 정책

고급 설정을 사용해 액세스 제어와 하위 정책(SSL, ID,)을 연결하려면 액세스 제어에 다른 정책 연결, 1641 페이지를 참조하십시오.

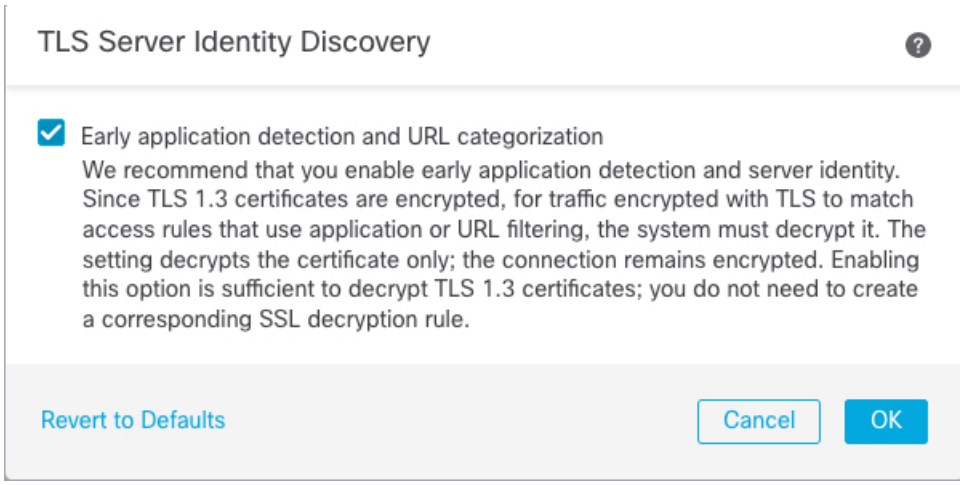
TLS 서버 **ID** 검색

RFC 8446에서 정의한 TLS(Transport Layer Security) 프로토콜 1.3의 최신 버전은 보안 통신을 제공하기 위해 많은 웹 서버에서 선호하는 프로토콜입니다. TLS 1.3 프로토콜은 추가 보안을 위해 서버의 인증서를 암호화하며, 액세스 제어 규칙의 애플리케이션 및 URL 필터링 기준과 일치하는 데 인증서가 필요하므로 Firepower System은 전체 패킷의 암호를 해독하지 않고 서버 인증서를 추출하는 방법을 제공합니다.

다음과 같은 경우, *TLS* 서버 *ID* 검색이라고 하는 기능을 활성화할 수 있습니다.

- SSL 정책을 액세스 제어 정책과 연결
- 액세스 제어 정책에 대한 고급 설정 설정

새 액세스 제어 정책을 생성하면 **Advanced(**고급**)** 탭에 기능 활성화를 고려해야 한다는 경고가 표시됩니다. 다음 그림과 같이 제어 항목을 Enabled(활성화됨)로 이동하면 경고 메시지에서 이를 확인할 수 있습니다.

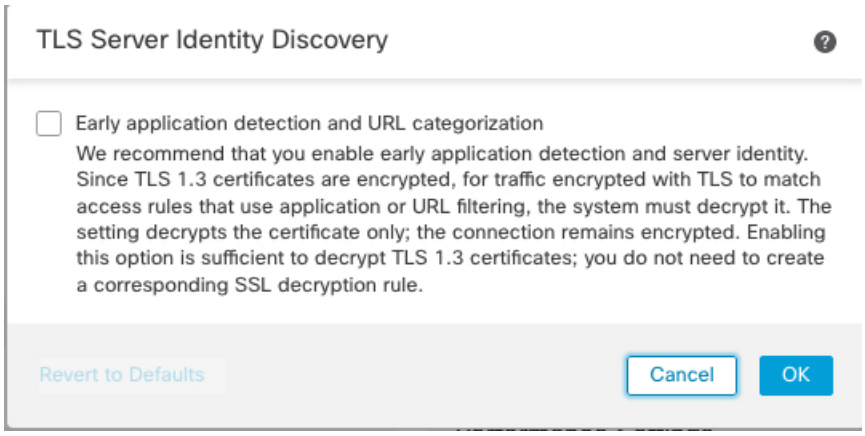


애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.

참고

- TLS 서버 ID 검색은 하드웨어 플랫폼에 따라 성능을 저하시킬 수 있습니다.
- TLS 서버 ID 검색은 인라인 탭 모드 또는 패시브 모드 구축에서 지원되지 않습니다.

다음 그림에는 액세스 제어 정책의 고급 설정에서 TLS 서버 ID 검색을 활성화하는 예가 나와 있습니다.



네트워크 분석 및 침입 정책

고급 네트워크 분석 및 침입 정책을 설정하면 다음을 수행할 수 있습니다.

- 시스템이 트래픽을 검사하는 방법을 정확히 결정하기 전에 통과해야 하는 패킷을 검사하는 데 사용되는 침입 정책 및 관련 변수 세트를 지정합니다.
- 다양한 사전 처리 옵션을 제어하는 액세스 제어 정책의 기본 네트워크 분석 정책을 변경합니다

- 사전 처리 옵션을 특정 보안 영역, 네트워크, VLAN에 맞춰 조정하기 위해 맞춤형 네트워크 분석 규칙과 네트워크 분석 정책을 사용합니다.

자세한 내용은 네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정, 2201 페이지를 참고하십시오.

위협 방어 서비스 정책

특정 트래픽 클래스에 서비스를 적용하기 위해 위협 방어 서비스 정책을 사용할 수 있습니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 컨피그레이션을 만드는 서비스 정책을 사용할 수 있습니다. 이 정책은 Firepower Threat Defense 디바이스에만 적용되며 다른 디바이스 유형에 대해서는 무시됩니다. 서비스 정책 규칙은 액세스 제어 규칙 이후에 적용됩니다. 자세한 내용은 Threat Defense Service 정책, 1249 페이지를 참고하십시오.

파일 및 악성코드 설정

파일 및 악성코드 탐지 성능 및 저장 조정, 1903 페이지은 파일 컨트롤 및 AMP for Networks 에 대한 성능 옵션과 관련된 정보를 제공합니다.

Intelligent Application Bypass Settings(IAB(Intelligent Application Bypass) 설정)

IAB(Intelligent Application Bypass)는 트래픽이 검사 성능 및 플로우 임계값 조합을 초과하는 경우 건너뛸 애플리케이션이나 우회할 테스트를 지정하는 전문가 레벨 컨피그레이션입니다. 자세한 내용은 IAB(Intelligent Application Bypass), 1745 페이지를 참고하십시오.

전송/네트워크 레이어 전처리 설정

고급 전송 및 네트워크 전처리 설정은 액세스 제어 정책을 배포하는 모든 네트워크, 영역 및 VLAN에 글로벌로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다. 자세한 내용은 고급 전송/네트워크 전처리기 설정, 2312 페이지를 참고하십시오.

탐지 향상 설정

고급 탐지 개선 설정을 통해 적응형 프로파일을 사용하여 호스트 운영 체제에 따라 수동 구축에서 패킷 프래그먼트 및 TCP 스트림 리어셈블리를 개선할 수 있습니다. 자세한 내용은 적응형 프로파일, 2371 페이지를 참고하십시오.

성능 설정 및 대기 시간 기반 성능 설정

침입 방지 성능 조정 정보, 2185 페이지는 시도된 침입의 트래픽을 분석할 때 시스템 성능 향상에 관한 정보를 제공합니다.

레이턴시 기반 성능 설정 관련 정보는 패킷 및 침입 규칙 레이턴시 임계값 구성, 2190 페이지을 참조하십시오.

액세스 제어에 다른 정책 연결

액세스 제어 정책의 고급 설정을 사용하여 다음 각각의 하위 정책 중 하나를 액세스 제어 정책과 연결합니다.

- SSL 정책 — SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security)로 암호화된 애플리케이션 레이어 프로토콜 트래픽을 모니터링, 암호 해독, 차단하거나 허용합니다.

  주의 SSL 정책을 추가 또는 제거하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

- ID 정책 — 영역 및 트래픽과 관련된 인증 방법에 따라 사용자 인증을 수행합니다.

시작하기 전에

SSL 정책을 액세스 제어 정책과 연결하기 전에 액세스 제어 정책 고급 설정, 1637 페이지에서 TLS 서버 ID 검색에 대한 정보를 검토합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** 해당하는 Policy Settings(정책 설정) 영역에서 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** 드롭다운 목록에서 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, 표시된 편집 내용을 클릭하여 정책을 수정할 수 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Snort® 재시작 시나리오, 505 페이지

정책 적중 횟수 보기

적중 횟수는 정책 규칙이 일치하는 연결을 트리거한 횟수를 나타냅니다. 이 정보를 사용하여 규칙의 효과를 식별할 수 있습니다. 적중 횟수 정보는 액세스 제어 및 FTD 디바이스에 적용되는 사전 필터 규칙에만 사용할 수 있습니다. 지원되는 정책의 경우 적중 횟수 정보는 정책에 대해 설정된 기본 작업에 대해서도 표시됩니다.

참고

- Firepower Threat Defense 디바이스가 리부팅되면 모든 적중 횟수 정보가 재설정됩니다.
- 디바이스에서 구축이나 작업이 진행 중일 때 적중 횟수 정보를 얻을 수 없습니다.

프로시저

단계 **1** 액세스 제어 또는 사전 필터 정책 페이지로 이동합니다.

단계 **2** 적중 횟수 정보를 확인하려는 정책을 클릭합니다.

단계 **3** 정책 페이지의 오른쪽 상단에서 **Analyze Hit Counts(**적중 횟수 분석**)**를 클릭합니다.

단계 **4** Hit Count(적중 횟수) 페이지에서 **Select a device(**디바이스 선택**)** 드롭다운 목록에서 디바이스를 선택합니다.

참고 이 디바이스에 대한 적중 횟수를 생성하는 것이 처음이 아닌 경우 드롭다운 상자 옆에 마지막으로 조회된 적중 횟수 정보가 표시됩니다. 또한 **Last Deployed(**마지막 구축**)** 시간을 확인하여 최근 정책 변경 내용을 확인합니다.

단계 **5** 적중 횟수 데이터를 얻으려면 현재 **Fetch Current Hit Count(**현재 적중 횟수 검색**)**를 클릭합니다.

선택한 디바이스에 대한 적중 횟수 정보에 처음 액세스하는 것이 아니라면, **Fetch Current Hit Count(**현재 적중 횟수 검색**)** 대신 **Refresh(**새로 고침**)**가 표시됩니다. 최신 적중 횟수 정보를 얻으려면 **Refresh(**새로고침**)**를 클릭하십시오.

단계 **6** (선택 사항) 톱니바퀴( )와 함께 **Filter Rules/Policy(**필터 규칙/정책**)** 상자 또는 **Filter by(**필터 기준**)** 및 **In Last(**마지막**)** 드롭다운 상자를 사용하여 테이블 내의 테이블 및 목록을 사용자 지정합니다.

Filter by(필터 기준**)** 드롭 다운 상자는 중요한 규칙을 식별하는 데 도움이 되는 Hit Rules(적중 규칙) 및 Never Hit Rules(적중 실패 규칙)와 같은 중요한 필터 옵션을 제공합니다. **In Last(**마지막**)** 드롭 다운 상자에서는 사전 설정된 기간을 기준으로 규칙을 필터링하는 옵션을 제공합니다.

단계 **7** (선택 사항) 규칙 이름을 클릭하여 편집하거나 마지막 열의 보기 ( )을 클릭하여 규칙 세부 정보를 봅니다.

규칙 이름을 클릭하면 편집할 수 있는 정책 페이지에서 규칙 이름이 강조 표시됩니다.

참고 액세스 제어 정책 페이지에서 Hit Count(적중 횟수) 페이지에 액세스한 경우 사전 필터 규칙을 보거나 편집할 수 없으며 그 반대의 경우도 마찬가지입니다.

단계 **8** (선택 사항) 규칙을 오른쪽 클릭하고 **Clear Hit Count(**적중 횟수 지우기**)**를 선택하여 규칙의 적중 횟수 정보를 지웁니다.

여러 규칙의 적중 횟수 정보를 지우려면 **Ctrl** 버튼을 사용하여 여러 규칙을 선택하고, 선택한 규칙 중 하나를 마우스 오른쪽 버튼으로 클릭한 후 **Clear Hit Count(**적중 횟수 지우기**)**를 선택하면 됩니다.

참고 적중 횟수 정보를 지우면 적중 횟수가 0으로 설정되며, 이 변경 사항은 취소할 수 없습니다.

단계 **9** (선택 사항) 페이지의 왼쪽 하단에 있는 **Generate CSV(CSV** 생성**)**를 클릭하여 페이지의 세부 정보에 대한 CSV 보고서를 생성합니다.

단계 **10** **Close(**닫기**)**를 클릭하여 Policy(정책) 페이지로 돌아갑니다.

액세스 제어 정책 히스토리

기능	버전	세부 사항
DNS 필터링	6.7(실험)	URL 필터링이 활성화 및 구성된 경우 범주 및 평판 필터링 효율성을 개선하기 위한 새 옵션이 각 새 액세스 제어 정책에 대해 사용할 수 있습니다. 중요**!** 이는 실험적인 기능이며 예상대로 작동하지 않을 수 있습니다. 프로덕션 환경에서는 사용하지 마십시오. 자세한 내용은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타), 1678 페이지 및 하위 항목을 참조하십시오. 수정된 화면 : 액세스 제어 정책의 Advanced(고급) 탭에 General Settings(일반 설정) : **Enable reputation enforcement on DNS traffic(DNS** 트래픽에서 평판 시행 활성화**)** 아래에 새 옵션이 있습니다. 지원되는 플랫폼: 전체

기능	버전	세부 사항
TLS 서버 ID 검색	6.7	클라이언트가 TLS 1.3 지원 서버에 연결할 때 URL 및 애플리케이션 조건을 평가하도록 액세스 제어 정책을 활성화합니다. TLS 서버 ID 검색을 사용하면 트래픽 암호 해독 없이 이러한 조건을 평가할 수 있습니다. 참고: 이 기능을 활성화하면 매니지드 디바이스 모델에 따라 성능에 영향을 줍니다. 수정된 화면 : 액세스 제어 정책의 고급 탭 페이지에 새로운 옵션이 추가되었습니다. • Advanced(고급) 탭에 경고가 표시됩니다. 슬라이더를 오른쪽으로 이동하면 TLS 서버 ID 검색이 활성화됩니다. • Advanced(고급) 탭 페이지의 새로운 옵션: **TLS Server Identity Discovery(TLS 서버 ID 검색)**
새로운 보안 인텔리전스 범주	--	다음 범주는 6.6 릴리스 시점에 도입되었지만 6.6에만 해당되지는 않습니다. • banking_fraud • high_risk • ioc • link_sharing • 발생하는 것만은 아님 • newly_seen • 스파이웨어 신규/수정된 페이지: Access control policy(액세스 제어 정책) > Security Intelligence(보안 인텔리전스) 탭 지원되는 플랫폼: FMC

61 장

액세스 제어 규칙

다음 주제에서는 액세스 제어 규칙을 구성하는 방법을 설명합니다.

- 액세스 제어 규칙 소개, 1645 페이지
- 액세스 제어 규칙 요구 사항 및 사전 요건, 1650 페이지
- 액세스 제어 규칙 범주 추가, 1651 페이지
- 액세스 제어 규칙 생성 및 수정, 1651 페이지
- 액세스 제어 규칙 활성화 및 비활성화, 1653 페이지
- 하나의 액세스 제어 정책에서 다른 정책으로 액세스 제어 규칙 복사, 1654 페이지
- 사전 필터 정책으로 액세스 제어 규칙 이동, 1654 페이지
- 액세스 제어 규칙 포지셔닝, 1657 페이지
- 액세스 제어 규칙 작업, 1658 페이지
- 액세스 제어 규칙 코멘트, 1661 페이지
- 액세스 컨트롤 규칙 기록, 1662 페이지

액세스 제어 규칙 소개

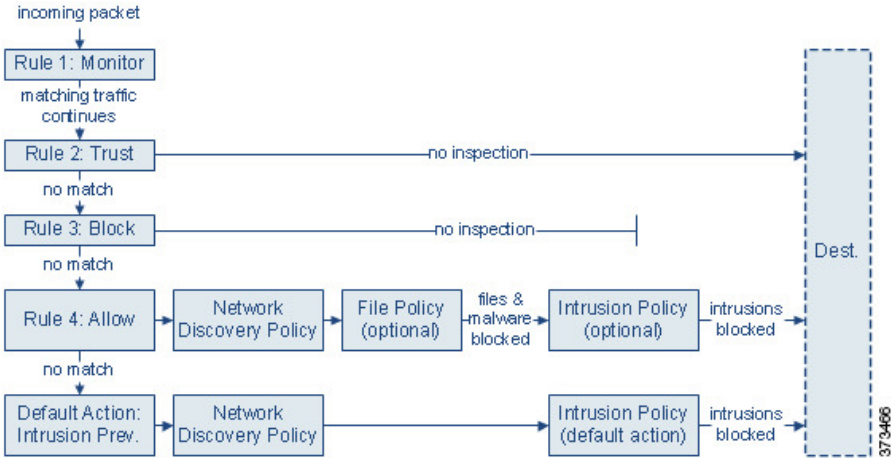
액세스 제어 정책 내에서 액세스 제어 규칙은 여러 매니지드 디바이스에서 네트워크 트래픽을 처리하는 세분화된 방법을 제공합니다.

참고 8000 시리즈 단축 경로 지정, 보안 인텔리전스 필터링, SSL 검사, 사용자 식별, 일부 디코딩 및 전처리는 액세스 컨트롤 규칙이 네트워크 트래픽을 평가하기 전에 수행됩니다.

시스템은 사용자가 지정하는 순서로 액세스 제어 규칙에 트래픽을 일치시킵니다. 대부분의 경우, 시스템은 모든 규칙의 조건이 트래픽과 일치하는 첫 번째 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다.

각 규칙에는 일치하는 트래픽의 모니터링, 신뢰, 차단 또는 허용 여부를 결정하는 작업이 있습니다. 트래픽을 허용하는 경우, 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다.

다음 시나리오에서는 트래픽이 인라인 침입 방지 배포에서 액세스 제어 규칙에 의해 평가될 수 있는 방법을 요약합니다.



이 시나리오에서, 트래픽은 다음과 같이 평가됩니다.

- 규칙 **1:** 모니터링은 가장 먼저 트래픽을 평가합니다. 모니터링 규칙은 네트워크 트래픽을 추적하고 로깅합니다. 시스템은 허용할지 아니면 거부할지 여부를 결정하기 위해 계속해서 트래픽을 추가 규칙에 일치시킵니다. (액세스 제어 규칙 모니터 작업, 1658 페이지에서 중요 예외 및 주의 사항을 확인하십시오.)
- 규칙 **2:** 신뢰는 두 번째로 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 목적지로 전달되는 것이 허용되지만 ID 요건과 속도 제한은 계속 적용됩니다. 매칭하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- 규칙 **3:** 차단은 세 번째로 트래픽을 평가합니다. 매칭하는 트래픽은 추가 검사 없이 차단됩니다. 매칭하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- 규칙 **4:** 허용은 마지막 규칙입니다. 이 규칙에서, 일치하는 트래픽은 허용되지만 해당 트래픽 내 금지된 파일, 악성코드, 침입 및 익스플로잇은 탐지 및 차단됩니다. 나머지 금지되지 않은 비악성 트래픽은 목적지까지 허용되지만 ID 요건과 속도 제한은 계속 적용됩니다. 파일 검사나 침입 검사 중 하나만 수행하거나 둘 다 수행하지 않는 허용 규칙을 구성할 수 있습니다.
- 기본 작업은 어느 규칙과도 일치하지 않는 모든 트래픽을 처리합니다. 이 시나리오에서 기본 작업은 비악성 트래픽의 통과를 허용하기 전에 침입 방지를 수행하는 것입니다. 다른 배포에서는 추가 검사 없이 모든 트래픽을 신뢰하거나 차단하는 기본 작업이 있을 수 있습니다. (기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.)

액세스 제어 규칙 또는 기본 작업을 통해 허용되는 트래픽은 자동으로 네트워크 검색 정책에 의한 호스트, 애플리케이션, 사용자 데이터 검사 대상이 됩니다. 검색을 강화 또는 비활성화할 수는 있지만 명시적으로 활성화하지는 마십시오. 그러나 트래픽을 허용한다고 해서 자동으로 검색 데이터 수집이 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에 의해 명시적으로 모니터링되는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다. 또한 암호화된 세션에 대해서는 애플리케이션 검색이 제한됩니다.

SSL 검사 구성에서 암호화 트래픽의 통과를 허용하는 경우 또는 SSL 검사를 구성하지 않은 경우, 액세스 제어 규칙이 암호화된 트래픽을 처리합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

액세스 제어 규칙 관리

액세스 제어 정책 편집기의 **Rules(**규칙**)** 탭에서는 현재 정책의 액세스 제어 규칙을 추가, 편집, 분류, 검색, 필터링, 이동, 활성화, 비활성화, 삭제하고 그 밖의 방식으로 관리할 수 있습니다. 검색 표시줄을 사용하여 액세스 제어 정책 규칙 목록을 필터링합니다. 필터 기준과 일치하는 규칙 목록 및 현재 액세스 제어 정책의 모든 규칙을 전환하려면 **Toggle(**전환**)**을 클릭합니다.

정책 편집기에는 각 액세스 제어 규칙의 이름, 조건의 요약, 규칙 작업, 규칙의 검사 옵션 또는 상태를 알리는 아이콘이 표시됩니다. 이러한 아이콘은 다음을 나타냅니다.

- 시간 범위 옵션( )
- 침입 정책()
- 파일 정책()
- 로깅()
- 코멘트()
- 경고()
- 오류()
- 중요 정보()

비활성화된 규칙은 흐리게 표시되며, 규칙 이름 아래에 `(disabled(비활성화))`가 표시됩니다.

규칙을 생성하거나 편집하려면 액세스 제어 규칙 편집기를 사용합니다. 다음 작업을 수행할 수 있습니다.

- 편집기의 상단에서 규칙의 이름, 상태, 위치 및 작업과 같은 기본 속성을 구성합니다.
- 편집기 하단의 왼쪽 탭을 사용하여 조건을 추가합니다.
- 편집기 하단의 오른쪽 탭을 사용하여 검사 및 로깅 옵션을 구성하고 규칙에 코멘트를 추가합니다. 편의를 위해, 사용자가 어떤 탭에 있든 편집기에는 규칙의 검사 및 로깅 옵션이 나열됩니다.

참고 액세스 제어 규칙을 올바르게 생성하고 지시하는 것은 복잡한 과제이지만 효율적인 배포 구축에 필수적입니다. 정책을 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이선스를 요구하거나, 잘못된 구성을 포함할 수 있습니다. 시스템이 트래픽을 예상대로 처리하도록 보장하기 위해, 액세스 제어 정책 인터페이스에는 규칙에 대한 강력한 경고 및 오류 피드백 시스템이 있습니다.

관련 항목

액세스 제어 규칙 구성 요소, 1648 페이지
예: 맞춤형 사용자 역할 및 액세스 제어
맞춤형 사용자 역할 생성, 127 페이지
액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

액세스 제어 규칙 구성 요소

각 액세스 제어 규칙에는 고유한 이름 외에도, 다음과 같은 기본 구성 요소가 있습니다.

상태

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하지 않으며, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 정책 상속을 사용하는 경우, 규칙 1이 가장 바깥쪽 정책의 첫 번째 규칙입니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

규칙은 섹션과 카테고리에 속할 수도 있는데, 이는 체계상 그런 것뿐이며 규칙 위치에 영향을 주지 않습니다. 규칙 위치는 섹션과 카테고리에 걸쳐 이동합니다.

섹션 및 카테고리

액세스 제어 규칙을 쉽게 구성할 수 있도록, 모든 액세스 제어 정책에는 시스템에서 제공하는 Mandatory(필수) 및 Default(기본값)라는 두 가지 섹션이 있습니다. 액세스 제어 규칙을 더욱 체계화하기 위해 Mandatory(필수) 및 Default(기본값) 섹션 내에 맞춤 설정 규칙 카테고리를 생성할 수 있습니다.

정책 상속을 사용 중인 경우, 현재 정책의 규칙은 상위 정책의 Mandatory(필수) 및 Default(기본값) 섹션 사이에 중첩됩니다.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 조건은 단순하거나 복잡할 수 있으며 사용법은 라이선스에 따라 달라지는 경우가 많습니다.

트래픽은 규칙의 모든 탭에 지정된 조건을 전부 충족해야 합니다. 예를 들어, Applications(애플리케이션) 탭에서 HTTPS는 지정하지 않고 HTTP를 지정하는 경우, URLs 탭의 URL 범주 및 평판 조건이 HTTPS 트래픽에 적용되지 않습니다.

적용 가능한 시간

규칙을 적용 가능한 기간의 날짜와 시간을 지정할 수 있습니다.

작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용(추가 검사 실행 또는 실행 안 함)할 수 있습니다. 시스템은 신뢰할 수 있거나 차단되거나 암호화된 트래픽에서 심층 검사를 수행하지 않습니다.

인스펙션

심층 검사 옵션은 사용자가 허용할 수도 있는 악성 트래픽을 시스템이 검사 및 차단하는 방법을 제어합니다. 규칙으로 트래픽을 허용하는 경우 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에, 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다.

로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다. 규칙과 매칭하는 트래픽을 기록할 수 있습니다. 일반적으로 연결의 시작이나 끝 또는 시작과 끝에서 세션을 로깅할 수 있습니다. 데이터베이스 및 시스템 로그(syslog) 또는 SNMP 트랩 서버에 대한 연결을 로깅할 수 있습니다.

Comments(의견)

액세스 제어 규칙의 변경 사항을 저장할 때마다 코멘트를 추가할 수 있습니다.

관련 항목

액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지
액세스 제어 규칙 관리, 1647 페이지
액세스 제어 규칙 생성 및 수정, 1651 페이지
규칙 조건 유형, 525 페이지
액세스 제어 규칙 작업, 1658 페이지
파일 및 침입 정책을 사용한 심층 검사, 1612 페이지
연결 로깅 모범 사례, 2868 페이지
액세스 제어 규칙 코멘트, 1661 페이지

액세스 제어 규칙 순서

액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 액세스 제어 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 모든 규칙의 조건이 트래픽과 일치하는 첫 번째 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 모니터링 규칙을 제외하고, 시스템은 트래픽이 규칙과 일치하는 것으로 확인되고 나면 우선 순위가 낮은 추가 규칙을 기준으로 트래픽을 계속 평가하지 않습니다.

액세스 제어 규칙을 쉽게 구성할 수 있도록, 모든 액세스 제어 정책에는 시스템에서 제공하는 Mandatory(필수) 및 Default(기본값)라는 두 가지 섹션이 있습니다. 추가로 구성하려면 Mandatory(필수) 또는 Default(기본값) 섹션 내에서 맞춤형 규칙 카테고리를 생성하면 됩니다. 카테고리를 생성한 후에는 삭제 및 이름 바꾸기가 가능하고 규칙을 카테고리 안으로, 밖으로, 내부에서, 주변으로 이동할 수는 있으나 카테고리를 이동할 수는 없습니다. 시스템은 섹션 및 카테고리 전반에 걸쳐 규칙 번호를 할당합니다.

정책 상속을 사용할 경우, 현재 정책의 규칙은 상위 정책의 Mandatory(필수) 및 Default(기본값) 규칙 섹션 사이에 중첩됩니다. 규칙 1은 현재 정책이 아닌 가장 바깥쪽 정책의 첫 번째 규칙이며, 시스템은 정책, 섹션, 카테고리 전반에 걸쳐 규칙 번호를 할당합니다.

액세스 제어 정책의 수정을 허용하는 사전 정의된 사용자 역할을 사용하면 규칙 카테고리 내에서 그리고 규칙 카테고리 간에 액세스 제어 규칙을 이동 및 수정할 수도 있습니다. 하지만, 사용자가 규칙을 이동하거나 변경하지 못하도록 제한하는 사용자 역할을 만들 수 있습니다. 액세스 제어 정책을 수정할 수 있는 모든 사용자는 맞춤형 카테고리에 규칙을 추가하고 해당 카테고리의 규칙을 제한 없이 수정할 수 있습니다.

팁 적절한 액세스 제어 규칙 순서는 네트워크 트래픽을 처리하는 데 필요한 리소스를 줄이고 규칙의 사전 대응을 방지합니다. 사용자가 생성한 규칙이 모든 조직과 배포에 고유하더라도 사용자의 필요를 처리하는 동안 성능을 최적화할 수 있는 규칙을 언제 지시할지에 대해 몇 가지 따라야 할 지침이 있습니다.

관련 항목

규칙 순서 지정 모범 사례, 1618 페이지

액세스 제어 규칙 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

액세스 제어 규칙 범주 추가

액세스 제어 정책의 Mandatory(필수) 및 Default(기본) 규칙 섹션을 맞춤 설정 카테고리로 나눌 수 있습니다. 카테고리를 생성한 후에는 삭제 및 이름 바꾸기가 가능하고 규칙을 카테고리 안으로, 밖으로, 내부에서, 주변으로 이동할 수는 있으나 카테고리를 이동할 수는 없습니다. 시스템은 섹션 및 카테고리 전반에 걸쳐 규칙 번호를 할당합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Add Category(**카테고리 추가**)**를 클릭합니다.

팁 정책에 이미 규칙이 포함된 경우, 새로운 규칙을 추가하기 전에 기존 규칙에 대한 행의 빈 영역을 클릭하여 새로운 카테고리의 위치를 지정합니다. 기존 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Insert new category(**새 카테고리 삽입**)**를 선택할 수도 있습니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** **Insert(**삽입**)** 드롭다운 목록에서 카테고리를 추가할 곳을 선택합니다.

- 섹션의 모든 기존 카테고리 아래에 카테고리를 삽입하려면 **into Mandatory(**필수로**)** 또는 **into Default(**기본으로**)**를 선택합니다.
- 기존 카테고리 위에 카테고리를 삽입하려면 **above category(**카테고리 위**)**를 선택한 다음 카테고리를 선택합니다.
- 액세스 제어 규칙 위 또는 아래에 카테고리를 삽입하려면 **above rule(**규칙 위**)** 또는 **below rule(**규칙 아래**)**를 선택한 다음 기존 규칙 번호를 입력합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 제어 규칙 생성 및 수정

능동적으로 사용 중인 액세스 제어 규칙을 수정한다면, 구축 시 설정 된 연결에는 변경 사항이 적용되지 않습니다. 업데이트된 규칙은 이후 연결의 일치 여부를 확인하는 데 사용됩니다. 그러나 시스템이 (예를 들어 침입 정책을 사용해) 연결을 능동적으로 검사한다면, 변경된 매칭 또는 작업 기준을 기존 연결에 적용합니다.

Firepower Threat Defense의 경우에는 설정된 연결을 FTD **clear conn** CLI 명령을 사용해 중단하면, 변경 사항을 모든 현재 연결에 적용할 수 있습니다. 연결 소스가 연결을 다시 설정하며 따라서 새로운 규칙에 대해 적절히 매칭됨이 예상되기 때문에, 이러한 연결을 중단해도 괜찮을 때만 이 작업을 수행하십시오.

프로시저

단계 **1** 액세스 제어 정책 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하려면 **Add Rule(**규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 수정( )을 클릭합니다.
- 여러 규칙을 편집하려면 규칙 범위를 Shift 키를 누른 상태에서 클릭하거나 편집할 여러 규칙을 Ctrl 키를 누른 상태에서 마우스 오른쪽 버튼을 클릭하고 옵션을 선택합니다.

규칙 옆에 보기 ( )가 대신 표시되는 경우에는 해당 규칙이 상위 정책에 속하거나 규칙을 수정할 권한이 없는 것입니다.

단계 **2** 새 규칙인 경우 **Name(**이름**)**을 입력합니다.

단계 **3** 규칙 구성 요소를 설정하거나 기본값을 승인합니다.

여러 규칙을 대량 편집하는 경우에는 옵션의 하위 집합만 사용할 수 있습니다.

- Enabled(활성화) — 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.
- Position(위치) — 규칙 위치를 지정합니다(액세스 제어 규칙 순서, 1649 페이지 참조).
- Action(작업) — 규칙 **Action(**작업**)**을 선택합니다(액세스 제어 규칙 작업, 1658 페이지 참조).

  참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. 방화벽 인터페이스에 적용된 액세스 규칙에는 사용할 수 없습니다.

- Time Range(시간 범위) — (FTD 디바이스에서만 지원됨) 규칙을 적용할 수 있는 날짜와 시간을 추가하거나 선택합니다. 자세한 내용은 시간 범위 개체 생성, 578 페이지 섹션을 참조해 주십시오.
- Conditions(조건) — 추가할 조건에 해당하는 항목을 클릭합니다. 자세한 내용은 규칙 조건 유형, 525 페이지의 내용을 참조하십시오.
- Deep Inspection(심층 검사)—Allow and Interactive Block(허용 및 인터랙티브 차단) 규칙의 경우, 침입 정책( ) 또는 파일 정책( )을 클릭하여 규칙의 **Inspection(**검사**)** 옵션을 설정합니다. 옵션이 흐리게 표시되면, 규칙에 해당 유형의 정책이 선택되지 않은 것입니다. 자세한 내용은 액세스 제어의 이해, 1609 페이지를 참조하십시오.
- Logging(로깅) — 로깅( )을 클릭하여 **Logging(**로깅**)** 옵션을 지정합니다. 옵션이 흐리게 표시되면, 규칙에 연결 로깅이 비활성화된 것입니다. 자세한 내용은 연결 로깅 모범 사례, 2868 페이지를 참조하십시오.

- Comments(코멘트) — 코멘트 열의 번호를 클릭하여 **Comments(**코멘트**)**를 추가합니다. 번호는 규칙에 이미 포함된 코멘트의 수를 나타냅니다. 자세한 내용은 액세스 제어 규칙 코멘트, 1661 페이지를 참조하십시오.

단계 **4** 규칙을 저장합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

시간 기반 규칙을 구축할 경우, 정책이 할당된 디바이스의 표준 시간대를 지정합니다. 정책 애플리케이션에 대한 디바이스 표준 시간대 구성, 1464 페이지의 내용을 참조하십시오.

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

액세스 제어 규칙 활성화 및 비활성화

액세스 제어 규칙을 만드는 경우, 이는 기본적으로 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다. 액세스 제어 정책에서 규칙 목록을 볼 때, 비활성화된 규칙은 계속 수정할 수 있지만 회색으로 표시됩니다.

팁 규칙 편집기를 사용하여 액세스 제어 규칙을 활성화하거나 비활성화할 수도 있습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 규칙을 마우스 오른쪽 버튼으로 클릭하고 규칙 상태를 선택합니다.

규칙 옆에 보기 ( )가 대신 표시되는 경우에는 해당 규칙이 상위 정책에 속하거나 규칙을 수정할 권한이 없는 것입니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

액세스 제어 규칙 구성 요소, 1648 페이지

하나의 액세스 제어 정책에서 다른 정책으로 액세스 제어 규칙 복사

액세스 제어 규칙을 한 액세스 제어 정책에서 다른 액세스 제어 정책으로 복사할 수 있습니다. 액세스 제어 정책의 **Default(**기본**)** 섹션 또는 **Mandatory(**필수**)** 섹션에 규칙을 복사할 수 있습니다.

시작하기 전에

계속하기 전에 다음 사항에 유의하십시오.

- 주석을 제외한 복사된 규칙의 모든 설정은 붙여 넣은 버전으로 유지됩니다. 그러나 소스 액세스 제어 정책을 언급하는 새로운 주석이 복사된 규칙에 추가됩니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 마우스 왼쪽 버튼을 클릭하여 복사할 규칙을 선택합니다.

팁 여러 규칙을 선택하려면 키보드에서 Ctrl(컨트롤) 키를 사용합니다.

단계 **2** 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Copy to(**복사 대상**)** > **Another policy(**다른 정책**)**를 선택합니다.

단계 **3** **Access Policy(**액세스 정책**)** 드롭 다운 목록에서 대상 액세스 제어 정책을 선택합니다.

단계 **4** **Place Rules(**규칙 배치**)** 드롭 다운 목록에서 복사한 규칙을 배치할 위치를 선택합니다.

- **Default(**기본값**)** 섹션에서 마지막 규칙 집합으로 배치하려면 **At the bottom(**맨 아래 **)(Default(**기본**)** 섹션 내**)**를 선택합니다.
- **Mandatory(**의무**)** 섹션에서 첫번째 규칙 집합으로 배치하려면 **At the top(**맨 위 **)(Mandatory(**의무**)** 섹션 내**)**를 선택합니다.

단계 **5** **Copy(**복사**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

사전 필터 정책으로 액세스 제어 규칙 이동

액세스 제어 규칙을 액세스 제어 정책에서 연결된 사전 필터 정책으로 이동할 수 있습니다.

시작하기 전에

계속하기 전에 다음 사항에 유의하십시오.

- 액세스 제어 규칙을 사전 필터 정책으로 이동할 때는 액세스 제어 규칙의 레이어 7(L7) 매개 변수를 이동할 수 없습니다. L7 매개 변수는 작업 중에 삭제됩니다.
- 규칙을 이동하면 액세스 제어 규칙 구성의 코멘트가 손실됩니다. 그러나 소스 액세스 제어 정책을 언급하는 새로운 주석이 이동된 규칙에 추가됩니다.
- **Action(**작업**)** 매개 변수로 **Monitor(**모니터링**)**가 설정된 상태에서는 액세스 제어 규칙을 이동할 수 없습니다.
- 액세스 제어 규칙의 **Action(**작업**)** 매개 변수는 이동할 때 사전 필터 규칙의 적절한 작업으로 변경됩니다. 액세스 제어 규칙의 각 작업이 무엇에 매핑되는지 확인하려면 다음 표를 참조하십시오.

액세스 제어 규칙 작업	사전 필터 규칙의 작업
허용	분석
차단	Block(차단)
Block with Reset(차단 후 재설정)	Block(차단)
인터랙티브 차단(Block)	Block(차단)
재설정 인터랙티브 차단(Block)	Block(차단)
신임	Fastpath(단축 경로)

- 마찬가지로 액세스 제어 규칙에 구성된 작업을 기반으로 다음 표에 나와 있는 것처럼 규칙을 이동한 후 로깅 구성이 적절한 설정으로 설정됩니다.

액세스 제어 규칙 작업	사전 필터 규칙에서 활성화된 로깅 구성
허용	확인란이 선택되지 않았습니다.
Block(차단)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩

액세스 제어 규칙 작업	사전 필터 규칙에서 활성화된 로깅 구성
Block with Reset(차단 후 재설정)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩
인터랙티브 차단(Block)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩
재설정 인터랙티브 차단(Block)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩
신임	• Log at Beginning of Connection(연결 시작 시 로깅) • Log at End of Connection(연결 종료 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩

- 기본 사전 필터 정책에는 규칙을 사용할 수 없으므로 액세스 제어 규칙을 기본 사전 필터 정책으로 이동할 수 없습니다.
- 소스 정책에서 규칙을 이동하는 동안 다른 사용자가 해당 규칙을 수정하면 FMC에 메시지가 표시됩니다. 페이지를 새로 고친 후 프로세스를 계속 진행할 수 있습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 마우스 왼쪽 버튼을 클릭하여 이동할 규칙을 선택합니다.

팁 여러 규칙을 선택하려면 키보드에서 Ctrl(컨트롤) 키를 사용합니다.

단계 **2** 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Move to another policy(**다른 정책으로 이동**)**를 선택합니다.

단계 **3** **Place Rules(**규칙 배치**)** 드롭 다운 목록에서 이동한 규칙을 배치할 위치를 선택합니다.

- 마지막 규칙 집합으로 배치하려면 맨 아래에를 선택합니다.
- 첫 번째 규칙 집합으로 배치하려면 상단에를 선택합니다.

단계 **4** **Move(**이동**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 제어 규칙 포지셔닝

액세스 제어 정책 내에서 기존 규칙을 이동할 수 있습니다. 카테고리에 규칙을 추가하거나 카테고리로 규칙을 이동하면 시스템은 해당 규칙을 카테고리 마지막에 배치합니다.

팁 여러 규칙을 선택한 다음 마우스 오른쪽 버튼 메뉴를 사용하여 잘라 붙여 넣으면 한 번에 여러 규칙을 이동할 수 있습니다.

시작하기 전에

액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지에서 규칙 순서 지침을 검토합니다.

프로시저

단계 **1** 액세스 제어 규칙 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하는 경우, **Insert(**삽입**)** 드롭다운 목록을 사용합니다.
- 기존 규칙을 수정하는 경우, **Move(**이동**)**를 클릭합니다.

단계 **2** 규칙을 이동하거나 삽입할 곳을 선택합니다.

- **into Mandatory(**필수로**)** 또는 **into Default(**기본으로**)**를 선택합니다.
- **into Category(**카테고리로**)**를 선택한 다음 사용자 정의 카테고리를 선택합니다.

- **above rule(**규칙 위**)** 또는 **below rule(**규칙 아래**)**를 선택한 다음 적절한 규칙 번호를 입력합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 제어 규칙 작업

모든 액세스 제어 규칙에는 시스템이 일치하는 트래픽을 처리하고 로깅하는 방법을 결정하는 작업이 있습니다. 추가 검사와 함께 또는 추가 검사 없이, 모니터링, 신뢰, 차단 또는 허용할 수 있습니다.

액세스 제어 정책의 기본 작업은 모니터링을 제외한 작업을 이용하는 액세스 제어 규칙의 조건을 충족하지 않는 트래픽을 처리합니다.

액세스 제어 규칙 모니터 작업

Monitor(모니터링**)** 작업은 트래픽을 허용하거나 거부하도록 설계되지 않았습니다. 이 작업의 기본 목적은 일치하는 트래픽의 처리 방식에 상관없이 연결 로깅을 강제하는 것입니다.

연결이 모니터링 규칙과 일치한다면, 연결과 일치하는 다음 비 모니터링 규칙으로 트래픽 처리 및 추가 검사를 결정해야 합니다. 일치하는 다른 규칙이 없다면, 시스템은 기본 작업을 사용해야 합니다.

그러나 예외가 있습니다. 모니터링 규칙에 레이어 7 조건(예: 애플리케이션 조건)이 포함된다면, 시스템은 초기 패킷을 전달하고 연결을 설정하도록(또는 SSL 핸드셰이크를 완료하도록) 허용할 수 있습니다. 후속 규칙으로 연결을 차단해야 하는 경우도 마찬가지입니다. 이러한 초기 패킷은 후속 규칙을 기준으로 평가되지 않기 때문입니다. 이러한 패킷이 완전히 검사되지 않은 대상에 도달하지 않도록 하려면 액세스 제어 정책의 고급 설정에서 이러한 목적을 위한 침입 정책을 지정할 수 있습니다. 트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지을 참조하십시오. 레이어 7 식별을 완료하면, 시스템은 나머지 세션 트래픽에 적절한 작업을 적용합니다.

⚠

주의 모범 사례는 트래픽이 실수로 네트워크로 들어오지 않도록, 광범위하게 정의되는 모니터링 규칙의 레이어 7 조건을 규칙 우선순위 상위에 놓지 않는 것입니다. 또한 로컬에서 바인딩된 트래픽이 레이어 3 구축의 모니터링 규칙과 일치하면, 해당 트래픽은 검사를 우회할 수 있습니다. 트래픽의 검사를 보장하려면 트래픽을 라우팅하는 매니지드 디바이스의 고급 디바이스 설정에서 **Inspect Local Router Traffic(**로컬 라우터 트래픽 검사**)**을 활성화하십시오.

관련 항목

모니터링된 연결에 대한 로깅, 2862 페이지

액세스 제어 규칙 신뢰 작업

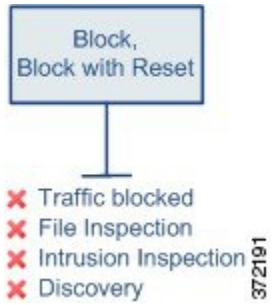
Trust(신뢰**)** 작업은 심층 검사 또는 네트워크 검색 없이 트래픽이 통과하도록 허용합니다. 신뢰할 수 있는 트래픽에는 ID 요건 및 속도 제한이 계속 적용됩니다.

관련 항목

신뢰할 수 있는 연결에 대한 로깅, 2862 페이지

액세스 제어 규칙 차단 작업

Block(차단**)** 및 **Block with reset(**차단 후 초기화**)** 작업은 어떤 종류의 추가 검사도 없이 트래픽을 거부합니다.



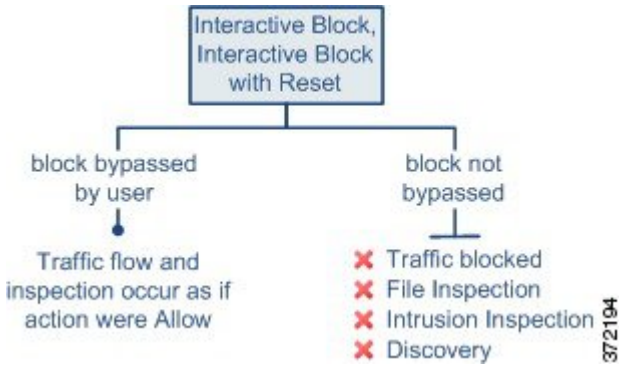
Block with reset(차단 후 재설정) 규칙은 *HTTP* 응답 페이지에 도달한 웹 요청을 제외하고 연결을 재설정합니다. 이것은 연결이 즉시 재설정되면 시스템이 웹 요청을 차단하는 경우에 표시되도록 사용자가 구성하는 응답 페이지가 표시될 수 없기 때문입니다. 자세한 내용은 HTTP 응답 페이지 및 인터랙티브 차단, 1689 페이지를 참고하십시오.

관련 항목

차단된 연결에 대한 로깅, 2863 페이지
HTTP 응답 페이지 정보, 1689 페이지

액세스 제어 규칙 인터랙티브 차단 작업

자세한 내용은 HTTP 응답 페이지 및 인터랙티브 차단, 1689 페이지를 참고하십시오.



사용자가 차단을 우회하는 경우, 규칙은 허용 규칙을 모방합니다. 따라서 인터랙티브 차단 규칙을 파일 및 침입 정책에 연결할 수 있으며, 일치하는 트래픽도 네트워크 검색 대상이 됩니다.

사용자가 차단을 우회하지 않거나 우회할 수 없는 경우, 규칙은 차단 규칙을 모방합니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.

인터랙티브 차단을 활성화하면 모든 차단된 연결을 재설정할 수 없습니다. 이것은 연결이 즉시 재설정되면 응답 페이지가 표시될 수 없기 때문입니다. **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 작업을 사용하여 웹 트래픽이 아닌 모든 트래픽을 차단 후 재설정하고, 웹 요청에 대해서는 계속 인터랙티브 차단을 활성화하십시오.

자세한 내용은 HTTP 응답 페이지 및 인터랙티브 차단, 1689 페이지를 참고하십시오.

관련 항목

허용된 연결에 대한 로깅, 2864 페이지
TLS/SSL 규칙 차단 작업, 1819 페이지

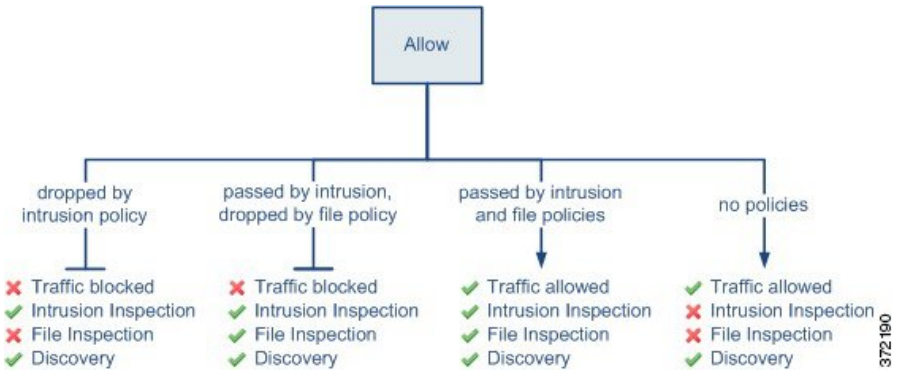
액세스 제어 규칙 허용 작업

Allow(허용**)** 작업은 일치하는 트래픽이 통과하도록 허용하지만 ID 요건과 속도 제한은계속 적용됩니다.

원하는 경우, 심층 검사를 사용하여 암호화되지 않은 트래픽과 해독된 트래픽이 목적지에 도달하기 전에 추가 검사하고 차단할 수 있습니다.

- 침입 정책을 사용하여 침입 탐지 및 방지 구성에 따라 네트워크 트래픽을 분석하고 해당 구성에 따라 문제가 되는 패킷을 삭제할 수 있습니다.
- 파일 정책을 사용하여 파일 제어를 수행할 수 있습니다. 파일 제어를 수행하면, 사용자가 특정 애플리케이션 프로토콜에서 특정 유형의 파일을 업로드(전송) 또는 다운로드(수신)하는 행동을 탐지하고 차단할 수 있습니다.
- 또한 파일 정책을 사용하여 네트워크 기반 AMP(Advanced Malware Protection)를 수행할 수 있습니다. AMP for Networks 는 파일에서 악성 코드를 검사하고 구성에 따라 탐지된 악성코드를 차단할 수 있습니다.

다음 다이어그램은 허용 규칙 또는 사용자가 우회한 인터랙티브 차단 규칙의 조건을 충족하는 트래픽에서 수행되는 검사 유형을 보여줍니다. 파일 검사는 침입 검사 전에 발생합니다. 차단된 파일에 대해서는 침입 관련 익스플로잇을 검사하지 않습니다.



간소화를 위해, 다이어그램은 액세스 제어 규칙과 침입 정책 및 파일 정책 둘 다 연관되어 있는 또는 둘 다 연관되어 있지 않은 상황을 위한 트래픽 흐름을 표시합니다. 그러나 하나가 없더라도 다른 하나를 구성할 수 있습니다. 파일 정책이 없으면 트래픽 흐름은 침입 정책에 의해 결정되고, 침입 정책이 없으면 트래픽 흐름은 파일 정책에 의해 결정됩니다.

침입 또는 파일 정책에 의해 트래픽이 검사되든 삭제되든 상관없이 시스템은 네트워크 검색을 사용하여 트래픽을 검사할 수 있습니다. 그러나 트래픽을 허용한다고 해서 자동으로 검색 검사가 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에 의해 명시적으로 모니터링되는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다. 또한 암호화된 세션에 대해서는 애플리케이션 검색이 제한됩니다.

관련 항목

허용된 연결에 대한 로깅, 2864 페이지

액세스 제어 규칙 코멘트

액세스 제어 규칙을 만들거나 수정할 때 코멘트를 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다. 각 코멘트 및 코멘트가 추가된 각 날짜를 추가한 사용자와 마찬가지로 규칙을 위한 모든 코멘트의 목록을 표시할 수 있습니다.

규칙을 저장할 때, 마지막 저장 이후 만들어진 모든 코멘트는 읽기 전용이 됩니다.

액세스 제어 규칙 코멘트를 검색하려면 Rule listing(규칙 목록) 페이지의 "Search Rules(규칙 검색)" 표시줄을 사용합니다. 규칙 검색, 551 페이지의 내용을 참조하십시오.

관련 항목

액세스 제어 정책 환경설정

액세스 제어 규칙에 설명 추가

프로시저

단계 **1** 액세스 제어 규칙 편집기에서 **Comments(**코멘트**)**를 클릭합니다.

단계 **2** **New Comment(**새 코멘트**)**를 클릭합니다.

단계 **3** 코멘트를 입력하고 **OK(**확인**)**를 클릭합니다. 규칙을 저장할 때까지 이 코멘트를 수정하거나 삭제할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

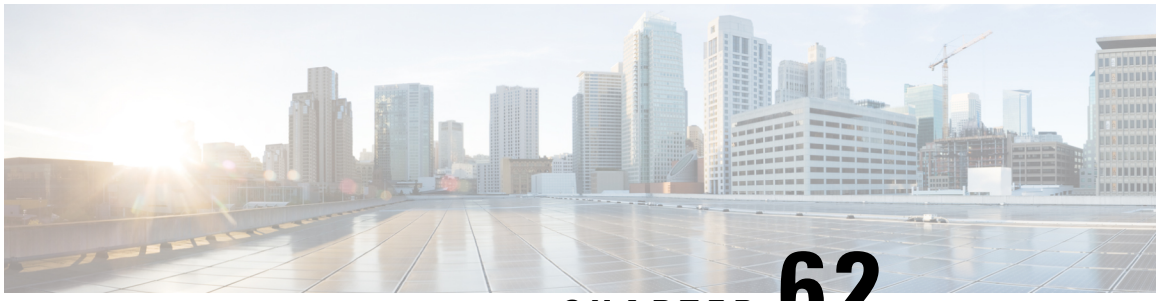
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 컨트롤 규칙 기록

기능	버전	세부 사항
액세스 제어 규칙 코멘트 검색	6.7	이제 **Search Rules(**검색 규칙**)** 표시줄에 코멘트를 검색할 수 있는 옵션이 제공됩니다. 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지, **Search Rules(**검색 규칙**)** 텍스트 입력 필드 지원되는 플랫폼: FMC
액세스 제어 및 사전 필터 정책 간에 규칙 복사 또는 이동	6.7	액세스 제어 규칙을 한 액세스 제어 정책에서 다른 액세스 제어 정책으로 복사할 수 있습니다. 액세스 제어 규칙을 액세스 제어 정책에서 연결된 사전 필터 정책으로 이동할 수도 있습니다. 신규/수정된 페이지: Access control policy(액세스 제어 정책) 페이지 - 선택한 규칙에 대해 마우스 오른쪽 버튼을 클릭하면 복사 및 이동에 대한 추가 옵션이 제공됩니다. 지원되는 플랫폼: FMC

기능	버전	세부 사항
액세스 제어 규칙에서 특정 설정 대량 편집	6.6	정책의 규칙 목록에서 Shift 키나 Control 키를 누른 상태에서 클릭하여 여러 규칙을 선택한 다음 마우스 오른쪽 버튼을 클릭하여 옵션을 선택합니다. 대량 작업으로는 규칙 활성화 또는 비활성화, 규칙 작업 선택, 대부분의 검사 및 로깅 설정 편집을 예로 들 수 있습니다. 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지 지원되는 플랫폼: FMC
설정된 규칙에 대한 향상된 검색	6.6	설정된 규칙에 대한 검색을 개선했습니다. 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지 지원되는 플랫폼: FMC
규칙 애플리케이션의 시간 범위	6.6	적용할 규칙에 대해 절대적이거나 반복되는 시간 또는 시간 범위를 지정할 수 있습니다. 규칙은 트래픽을 처리하는 디바이스의 표준 시간대에 따라 적용됩니다. 신규/수정된 페이지: • Access Control Add Rule(액세스 제어 규칙 추가) 페이지의 새로운 옵션 • 매니지드 디바이스의 표준 시간대를 지정하기 위한 **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**) > FTD** 페이지의 관련 새 옵션 지원되는 플랫폼: FTD 디바이스 전용

기능	버전	세부 사항
Access control rules(액세스 제어 규칙) 페이지에서 개체 세부 사항 보기	pre-6.6	규칙 목록 또는 규칙 설정 대화 상자에서 개체에 대한 정보를 보려면 개체를 마우스 오른쪽 버튼으로 클릭합니다. 신규/수정된 페이지: **Policies(**정책**) > Access Control(**액세스 제어**) > Access Control(**액세스 제어**)** 및 **Add Rule(**규칙 추가**)** 페이지 지원되는 플랫폼: FMC



CHAPTER 62

URL 필터링

- URL 필터링 개요, 1665 페이지
- URL 필터링 모범 사례, 1667 페이지
- URL 필터링의 라이선스 요건, 1671 페이지
- URL 필터링을 위한 요구 사항 및 사전 요건, 1671 페이지
- 범주 및 평판을 사용한 URL 필터링 설정 방법, 1672 페이지
- 수동 URL 필터링, 1679 페이지
- URL 필터링 상태 모니터 설정, 1682 페이지
- URL 범주 및 평판, 1682 페이지
- URL 범주 집합이 변경되면 작업 수행, 1683 페이지
- URL 필터링 기록, 1685 페이지

URL 필터링 개요

네트워크의 사용자가 액세스할 수 있는 웹사이트를 제어하려면 URL 필터링 기능을 사용합니다.

- 범주 및 평판 기반 URL 필터링 - URL 필터링 라이선스를 사용하면 URL의 일반 분류(범주) 및 위험 레벨(평판)을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다. 권장 옵션입니다.
- 수동 URL 필터링 - 임의의 라이선스를 사용하여 개별 URL, URL 그룹 및 URL 목록과 피드를 수동으로 지정해 웹 트래픽을 맞춤형 방식으로 더 상세하게 제어할 수 있습니다. 자세한 내용은 수동 URL 필터링, 1679 페이지를 참고하십시오.

악성 URL, 도메인 및 IP 주소를 차단하는 비슷하지만 다른 기능인 보안 인텔리전스 차단 목록, 1695 페이지도 참조하십시오.

카테고리 및 평판을 사용한 URL 필터링 정보

ULR 필터링 라이선스가 있으면 요청한 URL의 범주 및 평판을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.

- 범주 - URL의 일반 분류입니다. 예를 들어 ebay.com은 경매 범주에 속하고 monster.com은 구직 범주에 속합니다.

하나의 URL이 여러 카테고리에 속할 수 있습니다.

- 평판 - URL이 사용자가 속한 조직의 보안 정책에 어긋나는 용도로 사용될 가능성입니다. 평판의 범위는 알려지지 않음(레벨 0) 또는 신뢰할 수 없음(레벨 1)에서 신뢰할 수 있음(레벨 5)까지로 나타냅니다.

카테고리 및 평판 기반 URL 필터링의 이점

URL 범주 및 평판을 사용하면 URL 필터링을 빠르게 구성할 수 있습니다. 예를 들어 액세스 제어를 사용해 Hacking(해킹) 카테고리에서 신뢰할 수 없음 URL을 차단할 수 있습니다. 또는 QoS를 사용해 스트리밍 비디오 범주의 사이트에서 생성되는 트래픽의 속도를 제한할 수 있습니다. 스파이웨어 또는 애드웨어 카테고리 등과 같은 위협 유형 카테고리도 있습니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 정상적으로 제어할 수 있습니다. Cisco에서는 새로운 URL 및 기존 URL에 대한 새 범주와 위험을 포함하여 위협 인텔리전스를 지속적으로 업데이트하므로, 시스템이 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 보안 위협을 나타내거나 부적절한 콘텐츠를 제공하는 사이트가 나타나고 사라지는 속도는 새 정책을 업데이트하고 구축하는 속도보다 빠를 수 있습니다.

시스템을 조정할 수 있는 방법의 몇 가지 예는 다음과 같습니다.

- 액세스 제어 규칙이 모든 게임 사이트를 차단하는 경우, 새로운 도메인이 게임으로 등록되고 분류되면 시스템은 해당 사이트를 자동으로 차단할 수 있습니다. 마찬가지로 QoS 규칙이 모든 스트리밍 비디오 사이트의 속도를 제한하는 경우 시스템은 새 스트리밍 비디오 사이트로의 트래픽을 자동으로 제한할 수 있습니다.
- 액세스 제어 규칙이 모든 악성코드 사이트를 차단하는 경우, 쇼핑 페이지 하나가 악성코드에 감염되면 시스템은 쇼핑의 URL을 악성코드 사이트로 재분류하고 해당 사이트를 차단할 수 있습니다.
- 액세스 제어 규칙이 신뢰할 수 없음인 소셜 네트워킹 사이트를 차단하고 누군가가 악성 페이로드 링크를 포함하는 프로파일 페이지에 링크를 게시하는 경우, 시스템은 해당 페이지의 평판을 선호 사이트에서 신뢰할 수 없음으로 변경하고 해당 페이지를 차단할 수 있습니다.

관련 항목

Snort® 재시작 시나리오, 505 페이지

URL 카테고리 및 평판 설명

카테고리 설명

각 URL 카테고리에 대한 설명은 https://www.talosintelligence.com/categories에 나와 있습니다.

범주를 보려면 **Threat Categories(**위협 범주**)**를 클릭해야 합니다.

평판 레벨 설명

https://talosintelligence.com/reputation_center/support(으)로 이동해 Common Questions(자주 하는 질문) 섹션에서 확인하십시오.

Cisco Cloud의 URL 필터링 데이터

카테고리와 평판을 기반으로 한 URL 필터링에는 클라우드 서비스인 Cisco Cloud가 제공하는 데이터 집합이 필요합니다.

일반적으로는 유효한 URL 필터링 라이선스가 활성 디바이스에 적용되면 기본적으로 Cisco Cloud에서 Firepower Management Center로 URL 카테고리 및 평판 데이터 집합이 다운로드되고 디바이스에 푸시됩니다. 로컬에 저장된 이 데이터 집합은 주기적으로 업데이트됩니다.

네트워크의 사용자가 URL에 액세스하는 경우, 시스템은 (다운로드된) 로컬 데이터 집합에서 일치 항목을 찾습니다. 일치 항목이 없으면 시스템은 이전에 Cisco Cloud에서 조회했던 결과의 캐시를 확인합니다. 그래도 일치 항목이 없으면 시스템은 Cisco Cloud에서 URL을 조회하고 결과를 캐시에 추가합니다.

URL 카테고리 집합은 주기적으로 변경될 수 있습니다. 이러한 변경의 알림을 수신하는 경우, 정책에서 URL 규칙을 검토하여 변경이 필요한지 확인해야 합니다. 자세한 내용은 URL 범주 집합이 변경되면 작업 수행, 1683 페이지를 참고하십시오.

URL 필터링 모범 사례

URL 필터링을 위한 다음 지침 및 제한 사항을 유념하십시오.

범주 및 평판을 기준으로 필터링

범주 및 평판을 사용한 URL 필터링 설정 방법, 1672 페이지의 지침을 따릅니다.

URL을 식별하기 전에 통과해야 하는 패킷을 검사하도록 정책 설정

시스템은 다음 작업을 수행한 후 URL을 필터링할 수 있습니다.

- 클라이언트와 서버 간 모니터링된 연결이 설정됩니다.
- 시스템은 세션에서 DNS, HTTP 또는 HTTPS 애플리케이션을 식별합니다.
- 시스템은 (암호화된 세션의 경우 암호화되지 않은 도메인 이름, ClientHello 메시지 또는 서버 인증서로부터) 요청된 도메인 또는 URL을 식별합니다.

이 식별은 3~5개 패킷 내에서 또는 트래픽이 암호화된 경우 TLS/SSL 핸드셰이크의 서버 인증서 교환 후에 이루어져야 합니다.

중요! 시스템이 통과할 이러한 초기 패킷을 검사하도록 하려면 트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지 및 하위 주제를 참조하십시오.

초기 트래픽이 기타 모든 규칙 조건과 일치하지만 식별이 불완전한 경우 시스템은 패킷 통과 및 연결 설정 (또는 TLS/SSL 핸드셰이크 완료)을 허용합니다. 시스템은 식별을 완료하면 나머지 세션 트래픽에 적절한 규칙 작업을 적용합니다.

위협 범주 차단

정책은 잘 알려진 악성 사이트를 식별하는 위협 카테고리를 해결해야 합니다. 평판이 불량한 사이트를 차단하는 것 외에 이 작업을 수행합니다.

예를 들어, 악의적인 사이트로부터 네트워크를 보호하려면 평판이 불량하거나 의심스러운 사이트를 차단하는 것 외에도 모든 위협 범주를 차단해야 합니다.

자세한 내용은 URL 카테고리 및 평판 설명, 1666 페이지의 URL의 위협 범주를 참조하십시오.

URL 조건 및 규칙 순서

- 적중해야 하는 다른 모든 규칙 뒤에 URL 규칙을 배치합니다.
- URL은 여러 카테고리에 속할 수 있습니다. 명시적으로 또는 기본 작업에 의존하여, 특정 웹사이트 범주는 허용하고 다른 범주는 차단할 수도 있습니다. 이 경우 블록 허용 또는 차단 중 무엇을 우선하는 가에 따라, 원하는 효과를 얻을 수 있도록 URL 규칙을 생성하고 순서를 지정해야 합니다.

규칙에 대한 자세한 지침은 액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지 및 규칙 조건 메커니즘, 527 페이지 주제를 참조하십시오.

미분류 또는 무평판 **URL**

URL 규칙을 만들 때 일치시키려는 카테고리를 먼저 선택합니다. **Uncategorized(**미분류**)** URL을 명시적으로 선택하면 평판에 따른 추가 제한이 불가능합니다.

신뢰할 수 없음 평판이 있는 미분류 URL은 악성 사이트 카테고리로 처리됩니다. (의심스러움 등의) 다른 평판 수준을 사용해 분류되지 않은 사이트를 차단하려는 경우에는 분류되지 않은 모든 사이트를 차단해야 합니다.

범주 및 평판 레벨을 선택한 후 필요에 따라 **Apply to unknown reputation(**알 수 없는 평판에 적용**)**을 선택할 수 있습니다. 예를 들어, 신뢰할 수 없음, 의심스러움, 알 수 없는 평판의 사이트에 적용되는 규칙을 생성할 수 있습니다.

URL에는 범주와 평판을 수동으로 할당할 수 없지만, 액세스 제어 및 QoS 정책에서는 특정 URL을 수동으로 차단할 수 있습니다. 수동 URL 필터링, 1679 페이지의 내용을 참조하십시오. URL 범주 및 평판, 1682 페이지도 참조하십시오.

암호화된 웹 트래픽에 대한 **URL** 필터링

암호화된 웹 트래픽에 대해 URL 필터링을 수행할 때 시스템은 다음 작업을 수행합니다.

- (DNS 필터링이 활성화된 경우) 시스템이 이전에 원래 도메인을 파악했는지 또는 도메인이 로컬 평판 데이터베이스에 있는지 확인하고, 있는 경우 도메인의 평판 및 범주를 기반으로 조치를 취합니다. 그렇지 않으면 시스템은 액세스 제어 정책의 고급 설정에서 **Retry URL cache miss lookup(URL** 캐시 누락 조회 다시 시도**)**가 활성화된 경우에도 암호화된 트래픽에 대한 설정에 따라 트래픽을 처리합니다.
- 암호화 프로토콜을 무시합니다. 규칙에 URL 조건은 있지만 프로토콜을 지정하는 애플리케이션 조건이 없는 경우 해당 규칙은 HTTPS 및 HTTP 트래픽 두 가지 모두와 일치합니다.

- URL 목록을 사용하지 않습니다. 그 대신 URL 개체 및 그룹을 사용해야 합니다.
- 트래픽을 암호화하는 데 사용되는 공개 키 인증서의 주체 공통 이름을 기반으로 HTTPS 트래픽과 일치시키며, 암호 해독 후 HTTP URL을 포함하여 트랜잭션 중에 언제든지 표시되는 다른 URL의 평판도 평가합니다.
- 주체 공통 이름 내의 서브도메인을 무시합니다.
- 액세스 제어 규칙이나 기타 컨피그레이션에서 차단한 암호화된 연결에 대해 HTTP 응답 페이지를 표시하지 않습니다(HTTP 대응 페이지의 제한, 1689 페이지 참조).

URL 필터링 및 TLS 서버 ID 검색

RFC 8446에서 정의한 TLS(Transport Layer Security) 프로토콜 1.3의 최신 버전은 보안 통신을 제공하기 위해 많은 웹 서버에서 선호하는 프로토콜입니다. TLS 1.3 프로토콜은 추가 보안을 위해 서버의 인증서를 암호화하며, 액세스 제어 규칙의 애플리케이션 및 URL 필터링 기준과 일치하는 데 인증서가 필요하므로 Firepower System은 전체 패킷의 암호를 해독하지 않고 서버 인증서를 추출하는 방법을 제공합니다.

액세스 제어 정책 고급 설정은 TLS 서버 ID 검색을 위한 **Early application detection and URL categorization(**초기 애플리케이션 탐지 및 **URL** 분류**)** 옵션을 제공합니다.

애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.

참고

- TLS 서버 ID 검색은 하드웨어 플랫폼에 따라 성능을 저하시킬 수 있습니다.
- TLS 서버 ID 검색은 인라인 탭 모드 또는 패시브 모드 구축에서 지원되지 않습니다.

자세한 내용은 액세스 제어 정책 고급 설정, 1637 페이지를 참고하십시오.

HTTP/2

시스템은 TLS 인증서에서 HTTP/2 URL을 추출할 수 있지만 페이로드에서는 추출할 수 없습니다.

수동 URL 필터링

- 사용자 지정 보안 인텔리전스 목록 또는 피드 개체를 사용하여 URL을 지정합니다. URL 개체를 사용하거나 규칙에 URL을 직접 입력하지 마십시오. 자세한 내용은 수동 URL 필터링 옵션, 1680 페이지 섹션을 참조해 주십시오.
- URL 개체를 사용하거나 규칙에 URL을 직접 입력하여 특정 URL을 수동으로 필터링하는 경우, 영향을 받을 수 있는 다른 트래픽을 신중하게 고려하십시오. URL 조건이 네트워크 트래픽과 일치하는지 확인하기 위해 시스템은 간단한 부분 문자열 일치를 실행합니다. 요청한 URL은 문자열의 일부분과 일치하는 경우 일치 항목으로 간주됩니다.

- 수동 URL 필터링을 사용하여 다른 규칙에 대한 예외를 생성하는 경우, 예외를 생성하지 않으면 적용될 일반 규칙 위에 예외가 있는 특정 규칙을 배치합니다.

URL 내 검색 쿼리 매개변수

시스템은 URL 조건과 일치하도록 URL에서 검색 쿼리 매개변수를 사용하지 않습니다. 예를 들어, 모든 쇼핑 트래픽을 차단하는 시나리오를 생각해 보십시오. 이 경우, amazon.com을 검색하기 위해 웹 검색을 사용하는 것은 차단되지 않지만 amazon.com 브라우징은 차단됩니다.

선택한 디바이스 모델의 메모리 제한

- NGIPSv를 사용하는 경우 카테고리 및 평판 기반 URL 필터링을 수행하기 위한 정확한 메모리 할당에 대한 정보는 VMware용 Cisco Firepower NGIPSv 빠른 시작 가이드을 참조하십시오.
- 메모리가 적은 디바이스 모델은 적은 URL 데이터를 로컬로 저장하며, 따라서 시스템은 클라우드를 더 자주 확인해 로컬 데이터베이스에 없는 사이트의 카테고리와 평판을 확인합니다.

  하위 메모리 디바이스는 다음과 같습니다.

  - FTD 1010
  - 8GB RAM의 가상 FTD(FTDv)
  - ASA 5508-X 및 ASA 5516-X
  - 7100 시리즈

관련 항목

트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지

HTTPS 트래픽 필터링

시스템은 암호화 트래픽을 필터링하기 위해 TLS/SSL 핸드셰이크 중에 전달된 정보(트래픽을 암호화하는 데 사용된 공개 키 인증서의 주체 공용 이름)를 기준으로 요청된 URL을 확인합니다.

HTTP 필터링과 달리, HTTPS 필터링은 주체 공용 이름 내의 서브도메인을 무시합니다. 액세스 제어 또는 QoS 정책에서 HTTPS URL을 수동으로 필터링할 경우, 서브도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

또한, HTTPS 필터링은 URL 목록을 지원하지 않습니다. 그 대신 URL 개체 및 그룹을 사용해야 합니다.

팁 SSL 정책에서는 고유 이름 SSL 규칙 조건을 정의하여 특정 URL에 대한 트래픽을 처리하고 암호를 해독할 수 있습니다. 인증서의 주체 고유 이름의 공용 이름 속성에는 사이트의 URL이 포함됩니다. HTTPS 트래픽을 암호 해독하면 액세스 제어 규칙이 암호 해독된 세션을 평가할 수 있으므로 URL 필터링 성능이 개선됩니다.

암호화 프로토콜을 통해 트래픽 제어

시스템은 액세스 제어 또는 QoS 정책에서 URL 필터링을 수행할 때 암호화 프로토콜(HTTP 또는 HTTPS)을 무시합니다. 이는 수동 및 평판 기반 URL 조건 모두에 해당됩니다. 즉, URL 필터링에서는 다음 웹 사이트에 대한 트래픽을 동일하게 처리합니다.

- http://example.com/
- https://example.com/

HTTP 또는 HTTPS 트래픽에만 일치하는 규칙을 구성하려면 규칙에 애플리케이션 조건을 추가합니다. 예를 들어 각각 애플리케이션 및 URL 조건을 갖춘 2개의 액세스 제어 규칙을 작성하여 어떤 사이트에 대한 HTTPS 액세스를 허용하되 HTTP 액세스는 허용하지 않을 수 있습니다.

첫 번째 규칙은 웹 사이트에 대한 HTTPS 트래픽을 허용합니다.

작업: Allow(허용)
애플리케이션: HTTPS
URL: example.com

두 번째 규칙은 동일한 웹 사이트에 대한 HTTP 액세스를 차단합니다.

작업: Block(차단)
애플리케이션: HTTP
URL: example.com

URL 필터링의 라이선스 요건

FTD 라이센스

- 범주 및 평판 필터링 -URL 필터링
- 수동 필터링 - 추가 라이선스가 없습니다.

기본 라이선스

- 범주 및 평판 필터링 -URL 필터링
- 수동 필터링 - 추가 라이선스가 없습니다.

URL 필터링을 위한 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

범주 및 평판을 사용한 URL 필터링 설정 방법

	수행해야 할 작업	추가 정보
단계	NGIPSv 장치에서 카테고리 및 평판 기반 URL 필터링을 사용하는 경우, 필요한 양의 메모리를 할당합니다.	VMware용 Cisco Firepower NGIPSv 빠른 시작 가이드
단계	올바른 라이선스가 있는지 확인합니다.	Firepower System 라이선싱, 157 페이지, 다음 항목 포함. • 클래식 디바이스에 대한 URL 필터링 라이선스, 163 페이지 URL을 필터링할 관리되는 각 디바이스에 URL 필터링 라이선스를 할당합니다. 기능을 활성화하려면 적어도 한 대의 매니지드 디바이스에는 할당된 URL 필터링 라이선스가 있어야 합니다.
단계	Firepower Management Center가 클라우드와 통신하여 URL 필터링 데이터를 가져올 수 있는지 확인합니다.	인터넷 액세스 요구 사항, 3108 페이지 및 통신 포트 요구 사항, 3110 페이지.
단계	제한 사항과 지침을 이해하고 필요한 조치를 취합니다.	URL 필터링 모범 사례, 1667 페이지
단계	URL 필터링 기능을 활성화합니다.	범주 및 평판을 사용한 URL 필터링 활성화, 1674 페이지

	수행해야 할 작업	추가 정보
단계	범주 및 평판을 기준으로 URL을 필터링하는 규칙을 설정합니다.	URL 조건 설정, 1675 페이지 악의적인 사이트로부터 최상의 보호를 받으려면 평판으로 사이트를 차단하고 모든 위협 범주에서 URL을 차단해야 합니다. (선택사항) 범주 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의, 1681 페이지
단계	(선택 사항) 사용자가 경고 페이지에서 클릭하면 웹사이트 차단을 우회할 수 있게 합니다.	HTTP 응답 페이지 및 인터랙티브 차단, 1689 페이지
단계	트래픽이 주요 규칙에 먼저 적중하도록 규칙 순서를 정합니다.	URL 규칙 순서, 1622 페이지
단계	베타 기능: DNS 필터링을 사용하여 URL 필터링 효율성을 개선합니다.	참조: • DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타), 1678 페이지 • 도메인 조회 중 URL을 식별하도록 DNS 필터링 활성화(베타), 1678 페이지.
단계	(선택 사항) URL 필터링과 관련된 고급 옵션을 수정합니다.	일반적으로 기본값을 변경해야 하는 특별한 이유가 없는 한 기본값을 사용합니다. 다음을 비롯한 고급 옵션에 대한 자세한 내용은 액세스 제어 정책 고급 설정, 1637 페이지의 내용을 참조하십시오. • 연결 이벤트에 저장하고자 하는 최대 URL 문자 • 인터랙티브 차단을 허용하여 다음 시간(초) 동안 차단 바이패스
단계	변경 사항을 배포합니다.	컨피그레이션 변경 사항 구축, 498 페이지
단계	시스템이 예상대로 향후 URL 데이터 업데이트를 수신하는지 확인합니다.	URL 필터링 상태 모니터 설정, 1682 페이지
단계	악성 사이트로부터 네트워크를 보호하는 다른 Firepower 기능을 활성화했는지 확인하십시오.	보안 인텔리전스 차단 목록, 1695 페이지의 내용을 참조하십시오.

범주 및 평판을 사용한 URL 필터링 활성화

이 작업을 수행하려면 관리자 사용자여야 합니다.

시작하기 전에

범주 및 평판을 사용한 URL 필터링 설정 방법, 1672 페이지에 설명된 사전 요건을 완료합니다.

프로시저

단계 **1** **System(**시스템**)** > **Integration(**통합**)**를 선택합니다.
단계 **2** **Cloud Services** 버튼을 클릭합니다.
단계 **3** URL 필터링 옵션, 1674 페이지을 구성합니다.
단계 **4** **Save(**저장**)**를 클릭합니다.

URL 필터링 옵션

다음 옵션은 **System(**시스템**)** > **Integration(**통합**)** 페이지에서 확인할 수 있습니다.

URL 필터링 활성화

웹사이트의 일반 분류 또는 카테고리와 위험 수준 또는 평판에 따른 트래픽 필터링을 허용합니다. URL 필터링 라이선스를 추가하면 **Enable URL Filtering(URL** 필터링 활성화**)**이 자동으로 활성화됩니다. URL 필터링을 활성화해야 다른 URL 필터링 옵션을 선택할 수 있습니다.

URL 필터링을 활성화하면 마지막으로 URL 필터링을 활성화한 후 얼마나 지났는지 또는 이번에 처음 URL 필터링을 활성화하는지에 따라, Firepower Management Center이(가) Cisco Cloud에서 URL 데이터를 다운로드합니다. 이 프로세스는 시간이 걸릴 수 있습니다.

자동 업데이트 활성화

URL 필터링 위협 데이터를 업데이트 하기 위한 옵션:

- 이 페이지에서 **System(**시스템**)** > **Integration(**통합**)** 페이지에서 **Enable Automatic Updates(**자동 업데이트 활성화**)** 옵션을 활성화하면, Firepower Management Center은(는) 30분마다 클라우드에서 업데이트를 확인합니다. URL 필터링 라이선스를 추가하면 이 옵션은 기본적으로 활성화됩니다.
- 시스템이 외부 리소스와 접촉하는 시기를 엄격히 제어해야 하는 경우, 이 페이지의 자동 업데이트를 비활성화하고 대신 스케줄러를 사용하여 반복 작업을 생성하십시오. 예약된 작업을 통해 URL 필터링 업데이트 자동화, 263 페이지의 내용을 참조하십시오.

지금 업데이트

이 대화 상자 상단에 있는 **Update Now(**지금 업데이트**)** 버튼을 클릭하면 일회성 온디맨드 업데이트를 수행할 수 있지만 자동 업데이트를 활성화하거나 스케줄러를 사용하여 반복 작업을 생성해야 합니다. 업데이트가 이미 진행 중인 경우, 온디맨드 업데이트를 시작할 수 없습니다.

일일 업데이트 용량은 작지만 마지막 업데이트 후 5일 이상이 경과했다면 대역폭에 따라 새 URL 데이터를 다운로드하는 데 20분 이상이 소요될 수 있습니다. 그런 다음 업데이트 자체를 수행하는 데 30분이 걸릴 수 있습니다.

Cisco Cloud에서 알 수 없는 **URL** 쿼리

로컬 데이터베이스에 카테고리와 평판이 없는 웹사이트를 사용자가 탐색하는 경우, 위협 인텔리전스 평가를 위해 시스템이 클라우드에 URL을 제출하도록 허용합니다. 예를 들어 사생활 보호를 위해 미분류 URL을 제출하기를 원치 않는 경우, 이 옵션을 비활성화하십시오.

적어도 하나의 매니지드 디바이스에 유효한 URL 필터링 라이선스가 있는 경우, 이 옵션은 기본적으로 활성화됩니다.

미분류 URL에 대한 연결은 카테고리 또는 평판 기반 URL 규칙과 일치하지 않습니다. URL에 카테고리 또는 평판을 수동으로 할당할 수 없습니다.

SSL 규칙을 사용하여 암호화 트래픽을 처리하는 경우, TLS/SSL 규칙 지침 및 제한 사항, 1804 페이지도 참조하십시오.

캐시된 **URL** 만료

이 설정은 **Query Cisco Cloud for Unknown URLs(Cisco Cloud**에서 알 수 없는 **URL** 쿼리**)**가 활성화된 경우에만 사용할 수 있습니다.

카테고리 및 평판 데이터를 캐싱하면 웹 브라우징 속도가 빨라집니다. 가장 빠른 성능을 위해 캐시된 URL 데이터는 기본적으로 만료되지 않습니다.

오래된 데이터에서 URL 일치 인스턴스를 최소화하려면 캐시의 URL이 만료되도록 설정할 수 있습니다. 위협 데이터의 정확성과 유효 기간을 높이려면 더 짧은 만료 기간을 선택하십시오.

캐시된 URL은 지정된 시간이 경과한 후 네트워크의 사용자가 처음 해당 URL에 액세스한 후 새로 고침됩니다. 첫 번째 사용자는 새로 고침된 결과를 볼 수 없지만 이 URL을 방문하는 다음 사용자는 새로 고침된 결과를 볼 수 있습니다.

URL 데이터 캐싱에 대한 자세한 내용은 Cisco Cloud의 URL 필터링 데이터 , 1667 페이지의 내용을 참조하십시오.

URL 조건 설정

URL 범주 및 평판을 기반으로 사이트에 대한 액세스를 제어하여 네트워크를 보호합니다.

프로시저

단계 **1** 규칙 편집기에서 URL 조건에 대해 다음을 클릭합니다.

- 액세스 제어 또는 QoS - **URLs(URL)**을 클릭합니다.
- SSL - **Category(**범주**)**를 클릭합니다.

단계 **2** 제어할 URL 범주를 찾아 선택합니다.

액세스 제어 또는 QoS 규칙에서 **Category(**범주**)**를 클릭합니다.

악의적인 사이트로부터 효과적으로 보호하려면 평판이 불량하거나 의심스러운 URL을 차단하는 것 외에도 위협 범주에 속하는 모든 URL을 차단해야 합니다. 위협 범주 목록은 URL 카테고리 및 평판 설명, 1666 페이지의 내용을 참조하십시오.

사용 가능한 모든 범주를 보려면 목록 하단에 있는 화살표를 클릭해야 합니다.

단계 **3** (선택 사항) **Reputations(**평판**)**를 선택하여 URL 카테고리를 제한합니다.

명시적으로 **Uncategorized(**미분류**)** URL에 일치시키면 미분류 URL에는 평판을 기준으로 한 추가 제한이 불가능합니다. 평판 레벨을 선택하면 규칙 작업에 따라 선택하는 레벨보다 더 심각하거나 덜 심각한 평판도 포함됩니다.

- 덜 심각한 평판을 포함 - 규칙이 웹 트래픽을 허용하거나 신뢰하는 경우. 예를 들어 선호 사이트(레벨 4)를 허용하는 규칙을 구성한다면, 신뢰할 수 있음(레벨 5) 사이트도 자동으로 허용합니다.
- 더 심각한 평판을 포함 - 규칙이 웹 트래픽을 속도 제한, 해독, 차단 또는 모니터링하는 경우. 예를 들어 수상한 사이트(레벨 2)를 차단하는 액세스 제어 규칙을 구성하면 해당 규칙은 신뢰할 수 없음(레벨 1) 사이트도 차단합니다.

규칙 작업을 변경하면 시스템은 URL 조건의 평간 레벨을 자동으로 변경합니다.

필요에 따라 **Apply to unknown reputation(**알 수 없는 평판에 적용**)**을 선택합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

예**:** 액세스 제어 규칙의 **URL** 조건

다음 그림은 모든 악성코드 사이트, 모든 신뢰할 수 없음 사이트 및 평판 수준이 보통 이하인 모든 소셜 네트워킹 사이트를 차단하는 액세스 제어 규칙의 URL 조건을 보여줍니다.

다음 표에는 조건을 만드는 방법이 요약되어 있습니다.

차단된 URL	카테고리	평판
평판과 상관없이 악성코드 사이트	Malware Sites(악성코드 사이트)	Any(모두)
모든 신뢰할 수 없는 URL(레벨 1)	Any(모든)	1 - 신뢰할 수 없음
위험도가 평판 수준이 보통 이하인(레벨 1부터 3까지의) 소셜 네트워킹 사이트	소셜 네트워크	3 - 보통인 일반 사이트

다음에 수행할 작업

- (선택사항) 범주 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의, 1681 페이지
- 범주 및 평판을 사용한 URL 필터링 설정 방법, 1672 페이지으로 돌아갑니다.
- 변경이 완료되면, 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

URL 조건이 포함된 규칙

아래 표에는 URL 조건을 지원하는 규칙과 각 규칙 유형이 지원하는 필터링 유형이 나와 있습니다.

규칙 유형	카테고리 및 평판 필터링을 지원합니까?	수동 필터링 지원 여부
액세스 제어	예	예
SSL	예	아닙니다. 대신 고유 이름 조건을 사용합니다.
QoS	예	예

URL 규칙 순서

가장 효과적인 URL 일치를 위해 특히 URL 규칙이 차단 규칙이고 다른 규칙이 다음 조건을 모두 만족하는 경우 다른 규칙 전에 URL 조건을 포함하는 규칙을 배치합니다.

- 애플리케이션 조건을 포함합니다.
- 검사할 트래픽은 암호화되어야 합니다.

규칙에 대해 예외를 설정하는 경우 다른 규칙 위에 예외를 배치합니다.

DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타)

이 기능은 릴리스 **6.7**에서 실험적으로 제공됩니다. 따라서 예상대로 작동하지 않을 수 있습니다. 프로덕션 환경에서는 사용하지 마십시오.

이 옵션은 URL 필터링 동작을 약간 수정하며 URL 필터링이 활성화 및 설정된 경우에만 적용 가능합니다.

이 옵션이 활성화된 경우:

- 브라우저가 도메인 이름을 조회하여 IP 주소를 가져올 때 시스템은 URL 트랜잭션 초기에 도메인 범주 및 평판을 평가합니다.
- 암호화된 트래픽의 범주 및 평판은 암호 해독 없이 확인할 수 있는 경우가 많습니다.

  DNS 필터링에서 암호화된 트래픽의 URL을 확인할 수 없는 경우, 해당 트래픽은 암호화된 트래픽에 대한 설정을 사용하여 처리됩니다.

도메인 조회 중 URL을 식별하도록 DNS 필터링 활성화(베타)

참고 이 기능은 릴리스 **6.7**에서 실험적으로 제공됩니다. 따라서 예상대로 작동하지 않을 수 있습니다. 프로덕션 환경에서는 사용하지 마십시오.

시작하기 전에

- 범주 및 평판을 사용하는 URL 필터링은 라이선스가 부여되고 활성화 및 설정되어야 합니다.

  (DNS 필터링은 URL 탭인 URL 그룹, URL 개체, URL 목록 및 피드, "Enter URL(URL 입력)" 텍스트 상자에 입력한 URL에서 다음 설정을 사용하지 않습니다.)

- DNS 필터링 제한, 1679 페이지의 제한 사항을 참조하십시오.

프로시저

단계 **1** 액세스 제어 정책의 **Advanced(고급)** 탭에서 **Enable reputation enforcement on DNS traffic(DNS 트래픽에 대한 평판 시행 활성화)**을 선택합니다.

단계 **2** 동일한 정책에서 URL 범주 및 평판 차단이 설정된 각 액세스 제어 규칙에 대해 다음을 수행합니다.

- **Applications(애플리케이션)** 탭에서 다음을 수행합니다.

  Selected Applications and Filters(선택한 애플리케이션 및 필터) 아래에 **any** 외에 아무것도 없는 경우, 해당 목록에 **DNS**를 추가합니다.

  (사용 가능한 애플리케이션 목록의 기타 DNS 관련 옵션은 이 목적과 관련이 없습니다.)

- **Ports(포트)** 탭에서 다음을 수행합니다.

Selected Destination Ports(선택한 대상 포트**)** 아래에 **any** 외에 아무것도 없는 경우, **DNS_over_TCP** 및 **DNS_over_UDP**를 추가합니다.

단계 **3** 변경 내용을 저장합니다.

다음에 수행할 작업

변경이 완료되면, 컨피그레이션 변경 사항 구축, 498 페이지.

DNS 필터링 제한

Block with reset(차단 후 재설정**)**, **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 작업이 있는 규칙과 일치하는 트래픽은 규칙 작업이 차단인 것처럼 처리됩니다.

차단된 URL에 액세스하려는 최종 사용자는 설명할 수 없는 페이지 연결 불가능을 경험하게 됩니다. 연결이 끊긴 다음 시간이 초과됩니다.

DNS 필터링 및 이벤트

DNS 필터링에 의해 생성된 연결 이벤트는 DNS 쿼리, URL 범주, URL 평판 및 대상 포트 필드를 사용하여 로깅됩니다. DNS 쿼리 필드에는 도메인 이름이 있습니다. DNS 필터링 일치의 경우 URL 필드가 비어 있습니다. 대상 포트는 53입니다.

또한:

- 액세스 제어 규칙 작업이 **Allow(**허용**)** 또는 **Trust(**신뢰**)**인 경우, 동일한 트래픽에 대해 두 개의 연결 이벤트가 생성됩니다. 하나는 DNS 필터링(**DNS** 쿼리 필드 입력) 및 하나는 URL 필터링(**URL** 필드 입력)입니다.
- 시스템에서 특정 URL을 처음 발견하면 해당 단일 세션에 대해 2개의 이벤트가 표시됩니다. 하나는 DNS 쿼리에 대해 분류되지 않았거나 평판이 없음을 표시하는 이벤트이고, 다른 하나는 DNS 쿼리 중에 검색된 URL의 실제 범주 및 평판을 표시하며 표준 URL 필터링을 사용하여 처리하는 동안 해당 세션에 적용됩니다.

수동 URL 필터링

액세스 제어 규칙에서는 개별 URL, URL 그룹 또는 URL 목록과 피드를 수동으로 필터링하여 카테고리 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의할 수 있습니다.

예를 들어 액세스 제어를 사용하여 조직에 적합하지 않은 웹 사이트 범주를 차단할 수 있습니다. 그러나 해당 범주에 액세스 권한을 제공하려는 적절한 웹 사이트가 포함된 경우에는 해당 사이트용으로 수동 허용 규칙을 생성한 다음 범주에 대한 차단 규칙 앞에 배치할 수 있습니다.

이러한 유형의 URL 필터링을 수행하는 데는 특별한 라이선스가 필요하지 않습니다.

수동 URL 필터링은 SSL 규칙에서는 지원되지 않습니다. SSL 규칙에서는 고유 이름 조건을 대신 사용해야 합니다.

주의 수동 URL 필터링을 구현하는 방법에 따라 URL 일치가 의도한 것과 다를 수 있습니다. 수동 URL 필터링 옵션, 1680 페이지의 내용을 참조하십시오.

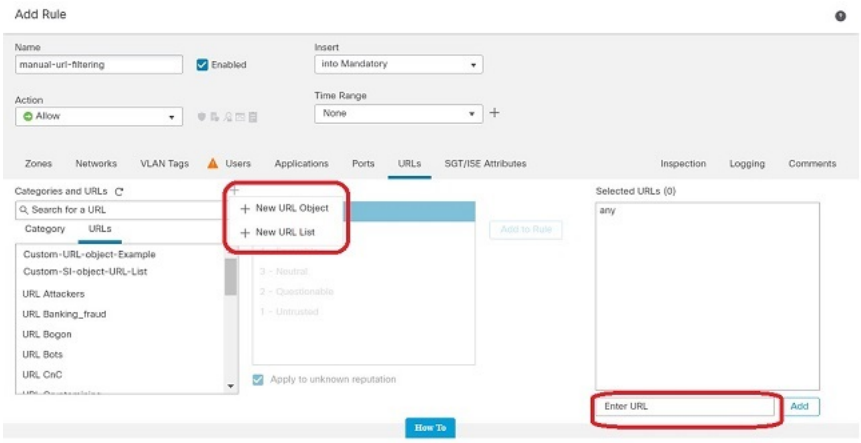
관련 항목

보안 인텔리전스 목록 및 피드, 597 페이지

수동 URL 필터링 옵션

수동 URL 필터링을 위해 URL을 지정하는 방법에는 여러 가지가 있습니다.

그림 *67:* 액세스 제어 규칙의 수동 *URL* 필터링 옵션



옵션	설명
(모범 사례) 사용자 지정 보안 인텔리전스 URL 목록 또는 피드 개체를 사용합니다. 웹 인터페이스의 규칙 페이지에 있는 **New URL List(**새 **URL** 목록**)** 옵션입니다.	이는 수동 URL 필터링에 권장되는 방법입니다. 새 목록 또는 피드를 생성하거나 액세스 제어 규칙의 URL 탭에 있는 URL 하위 탭에서 기존 목록 또는 피드를 선택할 수 있습니다. 자세한 내용은 사용자 지정 보안 인텔리전스 목록 및 피드, 603 페이지 및 하위 항목을 참조하십시오.

옵션	설명
URL 개체를 개별적으로 또는 그룹으로 사용합니다. (URL 개체는 URL URL 개체, 575 페이지에 설명되어 있습니다.)	URL 조건이 네트워크 트래픽과 일치하는지 확인하기 위해 시스템은 간단한 부분 문자열 일치를 실행합니다. 일치는 최상위 도메인에 고정되지 않습니다. 허용되는 문자열이 요청한 URL의 일부분과 일치하는 경우 URL은 일치 항목으로 간주됩니다. 예 1: **ign.com**(게임 사이트)를 명시적으로 차단하려는 경우 그러나 하위 문자열 일치 시에는 **ign.com**을 차단하면 **verisign.com**도 차단됩니다.
액세스 제어 규칙에 URL을 직접 입력합니다. (웹 인터페이스의 규칙 페이지에 있는 **Enter URL(URL 입력)** 옵션)	예 2: **example.com**의 모든 트래픽을 허용하는 경우, 사용자는 다음을 포함하는 URL을 찾아볼 수 있습니다. • **malicious-site.com/example.com** • **malicious-example.com** • **example.com.malicious-site.com** • **example.com.mx** • **example.com/** • **example.com/newexample** • **www.example.com/** **Enter URL(URL 입력)** 옵션은 와일드카드를 지원하지 않습니다.

범주 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의

액세스 제어 또는 QoS 규칙에서 보안 인텔리전스 URL 목록 및 피드를 사용하여 범주 및 평판 기반 URL 필터링 규칙을 보완하거나 예외를 지정할 수 있습니다.

(SSL 규칙에서 고유 이름 조건을 사용하여 이 목적을 제공합니다.)

시작하기 전에

- 범주 및 평판을 사용하여 URL 필터링을 설정합니다. URL 조건 설정, 1675 페이지의 내용을 참조하십시오.
- 수동 URL 필터링에 대한 중요한 모범 사례를 이해합니다. URL 필터링 모범 사례, 1667 페이지 및 수동 URL 필터링 옵션, 1680 페이지를 참조하십시오.
- 수동 필터링에 사용할 URL이 포함된 하나 이상의 보안 인텔리전스 개체(목록 또는 피드)를 설정합니다. 사용자 지정 보안 인텔리전스 목록 및 피드, 603 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 규칙을 정의할 액세스 제어 또는 QoS 정책으로 이동합니다.

단계 **2** 새 조건을 추가할 규칙을 생성하거나 편집합니다.

- 범주 또는 평판 기반 URL 필터링 규칙을 보완하는 경우, 기존 규칙을 편집합니다.
- 범주 또는 평판 기반 URL 필터링 규칙에 대한 예외를 재정의하거나 생성하는 경우, 새 규칙을 생성합니다.

단계 **3** 새 규칙을 생성하는 경우, 규칙 맨 위에 규칙 이름, 위치, 작업 및 기타 옵션을 설정합니다.

중요! 이 절차에서 설정 중인 목록 또는 피드에 범주 또는 평판 기반 규칙에 대한 예외가 포함된 경우, 규칙 순서에서 이 규칙 위에 해당 규칙을 추가합니다.

단계 **4** **URL**을 클릭합니다.

단계 **5** **Category(**범주**)** 탭 옆에 있는 **URL**을 클릭합니다.

단계 **6** 이 작업의 사전 요건에서 생성한 목록 또는 피드를 선택합니다.

단계 **7** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

단계 **8** **Add(**추가**)**를 클릭하거나 규칙을 계속 수정합니다.

다음에 수행할 작업

(선택 사항) SSL 규칙에서 고유 이름 조건을 사용하여 병렬 동작을 설정합니다.

URL 필터링 상태 모니터 설정

다음 상태 정책은 URL 카테고리 및 평판 데이터를 가져오거나 업데이트하는 데 문제가 발생하는 경우 알려줍니다.

- URL 필터링 모니터
- 디바이스에서 위협 데이터 업데이트

이것이 원하는 방식으로 구성되어 있는지 확인하려면 상태 모듈, 389 페이지 및 상태 모니터링 구성, 397 페이지를 참조하십시오.

URL 범주 및 평판

Talos에 의해 할당된 카테고리 또는 평판에 이의가 있는 경우, 재평가 요청을 제출할 수 있습니다.

시작하기 전에

Cisco 계정 자격 증명이 필요합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 다음 중 하나를 수행합니다.

분쟁 위치 옵션	분쟁 경로 옵션
클라우드 서비스 설정 페이지	a. **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)** 페이지로 이동합니다. b. **Dispute URL categories and reputations(URL** 카테고리 및 평판 이의 제기**)**를 선택합니다.
수동 URL 조회 페이지	a. 수동 URL 조회 페이지: **Analysis(**분석**) > Advanced(**고급**) > URL**로 이동합니다. b. 해당 URL을 조회합니다. c. 테이블 행 끝에서 **Disupte(**이의 제기**)**를 보려면 결과 목록에서 관련 항목 위에 마우스 커서를 올려놓은 다음 Disupte(이의 제기)를 클릭합니다.
URL 연결 이벤트	a. **Analysis(**분석**) > Connections(**연결**)** 메뉴에서 URL이 포함된 테이블이 있는 페이지로 이동합니다. b. **URL Category(URL** 카테고리**)** 또는 **URL Reputation(URL** 평판**)** 열에 있는 항목을 마우스 오른쪽 버튼으로 클릭하고(필요할 경우 숨겨진 열 표시) 옵션을 선택합니다.

별도의 브라우저 창에 Talos 웹사이트가 열립니다.

단계 **2** Cisco 자격 증명으로 Talos 사이트에 로그인합니다.

단계 **3** 정보를 검토하고 Talos 페이지의 지침을 따릅니다.

단계 **4** 제출된 이의 제기를 처리하는 방법과 예상할 수 있는 응답(있는 경우)에 대한 정보를 Talos 사이트에서 찾습니다.

이의 제기 프로세스는 Firepower 제품과 독립적입니다.

URL 범주 집합이 변경되면 작업 수행

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
URL 필터링	URL 필터링	Any(모든)	Any(모든)	관리자/액세스 관리자/네트워크 관리자

새로운 웹 동향과 발전하는 사용 패턴을 수용하기 위해 URL 필터링 카테고리 집합이 때때로 변경될 수 있습니다.

이러한 변경은 정책과 이벤트 모두에 영향을 미칩니다.

URL 범주 변경이 발생하기 직전에 발생하고, 발생한 후에는 변경의 영향을 받는 모든 액세스 제어, SSL 및 QoS 정책에서 규칙 목록에 알림이 표시되며, 사용자가 수정하는 규칙의 URL 또는 범주에서 알림이 표시됩니다.

이러한 알림이 표시되면 조치를 취해야 합니다.

참고 이 주제에서 설명하는 URL 카테고리 집합 업데이트는 단순히 새 URL을 기존 범주에 추가하고 잘못 분류된 URL을 다시 분류하는 변경 작업과는 다릅니다. 이 주제는 개별 URL의 카테고리 변경에는 적용되지 않습니다.

프로시저

단계 **1** 액세스 제어 정책에서 규칙 옆에 경고가 표시된다면, 알림 위에 마우스 커서를 올려 상세정보를 확인합니다.

단계 **2** 경고에서 URL 범주 변경 사항을 언급한다면, 규칙을 편집하여 상세정보를 확인합니다.

단계 **3** 규칙 대화상자의 URL 또는 Category(범주) 위에 마우스 커서를 올려 변경 유형에 대한 일반 정보를 확인합니다.

단계 **4** 범주 옆에 알림이 표시된다면 알림을 클릭하여 상세정보를 확인합니다.

단계 **5** 변경 사항 설명에 'More information(추가 정보)' 링크가 표시된다면, 링크를 클릭해 Talos 웹사이트에서 범주 관련 정보를 확인합니다.

대신 URL 카테고리 및 평판 설명, 1666 페이지에 있는 링크에서 모든 범주 목록과 설명을 확인해도 됩니다.

단계 **6** 변경 유형에 따라 적절한 조치를 취합니다.

카테고리 변경 유형	시스템이 수행할 작업	사용자가 수행해야 할 작업
기존 카테고리 사용은 조만간 중단됩니다.	아직은 적용되지 않습니다. 영향받는 규칙을 몇 주 안에 변경해야 합니다. 이 기간에 조치를 취하지 않으면, 시스템에서 정책을 재구축할 수 없게 됩니다.	이 범주를 포함하는 모든 규칙에서 이 범주를 제거합니다. 비슷한 새 범주가 있다면, 해당 범주를 사용하는 것도 고려해 보십시오.
새 카테고리가 추가됨	기본적으로 시스템에서는 새로 추가된 카테고리를 사용하지 않습니다.	새 카테고리에 대한 새 규칙을 생성하는 것이 좋습니다.

카테고리 변경 유형	시스템이 수행할 작업	사용자가 수행해야 할 작업
기존 카테고리가 삭제됨	해당 카테고리는 규칙에서 취소선 텍스트로 표시됩니다(즉 카테고리 이름에 취소선이 그어집니다).	구축하기 전에 사용하지 않는 카테고리를 규칙에서 삭제해야 합니다.

단계 **7** 이러한 변경 사항에 대한 SSL 규칙(Category(범주))을 확인하고 필요에 따라 조치를 취합니다.

단계 **8** 이러한 변경 사항에 대한 QoS 규칙(URL)을 확인하고 필요에 따라 조치를 취합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

URL 카테고리 및 평판 변경: 이벤트에 미치는 영향

- URL 카테고리가 변경되면 카테고리 변경 전에 시스템에서 처리한 이벤트는 원래 카테고리 이름과 연결되고 **Legacy** 레이블이 지정됩니다. 카테고리 변경 후 시스템에서 처리하는 이벤트는 새 카테고리에 연결됩니다.

  그보다 오래된 레거시 이벤트는 시간이 지나면 시스템에서 삭제됩니다.

- URL이 처리될 때 평판이 없었다면 이벤트 뷰어의 URL 평판 열이 비어 있게 됩니다.

URL 필터링 기록

기능	버전	세부 사항
DNS 필터링	6.7(베타)	각 액세스 제어 정책에 대한 고급 설정의 새로운 옵션을 사용하면 범주 및 평판별로 웹 트래픽을 조기에 필터링할 수 있습니다. 지원되는 플랫폼: 지원되는 버전의 FMC 7.0 및 관리되는 디바이스
평판이 알려지지 않은 사이트에 대한 처리를 지정할 수 있는 기능	6.7	이제 평판이 알려지지 않은 URL에 대한 처리를 지정할 수 있습니다. 수정된 화면: 액세스 제어 정책 및 QoS 정책의 URL 규칙 및 SSL 정책의 범주 규칙에는 평판 선택 영역 아래에 이 용도의 새 확인란이 포함되어 있습니다. 지원되는 플랫폼: 전체

기능	버전	세부 사항
신규 및 변경된 URL 카테고리 평판 수준의 새 이름	6.5	다음 변경 사항은 액세스 제어 및 QoS 정책의 URL 규칙과, SSL 정책의 범주 규칙에 적용됩니다. URL 범주 모음이 변경되었습니다. 이제 URL 규칙을 생성할 때 선택하는 범주가 두 '페이지'로 표시됩니다. 각 평판 수준과 연결된 이름이 변경되었습니다. 새 범주 및 평판 이름에 설명은 URL 카테고리 및 평판 설명, 1666 페이지의 내용을 참조하십시오. 업그레이드와 관련된 전체 상세정보는 버전 6.5 릴리스 노트 및 업그레이드 지침에서 확인할 수 있습니다. 나중에 범주 집합을 변경한다면, 이를 알리는 아이콘이 규칙에 표시됩니다. 수정된 화면: 액세스 제어 정책, SSL 정책, QoS 정책의 URL 규칙, URL 카테고리에 관련된 이벤트 데이터. 지원되는 플랫폼: 릴리스 6.5를 실행하는 FMC 및 디바이스
클래식 디바이스 라이선싱 관련 경미한 변경	6.5	기본 라이선스를 사용하는 디바이스의 경우, URL 필터링은 디바이스가 FMC에 등록되고 디바이스에 URL 필터링 라이선스가 할당된 후에 활성화됩니다. 지원되는 플랫폼: NGIPSv 및 FirePOWER 서비스 디바이스를 사용하는 ASA
Cisco Cloud에서 URL 데이터를 검색하는 주소 변경됨	6.5	인터넷 액세스 요구 사항, 3108 페이지의 URL 필터링 행을 참조하십시오.

기능	버전	세부 사항
할당된 URL 카테고리에 대한 이의 제기 기회	6.5	시스템에서 URL에 할당한 카테고리에 이의가 있는 경우, 카테고리 변경 요청을 제출할 수 있습니다. 신규/수정된 화면: • **Analysis(**분석**)** 메뉴 아래 연결 이벤트의 테이블에서 URL 카테고리 또는 평판을 마우스 오른쪽 버튼으로 클릭할 경우 새 메뉴 옵션. • URL 조회 페이지(**Analysis(**분석**) > Advanced(**고급**) > URL**)의 새 버튼. (버튼을 표시하려면 URL 위에 마우스 포인터를 올려놓으십시오.) • **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)** 페이지의 새로운 옵션 지원되는 플랫폼: 전체
Cisco CSI 탭 이름이 **Cloud Services(**클라우드 서비스**)**로 변경됨	6.4	수정된 화면 및 탐색: **System(**시스템**) > Integration(**통합**) > Cisco CSI**가 **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)**로 바뀜 지원되는 플랫폼: FMC
다양한 위치의 URL 필터링 정보를 이 새 URL 필터링 장으로 이동	6.3	URL 필터링을 위한 클라우드 통신 구성에 대한 정보를 이 새로운 URL 필터링 장으로 이동 그 밖의 일부 URL 필터링 정보를 다른 위치에서 이 장으로 이동 이와 관련하여 이 장의 Cisco CSI 주제의 구조를 변경
새 옵션: Cached URLs Expire(캐시된 URL 만료)	6.3	오래된 데이터에서 일치하는 URL의 인스턴스를 최소화하려면 이 제어를 사용하여 성능과 URL 카테고리 및 평판 데이터 새로 고침 사이의 균형을 유지하십시오. 수정된 화면: **System(**시스템**) > Integration(**통합**) > Cisco CSI**. 지원되는 플랫폼: 전체.

기능	버전	세부 사항
변경된 메뉴 경로	6.3	수동 URL 조회 페이지의 경로가 **Analysis(**분석**) > Lookup(**조회**) > URL**에서 **Analysis(**분석**) > Advanced(**고급**) > URL**로 변경되었습니다.

63 장

HTTP 응답 페이지 및 인터랙티브 차단

다음 주제에서는 시스템에서 웹 요청을 차단할 때 표시할 맞춤형 페이지를 구성하는 방법을 설명합니다.

- HTTP 응답 페이지 정보, 1689 페이지
- HTTP 응답 페이지 요구 사항 및 사전 요건, 1690 페이지
- HTTP 응답 페이지 선택, 1691 페이지
- HTTP 응답 페이지를 사용한 인터랙티브 차단, 1691 페이지

HTTP 응답 페이지 정보

액세스 제어의 일환으로 액세스 제어 규칙 또는 액세스 제어 정책 기본 작업을 사용하여 시스템이 웹 요청을 차단할 때 표시할 *HTTP* 응답 페이지를 구성할 수 있습니다.

표시되는 응답 페이지는 세션을 차단하는 방법에 따라 달라집니다.

- 응답 페이지 차단: 연결이 거부되었음을 설명하는 기본 브라우저 또는 서버 페이지를 재정의합니다.
- 응답 페이지 인터랙티브 차단: 사용자에게 경고하지만 사용자가 버튼을 클릭하거나 페이지를 새로 고쳐 원래 요청한 사이트를 로드하도록 허용합니다. 사용자는 로드하지 않은 페이지 요소를 로드하기 위해 응답 페이지를 우회한 후 새로 고침해야 할 수 있습니다.

응답 페이지를 선택하지 않으면 상호작용 또는 설명 없이 세션이 차단됩니다.

HTTP 대응 페이지의 제한

응답 페이지는 액세스 제어 규칙/기본 작업에 한정

시스템은 액세스 제어 규칙 또는 액세스 제어 정책 기본 작업을 통해 차단되거나 인터랙티브 차단된 암호화되지 않은 연결 또는 암호 해독된 연결에 대해서만 응답 페이지를 표시합니다. 다른 정책 또는 메커니즘에 의해 차단되거나 차단 목록에 추가된 연결에 대한 응답 페이지는 표시되지 않습니다.

응답 페이지를 표시하면 연결 재설정 비활성화

연결이 재설정되면 시스템이 응답 페이지를 표시할 수 없습니다(RST 패킷 전송). 응답 페이지를 활성화하면 시스템은 해당 구성에 우선 순위를 둡니다. **Block with reset(**차단 후 재설정**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)**을 규칙 작업으로 선택하는 경우, 시스템은 응답 페이지를 표시하고 일치하는 웹 연결을 재설정하지 않습니다. 차단된 해당 웹 연결을 재설정하려면 응답 페이지를 비활성화해야 합니다.

규칙과 일치하는 모든 비 웹 트래픽은 차단 후 재설정됩니다.

암호화된 연결의 응답 페이지 없음

시스템은 세션이 암호화되어 있거나 암호화되었던 경우 응답 페이지를 표시하지 않습니다.

'승격된' 연결의 응답 페이지 없음

승격된 액세스 제어 규칙(단순한 네트워크 조건만 사용하여 초기에 배치된 차단 규칙)으로 인해 웹 트래픽이 차단될 때는 시스템에서 응답 페이지를 표시하지 않습니다.

리디렉트된 특정 연결의 응답 페이지 없음

'http' 또는 'https'를 지정하지 않고 URL을 입력했으며, 브라우저가 포트 80에서 연결을 시작했고, 사용자가 응답 페이지를 클릭하고, 이후 연결이 포트 443으로 리디렉트된다면, 사용자는 두 번째 인터랙티브 페이지를 볼 수 없습니다. 이 URL에 대한 응답이 이미 캐시되었기 때문입니다.

URL 식별 전 응답 페이지 없음

시스템에서 요청된 URL을 식별하기 전에 웹 트래픽이 차단되면 시스템은 응답 페이지를 표시하지 않습니다. URL 필터링 모범 사례, 1667 페이지를 참조하십시오.

특정 디바이스에 대한 **URL** 범주가 있는 응답 페이지 없음

5506-X 및 5508-X 디바이스(FMC에서 관리하든 Adaptive Device Security Manager를 사용하든 상관없음)는 URL 범주를 사용하는 액세스 제어 규칙이 TLS 거짓 시작 트래픽과 일치하는 경우 응답 페이지를 표시하지 않습니다. TLS 거짓 시작 트래픽은 RFC 7918에 의해 정의됩니다.

HTTP 응답 페이지 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

HTTP 응답 페이지 선택

HTTP 응답 페이지의 안정적 표시 여부는 네트워크 구성, 트래픽 로드, 페이지 크기에 따라 달라집니다. 페이지 크기가 작을수록 성공적으로 표시될 가능성이 높습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **HTTP Responses(HTTP** 응답**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** **Block Response Page(**차단 응답 페이지**)** 및 **Interactive Block Resposne Page(**인터랙티브 차단 응답 페이지**)**를 선택합니다.

- System-provided(시스템 제공) - 일반 응답을 표시합니다. 보기 ( )를 클릭하면 이 페이지의 코드를 확인할 수 있습니다.
- Custom(맞춤형) - 맞춤형 응답 페이지를 생성합니다. 수정( )을 클릭하면 교체 또는 수정할 수 있는 시스템 제공 코드가 미리 채워진 팝업 창이 나타납니다. 사용한 문자 수가 카운터에 표시됩니다.
- None(없음) - 응답 페이지를 비활성화하고 상호작용 또는 설명 없이 세션을 차단합니다. 전체 액세스 제어 정책에서 인터랙티브 차단을 빠르게 비활성화하려면 이 옵션을 선택하십시오.

단계 **3** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

HTTP 응답 페이지를 사용한 인터랙티브 차단

인터랙티브 차단을 설정하면 사용자는 경고를 읽은 후 원래 요청된 사이트를 로드할 수 있습니다. 사용자는 로드하지 않은 페이지 요소를 로드하기 위해 응답 페이지를 우회한 후 새로 고침해야 할 수 있습니다.

팁 전체 액세스 제어 정책에서 인터랙티브 차단을 빠르게 비활성화하려면 시스템 제공 페이지나 맞춤형 페이지를 표시하지 마십시오. 그러면 시스템은 상호작용 없이 모든 연결을 차단합니다.

사용자가 인터랙티브 차단을 우회하지 않는 경우, 일치하는 트래픽은 추가 검사 없이 거부됩니다. 사용자가 인터랙티브 차단을 우회하는 경우, 액세스 제어 규칙은 트래픽을 허용하지만 해당 트래픽은 계속 심층 검사 및 차단 대상이 될 수 있습니다.

기본적으로 사용자 우회는 후속 방문 시 경고 페이지 표시 없이 10분(600초) 동안 유효합니다. 이 기간은 최대 1년까지 설정할 수 있으며, 사용자가 매번 차단을 강제로 우회하도록 할 수도 있습니다. 이러한 제한은 정책에서 모든 Interactive Block(인터랙티브 차단) 규칙을 적용합니다. 규칙별 제한은 설정할 수 없습니다.

인터랙티브 차단된 트래픽에 대한 로깅 옵션은 허용된 트래픽의 옵션과 동일하지만 사용자가 인터랙티브 차단을 우회하지 않는 경우, 시스템은 연결 시작 이벤트만 로깅할 수 있습니다. 시스템은 사용자에게 처음 경고할 때 인터랙티브 차단 또는 인터랙티브 차단 후 재설정 작업과 함께 로깅된 모든 연결 시작 이벤트를 표시합니다. 사용자가 차단을 우회하는 경우, 세션에 대해 로깅된 추가 연결 이벤트에는 `Allow(허용)` 작업이 있습니다.

인터랙티브 차단 설정

프로시저

단계 **1** 액세스 제어의 일부로 웹 트래픽과 일치하는 액세스 제어 규칙을 구성하십시오. 액세스 제어 규칙 생성 및 수정, 1651 페이지의 내용을 참조하십시오.

- 작업 - 규칙 작업을 **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)**으로 설정하십시오. 액세스 제어 규칙 인터랙티브 차단 작업, 1659 페이지의 내용을 참조하십시오.
- 조건 - URL 조건을 사용하여 인터랙티브 차단할 웹 트래픽을 지정합니다. URL 조건(URL 필터링), 545 페이지의 내용을 참조하십시오.
- 로깅 - 사용자가 차단을 우회할 것이라고 가정하고 그에 따라 로깅 옵션을 선택합니다. 허용된 연결에 대한 로깅, 2864 페이지의 내용을 참조하십시오.
- 검사 - 사용자가 차단을 우회할 것이라고 가정하고 그에 따라 심층 검사 옵션을 선택합니다. 액세스 제어의 이해, 1609 페이지의 내용을 참조하십시오.

단계 **2** (선택 사항) 액세스 제어 정책 **HTTP Responses(HTTP** 응답**)**에서 맞춤형 인터랙티브 차단 HTTP 응답 페이지를 선택합니다. HTTP 응답 페이지 선택, 1691 페이지의 내용을 참조하십시오.

단계 **3** (선택 사항) 액세스 제어 정책 **Advanced(**고급**)**에서 사용자 우회 시간 제한을 변경합니다. 차단된 웹사이트의 사용자 우회 시간 제한 설정, 1693 페이지의 내용을 참조하십시오.

사용자가 차단을 우회한 후 시스템은 시간 제한 기간이 경과할 때까지 사용자가 해당 페이지를 탐색하는 것을 경고 없이 허용합니다.

단계 **4** 액세스 제어 정책을 저장합니다.

단계 **5** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

차단된 웹사이트의 사용자 우회 시간 제한 설정

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** General Settings(일반 설정) 옆의 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Allow an Interactive Block to bypass blocking for (seconds)((**초**)** 동안 차단 우회를 위한 인터랙티브 차단 허용**)** 필드에 사용자 우회가 만료되기 전에 경과해야 하는 시간(초)을 입력합니다. 0을 지정하면 사용자가 매번 차단을 강제로 우회하도록 합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

64 장

보안 인텔리전스 차단 목록

다음 주제는 트래픽 차단 및 허용 트래픽 목록과 기본 구성 사용을 포함한 Security Intelligence의 개요를 제공합니다.

- 보안 인텔리전스 정보, 1695 페이지
- 보안 인텔리전스 모범 사례, 1696 페이지
- 보안 인텔리전스를 위한 라이선스 요건, 1697 페이지
- 보안 인텔리전스 요구 사항 및 사전 요건, 1697 페이지
- 보안 인텔리전스 소스, 1697 페이지
- 보안 인텔리전스 설정, 1698 페이지
- 보안 인텔리전스 모니터링, 1706 페이지
- 보안 인텔리전스 차단 재정의, 1706 페이지
- 보안 인텔리전스 문제 해결, 1707 페이지
- 보안 인텔리전스 차단 목록 히스토리, 1708 페이지

보안 인텔리전스 정보

악성 인터넷 콘텐츠를 차단하는 초기 방어선인 보안 인텔리전스는 평판 정보를 사용하여 IP 주소, URL, 도메인 이름과의 연결을 신속하게 차단합니다. 이를 보안 인텔리전스 차단 목록이라고 합니다.

보안 인텔리전스는 시스템에서 더 많은 리소스를 사용하는 평가를 수행하기 전에 이루어지는 첫 번째 액세스 제어 단계입니다. 차단 목록은 검사가 필요하지 않은 트래픽을 신속하게 제외하여 성능을 향상합니다.

참고 차단 목록을 사용하여 빠른 경로의 트래픽을 차단할 수 없습니다. 8000 Series 단축 경로는 보안 인텔리전스 필터링 이전에 지정됩니다. 단축 경로가 지정된 트래픽은 보안 인텔리전스를 비롯한 모든 추가적인 평가를 우회합니다.

사용자가 맞춤형 차단 목록을 설정할 수도 있으나, Cisco에서는 정기적으로 업데이트된 인텔리전스 피드에 대한 액세스를 제공합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다.

차단 안 함 목록 및 모니터링 전용 차단 목록을 사용하여 보안 인텔리전스 차단 목록을 세분화할 수 있습니다. 이러한 메커니즘에서는 트래픽이 차단 목록에 의해 차단되지 않지만, 일치하는 트래픽을 자동으로 신뢰하거나 일치하는 트래픽에 단축 경로를 지정하지 않습니다. 보안 인텔리전스 단계에서 차단 안 함 목록에 추가되거나 모니터링된 트래픽은 나머지 액세스 제어를 통해 추가적으로 분석됩니다.

관련 항목

보안 인텔리전스 목록 및 피드, 597 페이지
로깅할 수 있는 기타 연결, 2861 페이지
연결 및 보안 인텔리전스 이벤트 테이블 사용, 2900 페이지

보안 인텔리전스 모범 사례

- Cisco에서 제공하는 보안 인텔리전스 피드에서 탐지한 위협을 차단하도록 액세스 제어 정책을 구성합니다. 설정 예 : 보안 인텔리전스 차단, 1704 페이지의 내용을 참조하십시오.
- 사용자 지정 위협 데이터로 Cisco 제공 보안 인텔리전스 피드를 보완하거나 새로운 위협을 수동으로 차단하려는 경우:
  - IP 주소의 경우 사용자 지정 보안 인텔리전스 목록 및 피드 또는 네트워크 개체 또는 그룹을 사용합니다. 이러한 항목을 생성하려면 보안 인텔리전스 목록 및 피드, 597 페이지, 네트워크 개체, 571 페이지 및 해당 하위 항목을 참조하십시오. 보안 인텔리전스에 사용하려면 보안 인텔리전스 설정, 1698 페이지의 내용을 참조하십시오.
  - URL 및 도메인의 경우 개체 또는 그룹이 아닌 사용자 지정 보안 인텔리전스 목록 및 피드를 사용합니다. 자세한 내용은 수동 URL 필터링 옵션, 1680 페이지의 내용을 참조하십시오.
  - 이벤트의 차단 목록에 항목을 추가할 수도 있습니다. 글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지의 내용을 참조하십시오.
- 새 피드를 테스트하거나 수동 구축을 수행하려면 작업을 차단에서 모니터링 전용으로 설정합니다. 보안 인텔리전스 모니터링, 1706 페이지의 내용을 참조하십시오.
- 보안 인텔리전스 차단에서 특정 사이트 또는 주소를 제외해야 하는 경우 보안 인텔리전스 차단 재정의, 1706 페이지의 내용을 참조하십시오.
- Firepower 구축이 SecureX 또는 관련 툴 Cisco SecureX Threat Response(이전의 Cisco Threat Response 또는 CTR)과 통합되어 있고 사용자 지정 보안 인텔리전스 목록 및 피드를 사용하는 경우 이러한 목록 및 피드로 SSE(Security Services Exchange)를 업데이트해야 합니다. 자세한 내용은 SSE 온라인 도움말에서 이벤트 자동 승격 구성에 대한 지침을 참조하십시오. 이 통합에 대한 일반 정보는 Cisco SecureX와의 통합, 2749 페이지의 내용을 참조하십시오
- 시스템 제공 보안 인텔리전스 범주는 시간이 지남에 따라 알림 없이 변경될 수 있습니다. 정기적으로 변경 사항을 확인하고 그에 따라 정책을 수정해야 합니다.
- 또한 악성 사이트에 대한 추가 보호를 위해 별도의 라이선싱 요건이 있는 별도의 기능인 URL 필터링도 구성해야 합니다. URL 필터링, 1665 페이지의 내용을 참조하십시오.

보안 인텔리전스를 위한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

보안 인텔리전스 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

보안 인텔리전스 소스

- 시스템에서 제공한 피드

  Cisco에서는 도메인, URL 및 IP 주소에 대해서 정기적으로 업데이트된 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 자세한 내용은 보안 인텔리전스 목록 및 피드, 597 페이지를 참고하십시오.

  이름에 "TID"가 포함된 피드가 표시되는 경우 보안 인텔리전스에서 이 피드를 사용하지 않습니다. 대신 이 피드는 Cisco Threat Intelligence Director(TID), 1909 페이지에 설명된 기능에 사용됩니다.

- 서드파티 피드

  서드파티 피드 - Firepower Management Center이(가) 인터넷에서 정기적으로 다운로드하는 동적 목록인 서드파티 평판 피드로 Cisco 제공 피드를 보완합니다. 맞춤형 보안 인텔리전스 피드, 605 페이지의 내용을 참조하십시오.

- 맞춤형 차단 목록 또는 피드(또는 개체 또는 그룹)

  수동으로 생성된 목록 또는 피드를 사용하여 특정 IP 주소, URL 또는 도메인 이름을 차단합니다(IP 주소의 경우 네트워크 개체 또는 그룹을 사용할 수도 있음).

  예를 들어 피드에 의해 아직 차단되지 않은 악성 사이트 또는 주소를 알고 있는 경우 이러한 사이트를 맞춤형 보안 인텔리전스 목록에 추가하고 이 맞춤형 목록을 액세스 제어 정책의 보안 인텔리전스 탭에 있는 차단 목록에 추가합니다. 이 내용은 맞춤형 보안 인텔리전스 목록, 607 페이지 및 보안 인텔리전스 설정, 1698 페이지에 설명되어 있습니다.

  IP 주소의 경우 목록 또는 피드 대신 네트워크 개체를 선택적으로 사용할 수 있습니다. 자세한 내용은 네트워크 개체, 571 페이지를 참고하십시오. (URL의 경우 다른 방법보다 목록 및 피드를 사용하는 것이 좋습니다.)

- 맞춤형 차단 금지 목록 또는 피드

  특정 사이트 또는 주소에 대한 보안 인텔리전스 차단을 재정의합니다. 보안 인텔리전스 차단 재정의, 1706 페이지의 내용을 참조하십시오.

- 글로벌 차단 목록(네트워크, URL 및 DNS에 하나씩)

  이벤트를 검토하는 동안 보안 인텔리전스가 해당 소스의 향후 트래픽을 처리할 수 있도록 이벤트의 IP 주소, URL 또는 도메인을 즉시 적용 가능한 전역 차단 목록에 추가할 수 있습니다. 글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지의 내용을 참조하십시오.

- 전역 차단 금지 목록(네트워크, URL 및 DNS에 하나씩)

  보안 인텔리전스가 해당 소스의 향후 트래픽을 차단하지 않도록 하려면 이벤트를 검토하는 동안 이벤트의 IP 주소, URL 또는 도메인을 해당 Global Do Not Block List(글로벌 차단 금지 목록)에 즉시 추가할 수 있습니다. 글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지의 내용을 참조하십시오.

보안 인텔리전스 설정

액세스 제어 정책마다 보안 인텔리전스 옵션이 있습니다. 네트워크 개체, URL 개체 및 목록, 보안 인텔리전스 피드 및 목록을 차단 목록 또는 차단 안 함 목록에 추가할 수 있으며, 이 모두를 보안 영역으로 제한할 수 있습니다. 또한 DNS 정책을 액세스 제어 정책에 연결하고 도메인 이름을 차단 목록 또는 차단 안 함 목록에 추가할 수 있습니다.

차단 안 함 목록의 개체 수와 차단 목록의 개체 수를 합해 125개의 네트워크 개체 또는 32767개의 URL 개체 및 목록을 초과할 수 없습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

주의 액세스 제어 정책의 Security Intelligence(보안 인텔리전스)에서 차단 안 함 목록 또는 차단 목록에 여러 개체를 추가하거나 삭제하면 경우에 따라 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. Snort 프로세스가 재시작되는지 여부는 검사에 사용할 수 있는 메모리에 따라 디바이스별로 달라질 수 있습니다.

시작하기 전에

- 팁 : 최소 구성 권장 사항에 대한 지침은 설정 예 : 보안 인텔리전스 차단, 1704 페이지의 내용을 참조하십시오.
- 모든 옵션을 선택할 수 있게 하려면, 관리 센터에 매니지드 디바이스를 하나 이상 추가합니다.
- 수동 구축에서 또는 보안 인텔리전스 필터링을 모니터링 한정으로 설정하려면 로깅을 활성화하십시오. 보안 인텔리전스로 연결 로깅, 2871 페이지의 내용을 참조하십시오.
- 도메인에 대한 보안 인텔리전스 작업을 수행하도록 DNS 정책을 설정합니다. 자세한 내용은 DNS 정책, 1709 페이지를 참고하십시오.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- **Networks(**네트워크**)**를 클릭하여 네트워크 개체(IP 주소)를 추가합니다.
- **URL**을 클릭하여 URL 개체를 추가합니다.

단계 **3** 차단 또는 차단 안 함 목록에 추가 할 **Available Objects(**사용 가능한 개체**)**를 찾습니다. 다음 옵션을 이용할 수 있습니다.

- **Search by name or value(**이름 또는 값으로 검색**)** 필드에 입력하여 사용할 수 있는 개체를 검색합니다. 다시 로드( ) 또는 지우기( )를 클릭하여 검색 문자열을 지웁니다.
- 요구를 충족하는 기존 목록이나 피드가 없는 경우, 추가( )을 클릭하고 **New Network List(**새 네트워크 목록**)** 또는 **New URL List(**새 **URL** 목록**)**를 선택하고 보안 인텔리전스 피드 생성, 606 페이지 또는 새 보안 인텔리전스 목록을 다음에 업로드 Firepower Management Center, 608 페이지의 설명에 따라 계속합니다.

- 요구를 충족하는 기존 개체가 없는 경우, 추가( )을 클릭하고 **New Network Object(**새 네트워크 개체**)** 또는 **New URL Object(**새 **URL** 개체**)**를 선택하고 네트워크 개체 생성, 571 페이지의 설명에 따라 계속합니다.

보안 인텔리전스는 /0 넷마스크를 사용하는 IP 주소 차단을 무시합니다.

단계 **4** 추가할 하나 이상의 사용 가능한 개체를 선택합니다.

단계 **5** (선택 사항) **Available Zone(**가용 영역**)**을 선택하여 선택된 개체를 영역별로 제한합니다.

시스템에서 제공한 보안 인텔리전스 목록은 영역별로 제한할 수 없습니다.

단계 **6** **Add to Do Not Block list(**차단 안 함 목록에 추가**)** 또는 **Add to Block list(**차단 목록에 추가**)**를 클릭하거나 선택한 항목을 클릭하고 차단 안 함 또는 차단 목록으로 끕니다.

차단 안 함 또는 차단 목록에서 개체를 제거하려면 삭제( )을 클릭합니다. 여러 개체를 제거하려면 여러 개체를 선택하고 **Delete Selected(**선택한 항목 삭제**)**를 마우스 오른쪽 버튼으로 클릭합니다.

단계 **7** (선택 사항) **Block List(**차단 목록**)**에서 마우스 오른쪽 버튼으로 개체를 클릭한 다음 **Monitor-only (do not block)(**모니터링 한정**(**차단 안 함**))**을 선택하여 차단 목록에 추가된 개체를 모니터링 한정으로 설정합니다.

시스템에서 제공한 전역 보안 인텔리전스 목록을 모니터링용으로만 설정할 수 없습니다.

단계 **8** **DNS Policy(DNS** 정책**)** 드롭다운 목록에서 DNS 정책을 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

보안 인텔리전스 목록 및 피드, 597 페이지
Snort® 재시작 시나리오, 505 페이지

보안 인텔리전스 옵션

액세스 제어 정책 편집기의 Security Intelligence(보안 인텔리전스) 탭을 사용하여 네트워크(IP 주소) 및 URL 보안 인텔리전스를 설정하고 도메인에 대해 보안 인텔리전스를 설정한 DNS 정책과 액세스 제어 정책을 연결합니다.

사용 가능한 개체

사용 가능한 개체는 다음과 같습니다.

- 시스템에서 제공하는 피드로 채워진 보안 인텔리전스 범주입니다.

  자세한 내용은 보안 인텔리전스 카테고리, 1702 페이지 섹션을 참조해 주십시오.

- 시스템에서 제공하는 전역 차단 및 차단 안 함 목록입니다.

  자세한 내용은 보안 인텔리전스 소스, 1697 페이지를 참조하십시오.

- Security Intelligence(보안 인텔리전스)에는 Object(개체) > Object Management(개체 관리) > Security Intelligence(보안 인텔리전스) 아래에서 생성되는 피드와 목록이 나열됩니다.

  자세한 내용은 보안 인텔리전스 소스, 1697 페이지를 참조하십시오.

- Object(개체) > Object Management(개체 관리) 아래의 해당 페이지에 설정된 네트워크 및 URL 개체와 그룹입니다. 이는 이전 글머리 기호의 보안 인텔리전스 개체와 다릅니다.

  네트워크 개체에 대한 자세한 내용은 네트워크 개체, 571 페이지의 내용을 참조하십시오. (URL의 경우, 개체 또는 그룹 대신 보안 인텔리전스 목록 또는 피드를 사용합니다.)

사용 가능한 영역

시스템에서 제공하는 전역 목록을 제외하고 보안 인텔리전스 필터링을 영역별로 제한할 수 있습니다.

예를 들면, 성능을 개선하기 위해 대상 엔타이틀먼트를 지정할 수 있습니다. 보다 구체적으로는, 이메일 트래픽을 처리하는 보안 영역에 대해서만 스팸을 차단할 수 있습니다.

여러 영역에서 하나의 개체를 대상으로 보안 인텔리전스 필터링을 수행하려면 개체를 각 영역에 대해 별개로 차단 목록 또는 차단 안 함 목록에 추가해야 합니다.

DNS 정책

보안 인텔리전스를 사용하여 DNS 트래픽을 일치시키려면 보안 인텔리전스 설정에 대한 DNS 정책을 선택해야 합니다.

DNS 목록 또는 피드를 기준으로 차단 목록 또는 차단 안 함 목록에 추가하거나 트래픽을 모니터링하려면 다음을 수행해야 합니다.

- DNS 보안 인텔리전스 목록 및 피드를 구성합니다. 보안 인텔리전스 목록 및 피드, 597 페이지의 내용을 참조하십시오.
- DNS 정책을 생성합니다. 자세한 내용은 기본 DNS 정책 생성, 1712 페이지를 참조하십시오.
- DNS 목록 또는 피드를 참조하는 DNS 규칙을 설정합니다. 자세한 내용은 DNS 규칙 생성 및 편집, 1714 페이지를 참조하십시오.
- 액세스 제어 정책의 일부로 DNS 정책을 구축하기 때문에 두 정책을 모두 연결해야 합니다. 자세한 내용은 DNS 정책 구축, 1721 페이지를 참조하십시오.

차단 안 함 목록

보안 인텔리전스 차단 재정의, 1706 페이지의 내용을 참조하십시오.

목록의 모든 개체를 선택하려면 개체를 마우스 오른쪽 버튼으로 클릭합니다.

차단 목록

이 장의 설정 예 : 보안 인텔리전스 차단, 1704 페이지 및 기타 주제를 참조하십시오.

차단 목록의 시각적 표시기에 대한 설명은 차단 목록 아이콘, 1704 페이지의 내용을 참조하십시오.

목록의 모든 개체를 선택하려면 개체를 마우스 오른쪽 버튼으로 클릭합니다.

로깅

기본적으로 활성화되어 있는 보안 인텔리전스 로깅은 액세스 제어 정책의 대상 디바이스에 의해 처리되는 차단된 연결 및 모니터링되는 연결을 모두 로깅합니다. 그러나 시스템은 차단 안 함 목록에 일치하는 연결은 로깅하지 않습니다. 차단 안 함 목록으로 분류된 연결의 로깅은 최종 처리에 따라 다릅니다. 차단 목록의 연결에 대해 로깅을 활성화해야 해당 목록의 개체를 모니터링 전용으로 설정할 수 있습니다.

로깅 설정을 활성화, 비활성화 또는 확인하려면 차단 목록에서 개체를 마우스 오른쪽 버튼으로 클릭합니다.

관련 항목

글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지
보안 인텔리전스 목록 및 멀티테넌시, 599 페이지

보안 인텔리전스 카테고리

보안 인텔리전스 범주는 보안 인텔리전스 목록 및 피드, 597 페이지에 설명된 시스템 제공 피드에 의해 결정됩니다.

이러한 범주는 다음 위치에서 사용됩니다.

- 액세스 제어 정책의 Security Intelligence(보안 인텔리전스) 탭에 있는 Networks(네트워크) 하위 탭
- 액세스 제어 정책의 Security Intelligence(보안 인텔리전스) 탭에서 Networks(네트워크) 탭 옆에 있는 URL 하위 탭
- DNS 규칙 구성 페이지의 DNS 탭에 있는 DNS 정책에서
- 트래픽이 위 위치의 차단 또는 모니터링 구성과 일치할 때 생성되는 이벤트에서

참고 조직에서 Cisco Threat Intelligence Director(TID)을(를) 사용하는 경우: 이벤트를 확인할 때, `TID URL Block(TID URL 차단)` 같은 작업을 TID가 수행했음을 알리는 범주가 표시될 수도 있습니다.

Talos가 클라우드에서 범주를 업데이트하며, 이 목록은 Firepower 릴리스와 관계 없이 변경될 수 있습니다.

표 ***101: Cisco Talos Intelligence Group(Talos)*** 피드 카테고리

보안인텔리전스카테고리	설명
Attackers	아웃바운드의 악의적 활동으로 알려진 액티브 스캐너 및 호스트
Banking_fraud	전자 뱅킹과 관련된 사기성 활동을 수행하는 사이트
Bogon	bogon 네트워크 및 할당되지 않은 IP 주소
Bots	바이너리 악성코드 드로퍼를 호스팅하는 사이트
CnC	봇넷용 CnC(Command-and-Control) 서버를 호스팅하는 사이트
Cryptomining	크립토마이닝 마이닝을 위해 풀 및 월렛에 대한 원격 액세스를 제공하는 호스트
Dga	CnC 서버에서 RP(Rendezvous Point) 역할을 하는 많은 수의 도메인 이름을 생성하는 데 사용되는 악성코드 알고리즘
Exploitkit	클라이언트에서 소프트웨어 취약성을 식별하도록 설계된 소프트웨어 킷
High_risk	보안 그래프의 OpenDNS 예측 보안 알고리즘과 일치하는 도메인 및 호스트 이름
Ioc	IOC(Indicator of Compromise)에 관련된 것으로 관찰된 호스트
Link_sharing	저작권이 있는 파일을 허가 없이 공유하는 웹사이트
Malicious	반드시 더 세부적인 또 다른 위협 범주에 해당하지는 않지만 악의적인 행동을 보이는 사이트
Malware	악성코드 바이너리 또는 익스플로잇 킷을 호스팅하는 사이트
Newly_seen	최근에 등록되었거나 텔레메트리를 통해 아직 확인되지 않은 도메인
Open_proxy	익명의 웹 브라우징을 허용하는 오픈 프록시
Open_relay	스팸에 사용되는 것으로 알려진 오픈 메일 릴레이
Phishing	피싱 페이지를 호스팅하는 사이트
Response	악성 활동 또는 의심스러운 활동에 적극적으로 참여하고 있는 IP 주소 및 URL
Spam	스팸을 전송하는 것으로 알려진 메일 호스트
Spyware	스파이웨어 및 애드웨어 활동을 포함, 제공 또는 지원하는 것으로 알려진 사이트
Suspicious	알려진 악성코드와 유사한 특성을 지니고 있으며 의심스러워 보이는 파일

보안 인텔리전스 카테고리	설명
tor_exit_node	Tor Anonymizer 네트워크에 대한 종료 노드 서비스를 제공하는 것으로 알려진 호스트

차단 목록 아이콘

액세스 제어 정책에서 Security Intelligence(보안 인텔리전스) 탭의 Block(차단) 목록에 다음과 같은 시각적 표시가 나타날 수 있습니다.

아이콘 또는 시각적 표시	설명
차단( )	개체가 차단으로 설정되어 있습니다.
모니터( )	개체가 모니터링 전용으로 설정되어 있습니다. 보안 인텔리전스 모니터링, 1706 페이지의 내용을 참조하십시오.
개체는 취소선 텍스트로 표시됩니다.	동일한 개체가 차단 금지 목록에 있으면 차단이 무시됩니다.

설정 예: 보안 인텔리전스 차단

시스템의 정기적으로 업데이트되는 보안 인텔리전스 피드에서 탐지할 수 있는 모든 위협을 차단하도록 액세스 제어 정책을 설정합니다.

차단 목록의 개체 수와 차단 안 함 목록의 개체 수를 합해 125개의 네트워크 개체 또는 32767개의 URL 개체 및 목록을 초과할 수 없습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

주의 액세스 제어 정책의 Security Intelligence(보안 인텔리전스)에서 차단 목록 또는 차단 안 함 목록에 여러 개체를 추가하거나 삭제하면 경우에 따라 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. Snort 프로세스가 재시작되는지 여부는 검사에 사용할 수 있는 메모리에 따라 디바이스별로 달라질 수 있습니다.

시작하기 전에

- 모든 옵션을 선택할 수 있게 하려면, 관리 센터에 매니지드 디바이스를 하나 이상 추가합니다.
- 도메인에 대한 모든 보안 인텔리전스 위협 범주를 차단하도록 DNS 정책을 설정합니다. 자세한 내용은 DNS 정책, 1709 페이지를 참고하십시오.
- 차단할 사용자 지정 엔터티 목록이 있거나 있을 예정인 경우 각 유형(URL, DNS, 네트워크)의 보안 인텔리전스 개체를 생성합니다. 보안 인텔리전스 목록 및 피드, 597 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.

단계 **2** 새로운 액세스 제어 정책을 만들거나 기존 정책을 편집합니다.

단계 **3** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **4** IP 주소에 대한 차단 기준을 추가하려면 **Networks(**네트워크**)**를 클릭합니다.

a) Networks(네트워크) 목록에서 아래로 스크롤하여 Global(전역) 목록 아래에 나열된 모든 위협 범주를 선택합니다.
b) 해당하는 경우 이러한 위협을 차단할 보안 영역을 선택합니다.
c) **Add to Block List(**차단 목록에 추가**)**를 클릭합니다.
d) 차단할 주소가 있는 맞춤형 목록 또는 피드를 생성한 경우 위와 동일한 단계를 사용하여 차단 목록에 추가합니다.

단계 **5** URL에 대한 차단 기준을 추가하려면 **URL**을 클릭하고 네트워크에 대해 수행한 단계를 반복합니다.

단계 **6** **DNS Policy(DNS** 정책**)** 드롭다운 목록에서 DNS 정책을 선택합니다. DNS 정책 개요, 1709 페이지의 내용을 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 이러한 연결에 대한 로깅을 활성화합니다. 보안 인텔리전스로 연결 로깅, 2871 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

보안 인텔리전스 모니터링

모니터링은 보안 인텔리전스에 의해 차단되었지만 트래픽을 차단하지는 않는 트래픽에 대한 연결 이벤트를 로깅합니다. 모니터링은 특히 다음에 유용합니다.

- 피드를 구현하기 전에 테스트합니다.

  서드파티 피드 사용에 대한 차단을 실행하기 전에 해당 피드 테스트를 원하는 시나리오를 고려해 보십시오. 피드를 모니터링 한정으로 설정하면, 시스템은 시스템이 추가 분석을 위해 차단할 수도 있었던 연결을 허용하며, 사용자 평가를 위해 각 연결의 레코드를 로깅합니다.

- 패시브 구축-성능 최적화

  수동으로 구축된 매니지드 디바이스는 트래픽 흐름에 영향을 줄 수 없으며, 트래픽을 차단하도록 시스템을 구성해도 이점이 없습니다. 또한, 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에 시스템은 각 차단된 연결에 대한 여러 초기 연결 이벤트를 보고할 수 있습니다.

보안 인텔리전스 피드를 구성하려면 다음을 수행합니다.

의 지침에 따라 보안 인텔리전스 차단을 구성한 후 Block (차단) 목록에서 해당하는 각 개체를 마우스 오른쪽 버튼으로 클릭하고 Monitor-only (모니터링 전용)를 선택합니다.설정 예 : 보안 인텔리전스 차단, 1704 페이지 시스템에서 제공한 보안 인텔리전스 목록을 모니터링용으로만 설정할 수 없습니다.

보안 인텔리전스 차단 재정의

아니면 Do Not Block(차단 안 함) 목록을 사용하여 특정 도메인, URL 또는 IP 주소가 보안 인텔리전스 목록 또는 피드에 의해 차단되지 않도록 제외할 수 있습니다.

예를 들어, 다음이 가능합니다.

- 평판이 좋은 보안 인텔리전스 피드에서 가끔 오탐 블록을 재정의합니다.
- 평판을 기준으로 특정 트래픽을 조기에 차단하는 대신 심층적으로 검사
- 보안 인텔리전스 차단에서 영역을 기준으로 달리 제한되는 트랜잭션 제외

  잘못 분류된 URL을 Do Not Block(차단 안 함) 목록에 추가한 다음 이러한 URL에 액세스해야 하는 조직 내 사용자들이 사용하는 보안 영역을 사용하여 Do Not Block(차단 안 함) 개체를 제한할 수 있습니다. 이렇게 하면 업무상 필요가 있는 사용자만 Do Not Block(차단 안 함) 목록에 추가된 URL에 액세스할 수 있습니다.

참고 Do Not Block(차단 안 함) 목록의 항목은 자동으로 신뢰되거나 빠른 경로가 아닙니다. 이 트래픽은 나머지 액세스 제어를 통해 의도적으로 추가 분석될 수 있습니다.

프로시저

단계 **1** 옵션 1: 이벤트의 IP 주소, URL 또는 도메인을 Global Do Not Block(전역 차단 금지) 목록에 추가합니다. 글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지의 내용을 참조하십시오.

단계 **2** 옵션 2: 맞춤형 보안 인텔리전스 목록 또는 피드를 사용합니다.

a) 맞춤형 보안 인텔리전스 목록 또는 피드를 생성합니다. 맞춤형 보안 인텔리전스 목록, 607 페이지 또는 보안 인텔리전스 피드 생성, 606 페이지를 참조하십시오.

b) IP 주소(네트워크) 및 URL의 경우: 액세스 제어 정책을 수정하려면 Security Intelligence(보안 인텔리전스) 탭을 클릭한 다음 Networks or URLs(네트워크 또는 URL) 하위 탭에서 맞춤형 목록 또는 피드를 클릭하고 **Add to Do Not Block List(**차단 안 함 목록에 추가**)**를 클릭합니다.

c) 변경 내용을 저장합니다.

d) 도메인(DNS)의 경우: 보안 인텔리전스 옵션, 1700 페이지 항목의 "DNS 정책" 섹션을 참조하십시오.

e) 변경 사항을 배포합니다.

보안 인텔리전스 문제 해결

사용 가능한 옵션 목록에 보안 인텔리전스 범주가 없음

증상**:** 액세스 제어 정책의 Security Intelligence(보안 인텔리전스) 탭에서, 보안 인텔리전스 범주(CnC, Exploitkit 등)는 Available Options(사용 가능한 옵션)의 Networks(네트워크) 탭에 표시되지 않습니다.

원인**:**

- 이러한 범주는 관리 센터에 하나 이상의 매니지드 디바이스를 추가할 때까지 표시되지 않습니다. 모든 TALOS 피드를 가져오려면 디바이스를 추가해야 합니다.
- URL 필터링 기능은 보안 인텔리전스 기능과 다른 범주 집합을 사용합니다. 표시되는 범주는 URL 필터링 범주일 수 있습니다. URL 필터링 범주를 보려면 액세스 제어 규칙의 **URL** 탭을 확인하십시오.

메모리 사용 문제 해결

증상**:** 보안 인텔리전스 차단 목록에 의해 차단되어야 하는 연결이 대신 액세스 제어 규칙에 의해 평가됩니다. 보안 인텔리전스 상태 모듈이 메모리가 부족하다고 알립합니다.

원인**:** 메모리 제한. Cisco Intelligence Feeds는 Cisco Talos Intelligence Group(Talos)의 최신 위협 인텔리전스에 기반합니다. 이러한 피드는 시간이 지남에 따라 커지는 경향이 있습니다. Firepower 디바이스는 피드 업데이트를 수신할 때 보안 인텔리전스에 할당한 메모리에 최대한 많은 항목을 로드합니다. 디바이스가 모든 항목을 로드할 수 없는 경우, 정상적으로 트래픽을 차단하지 못할 수 있습니다. 차단 목록에 의해 차단되어야 하는 일부 연결이 차단되는 대신 액세스 제어 규칙에 의해 계속 평가됩니다.

영향을 받는 플랫폼**:** 메모리가 적은 디바이스는 많은 보안 인텔리전스 범주를 차단 목록에 포함하거나 범주와 평판을 기준으로 URL도 필터링하는 경우, 이 문제가 발생할 가능성이 특히 높습니다. 이러한 디바이스에는 Firepower 7010, 7020, 7030; 5508-X, 5516-X NGIPSv가 포함됩니다.

해결 방법**:** 이 문제가 발생하고 있다고 생각하는 경우, 영향을 받는 디바이스에 설정을 다시 구축하십시오. 이렇게 하면 보안 인텔리전스에 더 많은 메모리를 할당할 수 있습니다. 문제가 계속되면 Cisco TAC(Technical Assistance Center)에 문의하십시오. 문제 확인을 돕고 구축에 적합한 솔루션을 제안할 수 있습니다.

보안 인텔리전스 차단 목록 히스토리

기능	버전	세부 사항
새로운 보안 인텔리전스 범주	모두	Talos는 다음과 같은 새로운 보안 인텔리전스 범주를 추가했습니다. • banking_fraud • ioc • high_risk • link_sharing • 발생하는 것만은 아님 • newly_seen • 스파이웨어 액세스 제어 및 DNS 정책을 업데이트하여 새 범주를 처리하고 향후 변경 사항을 주기적으로 확인해야 합니다. 신규/수정 페이지: Security Intelligence(보안 인텔리전스) 탭, Networks and URLs(네트워크 및 URL) 하위 탭; DNS 정책의 DNS 규칙 지원되는 플랫폼: FMC

65 장

DNS 정책

다음 주제에서는 DNS 정책, DNS 규칙 및 매니지드 디바이스에 DNS 정책을 구축하는 방법을 설명합니다.

- DNS 정책 개요, 1709 페이지
- DLP 정책 구성 요소, 1710 페이지
- DNS 정책을 위한 라이선스 요구 사항, 1711 페이지
- DNS 프로파일 요구 사항 및 사전 요건, 1711 페이지
- DNS 정책 관리, 1711 페이지
- DNS 규칙, 1713 페이지
- DNS 정책 구축, 1721 페이지

DNS 정책 개요

DNS 기반 보안 인텔리전스를 사용하면 클라이언트가 요청한 도메인 이름을 바탕으로 보안 인텔리전스 차단 목록을 통해 트래픽을 차단할 수 있습니다. Cisco에서는 트래픽을 필터링하는 데 사용할 수 있는 도메인 이름 인텔리전스를 제공합니다. 또한 환경에 맞는 도메인 이름 목록 및 피드를 사용자 설정할 수도 있습니다.

DNS 정책 차단 목록의 트래픽은 즉시 차단되므로 침입, 익스플로잇, 악성코드에 대한 추가 검사 대상이 되지 않을 뿐 아니라 네트워크 검색 대상도 되지 않습니다. 보안 인텔리전스 차단 안 함 목록을 사용하여 차단 목록을 재정의하고 액세스 제어 규칙 평가를 강제 적용할 수 있으며 보안 인텔리전트 필터링에 "모니터링 전용" 설정을 사용할 수도 있습니다(패시브 구축에 권장됨). 이렇게 하면 시스템에서 차단 목록에 의해 차단되었을 가능성이 있는 연결을 분석할 수 있을 뿐 아니라 차단 목록과 일치하는 항목을 로깅하고 연결 종료 보안 인텔리전스 이벤트를 생성할 수 있습니다.

참고 DNS 서버가 만료로 인해 도메인 캐시를 삭제하거나 클라이언트의 DNS 캐시 또는 로컬 DNS 서버의 캐시가 지워지거나 만료되지 않는 경우, DNS 기반 보안 인텔리전스가 도메인 이름에서 예상대로 작동하지 않을 수 있습니다.

DNS 정책 및 관련 DNS 규칙을 사용하여 DNS 기반 보안 인텔리전스를 구성합니다. 이 보안 인텔리전스를 디바이스에 구축하려면 DNS 정책을 액세스 제어 정책에 연결한 다음 매니지드 디바이스에 설정을 구축해야 합니다.

DLP 정책 구성 요소

DNS 정책을 사용하면 차단 목록을 사용하여 도메인 이름을 기준으로 연결을 차단하거나 Do Not Block(차단 금지) 목록을 사용하여 이러한 연결을 차단에서 제외할 수 있습니다. 다음 목록에서는 DNS 정책을 생성한 후에 변경할 수 있는 컨피그레이션에 대해 설명합니다.

이름 및 설명

각 DNS 정책에는 고유한 이름이 있어야 합니다. 설명은 선택 사항입니다.

다중 도메인 구축에서 정책 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 정책 이름과의 충돌을 식별할 수 있습니다.

규칙

규칙을 사용하면 도메인 이름을 기준으로 네트워크 트래픽을 더 자세히 처리할 수 있습니다. DNS 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 DNS 규칙과 일치하는지 확인합니다.

DNS 정책을 생성하면 시스템은 해당 정책에 DNS 규칙에 대한 기본 글로벌 화이트리스트 그리고 DNS 규칙에 대한 기본 글로벌 차단 목록을 입력합니다. 두 규칙 모두 해당 카테고리의 첫 번째 위치에 고정됩니다. 이러한 규칙을 수정할 수는 없지만 비활성화할 수는 있습니다.

다중 도메인 구축에서 시스템은 상위 도메인의 DNS 정책에 하위 항목 DNS 화이트리스트 및 하위 항목 DNS 차단 목록 규칙도 추가합니다. 이러한 규칙은 해당 카테고리의 두 번째 위치에 고정됩니다.

참고 Firepower Management Center에 멀티테넌시가 활성화된 경우, 시스템은 상위 및 하위 항목 도메인을 포함한 도메인 계층으로 구성됩니다. 이러한 도메인은 고유하며 DNS 관리에 사용되는 도메인 이름과 구별됩니다.

하위 항목 목록에는 Firepower System 서브도메인 사용자의 차단 또는 차단 금지 목록에 대한 도메인이 포함됩니다. 상위 도메인에서 하위 목록의 내용을 볼 수 없습니다. 하위 도메인 사용자가 차단 또는 차단 금지 목록에 도메인을 추가하지 못하게 하려면 다음을 수행합니다.

- 하위 항목 목록 규칙을 비활성화하고
- 액세스 제어 정책 상속 설정을 사용하여 보안 인텔리전스를 적용합니다.

시스템은 다음 순서로 규칙을 평가합니다.

- DNS 규칙에 대한 글로벌 화이트리스트 (활성화되어 있을 경우)
- 하위 항목 DNS 화이트리스트 규칙(활성화된 경우)

- 화이트리스트 규칙
- DNS 규칙에 대한 글로벌 차단 목록(활성화된 경우)
- 하위 항목 DNS 차단 목록 규칙(활성화된 경우)
- 화이트리스트 이외 작업 규칙

일반적으로 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 DNS 규칙에 따라 DN 기반 네트워크 트래픽을 처리합니다. 트래픽과 일치하는 DNS 규칙이 없으면 시스템은 연결된 액세스 제어 정책의 규칙을 기준으로 트래픽을 계속 평가합니다. DNS 규칙 조건은 단순할 수도 있고 복잡할 수도 있습니다.

DNS 정책을 위한 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

DNS 프로파일 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

DNS 정책 관리

DNS 정책 페이지(**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**)를 사용하여 맞춤형 DNS 정책을 관리합니다. 사용자가 생성하는 맞춤형 정책 외에도 시스템은 기본 차단 목록과 차단 금지 목록을

사용하는 기본 DNS 정책을 제공합니다. 시스템이 제공하는 이러한 맞춤형 정책을 편집하고 사용할 수 있습니다. 다중 도메인 구축에서 이 기본 정책은 기본 전역 DNS 차단 목록, 전역 DNS 차단 금지 목록, 하위 항목 DNS 차단 목록, 하위 항목 DNS 차단 금지 목록을 사용하며, 전역 도메인에서만 편집할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**을(를) 선택합니다.

단계 **2** DNS 정책을 관리합니다.

- 비교 - DNS 정책을 비교하려면 **Compare Policies(**정책 비교**)**를 클릭하고 정책 비교, 514 페이지에 설명된 대로 진행합니다.
- 복사 - DNS 정책을 복사하려면 복사( )을 클릭하고 DNS 정책 편집, 1713 페이지에 설명된 대로 진행합니다.
- 생성 - 새 DNS 정책을 생성하려면 **Add DNS Policy(DNS** 정책 추가**)**를 클릭하고 기본 DNS 정책 생성, 1712 페이지에 설명된 대로 진행합니다.
- 삭제 - DNS 정책을 삭제하려면 삭제( )을 클릭한 다음 정책 삭제 여부를 확인합니다.
- 편집 - 기존 DNS 정책을 편집하려면 수정( )을 클릭하고 DNS 정책 편집, 1713 페이지에 설명된 대로 진행합니다.

기본 DNS 정책 생성

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**을(를) 선택합니다.

단계 **2** **Add DNS Policy(DNS** 정책 추가**)**를 클릭합니다.

단계 **3** 정책에 고유한 **Name(**이름**)** 또는 **Description(**설명**)**을 지정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

정책 구성 DNS 정책 편집, 1713 페이지의 내용을 참조하십시오.

DNS 정책 편집

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 DNS 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장하려고 하면 저장된 변경 사항의 첫 번째 집합만 유지됩니다.

세션 프라이버시를 보호하기 위해 정책 편집기에서 30분간 아무런 활동이 없으면 경고가 표시됩니다. 60분이 지나면 시스템은 변경 사항을 삭제합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**을(를) 선택합니다.

단계 **2** 편집하려는 DNS 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** DNS 정책을 수정합니다.

- Name(이름) 및 Description(설명) - 이름이나 설명을 변경하려면 해당 필드를 클릭하고 새 정보를 입력합니다.
- Rules(규칙) - DNS 규칙을 추가, 분류, 활성화, 비활성화 또는 기타 방식으로 관리하려면 **Rules(**규칙**)**를 클릭하고 DNS 규칙 생성 및 편집, 1714 페이지의 설명대로 작업을 진행합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 필요한 경우, 보안 인텔리전스로 연결 로깅, 2871 페이지의 설명에 따라 새 정책을 설정합니다.
- 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참고하십시오.

DNS 규칙

DNS 규칙은 호스트가 요청한 도메인 이름에 따라 트래픽을 처리합니다. 이 평가는 보안 인텔리전스의 일환으로 트래픽 암호 해독 이후/액세스 제어 평가 전에 수행됩니다.

시스템은 사용자가 지정하는 순서대로 트래픽이 DNS와 일치하는지 확인합니다. 대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 DNS 규칙에 따라 네트워크 트래픽을 처리합니다.

각 DNS 규칙에는 고유한 이름이 지정되며 다음과 같은 기본 구성 요소가 포함됩니다.

상태

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

DNS 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. DNS 규칙은 DNS 피드 또는 목록 조건을 포함해야 하며, 보안 영역, 네트워크 또는 VLAN을 기준으로 트래픽 일치 여부를 확인할 수도 있습니다.

조치

규칙의 작업에 따라 시스템에서 일치하는 트래픽을 처리하는 방법이 결정됩니다.

- 화이트리스트 동작이 있는 트래픽은 허용되며 추가 액세스 제어 검사가 수행됩니다.
- 모니터링된 트래픽의 경우 DNS 차단 목록에 대한 나머지 규칙에 따라 추가 평가가 수행됩니다. DNS 차단 목록 규칙과 일치하지 않는 트래픽의 경우 액세스 제어 규칙을 사용하여 검사합니다. 시스템은 트래픽에 대해 보안 인텔리전스 이벤트를 로깅합니다.
- 차단 목록의 트래픽은 추가 검사 없이 삭제됩니다. 또한 Domain Not Found(도메인을 찾을 수 없음) 응답을 반환하거나 DNS 쿼리를 싱크홀 서버로 리디렉션할 수도 있습니다.

관련 항목

보안 인텔리전스 정보, 1695 페이지

DNS 규칙 생성 및 편집

DNS 정책에서는 차단 목록 및 차단 금지 목록 규칙에 총 32767개의 DNS 목록을 추가할 수 있습니다. 즉, DNS 정책의 목록 수는 32767개를 초과할 수 없습니다.

프로시저

단계 **1** DNS 정책 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하려면 **Add DNS Rule(DNS** 규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 수정( )을 클릭합니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** 규칙 구성 요소를 구성하거나 기본값을 승인합니다.

- Action(작업) — 규칙 **Action(**작업**)**을 선택합니다(DNS 규칙 작업, 1716 페이지 참조).

- Conditions(조건) - 규칙의 조건을 구성합니다(DNS 규칙 조건, 1718 페이지 참조).
- Enabled(활성화) — 규칙이 **Enabled(활성화)** 상태인지 여부를 지정합니다.

단계 **4** **Save(저장)**를 클릭합니다.

다음에 수행할 작업

- 컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지를 참고하십시오.

DNS 규칙 관리

DNS 정책 편집기의 **Rules(규칙)** 탭에서는 정책 내의 DNS 규칙을 추가, 편집, 이동, 활성화, 비활성화, 삭제하고 기타 방식으로 관리할 수 있습니다.

정책 편집기는 각 규칙에 대해 그 이름, 조건의 요약, 규칙 작업을 표시합니다. 기타 아이콘은 경고( ), 오류( ), 기타 중요한 정보() 을 나타냅니다. 비활성화된 규칙은 흐리게 표시되며, 규칙 이름 아래에 `(disabled(비활성화))`가 표시됩니다.

DNS 규칙 활성화 및 비활성화

DNS 규칙은 생성하면 기본적으로 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다. DNS 정책에서 규칙의 목록을 볼 때 비활성화된 규칙은 흐리게 표시됩니다. 단, 이 규칙은 수정 가능합니다. DNS 규칙 편집기를 사용하여 DNS 규칙을 활성화하거나 비활성화할 수도 있습니다.

프로시저

단계 **1** DNS 정책 편집기에서 규칙을 마우스 오른쪽 버튼으로 클릭하고 규칙 상태를 선택합니다.

단계 **2** **Save(저장)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

DNS 규칙 순서 평가

DNS 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 DNS 규칙과 일치하는지 확인합니다. 대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 DNS 규칙에 따라 네트워크 트래픽을 처리합니다.

- 모니터링 규칙의 경우, 시스템은 트래픽을 로깅한 다음 우선 순위가 낮은 DNS 차단 목록 규칙을 기준으로 트래픽을 계속 평가합니다.
- 모니터링 규칙이 아닌 규칙의 경우, 시스템은 트래픽이 규칙과 일치하는 것으로 확인되고 나면 우선 순위가 낮은 추가 DNS 규칙을 기준으로 트래픽을 계속 평가하지 않습니다.

규칙 순서와 관련하여 다음 사항에 유의하십시오.

- DNS의 글로벌 화이트리스트이 항상 첫 번째 규칙이며 기타 모든 규칙보다 우선적으로 적용됩니다.
- 하위 항목 DNS 화이트리스트 규칙은 리프가 아닌 도메인의 다중 도메인 구축에서만 표시됩니다. 이 규칙은 항상 두 번째이며, 글로벌 화이트리스트을 제외한 다른 모든 규칙보다 우선적으로 적용됩니다.
- 차단 안 함 목록 섹션이 차단 목록 섹션보다 위에 있으며 차단 안 함 목록 규칙이 항상 다른 규칙보다 우선적으로 적용됩니다.
- DNS에 대한 전역 차단 목록은 항상 차단 목록 섹션의 첫 번째 항목이며 다른 모든 모니터링 및 차단 목록 규칙보다 우선합니다.
- 하위 항목 DNS 차단 목록 규칙은 리프가 아닌 도메인의 다중 도메인 구축에서만 표시됩니다. 이는 항상 차단 목록 섹션의 두 번째 항목이며 전역 차단 목록을 제외한 다른 모든 모니터링 및 차단 목록 규칙보다 우선합니다.
- 차단 목록 섹션에는 모니터링 및 차단 목록 규칙이 포함됩니다.
- DNS 규칙을 처음 생성할 때 차단 안 함 작업을 할당하면 해당 규칙이 차단 안 함 섹션의 마지막에 배치되고, 다른 작업을 할당하면 차단 목록 섹션의 마지막에 배치됩니다.

규칙을 끌어 놓으면 규칙 순서를 변경할 수 있습니다.

DNS 규칙 작업

각 DNS 제어 규칙에는 일치하는 트래픽에 대해 다음을 결정하는 작업이 있습니다.

- 처리-차단 또는 차단 금지 목록을 기반으로 시스템이 규칙의 조건과 일치하는 트래픽을 차단, 차단 금지, 차단, 또는 모니터링할지를 제어하는 가장 중요한 규칙 작업
- 로깅-일치하는 트래픽에 관한 세부 사항을 로깅하는 시기와 방법을 결정하는 규칙 작업

화이트리스트 작업

화이트리스트 작업은 트래픽이 검사의 다음 단계(액세스 제어 규칙)로 전달되도록 허용합니다.

시스템은 화이트리스트 일치 항목을 로깅하지 않습니다. 이러한 연결의 로깅 여부는 해당 연결의 최종 속성에 따라 달라집니다.

모니터링 작업

Monitor(모니터링**)** 작업은 연결 로깅을 강제하도록 설계됩니다. 따라서 일치하는 트래픽이 즉시 허용되거나 차단되지 않습니다. 대신, 트래픽이 허용할지 아니면 거부할지 여부를 결정하기 위해 추가 규칙에 일치됩니다. 첫 번째로 일치한 비모니터링 DNS 규칙이 시스템이 트래픽을 차단할지를 결정합니다. 추가로 일치하는 규칙이 없으면 트래픽에 대해 액세스 제어 평가가 수행됩니다.

DNS 정책에 의해 모니터링되는 연결의 경우, 시스템은 연결 종료 보안 인텔리전스 및 연결 이벤트를 Firepower Management Center 데이터베이스에 로깅합니다.

차단 작업

이들 작업은 어떤 종류의 추가 검사도 수행하지 않고 트래픽을 차단합니다.

- **Drop(**삭제**)** 작업에서는 패킷을 삭제합니다.
- **Domain Not Found(**도메인을 찾을 수 없음**)** 작업에서는 없는 인터넷 도메인 응답을 DNS 쿼리에 반환하므로 클라이언트가 DNS 요청을 확인할 수 없습니다.
- **Sinkhole(**싱크홀**)** 작업에서는 DNS 쿼리에 대한 응답으로 싱크홀 개체의 IPv4 또는 IPv6 주소를 반환합니다. 싱크 홀 서버는 IP 주소에 대한 후속 연결을 로깅하거나 로깅 후 차단할 수 있습니다. **Sinkhole(**싱크홀**)** 작업을 구성하는 경우에는 싱크홀 개체도 구성해야 합니다.

Drop(삭제**)** 또는 **Domain Not Found(**도메인을 찾을 수 없음**)** 작업에 따라 차단된 연결의 경우, 시스템은 연결 시작 보안 인텔리전스 및 연결 이벤트를 로깅합니다. 차단된 트래픽은 추가 검사 없이 즉시 거부 당하기 때문에, 연결을 로깅하는 데 고유한 마무리 단계는 없습니다.

Sinkhole(싱크홀**)** 작업에 따라 차단된 연결의 경우에는 싱크홀 개체 구성에 따라 로깅 여부가 달라집니다. 싱크홀 연결만 로깅하도록 싱크홀 개체를 구성하면 시스템은 후속 연결에 대해 연결 종료 연결 이벤트를 로깅합니다. 싱크홀 연결을 로깅 후에 차단하도록 싱크홀 개체를 구성하면 시스템은 후속 연결에 대해 연결 시작 연결 이벤트를 로깅한 다음 해당 연결을 차단합니다.

참고 ASA FirePOWER 디바이스에서 싱크홀 작업을 통해 DNS 규칙을 구성하고 트래픽이 규칙과 일치하는 경우, ASA는 기본적으로 후속 싱크홀 연결을 차단합니다. 이 문제를 해결하려면 ASA 명령줄에서 다음 명령을 실행합니다.

```
asa(config)# policy-map global_policy
asa(config-pmap)# class inspection_default
asa(config-pmap-c)# no inspect dns preset_dns_map
```

ASA가 연결을 계속 차단하는 경우, 지원에 문의하십시오.

관련 항목

규칙 및 정책 작업이 로깅에 미치는 영향, 2861 페이지

DNS 규칙 조건

SSL 규칙의 조건은 규칙에서 처리하는 트래픽의 유형을 식별합니다. 조건은 단순할 수도 있고 복잡할 수도 있습니다. DNS 규칙 내에서 DNS 피드 또는 목록 조건을 정의해야 합니다. 필요한 경우, 보안 영역, 네트워크 또는 VLAN별로 트래픽을 제어할 수도 있습니다.

DNS 규칙에 조건을 추가할 때 적용되는 사항은 다음과 같습니다.

- 규칙에 대해 특정 조건을 구성하지 않으면 시스템은 해당 기준에 따라 트래픽을 매칭하지 않습니다.
- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용할 수 있으려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어 DNS 피드 또는 목록 조건과 네트워크 조건은 있지만 VLAN 태그 조건은 없는 규칙은 세션의 VLAN 태깅에 관계없이 도메인 이름과 소스 또는 대상을 기준으로 트래픽을 평가합니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어 규칙 하나를 사용하여 최대 50개의 DNS 목록과 피드를 기준으로 트래픽을 차단할 수 있습니다.

DNS 및 보안 영역을 기준으로 트래픽 제어

DNS 규칙의 영역 조건을 사용하면 해당 소스 보안 영역에 따라 트래픽을 제어할 수 있습니다. 보안 영역이란 하나 이상의 인터페이스를 그룹화한 것이며, 이 인터페이스는 여러 디바이스에 걸쳐 위치할 수도 있습니다.

프로시저

단계 **1** DNS 규칙 편집기에서 **Zones(**영역**)**을 클릭합니다.

단계 **2** **Available Zones(**사용 가능한 영역**)**에서 추가하려는 영역을 찾아 선택합니다. 영역을 찾아 추가하려면, **Available Zones(**사용 가능한 영역**)** 목록 위에 있는 **Search by name(**이름으로 검색**)** 프롬프트를 클릭한 후, 영역 이름을 입력합니다. 일치하는 영역을 입력하여 표시하면 목록이 업데이트됩니다.

단계 **3** 영역을 하나 클릭하여 선택하거나 마우스 오른쪽 버튼을 클릭하고 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Source(**소스에 추가**)**를 클릭하거나 마우스로 끌어서 놓습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

DNS 및 네트워크를 기준으로 트래픽 제어

DNS 규칙의 네트워크 조건을 통해 소스 IP 주소로 트래픽을 제어할 수 있습니다. 제어하려는 트래픽에 대해 소스 IP 주소를 명시적으로 지정할 수 있습니다.

프로시저

단계 **1** DNS 규칙 편집기에서 **Networks(**네트워크**)**를 클릭합니다.

단계 **2** 다음과 같이, **Available Networks(**사용 가능한 네트워크**)**로부터 추가하려는 네트워크를 찾아 선택합니다.

- 네트워크 개체를 즉시 추가하려면(나중에 이 개체를 조건에 추가할 수 있음) **Available Networks(**사용 가능한 네트워크**)** 목록 위에 있는 추가( )을 클릭하고 네트워크 개체 생성, 571 페이지의 설명대로 작업을 진행합니다.
- 추가할 네트워크 개체를 검색하려면 **Available Networks(**사용 가능한 네트워크**)** 목록 위에 있는 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 후 개체 이름이나 개체 구성 요소 중 하나의 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.

단계 **3** **Add to Source(**소스에 추가**)**를 클릭하거나 마우스로 끌어서 놓습니다.

단계 **4** 수동으로 지정하려는 소스 IP 주소 또는 주소 블록을 추가합니다. **Source Networks(**소스 네트워크**)** 목록 아래에 있는 **Enter an IP address(IP** 주소 입력**)** 프롬프트를 클릭한 후 IP 주소 또는 주소 블록을 입력하고 **Add(**추가**)**를 클릭합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

DNS 및 VLAN을 기준으로 트래픽 제어

DNS 규칙의 VLAN 조건을 사용하면 VLAN 태그가 지정된 트래픽을 제어할 수 있습니다. 시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다.

VLAN 기반 DNS 규칙 조건을 작성할 때 VLAN 태그를 수동으로 지정할 수 있습니다. 또는 VLAN 태그 객체를 사용하여 VLAN 조건을 구성할 수 있습니다. 이 객체는 재사용 가능하며 이름을 하나 이상의 VLAN 태그와 연결합니다.

프로시저

단계 **1** DNS 규칙 편집기에서 **VLAN Tags(VLAN** 태그**)**를 선택합니다.

단계 **2** **Available VLAN Tags(**사용 가능한 **VLAN** 태그**)**에서 추가할 VLAN을 다음과 같이 찾아 선택합니다.

- VLAN 태그 개체를 즉시 추가한 다음 조건에 추가하려면 Available VLAN Tags(사용 가능한 VLAN 태그) 목록 위의 추가(+)을 클릭하고 VLAN 태그 개체 생성, 574 페이지에 설명된 대로 진행합니다.
- 추가할 VLAN 태그 개체 및 그룹을 검색하려면 **Available VLAN Tags(**사용 가능한 **VLAN** 태그**)** 목록 위에서 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 후 개체 이름 또는 개체의 VLAN 태그 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.

단계 **3** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

단계 **4** 수동으로 지정할 VLAN 태그를 추가합니다. **Selected VLAN Tags** 목록 아래의 **Enter a VLAN Tag** 프롬프트를 클릭합니다. 그런 다음 VLAN 태그 또는 범위를 입력하고 **Add**를 클릭합니다. 1~4094 범위의 VLAN 태그를 지정할 수 있으며, 하이픈을 사용하여 VLAN 태그의 범위를 지정합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

DNS 목록, 피드 또는 카테고리를 기준으로 트래픽 제어

DNS 규칙의 DNS 조건을 사용하면 DNS 목록, 피드 또는 카테고리에 클라이언트가 요청한 도메인 이름이 포함되어 있는 경우 트래픽을 제어할 수 있습니다. DNS 규칙에서 DNS 조건을 정의해야 합니다.

DNS 조건에 추가하는 항목(글로벌 또는 맞춤형 차단 또는 차단 안 함 목록)에 관계없이 시스템은 구성된 규칙 작업을 트래픽에 적용합니다. 예를 들어 규칙에 글로벌 차단 안 함 목록을 추가하고 **Drop(**삭제**)** 작업을 구성하면 시스템은 다음 검사 단계로 전달하도록 허용되어야 하는 모든 트래픽을 차단합니다.

프로시저

단계 **1** DNS 규칙 편집기에서 **DNS**를 클릭합니다.

단계 **2** 다음과 같이 **DNS Lists and Feeds(DNS** 목록 및 피드**)**에서 추가할 DNS 목록과 피드를 찾아서 선택합니다.

- DNS 목록이나 피드를 즉시 추가한 다음 조건에 추가하려면 **DNS Lists and Feeds(DNS** 목록 및 피드**)** 목록 위에 있는 추가( )을 클릭하고 보안 인텔리전스 피드 생성, 606 페이지의 설명대로 작업을 진행합니다.
- 추가할 DNS 목록, 피드 또는 카테고리를 검색하려면 **DNS Lists and Feeds(DNS** 목록 및 피드**)** 목록 위에 있는 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 후 개체 이름이나 개체 구성 요소 중 하나의 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.
- 새 범주에 대한 설명은 보안 인텔리전스 카테고리, 1702 페이지의 내용을 참조하십시오.

단계 **3** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

단계 **4** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

DNS 정책 구축

DNS 정책 구성 업데이트를 완료한 후 해당 업데이트를 액세스 제어 구성의 일부로 구축해야 합니다.

- 보안 인텔리전스 설정, 1698 페이지의 설명대로 DNS 정책을 액세스 제어 정책과 연결해야 합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

66 장

사전 필터링 및 사전 필터 정책

- 사전 필터링 정보, 1723 페이지
- 사전 필터링 모범 사례, 1727 페이지
- 사전 필터 정책 요구 사항 및 사전 요건, 1727 페이지
- 사전 필터링 설정, 1728 페이지
- 터널 영역 및 사전 필터링, 1733 페이지
- 사전 필터 규칙을 액세스 제어 정책으로 이동, 1737 페이지
- 사전 필터 정책 적중 횟수, 1739 페이지
- 대규모 플로우 오프로드, 1739 페이지
- 사전 필터링 기록, 1742 페이지

사전 필터링 정보

사전 필터링은 시스템에서 더 많은 리소스를 사용하는 평가를 수행하기 전에 이루어지는 첫 번째 액세스 제어 단계입니다. 사전 필터링은 간단하고 빠르며 일찍 이루어집니다. 사전 필터링은 제한된 외부 헤더 기준을 사용하여 신속하게 트래픽을 처리합니다. 내부 헤더를 사용하며 검사 기능이 더 강력한 후속 평가와 사전 필터링을 비교해 보십시오.

다음 경우에 사전 필터링을 구성하십시오.

- 성능 향상 - 검사가 필요하지 않은 트래픽은 일찍 제외할수록 좋습니다. 캡슐화된 연결을 검사하지 않고 외부 캡슐화 헤더를 기반으로 특정 유형의 일반 텍스트, 패스스루 터널을 단축 경로 지정 또는 차단할 수 있습니다. 조기에 처리하는 것이 유리한 그 밖의 연결도 단축 경로를 지정하거나 차단할 수 있습니다.
- 캡슐화된 트래픽에 심층 검사 맞춤 설정 - 동일한 검사 기준을 사용하여 나중에 캡슐화된 연결을 처리할 수 있도록 특정 터널 유형의 영역을 다시 지정할 수 있습니다. 영역 재지정이 필요한 이유는 사전 필터링 후 액세스 제어가 내부 헤더를 사용하기 때문입니다.

사전 필터링 및 액세스 제어 비교

사전 필터 정책과 액세스 제어 정책은 모두 트래픽을 차단하고 신뢰하도록 해 주지만 사전 필터링 '신뢰' 기능은 더 많은 검사를 건너뛰기 때문에 '단축 경로 설정(fastpathing)'이라고 합니다. 다음 표에서

는 맞춤형 사전 필터링을 구성해야 하는지 결정하는 데 도움이 되도록 사전 필터링과 액세스 제어의 이러한 차이점 및 그 밖의 차이점을 설명합니다.

맞춤형 사전 필터링을 구성하지 않는 경우, 액세스 제어 정책에서 조기 배치된 Block(차단) 및 Trust(신뢰) 규칙으로 사전 필터 기능을 비슷하게 모방할 수 있을 뿐 복제할 수는 없습니다.

특성	사전 필터링	액세스 제어	자세한 내용은 다음을 참고하십시오.
기본 기능	특정 유형의 일반 텍스트 통과 터널을 신속히 단축 경로 지정 또는 차단(캡슐화 조건 참조)하거나 캡슐화된 트래픽에 맞게 후속 검사를 조정합니다. 조기에 처리하는 것이 유리한 그 밖의 연결도 단축 경로를 지정하거나 차단할 수 있습니다.	상황별 정보 및 심층 검사 결과를 포함하여 간단하거나 복잡한 기준을 사용하여 모든 네트워크 트래픽을 검사하고 제어합니다.	사전 필터링 정보, 1723 페이지
구현	사전 필터 정책. 사전 필터 정책은 액세스 제어 정책에 의해 호출됩니다.	액세스 제어 정책 액세스 제어 정책은 주요 구성입니다. 액세스 제어 정책은 하위 정책 호출 외에도 자체 규칙을 갖습니다.	사전 필터 정책 정보, 1729 페이지 액세스 제어에 다른 정책 연결, 1641 페이지
액세스 제어 내 순서	첫 번째. 시스템은 다른 모든 액세스 제어 구성 전에 트래픽과 사전 필터 기준의 일치를 확인합니다.	—	—
규칙 작업	더 적습니다. 추가 검사(단축 경로 지정 및 차단)를 중지하거나 나머지 액세스 제어(분석)로 추가 분석을 허용할 수 있습니다.	자세한 내용. 액세스 제어 규칙에는 모니터링, 심층 검사, 차단 후 재설정, 인터랙티브 차단을 포함하여 훨씬 다양한 작업이 있습니다.	터널 및 사전 필터 규칙 구성 요소, 1731 페이지 액세스 제어 규칙 작업, 1658 페이지

특성	사전 필터링	액세스 제어	자세한 내용은 다음을 참고하십시오.
우회 기능	단축 경로 지정 규칙 작업. 사전 필터 단계에서 트래픽 단축 경로를 지정하면 다음을 포함한 모든 추가 검사 및 처리를 우회합니다. • 보안 인텔리전스 • ID 정책이 적용하는 인증 요건 • SSL 암호 해독 • 액세스 제어 규칙 • 패킷 페이로드 심층 검사 • 검색 • 속도 제한	Trust(신뢰) 규칙 작업. 액세스 제어 규칙이 신뢰할 수 있는 트래픽은 심층 검사 및 검색에서만 제외됩니다.	액세스 제어 규칙 소개, 1645 페이지
규칙 기준	Limited(제한적). 사전 필터 정책의 규칙은 IP 주소, VLAN 태그, 포트, 프로토콜 등 간단한 네트워크 기준을 사용합니다. 터널의 경우, 터널 엔드포인트 조건은 터널 양쪽에 있는 네트워크 디바이스의 라우팅된 인터페이스의 IP 주소를 지정합니다.	강력합니다. 액세스 제어 규칙은 네트워크 기준뿐 아니라 사용자, 애플리케이션, 요청된 URL 및 패킷 페이로드에서 사용할 수 있는 기타 상황별 정보도 사용합니다. 네트워크 조건은 소스 및 대상 호스트의 IP 주소를 지정합니다.	터널 규칙과 사전 필터 규칙 비교, 1730 페이지 규칙 조건 유형, 525 페이지
사용되는 IP 헤더(터널 처리)	가장 바깥쪽입니다. 외부 헤더를 사용하면 전체 일반 텍스트, 통과 터널을 처리할 수 있습니다. 비캡슐화 트래픽의 경우, 사전 필터링은 '외부' 헤더(이 경우에는 유일한 헤더)를 계속 사용합니다.	가장 안쪽도 가능합니다. 암호화되지 않은 터널의 경우, 액세스 제어는 전체 터널이 아니라 캡슐화된 개별 연결에 적용됩니다.	통과 터널 및 액세스 제어, 1726 페이지

특성	사전 필터링	액세스 제어	자세한 내용은 다음을 참고하십시오.
추가 분석을 위해 캡슐화된 연결 영역 다시 지정	터널링된 트래픽 영역을 다시 지정합니다. 터널 영역을 사용하면 사전 필터링된 캡슐화된 트래픽에 맞게 후속 검사를 조정할 수 있습니다.	터널 영역을 사용합니다. 액세스 제어는 사전 필터링 중에 할당하는 터널 영역을 사용합니다.	터널 영역 및 사전 필터링, 1733 페이지
연결 로깅	단축 경로가 지정되고 차단된 트래픽만. 허용되는 연결은 다른 구성에 의해 계속 로깅될 수 있습니다.	모든 연결.	로깅할 수 있는 기타 연결, 2861 페이지
지원되는 장치	Firepower Threat Defense 수정할 수 있습니다.	All.	사전 필터링 모범 사례, 1727 페이지

통과 터널 및 액세스 제어

일반 텍스트(암호화되지 않은) 터널은 종종 불연속 네트워크 사이를 흐르는 다중 연결을 캡슐화할 수 있습니다. 이러한 터널은 IP 네트워크를 통한 맞춤형 프로토콜, IPv4 네트워크를 통한 IPv6 트래픽 등을 라우팅하는 데 특히 유용합니다.

외부 캡슐화 헤더는 터널 양쪽에 있는 네트워크 디바이스의 라우티드 인터페이스인 터널 엔드포인트의 소스 및 대상 IP 주소를 지정합니다. 내부 페이로드 헤더는 캡슐화된 연결의 실제 엔드포인트의 소스 및 대상 IP 주소를 지정합니다.

네트워크 보안 디바이스는 종종 일반 텍스트 터널을 통과 트래픽으로 처리합니다. 즉, 해당 디바이스는 터널 엔드포인트 중 하나가 아닙니다. 그 대신, 이러한 디바이스는 터널 엔드포인트 간에 구축되고 터널 엔드포인트 간의 트래픽 플로우를 모니터링합니다.

(Firepower Threat Defense 대신) Cisco ASA 소프트웨어를 실행하는 Cisco ASA 방화벽과 같은 일부 네트워크 보안 디바이스는 외부 IP 헤더를 사용하여 보안 정책을 시행합니다. 일반 텍스트 터널의 경우에도, 이러한 디바이스는 캡슐화된 개별 연결 및 해당 페이로드를 제어할 수 없거나 이를 파악할 수 없습니다.

이와 달리, Firepower System은 다음과 같이 액세스 제어를 활용합니다.

- 외부 헤더 평가 — 첫째, 사전 필터링이 외부 헤더를 사용하여 트래픽을 처리합니다. 이 단계에서 전체 일반 텍스트, 통과 터널을 차단하거나 단축 경로를 지정할 수 있습니다.
- 내부 헤더 평가 — 그 다음, 나머지 액세스 제어(및 QoS 같은 기타 기능) 기능은 가장 내부에 있는 탐지 가능한 수준의 헤더를 사용하여 가장 세부적인 수준의 검사 및 처리를 보장합니다.

  통과 터널이 암호화되지 않은 경우, 이 단계에서 시스템은 캡슐화된 개별 연결에서 작동합니다. 모든 캡슐화된 연결에서 작동하려면 (터널 영역 및 사전 필터링, 1733 페이지 참조) 터널의 영역을 다시 지정해야 합니다.

액세스 제어로는 암호화된 통과 터널을 파악할 수 없습니다. 예를 들어 액세스 제어 규칙은 통과 VPN 터널을 하나의 연결로 간주합니다. 시스템은 외부의 캡슐화 헤더에 있는 정보만 사용하여 전체 터널을 처리합니다.

사전 필터링 모범 사례

다음 사전 필터링 지침 및 제한 사항을 고려하십시오.

관리 네트워크 트래픽

FTD 디바이스를 통과하는 빠른 경로 관리 트래픽을 사용해야 합니다. 액세스 제어 정책을 사용하여 관리 트래픽에 대한 심층 검사를 수행하면 문제가 발생할 수 있습니다.

모델 요구 사항

사전 필터링은 Firepower Threat Defense 디바이스에서만 지원됩니다. 사전 필터 구성은 다른 디바이스에 영향을 주지 않습니다.

비 **FTD** 디바이스의 사전 필터 유사 기능

기본 디바이스(7000/8000 시리즈, ASA FirePOWER, NGIPSv):

- 두 기능의 차이점을 염두에 두고 조기 배치된 Trust(신뢰) 및 Block(차단) 액세스 제어 규칙을 사용하여 사전 필터 기능과 비슷한 기능을 구현합니다. 사전 필터링 및 액세스 제어 비교, 1723 페이지의 내용을 참조하십시오.
- 몇 가지 제한과 함께 액세스 제어 규칙을 사용하여 전체 GRE 캡슐화 터널의 일치를 확인합니다. 포트 및 ICMP 코드 조건, 532 페이지의 내용을 참조하십시오.
- (8000 시리즈에만 해당) 디바이스별 단축 경로 지정 규칙은 액세스 제어를 우회할 수 있지만 트래픽을 차단할 수는 없습니다. 빠른 경로 규칙(8000 Series) 설정, 347 페이지의 내용을 참조하십시오.

사전 필터 정책 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

- 관리자

- 액세스 관리자
- Network Admin(네트워크 관리자)

사전 필터링 설정

맞춤형 사전 필터링을 수행하려면 사전 필터 정책을 액세스 제어의 일부로 매니지드 디바이스에 구성하고 구축합니다.

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장한 변경사항이 유지됩니다. 편의상 시스템에는 현재 각 정책을 수정하고 있는 사용자(있는 경우)에 대한 정보가 표시됩니다. 세션의 개인 정보를 보호하기 위해 정책 편집기에서 30분 동안 아무런 작업을 하지 않으면 경고가 표시됩니다. 60분이 지나면 시스템에서 변경사항을 삭제합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Prefilter(**사전 필터**)**을(를) 선택합니다.

단계 **2** **New Policy(**새 정책**)**을 클릭하여 맞춤형 사전 필터 정책을 생성합니다.

새 사전 필터 정책에는 Analyze all tunnel traffic(모든 터널 트래픽 분석)에 대한 규칙 및 기본 작업이 없습니다. 이 정책은 로깅을 수행하거나 터널 영역을 다시 지정하지 않습니다. 기존 정책을 복사( )하거나 수정( )할 수도 있습니다.

단계 **3** 사전 필터 정책의 기본 작업 및 로깅 옵션을 구성합니다.

- 기본 작업 — 지원되는 일반 텍스트, 통과 터널에 대한 기본 작업을 **Analyze all tunnel traffic(**모든 터널 트래픽 분석**)**(액세스 제어 포함) 또는 **Block all tunnel traffic(**모든 터널 트래픽 차단**)** 중에서 선택합니다.
- 기본 작업 로깅 — 기본 작업 옆에 있는 로깅( )을 클릭합니다(정책 기본 작업으로 연결 로깅, 2873 페이지 참조). 차단된 터널에 대해서만 기본 작업 로깅을 구성할 수 있습니다.

단계 **4** 터널 및 사전 필터 규칙을 구성합니다.

맞춤형 사전 필터 정책에서 순서에 상관없이 두 가지 규칙을 모두 사용할 수 있습니다. 일치할 특정 유형의 트래픽, 그리고 수행하려는 작업이나 추가 분석에 따라 규칙을 생성합니다(터널 규칙과 사전 필터 규칙 비교, 1730 페이지 참조).

주의 터널 규칙을 사용하여 터널 영역을 할당할 경우 주의하십시오. 향후 평가 시, 영역이 다시 지정된 터널의 연결은 보안 영역 제약 조건과 일치하지 않을 수 있습니다. 자세한 내용은 터널 영역 및 사전 필터링, 1733 페이지를 참고하십시오.

규칙 구성 요소를 구성하는 방법에 대한 자세한 내용은 터널 및 사전 필터 규칙 구성 요소, 1731 페이지 및 규칙 관리: 일반 특성, 523 페이지를 참조하십시오.

단계 **5** 규칙 순서를 평가합니다. 규칙을 이동하려면 클릭하여 끌거나, 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

규칙을 올바르게 생성하고 순서를 지정하는 것은 복잡한 작업이지만, 효과적인 구축에 필수적입니다. 정책을 신중하게 계획하지 않을 경우, 규칙이 다른 규칙을 선점하거나 잘못된 컨피그레이션을 포함할 수 있습니다. 자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지를 참고하십시오.

단계 **6** 사전 필터 정책을 저장합니다.

단계 **7** 터널 영역 제약 조건을 지원하는 컨피그레이션의 경우, 영역이 다시 지정된 터널을 올바르게 처리합니다.

터널 영역을 소스 영역 제약 조건으로 사용하면서 영역 재지정 터널에서 연결을 매치합니다. 인터페이스 조건 구성의 내용을 참조하십시오.

단계 **8** 사전 필터 정책을 매니지드 디바이스에 구축된 액세스 제어 정책과 연결합니다.

액세스 제어에 다른 정책 연결, 1641 페이지의 내용을 참조하십시오.

단계 **9** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

다음에 수행할 작업

시간 기반 규칙을 구축할 경우, 정책이 할당된 디바이스의 표준 시간대를 지정합니다. 정책 애플리케이션에 대한 디바이스 표준 시간대 구성, 1464 페이지의 내용을 참조하십시오.

사전 필터 정책 정보

사전 필터링은 정책 기반 기능입니다. Firepower System에서 액세스 제어 정책은 사전 필터 정책을 비롯한 하위 정책 및 기타 구성을 호출하는 마스터 구성입니다.

정책 구성 요소: 규칙 및 기본 작업

사전 필터 정책에서는 터널 규칙, 사전 필터 규칙, 기본 작업이 네트워크 트래픽을 처리합니다.

- 터널 및 사전 필터 규칙 - 우선 사전 필터 정책의 규칙은 사용자가 지정하는 순서로 트래픽을 처리합니다. 터널 규칙은 특정 터널만 일치를 확인하고 영역 다시 지정을 지원합니다. 사전 필터 규칙은 제약 조건이 더 광범위하고 영역 다시 지정을 지원하지 않습니다. 자세한 내용은 터널 규칙과 사전 필터 규칙 비교, 1730 페이지를 참고하십시오.
- 기본 작업(터널만 해당) - 터널이 어느 규칙과도 일치하지 않으면 기본 작업이 이를 처리합니다. 기본 작업은 이러한 터널을 차단하거나 캡슐화된 개별 연결에서 액세스 제어를 계속할 수 있습니다. 기본 작업으로 터널의 영역을 다시 지정할 수 없습니다.

  캡슐화되지 않은 트래픽에 대한 기본 작업은 없습니다. 캡슐화되지 않은 연결이 어느 사전 필터 규칙과도 일치하지 않으면 시스템이 액세스 제어를 계속합니다.

연결 로깅

사전 필터 정책에 의해 단축 경로가 지정되고 차단된 연결을 로깅할 수 있습니다. 로깅할 수 있는 기타 연결, 2861 페이지 참조.

연결 이벤트에는 전체 터널을 포함하여 로깅된 연결이 사전 필터링되었는지 여부와 그 방법에 대한 정보가 포함되어 있습니다. 이벤트 보기(워크플로), 대시보드, 보고서에서 이 정보를 확인하고 상관관계 기준으로 사용할 수 있습니다. 단축 경로가 지정되고 차단된 연결은 심층 검사 대상이 아니므로 연결된 연결 이벤트에는 제한된 정보가 포함되어 있음에 유의하십시오.

기본 사전 필터 정책

모든 액세스 제어 정책에는 연결된 사전 필터 정책이 있습니다.

맞춤형 사전 필터링을 구성하지 않은 경우, 기본 정책이 사용됩니다. 시스템이 제공하는 이 정책은 처음에는 모든 트래픽을 액세스 제어의 다음 단계로 통과시킵니다. 정책의 기본 작업을 변경하고 로깅 옵션을 구성할 수 있지만 규칙을 추가하거나 삭제할 수는 없습니다.

사전 필터 정책 상속 및 멀티 테넌시

액세스 제어는 멀티 테넌시를 보완하는 계층적 구현을 사용합니다. 다른 고급 설정과 함께 사전 필터 정책 연결을 잠가 모든 하위 항목 액세스 제어 정책에서 해당 연결을 적용할 수 있습니다. 자세한 내용은 액세스 제어 정책 상속, 1615 페이지를 참고하십시오.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 기본 사전 필터 정책은 전역 도메인에 속합니다.

터널 규칙과 사전 필터 규칙 비교

터널 규칙 또는 사전 필터 규칙 중 어느 것을 구성할 것인지는 일치할 특정 유형의 트래픽, 그리고 수행하려는 작업이나 추가 분석에 따라 결정됩니다.

특성	터널 규칙	사전 필터 규칙
기본 기능	일반 텍스트, 통과 터널의 단축 경로 지정, 차단, 영역 다시 지정을 신속하게 수행합니다.	조기에 처리하는 것이 유리한 모든 기타 연결의 단축 경로 지정 또는 차단을 신속하게 수행합니다.
캡슐화 및 포트/프로토콜 기준	캡슐화 조건은 캡슐화 조건에 나와 있는 선택한 프로토콜을 통한 일반 텍스트 터널에만 일치됩니다.	포트 조건은 터널 규칙보다 더 광범위한 포트 및 프로토콜 제약 조건을 사용할 수 있습니다(포트 및 ICMP 코드 조건, 532 페이지 참조).
네트워크 기준	터널 엔드포인트 조건은 처리할 터널의 엔드포인트를 제한합니다(터널 엔드포인트 조건 참조).	네트워크 조건은 각 연결의 소스 및 대상 호스트를 제약합니다. 네트워크 조건, 530 페이지의 내용을 참조하십시오.

특성	터널 규칙	사전 필터 규칙
Direction(방향)	양방향 또는 단방향(구성 가능). 터널 규칙은 기본적으로 양방향이므로, 터널 엔드포인트 간의 모든 트래픽을 처리할 수 있습니다.	단방향 전용(구성 불가). 사전 필터 규칙은 소스-대상 트래픽만 매치합니다.
추가 분석을 위한 세션 영역 다시 지정	지원됨, 터널 영역 사용(터널 영역 및 사전 필터링, 1733 페이지 참조).	지원되지 않음

터널 및 사전 필터 규칙 구성 요소

상태(활성화/비활성화)

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하지 않으며, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽과 일치하는 첫 번째 규칙은 규칙 유형(터널 또는 사전 필터)에 관계없이 트래픽을 처리하는 규칙입니다.

작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하고 로깅하는 방법을 결정합니다.

- Fastpath(단축 경로) - 액세스 제어, ID 요건, 속도 제한 등의 모든 이후 검사와 제어에서 일치하는 트래픽을 제외합니다. 터널을 빠른 경로로 지정하면 캡슐화된 모든 연결이 빠른 경로로 지정됩니다.
- Block(차단) - 어떤 종류든 추가 검사 없이 일치하는 트래픽을 차단합니다. 터널을 차단하면 캡슐화된 모든 연결이 차단됩니다.
- Analyze(분석) - 내부 헤더를 사용하여 나머지 액세스 제어를 통해 트래픽을 계속 분석할 수 있습니다. 트래픽이 액세스 제어 및 관련 심층 검사에서 통과하는 경우 트래픽 속도도 제한할 수 있습니다. 터널 규칙의 경우, Assign Tunnel Zone(터널 영역 할당) 옵션으로 영역 다시 지정을 활성화합니다.

방향(터널 규칙에만 해당)

터널 규칙의 방향에 따라 시스템의 소스 및 대상 기준으로 다음 작업을 수행하는 방식이 결정됩니다.

- 소스로부터만 터널 매치(단방향) - 소스-대상 트래픽만 매치합니다. 매치하는 트래픽은 지정된 소스 인터페이스 또는 터널 엔드포인트 중 하나에서 시작되고 대상 인터페이스 또는 터널 엔드포인트 중 하나에서 끝나야 합니다.

- 소스 및 대상으로부터 터널 매치(양방향) - 소스-대상 트래픽과 대상-소스 트래픽 모두 매치합니다. 두 개의 단방향 규칙을 작성하는 데 미치는 영향은 동일하며, 한쪽이 다른 한쪽을 미러링합니다.

사전 필터 규칙은 항상 단방향입니다.

터널 영역 할당**(**터널 규칙에만 해당**)**

터널 규칙의 경우, 터널 영역(기존 또는 즉시 생성된 영역 모두 해당)을 할당하면 일치하는 터널의 영역이 다시 지정됩니다. 영역을 다시 지정하려면 Analyze(분석) 작업을 수행해야 합니다.

터널의 영역을 다시 지정하면 기타 컨피그레이션(예: 액세스 제어 규칙)은 모든 터널의 캡슐화된 연결을 서로에게 속한 것으로 인식할 수 있습니다. 터널의 할당된 터널 영역을 인터페이스 제약 조건으로 사용하여, 검사를 캡슐화된 연결에 맞춤 설정할 수 있습니다. 자세한 내용은 터널 영역 및 사전 필터링, 1733 페이지를 참고하십시오.

주의 터널 영역을 할당할 경우 주의하십시오. 향후 평가 시, 영역이 다시 지정된 터널의 연결은 보안 영역 제약 조건과 일치하지 않을 수 있습니다. 터널 영역 구현에 대한 간략한 단계별 안내, 그리고 영역이 다시 지정된 트래픽을 명시적으로 처리하지 않고 영역을 다시 지정했을 때 발생하는 영향에 대한 내용은 터널 영역 사용, 1734 페이지을 참조하십시오.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 트래픽은 규칙과 일치하는 모든 규칙의 조건과 일치해야 합니다. 각 조건 유형은 규칙 편집기에 고유한 탭이 있습니다.

다음 외부 헤더 제약 조건을 사용하여 트래픽을 사전 필터링할 수 있습니다.

- 인터페이스 —인터페이스 조건
- 네트워크 - 터널 엔드포인트 조건 또는 네트워크 조건, 530 페이지
- 포트 — 캡슐화 조건 또는 포트 및 ICMP 코드 조건, 532 페이지
- VLAN —VLAN 조건, 531 페이지

캡슐화 프로토콜별로 터널 규칙을 제한해야 합니다.

적용 가능한 시간

규칙이 적용되는 날짜와 시간을 지정할 수 있습니다.

로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다.

터널 및 사전 필터 규칙에서는 단축 경로가 지정되고 차단된 트래픽을 로깅할 수 있습니다(단축 경로 및 차단 작업). 추가 분석(분석 작업)할 트래픽의 경우, 다른 컨피그레이션에 의해 일치하는 연결이

계속 로깅될 수 있긴 하지만 사전 필터 정책에서 로깅이 비활성화됩니다. 자세한 내용은 터널 및 사전 필터 규칙으로 연결 로깅를 참고하십시오.

코멘트

규칙에 대한 변경 사항을 저장할 때마다 코멘트를 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다.

규칙을 저장한 후에는 이러한 코멘트를 수정하거나 삭제할 수 없습니다.

관련 항목

액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

터널 영역 및 사전 필터링

터널 영역은 사전 필터링을 사용하여 후속 트래픽 처리를 캡슐화된 연결에 맞춰 설정할 수 있도록 지원합니다.

일반적으로 시스템은 가장 내부에 있는 탐지 가능한 수준의 헤더를 사용하여 트래픽을 처리하므로 특수 메커니즘이 필요합니다. 이를 통해 가장 세부적인 수준의 검사를 보장할 수 있습니다. 그러나 이는 통과 터널이 암호화되지 않은 경우, 시스템은 캡슐화된 개별 연결에서 작동한다는 것을 의미하기도 합니다(통과 터널 및 액세스 제어, 1726 페이지 참조).

터널 영역으로 이 문제를 해결할 수 있습니다. 액세스 제어의 첫 번째 단계(사전 필터링) 동안 외부 헤더를 사용하여 특정 유형의 일반 텍스트, 통과 터널을 식별할 수 있습니다. 그런 다음, 맞춤형 터널 영역을 할당하여 이러한 터널의 영역을 다시 지정할 수 있습니다.

터널의 영역을 다시 지정하면 기타 컨피그레이션(예: 액세스 제어 규칙)은 모든 터널의 캡슐화된 연결을 서로에게 속한 것으로 인식할 수 있습니다. 터널의 할당된 터널 영역을 인터페이스 제약 조건으로 사용하여, 검사를 캡슐화된 연결에 맞춤 설정할 수 있습니다.

터널 영역은 이름과 달리, 보안 영역이 아닙니다. 터널 영역은 인터페이스 집합을 의미하지 않습니다. 터널 영역은 일종의 태그로 간주하는 편이 더 정확하며, 캡슐화된 연결과 관련된 보안 영역을 대체하는 경우가 있습니다.

주의 터널 영역 제약 조건을 지원하는 컨피그레이션의 경우, 영역이 다시 지정된 터널의 연결은 보안 영역 제약 조건과 일치하지 않습니다. 예를 들어 터널의 영역을 다시 지정하면, 액세스 제어 규칙은 캡슐화된 연결을 원래 보안 영역이 아닌 새로 할당된 터널 영역과 일치시킬 수 있습니다.

터널 영역 구현에 대한 간략한 단계별 안내, 그리고 영역이 다시 지정된 트래픽을 명시적으로 처리하지 않고 영역을 다시 지정했을 때 발생하는 영향에 대한 내용은 터널 영역 사용, 1734 페이지을 참조하십시오.

터널 영역 제약 조건을 지원하는 컨피그레이션

터널 영역 사용

이 예시 절차에는 터널 영역을 사용하여 추가 분석을 위해 GRE 터널의 영역을 다시 지정할 수 있는 방법이 요약되어 있습니다. 일반 텍스트, 통과 터널의 캡슐화된 연결에 대한 트래픽 검사를 맞춤 설정해야 하는 다른 시나리오를 대상으로 이 예시에 설명된 개념을 응용할 수 있습니다.

조직의 내부 트래픽 플로우가 신뢰할 수 있는 보안 영역을 통과하는 Firepower System 구축 사례를 고려해보십시오. 신뢰할 수 있는 보안 영역은 다양한 위치에 구축된 여러 매니지드 디바이스 전체의 센싱 인터페이스 집합을 나타냅니다. 조직의 보안 정책은 익스플로잇 및 악성코드에 대한 심층 검사 후 내부 트래픽을 허용해야 합니다.

내부 트래픽에 특정 엔드포인트 간의 일반 텍스트, 통과, GRE 터널이 포함될 때가 있습니다. 이러한 캡슐화된 트래픽의 트래픽 프로파일은 알려진 무해한 프로파일이라고 해도 "정상적인" 사내 활동과 다르기 때문에, 특정한 캡슐화된 트래픽에 대한 검사를 제한하는 동시에 보안 정책을 계속 준수할 수 있습니다.

이 예에서 컨피그레이션 변경 사항을 구축한 후의 결과는 다음과 같습니다.

- 신뢰할 수 있는 영역에서 탐지된 일반 텍스트, 통과, GRE 캡슐화 터널의 캡슐화된 개별 연결은 단일한 침입 및 파일 정책 집합으로 평가되었습니다.
- 신뢰할 수 있는 영역의 모든 기타 트래픽은 다른 침입 및 파일 정책으로 평가되었습니다.

GRE 터널의 영역을 다시 지정하여 이 작업을 수행합니다. 영역을 다시 지정하면 액세스 제어에서는 GRE 캡슐화 연결을 원래의 신뢰할 수 있는 보안 영역이 아닌 맞춤형 터널 영역과 연결합니다. 영역을 다시 지정해야 하는 이유는 Firepower System 및 액세스 제어에서 캡슐화된 트래픽을 처리하는 방식 때문입니다(통과 터널 및 액세스 제어, 1726 페이지 및 터널 영역 및 사전 필터링, 1733 페이지 참조).

프로시저

단계 **1** 캡슐화된 트래픽에 심층 검사를 맞춤 설정하는 맞춤형 침입 및 파일 정책을 구성하고, 비 캡슐화된 트래픽에 맞춤 설정된 다른 침입 및 파일 정책을 구성합니다.

단계 **2** 맞춤형 사전 필터링을 구성하여 신뢰할 수 있는 보안 영역을 통과하는 GRE 터널의 영역을 다시 지정합니다.

맞춤형 사전 필터 정책을 생성하고 이를 액세스 제어와 연결합니다. 맞춤형 사전 필터 정책에서 터널 규칙(이 예에서는**`GRE_tunnel_rezone`**) 및 해당 터널 영역(**`GRE_tunnel`**)을 생성합니다. 자세한 내용은 사전 필터링 설정, 1728 페이지를 참고하십시오.

표 ***102: GRE_tunnel_rezone*** 터널 규칙

규칙 구성 요소	설명
터널 엔드포인트 조건	조직에서 사용된 GRE 터널에 대한 소스 및 대상 엔드포인트를 지정합니다. 터널 규칙은 기본적으로 양방향입니다. **Match tunnels from...(**다음의 터널 매치**)** 옵션을 변경하지 않으면 어떤 엔드포인트를 소스 및 대상으로 지정하는지는 중요하지 않습니다.
캡슐화 조건	GRE 트래픽과 일치합니다.
터널 영역 지정	**`GRE_tunnel`** 터널 영역을 생성하고, 이를 규칙과 일치하는 터널에 할당합니다.
작업	분석(나머지 액세스 제어와 함께 사용).

단계 **3** 영역이 다시 지정된 터널의 연결을 처리하기 위한 액세스 제어를 구성합니다.

매니지드 디바이스에 구축된 액세스 제어 정책에서, 영역을 다시 지정한 트래픽을 처리하는 규칙(이 예에서는 **`GRE_inspection`**)을 구성합니다. 자세한 내용은 액세스 제어 규칙 생성 및 수정, 1651 페이지를 참고하십시오.

표 ***103: GRE_inspection*** 액세스 제어 규칙

규칙 구성 요소	설명
보안 영역 조건	GRE_tunnel 보안 영역을 소스 영역 제약의 내용을 참조하십시오.
작업	허용(심층 검사 활성화됨). 캡슐화된 내부 트래픽을 검사하도록 맞춤 설정된 파일 및 침입 정책을 선택합니다.

주의 이 단계를 건너뛸 경우, 영역이 다시 지정된 연결은 보안 영역에 의해 제한되지 않는 모든 액세스 제어 규칙과 일치할 수 있습니다. 영역이 다시 지정된 연결이 액세스 제어 규칙과 일치하지 않을 경우, 이는 액세스 제어 정책 기본 작업으로 처리됩니다. 이 작업이 원하는 설정인지 확인하십시오.

단계 **4** 신뢰할 수 있는 보안 영역을 통과하는 비 캡슐화된 연결을 처리하기 위한 액세스 제어를 구성합니다.

동일한 액세스 제어 정책에서, 신뢰할 수 있는 보안 영역의 영역이 다시 지정되지 않은 트래픽을 처리하는 규칙(이 예에서는 **`internal_default_inspection`**)을 구성합니다.

표 *104: internal_default_inspection* 액세스 제어 규칙

규칙 구성 요소	설명
보안 영역 조건	신뢰 보안 영역을 보안 영역 및 대상 영역 제약 조건 모두로 사용하면서 영역 재지정되지 않은 내부 전용 트래픽을 매치합니다.
작업	허용(심층 검사 활성화됨). 비캡슐화된 내부 트래픽을 검사하도록 맞춤 설정된 파일 및 침입 정책을 선택합니다.

단계 **5** 기존 규칙과 관련하여 새 액세스 제어 규칙의 위치를 평가합니다. 필요한 경우 규칙 순서를 변경합니다.

새로운 액세스 제어 규칙 두 개를 나란히 함께 배치할 경우, 어떤 규칙을 먼저 배치해도 무관합니다. GRE 터널의 영역을 다시 지정했으므로, 두 가지 규칙이 서로를 선점할 수 없습니다.

단계 **6** 모든 변경된 컨피그레이션을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

Creating Tunnel Zones

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Tunnel Zone(**터널 영역**)**을 선택합니다.

단계 **3** **Add Tunnel Zone(**터널 영역 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력하고 필요한 경우, **Description(**설명**)**을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 사전 필터링의 일부로 일반 텍스트, 통과 터널에 터널 영역을 할당합니다. 사전 필터링 설정, 1728 페이지 참조.

사전 필터 규칙을 액세스 제어 정책으로 이동

액세스 제어 규칙을 액세스 제어 정책에서 연결된 사전 필터 정책으로 이동할 수 있습니다.

시작하기 전에

계속하기 전에 다음 사항에 유의하십시오.

- 사전 필터 규칙만 액세스 제어 정책으로 이동할 수 있습니다. 터널 규칙은 이동할 수 없습니다.
- 사전 필터 규칙은 연결된 액세스 제어 정책으로만 이동할 수 있습니다.
- 구성된 인터페이스 그룹이 있는 사전 필터 규칙은 이동할 수 없습니다.
- 이동하면 사전 필터 규칙의 **Action(**작업**)** 매개 변수가 액세스 제어 규칙의 적절한 작업으로 변경됩니다. 사전 필터 규칙의 각 작업이 무엇에 매핑되는지 확인하려면 다음 표를 참조하십시오.

사전 필터 규칙의 작업	액세스 제어 규칙 작업
분석	허용
차단	Block(차단)
Fastpath(단축 경로)	신임

- 마찬가지로 사전 필터 규칙에 구성된 작업을 기반으로 다음 표에 나와 있는 것처럼 규칙을 이동한 후 로깅 구성이 적절한 설정으로 설정됩니다.

사전 필터 규칙의 작업	액세스 제어 규칙에서 활성화된 로깅 구성
분석	활성화된 로그 설정이 없습니다.
Block(차단)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩

사전 필터 규칙의 작업	액세스 제어 규칙에서 활성화된 로깅 구성
Fastpath(단축 경로)	• Log at Beginning of Connection(연결 시작 시 로깅) • Log at End of Connection(연결 종료 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩

- 규칙을 이동하면 사전 필터 규칙 구성의 코멘트가 손실됩니다. 그러나 소스 사전 필터 정책을 언급하는 새로운 주석이 이동된 규칙에 추가됩니다.
- 소스 정책에서 규칙을 이동하는 동안 다른 사용자가 해당 규칙을 수정하면 FMC에 메시지가 표시됩니다. 페이지를 새로 고친 후 프로세스를 계속 진행할 수 있습니다.

프로시저

단계 **1** 사전 필터 정책 편집기에서 마우스 왼쪽 버튼을 클릭하여 이동할 규칙을 선택합니다.

팁 여러 규칙을 선택하려면 키보드에서 Ctrl(컨트롤) 키를 사용합니다.

단계 **2** 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Move to another policy(**다른 정책으로 이동**)**를 선택합니다.

단계 **3** **Access Policy(**액세스 정책**)** 드롭 다운 목록에서 대상 액세스 제어 정책을 선택합니다.

단계 **4** **Place Rules(**규칙 배치**)** 드롭 다운 목록에서 이동한 규칙을 배치할 위치를 선택합니다.

- **Default(**기본값**)** 섹션에서 마지막 규칙 집합으로 배치하려면 **At the bottom(**맨 아래 **)(Default(**기본**)** 섹션 내**)**를 선택합니다.
- **Mandatory(**의무**)** 섹션에서 첫번째 규칙 집합으로 배치하려면 **At the top(**맨 위 **)(Mandatory(**의무**)** 섹션 내**)**를 선택합니다.

단계 **5** **Move(**이동**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

사전 필터 정책 적중 횟수

적중 횟수는 정책 규칙이 일치하는 연결을 트리거한 횟수를 나타냅니다.

사전 필터 정책 적중 횟수 보기에 대한 자세한 내용은 정책 적중 횟수 보기, 1642 페이지를 참조하십시오.

대규모 플로우 오프로드

FXOS를 실행하는 디바이스(예: Firepower 4100/9300 섀시)에서 사전 필터 정책에 의해 단축 경로가 되도록 구성하는 특정 트래픽은 Firepower Threat Defense 소프트웨어가 아닌 하드웨어(특히 NIC)에서 처리됩니다. 이러한 연결 플로우를 오프로드하면 처리량이 증가하고, 특히 다량 파일 전송과 같은 데이터 집약적인 애플리케이션의 경우 레이턴시가 낮아집니다. 이 기능은 특히 데이터 센터에 유용합니다. 이것을 정적 플로우 오프로드라고 합니다.

또한 기본적으로 Firepower Threat Defense 디바이스 오프로드는 신뢰를 비롯한 다른 기준에 따라 플로우를 오프로드합니다. 이것을 동적 플로우 오프로드라고 합니다.

오프로드 플로우는 기본 TCP 플래그 및 옵션 확인 등 제한된 상태를 추적할 수 있는 검사를 계속 진행합니다. 시스템은 필요한 경우 추가 처리를 위해 선택적으로 패킷을 방화벽 시스템에 에스컬레이트할 수 있습니다.

대규모 플로우 오프로드의 이점을 누릴 수 있는 애플리케이션의 예는 다음과 같습니다.

- HPC(고성능 컴퓨팅) 연구 사이트는 스토리지와 고성능 컴퓨팅 스테이션 간 Firepower Threat Defense 디바이스가 구축되는 곳입니다. 하나의 연구 사이트가 FTP 파일 전송 또는 NFS를 통한 파일 동기화를 통해 백업되면 대규모 데이터 트래픽이 모든 연결에 영향을 끼칩니다. FTP 파일 전송 및 NFS를 통한 파일 전송을 오프로드하면 다른 트래픽에 끼치는 영향을 줄일 수 있습니다.
- HTF(고주파수 거래)는 주로 규정 준수를 위해 워크스테이션과 익스체인지 간 Firepower Threat Defense 디바이스가 구축되는 곳입니다. 보안은 주요 관심사가 아니지만 지연은 주요 관심사입니다.

다음 유형의 플로우는 오프로드할 수 없습니다.

- (정적 플로우 오프로드에만 해당합니다.) 사전 필터 정책에 따라 단축 경로가 지정됩니다.
- 표준 또는 802.1Q 태그 지정된 이더넷 프레임에만 해당합니다.
- (동적 플로우 오프로드에만 해당합니다.)
  - 검사 완료된 플로우는 검사 엔진이 검사가 필요하지 않다고 결정한 것입니다. 이러한 플로우는 다음과 같습니다.
    - 신뢰 작업을 적용하며 보안 영역, 소스 및 대상 네트워크 및 포트 일치만 기반으로 하는 액세스 제어 규칙에 의해 처리되는 플로우입니다.
    - SSL 정책을 사용하여 암호 해독을 위해 선택되지 않은 TLS/SSL 플로우.

- 명시적이거나 플로우 우회 한도 초과로 IAB(Intelligent Application Bypass) 정책에 의해 신뢰할 수 있는 플로우입니다.
- 플로우를 신뢰하게 하는 파일 또는 침입 정책과 일치하는 플로우입니다.
- 더 이상 검사할 필요가 없는 허용되는 모든 플로우

- 다음 IPS 전처리기 흐름을 검사합니다.
  - SSH 및 SMTP
  - FTP 전처리기 보조 연결을 검사합니다.
  - SIP(세션 시작 프로토콜) 전처리기 보조 연결을 검사합니다.
- (옵션이라고도 하는) 키워드를 사용하는 침입 규칙

중요 위의 세부 사항, 예외 및 제한 사항은 플로우 오프로드 제한, 1741 페이지의 내용을 참조하십시오.

정적 플로우 오프로드 사용

적합한 트래픽을 하드웨어에 오프로드하려면 **Fastpath** 작업에 적용되는 사전 필터 정책 규칙을 생성합니다. TCP/UPD에 사전 필터 규칙을, GRE에 터널 규칙을 사용합니다.

(Not recommended.) 정적 플로우 오프로드를 비활성화하고 부산물로서 제품의 동적 플로우 오프로드를 비활성화하려면 FlexConfig를 사용하여 **no flow-offload enable** 명령을 실행합니다. 구축 후 변경 사항을 구현하려면 디바이스를 다시로드해야 합니다. 이 명령에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html에서 제공되는 *Cisco ASA Series Command Reference*를 참조하십시오.

동적 플로우 오프로드 사용

동적 플로우 오프로드는 기본적으로 활성화되어 있습니다.

동적 오프로드를 비활성화하려면

```
> configure flow-offload dynamic whitelist disable
```

동적 오프로드를 다시 활성화하려면

```
> configure flow-offload dynamic whitelist enable
```

동적 오프로드는 사전 필터링의 구성 여부에 관계 없이 정적 플로우 오프로드가 활성화된 경우에만 발생합니다.

플로우 오프로드 제한

모든 플로우의 오프로드가 가능한 것은 아닙니다. 오프로드 후에도 특정 조건을 만족하는 경우 플로우가 오프로드에서 제거될 수 있습니다. 다음은 몇 가지 제한 사항입니다.

오프로드가 불가능한 플로우

다음 유형의 플로우는 오프로드할 수 없습니다.

- IPv4 주소 지정을 사용하지 않는 모든 플로우(예: IPv6 주소 지정).
- TCP, UDP, GRE 외의 프로토콜을 사용하는 플로우

참고 PPTP GRE 연결은 오프로드할 수 없습니다.

- 패시브, 인라인, 인라인 탭 모드에서 구성된 인터페이스의 플로우 라우팅 및 스위치 인터페이스 유형만 지원됩니다.
- Snort 또는 다른 검사 엔진에서 검사해야 하는 플로우 FTP와 같은 일부 경우에는 제어 채널은 오프로드되지 않지만 보조 데이터 채널은 오프로드될 수 있습니다.
- 디바이스에서 종료되는 IPsec 및 TLS/DTLS VPN 연결.
- TTL(Time-to-Live) 값을 감소시키도록 정책을 구성한 플로우.
- 암호화 또는 암호 해독이 필요한 플로우 예를 들어, SSL 정책으로 인해 연결이 암호 해독되었습니다.
- 라우팅 모드의 멀티캐스트 플로우 이는 브리지 그룹에 멤버 인터페이스가 2개 뿐인 경우 투명 모드에서 지원됩니다.
- TCP 인터셉트 플로우
- 패킷 캡처 필터와 추적 옵션을 일치시키는 플로우.
- 보안 그룹 태그가 지정된 플로우
- 하나의 클러스터에 대해 비대칭플로우일 때 다른 클러스터 노드에서 포워딩된 역방향 플로우
- 플로우 소유자가 제어 유닛이 아닌 경우 클러스터에 중앙 집중된 플로우
- 동적 오프로드가 불가능한 IP 옵션을 포함한 플로우

추가 제한 사항

- 플로우 오프로드 및 DCD(Dead Connection Detection)가 호환되지 않습니다. 오프로드할 수 있는 연결에서 DCD를 구성하지 마십시오.
- 플로우 오프로드 조건과 일치하는 둘 이상의 플로우가 하드웨어의 동일한 위치에 동시에 오프로드되도록 대기열에 있는 경우 첫 번째 플로우만 오프로드됩니다. 다른 플로우는 정

상적으로 처리됩니다. 이를 충돌이라고합니다. 이 상황에 대한 통계를 표시하려면 CLI에서 **show flow-offload flow** 명령을 사용합니다.

- 동적 플로우 오프로드는 모든 TCP 노멀라이저 검사를 비활성화합니다.

역방향 오프로드 조건

플로우 오프로드 이후 플로우 내 패킷이 다음 조건을 만족할 경우 추가 처리를 위해 Firepower Threat Defense 디바이스로 반환됩니다.

- 타임스탬프 이외의 TCP 옵션이 포함됩니다.
- 프래그먼트화됩니다.
- 이들은 ECMP(Equal-cost Multi-path) 라우팅의 대상이며 인그래스 패킷은 하나의 인터페이스에서 다른 인터페이스로 이동합니다.

사전 필터링 기록

기능	버전	세부 사항
사전 필터 규칙을 액세스 제어 정책으로 이동	6.7	액세스 제어 규칙을 액세스 제어 정책에서 연결된 사전 필터 정책으로 이동할 수 있습니다. New/modified(신규/수정) 페이지: 사전 필터 정책 페이지에서 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하면 **Move to another policy(**새로운 정책으로 이동**)** 옵션이 제공됩니다. 지원되는 플랫폼: FMC
시간 기준 규칙	6.6	FTD 디바이스의 표준 시간대에 따라 결정되는 날짜 및 시간에 따라 사전 필터 및 터널 규칙을 적용하는 기능입니다. 액세스 컨트롤 규칙 기록, 1662 페이지의 설명을 참조하십시오.

기능	버전	세부 사항
사전 필터 규칙 페이지의 개체 세부 사항 보기	6.6	도입된 기능: 사전 필터 규칙을 확인할 때 개체 또는 개체 그룹의 세부 사항을 볼 수 있는 옵션입니다. 신규 옵션: 사전 필터 규칙의 다음 열 중 하나에 있는 값을 클릭하면 소스 네트워크, 대상 네트워크, 소스 포트, 대상 포트, VLAN 태그 등 개체 세부 사항을 볼 수 있는 옵션이 제공됩니다. 지원되는 플랫폼: Firepower Management Center

67 장

IAB(Intelligent Application Bypass)

다음 주제에서는 Intelligent Application Bypass(IAB)를 사용하도록 액세스 제어 정책을 구성하는 방법을 설명합니다.

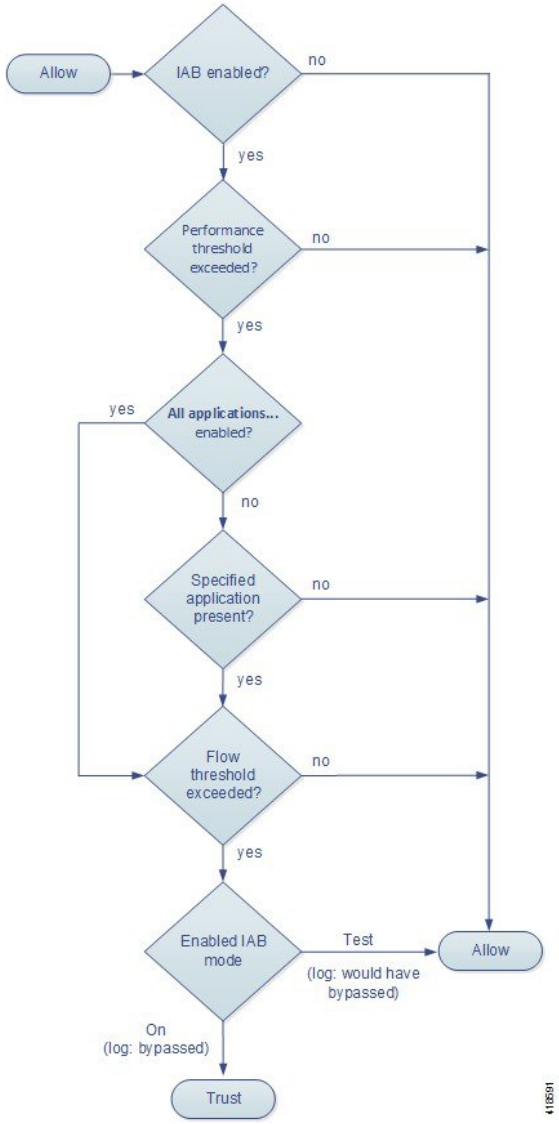
- IAB 소개, 1745 페이지
- IAB 옵션, 1746 페이지
- 인텔리전트 애플리케이션 우회에 대한 요구 사항 및 사전 조건, 1748 페이지
- Intelligent Application Bypass 구성, 1748 페이지
- IAB 로깅 및 분석, 1750 페이지

IAB 소개

IAB는 성능 및 플로우 임계값 초과 시 추가 검사 없이 네트워크를 통과하도록 신뢰하는 애플리케이션을 식별합니다. 예를 들어 야간 백업이 시스템 성능에 크게 영향을 주는 경우 초과 시에 백업 애플리케이션에서 생성하는 트래픽을 신뢰하는 임계값을 구성할 수 있습니다. 이 옵션에는 6.0.1.4 버전 또는 후속 6.0.1.x 패치가 필요합니다. 필요에 따라 애플리케이션 유형에 관계없이 검사 성능 임계값을 초과할 때 IAB가 플로우 바이패스 임계값을 초과하는 모든 트래픽을 신뢰하도록 IAB를 구성할 수 있습니다.

시스템은 트래픽을 심층 검사하기 전에 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업에서 허용하는 트래픽에 대해 IAB를 구현합니다. 테스트 모드를 적용하면 임계값 초과 여부를 확인할 수 있으며, 임계값이 초과되는 경우에는 IAB를 실제로 활성화했을 때(바이패스 모드) 바이패스되는 애플리케이션 플로우를 식별할 수 있습니다.

다음 그래픽에서는 IAB 관련 의사 결정 프로세스를 보여줍니다.



IAB 옵션

상태

IAB를 활성화하거나 비활성화합니다.

성능 샘플링 간격

IAB 성능 샘플링 검사 간의 시간(초)을 지정합니다. IAB 성능 샘플링 검사에서는 시스템이 IAB 성능 임계값과 비교할 시스템 성능 메트릭을 수집합니다. 값을 **0**으로 설정하면 IAB가 비활성화됩니다.

바이패스 가능한 애플리케이션 및 필터

이 기능은 함께 사용할 수 없는 두 가지 옵션을 제공합니다.

애플리케이션/필터
: 우회할 수 있는 애플리케이션 및 애플리케이션 집합(필터)을 지정할 수 있는 편집기를 제공합니다. 애플리케이션 조건(애플리케이션 컨트롤), 535 페이지의 내용을 참조하십시오.

알 수 없는 애플리케이션을 포함한 모든 애플리케이션
: 애플리케이션 유형에 관계없이 검사 성능 임계값을 초과할 때 플로우 바이패스 임계값을 초과하는 모든 트래픽을 신뢰합니다.

성능 및 플로우 임계값

적어도 하나의 검사 성능 임계값과 하나의 흐름 우회 임계값을 구성해야 합니다. 성능 임계값이 초과되면 시스템은 흐름 임계값을 검사하고 하나의 임계값이 초과된 경우, 지정된 트래픽을 신뢰합니다. 두 임계값을 모두 활성화한 경우, 그중 하나만 초과되어야 합니다.

검사 성능 임계값은 초과하는 경우 플로우 임계값 검사를 트리거하는 침입 검사 성능 제한을 제공합니다. IAB는 **0**으로 설정된 검사 성능 임계값을 사용하지 않습니다. 다음 검사 성능 임계값 중 하나 이상을 구성할 수 있습니다.

삭제율

: 고가의 침입 규칙, 파일 정책, 압축 해제 등으로 인해 발생하는 성능 오버로드 때문에 패킷이 삭제될 때 삭제되는 평균 패킷 수(총 패킷의 퍼센트)입니다. 침입 규칙 등의 일반 컨피그레이션으로 인해 삭제되는 패킷은 포함되지 않습니다. 1보다 큰 정수를 지정하는 경우 지정된 퍼센트만큼 패킷이 삭제되면 IAB가 활성화됩니다. 값을 **1**로 지정하는 경우, 퍼센트가 0~1 사이이면 IAB가 활성화됩니다. 즉, 삭제되는 패킷 수가 적더라도 IAB를 활성화할 수 있습니다.

프로세서 사용률

: 사용되는 프로세서 리소스의 평균 퍼센트입니다.

패키지 레이턴시

: 평균 패킷 레이턴시(마이크로초)입니다.

플로우 속도

: 초당 플로우 수로 측정된 시스템 프로세스가 이동하는 속도입니다. 이 옵션은 플로우 개수가 아닌 플로우 속도를 측정하도록 IAB를 구성합니다.

플로우 바이패스 임계값은 초과하는 경우 IAB가 우회 가능한 애플리케이션 트래픽을 신뢰(우회 모드)하도록 하거나 애플리케이션 트래픽을 추가로 검사(테스트 모드)할 수 있도록 하는 플로우 제한을 제공합니다. IAB는 **0**으로 설정된 플로우 바이패스 임계값을 사용하지 않습니다. 다음 흐름 우회 임계값 중 하나 이상을 구성할 수 있습니다.

플로우당 바이트

: 플로우가 포함할 수 있는 최대 킬로바이트 수입니다.

플로우당 패킷

: 플로우가 포함할 수 있는 최대 패킷 수입니다.

플로우 지속시간

플로우를 열어 둘 수 있는 최대 시간(초)입니다.

플로우 속도

최대 전송 속도(초당 킬로바이트)입니다.

인텔리전트 애플리케이션 우회에 대한 요구 사항 및 사전 조건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

Intelligent Application Bypass 구성

⚠

주의 모든 구축에 IAB가 필요한 것은 아니며 IAB가 필요한 구축에서는 제한된 방식으로 IAB를 사용합니다. 네트워크 트래픽(특히 애플리케이션 트래픽)과 시스템 성능(예측 가능한 성능 문제의 원인 포함)에 대해 철저하게 파악하고 있지 않다면 IAB를 활성화하지 마십시오. 바이패스 모드에서 IAB를 실행하기 전에 지정한 트래픽을 신뢰하는 경우 위험이 발생하지 않는지를 확인하십시오.

시작하기 전에

클래식 디바이스의 경우에는 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(고급)**를 클릭하고 **Intelligent Application Bypass Settings(Intelligent Application Bypass** 구성**)** 옆의 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** IAB 옵션을 구성합니다.

- State(상태) - IAB **Off(**끄기**)** 또는 **On(**켜기**)**을 선택하거나 **Test(**테스트**)** 모드에서 IAB를 활성화합니다.
- Performance Sample Interval(성능 샘플링 간격) - IAB 성능 샘플링 검사 간의 시간(초)을 입력합니다. IAB를 활성화하는 경우에는 테스트 모드에서도 0이 아닌 값을 입력합니다. **0**을 입력하면 IAB가 비활성화됩니다.
- Bypassable Applications and Filters(바이패스 가능한 애플리케이션 및 필터) - 다음 중에서 선택합니다.
  - 우회한 애플리케이션 및 필터 수를 클릭하고 트래픽을 우회하려는 애플리케이션을 지정합니다. 애플리케이션 조건 및 필터 구성, 536 페이지 참조.
  - **All applications including unidentified applications(**알 수 없는 애플리케이션을 포함한 모든 애플리케이션**)**를 클릭합니다. 그러면 애플리케이션 유형에 관계없이 검사 성능 임계값을 초과할 때 IAB가 플로우 바이패스 임계값을 초과하는 모든 트래픽을 신뢰합니다.
- Inspection Performance Thresholds(검사 성능 임계값) - **Configure(**구성**)**를 클릭하고 임계값을 하나 이상 입력합니다.
- Flow Bypass Thresholds(플로우 바이패스 임계값) - **Configure(**구성**)**를 클릭하고 임계값을 하나 이상 입력합니다.

검사 성능 임계값과 플로우 바이패스 임계값을 각각 하나 이상 지정해야 합니다. 이 두 임계값을 모두 초과해야 IAB가 플로우를 신뢰합니다. 각 유형의 임계값을 여러 개 입력하는 경우에는 각 유형의 임계값을 하나만 초과하면 됩니다. 자세한 정보는 IAB 옵션, 1746 페이지의 내용을 참고하십시오.

단계 **3** **OK(**확인**)**를 클릭하여 IAB 설정을 저장합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 일부 패킷은 애플리케이션이 탐지되기 전에 통과하도록 허용해야 하므로 해당 패킷을 검사하도록 시스템을 설정해야 합니다.

  트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례, 2202 페이지 및 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정, 2203 페이지를 참조하십시오.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

IAB 로깅 및 분석

IAB는 연결 로깅을 활성화했는지 여부에 관계없이 실제로 바이패스된 플로우와 IAB 활성화 시 바이패스되었을 플로우를 로깅하는 연결 종료 이벤트를 강제로 생성합니다. 연결 이벤트는 바이패스 모드에서 바이패스된 플로우와 테스트 모드에서 IAB 활성화 시 바이패스되었을 플로우를 나타냅니다. 연결 이벤트를 기반으로 하는 맞춤형 대시보드 위젯과 보고서에 바이패스된 플로우와 바이패스되었을 플로우의 장기 통계를 표시할 수 있습니다.

IAB 연결 이벤트

작업

Reason(이유**)**에 `Intelligent App Bypass`가 포함된 경우:

`Allow(`허용**`)` -**

적용된 IAB 구성이 테스트 모드였으며 **Application Protocol(**애플리케이션 프로토콜**)**로 지정된 애플리케이션의 트래픽이 계속 검사할 수 있는 상태임을 나타냅니다.

`Trust(`신뢰**`)` -**

적용된 IAB 구성이 우회 모드였으며 **Application Protocol(**애플리케이션 프로토콜**)**로 지정된 애플리케이션의 트래픽이 추가 검사 없이 네트워크를 통과하도록 신뢰되었음을 나타냅니다.

이유

`Intelligent App Bypass`는 IAB가 바이패스 또는 테스트 모드에서 이벤트를 트리거했음을 나타냅니다.

애플리케이션 프로토콜

이 필드에는 이벤트를 트리거한 애플리케이션 프로토콜이 표시됩니다.

예

아래의 잘린 그래픽에서는 일부 필드가 생략되었습니다. 이 그래픽에는 두 개별 액세스 제어 정책의 각기 다른 IAB 설정에서 생성되는 연결 이벤트 2개에 대한 **Action(**작업**)**, **Reason(**이유**)** 및 **Application Protocol(**애플리케이션 프로토콜**)** 필드가 나와 있습니다.

첫 번째 이벤트에서 `Trust(신뢰)` 작업은 IAB가 바이패스 모드에서 활성화되었으며 Bonjour 프로토콜 트래픽이 추가 검사 없이 통과하도록 신뢰되었음을 나타냅니다.

두 번째 이벤트에서 `Allow(허용)` 작업은 IAB가 테스트 모드에서 활성화되었으므로 Ubuntu Update Manager 트래픽이 추가로 검사되지만 IAB가 바이패스 모드였다면 바이패스되었을 것임을 나타냅니다.

Action	Reason	Application Protocol
Trust	Intelligent App Bypass	Bonjour
Allow	Intelligent App Bypass	Ubuntu Update Manager

404433

예

아래의 잘린 그래픽에서는 일부 필드가 생략되었습니다. 두 번째 이벤트의 플로우는 둘 다 바이패스되었으며(**Action(**작업**)**: `Trust(신뢰)`, **Reason(**이유**)**: `Intelligent App Bypass`) 침입 규칙을 통해 검사되었습니다(**Reason(**이유**)**: `Intrusion Monitor(침입 모니터링)`). 이유가 `Intrusion Monitor(침입 모니터링)`인 경우 **Generate Events(**이벤트 생성**)**로 설정된 침입 규칙이 탐지되었지만 연결 중에 익스플로잇이 차단되지는 않았음을 나타냅니다. 애플리케이션이 탐지되기 전에 침입 규칙이 탐지된 경우를 예로 들 수 있습니다. 애플리케이션이 탐지되고 나면 IAB는 해당 애플리케이션을 바이패스 가능한 것으로 인식하고 플로우를 신뢰합니다.

Last Packet	Action	Reason	Application Protocol
2015-06-12 10:53:09	Trust	Intelligent App Bypass	Skype Probe
2015-06-12 10:53:08	Trust	Intelligent App Bypass, Intrusion Monitor	HTTP

404541

IAB 맞춤형 대시보드 위젯

연결 이벤트에 따라 장기 IAB 통계를 표시할 맞춤형 분석 대시보드 위젯을 생성할 수 있습니다. 위젯을 생성할 때는 다음 사항을 지정합니다.

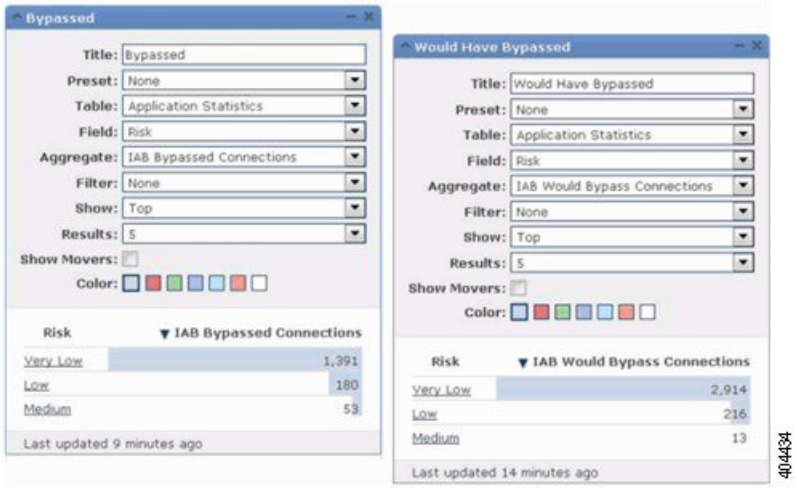
- **Preset(**사전 설정**)**: `None(없음)`
- **Table(**테이블**)**: `Application Statistics(애플리케이션 통계)`
- **Field(**필드**)**: any(모두)
- **Aggregate(**집계**)**: 다음 중 하나
  - `IAB에서 바이패스된 연결 수`
  - `IAB에서 바이패스되는 연결 수`
- **Filter(**필터**)**: any(모두)

예

아래에는 맞춤형 분석 대시보드 위젯의 예시와 해당 설명이 나와 있습니다.

- *Bypassed(*바이패스됨*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 바이패스 모드로 활성화되었기 때문에 바이패스된 애플리케이션 트래픽에 대한 통계를 보여줍니다.

- *Would Have Bypassed(*바이패스되었을 것임*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 테스트 모드로 활성화되었기 때문에 실제로 IAB가 활성화되면 바이패스되었을 애플리케이션 트래픽에 대한 통계를 보여줍니다. .



IAB 맞춤형 보고서

연결 이벤트에 따라 장기 IAB 통계를 표시할 맞춤형 보고서를 생성할 수 있습니다. 보고서를 생성할 때는 다음 사항을 지정합니다.

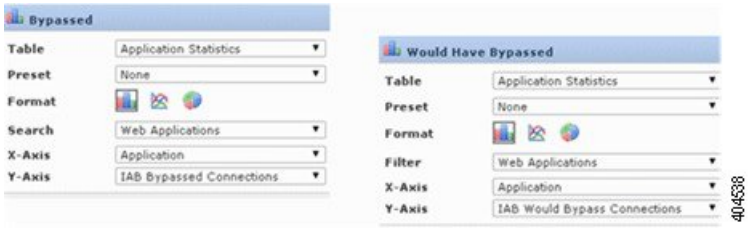
- **Table(**테이블**)**: `Application Statistics(애플리케이션 통계)`
- **Preset(**사전 설정**)**: `None(없음)`
- **Filter(**필터**)**: any(모두)
- **X-Axis(X**축**)**: any(모두)
- **Y-Axis(Y**축**)**: 다음 중 하나
  - `IAB에서 바이패스된 연결 수`
  - `IAB에서 바이패스되는 연결 수`

예

다음 그래픽은 간략하게 표시된 두 보고서 예시를 보여줍니다.

- *Bypassed(*바이패스됨*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 바이패스 모드로 활성화되었기 때문에 바이패스된 애플리케이션 트래픽에 대한 통계를 보여줍니다.
- *Would Have Bypassed(*바이패스되었을 것임*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 테스트 모드로 활성화되

었기 때문에 실제로 IAB가 활성화되면 바이패스되었을 애플리케이션 트래픽에 대한 통계를 보여줍니다.



관련 항목

연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지
맞춤형 분석 위젯, 369 페이지
대시보드에 위젯 추가, 379 페이지
보고서 템플릿, 2653 페이지

68 장

콘텐츠 제한을 사용하는 액세스 제어

다음 주제에서는 콘텐츠 제한 기능을 사용하도록 액세스 제어 정책을 구성하는 방법을 설명합니다.

- 콘텐츠 제한 정보, 1755 페이지
- 콘텐츠 제한 요구 사항 및 사전 요건, 1757 페이지
- 액세스 제어 규칙을 사용하여 콘텐츠 제한 시행, 1757 페이지
- DNS 싱크홀을 사용하여 콘텐츠 제한 적용, 1759 페이지

콘텐츠 제한 정보

주요 검색 엔진 및 콘텐츠 제공 서비스에서는 검색 결과 및 웹 사이트 콘텐츠를 제한할 수 있는 기능을 제공합니다. 예를 들어 학교에서는 콘텐츠 제한 기능을 사용하여 CIPA(Children's Internet Protection Act)를 준수합니다.

검색 엔진 및 콘텐츠 제공 서비스를 통해 구현한 경우, 개별 브라우저 또는 사용자에 대해서만 콘텐츠 제한 기능을 시행할 수 있습니다. Firepower System을 사용하면 이러한 기능을 전체 네트워크에 확장할 수 있습니다.

이 시스템에서 시행할 수 있는 기능:

- 안전 검색 — 대다수의 주요 검색 엔진에서 지원되는 이 서비스는 기업, 정부기관, 교육 환경에서 유해물로 분류하는 노골적인 성인 콘텐츠를 필터링하여 제외합니다. 이 시스템은 지원되는 검색 엔진의 홈 페이지에 사용자가 액세스할 수 있는 기능을 제한하지 않습니다.
- *YouTube EDU* — 이 서비스는 교육 환경에서 YouTube 콘텐츠를 필터링합니다. 학교에서는 이 서비스를 사용하여 교육 콘텐츠에 대한 액세스를 설정하는 동시에 비교육 콘텐츠에 대한 액세스를 제한할 수 있습니다. YouTube EDU는 YouTube 제한 모드와는 다른 것으로, Google 세이프서치 기능의 일부로서 YouTube 검색 결과를 제한합니다. YouTube 제한 모드는 세이프서치의 하위 기능입니다. YouTube EDU를 활용하면 사용자는 일반적인 YouTube 홈 페이지 대신 YouTube EDU 홈 페이지에 액세스하게 됩니다.

두 가지 방법을 사용하여 다음 기능을 시행하도록 시스템을 구성할 수 있습니다.

방법**:** 액세스 제어 규칙
콘텐츠 제한 기능은 요청 URI의 요소, 연관된 쿠키 또는 맞춤형 HTTP 헤더 요소를 통해 제한된 상태의 검색 또는 콘텐츠 쿼리를 전달합니다. 시스템에서 트래픽을 처리할 때 이러한 요소를 수정하도록 액세스 제어 규칙을 구성할 수 있습니다.

방법**: DNS** 싱크홀
Google 검색의 경우, 트래픽이 Google 세이프서치 VIP(Virtual IP Address)로 리디렉션하도록 구성할 수 있습니다. 이렇게 하면 세이프서치를 위한 필터가 부여됩니다.

아래 표에는 이러한 시행 방법 간의 차이가 설명되어 있습니다.

표 ***105:*** 콘텐츠 제한 방법 비교

Attribute(속성**)**	방법**:** 액세스 제어 규칙	방법**: DNS** 싱크홀
지원되는 장치	모두	Firepower Threat Defense 전용
검색 엔진 지원	규칙 편집기의 **Applications(**애플리케이션**)** 탭에서 `safesearch supported` 태그가 있는 모든 애플리케이션	Google 전용
YouTube 제한 모드 지원	예	예
YouTube EDU 지원	예	아니요
SSL 정책 필요	예	아니요
호스트에서 IPv4를 사용 중이어야 함	아니요	예
연결 이벤트 로깅	예	예

사용할 방법을 결정할 때에는 다음 제한 사항을 고려하십시오.

- 액세스 제어 규칙 방법에는 SSL 정책이 필요하며, 이는 성능에 영향을 미칩니다.
- Google 세이프서치 VIP는 IPv4 트래픽만 지원합니다. Google 검색을 관리하기 위해 DNS 싱크홀을 구성할 경우, 영향을 받는 네트워크의 모든 호스트에서 IPv4를 사용 중이어야 합니다.

시스템에 로깅되는 연결 이벤트의 **Reason(**이유**)** 필드 값은 방법에 따라 달라집니다.

- 액세스 제어 규칙 — 콘텐츠 제한
- DNS 싱크홀 — `DNS 차단`

콘텐츠 제한 요구 사항 및 사전 요건

모델 지원

Any(모두) 또는 절차에 나와 있는대로.

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

액세스 제어 규칙을 사용하여 콘텐츠 제한 시행

주의 규칙 사전 대응을 방지하려면 SSL 및 액세스 제어 정책에서 YouTube EDU 관리 규칙을 안전 검색 관리 규칙 위에 배치합니다. 콘텐츠 제한 규칙 순서, 1621 페이지 참조.

참고 액세스 제어 규칙에서 안전 검색 또는 YouTube EDU가 활성화되면 인라인 정규화가 자동으로 활성화됩니다. 자세한 내용은 인라인 정상화 전처리기, 2317 페이지를 참고하십시오.

시작하기 전에

클래식 디바이스의 경우에는 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** SSL 정책을 생성합니다(기본 SSL 정책 생성, 1798 페이지 참조).

단계 **2** 안전 검색 및 YouTube EDU 트래픽 처리용 SSL 규칙을 추가합니다.

- 규칙에 대한 **Action(**작업**)**으로 **Decrypt - Resign(**암호 해독 - 다시 서명**)**을 선택합니다. 시스템은 콘텐츠 제한 처리를 위한 다른 작업은 지원하지 않습니다.
- **Applications(**애플리케이션**)**에서 **Selected Applications and Filters(**선택한 애플리케이션 및 필터**)** 목록에 선택 항목을 추가합니다.

- YouTube EDU - `YouTube` 및 `YouTube Upload` 애플리케이션을 추가합니다.
- 안전 검색 - `Category: search engine`(카테고리: 검색 엔진) 필터를 추가합니다.

자세한 내용은 애플리케이션 조건(애플리케이션 컨트롤), 535 페이지을 참조해 주십시오.

단계 **3** 추가한 SSL 규칙의 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

사전 대응을 방지하기 위해 안전 검색 규칙을 YouTube EDU 규칙 뒤에 배치합니다.

단계 **4** 액세스 제어 정책을 생성 또는 편집하고 SSL 정책을 액세스 제어 정책에 연결합니다.

자세한 내용은 액세스 제어에 다른 정책 연결, 1641 페이지를 참고하십시오.

단계 **5** 액세스 제어 정책에서 안전 검색 및 YouTube EDU 트래픽 처리를 위한 규칙을 추가합니다.

- 규칙에 대한 **Action(**작업**)**으로 **Allow(**허용**)**를 선택합니다. 콘텐츠 제한 처리를 위해 다른 작업을 수행할 수는 없습니다.
- **Applications(**애플리케이션**)**에서 안전 검색( ) 또는 **YouTube EDU**( )에 대해 흐리게 표시하고 관련 옵션을 설정합니다. 액세스 제어 규칙에 대한 안전 검색 옵션, 1759 페이지 및 액세스 제어 규칙에 대한 YouTube EDU 옵션, 1759 페이지의 내용을 참조하십시오.

  규칙에 대해 **Allow(**허용**)**가 아닌 **Action(**작업**)**을 선택하면 이러한 옵션은 흐리게 표시되지 않고 비활성화됩니다.

  같은 액세스 제어 규칙에 대해 안전 검색 제한과 YouTube EDU 제한을 둘 다 활성화할 수는 없습니다.
- **Applications(**애플리케이션**)**의 **Selected Applications and Filters(**선택한 애플리케이션 및 필터**)** 목록에서 애플리케이션 선택 항목을 구체화합니다.

  대부분의 경우 안전 검색 또는 YouTube EDU를 활성화하면 **Selected Applications and Filters(**선택한 애플리케이션 및 필터**)** 목록에 적절한 값이 입력됩니다. 이 기능을 활성화할 때 안전 검색 또는 YouTube 애플리케이션이 목록에 이미 있으면 값이 목록에 자동으로 입력되지 않습니다. 애플리케이션이 자동으로 입력되지 않으면 다음과 같이 수동으로 추가합니다.

  - YouTube EDU - `YouTube` 및 `YouTube Upload` 애플리케이션을 추가합니다.
  - 안전 검색 - `Category: search engine`(카테고리: 검색 엔진) 필터를 추가합니다.

자세한 정보는 애플리케이션 조건 및 필터 구성, 536 페이지의 내용을 참고하십시오.

단계 **6** 추가한 액세스 제어 규칙의 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

사전 대응을 방지하기 위해 안전 검색 규칙을 YouTube EDU 규칙 뒤에 배치합니다.

단계 **7** 제한된 콘텐츠가 차단될 때 표시되는 HTTP 응답 페이지)를 구성합니다(HTTP 응답 페이지 선택, 1691 페이지 참조).

단계 **8** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 제어 규칙에 대한 안전 검색 옵션

Firepower System은 특정 검색 엔진에 대해서만 안전 검색 필터링을 지원합니다. 지원되는 검색 엔진 목록을 확인하려면 액세스 제어 규칙 편집기의 **Applications(**애플리케이션**)** 탭에서 `safesearch supported` 태그가 지정된 애플리케이션을 참고하십시오. 지원되지 않는 검색 엔진 목록을 확인하려면 `safesearch unsupported` 태그가 지정된 애플리케이션을 참고하십시오.

액세스 제어 규칙에 대해 안전 검색을 활성화할 때는 다음 파라미터를 설정합니다.

안전 검색 활성화
: 이 규칙과 일치하는 트래픽에 대해 안전 검색 필터링을 활성화합니다.

Unsupported Search Traffic(지원되지 않는 검색 트래픽**)**
: 지원되지 않는 검색 엔진의 트래픽을 처리할 때 시스템에서 수행하도록 할 작업을 지정합니다. **Block(**차단**)** 또는 **Block with Reset(**차단 후 재설정**)**을 선택하는 경우에는 제한된 콘텐츠가 차단될 때 시스템에 표시되는 HTTP 응답 페이지도 구성해야 합니다(HTTP 응답 페이지 선택, 1691 페이지 참조).

액세스 제어 규칙에 대한 **YouTube EDU** 옵션

액세스 제어 규칙에 대해 YouTube EDU를 활성화할 때는 다음 파라미터를 설정합니다.

Enable YouTube EDU(YouTube EDU 활성화**)**
: 이 규칙과 일치하는 트래픽에 대해 YouTube EDU 필터링을 활성화합니다.

맞춤형 **ID**
: YouTube EDU 이니셔티브에서 학교나 지역 네트워크를 고유하게 식별하는 값을 지정합니다. YouTube에서는 학교나 지역에서 YouTube EDU 계정을 등록하면 이 ID를 제공합니다.

참고 **Enable YouTube EDU(YouTube EDU** 활성화**)**를 선택하는 경우 **Custom ID(**맞춤형 **ID)**를 입력해야 합니다. 이 ID는 YouTube가 외부에서 정의합니다. YouTube 시스템에 대해 입력하는 내용은 검증되지 않습니다. 잘못된 ID를 입력하면 YouTube EDU 제한이 올바르게 수행되지 않을 수 있습니다.

DNS 싱크홀을 사용하여 콘텐츠 제한 적용

일반적으로 DNS 싱크홀은 특정 대상에서 멀리 트래픽을 전송합니다. 이 절차에서는 Google 및 YouTube 검색 결과에 콘텐츠 필터를 적용하는 Google SafeSearch Virtual IP Address(VIP)로 트래픽을 재전송하도록 DNS 싱크홀을 구성하는 방법을 설명합니다.

Google SafeSearch는 VIP에 단일 IPv4 주소를 사용하므로 호스트는 IPv4 주소 지정을 사용해야 합니다.

주의 네트워크에 프록시 서버가 포함된 경우, 이 콘텐츠 제한 방법은 Firepower Threat Defense 디바이스를 프록시 서버와 인터넷 사이에 배치하지 않는 한 효과가 없습니다.

이 절차에서는 Google 검색에 콘텐츠 제한을 적용하는 방법만 설명합니다. 다른 검색 엔진에 콘텐츠 제한을 적용하려면 액세스 제어 규칙을 사용하여 콘텐츠 제한 시행, 1757 페이지를 참조하십시오.

시작하기 전에

이 절차는 Firepower Threat Defense에만 적용되며 위협 라이선스가 필요합니다.

프로시저

단계 **1** 다음 URL을 통해 지원되는 Google 도메인 목록을 얻을 수 있습니다(https://www.google.com/supported_domains).

단계 **2** 로컬 컴퓨터에서 맞춤형 DNS 목록을 생성하고 다음 항목을 추가합니다.

- Google SafeSearch를 적용하려면 지원되는 Google 도메인마다 항목을 추가합니다.
- YouTube 제한 모드를 적용하려면 "youtube.com" 항목을 추가합니다.

맞춤형 DNS 목록은 텍스트 파일(.txt) 형식이어야 합니다. 텍스트 파일의 각 행은 앞에 마침표 없이 개별 도메인 이름을 지정해야 합니다. 예를 들어 지원되는 도메인 ".google.com"은 "google.com"으로 표시되어야 합니다.

단계 **3** 맞춤형 DNS 목록을 Firepower Management Center에 업로드합니다(새 보안 인텔리전스 목록을 다음에 업로드 Firepower Management Center, 608 페이지 참조).

단계 **4** Google SafeSearch VIP의 IPv4 주소를 결정합니다. 예를 들어 forcesafesearch.google.com에서 `nslookup`을 실행합니다.

단계 **5** SafeSearch VIP에 대한 싱크홀 개체를 생성합니다(싱크홀 개체 생성, 609 페이지 참조).

이 개체에 다음 값을 사용합니다.

- IPv4 Address(IPv4 주소) - SafeSearch VIP 주소를 입력합니다.
- IPv6 Address(IPv6 주소) - IPv6 루프백 주소(`::1`)를 입력합니다.
- Log Connections to Sinkhole(싱크 홀에 대한 로그 연결)-Log Connections(로그 연결)
- Type(유형) - **None(**없음**)**을 선택합니다.

단계 **6** 기본 DNS 정책을 생성합니다(기본 DNS 정책 생성, 1712 페이지 참조).

단계 **7** 싱크홀의 DNS 규칙을 추가합니다(DNS 규칙 생성 및 편집, 1714 페이지 참조).

이 규칙에서:

- **Enable(**활성화**)** 확인란을 선택합니다.
- **Action(**작업**)** 드롭다운 목록에서 `Sinkhole(싱크홀)`을 선택합니다.

- **Sinkhole(**싱크홀**)** 드롭다운 목록에서 생성한 싱크홀 개체를 선택합니다.
- 생성한 맞춤형 DNS 목록을 **DNS**에서 **Selected Items(**선택한 항목**)** 목록에 추가합니다.
- (선택 사항) 콘텐츠 제한을 특정 사용자로 제한하려면 **Networks(**네트워크**)**에서 네트워크를 선택합니다. 예를 들어 콘텐츠 제한을 학생 사용자로 제한하려면 학생들을 교직원과 다른 서브넷에 할당하고 이 규칙에서 해당 서브넷을 지정하십시오.

단계 **8** DNS 정책을 액세스 제어 정책에 연결합니다(액세스 제어에 다른 정책 연결, 1641 페이지 참조).

단계 **9** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

XV 부

암호화된 트래픽 처리

- 트래픽 해독 이해, 1765 페이지
- SSL 정책 생성 시작, 1793 페이지
- TLS/SSL 규칙 시작하기, 1803 페이지
- TLS/SSL 규칙을 사용한 암호 해독 조정, 1827 페이지
- SSL 하드웨어 엑셀러레이션(Hardware Acceleration) 모니터링, 1847 페이지
- TLS/SSL 규칙 문제 해결, 1851 페이지

69 장

트래픽 해독 이해

다음 주제에서는 TLS/SSL(Transport Layer Security/Secure Sockets Layer) 검사의 개요와 TLS/SSL 검사 구성 사전 조건을 설명하고 구축 시나리오를 자세히 설명합니다.

참고

TLS 및 SSL이 서로 번갈아 가며 자주 사용되기 때문에 프로토콜 중 하나에 대해 논의 중임을 나타내기 위해 식 *TLS/SSL*을 사용합니다. SSL 프로토콜은 보다 안전한 TLS 프로토콜을 위해 IETF에서 더 이상 사용되지 않으므로 일반적으로 TLS만 참조하는 것으로 *TLS/SSL*을 해석할 수 있습니다.

예외는 SSL 정책입니다. FMC 구성 옵션은 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**이므로 *SSL policies(SSL* 정책*)*라는 용어를 사용합니다. 단, 이러한 정책은 TLS 및 SSL 트래픽에 대한 규칙을 정의하는 데 사용될 수 있습니다.

SSL 및 TLS 프로토콜에 대한 자세한 내용은 SSL과 TLS 비교 - 차이점은 무엇입니까?와 같은 리소스를 참조하십시오.

- 트래픽 암호 해독 설명, 1765 페이지
- TLS 암호화 가속, 1767 페이지
- TLS/SSL 모범 사례, 1770 페이지
- TLS/SSL 정책 및 규칙을 구성하는 방법, 1780 페이지
- TLS/SSL 검사 어플라이언스 구축 시나리오, 1782 페이지
- TLS/SSL 기록, 1790 페이지

트래픽 암호 해독 설명

기본적으로 Firepower System은 SSL(Secure Socket Layer) 또는 그 후속 프로토콜인 TLS(Transport Layer Security) 프로토콜로 암호화된 트래픽을 검사할 수 없습니다. *TLS/SSL* 검사를 통해 검사 없이 암호화 트래픽을 차단하거나 액세스 제어를 사용하여 암호화되거나 해독된 트래픽을 검사할 수 있습니다. 시스템은 암호화된 세션을 처리할 때 트래픽에 대한 상세정보를 로깅합니다. 암호화된 트래픽의 검사 및 암호화된 세션 데이터의 분석을 결합하면 네트워크에서 암호화된 애플리케이션과 트래픽을 더 잘 인식하고 제어할 수 있습니다.

TLS/SSL 검사는 정책 기반 기능입니다. Firepower System에서 액세스 제어 정책은 SSL 정책을 비롯한 하위 정책 및 기타 구성을 호출하는 기본 구성입니다. SSL 정책을 액세스 제어와 연결하면 시스템은 해당 SSL 정책을 사용하여 암호화된 세션을 처리한 후 액세스 제어 규칙을 사용하여 해당 세션을 평가합니다. TLS/SSL 검사를 구성하지 않거나 디바이스에서 지원하지 않는 경우에는 액세스 제어 규칙이 암호화된 모든 트래픽을 처리합니다.

TLS/SSL 검사 구성에서 암호화된 트래픽 통과를 허용하는 경우에도 액세스 제어 규칙이 암호화된 트래픽을 처리합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우, 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

시스템은 TCP 연결을 통해 TLS/SSL 핸드셰이크를 탐지하는 경우, 탐지된 트래픽의 암호 해독 가능 여부를 확인합니다. 확인할 수 없는 경우 구성된 작업을 적용합니다.

- 암호화된 트래픽 차단
- 암호화된 트래픽을 차단하고 TCP 연결 재설정
- 암호화된 트래픽을 해독하지 않음

시스템은 트래픽을 해독할 수 있는 경우, 추가 검사 없이 트래픽을 차단하거나 해독되지 않은 트래픽을 액세스 제어로 평가하거나 다음 방법 중 하나를 사용하여 트래픽을 해독합니다.

- 알려진 개인 키로 해독합니다. 외부 호스트가 네트워크의 서버와 TLS/SSL 핸드셰이크를 시작하면 시스템은 교환된 서버 인증서가 전에 시스템에 업로드된 서버 인증서와 일치하는지 확인합니다. 그런 다음 업로드된 개인 키를 사용하여 트래픽을 해독합니다.
- 서버 인증서를 다시 서명하여 암호를 해독합니다. 네트워크의 호스트가 외부 서버와의 TLS/SSL 핸드셰이크를 시작하면 시스템은 교환된 서버 인증서를 전에 업로드된 CA(Certificate Authority) 인증서로 다시 서명합니다. 그런 다음 업로드된 개인 키를 사용하여 트래픽을 해독합니다.

참고 Firepower System은 상호 인증을 지원하지 않습니다. 즉, 클라이언트 인증서를 FMC에 업로드하여 암호 해독-다시 서명 또는 암호 해독-알려진 키 TLS/SSL 규칙 작업에 사용할 수 없습니다. 자세한 내용은 암호 해독 및 파기(발신 트래픽), 1772 페이지 및 알려진 키 암호 해독(수신 트래픽), 1773 페이지의 내용을 참조하십시오.

암호 해독된 트래픽에는 원래 암호화되지 않은 트래픽과 동일한 트래픽 처리 및 분석, 즉 네트워크, 평판, 사용자 기반 액세스 제어, 침입 탐지 및 방지, Cisco Advanced Malware Protection(Cisco AMP), 검색이 적용됩니다. 시스템은 암호 해독된 트래픽 사후 분석을 차단하지 않는 경우, 대상 호스트로 전달하기 전에 트래픽을 다시 암호화합니다.

참고 매니지드 디바이스에서 암호화된 트래픽을 처리하는 경우, 암호 해독 규칙만 설정합니다. 암호 해독 규칙에는 성능에 영향을 미칠 수 있는 처리 오버헤드가 필요합니다.

Firepower System은 현재 TLS 버전 1.3 암호화 또는 암호 해독을 지원하지 않습니다. 사용자가 TLS 1.3 암호화를 협상하는 웹사이트를 방문하면 웹 브라우저에서 다음과 유사한 오류가 표시될 수 있습니다.

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

이 동작을 제어하는 방법에 대한 자세한 내용은 Cisco TAC에 문의하십시오.

TLS 암호화 가속

TLS 암호화 가속 다음 항목의 속도를 높입니다.

- TLS/SSL 암호화 및 복호화
- TLS/SSL 및 IPsec을 포함한 VPN

지원되는 하드웨어

다음 하드웨어 모델은 TLS 암호화 가속을 지원합니다.

- Firepower Threat Defense가 포함된 Firepower 2100
- Firepower Threat Defense가 포함된 Firepower 4100/9300

  Firepower 4100/9300 FTD 컨테이너 인스턴스의 TLS 암호화 가속 지원에 대한 자세한 정보는 *FXOS* 환경 설정 가이드를 참조하십시오.

앞서 언급한 가상 어플라이언스 및 하드웨어 외에는 TLS 암호화 가속가 지원되지 않습니다.

참고 TLS 암호화 가속 및 4100/9300에 대한 자세한 정보는 *FXOS* 환경 설정 사이드를 참조하십시오.

지원되는 기능 **TLS** 암호화 가속

TLS 암호화 가속이 지원하는 기능에는 다음이 포함됩니다.

- IPv4-IPv4 터널링 프로토콜만 지원됩니다. 다른 IP 터널링 프로토콜은 지원되지 않습니다.
- TLS/SSL GRE(Generic Routing Encapsulation) 터널에서 캡슐화된 트래픽 암호 해독

지원되지 않는 기능 **TLS** 암호화 가속

TLS 암호화 가속가 지원하지 않는 기능에는 다음이 포함됩니다.

- 검사 엔진이 연결을 유지하도록 구성되고 검사 엔진이 예기치 않게 실패하는 경우 엔진이 재시작될 때까지 TLS/SSL트래픽이 중단됩니다.

  이 동작은 **configure snort preserve-connection {enable | disable}** 명령이 제어합니다.

TLS 암호화 가속 지침 및 제한 사항

매니지드 디바이스에서 TLS 암호화 가속이 활성화된 경우, 다음에 유의하십시오.

HTTP 전용 성능

트래픽을 암호 해독하지 않는 매니지드 디바이스에서 TLS 암호화 가속를 사용하면 성능에 영향을 줄 수 있습니다.

FIPS(Federal Information Processing Standards)

TLS 암호화 가속 및 FIPS(Federal Information Processing Standard)가 모두 활성화되는 경우, 다음 옵션과의 연결은 실패합니다.

- 크기가 2,048 바이트보다 작은 RSA 키
- RC4(Rivest Cpher 4)
- 단일 데이터 암호화 표준(단일 DES)
- MD5(Merkle–Damgard 5)
- SSL v3

보안 인증 컴플라이언스 모드에서 작동하도록 Firepower Management Center 및 매니지드 디바이스를 구성하는 경우 FIPS가 활성화됩니다. 해당 모드에서 작동 중 연결을 허용하려면 웹 브라우저를 구성하여 더 안전한 옵션을 선택합니다.

자세한 내용:

- FIPS에서 지원되는 암호: SSL 설정 정보, 1432 페이지
- 보안 인증 컴플라이언스 모드, 1469 페이지.
- 공통 평가 기준

TLS 하트비트

일부 애플리케이션은 *TLS* 하트비트를 TLS(Transport Layer Security) 및 DTLS(Datagram Transport Layer Security) 프로토콜로 확장합니다. 이 프로토콜은 RFC6520에서 정의합니다. TLS 하트비트는 연결 상태를 확인하는 방법을 제공합니다. 즉 클라이언트 또는 서버가 특정 바이트의 데이터를 전송하고 상대방의 에코 응답을 요청합니다. 성공한 경우, 암호화된 데이터가 전송됩니다.

자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지를 참고하십시오.

Max Heartbeat Length(최대 하트비트 길이**)**를 NAP(Network Analysis Policy)에서 구성하고 TLS 하트비트를 처리하는 방법을 결정할 수 있습니다. 자세한 내용은 SSL 전처리기, 2294 페이지을 참조하십시오.

TLS/SSL 초과 서브스크립션

TLS/SSL 오버서브스크립션은 매니지드 디바이스가 TLS/SSL 트래픽으로 오버로드된 상태입니다. 모든 매니지드 디바이스에서 TLS/SSL오버서브스크립션이 발생할 수 있지만 TLS 암호화 가속를 지원하는 매니지드 디바이스만 이를 처리하는 구성 방법을 제공합니다.

TLS 암호화 가속가 활성화된 매니지드 디바이스가 오버서브스크립션되는 경우, 매니지드 디바이스가 수신하는 모든 패킷은 SSL 정책 **Undecryptable Actions(**암호 해독 불가 작업**)**의 **Handshake Errors(**핸드셰이크 오류**)** 설정에 따라 수행됩니다.

- 기본 작업 상속
- Do not decrypt(암호 해독 안 함)
- Block(차단)
- Block with Reset(차단 후 재설정)

SSL 정책 **Undecryptable Actions(**암호 해독 불가 작업**)**의 **Handsake Errors(**핸드셰이크 오류**)**에 대한 설정이 **Do Not decrypt(**암호 해독 안 함**)**이며 관련 액세스 제어 정책이 트래픽을 검사하도록 구성하는 경우, 검사가 이루어지며 암호 해독은 진행되지 않습니다.

초과 서브스크립션이 많이 발생하는 경우, 다음 방법을 사용합니다.

- 매니지드 디바이스를 업그레이드하여 TLS/SSL 처리 용량을 늘립니다.
- SSL 정책을 변경하여 암호 해독 우선 순위가 높지 않은 트래픽의 **Do Not Decrypt(**암호 해독 안 함**)** 규칙을 추가합니다.

TLS 암호화 가속 상태 보기

이 주제에서는 TLS 암호화 가속 활성화 여부를 확인하는 방법을 설명합니다.

Firepower Management Center에서 다음 작업을 수행합니다.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 클릭합니다.

단계 **3** 수정( )을 클릭하여 매니지드 디바이스를 편집합니다.

단계 **4** **Device(**디바이스**)** 페이지를 클릭합니다. TLS 암호화 가속 상태가 General(일반) 섹션에 표시됩니다.

TLS/SSL 모범 사례

이 섹션에서는 암호 해독 정책 및 규칙을 생성할 때 고려해야 하는 정보를 설명합니다.

참고 TLS 및 SSL이 서로 번갈아 가며 자주 사용되기 때문에 프로토콜 중 하나에 대해 논의 중임을 나타내기 위해 식 *TLS/SSL*을 사용합니다. SSL 프로토콜은 보다 안전한 TLS 프로토콜을 위해 IETF에서 더 이상 사용되지 않으므로 일반적으로 TLS만 참조하는 것으로 *TLS/SSL*을 해석할 수 있습니다.

예외는 SSL 정책입니다. FMC 구성 옵션은 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**이므로 *SSL policies(SSL* 정책*)*라는 용어를 사용합니다. 단, 이러한 정책은 TLS 및 SSL 트래픽에 대한 규칙을 정의하는 데 사용될 수 있습니다.

SSL 및 TLS 프로토콜에 대한 자세한 내용은 SSL과 TLS 비교 - 차이점은 무엇입니까?와 같은 리소스를 참조하십시오.

관련 항목

암호 해독 사례, 1770 페이지
트래픽을 암호 해독해야 하는 경우와 하면 안 되는 경우, 1771 페이지
기타 TLS/SSL 규칙 작업, 1773 페이지
TLS/SSL 규칙 구성 요소, 1776 페이지
TLS/SSL 규칙 순서 평가, 1777 페이지

암호 해독 사례

해독된 트래픽만 Firepower 시스템의 위협 방어 및 정책 시행 기능을 사용할 수 있습니다. Firepower 시스템을 통과할 때 암호화되는 트래픽은 허용하거나 차단할 수 있지만, 심층 검사 또는 (침입 방지를 포함한) 전체 정책 시행의 대상이 되지는 못합니다.

모든 암호화된 연결은 다음과 같습니다.

- TLS/SSL 암호 해독 정책을 통해 전송하여 암호 해독 또는 차단 여부를 결정합니다.

  비보안 SSL 프로토콜을 사용하는 트래픽이나 만료 또는 유효하지 않은 인증서가 있는 트래픽 같은, 네트워크에서 허용하고 싶지 않은 유형의 암호화된 트래픽을 차단하도록 TLS/SSL 암호화 규칙을 구성할 수 있습니다.

- 암호 해독 여부와 관계없이 차단 해제된 연결은 모두 액세스 제어 정책을 통해 최종 허용 또는 차단 여부가 결정됩니다.

트래픽을 암호 해독한 다음 재암호화하면 디바이스의 처리 부하가 증가하므로 전체 시스템 성능이 감소된다는 점에 유의하십시오.

요약:

- 암호화된 트래픽은 정책을 이용해 허용 또는 차단할 수 있습니다. 암호화된 트래픽은 검사할 수 없습니다.

- 암호 해독한 트래픽은 위협 방어 및 정책 시행의 영향을 받습니다. 암호 해독된 트래픽은 정책을 이용해 허용하거나 차단할 수 있습니다.

관련 항목

파일 및 침입 정책을 사용한 심층 검사, 1612 페이지

트래픽을 암호 해독해야 하는 경우와 하면 안 되는 경우

이 섹션에서는 트래픽을 암호 해독해야 하는 경우와, 암호화된 방화벽을 통과하도록 허용해야 하는 경우에 대한 지침을 제공합니다.

트래픽을 암호 해독하면 안 되는 경우

다음에 의해 금지되는 경우 트래픽을 해독해서는 안 됩니다.

- 법. 예를 들어 일부 사법부는 금융 정보 해독을 금지합니다.
- 회사 정책. 예를 들어 회사에서 기밀 통신의 해독을 금지할 수 있습니다.
- 프라이버시 규정
- 인증서 고정(또는 *TLS/SSL*고정)을 사용하는 트래픽은 연결이 중단되지 않도록 암호화 상태를 유지해야 합니다.

특정 유형의 트래픽은 암호 해독을 우회하도록 선택하는 경우, 해당 트래픽에는 처리 작업이 수행되지 않습니다. 암호화된 트래픽은 먼저 SSL 정책에 따라 평가된 뒤 액세스 제어 정책으로 진행하여 최종 허용 또는 차단 결정을 수행합니다. 암호화된 트래픽은 다음을 포함하며 이에 국한되지 않는 모든 TLS/SSL 규칙 조건에서 허용 또는 차단될 수 있습니다.

- 인증서 상태(예: 만료됨 또는 유효하지 않은 인증서)
- 프로토콜 (예: 비보안 SSL 프로토콜)
- 네트워크(보안 영역, IP 주소, VLAN 태그 등)
- 정확한 URL 또는 URL 카테고리
- Port(포트)
- 사용자 그룹

SSL 정책은 이 트래픽에 대한 암호 해독 금지 작업을 제공하지 않습니다. 자세한 내용은 TLS/SSL 규칙 Do Not Decrypt(암호 해독 안 함) 작업, 1819 페이지의 내용을 참조하십시오.

참고 이 항목의 끝에 있는 관련 정보 링크를 이용하면 규칙 평가의 다양한 측면에 대한 설명을 확인할 수 있습니다. URL 및 애플리케이션 필터링 같은 조건에는 암호화된 트래픽 관련 제한이 적용됩니다. 이러한 제한을 이해하고 있어야 합니다.

트래픽을 암호 해독해야 하는 경우

암호화된 트래픽은 암호를 해독해야 Firepower 시스템의 위협 보호 및 정책 시행 기능을 사용할 수 있습니다. 매니지드 디바이스가 (메모리와 처리 능력에 따라) 트래픽 암호 해독을 허용한다면, 법률이나 관련 규정의 보호를 받지 않는 트래픽은 암호 해독해야 합니다. 암호 해독할 트래픽을 결정해야 한다면, 네트워크에서 트래픽을 허용하는 데 따르는 위험을 바탕으로 결정을 내리십시오. Firepower 시스템은 URL 평판, 암호 그룹, 프로토콜 및 기타 다양한 요소를 포함하는 규칙 조건을 사용하여 트래픽을 분류하는 유연한 프레임워크를 제공합니다.

Firepower 시스템은 다음 섹션에서 설명하는 두 가지 암호 해독 방법을 제공합니다.

관련 항목

암호 해독 및 파기(발신 트래픽), 1772 페이지
알려진 키 암호 해독(수신 트래픽), 1773 페이지
TLS/SSL 규칙 지침 및 제한 사항, 1804 페이지
SSL 규칙 순서, 1621 페이지
URL 조건(URL 필터링), 545 페이지
애플리케이션 규칙 순서, 1621 페이지

암호 해독 및 파기(발신 트래픽)

Decrypt - Resign(암호 해독 - 파기**)** TLS/SSL 규칙 작업은 Firepower 시스템이 중간자 역할을 해 차단, 암호 해독, (트래픽이 허용하는 경우) 검사, 재암호화를 수행하게 합니다. **Decrypt - Resign(**암호 해독 - 파기**)** 규칙 작업은 발신 트래픽과 함께 사용합니다. 즉 대상 서버가 보호되는 네트워크 외부에 있습니다.

FTD 디바이스는 규칙에 지정된 내부 CA(Certificate Authority) 개체를 이용해 클라이언트와 협상하며, 클라이언트와 FTD 디바이스 간의 SSL 터널을 구축합니다. 동시에 이 디바이스는 대상 웹 사이트에 접속하여 서버와 FTD 디바이스 간에 SSL 터널을 생성합니다.

따라서 클라이언트는 대상 서버에서 인증서 대신 SSL 암호 해독 규칙에 대해 구성된 CA 인증서를 보게 됩니다. 연결을 완료하려면 클라이언트가 인증서를 신뢰해야 합니다. 그러면 FTD 디바이스에서는 클라이언트와 대상 서버 간의 양방향 트래픽에서 암호 해독/재암호화를 수행합니다.

사전 요구 사항

Decrypt - Resign(암호 해독 - 파기**)** 규칙 작업을 사용하려면 CA 파일 및 페어링된 개인 키 파일을 이용해 내부 CA 개체를 만들어야 합니다. CA 및 개인 키가 없다면 Firepower System에서 생성하면 됩니다.

참고 Firepower System은 상호 인증을 지원하지 않습니다. 즉, 클라이언트 인증서를 FMC에 업로드하여 암호 해독-다시 서명 또는 암호 해독-알려진 키 TLS/SSL 규칙 작업에 사용할 수 없습니다. 자세한 내용은 암호 해독 및 파기(발신 트래픽), 1772 페이지 및 알려진 키 암호 해독(수신 트래픽), 1773 페이지의 내용을 참조하십시오.

관련 항목

TLS/SSL 규칙 암호 해독 작업, 1820 페이지

외부 인증서 개체, 626 페이지

알려진 키 암호 해독(수신 트래픽)

Decrypt - Known Key(암호 해독 - 알려진 키**)** TLS/SSL 규칙 작업은 서버의 개인 키를 사용하여 트래픽을 해독합니다. **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 작업은 수신 트래픽과 함께 사용합니다. 즉 대상 서버가 보호되는 네트워크 내부에 있습니다.

알려진 키로 암호 해독을 수행하는 주요 목적은 외부 공격으로부터 서버를 보호하는 것입니다.

사전 요구 사항

Decrypt - Known Key(암호 해독 - 알려진 키**)** 규칙 작업을 사용하려면 서버의 인증서 파일 및 페어링된 개인 키 파일을 이용해 내부 인증서 개체를 만들어야 합니다.

참고 Firepower System은 상호 인증을 지원하지 않습니다. 즉, 클라이언트 인증서를 FMC에 업로드하여 암호 해독-다시 서명 또는 암호 해독-알려진 키 TLS/SSL 규칙 작업에 사용할 수 없습니다. 자세한 내용은 암호 해독 및 파기(발신 트래픽), 1772 페이지 및 알려진 키 암호 해독(수신 트래픽), 1773 페이지의 내용을 참조하십시오.

관련 항목

TLS/SSL 규칙 암호 해독 작업, 1820 페이지
내부 인증서 개체, 627 페이지

기타 TLS/SSL 규칙 작업

다음 섹션에서는 다른 TLS/SSL 규칙 작업에 대해 설명합니다.

관련 항목

TLS/SSL 규칙 차단 작업, 1819 페이지
TLS/SSL 규칙 모니터링 작업, 1819 페이지

TLS 1.3 서버 ID 검색

RFC 8446에서 정의한 TLS(Transport Layer Security) 프로토콜 1.3의 최신 버전은 보안 통신을 제공하기 위해 많은 웹 서버에서 선호하는 프로토콜입니다. TLS 1.3 프로토콜은 추가 보안을 위해 서버의 인증서를 암호화하며, 액세스 제어 규칙의 애플리케이션 및 URL 필터링 기준과 일치하는 데 인증서가 필요하므로 Firepower System은 전체 패킷의 암호를 해독하지 않고 서버 인증서를 추출하는 방법을 제공합니다.

다음과 같은 경우, *TLS* 서버 *ID* 검색이라고 하는 기능을 활성화할 수 있습니다.

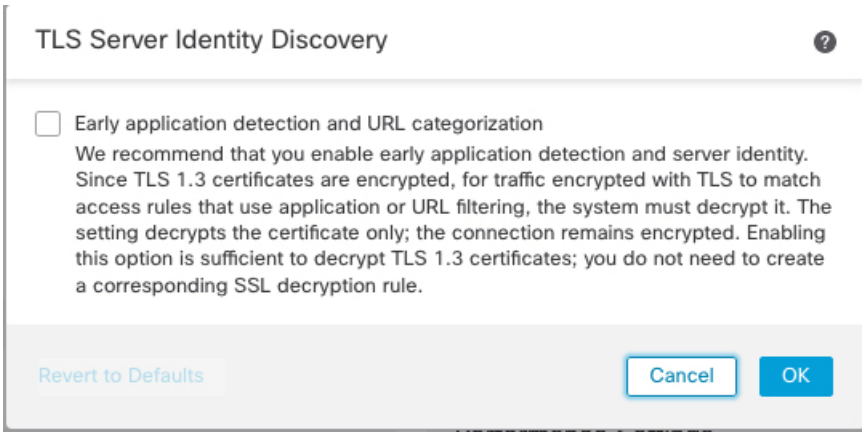
- SSL 정책을 액세스 제어 정책과 연결
- 액세스 제어 정책에 대한 고급 설정 설정

애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.

참고

- TLS 서버 ID 검색은 하드웨어 플랫폼에 따라 성능을 저하시킬 수 있습니다.
- TLS 서버 ID 검색은 인라인 탭 모드 또는 패시브 모드 구축에서 지원되지 않습니다.

다음 그림에는 액세스 제어 정책의 고급 설정에서 TLS 서버 ID 검색을 활성화하는 예가 나와 있습니다.



관련 항목

기본 SSL 정책 생성, 1798 페이지
액세스 제어에 다른 정책 연결, 1641 페이지

TLS/SSL 규칙 예시

다음 섹션에서는 권장되는 TLS/SSL 규칙을 설정하는 예시를 제공합니다.

관련 항목

비보안 프로토콜 차단, 1774 페이지

비보안 프로토콜 차단

이 예에서는 TLS 1.0, TLS 1.1 및 SSLv3 같은, 더 이상 안전하지 않은 것으로 간주되는 TLS 및 SSL 프로토콜을 네트워크에서 차단하는 방법을 보여줍니다.

모든 비보안 프로토콜은 악용 가능하기 때문에 네트워크에서 제외해야 합니다. 이 예에서는 다음을 수행합니다.

- SSL 규칙의 **Version(**버전**)** 페이지를 사용하여 일부 프로토콜을 차단할 수 있습니다.

- Firepower 시스템은 SSLv2르 해독 불가로 간주하기 때문에, SSL 정책에 대한 **Undecryptable Actions(**해독 불가 작업**)**을 사용하여 차단할 수 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management System에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**을 클릭합니다.

단계 **3** SSL 정책을 추가하거나 수정합니다.

단계 **4** **Add Rule(**규칙 추가**)**을 클릭합니다.

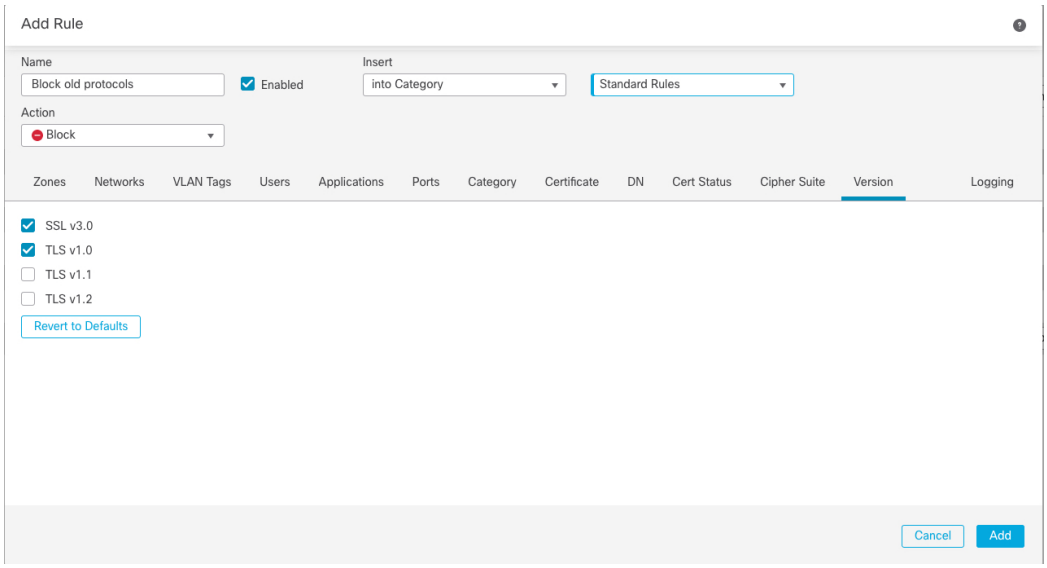
단계 **5** **Name(**이름**)** 필드에 규칙의 이름을 입력합니다.

단계 **6** **Action(**작업**)** 목록에서 **Block(**차단**)** 또는 **Block with reset(**차단 후 재설정**)**을 클릭합니다.

단계 **7** **Version(**버전**)** 페이지를 클릭합니다.

단계 **8** **SSL v3.0**, **TLS 1.0**, **TLS 1.1** 같은 더 이상 안전하지 않은 프로토콜의 확인란을 선택합니다. 안전한 것으로 간주되는 프로토콜의 확인란은 선택 취소합니다.

다음 그림은 예를 보여줍니다.

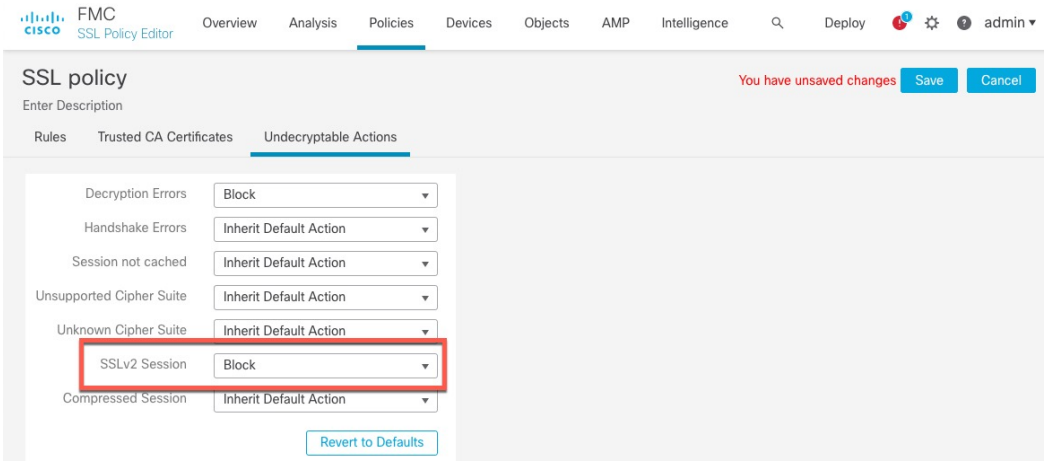


단계 **9** 필요에 따라 다른 규칙 조건을 선택합니다.

단계 **10** 규칙을 저장합니다.

단계 **11** SSL 정책 페이지에서 **Undecryptable Actions(**암호 해독할 수 없는 작업**)**를 클릭합니다.

단계 **12** **SSLv2 Session(SSLv2** 세션**)** 목록에서 **Block(**차단**)** 또는 **Block with reset(**차단 후 재설정**)**을 클릭합니다. 다음 그림은 예를 보여줍니다.



단계 **13** **Save(**저장**)**를 클릭합니다.

단계 **14** 이 규칙은 구체적인 규칙이므로, 정책에서 애플리케이션 매칭 규칙 같은 일반 규칙보다 순위가 높아야 합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

TLS/SSL 규칙 조건, 1816 페이지

TLS/SSL 규칙 구성 요소

각 TLS/SSL 규칙에는 다음과 같은 구성 요소가 있습니다.

상태

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

SSL 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 조건은 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 주체 또는 발급자, 인증서 상태, 암

호 그룹 또는 암호화 프로토콜 버전별로 트래픽 일치 여부를 확인할 수 있습니다. 조건의 사용은 대상 디바이스 라이선스에 따라 달라질 수 있습니다.

작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 일치하는 암호화 트래픽을 모니터링, 허용, 차단 또는 암호 해독할 수 있습니다. 해독되고 허용된 암호화 트래픽은 추가 검사 대상입니다. 시스템은 차단된 암호화 트래픽에 대해 검사를 수행하지 않습니다.

로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다. 규칙과 매칭하는 트래픽을 기록할 수 있습니다. SSL 정책의 설정에 따라 시스템이 암호화 세션을 차단하거나 암호 해독 없이 전달되도록 허용할 때 연결을 로깅할 수 있습니다. 또한 시스템이 나중에 트래픽을 처리하거나 검사하는 방법과 관계없이 액세스 제어 규칙을 통한 추가 평가를 위해 시스템이 해독하는 연결을 반드시 로깅하도록 설정할 수도 있습니다. Firepower Management Center 데이터베이스는 물론 시스템 로그(syslog)나 SNMP 트랩 서버에도 연결을 로깅할 수 있습니다.

로깅에 대한 자세한 내용은 연결 로깅 모범 사례, 2868 페이지를 참조하십시오.

팁 TLS/SSL 규칙을 올바르게 생성하고 순서를 지정하는 것은 복잡한 작업입니다. 정책을 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이선스를 요구하거나, 잘못된 구성을 포함할 수 있습니다. 시스템이 트래픽을 예상대로 처리할 수 있도록 SSL 정책 인터페이스는 규칙에 대한 강력한 경고 및 오류 피드백 시스템을 갖추고 있습니다.

관련 항목

보안 영역 조건, 528 페이지
네트워크 조건, 530 페이지
VLAN 조건, 531 페이지
포트 및 ICMP 코드 조건, 532 페이지
애플리케이션 조건(애플리케이션 컨트롤), 535 페이지
URL 조건(URL 필터링), 545 페이지
사용자, 영역 및 ISE 속성 조건(사용자 제어), 545 페이지
액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

TLS/SSL 규칙 순서 평가

SSL 정책에서 TLS/SSL 규칙을 생성할 때는, 규칙 편집기에서 **Insert(삽입)** 목록을 이용해 순위를 지정해야 합니다. SSL 정책의 TLS/SSL 규칙에는 1부터 시작하는 숫자가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 TLS/SSL 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 TLS/SSL 규칙에 따라 네트워크 트래픽을 처리합니다. Monitor(모니터링) 규칙(트래픽을 로깅하지만 트래픽 흐름에 영향을 주지 않음)의 경우를 제외하고 트래픽이 규칙과 일치하면 시스템은 추가적이고 우선 순위가 낮은 규칙

에 대해 계속해서 트래픽을 평가하지 않습니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 고유 이름(DN), 인증서 상태, 암호 그룹 또는 암호화 프로토콜 버전별로 트래픽을 제어할 수 있습니다.

각 규칙에는 작업이 있는데, 작업은 일치하는 암호화되거나 암호 해독된 트래픽을 액세스 제어로 모니터링, 차단 또는 검사할지 여부를 결정합니다. 시스템은 차단하는 암호화 트래픽을 추가 검사하지 않습니다. 암호화된 트래픽과 해독 불가 트래픽은 액세스 제어 대상입니다. 그러나 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적습니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

팁 TLS/SSL 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다. 사용자가 생성한 규칙이 모든 조직과 배포에 고유하더라도 사용자의 필요를 처리하는 동안 성능을 최적화할 수 있는 규칙을 언제 지시할지에 대해 몇 가지 따라야 할 지침이 있습니다.

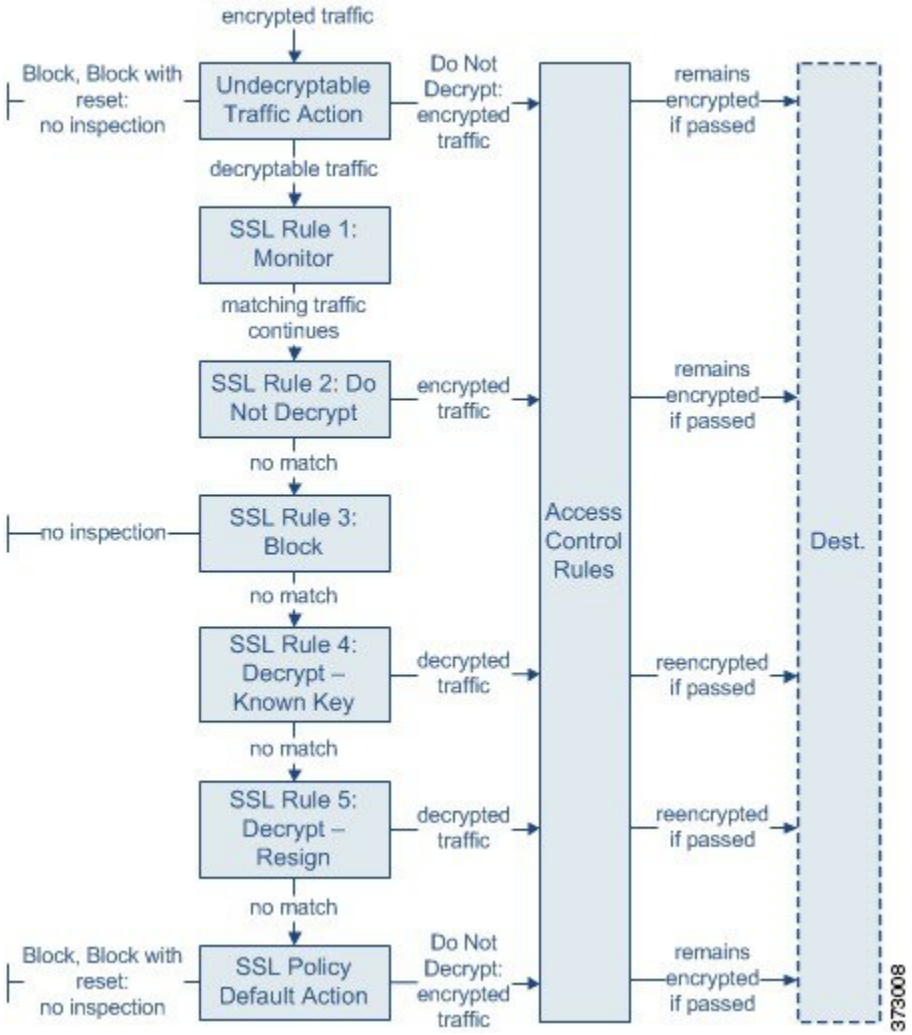
번호로 규칙의 순서를 지정하는 것 외에도 카테고리로 규칙을 그룹화할 수 있습니다. 기본적으로 시스템에서는 Administrator(관리자), Standard(표준) 그리고 Root(루트)의 3가지 카테고리를 제공합니다. 맞춤형 카테고리를 추가할 수는 있지만 시스템에서 제공하는 카테고리를 삭제하거나 순서를 변경할 수는 없습니다.

관련 항목

암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지
SSL 규칙 순서, 1621 페이지
액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

다중 규칙 예시

다음 시나리오는 인라인 구축에서 SSL 규칙이 트래픽을 처리하는 방식을 요약한 것입니다.



이 시나리오에서, 트래픽은 다음과 같이 평가됩니다.

- **Undecryptable Traffic Action**은 암호화 트래픽을 먼저 평가합니다. 시스템에서 해독할 수 없는 트래픽은 추가 검사 없이 차단하거나 액세스 제어 검사를 위해 전달합니다. 매칭하지 않는 암호화 트래픽은 다음 규칙으로 진행합니다.
- **TLS/SSL** 규칙 **1: Monitor(**모니터링**)**가 다음으로 암호화 트래픽을 평가합니다. Monitor(모니터링) 규칙은 암호화 트래픽을 추적하고 로깅하지만 트래픽 플로우에 영향을 주지 않습니다. 시스템은 허용할지 아니면 거부할지 여부를 결정하기 위해 계속해서 트래픽을 추가 규칙에 일치시킵니다.
- **TLS/SSL** 규칙 **2: Do Not Decrypt(**암호 해독 안 함**)**가 세 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 암호 해독되지 않습니다. 시스템은 이 트래픽을 액세스 제어로 검사하지만 파일 또는 침입 검사는 하지 않습니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **TLS/SSL** 규칙 **3: Block(**차단**)**에서 네 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 차단됩니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.

- **TLS/SSL** 규칙 **4: Decrypt - Known Key(**암호 해독 - 알려진 키**)**에서 다섯 번째로 암호화 트래픽을 평가합니다. 네트워크에 수신된 매칭 트래픽은 업로드된 개인 키를 사용하여 해독됩니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **TLS/SSL** 규칙 **5: Decrypt - Resign(**암호 해독 - 다시 서명**)**이 최종 규칙입니다. 트래픽이 이 규칙과 일치하면 시스템은 업로드된 CA 인증서로 서버 인증서를 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하여 트래픽 암호를 해독합니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **SSL Policy Default Action(SSL** 정책 기본 작업**)**은 어떤 TLS/SSL 규칙과도 일치하지 않는 모든 트래픽을 처리합니다. 이 기본 작업은 암호화 트래픽을 추가 검사 없이 차단하거나 해독하지 않고 액세스 제어 검사를 위해 전달합니다.

TLS/SSL 정책 및 규칙을 구성하는 방법

이 항목에서는 네트워크에서 TLS/SSL 트래픽을 차단, 모니터링 또는 허용하는 정책의 SSL 정책 및 TLS/SSL 규칙을 구성하려면 완료해야 하는 작업에 대한 개요를 제공합니다.

이 작업을 수행하려면 관리자, 액세스 관리자 또는 Network Admin(네트워크 관리자)여야 합니다. NGIPSv을(를) 제외한 모든 디바이스 유형에서 SSL 정책을 구성할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	SSL 정책을 생성합니다.	SSL 정책은 하나 이상의 규칙에 대한 컨테이너입니다. 액세스 제어를 위해 SSL 정책 및 해당 규칙을 사용하려면, 나중에 SSL 정책을 액세스 제어 정책과 연결해야 합니다. 자세한 내용은 기본 SSL 정책 생성, 1798 페이지의 내용을 참조하십시오.
단계 **2**	SSL 정책에 대한 기본 작업을 설정합니다.	기본 작업은 트래픽이 SSL 정책에 정의된 어떤 규칙과도 일치하지 않을 때 수행됩니다. SSL 정책 기본 작업, 1794 페이지의 내용을 참조하십시오.
단계 **3**	해독 불가 트래픽을 처리하는 방법을 지정합니다.	비보안 프로토콜, 사용 및 알 수 없는 암호 그룹을 비롯한 여러 이유 때문에, 혹은 핸드셰이크 또는 암호 해독 관련 오류 때문에 트래픽의 암호를 해독하지 못할 수도 있습니다. 암호 해

	명령 또는 동작	목적
		독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지의 내용을 참조하십시오.
단계 4	**Decrypt - Known Key(**암호 해독 - 알려진 키**)**(네트워크의 서버에 들어오는 트래픽을 암호 해독하는 용도) TLS/SSL 규칙의 경우에는 내부 인증서 개체를 생성합니다.	내부 인증서 개체는 사용자 서버의 인증서와 개인 키를 사용합니다. 내부 인증서 개체, 627 페이지의 내용을 참조하십시오.
단계 5	**Decrypt - Resign(**암호 해독 - 파기**)**(네트워크 외부에 있는 서버로 가는 트래픽을 암호 해독하는 용도) TLS/SSL 규칙의 경우에는 내부 인증 기관(CA) 개체를 생성합니다.	내부 CA 개체는 CA 및 개인 키를 사용합니다. 내부 인증 기관 개체, 619 페이지의 내용을 참조하십시오.
단계 6	TLS/SSL 규칙을 생성합니다.	• 차단, 차단 후 재설정, 인터랙티브 차단: TLS/SSL 규칙 동작 구성, 1820 페이지의 내용을 참조하십시오. • 암호 해독 안 함: TLS/SSL 규칙 동작 구성, 1820 페이지의 내용을 참조하십시오. • **Decrypt - Resign(**암호 해독 - 파기**)**: 암호 해독 설정 - 재서명 작업, 1821 페이지의 내용을 참조하십시오. • **Decrypt - Known Key(**암호 해독 - 알려진 키**)**: 암호 해독 설정 - 알려진 키 작업, 1822 페이지의 내용을 참조하십시오. • **Monitor(**모니터링**)**: TLS/SSL 규칙 동작 구성, 1820 페이지의 내용을 참조하십시오.
단계 7	SSL 정책을 액세스 제어 정책에 연결합니다.	SSL 정책을 액세스 제어 정책과 연결하지 않으면 아무런 효과도 발생하지 않습니다. 이 작업을 수행한 후에는 액세스 제어 규칙과 일치하는 트래픽을 허용 하거나 차단하고, 다른 작업을 수행할 수 있습니다. 액세스 제어에 다른 정책 연결, 1641 페이지의 내용을 참조하십시오.
단계 8	암호 해독된 트래픽을 허용 또는 차단하도록 액세스 제어 규칙을 구성합니다.	액세스 제어 정책 구성 요소, 1626 페이지의 내용을 참조하십시오.
단계 9	액세스 제어 정책을 매니지드 디바이스에 구축합니다.	효과를 발휘하려면 정책은 매니지드 디바이스에 구축해야 합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

TLS/SSL 검사 어플라이언스 구축 시나리오

이 섹션에서는 Life Insurance Example, Inc. 생명보험사(LifeIns)가 프로세스 감사를 위해 암호화된 트래픽에서 SSL 검사를 사용하는 몇 가지 시나리오를 보여줍니다. LifeIns는 비즈니스 프로세스를 기반으로 다음을 구축할 계획입니다.

- Underwriting 부서를 위한 인라인 구축의 FTD 디바이스 하나
- 두 디바이스를 관리하기 위한 Firepower Management Center 하나

Customer Service 비즈니스 프로세스

LifeIns는 고객을 위해 고객 대면 웹사이트를 생성했습니다. LifeIns는 웹사이트와 이메일을 통해 잠재 고객으로부터 보험 증권에 대한 암호화된 질문과 요청을 수신합니다. LifeIns의 Customer Service 부서는 24시간 내에 이를 처리하고 필요한 정보를 제공합니다. Customer Service는 수신 연락처 메트릭 수집을 확장하고자 합니다. LifeIns에는 Customer Service에 대해 설정된 내부 감사 검토가 있습니다.

LifeIns는 또한 온라인으로 암호화된 신청서를 수신합니다. Customer Service 부서는 사례 파일을 Underwriting 부서로 전송하기 전 24시간 내에 신청서를 처리합니다. Customer Service는 온라인 양식으로 전송된, 명백하게 잘못된 신청서를 필터링하며, 이 과정에 상당한 시간이 소요됩니다.

Underwriting 비즈니스 프로세스

LifeIns의 보험업자는 암호화된 의료 정보 요청을 Medical Repository Example, LLC 의료 데이터 저장소(MedRepo)에 온라인으로 제출합니다. MedRepo는 요청을 검토하고, 72시간 내에 암호화된 레코드를 LifeIns로 전송합니다. 그 후 보험업자는 신청서에 서명하고 보험 증권 및 요금 결정 사항을 제출합니다. Underwriting은 메트릭 수집을 확장하고자 합니다.

최근에 알 수 없는 소스에서 LifeIns에 스푸핑된 응답을 전송했습니다. LifeIns의 보험업자는 올바른 인터넷 사용에 대한 교육을 받았지만, LifeIns의 IT 부서는 의료 응답 양식을 전송하는 모든 암호화된 트래픽을 분석하고 모든 스푸핑 시도를 차단하고자 합니다.

LifeIns는 6개월 교육 기간을 거쳐 하급 보험업자를 배치합니다. 최근에 이러한 보험업자가 암호화된 의료 규제 요청을 MedRepo의 고객 서비스 부서에 잘못 제출했습니다. MedRepo는 응답 과정에서 여러 불만 사항을 LifeIns에 제출했습니다. LifeIns는 신입 보험업자 교육 기간을 연장하고 MedRepo에 제출하는 보험업자 요청에 대해 감사를 수행할 계획입니다.

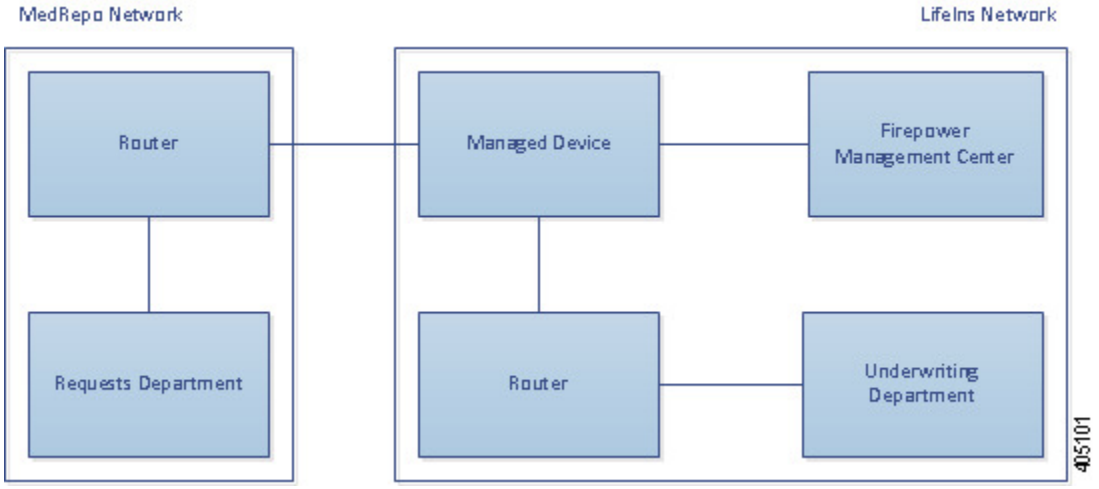
인라인 구축의 트래픽 암호 해독

LifeIns의 비즈니스 요구 사항에서는 Underwriting에서 다음을 수행하도록 규정합니다.

- 신입 및 하급 보험업자를 감사하여, MedRepo에 대한 정보 요청이 모든 해당 규정을 준수하는지 확인합니다.
- 보험 가입 메트릭 수집 프로세스 개선
- MedRepo에서 온 것처럼 보이는 모든 요청을 검토하고 모든 스푸핑 시도 삭제

- Underwriting 부서에서 MedRepo의 Customer Service 부서로 이동하는 모든 부적절한 규제 요청 삭제
- 상급 보험업자는 감사하지 않음

LifeIns는 Underwriting 부서를 위한 인라인 구축에 디바이스를 구축할 계획입니다.



MedRepo의 네트워크에서 오는 트래픽은 MedRepo의 라우터로 이동합니다. 트래픽이 LifeIns의 네트워크로 라우팅됩니다. 매니지드 디바이스는 트래픽을 수신하고, 허용되는 트래픽을 LifeIns의 라우터에 전달하고, 이벤트를 관리 Firepower Management Center로 전송합니다. LifeIns의 라우터는 트래픽을 목적지 호스트로 라우팅합니다.

관리 Firepower Management Center에서 Access Control 및 SSL Editor 맞춤형 역할을 보유한 사용자는 다음을 수행하도록 SSL 액세스 제어를 구성합니다.

- Underwriting 부서로 전송되는 모든 암호화된 트래픽 로깅
- LifeIns의 Underwriting 부서에서 MedRepo의 Customer Service 부서로 잘못 전송된 모든 암호화된 트래픽 차단
- MedRepo에서 LifeIns의 Underwriting 부서, 그리고 LifeIns의 하급 보험업자가 MedRepo의 Requests 부서로 전송한 모든 암호화된 트래픽 해독
- 상급 보험업자가 전송한 암호화된 트래픽은 해독하지 않음

또한 사용자는 해독된 트래픽을 맞춤형 침입 정책으로 검사하도록 액세스 제어를 구성하고 다음을 수행할 수 있습니다.

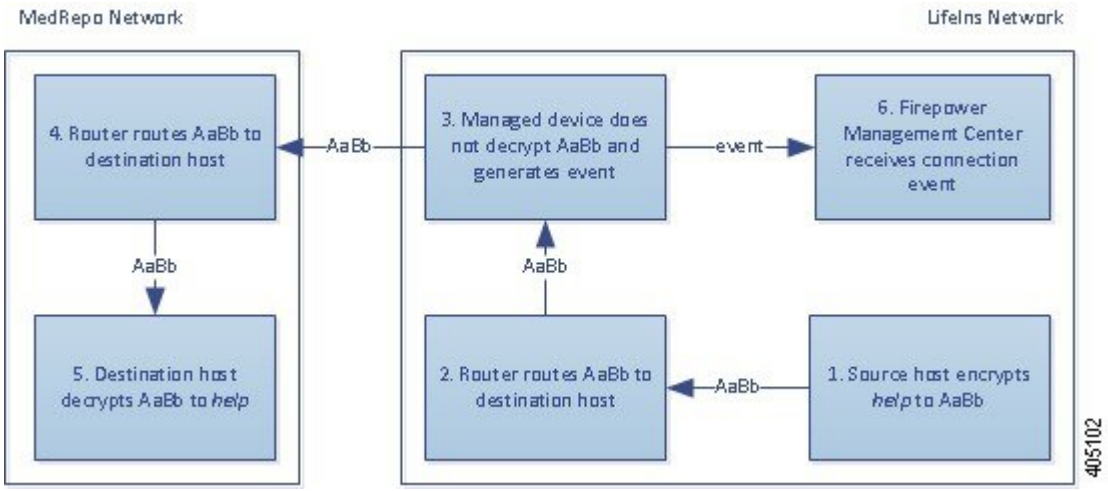
- 스푸핑 시도가 포함된 경우 해독된 트래픽을 차단하고 스푸핑 시도 로깅
- 규정을 준수하지 않는 정보가 포함된 해독된 트래픽을 차단하고 부적절한 정보 로깅
- 다른 모든 암호화된 트래픽 및 해독된 트래픽 허용

시스템은 해독된 트래픽을 목적지 호스트로 전송하기 전에 다시 암호화합니다.

다음 시나리오에서 사용자는 원격 서버에 온라인으로 정보를 제출합니다. 사용자의 브라우저는 서버와 TCP 연결을 설정하고 SSL 핸드셰이크를 시작합니다. 매니지드 디바이스는 이 트래픽을 수신합니다. 핸드셰이크와 연결 상세정보를 기반으로 시스템은 연결을 로깅하고 트래픽에 대해 조치를 취합니다. 시스템은 트래픽을 차단하는 경우 TCP 연결도 닫습니다. 그렇지 않은 경우, 클라이언트와 서버는 SSL 핸드셰이크를 완료하여 암호화된 세션을 설정합니다.

인라인 구축의 암호화된 트래픽 모니터링

Underwriting 부서에서 주고받는 모든 SSL 암호화 트래픽에 대해 시스템은 연결을 로깅합니다.



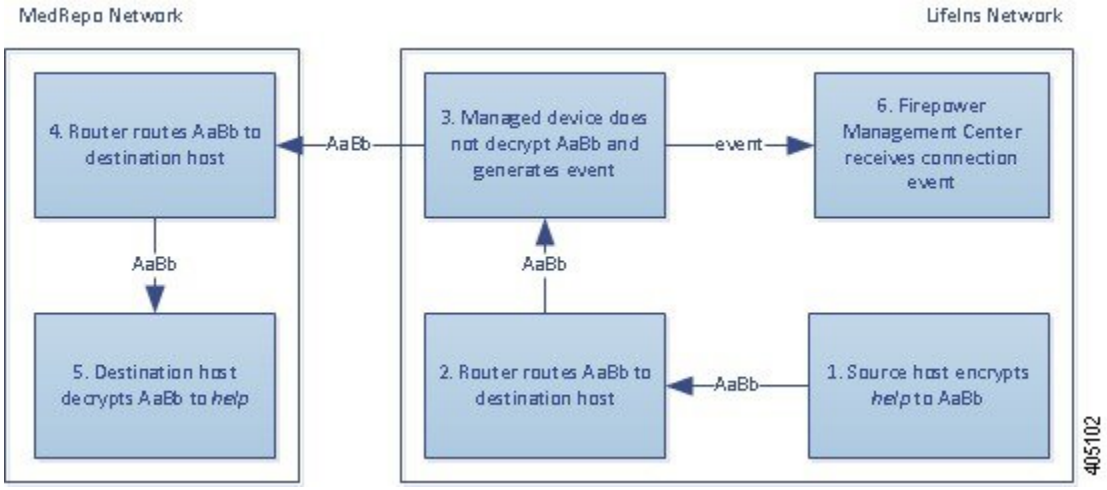
다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`help`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 MedRepo의 Requests 부서 서버로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 트래픽을 해독하지 않습니다.

   액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용한 다음, 세션이 종료된 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Underwriting 부서 서버는 암호화된 정보 요청을 수신하고(`AaBb`) 이를 일반 텍스트로 해독합니다(`help`).
6. Firepower Management Center은 연결 이벤트를 수신합니다.

인라인 구축의 암호화된 트래픽 암호 해독

상급 보험업자로부터 시작된 모든 TLS/SSL 암호화 트래픽의 경우, 매니지드 디바이스는 암호 해독 없이 트래픽을 허용하고 연결을 로깅합니다.



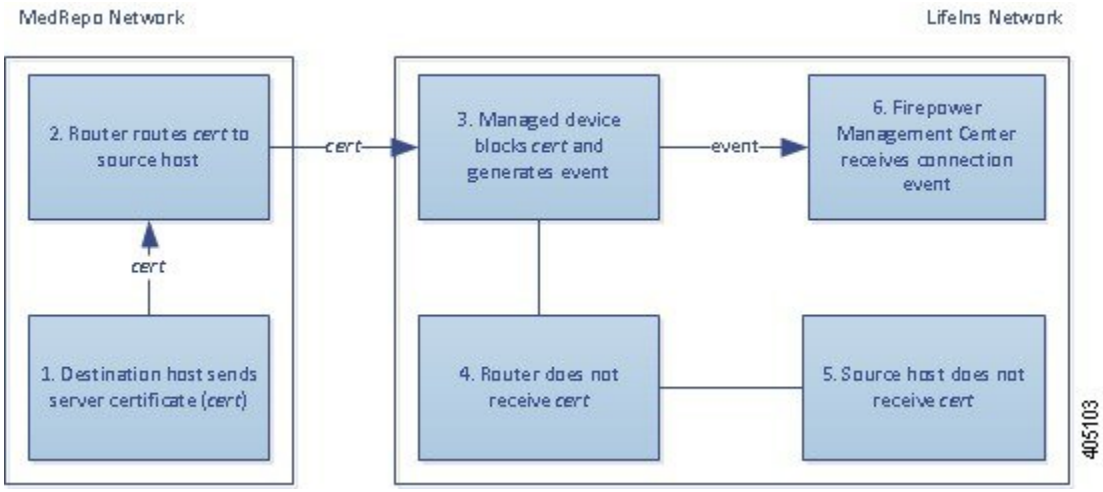
다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`help`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 MedRepo의 Requests 부서 서버로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 이 트래픽을 해독하지 않습니다.

   액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용한 다음, 세션이 종료된 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Requests 부서 서버는 암호화된 정보 요청을 수신하고(`AaBb`) 이를 일반 텍스트로 해독합니다(`help`).
6. Firepower Management Center은 연결 이벤트를 수신합니다.

인라인 구축의 암호화된 트래픽 차단

LifeIns의 Underwriting 부서에서 MedRepo의 Customer Service 부서로 부적절하게 전송된 모든 SMTPS 이메일 트래픽에 대해 시스템은 추가 검사 없이 SSL 핸드셰이크 중에 트래픽을 차단하고 연결을 로깅합니다.

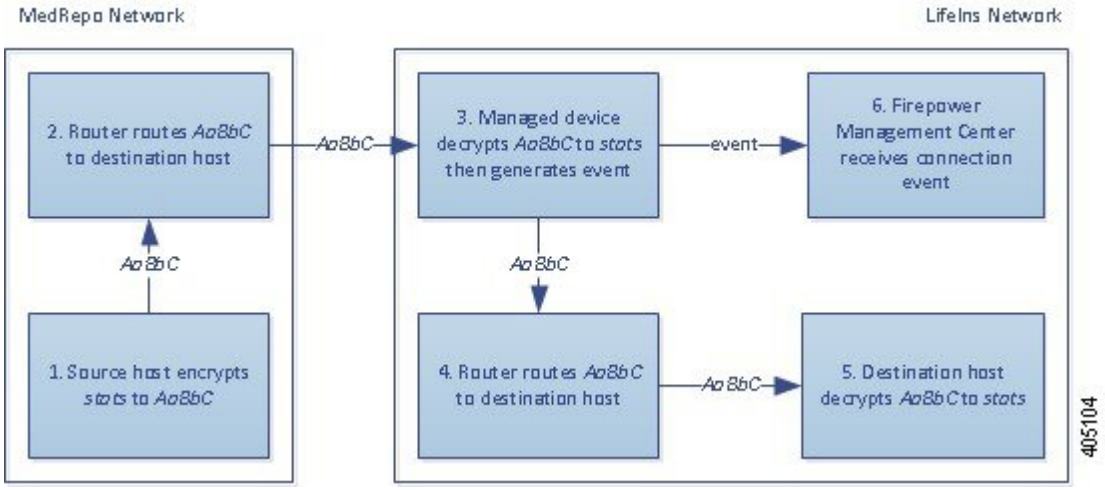


다음 단계가 발생합니다.

1. 클라이언트 브라우저에서 TLS/SSL 핸드셰이크 설정 요청을 받으면 Customer Service 부서 서버는 TLS/SSL 핸드셰이크의 다음 단계로서 LifeIns 보험업자에게 서버 인증서(`cert`)를 전송합니다.
2. MedRepo의 라우터는 인증서를 수신한 다음 LifeIns 보험업자에게 라우팅합니다.
3. 매니지드 디바이스는 추가 검사 없이 트래픽을 차단하고 TCP 연결을 종료하며, 연결 이벤트를 생성합니다.
4. 내부 라우터는 차단된 트래픽을 수신하지 않습니다.
5. 보험업자는 차단된 트래픽을 수신하지 않습니다.
6. Firepower Management Center은 연결 이벤트를 수신합니다.

인라인 구축에서 개인 키로 암호화된 트래픽 검사

MedRepo에서 LifeIns의 Underwriting 부서로 전송되는 모든 TLS/SSL 암호화 트래픽에 대해 시스템은 업로드된 서버 개인 키를 사용하여 세션 키를 가져온 다음 트래픽을 암호 해독하고 연결을 로깅합니다. 합법적인 트래픽은 Underwriting 부서로 전송되기 전에 허용되고 다시 암호화됩니다.

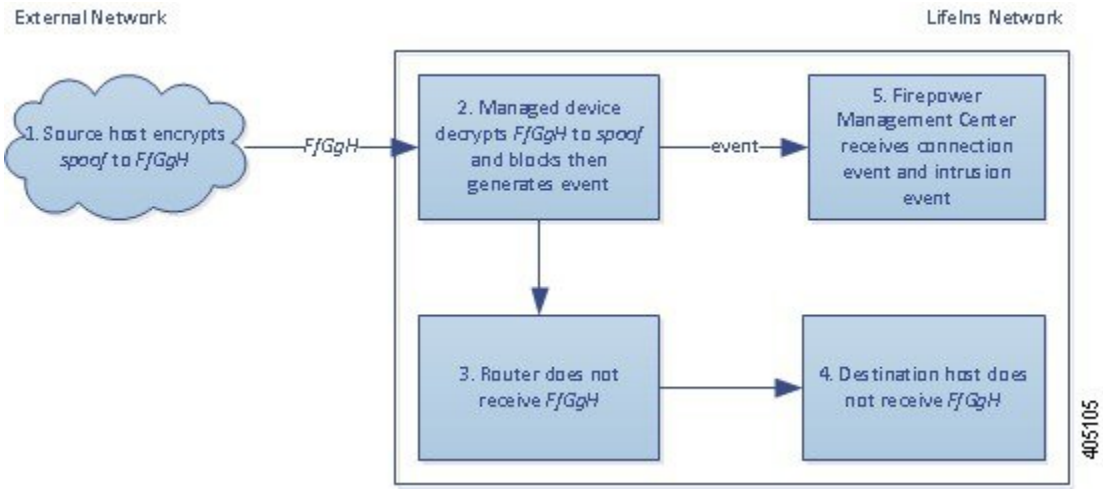


다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`stats`). 클라이언트가 이를 암호화하고(`AaBbC`) 암호화된 트래픽을 Underwriting 부서 서버로 전송합니다.
2. 외부 라우터가 트래픽을 수신한 다음 Underwriting 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`stats`).

   액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 스푸핑 시도를 찾지 않습니다. 디바이스는 암호화된 트래픽을 전달한 다음(`AaBbC`) 세션 종료 후 연결 이벤트를 생성합니다.
4. 내부 라우터가 트래픽을 수신한 다음 Underwriting 부서 서버로 라우팅합니다.
5. Underwriting 부서 서버는 암호화된 정보를 수신하고(`AaBbC`) 이를 일반 텍스트로 해독합니다(`stats`).
6. Firepower Management Center은 암호화된 트래픽과 해독된 트래픽에 대한 정보가 포함된 연결 이벤트를 수신합니다.

이와 반대로, 스푸핑 시도를 나타내는 해독된 트래픽은 삭제됩니다. 시스템은 연결 및 스푸핑 시도를 로깅합니다.



다음 단계가 발생합니다.

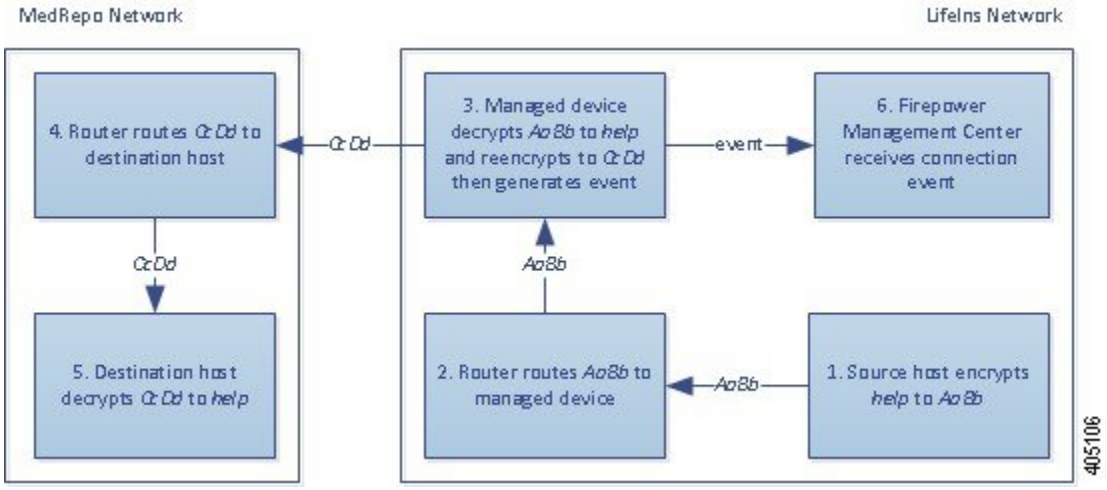
1. 사용자가 일반 텍스트 요청을 제출하고(`spoof`), MedRepo, LLC에서 시작된 것으로 보이는 트래픽을 변경합니다. 클라이언트가 이를 암호화하고(`FfGgH`) 암호화된 트래픽을 Underwriting 부서 서버로 전송합니다.
2. 매니지드 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`spoof`).

   액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 스푸핑 시도를 찾습니다. 디바이스는 트래픽을 차단한 다음 침입 이벤트를 생성하며, 세션 종료 후 연결 이벤트를 생성합니다.
3. 내부 라우터는 차단된 트래픽을 수신하지 않습니다.
4. Underwriting 부서 서버는 차단된 트래픽을 수신하지 않습니다.
5. Firepower Management Center은 암호화된 트래픽 및 해독된 트래픽에 대한 정보가 포함된 연결 이벤트, 그리고 스푸핑 시도에 대한 침입 이벤트를 수신합니다.

인라인 구축에서 다시 서명된 인증서로 암호화된 트래픽 검사

신입 및 하급 보험업자가 MedRepo의 Requests 부서로 전송하는 모든 TLS/SSL 암호화 트래픽에 대해 시스템은 다시 서명된 서버 인증서를 사용하여 세션 키를 얻은 다음 트래픽을 암호 해독하고 연결을 로깅합니다. 합법적인 트래픽은 MedRepo로 전송되기 전에 허용되고 다시 암호화됩니다.

참고 서버 인증서에 다시 서명하여 인라인 구축에서 트래픽을 해독할 때 디바이스는 중간자(man-in-the-middle) 역할을 합니다. 클라이언트와 매니지드 디바이스 간, 매니지드 디바이스와 서버 간에 각각 하나씩 2개의 TLS/SSL 세션을 생성합니다. 그 결과 각 세션에는 서로 다른 암호 세션 세부사항이 포함됩니다.



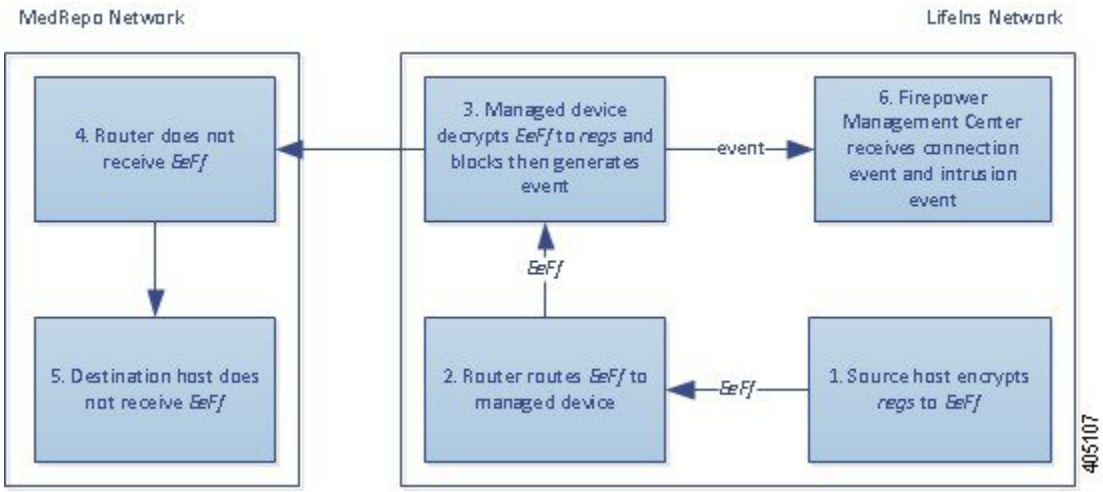
다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`help`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 Requests 부서 서버로 전송합니다.
2. 내부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 다시 서명된 서버 인증서 및 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`help`).

   액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 부적절한 요청을 찾지 않습니다. 디바이스는 트래픽을 다시 암호화하여(`CcDd`) 통과하도록 허용합니다. 세션 종료 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Requests 부서 서버는 암호화된 정보를 수신하고(`CcDd`) 이를 일반 텍스트로 해독합니다(`help`).
6. Firepower Management Center은 암호화된 트래픽과 해독된 트래픽에 대한 정보가 포함된 연결 이벤트를 수신합니다.

참고 다시 서명된 서버 인증서로 트래픽을 암호화하면 클라이언트 브라우저에 신뢰되지 않은 인증서에 대한 경고가 표시됩니다. 이 경고가 표시되지 않도록 하려면 CA 인증서를 조직의 도메인 루트 신뢰할 수 있는 인증서 저장소 또는 클라이언트 신뢰할 수 있는 인증서 저장소에 추가하십시오.

이와 반대로, 규정 요구 사항을 충족하지 못하는 정보를 포함하는 해독된 트래픽은 삭제됩니다. 시스템은 연결 및 비준수 정보를 로깅합니다.



다음 단계가 발생합니다.

1. 사용자가 규정 요구 사항을 준수하지 않는 일반 텍스트 요청을 제출합니다(`regs`). 클라이언트가 이를 암호화하고(`EeFf`) 암호화된 트래픽을 Requests 부서 서버로 전송합니다.
2. 내부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 다시 서명된 서버 인증서 및 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`regs`).

   액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 부적절한 요청을 찾습니다. 디바이스는 트래픽을 차단한 다음 침입 이벤트를 생성하며, 세션 종료 후 연결 이벤트를 생성합니다.
4. 외부 라우터는 차단된 트래픽을 수신하지 않습니다.
5. Requests 부서 서버는 차단된 트래픽을 수신하지 않습니다.
6. Firepower Management Center은 암호화된 트래픽 및 해독된 트래픽에 대한 정보가 포함된 연결 이벤트, 그리고 부적절한 요청에 대한 침입 이벤트를 수신합니다.

TLS/SSL 기록

기능	버전	세부 사항
평판이 알려지지 않은 URL의 처리를 지정할 수 있는 기능	6.7	자세한 내용은 URL 필터링 기록, 1685 페이지 섹션을 참조해 주십시오.
해독 - 알려진 키 규칙을 위한 ClientHello 수정	6.7	자세한 내용은 ClientHello 메시지 처리 섹션을 참조해 주십시오.

기능	버전	세부 사항
트래픽이 액세스 제어 규칙의 URL 및 애플리케이션 기준과 일치하도록 TLS 1.3 트래픽에서 인증서를 추출하는 기능.	6.7	새 화면/수정된 화면: **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **(**액세스 제어 정책 편집**)** > **Advanced(**고급**)**링크. 자세한 내용은 다음 섹션을 참조하십시오. TLS 1.3 서버 ID 검색, 1773 페이지
범주 및 평판 기반 URL 필터링 변경	6.5	자세한 내용은 URL 필터링 기록, 1685 페이지 섹션을 참조해 주십시오.
TLS 암호화 가속 비활성화할 수 없습니다.	6.4	TLS 암호화 가속 지원되는 모든 디바이스에서 활성화됩니다. 기본 인터페이스를 가진 매니지드 디바이스에서 TLS 암호화 가속을 비활성화할 수 없습니다. FTD 컨테이너 인스턴스에서 TLS 암호화 가속에 대한 지원은 이 테이블의 다음 행에 설명된 대로 제한됩니다. 제거된 명령: **system support ssl-hw-accel enable** **system support ssl-hw-accel disable** **system support ssl-hw-status**
Firepower 4100/9300 모듈/보안 엔진에서 하나의 FTD 컨테이너 인스턴스에서의 TLS 암호화 가속에 대한 지원	6.4	이제 모듈/보안 엔진에서 하나의 FTD 컨테이너 인스턴스에 대해 TLS 암호화 가속을 활성화할 수 있습니다. TLS 암호화 가속은 다른 컨테이너 인스턴스의 경우, 비활성화되지만 기본 인스턴스의 경우에는 활성화됩니다. 신규/수정된 명령: **config hwCrypto enable** **show crypto accelerator status**가 **system support ssl-hw-status**를 대체)
TLS/SSL 하드웨어 가속 이제 다음으로 지칭 *TLS* 암호화 가속	6.4	TLS/SSL 암호화 및 암호 해독 가속을 지원하는 디바이스가 늘어난 것을 반영하여 이름이 변경되었습니다. 가속화는 디바이스에 따라 소프트웨어 또는 하드웨어에서 수행될 수 있습니다. 영향을 받는 화면: TLS 암호화 가속의 상태를 보려면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)**, General(일반) 페이지.
지원되는 Extended Master Secret 확장 (RFC 7627 참조)	6.3.0.1	SSL 정책, 특히 **Decrypt - Resign(**암호 해독 - 다시 서명**)**또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 작업이 있는 정책의 경우, TLS Extended Master Secret 확장이 지원됩니다.
지원되지 않는 Extended Master Secret 확장	6.3	확장은 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙에 대한 Client_hello 수정 도중 제거됩니다.

기능	버전	세부 사항
TLS/SSL 하드웨어 가속 기본적으로 활성화	6.3	TLS/SSL 하드웨어 가속 지원되는 모든 디바이스에서 기본적으로 활성화되지만 원하는 경우 비활성화할 수 있습니다.
지원되는 Extended Master Secret 확장 (RFC 7627 참조)	6.2.3.9	SSL 정책, 특히 **Decrypt - Resign(**암호 해독 - 다시 서명**)**또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 작업이 있는 정책의 경우, TLS 확장 마스터 암호 확장이 지원됩니다.
지원되는 카테고리 및 평판 조건	6.2.2	카테고리/평판 조건이 있는 액세스 제어 규칙 또는 SSL 규칙.

70 장

SSL 정책 생성 시작

다음 주제는 SSL 정책 생성, 구성, 관리, 로깅의 개요를 제공합니다.

- SSL 정책 개요, 1793 페이지
- SSL 정책 기본 작업, 1794 페이지
- 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지
- SSL 정책 요구 사항 및 사전 요건, 1797 페이지
- SSL 정책 관리, 1797 페이지
- 기본 SSL 정책 생성, 1798 페이지
- 해독 불가 트래픽에 대한 기본 처리 설정, 1799 페이지
- SSL 정책 수정, 1800 페이지

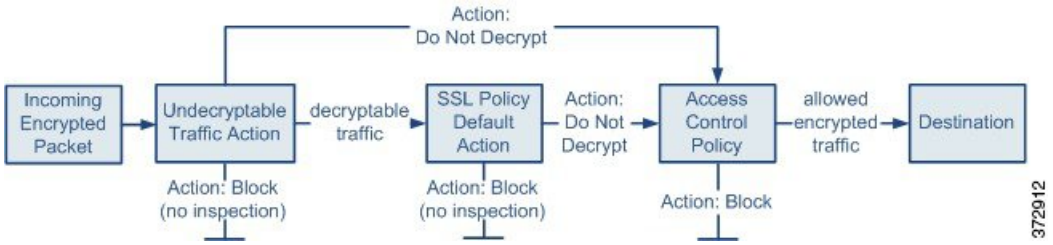
SSL 정책 개요

SSL 정책에 따라 시스템에서 네트워크의 암호화 트래픽을 처리하는 방식이 결정됩니다. 하나 이상의 SSL 정책을 구성하고 SSL 정책을 액세스 제어 정책에 연결한 다음 액세스 제어 정책을 매니지드 디바이스에 구축할 수 있습니다. 디바이스가 TCP 핸드셰이크를 탐지하면 먼저 액세스 제어 정책이 트래픽을 처리하고 검사합니다. 그 이후에 TCP 연결을 통한 TLS/SSL 암호화 세션을 식별할 경우, SSL 정책이 해당 과정을 이어받아 암호화 트래픽을 처리하고 해독합니다.

⚠

주의 SSL 정책을 추가 또는 제거하면 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

다음 다이어그램에서 보여주는 것처럼 가장 간단한 SSL 정책은 정책이 구축된 디바이스에게 단일 기본 작업을 통해 암호화 트래픽을 처리하도록 지시합니다. 추가 검사 없이 해독 가능 트래픽을 차단하거나 액세스 제어로 아직 해독되지 않은 해독 가능한 트래픽을 검사하도록 기본 작업을 설정할 수 있습니다. 그러면 시스템에서 암호화 트래픽을 허용하거나 차단할 수 있습니다. 디바이스는 암호 해독 불가 트래픽을 탐지할 경우, 추가 검사 없이 트래픽을 차단하거나 암호 해독하지 않고 액세스 제어로 검사합니다.



더 복잡한 SSL 정책에서는 다양한 유형의 해독 불가 트래픽을 각기 다른 작업으로 처리하고, CA(인증 기관)에서 암호화 인증서를 발급하였는지 신뢰하는지에 따라 트래픽을 제어하고, 암호화 트래픽 로깅 및 처리를 정밀하게 제어하기 위해 SSL 규칙을 사용할 수 있습니다. 이러한 규칙은 다양한 기준에 따라 암호화 트래픽을 매칭하고 검사하기 때문에 간단할 수도 있고 복잡할 수도 있습니다.

참고 TLS 및 SSL이 서로 번갈아 가며 자주 사용되기 때문에 프로토콜 중 하나에 대해 논의 중임을 나타내기 위해 식 *TLS/SSL*을 사용합니다. SSL 프로토콜은 보다 안전한 TLS 프로토콜을 위해 IETF에서 더 이상 사용되지 않으므로 일반적으로 TLS만 참조하는 것으로 *TLS/SSL*을 해석할 수 있습니다.

예외는 SSL 정책입니다. FMC 구성 옵션은 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**이므로 *SSL policies(SSL* 정책*)*라는 용어를 사용합니다. 단, 이러한 정책은 TLS 및 SSL 트래픽에 대한 규칙을 정의하는 데 사용될 수 있습니다.

SSL 및 TLS 프로토콜에 대한 자세한 내용은 SSL과 TLS 비교 - 차이점은 무엇입니까?와 같은 리소스를 참조하십시오.

관련 항목

TLS/SSL 규칙 조건, 1816 페이지

SSL 정책 기본 작업

SSL 정책의 기본 작업은 정책의 비 모니터 규칙과 일치하지 않는 해독 가능한 암호화 트래픽을 시스템이 처리하는 방법을 결정합니다. TLS/SSL 규칙이 없는 SSL 정책을 구축하는 경우, 기본 작업은 네트워크의 모든 해독 가능 트래픽이 처리되는 방법을 결정합니다. 기본 작업에 의해 차단된 암호화 트래픽에 대해서는 어떠한 검사도 수행하지 않습니다.

표 ***106: SSL*** 정책 기본 작업

기본 작업	암호화 트래픽에 미치는 영향
Block(차단)	추가 검사 없이 TLS/SSL 세션을 차단합니다.

기본 작업	암호화 트래픽에 미치는 영향
Block with Reset(차단 후 재설정)	추가 검사 없이 TLS/SSL 세션을 차단하고 TCP 연결을 재설정합니다. 트래픽이 UDP와 같은 연결 없는 프로토콜을 사용하는 경우, 이 옵션을 선택합니다. 이 경우, 연결 없는 프로토콜은 재설정 될 때까지 다시 연결하려고 시도합니다. 이 작업은 브라우저에 연결 재설정 오류도 표시하므로 사용자는 연결이 차단된 것을 알 수 있습니다.
Do not decrypt(암호 해독 안 함)	액세스 제어를 통해 암호화된 트래픽을 검사합니다.

관련 항목

기본 SSL 정책 생성, 1798 페이지

암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션

표 ***107:*** 해독 불가 트래픽 유형

유형	설명	기본 작업	사용 가능한 작업
압축된 세션	TLS/SSL 세션은 데이터 압축 방식을 적용합니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
SSLv2 세션	세션이 SSL 버전 2로 암호화됩니다. ClientHello 메시지가 SSL 2.0이고 전송된 트래픽의 나머지가 SSL 3.0일 경우 트래픽은 해독 가능합니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
알 수 없는 암호 그룹	시스템에서 암호화 솔루션을 인식하지 않습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속

유형	설명	기본 작업	사용 가능한 작업
지원되지 않는 암호 그룹	시스템에서 탐지된 암호화 솔루션 기반의 해독을 지원하지 않습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
캐싱되지 않는 세션	TLS/SSL 세션에서 세션 재사용이 활성화되었고 클라이언트 및 서버가 세션 식별자로 세션을 재설정했으며 시스템에서 해당 세션 식별자를 캐싱하지 않았습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
핸드셰이크 오류	TLS/SSL 핸드셰이크 협상 중에 오류가 발생했습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
해독 오류	트래픽 해독 중에 오류가 발생했습니다.	차단	Block(차단) Block with Reset(차단 후 재설정)

SSL 정책을 처음 생성할 때 기본 작업에 의해 처리되는 로깅 연결은 기본적으로 비활성화됩니다. 기본 작업에 대한 로깅 설정이 해독 불가 트래픽 처리에도 적용되므로 해독 불가 트래픽 작업에 의해 처리되는 로깅 연결은 기본적으로 비활성화됩니다.

브라우저가 인증서 고정을 사용하여 서버 인증서를 확인하는 경우 서버 인증서에 다시 서명을 하여 이 트래픽을 암호 해독할 수 없습니다. 자세한 내용은 TLS/SSL 규칙 지침 및 제한 사항, 1804 페이지을 참조하십시오.

관련 항목

해독 불가 트래픽에 대한 기본 처리 설정, 1799 페이지

SSL 정책 요구 사항 및 사전 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

SSL 정책 관리

SSL 정책 편집기에서 다음을 수행할 수 있습니다.

- 정책 구성.
- TLS/SSL 규칙 추가, 편집, 삭제, 활성화, 비활성화, 구성.
- 신뢰할 수 있는 CA 인증서 추가.
- 시스템에서 해독할 수 없는 암호화 트래픽의 처리 결정.
- 기본 작업 및 해독 불가 트래픽 작업에 의해 처리되는 트래픽 로깅.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**을(를) 선택합니다.

단계 **2** SSL 정책 관리:

- 연결 - SSL 정책을 액세스 제어 정책에 연결하려면 액세스 제어에 다른 정책 연결, 1641 페이지를 참조하십시오.
- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교, 514 페이지를 참조하십시오.

- 복사- 복사 ( )를 클릭합니다.
- 생성 - **New Policy(**새 정책**)**을 클릭합니다(기본 SSL 정책 생성, 1798 페이지 참조).
- 삭제- 삭제( )를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- 편집-수정( )를 클릭합니다. SSL 정책 수정, 1800 페이지의 내용을 참조하십시오. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 가져오기/내보내기 - 컨피그레이션 가져오기/내보내기 정보, 237 페이지를 참조하십시오.
- 보고서- 보고서( )를 클릭합니다. 현재 정책 보고서 생성, 515 페이지를 참조하십시오.

기본 SSL 정책 생성

SSL 정책을 구성하려면 정책에 고유한 이름과 기본 작업을 지정해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**을(를) 선택합니다.
단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.
단계 **3** 정책에 고유한 **Name(**이름**)** 또는 **Description(**설명**)**을 지정합니다.
단계 **4** **Default Action(**기본 작업**)**을 지정합니다(SSL 정책 기본 작업, 1794 페이지 참조).
단계 **5** 정책 기본 작업으로 연결 로깅, 2873 페이지에 설명된 대로 기본 작업에 대한 로깅 옵션을 구성합니다.
단계 **6** **Save(**저장**)**를 클릭합니다.

향후 작업

- SSL 정책에 추가할 규칙을 구성합니다(TLS/SSL 규칙 생성 및 수정, 1810 페이지 참조).
- 해독 불가 트래픽에 대한 기본 처리를 설정합니다(해독 불가 트래픽에 대한 기본 처리 설정, 1799 페이지 참조).
- 해독 불가 트래픽의 기본 처리에 대한 로깅 옵션을 구성합니다(정책 기본 작업으로 연결 로깅, 2873 페이지 참조).
- 액세스 제어에 다른 정책 연결, 1641 페이지의 설명대로 SSL 정책을 액세스 제어 정책에 연결합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

해독 불가 트래픽에 대한 기본 처리 설정

시스템에서 해독하거나 검사하지 못하는 암호화 트래픽의 특정 유형을 처리하도록 SSL 정책 레벨에서 해독 불가 트래픽 작업을 설정할 수 있습니다. TLS/SSL 규칙이 없는 SSL 정책을 구축하는 경우, 해독 불가 트래픽 작업은 네트워크의 모든 해독 불가 암호화 트래픽이 처리되는 방법을 결정합니다.

해독 불가 트래픽의 유형에 따라 다음 작업을 선택할 수 있습니다.

- 연결 차단.
- 연결을 차단한 다음 재설정. 이 옵션은 UDP와 같이 연결이 차단될 때까지 계속 연결을 시도하는 연결 없는 프로토콜의 경우에 바람직합니다.
- 액세스 제어를 통해 암호화된 트래픽 검사.
- SSL 정책에서 기본 작업 상속.

프로시저

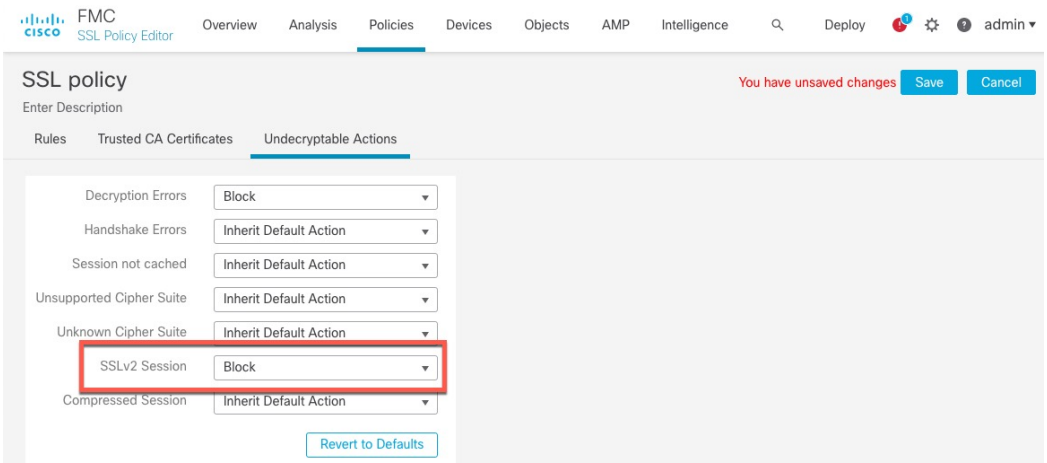
단계 **1** SSL 정책 편집기에서 **Undecryptable Actions(**암호 해독할 수 없는 작업**)**을 클릭합니다.

단계 **2** 각 필드에서 SSL 정책의 기본 작업 또는 해독 불가 트래픽 유형에서 수행할 다른 작업을 선택합니다. 자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지 및 SSL 정책 기본 작업, 1794 페이지를 참고하십시오.

단계 **3** **Save**를 클릭하여 정책을 저장합니다.

예

예를 들어 모든 SSLv2 트래픽을 차단하려면 옵션을 다음과 같이 설정합니다.



다음에 수행할 작업

- 해독 불가 트래픽 작업에 의해 처리되는 연결의 기본 로깅을 구성합니다(정책 기본 작업으로 연결 로깅, 2873 페이지 참조).
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

SSL 정책 수정

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장한 변경사항이 유지됩니다. 편의상 시스템에는 현재 각 정책을 수정하고 있는 사용자(있는 경우)에 대한 정보가 표시됩니다. 세션의 개인 정보를 보호하기 위해 정책 편집기에서 30분 동안 아무런 작업을 하지 않으면 경고가 표시됩니다. 60분이 지나면 시스템에서 변경사항을 삭제합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**를 선택합니다.

단계 **2** 구성할 SSL 정책 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** SSL 정책 구성:

- 설명 - SSL 정책 설명을 업데이트하려면 **Description(**설명**)** 필드를 클릭하고 새 설명을 입력합니다.
- 로깅 - 해독 불가 트래픽 처리 및 SSL 규칙과 일치하지 않는 트래픽에 대한 연결을 로깅하려면 정책 기본 작업으로 연결 로깅, 2873 페이지를 참조하십시오.
- 이름 변경 - SSL 정책 이름을 변경하려면 **Name(**이름**)** 필드를 클릭하고 새 이름을 입력합니다.
- 기본 작업 설정 - SSL 정책에서 SSL 규칙과 일치하지 않는 트래픽을 처리하는 방법을 구성하려면 SSL 정책 기본 작업, 1794 페이지를 참조하십시오.
- 해독 불가 트래픽에 대한 기본 작업 설정 - SSL 정책이 해독 불가 트래픽을 처리하는 방법을 구성하려면 해독 불가 트래픽에 대한 기본 처리 설정, 1799 페이지를 참조하십시오.
- 신뢰 - 신뢰할 수 있는 CA 인증서를 SSL 정책에 추가하려면 외부 인증 증명 신뢰, 1837 페이지를 참조하십시오.

단계 **4** SSL 정책에서 규칙 편집:

- 추가 - 규칙을 추가하려면 **Add Rule(**규칙 추가**)**를 클릭합니다.
- 복사 - 규칙을 복사 하려면 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Copy(**복사**)**를 선택합니다.

- 잘라내기 - 규칙을 잘라내려면 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Cut(**잘라내기**)**을 선택합니다.
- 삭제 - 규칙을 삭제하려면 규칙 옆의 삭제( )을 클릭한 다음 **OK(**확인**)**를 클릭합니다.
- 비활성화 - 활성화된 규칙을 비활성화하려면 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **State(**상태**)**를 선택한 다음 **Disable(**비활성화**)**을 선택합니다.
- 표시 - 특정 규칙 속성의 구성 페이지를 표시하려면 규칙 행의 조건 열에서 이름 또는 값을 클릭합니다. 이를테면 **Source Networks** 열의 이름이나 값을 클릭하여 선택한 규칙의 Networks 페이지를 표시합니다. 네트워크 조건, 530 페이지의 내용을 참조하십시오.
- 편집 - 규칙을 편집하려면 규칙 옆의 수정( )을 클릭합니다.
- 활성화 - 비활성화된 규칙을 활성화하려면 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **State(**상태**)**를 선택한 다음 **Enable(**활성화**)**을 선택합니다. 비활성화된 규칙은 흐리게 표시되며, 규칙 이름 아래에 `(disabled(비활성화))`가 표시됩니다.
- 붙여넣기 - 자르거나 복사한 규칙을 붙여넣으려면 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Paste Above(**위에 붙여넣기**)** 또는 **Paste Below(**아래 붙여넣기**)**를 선택합니다.

단계 **5** 컨피그레이션을 저장하거나 새로 고칩니다.

- 변경 사항을 저장하고 편집을 계속하려면 **Save(**저장**)**를 클릭합니다.
- 변경을 삭제하려면 **Cancel(**취소**)**을 클릭하고, 확인 메시지가 표시되면 **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- SSL 정책이 아직 액세스 제어 정책에 연결되지 않은 경우, 액세스 제어에 다른 정책 연결, 1641 페이지의 설명대로 연결합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

TLS/SSL 규칙 생성 및 수정, 1810 페이지

71 장

TLS/SSL 규칙 시작하기

다음 주제에서는 TLS/SSL 규칙 생성, 관리, 문제 해결의 개요를 제공합니다.

참고

TLS 및 SSL이 서로 번갈아 가며 자주 사용되기 때문에 프로토콜 중 하나에 대해 논의 중임을 나타내기 위해 식 *TLS/SSL*을 사용합니다. SSL 프로토콜은 보다 안전한 TLS 프로토콜을 위해 IETF에서 더 이상 사용되지 않으므로 일반적으로 TLS만 참조하는 것으로 *TLS/SSL*을 해석할 수 있습니다.

예외는 SSL 정책입니다. FMC 구성 옵션은 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**이므로 *SSL policies(SSL* 정책*)*라는 용어를 사용합니다. 단, 이러한 정책은 TLS 및 SSL 트래픽에 대한 규칙을 정의하는 데 사용될 수 있습니다.

SSL 및 TLS 프로토콜에 대한 자세한 내용은 SSL과 TLS 비교 - 차이점은 무엇입니까?와 같은 리소스를 참조하십시오.

- TLS/SSL 규칙 개요, 1803 페이지
- TLS/SSL 규칙 지침 및 제한 사항, 1804 페이지
- TLS/SSL 규칙 요구 사항 및 사전 요건, 1810 페이지
- TLS/SSL 규칙 생성 및 수정, 1810 페이지
- TLS/SSL 규칙 트래픽 처리, 1813 페이지
- TLS/SSL 규칙 조건, 1816 페이지
- TLS/SSL 규칙 작업, 1819 페이지
- TLS/SSL 관리 규칙, 1822 페이지

TLS/SSL 규칙 개요

TLS/SSL 규칙은 여러 매니지드 디바이스에서 암호화된 트래픽을 세부적으로 처리하는 방법을 제공합니다. 이를테면 추가 검사 없이 트래픽을 차단하거나 트래픽을 암호 해독하지 않고 액세스 제어로 검사하거나 액세스 제어 분석을 위해 트래픽을 암호 해독할 수 있습니다.

TLS/SSL 규칙 지침 및 제한 사항

TLS/SSL 규칙을 설정할 때는 다음 사항을 명심하십시오. TLS/SSL 규칙을 올바르게 설정하는 것은 복잡한 작업이지만 암호화된 트래픽을 처리하는 효과적인 구축에 필수적입니다. 제어할 수 없는 특정 애플리케이션 동작을 포함하여 여러 요인이 규칙을 구성하는 방법에 영향을 미칩니다.

또한 규칙은 다른 규칙을 선점하거나 추가 라이선스를 요구하거나 잘못된 구성을 포함할 수 있습니다. 규칙을 세심하게 구성하면 네트워크 트래픽 처리에 필요한 리소스도 줄일 수 있습니다. 지나치게 복잡한 규칙을 만들고 규칙의 순서를 잘못 지정하면 성능에 나쁜 영향을 줄 수 있습니다.

자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지를 참조하십시오.

관련 항목

규칙 및 기타 정책 경고, 554 페이지
액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지
TLS/SSL 암호 해독 사용 지침, 1804 페이지
TLS/SSL 규칙을 지원하지 않는 기능, 1804 페이지
TLS/SSL 암호 해독 금지 지침, 1805 페이지
TLS/SSL 암호 해독 - 파기 지침, 1806 페이지
TLS/SSL 암호 해독 - 알려진 키 지침, 1807 페이지
TLS/SSL 차단 지침, 1808 페이지
TLS/SSL 인증서 고정 지침, 1808 페이지
TLS/SSL 하트비트 지침, 1809 페이지
TLS/SSL 익명 암호 그룹 제한, 1809 페이지
TLS/SSL 노멀라이저 지침, 1809 페이지
기타 TLS/SSL 규칙 지침, 1809 페이지
SSL 규칙 순서, 1621 페이지

TLS/SSL 암호 해독 사용 지침

매니지드 디바이스에서 암호화된 트래픽을 처리하는 경우에만 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙을 설정합니다. 암호 해독 규칙에는 성능에 영향을 미칠 수 있는 처리 오버헤드가 필요합니다.

패시브 또는 인라인 탭 모드 인터페이스가 있는 디바이스에서는 트래픽을 암호 해독할 수 없습니다.

TLS/SSL 규칙을 지원하지 않는 기능

RC4 암호 그룹은 지원되지 않습니다**.**

Rivest Cipher 4(*RC4* 또는 *ARC4*라고도 함) 암호 그룹은 취약성이 있는 것으로 알려져 있으며 안전하지 않은 것으로 간주됩니다. SSL 정책은 RC4 암호 그룹을 지원되지 않는 것으로 식별하기 때문에 조직의 요구 사항에 일치시키려면 정책의 **Undecryptable Actions(**암호 해독 불가 작업**)**

페이지에서 **Unsupported Cipher Suite(**지원되지 않는 암호 그룹**)** 작업을 설정해야 합니다. 자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지를 참고하십시오.

패시브 및 인라인 탭 모드 인터페이스 지원되지 않음

TLS/SSL 패시브 또는 인라인 탭 모드 인터페이스에서 트래픽 암호를 해독할 수 없습니다.

TLS 1.3은 지원되지 않음

Firepower System은 현재 TLS 버전 1.3 암호화 또는 암호 해독을 지원하지 않습니다. 사용자가 TLS 1.3 암호화를 협상하는 웹사이트를 방문하면 웹 브라우저에서 다음과 유사한 오류가 표시될 수 있습니다.

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

이 동작을 제어하는 방법에 대한 자세한 내용은 Cisco TAC에 문의하십시오.

TLS/SSL 암호 해독 금지 지침

다음에 의해 금지되는 경우 트래픽을 해독해서는 안 됩니다.

- 법. 예를 들어 일부 사법부는 금융 정보 해독을 금지합니다.
- 회사 정책. 예를 들어 회사에서 기밀 통신의 해독을 금지할 수 있습니다.
- 프라이버시 규정
- 인증서 고정(또는 *TLS/SSL*고정)을 사용하는 트래픽은 연결이 중단되지 않도록 암호화 상태를 유지해야 합니다.

특정 유형의 트래픽은 암호 해독을 우회하도록 선택하는 경우, 해당 트래픽에는 처리 작업이 수행되지 않습니다. 암호화된 트래픽은 먼저 SSL 정책에 따라 평가된 뒤 액세스 제어 정책으로 진행하여 최종 허용 또는 차단 결정을 수행합니다. 암호화된 트래픽은 다음을 포함하며 이에 국한되지 않는 모든 TLS/SSL 규칙 조건에서 허용 또는 차단될 수 있습니다.

- 인증서 상태(예: 만료됨 또는 유효하지 않은 인증서)
- 프로토콜 (예: 비보안 SSL 프로토콜)
- 네트워크(보안 영역, IP 주소, VLAN 태그 등)
- 정확한 URL 또는 URL 카테고리
- Port(포트)
- 사용자 그룹

TLS/SSL 암호 해독 - 파기 지침

하나의 CA(Certificate Authority) 인증서와 개인 키를 **Decrypt – Resign(**암호 해독 - 다시 서명**)** 작업에 연결할 수 있습니다. 트래픽이 이 규칙과 일치하는 경우, 시스템은 서버 인증서를 CA 인증서로 다시 서명한 다음 중간자(man-in-the-middle) 역할을 합니다. 클라이언트와 매니지드 디바이스 간, 매니지드 디바이스와 서버 간에 각각 하나씩 2개의 TLS/SSL 세션을 생성합니다. 각 세션은 서로 다른 암호화 세션 세부사항을 포함하며 시스템이 트래픽을 암호 해독하고 다시 암호화할 수 있도록 합니다.

모범 사례

다음과 같은 방법을 권장합니다.

- 발신 트래픽 암호 해독을 위한 **Decrypt - Resign(**암호 해독 - 파기**)** 규칙 작업입니다. 수신 트래픽에는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 작업을 권장합니다.

  Decrypt - Known Key(암호 해독 - 알려진 키**)**에 대한 자세한 내용은 TLS/SSL 암호 해독 - 알려진 키 지침, 1807 페이지의 내용을 참조하십시오.

- 암호 해독 - 재서명 규칙 작업을 설정할 때는 키 교환 키만 바꾸기 확인란을 항상 확인해야 합니다.

  사용자가 직접 서명 인증서를 사용하는 웹사이트를 탐색하면, 웹 브라우저에서 보안 경고가 표시되며 안전하지 않은 사이트와 통신 중이라고 경고합니다.

  사용자가 신뢰할 수 있는 인증서를 사용하는 웹사이트를 탐색할 때는 보안 경고가 표시되지 않습니다.

세부 사항

Decrypt - Resign(암호 해독 - 다시 서명**)** 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 서명 알고리즘 유형을 기반으로 트래픽을 매칭합니다. CA 인증서를 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업과 연결하므로 서로 다른 서명 알고리즘으로 암호화된 여러 발신 트래픽 유형을 해독하는 TLS/SSL 규칙을 생성할 수 없습니다. 또한 규칙에 추가하는 외부 인증서 개체와 암호 그룹은 연결된 CA 인증서 암호화 알고리즘 유형과 매칭해야 합니다.

예를 들어 EC(Elliptic Curve) 알고리즘으로 암호화된 발신 트래픽은 작업에서 EC 기반 CA 인증서를 참조할 때만 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙과 일치합니다. 인증서 및 암호 그룹 규칙 조건을 생성하려면 EC 기반 외부 인증서와 암호 그룹을 규칙에 추가해야 합니다.

마찬가지로 RSA 기반 CA 인증서를 참조하는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙은 RSA 알고리즘으로 암호화된 발신 트래픽에만 일치합니다. EC 알고리즘으로 암호화된 발신 트래픽은 구성된 기타 모든 규칙 조건이 일치하더라도 이 규칙과 일치하지 않습니다.

지침 및 제한 사항

다음 사항도 유의하십시오.

익명 암호 그룹 지원되지 않음

본질적으로 익명 암호 그룹은 인증에 사용되지 않으며 키 교환을 사용하지 않습니다. 익명 암호 그룹은 제한적으로 사용됩니다. 자세한 내용은 RFC 5246, 섹션 A.5를 참조하십시오.

익명 암호 그룹이 인증에 사용되지 않으므로 규칙에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

일치하지 않는 암호 그룹

인증서와 일치하지 않는 암호 그룹으로 TLS/SSL 규칙을 저장하려고 시도하면 다음과 같은 오류가 표시됩니다. 문제를 해결하려면 TLS/SSL 암호 그룹 확인, 1856 페이지를 참조하십시오.

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

신뢰할 수 없는 인증 기관

클라이언트가 서버 인증서 재서명에 쓰이는 CA(Certificate Authority)를 신뢰하지 않을 경우 신뢰할 수 없는 인증서임을 사용자에게 경고합니다. 이를 방지하려면 클라이언트가 신뢰하는 CA 저장소에 CA 인증서를 가져오십시오. 또는 조직에 개인 PKI가 있을 경우, 조직의 모든 클라이언트가 자동으로 신뢰하는 루트 CA에 의해 서명된 중간 CA 인증서를 발급한 다음 그 CA 인증서를 디바이스에 업로드할 수 있습니다.

HTTP 프록시 제한

클라이언트와 매니지드 디바이스 사이에 HTTP 프록시가 있고 클라이언트와 서버가 CONNECT HTTP 메서드를 사용하여 터널링된 TLS/SSL 연결을 설정할 경우, 시스템은 트래픽을 암호 해독할 수 없습니다. 시스템에서 이 트래픽을 처리하는 방법은 핸드셰이크 오류 해독 불가 작업에 의해 결정됩니다.

서명된 **CA** 업로드

내부 CA 개체를 생성하고 CSR(certificate signing request) 생성을 선택할 경우, 서명된 인증서를 개체에 업로드해야 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업에 이 CA를 사용할 수 있습니다.

TLS/SSL 암호 해독 - 알려진 키 지침

Decrypt - Known Key(암호 해독 - 알려진 키**)** 작업을 구성할 때 하나 이상의 서버 인증서 및 쌍 개인 키를 이 작업과 연결할 수 있습니다. 트래픽이 규칙과 일치하며 트래픽을 암호화하는 데 사용된 인증서가 작업과 연결된 인증서와 일치하는 경우, 시스템은 적절한 개인 키를 사용하여 세션 암호화 및 암호 해독 키를 얻습니다. 개인 키에 대한 액세스 권한이 있어야 하므로 이 작업은 조직에서 제어하는 서버에서 수신하는 트래픽의 해독에 가장 적합합니다.

다음 사항도 유의하십시오.

익명 암호 그룹 지원되지 않음

본질적으로 익명 암호 그룹은 인증에 사용되지 않으며 키 교환을 사용하지 않습니다. 익명 암호 그룹은 제한적으로 사용됩니다. 자세한 내용은 RFC 5246, 섹션 A.5를 참조하십시오.

익명 암호 그룹이 인증에 사용되지 않으므로 규칙에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

고유 이름 또는 인증서와 매칭할 수 없음

Decrypt - Known Key(암호 해독 - 알려진 키**)** 작업으로 TLS/SSL 규칙을 생성할 때 **Distinguished Name(**고유 이름**)** 또는 **Certificate(**인증서**)** 조건에서 매칭할 수 없습니다. 이 규칙이 트래픽과 매칭할 경우 인증서, 주체 DN, 발급자 DN이 규칙과 연결된 인증서와 이미 매칭한다고 전제합니다.

불일치 서명 알고리즘

Decrypt - Resign(암호 해독 - 다시 서명**)** 작업으로 규칙을 설정한 경우, 하나 이상의 외부 인증서 개체나 암호 그룹에서 서명 알고리즘 유형 불일치가 있다면 정책 편집기는 규칙 옆에 정보() 을 표시합니다. 모든 외부 인증서 개체 또는 모든 암호 그룹에 대해 서명 알고리즘 유형을 잘못 매칭할 경우, 정책은 규칙 옆에 경고 아이콘(경고( ))을 표시하며, SSL 정책과 연결된 액세스 제어 정책을 구축할 수 없습니다.

인증서 고정

고객의 브라우저가 인증서 고정을 사용하여 서버 인증서를 확인하는 경우, 서버 인증서에 다시 서명하여 이 트래픽을 암호 해독할 수 없습니다. 이 트래픽을 허용하려면 서버 인증서 공통 이름 또는 고유 이름(DN)과 일치하도록 **Do not decrypt(**암호 해독 안 함**)** 작업을 사용하여 TLS/SSL 규칙을 구성합니다.

TLS/SSL 차단 지침

해독된 트래픽이 **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 작업이 있는 액세스 제어 규칙과 일치하는 경우, 시스템은 검사 없이 일치하는 연결을 차단하고 사용자 지정 가능한 응답 페이지를 표시하지 않습니다.

규칙에서 로깅을 활성화했다면, **Analysis(**분석**)** > **Events(**이벤트**)** > **Connections(**연결**)**에) 연결 이벤트 2개가 표시됩니다. 하나는 인터랙티브 차단용이며, 다른 이벤트는 사용자의 사이트 진행 선택 여부를 표시합니다.

관련 항목

HTTP 응답 페이지 정보, 1689 페이지

TLS/SSL 인증서 고정 지침

일부 애플리케이션이 *TLS/SSL* 피닝또는 인증서 피닝이라는 기법을 사용하는데 이 기법에서는 원본 서버 인증서 지문이 애플리케이션 자체에 내장됩니다. 따라서 TLS/SSL 규칙을 **Decrypt - Resign(**암호 해독 - 재서명**)** 작업으로 구성하는 경우, 애플리케이션이 매니지드 디바이스로부터 재서명된 인증서를 수신할 때 확인이 실패하고 연결이 중단됩니다.

TLS/SSL 피닝은 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이 문제를 방지하거나 해결하는 방법은 없습니다. 다음 옵션을 이용할 수 있습니다.

- **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙 앞에 오는 이러한 애플리케이션 규칙에 대해서는 **Do not Decrypt(**암호 해독 안 함**)**를 생성하십시오.
- 웹 브라우저를 사용하여 애플리케이션에 액세스하도록 사용자에게 지시합니다.

규칙 순서 지정에 대한 자세한 내용은 SSL 규칙 순서, 1621 페이지를 참조하십시오.

TLS/SSL 하트비트 지침

일부 애플리케이션은 *TLS* 하트비트를 TLS(Transport Layer Security) 및 DTLS(Datagram Transport Layer Security) 프로토콜로 확장합니다. 이 프로토콜은 RFC6520에서 정의합니다. TLS 하트비트는 연결 상태를 확인하는 방법을 제공합니다. 즉 클라이언트 또는 서버가 특정 바이트의 데이터를 전송하고 상대방의 에코 응답을 요청합니다. 성공한 경우, 암호화된 데이터가 전송됩니다.

Max Heartbeat Length(최대 하트비트 길이**)**를 NAP(Network Analysis Policy)에서 구성하고 TLS 하트비트를 처리하는 방법을 결정할 수 있습니다. 자세한 내용은 SSL 전처리기, 2294 페이지을 참조하십시오.

TLS/SSL 익명 암호 그룹 제한

본질적으로 익명 암호 그룹은 인증에 사용되지 않으며 키 교환을 사용하지 않습니다. 익명 암호 그룹은 제한적으로 사용됩니다. 자세한 내용은 RFC 5246, 섹션 A.5를 참조하십시오.

익명 암호 그룹이 인증에 사용되지 않으므로 규칙에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

익명 암호 그룹은 TLS/SSL 규칙의 암호 그룹 조건에 추가할 수 있지만 시스템은 ClientHello 처리 중에 자동으로 익명 암호 그룹을 제거합니다. 시스템이 규칙을 사용하도록 하려면 ClientHello가 처리되지 않도록 하는 순서로 TLS/SSL 규칙을 구성해야 합니다. 자세한 내용은 SSL 규칙 순서, 1621 페이지를 참고하십시오.

TLS/SSL 노멀라이저 지침

인라인 표준화 전처리기에서 **Normalize Excess Payload(**초과 페이로드 표준화**)** 옵션을 활성화할 경우, 전처리기가 해독된 트래픽을 표준화할 때 패킷을 삭제하고 잘린 패킷으로 대체할 수 있습니다. 이로써 TLS/SSL 세션이 종료되지는 않습니다. 트래픽이 허용될 경우, 잘린 패킷이 TLS/SSL 세션의 일부로 암호화됩니다.

기타 TLS/SSL 규칙 지침

사용자 및 그룹

규칙에 사용자 또는 그룹을 추가한 다음 해당 그룹이나 사용자를 제외하도록 영역 설정을 변경하는 경우, 해당 규칙은 효과가 없습니다. (영역을 비활성화하는 경우에도 마찬가지입니다.) 영역에 대한 자세한 내용은 영역 생성, 2466 페이지를 참조하십시오.

TLS/SSL 규칙의 카테고리

SSL 정책에 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업이 있지만 웹사이트가 암호 해독되지 않는 경우, 해당 정책에 연결된 규칙에서 **Category(**범주**)** 페이지를 확인합니다.

경우에 따라 웹사이트는 인증 또는 기타 목적을 위해 다른 사이트로 리디렉션되며, 리디렉션된 사이트의 URL 카테고리 분류는 암호 해독하려는 사이트의 URL 카테고리 분류와 다를 수 있습니다. 예를 들어 `gmail.com`(웹 기반 이메일 카테고리)은 인증을 위해 `accounts.gmail.com`(인

터넷 포털 카테고리)으로 리디렉션됩니다. SSL 규칙에 모든 관련 카테고리가 포함되어야 합니다.

참고 URL 범주를 기반으로 트래픽을 완전히 처리하려면 URL 필터링도 구성해야 합니다. URL 필터링, 1665 페이지 장을 참조하십시오.

로컬 데이터베이스에 없는 **URL**에 대한 쿼리

Decrypt - Resign(암호 해독 - 다시 서명**)** 규칙을 생성하고 로컬 데이터베이스에 카테고리와 평판이 없는 웹사이트로 사용자가 이동하는 경우, 데이터가 해독되지 않을 수 있습니다. 일부 웹사이트는 로컬 데이터베이스에서 카테고리가 분류되어 있지 않으며, 이 경우 이러한 웹사이트의 데이터는 기본적으로 암호 해독되지 않습니다.

이 동작은 **System(**시스템**) > Integration(**통합**) > Cloud Services** 설정에서 **Query Cisco cloud for unknown URLs(Cisco Cloud**에서 알 수 없는 **URL** 쿼리**)**를 선택하여 제어할 수 있습니다.

이 옵션에 대한 자세한 내용은 Cisco Cloud, 3107 페이지를 참고하십시오.

TLS/SSL 규칙 요구 사항 및 사정 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

TLS/SSL 규칙 생성 및 수정

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**) > Access Control(**액세스 제어**) > SSL** 버튼을 클릭합니다.

단계 **3** SSL 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 다음 옵션을 이용할 수 있습니다.

- 새 규칙을 추가하려면 **Add Rule(**규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 수정( )을 클릭합니다.

단계 **5** 규칙의 **Name(**이름**)**을 입력합니다.

단계 **6** 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.

단계 **7** 규칙 위치를 지정합니다(TLS/SSL 규칙 순서 평가, 1777 페이지 참고).

단계 **8** 규칙 **Action(**작업**)**을 클릭합니다(TLS/SSL 규칙 동작 구성, 1820 페이지 참고).

단계 **9** 규칙 조건 및 옵션을 구성합니다.

a) **Zones(**영역**)**를 클릭하고 보안 영역에 따라 규칙 조건을 구성합니다(인터페이스 조건 참고).

b) **Networks(**네트워크**)**를 클릭하고 네트워크 또는 지리적 위치에 따라 규칙 조건을 구성합니다(네트워크 조건, 530 페이지 참고).

c) **VLAN** 태그를 클릭하고 VLAN에 따라 규칙 조건을 구성합니다(VLAN 조건, 531 페이지 참고).

d) **Users(**사용자**)**를 클릭하고 사용자 및 그룹에 따라 규칙 조건을 구성합니다(사용자, 영역 및 ISE 속성 조건(사용자 제어), 545 페이지 참고).

e) **Applications(**애플리케이션**)**를 클릭하고 애플리케이션에 따라 규칙 조건을 구성합니다(애플리케이션 조건(애플리케이션 컨트롤), 535 페이지 참고).

f) **Ports(**포트**)**를 클릭하고 통신 포트에 따라 규칙 조건을 구성합니다(포트 및 ICMP 코드 조건, 532 페이지 참고).

g) **Category(**범주**)**를 클릭하고 URL 평판에 따라 규칙 조건을 구성합니다. URL 필터링, 1665 페이지에 관한 장(HTTPS 트래픽 필터링, 1670 페이지 포함)을 참고하십시오.

h) **Certificate(**인증서**)**를 클릭하고 TLS/SSL 서버 인증서에 따라 규칙 조건을 구성합니다(서버 인증서 기반 TLS/SSL 규칙 조건, 1828 페이지 참고).

i) **DN**을 클릭하고 고유 이름을 기준으로 규칙 조건을 구성합니다(인증서 고유 이름 TLS/SSL 규칙 조건, 1829 페이지 참고).

j) **Cert Status(**인증 상태**)**를 클릭하고 TLS/SSL 인증서 상태에 따라 규칙 조건을 구성합니다(인증서 상태 TLS/SSL 규칙 조건, 1833 페이지 참고).

k) **Cipher Suite(**암호 그룹**)**을 클릭하고 암호 그룹에 따라 규칙 조건을 구성합니다(암호 그룹 TLS/SSL 규칙 조건, 1841 페이지 참고).

l) **Version(**버전**)**을 클릭하고 TLS 또는 SSL 프로토콜 버전에 따라 규칙 조건을 구성합니다(암호화 프로토콜 버전 TLS/SSL 규칙 조건, 1844 페이지 참고).

m) **Logging(**로깅**)**을 클릭하고 규칙의 로깅 옵션을 구성합니다(연결 로깅 모범 사례, 2868 페이지 참고).

단계 **10** **Save(**저장**)**를 클릭합니다.

다음과 같은 오류가 표시되면 TLS/SSL 암호 그룹 확인, 1856 페이지: **Traffic cannot match this rule; none of your selected cipher suites contain a signature algorithm that the resigning CA's signature algorithm**를 참조하십시오.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

규칙 카테고리에 **TLS/SSL** 규칙 추가

프로시저

단계 **1** SSL 규칙 편집기의 **Insert(**삽입**)** 드롭다운 목록에서 **Into Category(**카테고리에**)**를 선택한 후 사용할 카테고리를 선택합니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

팁 규칙을 저장하면 최종적으로 해당 카테고리에 위치합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

번호로 **TLS/SSL** 규칙 포지셔닝

프로시저

단계 **1** SSL 규칙 편집기의 **Insert(**삽입**)** 드롭다운 목록에서 **above rule(**규칙 위**)** 또는 **below rule(**규칙 아래**)**을 선택한 후 적절한 규칙 번호를 입력합니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

팁 규칙을 저장하면 지정한 위치에 배치됩니다.

다음에 수행할 작업

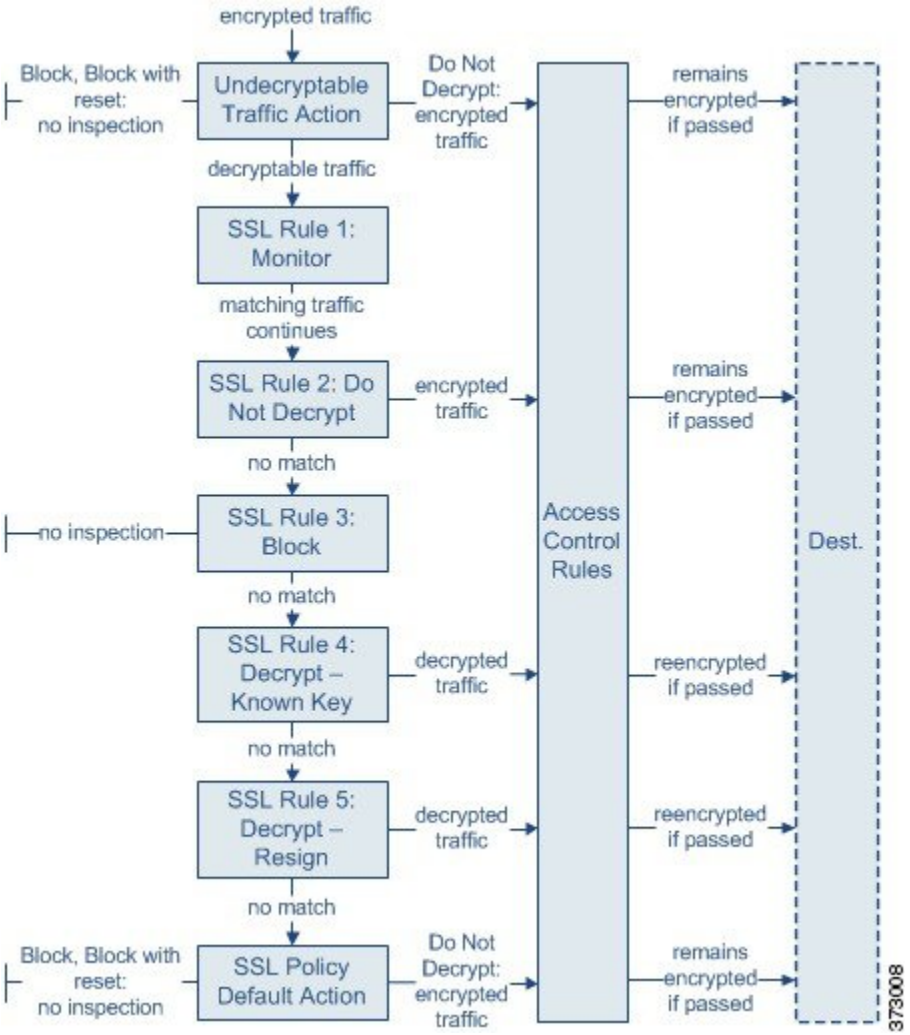
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

TLS/SSL 규칙 트래픽 처리

시스템은 사용자가 지정하는 순서대로 트래픽이 TLS/SSL 규칙과 일치하는지 확인합니다. 대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 TLS/SSL 규칙에 따라 암호화된 트래픽을 처리합니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 고유 이름(DN), 인증서 상태, 암호 그룹 또는 암호화 프로토콜 버전별로 트래픽을 제어할 수 있습니다.

각 규칙에는 작업이 있는데, 작업은 일치하는 암호화되거나 암호 해독된 트래픽을 액세스 제어로 모니터링, 차단 또는 검사할지 여부를 결정합니다. 시스템은 차단하는 암호화 트래픽을 추가 검사하지 않습니다. 암호화된 트래픽과 해독 불가 트래픽은 액세스 제어로 검사합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다.

다음 시나리오는 인라인 구축에서 SSL 규칙이 트래픽을 처리하는 방식을 요약한 것입니다.



이 시나리오에서, 트래픽은 다음과 같이 평가됩니다.

- **Undecryptable Traffic Action**은 암호화 트래픽을 먼저 평가합니다. 시스템에서 해독할 수 없는 트래픽은 추가 검사 없이 차단하거나 액세스 제어 검사를 위해 전달합니다. 매칭하지 않는 암호화 트래픽은 다음 규칙으로 진행합니다.
- **TLS/SSL** 규칙 **1: Monitor(**모니터링**)**가 다음으로 암호화 트래픽을 평가합니다. Monitor(모니터링) 규칙은 암호화 트래픽을 추적하고 로깅하지만 트래픽 플로우에 영향을 주지 않습니다. 시스템은 허용할지 아니면 거부할지 여부를 결정하기 위해 계속해서 트래픽을 추가 규칙에 일치시킵니다.
- **TLS/SSL** 규칙 **2: Do Not Decrypt(**암호 해독 안 함**)**가 세 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 암호 해독되지 않습니다. 시스템은 이 트래픽을 액세스 제어로 검사하지만 파일 또는 침입 검사는 하지 않습니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **TLS/SSL** 규칙 **3: Block(**차단**)**에서 네 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 차단됩니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **TLS/SSL** 규칙 **4: Decrypt - Known Key(**암호 해독 - 알려진 키**)**에서 다섯 번째로 암호화 트래픽을 평가합니다. 네트워크에 수신된 매칭 트래픽은 업로드된 개인 키를 사용하여 해독됩니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **TLS/SSL** 규칙 **5: Decrypt - Resign(**암호 해독 - 다시 서명**)**이 최종 규칙입니다. 트래픽이 이 규칙과 일치하면 시스템은 업로드된 CA 인증서로 서버 인증서를 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하여 트래픽 암호를 해독합니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **SSL Policy Default Action(SSL** 정책 기본 작업**)**은 어떤 TLS/SSL 규칙과도 일치하지 않는 모든 트래픽을 처리합니다. 이 기본 작업은 암호화 트래픽을 추가 검사 없이 차단하거나 해독하지 않고 액세스 제어 검사를 위해 전달합니다.

암호화된 트래픽 검사 설정

암호화 세션 특성을 기반으로 암호화 트래픽을 제어하고 암호화 트래픽을 해독하려면 재사용 가능한 PKI(Public Key Infrastructure) 개체를 생성해야 합니다. SSL 정책에 신뢰받는 CA(certificate authority) 인증서를 업로드하고 SSL 규칙 조건을 생성하는 시점에 이 정보를 추가하여 해당 개체를 생성할 수 있습니다. 그러나 이 개체를 미리 구성하면 잘못된 개체가 생성될 가능성이 줄어듭니다.

인증서 및 쌍 키를 사용하여 암호화 트래픽 해독

세션 암호화에 사용되는 서버 인증서와 개인 키를 업로드하여 내부 인증서 개체를 구성하면 들어오는 암호화된 트래픽을 암호 해독할 수 있습니다. **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업이

있는 SSL 규칙에서 해당 개체를 참조하고 트래픽이 해당 규칙과 일치하는 경우, 시스템은 업로드된 개인 키를 사용하여 세션의 암호를 해독합니다.

또한 CA 인증서와 개인 키를 업로드하여 내부 CA 개체를 구성하면 시스템이 나가는 트래픽도 암호 해독할 수 있습니다. **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업이 있는 SSL 규칙에서 해당 개체를 참조하고 트래픽이 해당 규칙과 일치하는 경우, 시스템은 클라이언트 브라우저로 전달된 서버 인증서에 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하여 트래픽 암호를 해독합니다.원하는 경우 전체 인증서가 아닌 SSC(자가 서명 인증서) 키만 교체할 수 있습니다. 이 경우 사용자의 브라우저에는 SSC(자가 서명 인증서) 키 알림이 표시됩니다.

암호화 세션 특성 기반의 트래픽 제어

시스템은 세션 협상에 사용된 암호 그룹 또는 서버 인증서를 기반으로 암호화 트래픽을 제어할 수 있습니다. 여러 재사용 가능 개체 중 하나를 구성하고 TLS/SSL 규칙 조건에서 해당 개체를 참조하여 트래픽의 일치 여부를 확인할 수 있습니다. 다음 표에서는 구성할 수 있는 재사용 가능 개체의 여러 유형에 대해 설명합니다.

다음을 구성할 경우	다음 조건을 기반으로 암호화 트래픽 제어 가능
하나 이상의 암호 그룹을 포함한 암호 그룹 목록	암호화 세션 협상에 사용되는 암호 그룹이 암호 그룹 목록에 있는 암호 그룹의 일치 여부를 확인합니다.
조직에서 신뢰하는 CA 인증서를 업로드하는 방법으로 신뢰할 수 있는 CA 개체 구성	다음 조건에서 신뢰할 수 있는 CA가 세션 암호화에 사용된 서버 인증서를 신뢰합니다. • CA가 직접 인증서를 발급한 경우 • CA가 중개 CA에 인증서를 발급했고, 이 중개 CA가 서버 인증서를 발급한 경우
서버 인증서를 업로드하는 방법으로 외부 인증서 개체 구성	세션 암호화에 사용된 서버 인증서가 업로드된 서버 인증서와 일치합니다
인증서 주체 또는 발급자 고유 이름(DN)을 포함하는 DN 개체	세션 암호화에 사용된 인증서의 주체 또는 발급자 공용 이름(CN), 국가, 조직 또는 조직 단위가 구성된 고유 이름(DN)과 일치합니다

관련 항목

암호 그룹 목록, 615 페이지
고유 이름 개체, 616 페이지
PKI 개체, 618 페이지

TLS/SSL 규칙 순서 평가

SSL 정책에서 TLS/SSL 규칙을 생성할 때는, 규칙 편집기에서 **Insert(**삽입**)** 목록을 이용해 순위를 지정해야 합니다. SSL 정책의 TLS/SSL 규칙에는 1부터 시작하는 숫자가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 TLS/SSL 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 TLS/SSL 규칙에 따라 네트워크 트래픽을 처리합니다. Monitor(모니터링) 규칙(트래픽을 로깅하지만 트래픽 흐름에 영향을 주지 않음)의 경우를 제외하고 트래픽이 규칙과 일치하면 시스템은 추가적이고 우선 순위가 낮은 규칙에 대해 계속해서 트래픽을 평가하지 않습니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 고유 이름(DN), 인증서 상태, 암호 그룹 또는 암호화 프로토콜 버전별로 트래픽을 제어할 수 있습니다.

각 규칙에는 작업이 있는데, 작업은 일치하는 암호화되거나 암호 해독된 트래픽을 액세스 제어로 모니터링, 차단 또는 검사할지 여부를 결정합니다. 시스템은 차단하는 암호화 트래픽을 추가 검사하지 않습니다. 암호화된 트래픽과 해독 불가 트래픽은 액세스 제어 대상입니다. 그러나 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적습니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

팁 TLS/SSL 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다. 사용자가 생성한 규칙이 모든 조직과 배포에 고유하더라도 사용자의 필요를 처리하는 동안 성능을 최적화할 수 있는 규칙을 언제 지시할지에 대해 몇 가지 따라야 할 지침이 있습니다.

번호로 규칙의 순서를 지정하는 것 외에도 카테고리로 규칙을 그룹화할 수 있습니다. 기본적으로 시스템에서는 Administrator(관리자), Standard(표준) 그리고 Root(루트)의 3가지 카테고리를 제공합니다. 맞춤형 카테고리를 추가할 수는 있지만 시스템에서 제공하는 카테고리를 삭제하거나 순서를 변경할 수는 없습니다.

관련 항목

암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지
SSL 규칙 순서, 1621 페이지
액세스 제어 규칙 순서에 대한 모범 사례, 1618 페이지

TLS/SSL 규칙 조건

SSL 규칙의 조건은 규칙에서 처리하는 암호화 트래픽의 유형을 식별합니다. 조건은 단순하거나 복잡할 수 있으며, 하나의 규칙에 둘 이상의 조건 유형을 지정할 수 있습니다. 트래픽이 규칙의 모든 조건을 충족해야 규칙이 트래픽에 적용됩니다.

규칙에 대해 특정 조건을 구성하지 않으면 시스템은 해당 기준에 따라 트래픽을 매칭하지 않습니다. 예를 들어 인증서 조건이 있지만 버전 조건이 없는 규칙은 세션 SSL 또는 TLS 버전과 무관하게 세션 협상에 쓰인 서버 인증서를 기반으로 트래픽을 평가합니다.

모든 TLS/SSL 규칙에는 일치하는 암호화 트래픽에 대해 다음을 결정하는 연결된 작업이 있습니다.

- 처리: 가장 중요한 것은 규칙의 조건과 일치하는 암호화된 트래픽을 시스템이 모니터링, 신뢰, 차단 또는 암호 해독할지 여부를 규칙 작업이 제어한다는 것입니다.
- 로깅: 이 규칙 작업은 일치하는 암호화 트래픽에 대한 상세정보를 언제 어떻게 로깅할 수 있는지 결정합니다.

TLS/SSL 검사 구성에서 해독된 트래픽을 처리, 검사, 로깅합니다.

- SSL 정책의 암호 해독 불가 작업은 시스템에서 암호 해독할 수 없는 트래픽을 처리합니다.
- 정책의 기본 작업은 Monitor(모니터링)가 아닌 TLS/SSL 규칙의 조건을 충족하지 않는 트래픽을 처리합니다.

시스템에서 암호화된 세션을 차단하거나 신뢰할 때 연결 이벤트를 로깅할 수 있습니다. 또한 시스템이 나중에 트래픽을 처리하거나 검사하는 방법과 관계없이 액세스 제어 규칙을 통한 추가 평가를 위해 시스템이 해독하는 연결을 반드시 로깅하도록 설정할 수도 있습니다. 암호화 세션의 연결 로그는 세션 암호화에 사용된 인증서와 같은 해독 세부 사항이 포함되어 있습니다. 연결 종료 이벤트만 로깅할 수 있지만 다음 예외가 적용됩니다.

- 차단된 연결(Block(차단), Block with reset(차단 후 재설정))의 경우, 시스템이 즉시 세션을 종료하고 이벤트를 생성합니다.
- Do not decrypt(암호 해독 안 함)로 지정된 신뢰할 수 있는 연결의 경우, 시스템이 세션 종료 시 이벤트를 생성합니다.

TLS/SSL 규칙 조건 유형

SSL 규칙을 추가하거나 수정할 때 규칙 편집기의 왼쪽 아래에 있는 탭을 사용하여 규칙 조건을 추가하고 수정합니다.

표 ***108: TLS/SSL*** 규칙 조건 유형

조건	암호화 트래픽 매칭	세부 사항
영역	특정 보안 영역의 인터페이스를 통해 디바이스에 들어오거나 디바이스에서 나감	보안 영역은 배포 및 보안 정책에 따라 하나 이상의 인터페이스를 논리적으로 그룹화한 것입니다. 한 영역의 인터페이스는 여러 디바이스에 위치할 수 있습니다.
네트워크	해당 소스 또는 대상 IP 주소, 국가 또는 대륙	명시적으로 IP 주소를 지정할 수 있습니다. 지리위치 기능을 사용하여 해당 소스 또는 대상 국가나 대륙에 근거하여 트래픽을 제어할 수도 있습니다.
VLAN 태그	VLAN별로 태그됨	시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다.

조건	암호화 트래픽 매칭	세부 사항
포트	해당 소스 또는 대상 포트	TCP 포트를 기반으로 암호화 트래픽을 제어할 수 있습니다.
사용자	세션에 개입된 사용자별	모니터링되는 암호화 세션에 쓰인 호스트에 로그인한 LDAP 사용자를 기반으로 암호화 트래픽을 제어할 수 있습니다. Microsoft Active Directory 서버에서 검색된 개별 사용자 또는 그룹을 기준으로 트래픽을 제어할 수 있습니다.
애플리케이션	세션에서 탐지되는 애플리케이션별	암호화 세션에서 개별 애플리케이션에 대한 액세스를 제어하거나 유형, 위험, 비즈니스 연관성, 범주와 같은 기본 특성에 따라 액세스를 필터링할 수 있습니다.
범주	인증서 주체 DN을 기반으로 하여 세션에서 요청된 URL을 기준으로 매칭	URL의 일반 분류 및 위험 레벨을 기반으로 네트워크 사용자가 액세스 가능한 웹사이트를 제한할 수 있습니다.
고유 이름(DN)	사용자가 브라우저에 입력하는 URL이 CN(Common Name)과 일치하거나, URL이 인증서의 SAN(Subject Alternative Name)에 포함되어 있습니다.	서버 인증서를 발급한 CA 또는 서버 인증서 소유자를 기반으로 암호화 트래픽을 제어할 수 있습니다.
인증서	암호화 세션의 협상에 쓰이는 서버 인증서를 기준으로 매칭	암호화 세션의 협상을 위해 사용자의 브라우저에 전달된 서버 인증서를 기반으로 암호화 트래픽을 제어할 수 있습니다.
인증서 상태	암호화 세션의 협상에 쓰이는 서버 인증서의 속성을 기준으로 매칭	서버 인증서의 상태를 기반으로 암호화 트래픽을 제어할 수 있습니다.
암호 그룹	암호화 세션의 협상에 쓰이는 암호 그룹을 기준으로 매칭	서버에서 암호화 세션의 협상을 위해 선택한 암호 그룹을 기반으로 암호화 트래픽을 제어할 수 있습니다.
버전	세션 암호화에 쓰이는 SSL 또는 TLS 버전을 기준으로 매칭	세션 암호화에 쓰이는 SSL 또는 TLS 버전을 기반으로 암호화 트래픽을 제어할 수 있습니다.

관련 항목

네트워크 기반 TLS/SSL 규칙 조건
사용자 기반 TLS/SSL 규칙 조건
암호화된 트래픽의 평판 기반 URL 차단
서버 인증서 기반 TLS/SSL 규칙 조건, 1828 페이지

TLS/SSL 규칙 작업

다음 섹션에서는 TLS/SSL 규칙과 함께 사용할 수 있는 작업을 설명합니다.

TLS/SSL 규칙 모니터링 작업

Monitor(모니터링**)** 작업은 트래픽을 허용하거나 거부하도록 설계되지 않았습니다. 이 작업의 기본 목적은 일치하는 트래픽의 처리 방식에 상관없이 연결 로깅을 강제하는 것입니다. 그런 다음 추가 규칙이 있다면 매칭하여 트래픽을 신뢰, 차단, 해독할지 여부를 결정합니다. 일치하는 첫 번째 비 Monitor(모니터링) 규칙은 트래픽 흐름과 추가 검사를 결정합니다. 추가로 일치하는 규칙이 없는 경우, 시스템은 기본 작업을 사용합니다.

Monitor(모니터링) 규칙의 주요 목표는 네트워크 트래픽을 추적하는 것이므로 시스템은 규칙의 로깅 구성이나 나중에 연결을 처리하는 기본 작업에 관계없이 모니터링되는 트래픽의 연결 종료 이벤트를 Firepower Management Center 데이터베이스에 자동으로 로깅합니다.

TLS/SSL 규칙 Do Not Decrypt(암호 해독 안 함) 작업

Do Not Decrypt(암호 해독 안 함**)** 작업은 액세스 제어 정책의 규칙 및 기본 작업을 통한 평가를 위해 암호화 트래픽을 전달합니다. 일부 액세스 제어 규칙 조건은 암호화되지 않은 트래픽을 요구하므로 이 트래픽이 더 적은 수의 규칙과 매칭할 수도 있습니다. 시스템은 암호화된 트래픽에 대해 침입 또는 파일 검사와 같은 심층 검사를 수행할 수 없습니다.

Do Not Decrypt(암호 해독 안 함**)** 규칙 작업의 일반적인 이유는 다음과 같습니다.

- TLS/SSL 트래픽 암호 해독이 법률로 금지되는 경우.
- 신뢰할 수 있는 사이트.
- 트래픽을 검사하면 지장을 줄 수 있는 사이트(예: Windows 업데이트).
- 연결 이벤트를 사용하여 TLS/SSL 연결 이벤트의 값을 보기 위해. (연결 이벤트 필드를 보기 위해 트래픽을 해독할 필요가 없습니다.) 자세한 내용은 연결 이벤트 필드 채우기 요구 사항, 2895 페이지를 참고하십시오.

자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 1795 페이지을 참조해 주십시오.

TLS/SSL 규칙 차단 작업

Firepower System은 시스템을 통과해선 안 되는 트래픽에 대한 다음 TLS/SSL 규칙 작업을 제공합니다.

- **Block(**차단**)**을 이용해 연결을 종료하면 클라이언트 브라우저에 오류가 발생합니다.

  오류 메시지는 사이트가 정책으로 인해 차단되었음을 나타내지 않습니다. 대신 일반적인 암호화 알고리즘이 없다는 오류가 표시될 수 있습니다. 이 메시지만으로는 연결이 의도적으로 차단되었는지를 명확하게 파악할 수 없습니다.

- **Block with reset(**차단 후 재설정**)**을 이용해 연결을 종료하고 재설정하면, 클라이언트 브라우저에 오류가 발생합니다.

  이 오류는 연결이 재설정되었음을 표시하지만 이유는 표시하지 않습니다.

팁 패시브 또는 인라인(탭 모드) 구축에서는 디바이스에서 직접 트래픽을 검사하지 않으므로 **Block(**차단**)** 또는 **Block with reset(**차단 후 재설정**)** 작업을 사용할 수 없습니다. **Block(**차단**)** 또는 **Block with reset(**차단 후 재설정**)** 작업의 규칙을 생성할 경우 여기에 보안 영역 조건의 패시브 또는 인라인(탭 모드) 인터페이스가 포함된다면 정책 편집기는 해당 규칙의 옆에 경고(⚠)를 표시합니다.

TLS/SSL 규칙 암호 해독 작업

Decrypt - Known Key(암호 해독 - 알려진 키**)** 및 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업은 암호화된 트래픽을 암호 해독합니다. 시스템에서는 액세스 제어를 통해 암호 해독된 트래픽을 검사합니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 검색 데이터를 위해 트래픽을 조사하고 침입, 금지된 파일, 악성코드를 탐지하여 차단할 수 있습니다. 허용된 트래픽은 다시 암호화되어 목적지에 전달됩니다.

신뢰할 수 있는 CA(Certification Authority)의 인증서를 사용하여 트래픽의 암호를 해독하는 것이 좋습니다. 이렇게 하면 연결 이벤트의 SSL Certificate Status(SSL 인증서 상태) 열에 **Invalid Issuer**가 표시되지 않습니다.

신뢰할 수 있는 개체를 추가하는 방법에 대한 자세한 내용은 신뢰할 수 있는 인증 기관 개체, 624 페이지를 참조하십시오.

TLS/SSL 규칙 동작 구성

시작하기 전에

참조:

- TLS/SSL 규칙 차단 작업, 1819 페이지
- TLS/SSL 규칙 Do Not Decrypt(암호 해독 안 함) 작업, 1819 페이지
- TLS/SSL 규칙 모니터링 작업, 1819 페이지

프로시저

단계 **1** SSL 정책 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하려면 **Add Rule(**규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 수정( )을 클릭합니다.

단계 **2** **Action(**작업**)** 드롭다운 목록에서 규칙 작업을 선택합니다.

- 암호화된 트래픽을 차단하려면 **Block(**차단**)**을 선택합니다.
- 암호화된 트래픽을 차단하고 연결을 재설정하려면 **Block with reset(**차단 후 재설정**)**을 선택합니다.
- 수신 트래픽을 해독하려면 암호 해독 설정 - 알려진 키 작업, 1822 페이지의 자세한 내용을 참조하십시오.
- 발신 트래픽을 해독하려면 암호 해독 설정 - 재서명 작업, 1821 페이지를 참조하십시오.
- 암호화된 트래픽을 로깅하려면 **Monitor(**모니터링**)**를 선택합니다.
- 암호화된 트래픽을 해독하지 않으려면 **Do not decrypt(**암호 해독 안 함**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

- 규칙 소개, 524 페이지에 설명된 대로 규칙 조건을 구성합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

암호 해독 설정 - 재서명 작업

시작하기 전에

TLS/SSL 암호 해독 - 파기 지침, 1806 페이지의 내용을 참조하십시오.

프로시저

단계 **1** SSL 규칙 편집기의 **Action(**작업**)** 목록에서 **Decrypt - Resign(**암호 해독 - 다시 서명**)**을 선택합니다.

단계 **2** 목록에서 내부 CA 인증서 개체를 선택합니다.

단계 **3** **Replace Key(**키 바꾸기**) Replace Key Only(**키만 바꾸기**)** 를 선택합니다.

암호 해독 - 재서명 규칙 작업을 설정할 때는 키 교환 키만 바꾸기 확인란을 항상 확인해야 합니다.

사용자가 직접 서명 인증서를 사용하는 웹사이트를 탐색하면, 웹 브라우저에서 보안 경고가 표시되며 안전하지 않은 사이트와 통신 중이라고 경고합니다.

사용자가 신뢰할 수 있는 인증서를 사용하는 웹사이트를 탐색할 때는 보안 경고가 표시되지 않습니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** 선택 사항. SSL 정책에서 신뢰할 수 있는 CA 인증서를 사용하여 연결 이벤트의 SSL Certificate Status(SSL 인증서 상태) 열에서 **Invalid Issuer**를 방지하려면 정책에 인증서를 추가합니다.

a) SSL 정책 편집기 페이지에서 **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)**를 클릭합니다.

b) 알려진 키에 해당하는 CA 인증서를 SSL 정책에 추가합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

암호 해독 설정 - 알려진 키 작업

시작하기 전에

TLS/SSL 암호 해독 - 알려진 키 지침, 1807 페이지의 내용을 참조하십시오.

프로시저

단계 **1** SSL 규칙 편집기의 **Action(**작업**)** 목록에서 **Decrypt - Known Key(**암호 해독 - 알려진 키**)**를 선택합니다.

단계 **2** **Click to select decryption certs** 필드를 클릭합니다.

단계 **3** **Available Certificates(**사용 가능한 인증서**)** 목록에서 하나 이상의 내부 인증서 개체를 클릭한 다음 **Add to Rule(**규칙에 추가**)**을 클릭합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** 선택 사항. SSL 정책에서 신뢰할 수 있는 CA 인증서를 사용하여 연결 이벤트의 SSL Certificate Status(SSL 인증서 상태) 열에서 **Invalid Issuer**를 방지하려면 정책에 인증서를 추가합니다.

a) SSL 정책 편집기 페이지에서 **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)**를 클릭합니다.

b) 알려진 키에 해당하는 CA 인증서를 SSL 정책에 추가합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

TLS/SSL 관리 규칙

SSL 정책 편집기의 **Rules(**규칙**)**를 사용하여 정책에서 TLS/SSL 규칙을 추가, 편집, 이동, 활성화, 비활성화, 삭제하고 기타 방식으로 관리할 수 있습니다.

TLS/SSL 규칙 검색

공백과 인쇄 가능 특수 문자가 포함된 영숫자 문자열을 사용하여 TLS/SSL 규칙의 목록에서 일치하는 값을 찾을 수 있습니다. 검색은 규칙에 추가한 규칙 조건 및 규칙 이름을 검사합니다. 규칙 조건을

위해 검색은 각 조건 유형(영역, 네트워크, 애플리케이션, 등)에 추가할 수 있는 모든 이름 또는 값에 일치합니다. 여기에는 개별 개체 이름 또는 값, 그룹 개체 이름, 그룹 내 개별 개체 이름 또는 값, 그리고 문자 값이 포함됩니다.

완전한 또는 부분 검색 문자열을 사용할 수 있습니다. 일치 값을 위한 열은 각 일치하는 규칙에 강조 표시됩니다. 예를 들어, 스트링 `100Bao`의 전체 또는 일부를 최소한도로 검색하는 경우, 애플리케이션 열은 100Bao 애플리케이션을 추가한 각 규칙에 강조 표시됩니다. `100Bao`라는 이름의 규칙도 있다면 Name 및 Applications 열 모두 하이라이트됩니다.

이전에 일치하는 규칙 또는 다음에 일치하는 규칙 각각으로 이동할 수 있습니다. 상태 메시지는 현재 일치하는 규칙과 일치하는 총 수를 나타냅니다.

일치는 여러 페이지로 구성된 규칙 목록의 어느 페이지에서나 발생할 수 있습니다. 첫 번째 일치가 첫 번째 페이지에 없는 경우, 첫 번째 일치가 발생한 페이지가 표시됩니다. 마지막 일치 중일 때 다음 일치를 선택하면 첫 번째 일치로 이동하며, 첫 번째 일치 중일 때 이전 일치를 선택하면 마지막 일치로 이동합니다.

TLS/SSL 규칙 검색

프로시저

단계 **1** SSL 정책 편집기에서 **Search Rules(**검색 규칙**)** 프롬프트를 클릭하고 검색 문자열을 입력한 다음 Enter를 누릅니다.

팁 일치하는 값을 가진 규칙의 열이 강조 표시되며, 이는 명시된 (첫 번째) 일치를 위한 강조 표시와는 차별화됩니다.

단계 **2** 관심이 가는 규칙을 찾으십시오.

- 일치하는 규칙을 탐색하려면 **Next-Match(**다음 일치**)** 또는 **Previous-Match(**이전 일치**)**를 클릭합니다.
- 페이지를 새로 고침하고 검색 문자열 및 강조 표시를 지우려면, 지우기(✕)을 클릭합니다.

TLS/SSL 규칙 활성화 및 비활성화

TLS/SSL 규칙을 생성하면 기본적으로 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다. SSL 정책에서 규칙의 목록을 볼 때 비활성화된 규칙은 회색으로 표시됩니다. 단, 이 규칙은 수정 가능합니다. 규칙 편집기를 사용하여 TLS/SSL 규칙을 활성화하거나 비활성화할 수도 있습니다.

프로시저

단계 1 SSL 정책 편집기에서 규칙을 마우스 오른쪽 버튼으로 클릭하고 규칙 상태를 선택합니다.

단계 2 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

TLS/SSL 규칙 이동

프로시저

단계 1 SSL 정책 편집기에서 각 규칙의 빈 영역을 클릭하여 규칙을 선택합니다.

단계 2 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Cut(**잘라내기**)**을 선택합니다.

단계 3 잘라낸 규칙을 붙여넣을 위치 옆에 있는 규칙의 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Paste above(**위 붙여넣기**)** 또는 **Paste below(**아래 붙여넣기**)**를 선택합니다.

팁 TLS/SSL 규칙을 복사하여 다른 SSL 정책에 붙여넣을 수는 없습니다.

단계 4 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

새새 TLS/SSL 규칙 카테고리 추가

추가 정책을 생성하지 않고 Standard Rules(표준 규칙) 카테고리와 Root Ruels(루트 규칙) 카테고리 사이에 맞춤형 카테고리를 생성하여 규칙을 추가 구성할 수 있습니다. 추가한 카테고리의 이름을 변경하고 삭제할 수 있습니다. 이 카테고리를 이동할 수는 없지만 이 카테고리 안으로, 이 카테고리 안에서, 이 카테고리 밖으로 규칙을 이동할 수는 있습니다.

프로시저

단계 1 정책 편집기에서 **Add Category(**카테고리 추가**)**를 클릭합니다.

팁 정책에 이미 규칙이 포함된 경우, 새로운 규칙을 추가하기 전에 기존 규칙에 대한 행의 빈 영역을 클릭하여 새로운 카테고리의 위치를 지정합니다. 기존 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Insert new category(**새 카테고리 삽입**)**를 선택할 수도 있습니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 첫 번째 **Insert(**삽입**)** 드롭다운 목록에서 **above Category(**카테고리 위**)**를 선택한 후 두 번째 드롭다운 목록에서 규칙을 배치할 위치 아래의 카테고리를 선택합니다.
- 드롭다운 목록에서 **below rule(**규칙 아래**)**을 선택한 다음, 기존 규칙 번호를 입력합니다. 이 옵션은 최소 하나의 규칙이 정책에 존재할 경우에만 유효합니다.
- 드롭다운 목록에서 **above rule(**규칙 위**)**을 선택한 다음 기존 규칙 번호를 입력합니다. 이 옵션은 최소 하나의 규칙이 정책에 존재할 경우에만 유효합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

팁 삭제한 카테고리의 규칙은 상위 카테고리에 추가됩니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

72 장

TLS/SSL 규칙을 사용한 암호 해독 조정

다음 주제에서는 TLS/SSL 조건 규칙을 구성하는 방법의 개요를 설명합니다.

- TLS/SSL 규칙 조건 개요, 1827 페이지
- 암호 해독 조정 요구 사항 및 사전 요건, 1828 페이지
- 서버 인증서 기반 TLS/SSL 규칙 조건, 1828 페이지

TLS/SSL 규칙 조건 개요

기본적인 TLS/SSL 규칙은 디바이스에서 검사하는 모든 암호화된 트래픽에 해당 규칙 작업을 적용합니다. 암호화된 트래픽의 제어 및 해독을 개선하기 위해, 특정 유형의 트래픽을 처리하고 로깅하도록 규칙 조건을 구성할 수 있습니다. 각 TLS/SSL 규칙에는 0개, 1개 또는 그 이상의 규칙 조건이 포함될 수 있습니다. 트래픽이 해당 TLS/SSL 규칙의 모든 조건과 일치하는 경우에만 규칙이 트래픽과 일치합니다.

참고 트래픽이 규칙과 일치하면 디바이스는 구성된 규칙 작업을 트래픽에 적용합니다. 트래픽 로깅이 구성되어 있는 경우, 연결이 종료될 때 디바이스는 트래픽을 로깅합니다.

각 규칙 조건을 사용하면 매칭하려는 트래픽의 속성을 하나 이상 지정할 수 있으며, 이러한 속성에는 다음에 대한 세부 정보가 포함됩니다.

- 트래픽이 이동할 때 통과하는 보안 영역, IP 주소 및 포트, 원본 또는 대상 국가, 원본 또는 대상 VLAN을 포함한 트래픽의 흐름.
- 탐지된 IP 주소에 연결된 사용자.
- 트래픽에서 탐지된 애플리케이션을 포함한 트래픽 페이로드.
- 연결을 암호화하는 데 사용되는 TLS/SSL 프로토콜 버전, 암호 그룹, 서버 인증서를 포함한 연결 암호화.
- 서버 인증서의 고유 이름(DN)에 지정된 URL의 카테고리 및 평판.

관련 항목

네트워크 조건, 530 페이지
VLAN 조건, 531 페이지
사용자, 영역 및 ISE 속성 조건(사용자 제어), 545 페이지
애플리케이션 조건(애플리케이션 컨트롤), 535 페이지
포트 및 ICMP 코드 조건, 532 페이지
HTTPS 트래픽 필터링, 1670 페이지
서버 인증서 기반 TLS/SSL 규칙 조건, 1828 페이지
인증서 고유 이름 TLS/SSL 규칙 조건, 1829 페이지
인증서 상태 TLS/SSL 규칙 조건, 1833 페이지
암호 그룹 TLS/SSL 규칙 조건, 1841 페이지
암호화 프로토콜 버전 TLS/SSL 규칙 조건, 1844 페이지

암호 해독 조정 요구 사항 및 사전 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

서버 인증서 기반 **TLS/SSL** 규칙 조건

TLS/SSL 규칙은 서버 인증서 특성을 기반으로 암호화된 트래픽을 처리하고 해독할 수 있습니다. 다음 서버 인증서 속성을 기반으로 TLS/SSL 규칙을 구성할 수 있습니다.

- 고유 이름(DN) 조건을 사용하면 서버 인증서를 발급한 CA 또는 인증서 보유자를 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다. 발급자 DN에 따라, 사이트의 서버 인증서를 발급한 CA를 기준으로 트래픽을 처리할 수 있습니다.
- TLS/SSL 규칙의 인증서 조건을 사용하면 트래픽을 암호화하는 데 사용된 서버 인증서를 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다. 하나 이상의 인증서로 규칙을 구성할 수 있습니다. 인증서가 조건의 모든 인증서와 매칭될 경우, 트래픽은 규칙과 매칭됩니다.

- TLS/SSL 규칙의 인증서 상태 조건을 사용하면 트래픽을 암호화하는 데 사용된 서버 인증서의 상태를 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다. 상태에는 인증서가 유효한지, 취소되었는지, 만료되었는지, 아직 유효하지 않은지, 자체 서명되었는지, 신뢰할 수 있는 CA가 서명했는지 여부, CRL(인증서 해지 목록)이 유효한지 여부, 인증서의 SNI(서버 이름 표시)가 요청의 서버와 일치하는지 여부가 포함됩니다.
- TLS/SSL 규칙의 암호 그룹 조건을 사용하면 암호화된 세션을 협상하는 데 사용된 암호 그룹을 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다.
- TLS/SSL 규칙의 세션 조건을 사용하면 트래픽을 암호화하는 데 사용된 SSL 또는 TLS 버전을 기준으로 암호화된 트래픽을 검사할 수 있습니다.

규칙의 여러 암호 그룹, 인증서 발급자 또는 인증서 보유자를 탐지하려는 경우, 재사용 가능한 암호 그룹 및 고유 이름(DN) 개체를 생성하고 이를 규칙에 추가할 수 있습니다. 서버 인증서 및 특정 인증서 상태를 탐지하려면 해당 규칙에 대한 외부 인증서 및 외부 CA 개체를 생성해야 합니다.

인증서 고유 이름 **TLS/SSL** 규칙 조건

규칙 조건을 구성할 경우 리터럴 값을 수동으로 지정하고, 고유 이름(DN) 개체를 참조하거나 여러 개체가 포함된 고유 이름 그룹을 참조할 수 있습니다.

참고 **Decrypt - Known Key(**암호 해독 **-** 알려진 키**)** 작업도 선택할 경우 고유 이름(DN) 조건을 구성할 수 없습니다. 이 작업은 서버 인증서 선택을 통한 트래픽 해독이 필요하므로 인증서가 트래픽과 이미 일치합니다.

단일한 인증서 상태 규칙 조건의 여러 주체 및 발급자 DN을 대상으로 매칭할 수 있습니다. 규칙과 매칭하려면 하나의 공용 이름 또는 고유 이름(DN)만 매칭해야 합니다.

고유 이름(DN)을 수동으로 추가할 경우, 공용 이름 특성(**CN**)을 포함할 수 있습니다. `CN=` 없이 공용 이름(CN)을 추가하면 개체를 저장하기 전에 시스템이 `CN=`을 앞에 추가합니다.

다음 속성(**C, CN, O, OU**) 중 하나가 있는 고유 이름을 쉼표로 구분하여 추가할 수도 있습니다.

단일한 DN 조건에서 최대 50개의 리터럴 값 및 고유 이름(DN) 개체를 **Subject DNs(**주체 **DN)**에 추가하고, 50개의 리터럴 값 및 고유 이름(DN) 개체를 **Issuer DNs(**발급자 **DN)**에 추가할 수 있습니다.

시스템에서 제공된 DN 개체 그룹인 Cisco-Undecryptable-Sites에는 시스템이 해독할 수 없는 트래픽이 있는 웹사이트가 포함됩니다. 이 그룹을 DN 조건에 추가하면, 이러한 웹사이트에서 나가고 들어오는 트래픽을 차단하거나 해독하지 않도록 할 수 있으므로, 트래픽 해독을 시도하느라 시스템 리소스를 낭비하지 않아도 됩니다. 이 그룹의 개별 항목을 수정할 수 있습니다. 단, 이 그룹은 삭제할 수 없습니다. 시스템 업데이트로 인해 이 목록의 항목이 수정될 수 있지만 사용자 변경 사항은 그대로 유지됩니다.

암호화된 트래픽을 인증서 고유 이름**(DN)**으로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 DN을 선택합니다.

단계 **2** **Available DNs(**사용 가능한 **DN)**에서 추가할 고유 이름을 다음과 같이 찾습니다.

- 고유 이름(DN) 개체를 즉시 추가한 다음 조건에 추가하려면 **Available DNs(**사용 가능한 **DN)** 목록 위의 추가( )을 클릭합니다.
- 추가할 고유 이름(DN) 개체 및 그룹을 검색하려면, **Available DNs(**사용 가능한 **DN)** 목록 위의 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 다음 개체의 이름을 입력하거나, 개체의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 개체를 표시합니다.

단계 **3** 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Subject(**주체에 추가**)** 또는 **Add to Issuer(**발급자에 추가**)**를 클릭합니다.

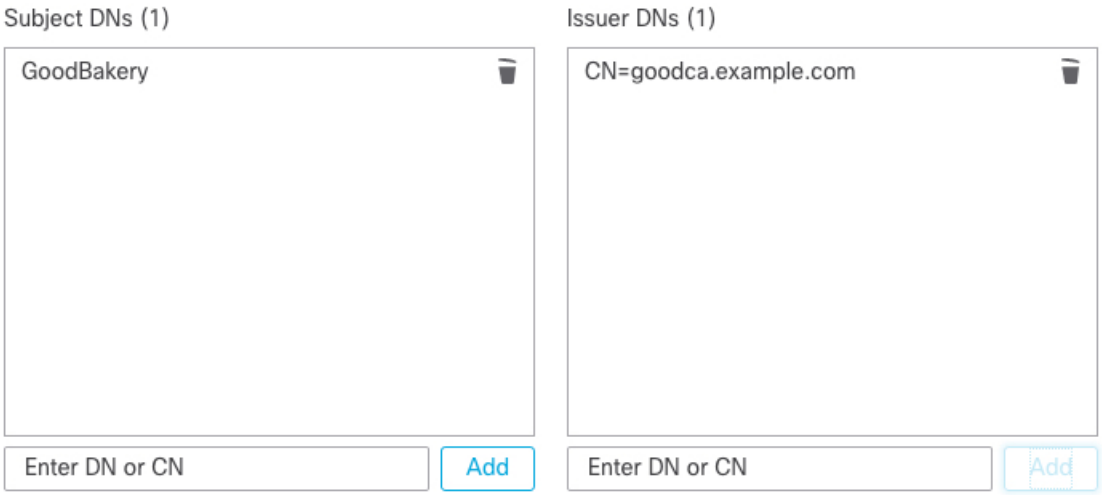
팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 **5** 수동으로 지정할 리터럴 공용 이름(CN) 또는 고유 이름(DN)을 추가합니다. **Subject DNs(**주체 **DN)** 또는 **Issuer DNs(**발급자 **DN)** 목록 아래의 **Enter DN or CN(DN** 또는 **CN** 입력**)** 프롬프트를 클릭한 다음, 공용 이름(CN) 또는 고유 이름(DN)을 입력하고 **Add(**추가**)**를 클릭합니다.

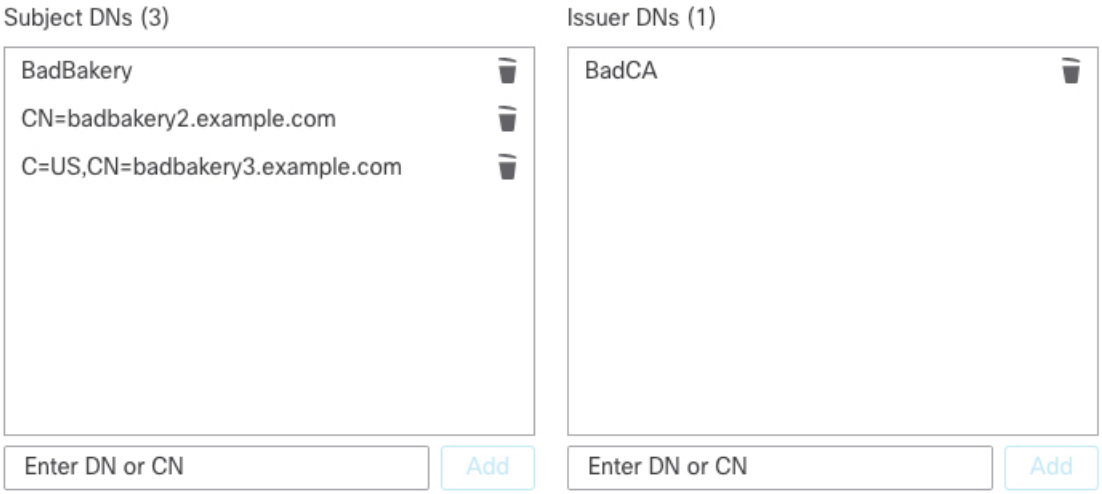
단계 **6** 규칙을 추가하거나 계속 수정합니다.

예

다음 그림에는 goodbakery.example.com에 발급되었거나 goodca.example.com에서 발급한 인증서를 검색하는 고유 이름(DN) 규칙이 나와 있습니다. 이러한 인증서로 암호화된 트래픽은 허용되며 액세스 제어 규칙의 대상이 됩니다.



다음 그림에는 badbakery.example.com에 발급된 인증서 및 연결된 도메인, 또는 badca.example.com에서 발급한 인증서를 검색하는 고유 이름(DN) 규칙 조건이 나와 있습니다. 이러한 인증서로 암호화된 트래픽은 다시 서명된 인증서를 사용하여 암호 해독됩니다.



다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

고유 이름 개체, 616 페이지

인증서 **TLS/SSL** 규칙 조건

인증서 기반 TLS/SSL 규칙 조건을 만들 경우, 서버 인증서를 업로드할 수 있습니다. 인증서를 재사용 가능한 외부 인증서 개체로 저장하고, 이름을 서버 인증서와 연결할 수 있습니다. 또는 기존 외부 인증서 개체 및 개체 그룹으로 인증서 조건을 구성할 수 있습니다.

다음과 같은 인증서 고유 이름(DN) 특성을 기준으로, 외부 인증서 개체 및 개체 그룹에 따라 규칙 조건의 **Available Certificates(**사용 가능한 인증서**)** 필드를 검색할 수 있습니다.

- 주체 또는 발급자 공용 이름(CN)
- 주체 또는 발급자 조직(O)
- 주체 또는 발급자 부서(OU)

단일한 인증서 규칙 조건의 여러 인증서와 매칭되도록 선택할 수 있습니다. 업로드된 인증서와 매칭되는 트래픽을 암호화하는 데 인증서가 사용된 경우, 암호화된 트래픽은 규칙과 매칭됩니다.

단일한 인증서 조건에서 최대 50개의 외부 인증서 개체 및 외부 인증서 개체 그룹을 **Selected Certificates(**선택한 인증서**)**에 추가할 수 있습니다.

다음 사항을 참고하십시오.

- **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업도 선택할 경우 인증서 조건을 구성할 수 없습니다. 이 작업은 서버 인증서를 선택하여 트래픽을 해독해야 하므로, 이렇게 할 경우 인증서가 트래픽과 이미 매칭됩니다.
- 외부 인증서 개체가 포함된 인증서 조건을 구성할 경우, 암호 그룹 조건에 추가하는 모든 암호 그룹 또는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업에 연결되는 내부 CA 개체는 외부 인증서의 시그니처 알고리즘 유형과 매칭되어야 합니다. 예를 들어 규칙의 인증서 조건이 EC 기반 서버 인증서를 참조할 경우, 추가되는 모든 암호 그룹 또는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업과 연결되는 CA 인증서도 EC 기반이어야 합니다. 이때 시그니처 알고리즘 유형이 매칭되지 않을 경우, 정책 편집기에서는 규칙 옆에 경고가 표시됩니다.

암호화된 트래픽을 인증서로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 Certificate(인증서)를 선택합니다.

단계 **2** **Available Certificates(**사용 가능한 인증서**)**에서 추가할 서버 인증서를 다음과 같이 찾습니다.

- 조건에 추가할 수 있는 외부 인증서 개체를 즉시 추가하려면 **Available Certificates(**사용 가능한 인증서**)** 목록 위의 추가(+)를 클릭합니다.
- 추가할 인증서 개체 및 그룹을 검색하려면, **Available Certificates(**사용 가능한 인증서**)** 목록 위의 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 다음 개체의 이름을 입력하거나, 개체의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 개체를 표시합니다.

단계 **3** 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 **5** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

외부 인증서 개체, 626 페이지

인증서 상태 **TLS/SSL** 규칙 조건

구성하는 각 인증서 상태 TLS/SSL 규칙 조건의 경우, 지정된 상태가 있는 경우 또는 없는 경우에 대해 트래픽을 매칭할 수 있습니다. 하나의 규칙 조건에서 여러 개의 상태를 선택할 수 있습니다. 인증서가 선택한 상태와 매칭되는 경우, 규칙은 트래픽과 매칭됩니다.

단일한 인증서 상태 규칙 조건에 여러 인증서 상태가 있는 경우 또는 없는 경우와 매칭하도록 선택할 수 있습니다. 인증서는 규칙과 매칭하는 조건 중 하나에만 매칭되어야 합니다.

이 매개변수를 설정할 때는 암호 해독 규칙을 구성하는지 차단 규칙을 구성하는지를 고려해야 합니다. 일반적으로 차단 규칙의 경우에는 **Yes(**예**)**를, 암호 해독 규칙의 경우에는 **No(**아니요**)**를 클릭해야 합니다. 예:

- **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙을 구성하는 경우, 기본 동작은 만료된 인증서가 있는 트래픽을 해독하는 것입니다. 이 동작을 변경하려면 만료된 인증서가 있는 트래픽이 해독 및 재서명되지 않도록 **Expired(**만료됨**)**에 대해 **No(**아니요**)**를 클릭하십시오.
- **Block(**차단**)** 규칙을 구성하는 경우, 기본 동작은 만료된 인증서가 있는 트래픽을 허용하는 것입니다. 이 동작을 변경하려면 만료된 인증서가 있는 트래픽이 차단되도록 **Expired(**만료됨**)**에 대해 **Yes(**예**)**를 클릭하십시오.

다음 표에는 암호화 서버 인증서 상태를 기준으로 암호화된 트래픽을 시스템이 평가하는 방법이 설명되어 있습니다.

표 ***109:*** 인증서 상태 규칙 조건 기준

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
취소	정책이 서버 인증서를 발급한 CA를 신뢰하며, 정책에 업로드된 CA 인증서에 서버 인증서를 취소하는 CRL이 포함되어 있습니다.	정책이 서버 인증서를 발급한 CA를 신뢰하며, 정책에 업로드된 CA 인증서에 해당 인증서를 취소하는 CRL이 포함되어 있지 않습니다.
자체 서명	탐지된 서버 인증서에 동일한 주체 및 발급자 DN이 포함되어 있습니다.	탐지된 서버 인증서에 다른 주체 및 발급자 DN이 포함되어 있습니다.
유효	다음의 모든 사항이 유효합니다. • 정책이 인증서를 발급한 CA를 신뢰합니다. • 서명이 유효함 • 발급자가 유효함 • 정책의 신뢰할 수 있는 CA가 인증서를 취소하지 않음 • 현재 날짜가 인증서의 유효 시작일과 유효 만료일 사이에 해당함	다음 중 하나 이상이 유효하지 않습니다. • 정책이 인증서를 발급한 CA를 신뢰하지 않음 • 서명이 유효하지 않음 • 발급자가 유효하지 않음 • 정책의 신뢰할 수 있는 CA가 인증서를 취소함 • 현재 날짜가 인증서의 유효 시작일보다 이전입니다. • 현재 날짜가 인증서의 유효 만료일을 경과했습니다.
잘못된 서명	인증서의 시그니처를 인증서의 내용과 올바르게 확인할 수 없습니다.	인증서의 시그니처를 인증서의 내용과 올바르게 확인할 수 있습니다.
잘못된 발급자	발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장되지 않습니다.	발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장됩니다.
만료	현재 날짜가 인증서의 유효 만료일을 경과했습니다.	현재 날짜가 유효 만료일 이전이거나 해당일입니다.
아직 유효하지 않음	현재 날짜가 인증서의 유효 시작일보다 이전입니다.	현재 날짜가 유효 시작일 이후이거나 해당일입니다.

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
잘못된 인증서		인증서가 유효합니다. 다음의 모든 사항이 유효합니다. • 유효한 인증서 확장. • 인증서를 지정된 용도로 사용할 수 있습니다. • 유효한 기본 제약 조건 경로 길이. • Not Before 및 Not After의 유효한 값. • 유효한 이름 제약 조건. • 루트 인증서를 지정된 용도로 신뢰할 수 있습니다. • 루트 인증서가 지정된 용도를 수락합니다.

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
	인증서가 유효하지 않습니다. 다음 중 하나 이상이 유효하지 않습니다. • 유효하지 않거나 일치하지 않는 인증서 확장. 즉, 인증서 확장에 유효하지 않은 값(예를 들어 잘못된 인코딩) 또는 다른 확장과 일치하지 않는 일부 값이 있습니다. • 인증서를 지정된 용도로 사용할 수 없습니다. • 기본 제약 조건 경로 길이 매개변수가 초과됐습니다. 자세한 내용은 RFC 5280, 섹션 4.2.1.9를 참조하십시오. • Not Before 또는 Not After의 인증서 값이 잘못되었습니다. 이러한 날짜는 UTCTime 또는 GeneralizedTime으로 인코딩될 수 있습니다. 자세한 내용은 RFC 5280 섹션 4.1.2.5를 참조하십시오. • 이름 제약 조건의 형식이 인식되지 않습니다. 예를 들어 RFC 5280, 섹션 4.2.1.10에서 언급되지 않은 양식의 이메일 주소 형식입니다. 이것은 잘못된 확장 또는 현재 지원되지 않는 일부 새로운 기능 때문일 수 있습니다. 지원되지 않는 이름 제약 조건 유형이 발생했습니다. OpenSSL은 현재 디렉터리 이름, DNS 이름, 이메일 및 URI 유형을 지원합니다. • 루트 인증서 인증 기관을 지정된 용도로 신뢰할 수 없습니다.	

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
	• 루트 인증서 인증 기관이 지정된 용도를 거부합니다.	
유효하지 않은 CRL	Certificate Revocation List(CRL) 디지털 서명이 유효하지 않습니다. 다음 중 하나 이상이 유효하지 않습니다. • CRL의 Next Update(다음 업데이트) 또는 Last Update(마지막 업데이트) 필드의 값이 유효하지 않습니다. • CRL이 아직 유효하지 않습니다. • CRL이 만료되었습니다. • CRL 경로를 확인하는 중에 오류가 발생했습니다. 이 오류는 확장된 CRL 확인이 활성화된 경우에만 발생합니다. • CRL을 찾을 수 없습니다. • 찾을 수 있는 유일한 CRL이 인증서의 범위와 일치하지 않습니다.	CRL이 유효합니다. 다음의 모든 사항이 유효합니다. • Next Update(다음 업데이트) 및 Last Update(마지막 업데이트) 필드가 유효합니다. • CRL의 날짜가 유효합니다. • 경로가 유효합니다. • CRL을 찾았습니다. • CRL이 인증서의 범위와 일치합니다.

인증서는 둘 이상의 상태와 일치할 수 있지만 규칙으로 인해 트래픽에서는 작업을 한 번만 수행할 수 있습니다.

CA가 인증서를 발급하거나 취소했는지 확인하려면 루트 및 중간 CA 인증서와 관련 CRL을 개체로 업로드해야 합니다. 그런 다음 이러한 신뢰할 수 있는 CA 개체를 SSL 정책의 신뢰할 수 있는 CA 인증서 목록에 추가합니다.

외부 인증 증명 신뢰

루트 및 중간 CA 인증서를 SSL 정책에 추가하여 CA를 신뢰할 수 있으며, 그런 다음 이러한 신뢰할 수 있는 CA를 활용하면 트래픽을 암호화하는 데 사용된 서버 인증서를 식별할 수 있습니다.

신뢰할 수 있는 CA 인증서에 업로드된 CRL(Certificate Revocation List: 인증서 폐기 목록)이 포함되어 있는 경우, 신뢰할 수 있는 CA가 암호 인증서를 취소한 것인지 확인할 수도 있습니다.

프로시저

단계 **1** SSL 규칙 편집기에서 **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)**를 선택합니다.

단계 **2** **Available Trusted CAs(**사용 가능한 신뢰할 수 있는 인증서**)**에서 추가할 신뢰할 수 있는 CA를 다음과 같이 찾습니다.

- 신뢰할 수 있는 CA 개체를 즉시 추가한 다음 조건에 추가하려면 **Available Trusted CAs(**사용 가능한 신뢰할 수 있는 **CA)** 목록 위의 추가(+)을 클릭합니다.
- 추가할 신뢰할 수 있는 CA 개체 및 그룹을 검색하려면, **Available Trusted CAs(**사용 가능한 신뢰할 수 있는 **CA)** 목록 위의 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 다음 개체의 이름을 입력하거나, 개체의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 개체를 표시합니다.

단계 **3** 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 **5** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 인증서 상태 TLS/SSL 규칙 조건을 SSL 규칙에 추가합니다. 자세한 내용은 인증서 상태를 기준으로 트래픽 매칭, 1839 페이지를 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

신뢰할 수 있는 인증 기관 개체, 624 페이지

신뢰할 수 있는 외부 인증서 기관 설정

식별된 서버 인증서에는 신뢰할 수 있는 CA가 서명한 인증서가 포함됩니다. 신뢰할 수 있는 CA 인증서를 SSL 정책에 추가한 후 인증서 상태 조건이 포함된 TLS/SSL 규칙을 구성하여 이 트래픽에 대해 매칭할 수 있습니다.

팁 루트 CA의 트러스트 체인 내의 모든 인증서를 신뢰할 수 있는 CA 인증서 목록에 업로드하며, 여기에는 루트 CA 인증서 및 모든 중간 CA 인증서가 포함됩니다. 이렇게 하지 않으면 중간 CA가 발급한 신뢰할 수 있는 인증서를 탐지하는 것이 더 어려워집니다. 또한 루트 발급자 CA를 기반으로 트래픽을 신뢰하도록 인증서 상태 조건을 구성하는 경우, 신뢰할 수 있는 CA의 신뢰 체인 내의 모든 트래픽은 불필요한 해독 없이 허용될 수 있습니다.

SSL 정책을 생성하면 은 Trusted CA Certificates(신뢰할 수 있는 CA 인증서) 탭에 기본 신뢰할 수 있는 CA 개체 그룹인 Cisco Trusted Authorities를 입력합니다.

그룹의 개별 항목을 수정하고, 이 그룹을 SSL 정책에 포함할지 선택할 수 있습니다. 단, 이 그룹은 삭제할 수 없습니다. 시스템 업데이트로 인해 이 목록의 항목이 수정될 수 있으나, 사용자 변경 사항은 그대로 유지됩니다.

인증서 상태를 기준으로 트래픽 매칭

시작하기 전에

- 신뢰할 수 있는 CA 개체 또는 그룹을 SSL 정책에 추가합니다. 자세한 내용은 외부 인증 증명 신뢰, 1837 페이지를 참조하십시오.

프로시저

단계 **1** Firepower Management Center에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**을 선택합니다.

단계 **2** 새 정책을 추가하거나 기존 정책을 편집합니다.

단계 **3** 새 TLS/SSL 규칙을 추가하거나 기존 규칙을 편집합니다.

단계 **4** Add Rule(규칙 추가) 또는 Editing Rule(규칙 편집) 대화 상자에서 **Cert Status(**인증서 상태**)**를 선택합니다.

단계 **5** 각 인증서 상태에는 다음과 같은 옵션이 있습니다.

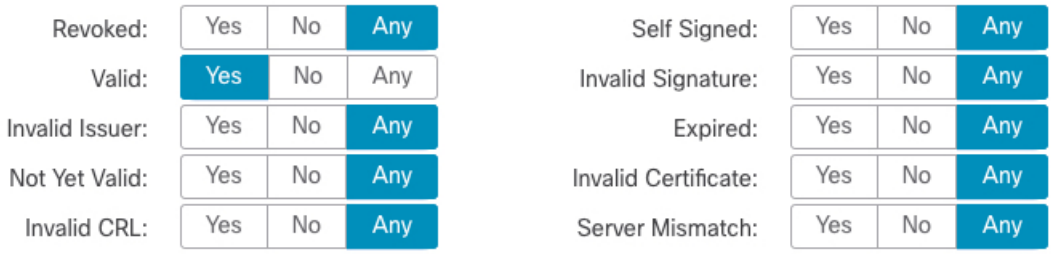
- 해당 인증서 상태가 있는 경우에 매칭하려면 **Yes**를 선택합니다.
- 해당 인증서 상태가 없는 경우에 매칭하려면 **No**를 선택합니다.
- 규칙을 매칭할 때 조건을 건너뛰려면 **Any(**모두**)**를 선택합니다. 다시 말해 **Any(**모두**)**를 선택하면 인증서 상태가 있건 없건 규칙이 매칭됩니다.

단계 **6** 규칙을 추가하거나 계속 수정합니다.

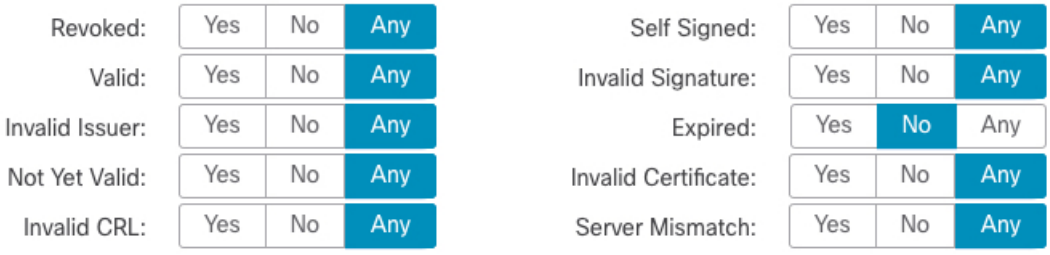
예

조직에서는 Verified Authority 인증 기관을 신뢰합니다. 조직에서는 Spammer Authority 인증 기관을 신뢰하지 않습니다. 시스템 관리자가 Verified Authority 인증서 및 Verified Authority에서 발급한 중간 CA 인증서를 시스템에 업로드합니다. Verified Authority가 이전에 발급한 인증서를 취소했으므로 시스템 관리자는 Verified Authority가 제공한 CRL을 업로드합니다.

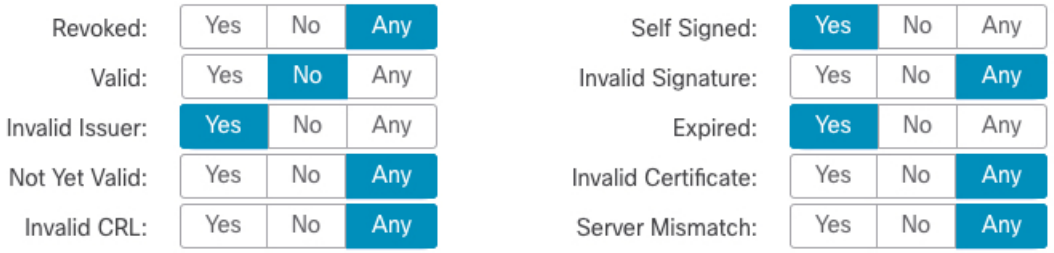
다음 그림에는 유효한 인증서를 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이러한 인증서는 Verified Authority에서 발급하였으며, CRL에 포함되지 않고, 유효 시작일과 유효 만료일 사이의 기간이 아직 남아 있는 상태입니다. 이러한 인증서로 암호화된 트래픽은 컨피그레이션으로 인해, 액세스 제어를 통해 해독 및 검사되지 않습니다.

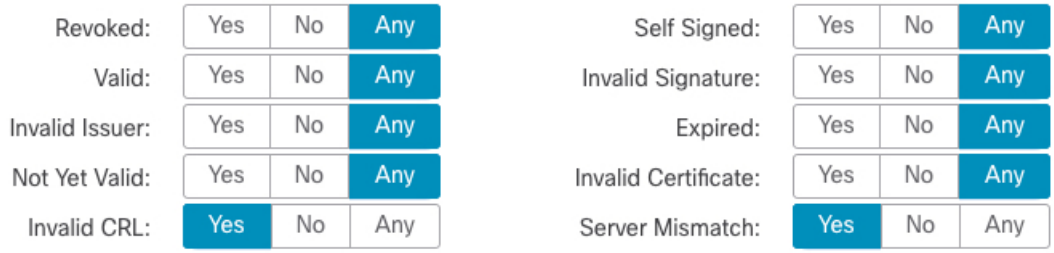


다음 그림에는 상태가 없는지 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이 경우 컨피그레이션으로 인해, 만료되지 않은 인증서로 암호화된 트래픽과 매칭을 수행하며 해당 트래픽을 모니터링합니다.



다음 그래픽에는 몇 가지 상태가 있는 경우 또는 없는 경우와 매칭하는 인증서 상태 규칙 조건이 나와 있습니다. 이 구성에서는 잘못된 사용자가 발급한 인증서, 자체 서명 인증서, 유효하지 않거나 만료된 인증서로 암호화된 수신 트래픽과 규칙이 일치하는 경우 알려진 키를 사용하여 트래픽이 암호 해독됩니다.





다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

암호 그룹 **TLS/SSL** 규칙 조건

시스템에서는 암호 그룹 규칙 조건에 추가할 수 있는 미리 정의된 암호 그룹을 제공합니다. 여러 암호 그룹이 포함된 암호 그룹 목록 개체를 추가할 수도 있습니다.

참고 새 암호 그룹을 추가할 수 없습니다. 또한 미리 정의된 암호 그룹을 수정하거나 삭제할 수 없습니다.

단일한 암호 그룹 조건의 **Selected Cipher Suites(**선택한 암호화 그룹**)**에 최대 50개의 암호 그룹 및 암호 그룹 목록을 추가할 수 있습니다. 다음과 같은 암호 그룹을 암호 그룹 조건에 추가할 수 있습니다.

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA

- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

다음에 유의하십시오.

- 구축에 대해 지원되지 않는 암호 그룹을 추가하는 경우, 구성을 구축할 수 없습니다. 예를 들어 패시브 구축은 DHE(Diffie-Hellman Ephemeral) 또는 ECDHE(Ephemeral Elliptic Curve Diffie-Hellman) 암호 그룹을 사용한 트래픽 암호 해독을 지원하지 않습니다. 이러한 암호 그룹이 포함된 규칙을 생성할 경우 액세스 제어 정책을 구축할 수 없습니다.
- 암호 그룹이 포함된 암호 그룹 조건을 구성할 경우, 인증서 조건에 추가하는 외부 인증서 개체 또는 **Decrypt - Resign(**암호 해독 **-** 다시 서명**)** 작업에 연결되는 내부 CA 개체는 암호 그룹의 시그니처 알고리즘 유형과 매칭되어야 합니다. 예를 들어 규칙의 암호 그룹 조건이 EC 기반 암호

그룹을 참조할 경우, 추가되는 모든 서버 인증서 또는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업과 연결되는 CA 인증서도 EC 기반이어야 합니다. 이때 시그니처 알고리즘 유형이 매칭되지 않을 경우, 정책 편집기에서는 규칙 옆에 경고 아이콘이 표시됩니다.

- 시스템은 익명 암호 그룹으로 암호화된 트래픽을 해독할 수 없습니다. 익명 암호 그룹을 **Cipher Suite(**암호 그룹**)** 조건에 추가할 경우, SSL 규칙에서 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

암호화된 트래픽을 암호 그룹으로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 Cipher Suite(암호 그룹)를 선택합니다.

단계 **2** **Available Cipher Suites(**사용 가능한 암호 그룹**)**에서 추가할 암호 그룹을 다음과 같이 찾습니다.

- 조건에 추가할 수 있는 암호 그룹 목록을 즉시 추가하려면 **Available Cipher Suites(**사용 가능한 암호 그룹**)** 목록 위의 추가( )를 클릭합니다.
- 추가할 암호 그룹 및 목록을 검색하려면, **Available Cipher Suites** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 암호 그룹의 이름을 입력하거나 암호 그룹의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 암호 그룹을 표시합니다.

단계 **3** 암호 그룹을 선택하려면 클릭합니다. 모든 암호 그룹을 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

팁 선택한 암호 그룹을 끌어서 놓을 수도 있습니다.

단계 **5** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

암호 그룹 목록, 615 페이지

암호화 프로토콜 버전 TLS/SSL 규칙 조건

SSL 버전 3.0, 또는 TLS 버전 1.0, 1.1, 1.2로 암호화된 트래픽과 매칭되도록 선택할 수 있습니다. 기본적으로, 규칙을 생성할 때 모든 프로토콜 버전이 선택됩니다. 여러 버전을 선택할 경우, 선택한 버전과 매칭되는 암호화된 트래픽은 규칙과 매칭됩니다. 규칙 조건을 저장할 경우 하나 이상의 프로토콜 버전을 선택해야 합니다.

SSL v2.0은 버전 규칙 조건에서 선택할 수 없습니다. 시스템에서는 SSL 버전 2.0으로 암호화된 트래픽의 암호 해독을 지원하지 않습니다. 해독 불가능한 작업을 구성하여 추가 검사 없이 이 트래픽을 허용하거나 차단하도록 할 수 있습니다.

트래픽을 암호화 프로토콜 버전으로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 Version(버전)을 선택합니다.

단계 **2** 매칭할 프로토콜 버전을 선택합니다.

단계 **3** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

73 장

SSL 하드웨어 엑셀러레이션(Hardware Acceleration) 모니터링

CLI에서 카운터 표시 명령을 사용해 TLS 암호화 가속 동작을 평가합니다. 이 명령은 정상적인 동작, 경고 및 잠재적인 심각한 문제에 대한 다양한 메트릭 목록을 표시합니다.

참고 **show counters description** 명령을 사용하여 각 카운터에 대한 설명을 확인합니다. TLS 암호화 가속 관련 카운터만 보려면 **show counters description | include TLS_TRK**를 사용합니다.

- 정보 카운터, 1847 페이지
- 알림 카운터, 1848 페이지
- 오류 카운터, 1848 페이지
- 치명적 카운터, 1849 페이지

정보 카운터

로드 중 시스템이 정상적으로 작동하는 경우, 다음 카운터에 대한 정상적으로 작동, 다음 카운터에 대한 큰 수를 확인해야 합니다. 연결당 추적기 프로세스에 2면이 있기 때문에 이러한 카운터가 연결당 2씩 증가합니다. PRIV_KEY_RECV 및 SECU_PARAM_RECV 카운터가 가장 중요하며 강조 표시됩니다. CONTEXT_CREATED 및 CONTEXT_DESTROYED 카운터는 암호화 칩 메모리과 관련이 있습니다.

```
> show counters
Protocol      Counter                        Value   Context
SSLENC        CONTEXT_CREATED               258225   Summary
SSLENC        CONTEXT_DESTROYED             258225   Summary
TLS_TRK       OPEN_SERVER_SESSION           258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION           258225   Summary
TLS_TRK       UPSTREAM_CLOSE                516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE              516450   Summary
TLS_TRK       FREE_SESSION                  516450   Summary
TLS_TRK       CACHE_FREE                    516450   Summary
TLS_TRK       PRIV_KEY_RECV                 258225   Summary
TLS_TRK       NO_KEY_ENABLE                 258225   Summary
```

```
TLS_TRK      SECU_PARAM_RECV                  516446   Summary
TLS_TRK      DECRYPTED_ALERT                  258222   Summary
TLS_TRK      DECRYPTED_APPLICATION          33568976   Summary
TLS_TRK      ALERT_RX_CNT                     258222   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT           258222   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY            258222   Summary
TCP_PRX      OPEN_SESSION                     516450   Summary
TCP_PRX      FREE_SESSION                     516450   Summary
TCP_PRX      UPSTREAM_CLOSE                   516450   Summary
TCP_PRX      DOWNSTREAM_CLOSE                 516450   Summary
TCP_PRX      FREE_CONN                        258222   Summary
TCP_PRX      SERVER_CLEAN_UP                  258222   Summary
TCP_PRX      CLIENT_CLEAN_UP                  258222   Summary
```

알림 카운터

TLS 1.2 사양에 따라 다음 카운터를 구현했습니다. FATAL 또는 BAD 경고는 문제가 있음을 의미할 수 있습니다. 그러나 ALERT_RX_CLOSE_NOTIFY는 정상입니다.

세부 정보는 RFC 5246 섹션 7.2를 참조하십시오.

```
TLS_TRK      ALERT_RX_CNT                     311   Summary
TLS_TRK      ALERT_TX_CNT                       2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT          2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT          2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT           308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT               3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT               2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY            308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC            2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC            2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE           1   Summary
```

오류 카운터

이 카운터는 시스템 오류를 나타냅니다. 이 수는 정상적인 시스템에서 낮아야 합니다. BY_PASS 카운터는 암호 해독 없이 (소프트웨어에서 실행되는) 검사 엔진(Snort) 프로세스에서 직접 전달된 패킷을 나타냅니다. 다음 예는 장애 카운터 목록을 보여줍니다.

값이 0인 카운터는 표시되지 않습니다. 카운터 전체 목록을 보려면 명령을 사용하십시오. **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                          Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM             2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET           2   Summary
TLS_TRK      ENC_FAIL                            82   Summary
TLS_TRK      DEC_FAIL                           211   Summary
TLS_TRK      DEC_CKE_FAIL                     43194   Summary
TLS_TRK      ENC_CB_FAIL                       4335   Summary
TLS_TRK      DEC_CB_FAIL                        909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                    818   Summary
TLS_TRK      RECORD_PARSE_ERR                   123   Summary
TLS_TRK      IN_ERROR                         44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD            43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE               123   Summary
```

```
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR          123   Summary
TLS_TRK      DECRYPT_FAIL                    43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                  127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                127   Summary
```

치명적 카운터

FATAL 카운터는 심각한 오류를 나타냅니다. 이러한 카운터는 정상적인 시스템에서 0이거나 0 근처에 있어야 합니다. 다음 예는 FATAL 카운터 목록을 보여줍니다.

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

RING_FULL 카운터는 FATAL 카운터는 아니지만 시스템이 암호화 칩을 오버로드하는 빈도를 나타냅니다. ACCELERATOR_RESET 카운터는 TLS 암호화 가속 프로세스가 예기치 않게 실패하여 보류 중인 작업까지 중단되는 횟수입니다. 이 수는 ACCELERATOR_CORE_TIMEOUT 및 RSA_PRIVATE_DECRYPT_FAILED에서도 확인할 수 있습니다.

지속적으로 문제가 발생하는 경우 TLS 암호화 가속(**system support ssl-hw-offload disable** 또는 **config hwCrypto disable**)를 비활성화하고 Cisco TAC과 협력하여 문제를 해결합니다.

참고 **show snort tls-offload** 및 **debug snort tls-offload** 명령을 사용하여 추가적인 문제 해결을 할 수 있습니다. **clear snort tls-offload** 명령을 사용하여 **show snort tls-offload** 명령에 표시된 카운터를 0으로 재설정합니다.

74 장

TLS/SSL 규칙 문제 해결

연결 이벤트를 사용해 네트워크의 애플리케이션이 TLS/SSL 피닝을 사용하고 있는지 여부를 진단할 수 있습니다. 애플리케이션이 TLS/SSL 피닝을 사용 중인 경우, TLS/SSL 규칙 지침 및 제한 사항, 1804 페이지를 참조하십시오.

- TLS/SSL 피닝 정보, 1851 페이지
- TLS/SSL 암호 그룹 확인, 1856 페이지

TLS/SSL 피닝 정보

일부 애플리케이션이 *TLS/SSL* 피닝또는 인증서 피닝이라는 기법을 사용하는데 이 기법에서는 원본 서버 인증서 지문이 애플리케이션 자체에 내장됩니다. 따라서 TLS/SSL 규칙을 **Decrypt - Resign(**암호 해독 - 재서명**)** 작업으로 구성하는 경우, 애플리케이션이 매니지드 디바이스로부터 재서명된 인증서를 수신할 때 확인이 실패하고 연결이 중단됩니다.

TLS/SSL 피닝이 발생하고 있는지 확인하려면, Facebook 같은 모바일 애플리케이션에 로그인을 시도합니다. 네트워크 연결 오류가 표시되는 경우, 웹 브라우저를 사용하여 로그인 합니다. (예를 들어, Facebook 모바일 애플리케이션에는 로그인이 불가능하더라도 Safari나 Chrome을 사용하여 Facebook에 로그인할 수 있습니다.) Firepower Management Center 연결 이벤트를 TLS/SSL 피닝의 추가 증거로 사용할 수 있습니다.

참고 TLS/SSL 피닝은 모바일 애플리케이션에 국한되지 않습니다.

관련 항목

TLS/SSL 피닝 문제 해결, 1851 페이지

TLS/SSL 피닝 문제 해결

연결 이벤트를 보고 디바이스에 SSL 피닝이 발생하는지 확인할 수 있습니다. 최소한 연결 이벤트의 테이블 보기에 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)** 열을 추가해야 합니다.

시작하기 전에

- SSL 규칙으로 암호 해독 가능 연결 로깅, 2870 페이지의 설명에 따라 TLS/SSL 규칙에 대한 로깅을 활성화합니다.
- Facebook 같은 모바일 애플리케이션에 로그인합니다. 네트워크 연결 오류가 표시되면 Chrome 또는 Safari를 사용하여 Facebook에 로그인합니다. 웹 브라우저를 사용한 로그인은 가능하지만 기본 애플리케이션을 사용한 로그인은 불가능할 경우, 피닝이 발생할 가능성이 높습니다.

프로시저

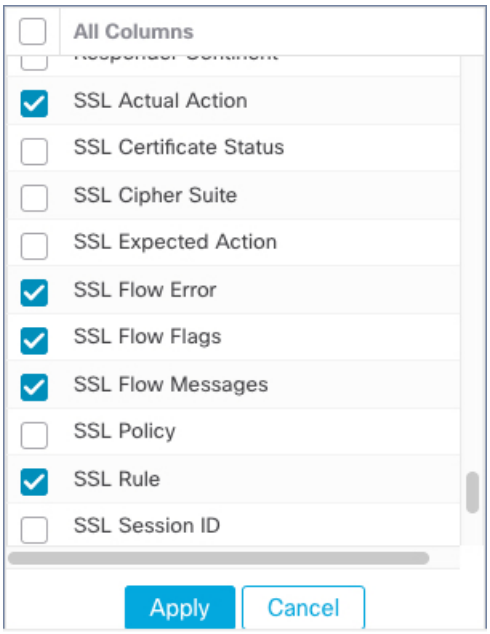
단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Analysis(분석) > Connections(연결) > Events(이벤트)**를 클릭합니다.

단계 **3** **Table View of Connection Events(연결 이벤트 테이블 보기)**를 클릭합니다.

단계 **4** 최소한 **SSL Flow Flags(SSL 플로우 플래그)** 및 **SSL Flow Messages(SSL 플로우 메시지)**에 대한 열을 추가하려면 연결 이벤트 테이블에 있는 임의의 열에서 **x**를 클릭합니다.

다음 예는 **SSL Actual Action(SSL 실제 작업)**, **SSL Flow Error(SSL 플로우 오류)**, **SSL Flow Flags(SSL 플로우 플래그)**, **SSL Flow Messages(SSL 플로우 메시지)**, **SSL Policy(SSL 정책)**, **SSL Rule(SSL 규칙)** 열을 연결 이벤트 테이블에 추가하는 방법을 보여줍니다.



열은 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지에 설명된 순서대로 추가됩니다.

단계 **5** **Apply(적용)**를 클릭합니다.

단계 **6** 다음 단락에서는 SSL 피닝 동작을 식별하는 방법을 설명합니다.

단계 **7** 네트워크의 애플리케이션이 SSL 피닝을 사용하는지 확인하려면 TLS/SSL 규칙 지침 및 제한 사항, 1804 페이지를 참조하십시오.

다음에 수행할 작업

TLS/SSL 연결 이벤트를 사용하여 다음 중 하나를 찾으면 TLS/SSL 피닝이 발생하는지 확인할 수 있습니다.

- 클라이언트가 서버에서 SERVER_HELLO, SERVER_CERTIFICATE, SERVER_HELLO_DONE 메시지를 수신하는 즉시 SSL ALERT 메시지와 TCP 재설정을 차례로 전송하는 애플리케이션이 다음과 같은 증상을 보입니다. (`Unknown CA (48)` 알림은 패킷 캡처를 사용하여 볼 수 있습니다.)
  - SSL Flow Flags(SSL 플로우 플래그) 열에 `ALERT_SEEN`이 표시되지만 `APP_DATA_C2S` 또는 `APP_DATA_S2C`는 표시되지 않습니다.
  - SSL Flow Messages(SSL 플로우 메시지) 열에는 일반적으로 `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`이 표시됩니다.
  - SSL Flow Error(SSL 플로우 오류) 열에 `Success`(성공)가 표시됩니다.
- 알림을 전송하지 않고 대신 SSL 핸드셰이크가 완료된 후 TCP 재설정을 전송하는 애플리케이션이 다음과 같은 증상을 보입니다.
  - SSL Flow Flags(SSL 플로우 플래그) 열에 `ALERT_SEEN`, `APP_DATA_C2S`, or `APP_DATA_S2C`가 표시되지 않습니다.
  - SSL Flow Messages(SSL 플로우 메시지) 열에는 일반적으로 `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`, `CLIENT_KEY_EXCHANGE`, `CLIENT_CHANGE_CIPHER_SPEC`, `CLIENT_FINISHED`,`SERVER_CHANGE_CIPHER_SPEC`, `SERVER_FINISHED`가 표시됩니다.
  - SSL Flow Error(SSL 플로우 오류) 열에 `Success`(성공)가 표시됩니다.

관련 항목

연결 및 보안 인텔리전스 이벤트 테이블 사용, 2900 페이지
연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지
연결 이벤트 필드에서 제공되는 정보, 2896 페이지
이벤트 검색, 2825 페이지
알 수 없는 또는 잘못된 인증서 또는 인증 기관 문제 해결, 1854 페이지

알 수 없는 또는 잘못된 인증서 또는 인증 기관 문제 해결

연결 이벤트를 보고 디바이스에 알 수 없는 인증 기관, 잘못된 인증서 또는 알 수 없는 인증서가 있는지 확인할 수 있습니다. TLS/SSL 인증서가 고정된 경우에도 이 절차를 사용할 수 있습니다. 최소한 연결 이벤트의 테이블 보기에 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)** 열을 추가해야 합니다.

시작하기 전에

- TLS/SSL 암호 해독 규칙을 설정합니다.
- SSL 규칙으로 암호 해독 가능 연결 로깅, 2870 페이지의 설명에 따라 TLS/SSL 규칙에 대한 로깅을 활성화합니다.

프로시저

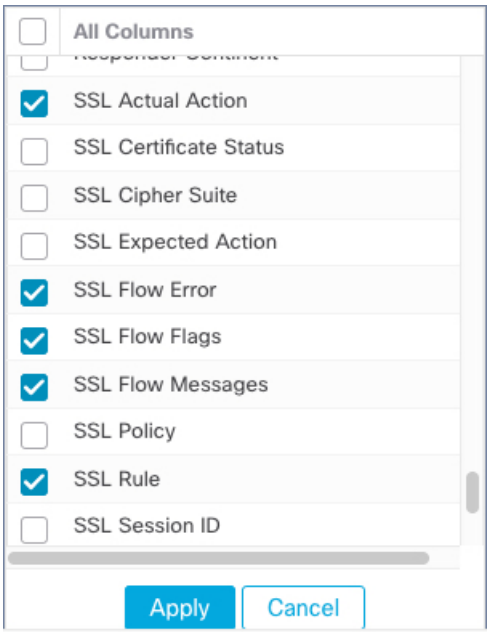
단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 클릭합니다.

단계 **3** **Table View of Connection Events(**연결 이벤트 테이블 보기**)**를 클릭합니다.

단계 **4** 최소한 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)**에 대한 열을 추가하려면 연결 이벤트 테이블에 있는 임의의 열에서 **x**를 클릭합니다.

다음 예는 **SSL Actual Action(SSL** 실제 작업**)**, **SSL Flow Error(SSL** 플로우 오류**)**, **SSL Flow Flags(SSL** 플로우 플래그**)**, **SSL Flow Messages(SSL** 플로우 메시지**)**, **SSL Policy(SSL** 정책**)**, **SSL Rule(SSL** 규칙**)** 열을 연결 이벤트 테이블에 추가하는 방법을 보여줍니다.



열은 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지에 설명된 순서대로 추가됩니다.

단계 **5** **Apply(**적용**)**를 클릭합니다.

단계 **6** 다음 표에서는 인증서 또는 인증 기관이 잘못되었거나 누락되었는지 확인할 수 있는 방법에 대해 설명합니다.

SSL 플로우 플래그	의미
CLIENT_ALERT_SEEN_UNKNOWN_CA	유효한 인증서 체인 또는 부분 체인이 SSL 클라이언트 애플리케이션에서 수신되었지만CA 인증서를 찾을 수 없거나 알려진 신뢰할 수있는 CA와 일치할 수 없으므로 인증서가 수락되지 않았음을 나타냅니다. 이 메시지는 항상 복구 불가능한 오류를 나타냅니다.
CLIENT_ALERT_SEEN_BAD_CERTIFICATE	인증서가 손상되었거나 올바르게 확인되지 않은 서명이 포함되어 있거나 다른 문제가 있습니다.
CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN	일부 다른(지정되지 않은) 문제가 발생하여 인증서를 처리할 수 없게 되었습니다.

TLS/SSL 암호 그룹 확인

시작하기 전에

이 주제에서는 암호 그룹 조건이 있는 TLS/SSL 규칙을 저장할 때 다음과 같은 오류가 표시되는 경우에 수행해야 하는 작업을 설명합니다.

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature
algorithm that the resigning CA's signature algorithm
```

이 오류는 TLS/SSL 규칙 조건에 대해 선택한 하나 이상의 암호 그룹이 TLS/SSL 규칙에 사용되는 인증서와 호환되지 않음을 나타냅니다. 이 문제를 해결하려면 사용 중인 인증서에 액세스할 수 있어야 합니다.

참고 이 주제에 나온 작업에서는 사용자가 TLS/SSL 암호화의 작동 원리에 대해 알고 있다고 가정합니다.

프로시저

단계 **1** 지정된 암호 그룹으로 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)**가 포함된 SSL 규칙을 저장하려고 하면 다음과 같은 오류가 표시됩니다.

예제**:**

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

단계 **2** 트래픽 암호 해독에 사용 중인 인증서를 찾고, 필요하다면 openssl 명령을 실행할 수 있는 시스템에 인증서를 복사합니다.

단계 **3** 인증서에서 사용되는 서명 알고리즘을 표시하려면 다음 명령을 실행합니다.

openssl x509 -in *CertificateName* **-text -noout**

출력의 처음 몇 행은 다음과 비슷하게 표시됩니다.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

단계 **4** **Signature algorithm**은 다음을 알려줍니다.

- 사용되는 암호화 기능(앞의 예에서 **ECDSA**은 Elliptic Curve Digital Signature Algorithm을 뜻합니다).
- 암호화된 메시지의 다이제스트를 생성하는 데 사용되는 해시 함수(앞의 예에서는 **SHA256**).

단계 **5** OpenSSL at University of Utah 같은 리소스에서 이러한 값과 일치하는 암호 그룹을 검색합니다. 암호 그룹은 RFC 형식이어야 합니다.

Mozilla wiki의 Server Side TLS 또는 RFC 5246의 부록 C 같은 다양한 다른 사이트도 검색할 수 있습니다. Microsoft 문서의 Cipher Suites in TLS/SSL (Schannel SSP)에는 암호 그룹에 대한 상세한 설명이 나와 있습니다.

단계 **6** 필요한 경우, OpenSSL 이름을 Firepower Management System서 사용하는 RFC 이름으로 변환합니다. `https://testssl.sh` 사이트의 RFC mapping list를 참조하십시오.

단계 **7** 앞의 예에서 **ecdsa-with-SHA256**는 Mozilla wiki의 Modern Compatibility List에서 찾을 수 있습니다.

a) 이름에 **ECDSA** 및 **SHA-256**가 있는 암호 그룹만 선택하십시오. 다음 암호 그룹이 뒤에 나옵니다.

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) RFC mapping list에서 해당 RFC 암호 그룹을 찾습니다. 다음 암호 그룹이 뒤에 나옵니다.

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

단계 **8** TLS/SSL 규칙에 이전 암호 그룹을 추가합니다.

XVI 부

AMP(Advanced Malware Protection) 및 파일 제어

- 파일 정책 및 악성코드 보호, 1861 페이지
- 파일 및 악성코드 탐지 성능 및 저장 조정, 1903 페이지

75 장

파일 정책 및 악성코드 보호

다음 주제에서는 파일 제어, 파일 정책, 파일 규칙, Advanced Malware Protection(AMP), 클라우드 연결, 동적 분석 연결의 개요를 제공합니다.

- 파일 정책 및 Advanced Malware Protection 정보, 1861 페이지
- 파일 정책 요구 사항 및 사전 요건, 1862 페이지
- 파일 및 악성코드 정책을 위한 라이선스 요구 사항, 1863 페이지
- 파일 정책 및 악성코드 탐지 모범 사례 , 1863 페이지
- 악성코드 차단 설정 방법, 1866 페이지
- 악성코드 차단을 위한 클라우드 연결, 1871 페이지
- 파일 정책 및 파일 규칙, 1880 페이지
- 회귀적 속성 변경, 1896 페이지
- (선택 사항) AMP for Endpoints를 사용한 악성코드 방지, 1896 페이지
- 파일 정책 및 악성코드 보호 히스토리, 1901 페이지

파일 정책 및 Advanced Malware Protection 정보

악성 코드를 탐지하고 차단하려면 파일 정책을 사용해야 합니다. 파일 정책을 사용하면 트래픽을 파일 유형별로 탐지하고 제어할 수 있습니다.

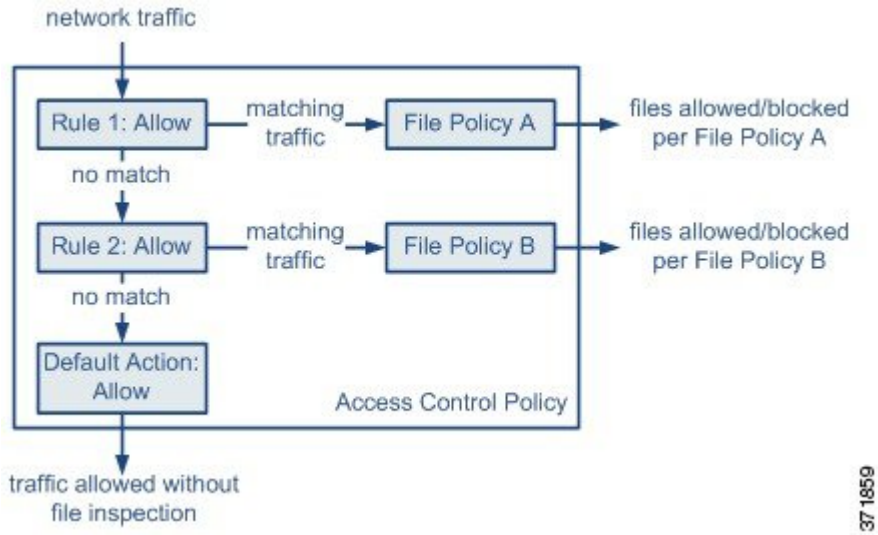
Firepower의 Advanced Malware Protection(AMP)은 네트워크에서 악성코드 전송을 탐지, 캡처, 추적, 분석, 로깅하고 선택적으로 차단할 수 있습니다. Firepower Management Center 웹 인터페이스에서 이 기능은 *AMP for Networks* 라고 하며 이전에는 *AMP for Firepower*라고 했습니다. AMP(Advanced Malware Protection)는 인라인으로 구축된 매니지드 디바이스와 Cisco Cloud의 위협 데이터를 사용하여 악성코드를 식별합니다.

파일 정책을 전반적 액세스 제어 구성의 일환으로 네트워크 트래픽을 처리하는 액세스 제어 규칙에 연결합니다.

시스템은 네트워크에서 악성코드를 탐지하면 파일 및 악성코드 이벤트를 생성합니다. 파일 및 악성코드 이벤트 데이터를 분석하려면 파일/악성코드 이벤트 및 네트워크 파일 경로 분석, 2963 페이지를 참조하십시오.

파일 정책

파일 정책은 악성코드 차단 및 파일 제어를 수행하기 위해 시스템에서 전체 액세스 제어 설정의 일부로 사용하는 구성 집합입니다. 이 연결은 시스템이 액세스 제어 규칙의 조건에 일치하는 트래픽에 파일을 통과시키기 전에 먼저 파일을 검사하도록 합니다. 인라인 배포에서 간단한 액세스 제어 정책의 다음 다이어그램을 참고하십시오.



정책에 두 개의 액세스 제어 규칙이 있으며, 두 규칙 모두 Allow(허용) 작업을 사용하고 파일 정책과 연결되어 있습니다. 정책의 기본 작업은 또한 파일 정책 검사 없이 트래픽을 허용하는 것입니다. 이 시나리오에서, 트래픽은 다음과 같이 처리됩니다.

- `Rule 1(규칙 1)`에 일치하는 트래픽은 `File Policy A(파일 정책 A)`로 검사합니다.
- `Rule 1(규칙 1)`에 일치하지 않는 트래픽은 `Rule 2(규칙 2)`에 대해 평가됩니다. `Rule 2(규칙 2)`에 일치하는 트래픽은 `File Policy B(파일 정책 B)`로 검사합니다.
- 둘 중 어느 규칙과도 일치하지 않는 트래픽은 허용됩니다. 파일 정책을 기본 작업과 연결할 수 없습니다.

다양한 파일 정책을 서로 다른 액세스 제어 규칙과 연결할 경우, 네트워크에 전송된 파일을 식별하고 차단하는 방법을 세부적으로 제어할 수 있습니다.

파일 정책 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자

파일 및 악성코드 정책을 위한 라이선스 요구 사항

수행할 작업	필요한 라이선스	파일 규칙 작업
특정 유형의 모든 파일 차단 또는 허용(예: 모든 .exe 파일 차단)	보호	허용, 차단, 차단 후 재설정
악성 코드를 포함하거나 포함할 가능성이 있다는 판단에 따라, 선택적으로 파일을 허용하거나 차단합니다.	보호 악성코드	악성코드 클라우드 조화, 악성코드 차단
파일 저장	보호 악성코드	**Store Files(**파일 저장**)**를 선택한 모든 파일 규칙 작업

악성 코드 라이선스 관련 정보는 다음을 참조하십시오.

- 클래식 디바이스에 대한 악성코드 라이선스, 164 페이지

파일 정책 및 악성코드 탐지 모범 사례

아래에 설명된 항목 외에도 악성코드 차단 설정 방법, 1866 페이지의 단계 및 참조 주제를 따르십시오.

파일 규칙 모범 사례

파일 규칙을 구성할 때 다음 지침 및 제한 사항에 유의하십시오.

- 수동 배포에 파일을 차단하기 위해 구성된 규칙은 일치하는 파일을 차단하지 않습니다. 연결이 계속해서 파일을 전송하므로, 연결의 시작을 로깅하는 규칙을 구성하는 경우, 이 연결에 대해 로깅된 여러 이벤트를 볼 수 있습니다.
- 정책에는 여러 규칙이 포함될 수 있습니다. 규칙을 만들 때는 이전 규칙에 의해 "숨겨진" 규칙이 없는지 확인합니다.
- 동적 분석이 지원되는 파일 유형은 다른 분석 유형이 지원되는 파일 유형의 하위 집합입니다. 각 분석 유형이 지원되는 파일 유형을 보려면 파일 규칙 구성 페이지로 이동하여 **Block Malware(**악성코드 차단**)** 작업을 선택하고 관심 있는 확인란을 선택합니다.

  시스템이 모든 파일 유형을 검사하도록 하려면 동적 분석을 위한 규칙과 기타 분석 유형을 위한 규칙을 동일 정책 내에서 별도로 생성합니다.

- 파일 규칙이 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 작업으로 구성되어 있고 Firepower Management Center이 AMP 클라우드와의 연결을 설정할 수 없는 경우, 연결이 복원될 때까지 시스템은 구성된 어떤 규칙 작업도 수행할 수 없습니다.
- Cisco는 TCP 연결이 재설정될 때까지 차단된 애플리케이션 세션이 계속 열려 있는 것을 방지하기 위해 **Block Files(**파일 차단**)** 및 **Block Malware(**악성코드 차단**)** 작업을 위한 **Reset Connection(**연결 재설정**)**을 활성화할 것을 권장합니다. 연결을 재설정하지 않으면 TCP 연결이 자체적으로 재설정될 때까지 클라이언트 세션이 계속 열려 있게 됩니다.
- 대량의 트래픽을 모니터링하는 경우, 모든 캡처 파일을 저장하거나 동적 분석을 위해 모든 캡처 파일을 전송하지 마십시오. 이렇게 하면 시스템 성능에 부정적인 영향을 줄 수 있습니다.
- 시스템에서 탐지된 모든 파일 유형에서 악성코드 분석을 수행할 수는 없습니다. 사용자가 **Application Protocol(**애플리케이션 프로토콜**)**, **Direction of Transfer(**전송 방향**)**, 및 **Action(**작업**)** 드롭다운 목록에서 값을 선택한 후에는 시스템이 파일 유형 목록을 제한합니다.

파일 탐지 모범 사례

파일 탐지에 대한 다음 참고 사항 및 제한 사항을 고려하십시오.

- 파일이 애플리케이션 프로토콜 조건을 갖춘 규칙에 일치하는 경우, 파일 이벤트 생성은 시스템이 파일의 애플리케이션 프로토콜을 확인한 후에 발생합니다. 확인되지 않은 파일은 파일 이벤트를 생성하지 않습니다.
- FTP는 다른 채널에 명령 및 데이터를 전송합니다. 패시브 또는 인라인 탭 모드 구축에서 FTP 데이터 세션 및 제어 세션의 트래픽은 동일한 내부 리소스로 부하 분산되지 않을 수 있습니다.
- POP3, POP, SMTP 또는 IMAP 세션에서 파일에 대한 모든 파일 이름의 총 바이트 수가 1024를 초과할 경우, 세션에서 파일 이벤트는 파일 이름 버퍼가 채워진 후 발견된 파일의 정확한 파일 이름을 반영하지 않을 수 있습니다.
- 텍스트 기반의 파일을 SMTP에 전송할 경우, 일부 메일 클라이언트는 줄 바꿈을 CRLF 줄 바꿈 문자 표준으로 변환합니다. Mac 기반의 호스트가 캐리지 리턴(CR) 문자를 사용하고 Unix/Linux 기반의 호스트가 라인 피드(LF) 문자를 사용하기 때문에 메일 클라이언트에 의한 줄 바꿈 변환은 파일의 크기를 변경할 수 있습니다. 인식 불가능한 파일 유형을 처리할 때 일부 메일 클라이언트가 줄 바꿈 변환을 기본값으로 설정한다는 점에 유의하십시오.
- ISO 파일을 탐지하려면 "Limit the number of bytes inspected when doing file type detection(파일 유형 탐지를 수행할 때 검사되는 바이트 수 제한)" 옵션을 파일 및 악성코드 탐지 성능 및 저장 옵션, 1903 페이지의 설명처럼 36870보다 큰 값으로 설정하십시오.
- rar5를 포함하여 일부 .rar 아카이브 내의 .Exe 파일을 검색할 수 없습니다.

파일 차단 모범 사례

파일 차단에 대한 다음 참고 사항 및 제한 사항을 고려하십시오.

- 파일의 파일 종료 마커가 탐지되지 않는 경우, 전송 프로토콜에 상관없이 해당 파일은 **Block Malware(**악성코드 차단**)** 규칙 또는 맞춤형 탐지 목록에 의해 차단되지 않습니다. 시스템은 파일 종료 마커에 표시된 대로 전체 파일을 받을 때까지 파일을 차단하기 위해 대기하며, 마커가 탐지된 후 파일을 차단합니다.
- FTP 파일 전송을 위한 파일 종료 마커가 마지막 데이터 세그먼트와 별도로 전송되는 경우, 마커는 차단되며 FTP 클라이언트는 파일 전송이 실패했다고 표시하지만 실제로 파일은 디스크에 완전히 전송됩니다.
- **Block Files(**파일 차단**)** 및 **Block Malware(**악성코드 차단**)** 작업을 가진 파일 규칙은 초기 파일 전송 시도가 발생한 후 24시간 동안 탐지된 동일한 파일, URL, 서버 및 클라이언트 애플리케이션의 새로운 세션을 차단함으로써 HTTP를 통한 파일 다운로드가 자동으로 재개되는 것을 차단합니다.
- 드물게 HTTP 업로드 세션의 트래픽이 작동하지 않는 경우, 시스템은 트래픽을 제대로 다시 어셈블할 수 없으므로 트래픽을 차단하거나 파일 이벤트를 생성하지 않습니다.
- **Block Files(**파일 차단**)** 규칙으로 차단된 파일을 NetBIOS-ssn으로 전송하는 경우(SMB 파일 전송 등), 대상 호스트에서 파일을 확인할 수 있습니다. 그러나, 파일은 다운로드가 시작된 후 차단되기 때문에 사용할 수 없으며, 그 결과 파일 전송은 완료되지 않습니다.
- NetBIOS ssn을 통해 전송되는 파일(예: SMB 파일 전송)을 탐지하거나 차단하는 규칙을 생성하는 경우, 시스템은 진행 중인 파일 전송을 검사하지 않습니다. 하지만 파일 정책을 호출하는 액세스 제어 정책을 구축한 후 전송되는 새 파일은 검사합니다.
- SMB에는 IP 주소는 같고 포트는 다른 여러 병렬 세션을 생성하는 다중 채널이라는 기능이 있습니다. 다중 채널을 통한 트랜잭션의 경우, 시스템에 의해 단일 파일로 검사되지 않는 이러한 세션에서 파일 다운로드가 멀티플렉싱됩니다.
- 단일 TCP 또는 SMB 세션에서 동시에 전송되는 파일은 검사되지 않습니다.
- 클러스터 환경에서 클러스터 역할 변경 또는 디바이스 장애로 인해 기존 SMB 세션을 새로운 디바이스로 이동하는 경우, 진행 중인 파일 전송의 파일은 검사되지 않을 수 있습니다.
- Microsoft Windows 시스템 간의 일부 SMB 파일 전송은 빠른 파일 전송을 위해 매우 높은 TCP 창 크기를 사용합니다. 이러한 파일 전송을 탐지하거나 차단하려면 **Network Analysis Policy(**네트워크 분석 정책**)** > **TCP Stream Configuration(TCP** 스트림 구성**)** > **Troubleshooting Options(**문제해결 옵션**)** 아래에서 **Maximum Queued Bytes(**최대 대기열 바이트**)**와 **Maximum Queued Segments(**최대 대기열 세그먼트**)**의 값을 늘리는 것이 좋습니다.

파일 정책 모범 사례

파일 정책을 구성할 때 다음 지침 및 제한 사항에 유의하십시오.

- **Allow(**허용**)**, **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재시작**)**의 작업을 가진 액세스 제어 규칙과 단일 파일 정책을 연결할 수 있습니다.
- 액세스 기본 작업에 의해 처리된 트래픽을 파일 정책을 사용하여 검사할 수 없습니다.

- 새로운 정책의 경우, 웹 인터페이스에 정책이 사용 중이 아닌 것으로 표시됩니다. 사용 중인 파일 정책을 수정하는 경우, 해당 파일 정책을 사용 중인 액세스 제어 정책의 수가 웹 인터페이스에 표시됩니다. 어느 경우든 텍스트를 클릭하면 Access Control Policies(액세스 제어 정책) 페이지로 이동할 수 있습니다.
- FTP를 위한 **Block Malware(**악성코드 차단**)** 규칙을 비롯한 파일 정책을 사용하는 액세스 제어 정책의 경우, 기본 작업을 **Drop when Inline(**인라인 시 드롭**)**을 비활성화한 침입 정책으로 설정한 다면 시스템은 탐지된 파일 또는 규칙에 일치하는 악성코드를 위한 이벤트를 생성하지만 파일을 드롭하지 않습니다. FTP 파일 전송을 차단하고 침입 정책을 파일 정책을 선택하는 액세스 제어 정책의 기본 작업으로 사용하려면 반드시 침입 정책을 선택하고 **Drop when Inline(**인라인 시 드롭**)**을 활성화해야 합니다.
- 구성에 따라 시스템이 처음 탐지할 때 파일을 검사하고 클라우드 조회 결과를 기다리거나 클라우드 조회 결과를 기다리지 않고 이 첫 번째 탐지에서 파일을 전달할 수 있습니다.
- 기본적으로 암호화된 페이로드의 파일 검사를 비활성화합니다. 이는 암호화 연결이 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

악성코드 차단 설정 방법

이 항목에서는 악성 소프트웨어로부터 네트워크를 보호하기 위해 Firepower 시스템을 설정이라는 단계를 요약하여 설명합니다.

프로시저

단계 **1** 악성 코드 차단 계획 및 준비, 1867 페이지

단계 **2** 파일 정책 구성, 1868 페이지

단계 **3** 액세스 제어 구성에 파일 정책 추가, 1869 페이지

단계 **4** 파일 및 악성코드 이벤트를 네트워크의 호스트에 연결할 수 있도록 네트워크 검색 정책을 구성합니다.

(네트워크 검색을 설정하기만 해선 안 됩니다. 네트워크의 호스트를 검색해 조직의 네트워크 맵을 구축하도록 구성해야 합니다.)

네트워크 검색 정책, 2537 페이지 및 하위 항목을 참조하십시오.

단계 **5** 매니지드 디바이스에 정책을 구축합니다.

컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

단계 **6** 시스템을 테스트하여 악성 파일이 예상대로 처리되는지 확인합니다.

단계 **7** 악성코드 차단 유지 보수 및 모니터링 설정, 1870 페이지

다음에 수행할 작업

- (선택 사항) 네트워크상의 악성코드 탐지를 강화할 수 있도록, Cisco의 AMP for Endpoints 제품을 구축하고 통합합니다. (선택 사항) AMP for Endpoints를 사용한 악성코드 방지, 1896 페이지 및 하위 항목을 참조하십시오.
- 파일 및 악성코드 이벤트를 조사하는 방법을 확인합니다.

  파일/악성코드 이벤트 및 네트워크 파일 경로 분석, 2963 페이지의 내용을 참조하십시오.

악성 코드 차단 계획 및 준비

이 절차는 악성코드 차단을 제공하도록 시스템을 구성하는 전체 프로세스의 첫 번째 단계입니다.

프로시저

단계 **1** 라이선스 구입해 설치합니다.

파일 및 악성코드 정책을 위한 라이선스 요구 사항, 1863 페이지 및 Firepower System 라이선싱, 157 페이지를 참조하십시오.

단계 **2** 파일 정책과 악성코드 방지가 액세스 제어 계획에 어떻게 부합하는지 이해합니다.

액세스 제어의 이해, 1609 페이지 장을 참조하십시오.

단계 **3** 파일 분석 및 악성 코드 보호 도구를 확인합니다.

파일 규칙 작업, 1886 페이지 및 하위 항목을 참조하십시오.

고급 및 아카이브 파일 검사 옵션, 1880 페이지도 고려하십시오.

단계 **4** 악성코드 차단(파일 분석 및 동적 분석)에 퍼블릭 클라우드를 사용할지 프라이빗(온프레미스) 클라우드를 사용할지 결정합니다.

악성코드 차단을 위한 클라우드 연결, 1871 페이지 및 하위 항목을 참조하십시오.

단계 **5** 악성코드 차단을 위해 프라이빗(온프레미스) 클라우드를 사용한다면, 이러한 제품을 구입, 구축 및 테스트합니다.

자세한 내용은 Cisco 영업 담당자 또는 공인 대리점에 문의하십시오.

단계 **6** 선택한 클라우드와의 통신을 허용하도록 방화벽을 구성합니다.

보안, 인터넷 액세스 및 통신 포트, 3107 페이지의 내용을 참조하십시오.

단계 **7** Firepower와 악성코드 차단 클라우드(퍼블릭 또는 프라이빗) 간의 연결을 구성합니다.

- AMP 클라우드의 경우에는 AMP 옵션 변경, 1876 페이지의 내용을 참조하십시오.

- 온프레미스 Cisco Threat Grid 어플라이언스를 구축한 경우, 온프레미스 동적 분석 어플라이언스에 연결, 1878 페이지를 참조하십시오. (퍼블릭 Threat Grid 클라우드에 액세스하는 데는 구성이 필요하지 않습니다.)

다음에 수행할 작업

악성코드 차단 워크플로의 다음 단계를 계속 진행합니다.

악성코드 차단 설정 방법, 1866 페이지의 내용을 참조하십시오.

파일 정책 구성

시작하기 전에

악성코드 차단 워크플로의 이 단계까지 작업을 완료합니다.

악성코드 차단 설정 방법, 1866 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 파일 정책 및 파일 규칙 제한 사항을 검토합니다.

파일 정책 및 악성코드 탐지 모범 사례 , 1863 페이지 및 하위 항목을 참조하십시오.

단계 **2** 파일 정책을 생성합니다.

파일 정책을 생성하거나 수정합니다., 1880 페이지의 내용을 참조하십시오.

단계 **3** 파일 정책 내에 규칙을 생성합니다.

파일 규칙, 1885 페이지 및 하위 항목을 참조하십시오.

단계 **4** 고급 옵션을 구성합니다.

고급 및 아카이브 파일 검사 옵션, 1880 페이지의 내용을 참조하십시오.

다음에 수행할 작업

악성코드 차단 워크플로의 다음 단계를 계속 진행합니다.

악성코드 차단 설정 방법, 1866 페이지의 내용을 참조하십시오.

액세스 제어 구성에 파일 정책 추가

액세스 제어 정책에는 파일 정책과 연결된 여러 액세스 제어 규칙이 포함될 수 있습니다. 모든 Allow or Interactive Block (허용 또는 인터랙티브 차단) 액세스 제어 규칙에 대해 파일 검사를 구성할 수 있습니다. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크 상에 있는 다양한 유형의 트래픽에 대해 다양한 파일 및 악성코드 검사 프로파일과 맞춰볼 수 있습니다.

시작하기 전에

악성코드 차단 워크플로의 이 단계까지 작업을 완료합니다.

악성코드 차단 설정 방법, 1866 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 액세스 제어 정책의 파일 정책 지침을 검토합니다. (이것은 앞에서 살펴본 파일 규칙 및 파일 정책 지침과는 다릅니다.)

파일 및 침입 검사 순서, 1614 페이지를 검토합니다.

단계 **2** 파일 정책을 액세스 제어 정책에 연결합니다.

악성코드 보호를 수행하는 액세스 제어 규칙 구성, 1869 페이지의 내용을 참조하십시오.

단계 **3** 액세스 제어 정책을 매니지드 디바이스에 할당합니다.

액세스 제어 정책에 대한 대상 디바이스 설정, 1635 페이지의 내용을 참조하십시오.

다음에 수행할 작업

악성코드 차단 워크플로의 다음 단계를 계속 진행합니다.

악성코드 차단 설정 방법, 1866 페이지의 내용을 참조하십시오.

악성코드 보호를 수행하는 액세스 제어 규칙 구성

⚠

주의 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 Enabling or disabling **Store Files(**파일 저장 활성화 또는 비활성화**)**를 활성화하거나 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)** 또는 **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**), Unknown(**알 수 없음**), Clean(**정상**)** 또는 **Custom(**맞춤형**))**과 결합하는 첫 번째 파일 규칙을 추가하거나 마지막 파일 규칙을 제거, 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

참고 파일 정책이 액세스 제어 규칙에 포함되면 인라인 표준화가 자동으로 활성화됩니다. 자세한 내용은 인라인 정상화 전처리기, 2317 페이지를 참고하십시오.

시작하기 전에

- 액세스 제어 규칙이 AMP를 비롯한 파일 제어를 수행하기 위해서는 적응형 프로파일 구성, 2374 페이지에 설명된 것처럼 적응형 프로파일이 반드시 활성화되어 있어야 합니다.
- 이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자 사용자여야 합니다.

프로시저

단계 **1** 액세스 제어 규칙 편집기(**Policies(**정책**) > Access Control(**액세스 제어**))**에서 **Allow(**허용**)**, **Interactive Block(**인터랙티브 차단**)**, **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 중 **Action(**작업**)**을 선택합니다.

단계 **2** **Inspection(**검사**)**을 클릭합니다.

단계 **3** **File Policy(**파일 정책**)**를 선택하여 액세스 제어 규칙과 일치하는 트래픽을 검사하거나 **None(**없음**)**을 선택하여 일치하는 트래픽 파일 검사를 비활성화합니다.

단계 **4** (선택 사항) **Logging(**로깅**)**을 클릭하고 **Log Files(**로그 파일**)** 선택을 취소하여 일치하는 연결의 파일 또는 악성코드 이벤트 로깅을 비활성화합니다.

참고 Cisco는 파일 및 악성코드 이벤트 로깅 활성화를 유지하는 것을 권장합니다.

단계 **5** 규칙을 저장합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

파일 정책을 생성하거나 수정합니다., 1880 페이지
Snort® 재시작 시나리오, 505 페이지

악성코드 차단 유지 보수 및 모니터링 설정

네트워크를 보호하려면 지속적인 유지 관리가 필수입니다.

시작하기 전에

악성코드로부터 네트워크를 보호하도록 시스템을 구성합니다.

악성코드 차단 설정 방법, 1866 페이지 및 참조된 절차를 참조하십시오.

프로시저

단계 **1** 시스템이 유효한 최신 보호 수단을 항상 갖추고 있는지 확인합니다.

시스템 유지 관리: 동적 분석 대상인 파일 유형 업데이트, 1879 페이지의 내용을 참조하십시오.

단계 **2** 악성코드 관련 이벤트 및 상태 모니터링에 대한 알림을 구성합니다.

다음 모듈에 대해서는 AMP for Networks 알림 설정, 2689 페이지 및 상태 모니터링, 387 페이지의 정보를 참조하십시오.

- 로컬 악성코드 분석
- 보안 인텔리전스
- 디바이스에서 위협 데이터 업데이트
- 침입 및 파일 이벤트 비율
- AMP for Firepower 상태
- AMP for Endpoints 상태

다음에 수행할 작업

악성코드 차단 워크플로에서 'What to do next items(다음 작업 항목)'를 검토합니다.

악성코드 차단 설정 방법, 1866 페이지의 내용을 참조하십시오.

악성코드 차단을 위한 클라우드 연결

악성코드로부터 네트워크를 보호하려면 퍼블릭 또는 프라이빗 클라우드와의 연결이 필요합니다.

AMP 클라우드

Advanced Malware Protection(AMP) 클라우드는 Cisco가 호스팅하는 서버로서 빅 데이터 분석과 지속적 분석을 사용하여 시스템이 네트워크에서 악성코드 탐지와 차단에 사용하는 인텔리전스를 제공합니다.

AMP 클라우드는 매니지드 디바이스에 의해 네트워크 트래픽에서 탐지되는 잠재적 악성코드의 속성뿐 아니라 로컬 악성코드 분석 및 파일 사전 분류를 위한 데이터 업데이트도 제공합니다.

조직에서 AMP for Endpoints를 구축하고 그 데이터를 가져오도록 Firepower를 구성한 경우, 시스템은 AMP 클라우드에서 스캔 레코드, 악성코드 탐지, 격리, 보안 침해 지표(IOC) 등의 데이터를 가져옵니다.

Cisco에서는 Cisco Cloud에서 알려진 악성 코드 위협 관련 데이터를 얻는 다음과 같은 방법을 제공합니다.

- **AMP** 퍼블릭 클라우드

  Firepower Management Center은(는) 공용 Cisco Cloud와 직접 통신합니다. 미국, 유럽, 아시아에는 3가지 공용 AMP 클라우드가 있습니다.

- **AMP** 프라이빗 클라우드

  AMP 프라이빗 클라우드는 네트워크에 구축되며, 압축된 온프레미스 AMP 클라우드에 연결하는 익명화된 프록시 역할도 합니다. 자세한 내용은 Cisco AMP Private Cloud, 1874 페이지 섹션을 참조해 주십시오.

동적 분석 클라우드

- **Cisco Threat Grid** 클라우드

  퍼블릭 클라우드는 동적 분석을 위해 전달하는 적격 파일을 처리하고 위협 점수 및 동적 분석 보고서를 제공합니다.

- 온프레미스 **Cisco Threat Grid** 어플라이언스

  조직의 보안 정책에서 Firepower 시스템이 네트워크 외부로 파일을 전송하는 것을 허용하지 않는다면, 온프레미스 어플라이언스를 구축할 수 있습니다. 이 어플라이언스는 퍼블릭 Cisco Threat Grid 클라우드에 접속하지 않습니다.

  자세한 내용은 동적 분석 온프레미스 어플라이언스(Cisco Threat Grid), 1877 페이지를 참고하십시오.

AMP 및 **Threat Grid** 클라우드에 대한 연결 구성

- AMP 클라우드 연결 구성, 1872 페이지
- 동적 분석 연결, 1877 페이지

AMP 클라우드 연결 구성

다음 주제에서는 다양한 시나리오의 AMP 클라우드 연결 구성을 설명합니다.

- AMP 클라우드 선택, 1873 페이지
- AMP 프라이빗 클라우드에 연결, 1874 페이지
- Firepower와 AMP for Endpoints 통합, 1898 페이지

다음 주제는 다음과도 관련됩니다.

- Cisco AMP Private Cloud, 1874 페이지
- AMP 클라우드 연결 요구 사항 및 모범 사례, 1873 페이지

• (퍼블릭 또는 프라이빗) AMP 클라우드와의 연결 관리 , 1875 페이지

AMP 클라우드 연결 요구 사항 및 모범 사례

AMP 클라우드 연결 요구 사항

AMP 클라우드를 설정하려면 관리자 사용자여야 합니다.

FMC가 AMP 클라우드와 통신할 수 있는지 확인하려면 보안, 인터넷 액세스 및 통신 포트, 3107 페이지 아래 항목을 참조하십시오.

AMP 통신에 레거시 포트를 사용하려면 통신 포트 요구 사항, 3110 페이지를 참조하십시오.

AMP 클라우드 연결 및 멀티테넌시

다중 도메인 구축에서는 전역 수준에서만 AMP for Networks 연결을 구성합니다. 각 Firepower Management Center에는 하나의 AMP for Networks 연결만 있을 수 있습니다.

AMP 클라우드 선택

기본적으로 Firepower System에서는 미국(US) AMP 퍼블릭 클라우드와의 연결이 구성 및 활성화되어 있습니다. (이 연결은 웹 인터페이스에 AMP for Networks 로 표시되며 경우에 따라 AMP for Firepower 로 표시됩니다.) AMP for Networks 클라우드 연결을 삭제하거나 비활성할 수는 없지만, 서로 다른 지리적 AMP 클라우드 간에 전환하거나 AMP 프라이빗 클라우드 연결을 구성할수 있습니다.

시작하기 전에

- AMP 프라이빗 클라우드를 사용할 계획이라면 이 항목 대신 AMP 프라이빗 클라우드에 연결, 1874 페이지 항목을 참조하십시오.
- Firepower를 AMP for Endpoints와 통합하지 않으면, AMP 클라우드 연결은 하나만 구성할 수 있습니다. 이 연결은 **AMP for Networks** 또는 **AMP for Firepower**라고 표시됩니다.
- AMP for Endpoints를 구축했고 하나 이상의 AMP 클라우드를 추가해 해당 애플리케이션을 Firepower와 통합하고 싶다면, Firepower와 AMP for Endpoints 통합, 1898 페이지의 내용을 참조하십시오.
- AMP 클라우드 연결 요구 사항 및 모범 사례, 1873 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** 연필을 클릭하여 기존 클라우드 연결을 편집합니다.

단계 **3** **Cloud Name(**클라우드 이름**)** 드롭다운 목록에서 Firepower Management Center와(과) 가장 가까이에 있는 지역 클라우드를 선택합니다.

APJC는 아시아/태평양/일본/중국입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) AMP 옵션 변경, 1876 페이지.

Cisco AMP Private Cloud

Firepower Management Center는 네트워크 트래픽에서 탐지된 파일의 속성 쿼리와 회귀적 악성코드 이벤트 수신을 위해 AMP 클라우드에 연결해야 합니다. 이 클라우드는 퍼블릭 클라우드이거나 프라이빗 클라우드일 수 있습니다.

참고 AMP 프라이빗 클라우드는 동적 분석을 수행하지 않으며, URL 및 보안 인텔리전스 필터링 같이 Cisco Collective Security Intelligence(CSI)에 의존하는 그 밖의 기능을 위한 위협 인텔리전스의 익명화된 검색을 지원하지 않습니다.

AMP 프라이빗 클라우드("AMPv"라고도 함)에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html를 참조하십시오.

AMP 프라이빗 클라우드에 연결

시작하기 전에

- 제품 설명서의 지침에 따라 Cisco AMP 프라이빗 클라우드를 구성합니다. 구성 도중 프라이빗 클라우드 호스트 이름을 적어둡니다. Firepower Management Center에서 연결을 구성하려면 이 호스트 이름이 필요합니다.
- Firepower Management Center가 AMP 프라이빗 클라우드와 통신할 수 있는지 확인하고, 프라이빗 클라우드가 인터넷에 연결해 퍼블릭 AMP 클라우드와 통신할 수 있는지 확인합니다. 보안, 인터넷 액세스 및 통신 포트, 3107 페이지의 항목을 참조하십시오.
- 구축을 AMP for Endpoints와 통합하지 않으면, 각 Firepower Management Center에는 AMP 클라우드 연결을 하나만 구성할 수 있습니다. 이 연결은 **AMP for Networks** 또는 **AMP for Firepower**라고 표시됩니다.

  AMP for Endpoints와 통합한다면, 여러 AMP for Endpoints 클라우드 연결을 구성할 수 있습니다.

프로시저

단계 **1** **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** **Add AMP Cloud Connection(AMP** 클라우드 연결 추가**)**를 클릭합니다.

단계 **3** **Cloud Name(**클라우드 이름**)** 드롭다운 목록에서 **Private Cloud(**프라이빗 클라우드**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

이 정보는 AMP 프라이빗 클라우드에서 생성하거나 전송한 악성코드 이벤트에 표시됩니다.

단계 **5** **Host(**호스트**)** 필드에 프라이빗 클라우드를 설정할 때 구성한 프라이빗 클라우드 호스트 이름을 입력합니다.

단계 **6** **Certificate Upload Path(**인증서 업로드 경로**)**필드 옆의 **Browse(**찾아보기**)**를 클릭하여 프라이빗 클라우드의 유효한 TLS 또는 SSL 암호화 인증서가 있는 위치로 이동합니다. 자세한 내용은 AMP 프라이빗 클라우드 설명서를 참조하십시오.

단계 **7** AMP for Networks 와 AMP for Endpoints 모두에 프라이빗 클라우드를 사용하려는 경우, **Use for AMP for Firepower(AMP for Firepower**에 사용**)** 확인란을 선택합니다.

AMP for Networks 통신을 처리할 다른 프라이빗 클라우드를 구성한 경우에는 이 확인란 선택을 취소할 수 있지만 이것이 유일한 AMP 프라이빗 클라우드 연결이라면 선택을 취소할 수 없습니다.

다중 도메인 구축에서 이 확인란은 전역 도메인에만 표시됩니다. 각 Firepower Management Center에는 하나의 AMP for Networks 연결만 있을 수 있습니다.

단계 **8** 프록시를 사용하여 AMP 프라이빗 클라우드와 통신하려면 **Use Proxy for Connection(**연결에 프록시 사용**)** 확인란을 선택합니다.

단계 **9** **Register(**등록**)**를 클릭하고 AMP 클라우드와의 기존 직접 연결을 비활성화한다고 확인한 다음 마지막으로 등록 완료를 위해 AMP 프라이빗 클라우드 관리 콘솔로 이동한다고 확인합니다.

단계 **10** 관리 콘솔에 로그인하고 등록 프로세스를 완료합니다. 자세한 지침은 AMP 프라이빗 클라우드 설명서를 참조하십시오.

(퍼블릭 또는 프라이빗) AMP 클라우드와의 연결 관리

Firepower Management Center을 사용하여 AMP for Networks 또는 AMP for Endpoints 또는 둘 모두에 사용되는 퍼블릭 및 프라이빗 AMP 클라우드 연결을 관리합니다.

더 이상 클라우드에서 악성코드 관련 정보를 수신하지 않으려는 경우, 퍼블릭 또는 프라이빗 AMP 클라우드와의 연결을 삭제할 수 있습니다. AMP for Endpoints 또는 AMP 프라이빗 클라우드 관리 콘솔을 사용하여 연결 등록을 취소하더라도 해당 연결은 시스템에서 제거되지 않습니다. 등록 취소된 연결은 Firepower Management Center 웹 인터페이스에서 실패 상태를 표시합니다.

연결을 일시적으로 비활성화할 수도 있습니다. 클라우드 연결을 다시 활성화하는 경우, 클라우드는 비활성된 기간의 대기 중 데이터를 포함한 데이터를 시스템에 다시 전송하기 시작합니다.

주의 비활성화된 연결의 경우, 퍼블릭 또는 프라이빗 AMP 클라우드는 연결이 다시 활성화될 때까지 악성코드 이벤트, 보안 침해 지표 등을 저장할 수 있습니다. 예를 들어 이벤트 발생률이 매우 높거나 오랫동안 연결이 비활성화되는 드문 경우에는 연결이 비활성화된 동안 생성된 모든 정보를 클라우드에서 저장하지 못할 수도 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 연결을 표시하며 이러한 연결은 관리할 수 있습니다. 상위 도메인에서 생성된 연결도 표시되지만 이러한 연결은 관리할 수 없습니다. 하위 도메인의 연결을 관리하려면 해당 도메인으로 전환하십시오. 각 Firepower Management Center에는 전역 도메인에 속하는 하나의 AMP for Networks 연결만 있을 수 있습니다.

프로시저

단계 **1** **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** AMP 클라우드 연결 관리:

- 삭제 - 삭제( )을 클릭한 다음 선택 내용을 확인합니다.
- 활성화 또는 비활성화 - 슬라이더를 클릭한 다음 선택 내용을 확인합니다.

AMP 옵션 변경

프로시저

단계 **1** **System(**시스템**)** > **Integration(**통합**)**를 선택합니다.

단계 **2** **Cloud Services** 버튼을 클릭합니다.

단계 **3** 옵션을 선택합니다.

표 ***110: AMP for Networks*** 옵션

옵션	설명
자동 로컬 악성코드 탐지 업데이트 활성화	로컬 악성코드 탐지 엔진은 Cisco가 제공하는 서명을 사용하여 파일을 정적으로 분석하고 사전 분류합니다. 이 옵션을 활성화하면 Firepower Management Center는 30분마다 서명 업데이트를 확인합니다.
악성코드 이벤트의 URI를 Cisco와 공유	시스템은 네트워크 트래픽에서 탐지된 파일에 대한 정보를 AMP 클라우드로 전송할 수 있습니다. 이러한 정보에는 탐지된 파일 및 SHA-256 해시 값과 관련된 URI 정보가 포함됩니다. 공유는 선택 사항이지만 이러한 정보를 Cisco에 전송하면 추후에 악성코드를 식별하고 추적하는 데 도움이 됩니다.
레거시 포트 32137 사용 AMP for Networks	기본적으로 Firepower는 포트 443/HTTPS를 통해 AMP 퍼블릭 또는 프라이빗 클라우드와 통신하여 파일 속성 데이터를 가져옵니다. 시스템은 이 옵션을 통해 포트 32137을 사용할 수 있습니다. 시스템의 이전 버전에서 업데이트하는 경우, 이 옵션이 활성화될 수 있습니다. FMC가 프록시 설정으로 구성된 경우, 이 옵션은 회색으로 표시됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

동적 분석 연결

동적 분석 요구 사항

동적 분석을 사용하려면 Admin, Access Admin 또는 Network Admin 사용자여야 하며 전역 도메인에 있어야 합니다.

Firepower System은 적절한 라이선스를 사용하여 자동으로 Cisco Threat Grid 퍼블릭 클라우드에 액세스합니다.

동적 분석을 수행하려면 매니지드 디바이스가 포트 443에서 Cisco Threat Grid 퍼블릭 클라우드 또는 온프레미스 Cisco Threat Grid 어플라이언스에 직접 또는 프록시를 통해 액세스할 수 있어야 합니다.

어떤 파일이 동적 분석에 적합합니까?, 1891 페이지도 참조하십시오.

온 프레미스 Threat Grid 어플라이언스에 연결할 계획이라면, 온프레미스 동적 분석 어플라이언스에 연결, 1878 페이지에서 설명하는 전제 조건도 참조하십시오.

기본 동적 분석 연결 보기

기본적으로 Firepower Management Center는 파일 제출 및 보고서 검색을 위해 퍼블릭 Cisco Threat Grid 클라우드에 연결할 수 있습니다. 이 연결은 구성하거나 삭제할 수 없습니다.

프로시저

단계 **1** **AMP** > **Dynamic Analysis Connections(**동적 분석 연결**)**을(를) 선택합니다.

단계 **2** 수정( ) 버튼을 클릭합니다.

동적 분석 온프레미스 어플라이언스**(Cisco Threat Grid)**

퍼블릭 Cisco Threat Grid 클라우드에 파일을 제출하는 것과 관련된 개인 정보 보호 또는 보안 우려가 조직에 있는 경우, 온프레미스 Cisco Threat Grid 어플라이언스를 구축할 수 있습니다. 온프레미스 어플라이언스는 퍼블릭 클라우드와 마찬가지로 샌드박스 환경에서 적격 파일을 실행하고 위협 점수와 동적 분석 보고서를 Firepower System에 반환합니다. 다만 온프레미스 어플라이언스는 퍼블릭 클라우드 또는 네트워크 외부의 다른 시스템과 통신하지 않습니다.

온프레미스 Cisco Threat Grid 어플라이언스에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/threat-grid/index.html를 참조하십시오.

온프레미스 동적 분석 어플라이언스에 연결

온프레미스 Cisco Threat Grid 어플라이언스를 네트워크에 설치하면 동적 분석 연결을 구성하여 파일을 제출하고 어플라이언스에서 보고서를 가져올 수 있습니다. 온프레미스 어플라이언스 동적 분석 연결을 구성할 때 Firepower Management Center를 온프레미스 어플라이언스에 등록합니다.

시작하기 전에

- 온프레미스 Cisco Threat Grid 어플라이언스를 설정합니다. *Cisco Threat Grid Appliance* 설정 및 구성 설명서를 참조하십시오.

  이 어플라이언스의 설명서는 https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html에서 구할 수 있습니다.

  버전 요구 사항은 *Cisco Firepower* 호환성 가이드를 참조하십시오.

- 온프레미스 어플라이언스에 로그인하는 데 사용할 공개 키 인증서를 Cisco Threat Grid 어플라이언스에서 다운로드합니다. 자세한 내용은 *Cisco Threat Grid Appliance* 관리자 가이드를 참조하십시오.

  CA(Certificate Authority)에서 서명한 인증서를 사용하는 경우 인증서는 다음 요구 사항을 충족해야 합니다.

  - 서버 키 및 서명된 인증서는 Threat Grid Appliance에 설치해야 합니다. *Threat Grid* 관리자 가이드의 업로드 지침을 따릅니다.
  - CA의 다중 레벨 서명 체인이 있는 경우 모든 필수 중간 인증서 및 루트 인증서가 FMC에 업로드될 단일 파일에 포함되어야 합니다.
  - 모든 인증서는 PEM으로 인코딩되어야 합니다.
  - 파일의 줄 바꿈은 DOS가 아닌 UNIX여야 합니다.

- 프록시를 사용하여 온프레미스 어플라이언스에 연결하려면 프록시를 구성합니다(FMC 관리 인터페이스 수정, 1358 페이지 참조).
- 매니지드 디바이스는 포트 443에서 Cisco Threat Grid 어플라이언스에 직접 또는 프록시를 경유하여 액세스할 수 있어야 합니다

프로시저

단계 **1** **AMP** > **Dynamic Analysis Connections(**동적 분석 연결**)**을(를) 선택합니다.

단계 **2** **Add New Connection(**새 연결 추가**)**을 클릭합니다.

단계 **3** **Name(**이름**)**을 입력합니다.

단계 **4** **Host URL(**호스트 **URL)**을 입력합니다.

단계 **5** **Certificate Upload(**인증서 업로드**)** 옆의 **Browse(**찾아보기**)**를 클릭하여 온프레미스 어플라이언스와의 연결 설정에 사용할 퍼블릭 키 인증서를 업로드합니다.

Threat Grid Appliance가 자체 서명 인증서를 제시할 경우, 해당 어플라이언스에서 다운로드한 인증서를 업로드합니다.

Threat Grid Appliance가 CA 서명 인증서를 제시할 경우, 인증서 서명 체인을 포함하는 파일을 업로드합니다.

단계 **6** 구성된 프록시를 사용하여 연결을 설정하려면 **Use Proxy When Available(**사용 가능한 경우 프록시 사용**)**를 선택합니다.

단계 **7** **Register(**등록**)**를 클릭합니다.

단계 **8** **Yes(**예**)**를 클릭하여 온프레미스 Cisco Threat Grid 어플라이언스 로그인 페이지를 표시합니다.

단계 **9** 온프레미스 Cisco Threat Grid 어플라이언스에 사용자 이름과 암호를 입력합니다.

단계 **10** **Sign in(**로그인**)**을 클릭합니다.

단계 **11** 다음 옵션을 이용할 수 있습니다.

- 이전에 Firepower Management Center를 온프레미스 어플라이언스에 등록했다면 **Return(**돌아가기**)**을 클릭합니다.
- Firepower Management Center를 등록하지 않았다면 **Activate(**활성화**)**를 클릭합니다.

시스템 유지 관리: 동적 분석 대상인 파일 유형 업데이트

동적 분석 대상 파일 유형 목록은 주기적으로 업데이트되는(단, 하루에 한 번 이상 업데이트되지 않음) 취약성 데이터베이스(VDB)에 의해 결정됩니다. 관리자인 경우 동적 분석에 적합한 파일 유형을 업데이트할 수 있습니다.

시스템에 최신 목록이 있는지 확인하려면

프로시저

단계 **1** 다음 중 하나를 수행합니다.

- (권장) 다음을 참조하십시오. 취약성 데이터베이스 업데이트 자동화, 260 페이지
- 새 VDB 업데이트를 정기적으로 확인하고 필요한 경우, VDB 수동 업데이트, 182 페이지합니다.

  이 옵션을 선택하는 경우, 이 작업을 수행하도록 정기적인 미리 알림을 예약하는 것이 좋습니다.

단계 **2** 파일 정책에서 **Dynamic Analysis Capable(**동적 분석 가능**)** 파일 유형 카테고리 대신 개별 파일 유형이 지정된 경우, 새로 지원되는 파일 유형을 사용할 수 있도록 파일 정책을 업데이트합니다.

단계 **3** 동적 분석 대상 파일 유형 목록이 변경되는 경우, 매니지드 디바이스에 이 목록을 구축합니다.

파일 정책 및 파일 규칙

파일 정책을 생성하거나 수정합니다.

시작하기 전에

악성 코드 보호를 위한 정책을 구성한다면 파일 정책 구성, 1868 페이지에서 모든 필수 절차를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)** 을(를) 선택합니다.

단계 **2** 새 정책을 만들거나 기존 정책을 편집합니다.

기존 정책을 수정하는 경우: 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

팁 기존 파일 정책의 복사본을 만들려면 복사 ( )을 클릭한 다음 표시되는 대화 상자에서 새로운 정책의 고유한 이름을 입력합니다. 그러면 복사본을 수정할 수 있습니다.

단계 **3** 파일 규칙 생성, 1894 페이지에 설명된 것처럼 파일 정책에 하나 이상의 규칙을 추가합니다.

단계 **4** 아니면 Advanced(고급) 탭을 선택하고 고급 및 아카이브 파일 검사 옵션, 1880 페이지에 설명된 것처럼 고급 옵션을 구성합니다.

단계 **5** 파일 정책을 저장합니다.

다음에 수행할 작업

- 악성 코드 보호를 위한 정책을 구성한다면 파일 정책 구성, 1868 페이지에서 다른 필수 절차를 참조하십시오.
- 그렇지 않을 경우,
  - 액세스 제어 구성에 파일 정책 추가, 1869 페이지에 설명된 것처럼 액세스 제어 규칙에 파일 정책을 추가합니다.
  - 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

고급 및 아카이브 파일 검사 옵션

파일 정책 편집기의 Advanced(고급) 설정에는 다음과 같은 일반 옵션이 있습니다.

- **First Time File Analysis(**최초 파일 분석**)** - AMP 클라우드 처리가 보류 중인 동안 처음 보는 파일을 분석하려면 이 옵션을 선택합니다. 악성코드 클라우드 조회 및 Spero 분석, 로컬 악성코드 분석 또는 동적 분석을 수행하려면 구성된 규칙과 파일이 일치해야 합니다. 이 옵션을 선택 취소하면 처음으로 탐지된 파일이 Unknown(알 수 없음) 속성으로 표시됩니다.
- **Enable Custom Detection List(**맞춤형 탐지 목록 활성화**)** - 맞춤형 탐지 목록에 있는 파일을 차단합니다.
- **Enable Clean List(**클린 목록 활성화**)** - 이 정책을 활성화하면 클린 목록에 있는 파일이 허용됩니다.
- **AMP** 클라우드 속성이 알 수 없음인 경우 위협 점수를 기준으로 속성을 재정의합니다**.** - 옵션 선택:
  - **Disabled(**비활성화됨**)**를 선택한 경우, 시스템은 AMP 클라우드에서 제공한 속성을 재정의하지 않습니다.
  - 한계치 위협 점수를 설정한 경우 동적 분석 점수가 한계치와 같거나 이보다 나쁘면 AMP 클라우드가 알 수 없음으로 판정된 파일은 악성코드로 간주됩니다.
  - 낮은 임계값을 선택하면 악성코드로 처리되는 파일 수가 늘어납니다. 파일 정책에서 선택한 작업에 따라서는 이렇게 할 경우, 차단되는 파일의 수가 늘어날 수 있습니다.
  - 숫자 위협 점수 범위는 위협 점수 및 동적 분석 요약 보고서, 2984 페이지의 내용을 참조하십시오.

파일 정책 편집기의 Advanced(고급) 설정에는 다음과 같은 아카이브 파일 검사 옵션이 있습니다.

- **Inspect Archives(**아카이브 검사**) - Maximum file size to store(**최대 저장 파일 크기**)** 고급 액세스 제어 설정만큼 큰 아카이브 파일의 경우, 아카이브 파일의 내용 검사를 활성화합니다.
- **Block Encrypted Archives(**암호화된 아카이브 차단**)** - 암호화된 내용이 있는 아카이브 파일을 차단합니다.
- **Block Uninspectable Archives(**검사할 수 없는 아카이브 차단**)** - 암호화 이외의 이유로 시스템이 검사할 수 없는 내용이 있는 아카이브 파일을 차단합니다. 이것은 일반적으로 손상된 파일이나 지정된 최대 아카이브 깊이를 초과하는 파일에 적용됩니다.
- **Max Archive Depth(**최대 아카이브 깊이**)** - 지정된 깊이를 초과하는 중첩된 아카이브 파일을 차단합니다. 최상위 아카이브 파일은 이 계산에서 고려되지 않으며, 깊이는 처음 중첩된 파일을 기점으로 1부터 시작합니다.

아카이브 파일

아카이브 파일이란 `.zip` 또는 `.rar` 파일처럼 다른 파일을 포함하는 파일입니다.

아카이브에 있는 개별 파일이 차단 작업이 포함된 파일 규칙과 일치하는 경우, 시스템은 개별 파일만이 아니라 전체 아카이브를 차단합니다.

아카이브 파일 검사 옵션에 대한 자세한 내용은 고급 및 아카이브 파일 검사 옵션, 1880 페이지를 참조하십시오.

검사할 수 있는 아카이브 파일

- 파일 유형

  검사할 수 있는 아카이브 파일 유형의 전체 목록은 FMC 웹 인터페이스 파일 규칙 구성 페이지에 나와 있습니다. 해당 페이지를 보려면 파일 규칙 생성, 1894 페이지를 참조하십시오.

  검사할 수 있는 포함된 파일도 같은 페이지에 표시됩니다.

- 파일 크기

  Maximum file size to store(최대 저장 파일 크기**)** 파일 정책 고급 액세스 제어 설정만큼 큰 아카이브 파일을 검사할 수 있습니다.

- 중첩된 아카이브

  아카이브 파일에는 다른 아카이브 파일이 포함될 수 있고, 이 아카이브 파일에도 아카이브 파일이 포함될 수 있습니다. 파일이 중첩되는 수준이 아카이브 파일 깊이입니다. 최상위 아카이브 파일은 깊이 계산에 포함되지 않으며, 깊이는 처음 중첩된 파일을 기점으로 1부터 시작합니다.

  시스템은 가장 바깥의 아카이브 파일(수준 0) 아래 있는 중첩된 파일을 3개 수준까지 검사할 수 있습니다. 이 깊이(또는 사용자가 지정하는 이보다 낮은 최대 깊이)를 초과하는 아카이브 파일을 차단하도록 파일 정책을 구성할 수 있습니다.

  최대 아카이브 파일 깊이인 3을 초과하는 파일을 차단하지 않도록 선택하는 경우, 추출 가능한 일부 내용과 3 이상의 깊이에서 중첩된 일부 내용을 포함하는 아카이브 파일이 모니터링되는 트래픽에 나타나면 시스템은 검사 가능한 파일의 데이터만 검사하고 보고합니다.

  압축되지 않은 파일에 적용 가능한 모든 기능(예: 동적 분석 및 파일 저장)은 아카이브 파일 내부의 중첩된 파일에도 사용할 수 있습니다.

- 암호화된 파일

  내용이 암호화되거나 그 밖에 검사할 수 없는 아카이브 파일을 차단하도록 시스템을 구성할 수 있습니다.

- 검사되지 않는 아카이브

  보안 인텔리전스 차단 또는 차단 금지 목록에 추가된 아카이브 파일이 트래픽에 포함되어 있거나 최상위 아카이브 파일의 SHA-256 값이 맞춤형 탐지 목록에 있는 경우 시스템은 아카이브 파일의 내용을 검사하지 않습니다.

  중첩된 파일이 차단되면 전체 아카이브가 차단됩니다. 하지만 중첩된 파일이 허용되더라도 아카이브가 자동으로 통과되지는 않습니다(다른 중첩된 파일 및 특성에 따라 달라짐).

  rar5를 포함하여 일부 .rar 아카이브 내의 .Exe 파일을 검색할 수 없습니다.

아카이브 파일 속성

아카이브 파일 속성은 아카이브 내부의 파일에 할당된 속성을 기준으로 합니다. 식별된 악성코드 파일을 포함하는 모든 아카이브에는 `Malware`라는 속성이 제공됩니다. 식별된 악성코드 파일이 없는 아카이브의 경우, 알 수 없는 파일이 포함되어 있으면 `Unknown`이라는 속성이 제공되고, 안전한 파일만 포함되어 있으면 `Clean`이라는 속성이 제공됩니다.

표 *111:* 내용별 아카이브 파일 속성

아카이브 파일 속성	알 수 없는 파일 수	안전한 파일 수	악성코드 파일 수
알 수 없음	1개 이상	Any(모든)	0
정상	0	1개 이상	0
악성코드	Any(모든)	Any(모든)	1개 이상

다른 파일과 마찬가지로 아카이브 파일은 `Custom Detection` 또는 `Unavailable` 속성의 조건이 적용될 경우, 해당 속성을 가질 수 있습니다.

아카이브 내용 및 세부 정보 보기

아카이브 파일 내용을 검사하도록 파일 정책을 구성할 경우, Analysis(분석) > Files(파일) 메뉴 아래 테이블의 컨텍스트 메뉴 및 네트워크 파일 전파 흔적 분석 뷰어를 사용하면 아카이브 파일이 파일 이벤트, 악성코드 이벤트에 표시되거나 캡처 파일로 표시될 때 아카이브 내부의 파일에 대한 정보를 볼 수 있습니다.

아카이브의 모든 파일 내용은 테이블 형식으로 나열되며, 관련 정보(이름, SHA-256 해시 값, 유형, 카테고리, 아카이브 깊이)가 짧게 요약되어 있습니다. 네트워크 파일 전파 흔적 분석 아이콘은 각 파일 옆에 표시되며, 클릭하면 해당 특정 파일에 대한 추가 정보를 볼 수 있습니다.

맞춤형 목록을 사용한 파일 속성 재정의

AMP 클라우드의 파일에 잘못된 속성이 있는 경우, 클라우드의 속성을 재정의하는 파일의 SHA-256 값을 파일 목록에 추가할 수 있습니다.

- AMP 클라우드가 안전 속성을 할당한 것처럼 파일을 처리하려면 파일을 안전 목록에 추가합니다.
- AMP 클라우드가 악성코드 속성을 할당한 것처럼 파일을 처리하려면 파일을 맞춤형 탐지 목록에 추가합니다.

후속 탐지 시 디바이스는 파일의 속성을 다시 평가하지 않고 파일을 허용하거나 차단합니다. 파일 정책별로 안전 목록 또는 맞춤형 탐지 목록을 사용할 수 있습니다.

참고 파일의 SHA-256 값을 계산하려면 파일 정책에서 규칙을 구성하여 악성코드 클라우드 조회를 수행하거나 일치하는 파일의 악성코드를 차단해야 합니다.

Firepower에서 파일 목록을 사용하는 방법에 대한 자세한 내용은 파일 목록, 610 페이지를 참조하십시오.

파일 정책 관리

File Policies(파일 정책) 페이지에는 기존 파일 정책의 목록이 최종 수정 날짜와 함께 표시됩니다. 이 페이지를 사용하여 파일 정책을 관리할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

참고 시스템에서는 동적 분석에 적합한 파일 유형의 목록이 업데이트되었는지 확인합니다(하루에 한 번만 수행). 적합한 파일 유형 목록이 변경되면 파일 정책이 변경됩니다. 해당 파일 정책을 사용하는 모든 액세스 제어 정책은 디바이스에 구축되는 경우, 기한이 지난 것으로 표시됩니다. 업데이트된 파일 정책이 디바이스에 적용되려면 먼저 정책을 구축해야 합니다. 시스템 유지 관리: 동적 분석 대상인 파일 유형 업데이트, 1879 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)** 을(를) 선택합니다.

단계 **2** 파일 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교, 514 페이지를 참조하십시오.
- 생성 - 파일 정책을 생성하려면 **New File Policy(**새 파일 정책**)**를 클릭하고 파일 정책을 생성하거나 수정합니다., 1880 페이지에 설명된 대로 진행합니다.
- 복사 - 파일 정책을 복사하려면 복사 ( )을 클릭합니다.

  보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - 파일 정책을 삭제하려면 삭제( )을 클릭한 다음 표시되는 메시지에 따라 **Yes(**예**)** 및 **OK(**확인**)**를 클릭합니다.

  컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- 수정 - 기존 파일 정책을 수정하려면 수정( )을 클릭합니다.
- 보고서- 보고서( )를 클릭합니다. 현재 정책 보고서 생성, 515 페이지를 참조하십시오.

파일 규칙

상위 액세스 제어 정책과 마찬가지로, 파일 정책에는 각 규칙의 조건과 일치하는 파일을 처리하는 방식을 결정하는 규칙이 포함됩니다. 별도의 파일 규칙을 구성하여 각기 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향마다 다른 작업을 실행할 수 있습니다.

예를 들어 파일이 규칙과 일치할 경우, 규칙은 다음을 수행할 수 있습니다.

- 간단한 파일 유형 일치를 기준으로 파일 허용 또는 차단
- 처리(평가에서 악성임이 나타나는지의 여부)를 기준으로 파일 차단
- 디바이스에 파일 저장 (자세한 내용은 참조 캡처된 파일 및 파일 스토리지, 1892 페이지)
- 로컬 악성코드 분석, Spero 분석 또는 동적 분석을 위해 저장(캡처)된 파일 제출

또한 파일 정책으로 다음을 수행할 수 있습니다.

- 정상 목록 또는 맞춤형 탐지 목록의 항목을 기준으로 파일을 안전한 파일 또는 악성코드로 자동 처리
- 파일의 위협 점수가 구성 가능한 임계값을 초과할 경우 파일을 악성코드로 처리
- `.zip` 또는 `.rar` 같은 아카이브 파일의 내용 검사
- 내용이 암호화되거나 지정된 최대 보관 깊이를 넘어 중첩되거나 그 밖에 검사할 수 없는 아카이브 파일을 차단

파일 규칙 구성 요소

표 ***112:*** 파일 규칙 구성 요소

파일 규칙 구성 요소	설명
애플리케이션 프로토콜:	시스템에서는 FTP, HTTP, SMTP, IMAP, POP3, NetBIOS-ssn(SMB)을 통해 전송된 파일을 탐지하고 검사할 수 있습니다. 기본값인 **Any(**모두**)**는 HTTP, SMTP, IMAP, POP3, FTP 및 NetBIOS-ssn(SMB) 트래픽에서 파일을 탐지합니다. 성능 향상을 위해 파일별 규칙을 기반으로 한 애플리케이션 프로토콜 중 하나만 대상으로 하여 파일 탐지를 제한할 수 있습니다.
전송 방향	다운로드한 파일에 대해 수신 FTP, HTTP, POP3, IMAP 및 NetBIOS-ssn(SMB) 트래픽을 검사할 수 있으며, 업로드한 파일에 대해서는 발신 FTP, HTTP, SMTP 및 NetBIOS-ssn(SMB) 트래픽을 검사할 수 있습니다. 팁 사용자가 전송하는지 또는 수신하는지에 상관없이, **Any(**모두**)**를 사용하여 여러 애플리케이션 프로토콜에서 파일을 탐색합니다.

파일 규칙 구성 요소	설명
파일 카테고리 및 유형	시스템에서는 다양한 유형의 파일을 탐지할 수 있습니다. 이러한 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent), PDF를 비롯한 기본적인 카테고리로 그룹화됩니다. 개별 파일 유형을 탐지하거나, 파일 유형의 전체 카테고리를 탐지하는 파일 규칙을 구성할 수 있습니다. 예를 들어, 모든 멀티미디어 파일을 차단할 수도 있고, ShockWave Flash(swf) 파일만 차단할 수도 있습니다. 또는 사용자가 BitTorrent(torrent) 파일을 다운로드할 경우 알림을 제공하도록 시스템을 구성할 수 있습니다. 실행 파일은 악성코드가 포함될 수 있으므로 매크로 및 스크립트를 실행할 수 있는 파일 유형으로 구성됩니다. 시스템이 검사할 수 있는 파일 유형 목록의 경우, **Policies(**정책**) > Access Control(**액세스 제어**) > Malware & File(**악성코드 및 파일**)**을 선택하고 임시 새 파일 정책을 생성한 다음 **Add Rule(**규칙 추가**)**를 클릭합니다. 파일 유형 카테고리를 선택하면 시스템이 검사할 수 있는 파일 유형이 **File Types(**파일 유형**)** 목록에 나타납니다. 참고 빈번하게 트리거되는 파일 규칙은 시스템 성능에 영향을 줄 수 있습니다. 예를 들어, HTTP 트래픽(예: 상당량의 Flash 콘텐츠를 전송하는 YouTube)의 멀티미디어 파일을 탐지할 경우 지나치게 많은 이벤트가 생성될 수 있습니다.
파일 규칙 작업	파일 규칙 작업에서는 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정합니다. 선택한 작업에 따라 시스템이 파일을 저장할지 또는 파일에서 Spero, 로컬 악성코드 또는 동적 분석을 수행할지 구성할 수 있습니다. 차단 작업을 선택하는 경우, 시스템이 차단된 연결을 재설정하는지도 구성할 수 있습니다. 이러한 작업과 옵션에 대한 설명은 파일 규칙 작업, 1886 페이지를 참조하십시오. 파일 규칙은 숫자나 순서가 아닌 규칙 작업으로 평가됩니다. 자세한 내용은 파일 규칙 작업: 평가 순서, 1894 페이지를 참조하십시오.

파일 규칙 작업

파일 규칙은 악성코드 탐지를 위해 어떤 파일 유형을 로깅하거나, 차단, 확인하기를 원하는지에 대해 세분화된 제어 기능을 제공합니다. 각 파일 규칙에는 시스템이 규칙의 조건과 일치하는 트래픽을 처

리하는 방법을 결정하는 관련 작업이 포함됩니다. 파일 정책은 하나 이상의 규칙을 포함해야 적용할 수 있습니다. 파일 정책 내에서 별도의 규칙을 사용하여 서로 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향에 맞는 다양한 작업을 실행할 수 있습니다.

파일 규칙 작업

- *Detect Files(*파일 탐지*)* 규칙을 사용하면 데이터베이스에 특정 파일 유형의 탐지를 로깅할 수 있지만 여전히 해당 전송을 허용합니다.
- *Block Files(*파일 차단*)* 규칙을 사용하면 특정 파일 유형을 차단할 수 있습니다. 파일 전송이 차단되었을 때 연결을 재설정하는 옵션을 구성하고 캡처된 파일을 매니지드 디바이스에 저장할 수 있습니다.
- *Malware Cloud Lookup(*악성코드 클라우드 조회*)* 규칙을 사용하면 네트워크를 통과하는 파일의 속성을 가져오고 로깅하면서 전송을 허용할 수 있습니다.
- *Block Malware(*악성코드 차단*)* 규칙을 사용하면 특정 파일 유형의 SHA-256 해시 값을 계산하고 AMP 클라우드를 조회하여 네트워크를 통과하는 파일이 악성코드를 포함하는지 확인한 다음 위협을 나타내는 파일을 차단할 수 있습니다.

파일 규칙 작업 옵션

선택하는 작업에 따라 여러 옵션이 있습니다.

파일 규칙 작업 옵션	파일 차단 가능?	악성 코드 차단 가능?	파일 탐지 가능?	악성코드 클라우드 조회 가능?
MSEXE의 Spero 분석*	아니요	예, 실행 파일을 제출할 수 있음	아니요	예, 실행 파일을 제출할 수 있음
동적 분석*	아니요	예, 파일 속성이 Unknown인 실행 파일을 제출할 수 있음	아니요	예, 파일 속성이 Unknown인 실행 파일을 제출할 수 있음
용량 처리	아니요	예	아니요	예
로컬 악성코드 분석*	아니요	예	아니요	예
연결 재설정	예(권장)	예(권장)	아니요	아니요
파일 저장	예, 일치하는 모든 파일 유형을 저장할 수 있음	예, 선택한 파일 속성과 일치하는 파일 유형을 저장할 수 있음	예, 일치하는 모든 파일 유형을 저장할 수 있음	예, 선택한 파일 속성과 일치하는 파일 유형을 저장할 수 있음

* 이러한 옵션에 대한 자세한 내용은 (파일 규칙 작업의) 악성코드 차단 옵션, 1888 페이지 및 하위 항목을 참조하십시오.

주의 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 Enabling or disabling **Store Files(**파일 저장 활성화 또는 비활성화**)**를 활성화하거나 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)** 또는 **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**), Unknown(**알 수 없음**), Clean(**정상**)** 또는 **Custom(**맞춤형**))**과 결합하는 첫 번째 파일 규칙을 추가하거나 마지막 파일 규칙을 제거, 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

(파일 규칙 작업의) 악성코드 차단 옵션

Firepower System은 여러 파일 검사 및 분석 방법을 사용하여 파일에 악성코드가 포함되어 있는지 확인합니다.

파일 규칙에서 활성화한 옵션에 따라 시스템은 다음 도구를 다음 순서로 사용하여 파일을 검사합니다.

1. Spero 분석, 1890 페이지 및 AMP 클라우드 조회, 1890 페이지
2. 로컬 악성코드 분석, 1890 페이지
3. 동적 분석, 1891 페이지

이러한 도구를 비교하려면 악성코드 차단 옵션 비교, 1888 페이지를 참조하십시오.

(원하는 경우, 파일 유형에 따라 모든 파일을 차단할 수도 있습니다. 자세한 내용은 유형별로 모든 파일 차단, 1894 페이지를 참고하십시오.

(선택 사항) AMP for Endpoints를 사용한 악성코드 방지, 1896 페이지 및 하위 항목에서 Cisco의 AMP for Endpoints 제품에 대한 정보도 참조하십시오.

악성코드 차단 옵션 비교

다음 표에서는 각 파일 분석 유형의 장단점과 각 악성코드 방지 방법이 파일 속성을 결정하는 방식을 자세히 설명합니다.

분석 유형	이점	제한 사항	악성코드 식별
Spero 분석	실행 파일의 구조 분석으로서 분석을 위해 Spero 서명을 AMP 클라우드로 전송	로컬 악성코드 분석 또는 동적 분석보다 덜 정밀하며 실행 파일만 분석	악성코드로 확인되는 경우에만 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.

분석 유형	이점	제한 사항	악성코드 식별
로컬 악성코드 분석	동적 분석보다 적은 리소스를 사용하며, 특히 탐지된 악성코드가 일반적인 경우, 결과를 보다 빨리 반환합니다.	동적 분석보다 덜 정밀한 결과	악성코드로 확인되는 경우에만 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
동적 분석	다음을 사용하여 알 수 없는 파일을 정밀 분석 Cisco Threat Grid	적격 파일은 퍼블릭 클라우드 또는 현장 어플라이언스에 업로드됩니다. 분석을 완료하는 데 시간이 소요됩니다	위협 점수는 파일의 악성 정도를 결정합니다. 속성은 파일 정책에서 구성된 위협 점수 임계값에 기반을 둘 수 있습니다.
Spero 분석 및 로컬 악성코드 분석	로컬 악성코드 분석 및 동적 분석 구성보다 적은 리소스를 사용하면서 AMP 클라우드를 사용하여 악성코드를 식별합니다	동적 분석보다 덜 정밀하며 Spero 분석은 실행 파일만 분석합니다	악성코드로 확인되는 경우에만 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
Spero 분석 및 동적 분석	파일 및 Spero 서명 제출에 AMP 클라우드의 모든 기능 사용	로컬 악성코드 분석을 사용하는 경우보다 결과를 얻는 속도가 느림	가능한 악성코드로 사전 분류된 파일에 대한 동적 분석 결과에 따라 위협 점수가 변경됩니다. 파일 정책에서 구성된 위협 점수 임계값에 따라 속성이 변경되며, Spero 분석이 악성코드를 식별하면 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
로컬 악성코드 분석 및 동적 분석	두 가지 파일 분석 유형 사용시 정밀한 결과	하나만 사용하는 것보다 많은 리소스를 사용	가능한 악성코드로 사전 분류된 파일에 대한 동적 분석 결과에 따라 위협 점수가 변경됩니다. 로컬 악성코드 분석에서 악성코드를 식별하는 경우, 또는 파일 정책에서 구성된 위협 점수 임계값에 따라 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.

분석 유형	이점	제한 사항	악성코드 식별
Spero 분석, 로컬 악성코드 분석, 동적 분석	가장 정밀한 결과	세 가지 유형의 파일 분석을 모두 실행 시 가장 많은 리소스 사용	가능한 악성코드로 사전 분류된 파일에 대한 동적 분석 결과에 따라 위협 점수가 변경됩니다. Spero 분석이나 로컬 악성코드 분석에서 악성코드를 식별하는 경우, 또는 파일 정책에서 구성된 위협 점수 임계값에 따라 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
(지정된 파일 유형의 모든 파일 전송을 차단)	악성코드 라이선스가 필요하지 않습니다. (이 옵션은 기술적으로 악성코드 방지 옵션이 아닙니다.)	적법한 파일도 차단됩니다.	(분석이 수행되지 않습니다.)

참고 사전 분류 자체는 파일의 속성을 확인하지 않으며, 파일이 동적 분석에 적합한지 결정하는 요소 중 하나일 뿐입니다.

Spero 분석

Spero 분석은 실행 파일의 메타데이터 및 헤더 정보와 같은 구조적 특성을 검사합니다. 이 정보를 기반으로 Spero 서명을 생성한 후 파일이 적격 실행 파일인 경우, 디바이스는 이를 AMP 클라우드의 Spero 휴리스틱 엔진에 제출합니다. Spero 엔진은 Spero 서명을 기반으로 파일이 악성코드인지 확인합니다. 또한 파일을 AMP 클라우드에 제출하지 않고 Spero 분석을 위해 제출하도록 규칙을 구성할 수도 있습니다.

Spero 분석을 위해 수동으로 파일을 제출할 수는 없습니다.

AMP 클라우드 조회

Advanced Malware Protection를 사용한 평가 대상 파일의 경우, Firepower Management Center는 악성코드 클라우드 조회를 수행하여 파일의 SHA-256 해시 값을 기반으로 파일의 속성을 AMP 클라우드에서 쿼리합니다.

시스템은 성능 향상을 위해 클라우드가 반환한 속성을 캐시하고 알려진 파일의 경우, AMP 클라우드를 쿼리하는 대신 캐시된 속성을 사용합니다. 이 캐시에 대한 자세한 내용은 캐시된 속성 수명, 1891 페이지를 참조하십시오.

로컬 악성코드 분석

로컬 악성코드 분석을 통해 매니지드 디바이스는 Cisco Talos Intelligence Group(Talos)가 제공하는 탐지 규칙 세트을 사용하여 실행 파일, PDF, Office 문서 및 기타 파일 유형에서 가장 일반적인 유형의

악성코드를 로컬로 검사할 수 있습니다. 로컬 악성코드 분석은 AMP 클라우드를 쿼리하지 않고 파일을 실행하지 않기 때문에 시간과 시스템 리소스가 절약됩니다.

시스템이 로컬 악성코드 분석을 통해 악성코드를 식별하는 경우, 기존 악성코드 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 업데이트됩니다. 그러면 시스템이 새로운 악성코드 이벤트를 생성합니다. 시스템이 악성코드를 식별하지 않으면 파일 속성이 Unknown(알 수 없음)에서 Clean(안전)으로 업데이트되지 않습니다. 시스템은 로컬 악성코드 분석을 실행한 후 SHA-256 해시 값, 타임스탬프, 속성 같은 파일 정보를 캐시하므로 일정 기간 내에 다시 탐지될 경우, 추가 분석 없이 악성코드를 식별할 수 있습니다. 캐시에 대한 자세한 내용은 캐시된 속성 수명, 1891 페이지를 참조하십시오.

로컬 악성 코드 분석은 Cisco Threat Grid 클라우드와의 통신이 필요하지 않습니다. 하지만 동적 분석을 위해 파일을 제출하고 로컬 악성코드 분석 규칙 집합 업데이트를 다운로드하려면 클라우드와의 통신을 구성해야 합니다.

캐시된 속성 수명

AMP 클라우드 쿼리에서 반환된 속성, 관련 위협 점수, 로컬 악성코드 분석에 의해 할당된 속성은 TTL(time-to-live) 값을 갖습니다. TTL 값에 지정된 기간 동안 속성이 업데이트되지 않고 유지될 경우, 시스템에서는 캐시된 정보를 삭제합니다. 속성 및 관련 위협 점수에는 다음과 같은 TTL 값이 포함됩니다.

- 안전 - 4시간
- 알 수 없음 - 1시간
- 악성코드 - 1시간

캐시에 대한 쿼리에서 시간 초과된 캐시된 속성이 식별되는 경우, 시스템은 로컬 악성코드 분석 데이터베이스와 AMP 클라우드에서 새로운 속성을 다시 쿼리합니다.

동적 분석

Cisco Threat Grid(이전의 AMP Threat Grid), Cisco의 파일 분석, 위협 인텔리전스 플랫폼을 사용하여 동적 분석을 위해 자동으로 파일을 제출하도록 파일 정책을 구성할 수 있습니다.

디바이스는 디바이스에 파일이 저장되어 있는지 여부에 상관없이 적격 파일을 Cisco Threat Grid(사용자가 지정한 퍼블릭 클라우드 또는 현장 어플라이언스)에 제출합니다.

Cisco Threat Grid 파일을 샌드박스 환경에서 실행하고 파일의 동작을 분석해 파일이 악성인지 확인하고 파일에 악성코드가 포함되었을 가능성을 나타내는 위협 점수를 반환합니다. 위협 점수에서 동적 분석 요약 보고서와 함께 할당된 위협 점수의 이유를 볼 수 있습니다. 또한 Cisco Threat Grid에서 조직이 제출한 파일의 상세한 보고서를 볼 수 있을 뿐 아니라 조직이 제출하지 않은 파일에 대한 삭제된 보고서를 제한된 데이터와 함께 볼 수 있습니다.

Cisco Cisco Threat Grid에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/threat-grid/index.html를 참조하십시오

동적 분석을 수행하도록 시스템을 구성하려면 동적 분석 연결, 1877 페이지 아래의 주제를 참조하십시오.

어떤 파일이 동적 분석에 적합합니까?

파일이 동적 분석에 적합한지 여부는 다음에 따라 달라집니다.

- 파일 형식
- 파일 크기
- 파일 규칙 작업

또한

- 시스템은 사용자가 구성하는 파일 규칙에 일치하는 파일만 제출합니다.
- 분석을 위해 전송될 때 파일에는 Unknown(알 수 없음) 또는 Unavailable(사용할 수 없음)의 악성코드 클라우드 조회 속성이 있어야 합니다.
- 시스템은 파일을 잠재적 악성코드로 사전 분류해야 합니다.

동적 분석 및 용량 처리

용량 처리를 사용하면 디바이스가 클라우드와 통신할 수 없거나 최대 제출 수에 도달했기 때문에 시스템이 일시적으로 클라우드에 파일을 전송할 수 없는 경우, 그렇지 않았다면 동적 분석되었을 파일을 일시적으로 저장할 수 있습니다. 전송을 방해하는 조건이 지나가면 시스템은 저장된 파일을 제출합니다.

일부 디바이스는 디바이스 하드 드라이브 또는 악성코드 스토리지 팩에 파일을 저장할 수 있습니다. 악성코드 스토리지 팩, 1893 페이지도 참조하십시오.

캡처된 파일 및 파일 스토리지

파일 스토리지 기능을 사용하면 트래픽에서 탐지된 선택된 파일을 캡처한 다음 디바이스의 하드 드라이브 또는 악성코드 스토리지 팩(설치된 경우)에 파일의 사본을 자동으로 임시 저장할 수 있습니다.

디바이스가 파일을 캡처한 후 다음을 수행할 수 있습니다.

- 나중에 분석하기 위해 캡처한 파일을 디바이스의 하드 드라이브에 저장합니다.
- 저장된 파일을 추가 수동 분석 또는 아카이브를 위해 로컬 컴퓨터로 다운로드합니다.
- AMP 클라우드 조회 또는 동적 분석을 위해 캡처된 적격 파일을 수동으로 제출합니다.

디바이스는 파일을 저장한 경우, 나중에 해당 파일이 탐지되었을 때 여전히 저장되어 있으면 다시 캡처하지 않습니다.

참고 네트워크에서 처음으로 파일이 탐지되면 파일의 탐지를 나타내는 파일 이벤트를 생성할 수 있습니다. 하지만 파일 규칙이 악성코드 클라우드 조회를 수행하는 경우, AMP 클라우드를 쿼리하고 속성을 반환하기 위한 추가 시간이 필요합니다. 이 지연으로 인해 시스템은 이 파일이 네트워크에 두 번째로 나타날 때까지 해당 파일을 저장할 수 없으며, 파일의 속성을 즉시 결정할 수 있습니다.

시스템이 파일을 캡처하든 저장하든 사용자는 다음을 수행할 수 있습니다.

- 파일이 저장되었는지 동적 분석을 위해 제출되었는지 여부, 파일 속성, 위협 점수 등 캡처된 파일에 대한 정보를 Analysis(분석) > Files(파일) > Captured Files(캡처된 파일)에서 검토할 수 있으며, 이를 통해 사용자는 네트워크에서 탐지된 악성코드 위협 가능성을 신속하게 검토할 수 있습니다.
- 파일의 전파 흔적을 보고 파일이 네트워크에서 어떻게 이동했고 어떤 호스트에 복사본이 있는지를 확인할 수 있습니다.
- 향후 탐지에서 정상 또는 악성코드 속성이 있는 것으로 항상 취급하려면 파일을 정상 목록 또는 맞춤형 탐지 목록에 추가하십시오.

사용 가능한 경우, 특정 유형 또는 특정 속성의 파일을 캡처 및 저장하도록 파일 정책에서 파일 규칙을 구성할 수 있습니다. 파일 정책을 액세스 제어 정책과 연결하고 디바이스에 구축하면 트래픽에서 일치하는 파일이 캡처 및 저장됩니다. 또한 저장할 최소 및 최대 파일 크기를 제한할 수도 있습니다.

저장된 파일은 시스템 백업에 포함되지 않습니다.

Analysis(분석) > Files(파일) > Captured Files(캡처된 파일)에서 캡처된 파일 정보를 보고 오프라인 분석을 위해 복사본을 다운로드할 수 있습니다.

악성코드 스토리지 팩

디바이스에서는 파일 정책 구성을 기반으로 상당한 양의 파일 데이터를 하드 드라이브에 저장할 수 있습니다. 디바이스에 악성코드 스토리지 팩을 설치할 수 있습니다. 시스템은 파일을 악성코드 스토리지 팩에 저장하므로 기본 하드 드라이브에 이벤트와 구성 파일을 저장하기 위한 공간이 좀 더 확보됩니다. 시스템은 주기적으로 오래된 파일을 삭제합니다. 디바이스의 기본 하드 드라이브에 여유 공간이 충분하지 않고 악성코드 스토리지 팩이 설치되어 있지 않으면 파일을 저장할 수 없습니다.

주의 Cisco에서 제공하지 않은 하드 드라이브를 디바이스에 설치하려고 하지 마십시오. 지원되지 않는 하드 드라이브를 설치하면 디바이스가 손상될 수 있습니다. 악성코드 스토리지 팩 키트는 Cisco에서만 구입할 수 있으며 8000 Series 디바이스에서만 사용할 수 있습니다. 악성코드 스토리지 팩과 관련하여 도움이 필요하면 고객 지원에 문의하십시오. 자세한 내용은 *Firepower System* 악성코드 스토리지 팩 설명서을 참조하십시오.

악성코드 스토리지 팩이 설치되지 않은 상태에서 파일을 저장하도록 디바이스를 구성하면 기본 하드 드라이브 공간의 일정 부분이 캡처된 파일 스토리지에 할당됩니다. 동적 분석을 위해 임시로 파일을 저장하도록 용량 처리를 구성하는 경우, 시스템은 클라우드에 파일을 다시 전송할 수 있을 때까지 동일한 하드 드라이브 할당을 사용하여 이 파일을 저장합니다.

디바이스에 악성코드 스토리지 팩을 설치하고 파일 저장소 또는 용량 처리를 구성하는 경우, 디바이스는 이러한 파일을 저장하기 위해 전체 악성코드 스토리지 팩을 할당합니다. 디바이스는 악성코드 스토리지 팩에 다른 정보를 저장할 수 없습니다.

캡처된 파일 스토리지에 할당된 공간이 다 차면 시스템은 할당된 공간이 시스템 정의 임계값에 도달할 때까지 저장된 파일 중 가장 오래된 파일을 삭제합니다. 저장된 파일 수를 기준으로 시스템이 파일을 삭제한 후 디스크 사용량이 상당히 줄어든 것을 볼 수 있습니다.

디바이스가 이미 파일을 저장한 상태에서 악성코드 스토리지 팩을 설치하면 디바이스를 다음에 다시 시작할 때 기본 하드 드라이브에 저장된 캡처된 파일 또는 용량 처리 파일이 악성코드 스토리지 팩으로 이동합니다. 이후 디바이스에서 저장하는 파일은 악성코드 스토리지 팩에 저장됩니다.

유형별로 모든 파일 차단

조직에서 악성코드뿐만 아니라 특정 유형의 모든 파일(파일의 악성코드 여부 포함 여부에 상관없이)의 전송을 차단하려는 경우, 차단이 가능합니다.

파일 제어는 시스템이 악성코드와 더불어 다양한 추가 파일 유형을 탐지할 수 있는 경우 모든 파일 유형을 지원합니다. 이러한 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent), PDF와 같은 기본적인 카테고리로 그룹화됩니다.

유형을 기준으로 모든 파일을 차단하는 것은 기술적으로는 악성코드 방지 기능이 아닙니다. 즉, 악성코드 라이선스가 필요하지 않고 AMP 클라우드를 쿼리하지 않습니다.

파일 규칙 작업: 평가 순서

파일 정책에는 상황마다 서로 다른 작업이 포함된 여러 규칙이 포함될 가능성이 높습니다. 특정 상황에 둘 이상의 규칙이 적용될 수 있는 경우, 이 주제에 설명된 평가 순서가 적용됩니다. 일반적으로 단순 차단은 악성코드 탐지 및 차단보다 우선하는데, 이는 단순 탐지 및 로깅에 우선하는 것입니다.

파일 규칙 작업의 우선 순위는 다음과 같습니다.

- 파일 차단
- 악성코드 차단
- 악성코드 클라우드 조회
- 파일 탐지

파일 규칙 생성

주의 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 Enabling or disabling **Store Files(**파일 저장 활성화 또는 비활성화**)**를 활성화하거나 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)** 또는 **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**), Unknown(**알 수 없음**), Clean(**정상**)** 또는 **Custom(**맞춤형**))**과 결합하는 첫 번째 파일 규칙을 추가하거나 마지막 파일 규칙을 제거, 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

시작하기 전에

악성 코드 보호를 위한 규칙을 구성한다면, 파일 정책 구성, 1868 페이지 섹션을 참조하십시오.

프로시저

단계 **1** 파일 정책 편집기에서 파일 규칙 추가클릭 합니다.

단계 **2** 파일 규칙 구성 요소, 1885 페이지에 설명된 대로 **Application Protocol(**애플리케이션 프로토콜**)**과 **Direction of Transfer(**전송 방향**)**을 선택합니다.

단계 **3** 하나 이상의 **File Types(**파일 유형**)**를 선택합니다.

표시되는 파일 유형은 선택한 애플리케이션 프로토콜, 전송 방향, 작업에 따라 달라집니다.

파일 유형 목록을 다음 방법으로 필터링할 수 있습니다.

- 하나 이상의 **File Type Categories(**파일 유형 카테고리**)**를 선택한 다음 **All types in selected Categories(**선택한 카테고리의 모든 유형**)**를 클릭합니다.
- 해당 이름 또는 설명으로 파일 유형을 검색합니다. 예를 들어, Microsoft Windows 특유의 파일 목록을 표시하려면 **`Windows`**를 **Search name and description(**이름 및 설명 검색**)** 필드에 입력합니다.

팁 해당 설명을 확인하려면 파일 유형 위에 마우스 포인터를 올려놓습니다.

단계 **4** 파일 규칙 작업, 1886 페이지S에 설명된 대로 파일 규칙 작업: 평가 순서, 1894 페이지을 고려하여 파일 규칙 **Action(**작업**)**을 선택합니다.

사용 가능한 작업은 설치한 라이선스에 따라 달라집니다. 파일 및 악성코드 정책을 위한 라이선스 요구 사항, 1863 페이지의 내용을 참조하십시오.

단계 **5** 선택한 작업에 따라 옵션을 구성합니다.

- 파일 차단 후 연결을 재설정
- 규칙과 일치하는 파일 저장
- Spero 분석* 활성화
- 로컬 악성 코드 분석* 활성화
- 동적 분석* 및 용량 처리 활성화

* 이러한 옵션에 대한 자세한 내용은 파일 규칙 작업, 1886 페이지과 (파일 규칙 작업의) 악성코드 차단 옵션, 1888 페이지 및 하위 항목을 참조하십시오.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 악성 코드 보호를 위한 정책을 구성한다면, 파일 정책 구성, 1868 페이지 섹션으로 돌아가십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

악성 코드 차단을 위한 액세스 제어 규칙 로깅

시스템이 파일 정책의 설정에 따라 (악성코드 등) 금지된 파일을 탐지하면 자동으로 Firepower Management Center 데이터베이스에 이벤트가 로깅됩니다. 파일 또는 악성코드 이벤트를 로깅하지 않으려는 경우, 액세스 제어 규칙마다 이러한 로깅을 비활성화할 수 있습니다.

시스템은 또한 액세스 제어 규칙 호출의 로깅 구성에 관계없이 Firepower Management Center 데이터베이스와 관련된 연결의 종료를 로깅합니다.

회귀적 속성 변경

파일 속성은 변경될 수 있습니다. 예를 들어 새로운 정보가 발견됨에 따라 AMP 클라우드는 이전에는 정상으로 간주되었던 파일이 지금은 악성코드로 식별되는 경우 또는 그 반대의 경우(악성코드로 식별된 파일이 실제로 정상임)를 결정할 수 있습니다. 지난주에 쿼리한 파일의 속성이 변경되는 경우, AMP 클라우드는 시스템에 이를 알려 시스템이 다음에 해당 파일의 전송을 탐지할 경우 적절한 조치를 취할 수 있도록 합니다. 변경된 속성은 회귀적 속성이라고 합니다.

(선택 사항) AMP for Endpoints를 사용한 악성코드 방지

Cisco의 AMP for Endpoints는 Firepower 시스템에서 제공하는 악성 코드 방지를 보완하고 Firepower 구축과 통합할 수 있는 별도의 악성 코드 방지 제품입니다.

AMP for Endpoints는 개별 사용자의 엔드포인트(컴퓨터 및 모바일 디바이스)에서 경량 커넥터로 실행되어 지능형 악성 코드 발생, 지능형 지속 위협 공격(APT) 표적 공격을 발견, 파악, 차단하는 Cisco의 엔터프라이즈급 지능형 악성코드 방지 솔루션입니다.

AMP for Endpoints의 이점은 다음과 같습니다.

- 조직 전체에 맞춤형 악성코드 탐지 정책 및 프로파일을 구성하고 모든 사용자의 파일에서 신속한 전체 검사 수행
- 보기 히트 맵, 자세한 파일 정보, 네트워크 파일 전파 흔적 분석, 위협 근본 원인을 비롯한 악성코드 분석 수행
- 자동 격리, 격리되지 않은 실행 파일의 실행을 막는 애플리케이션 차단, 제외 목록을 비롯하여 아웃브레이크 제어의 다양한 측면 구성
- 맞춤형 보호를 생성하고, 그룹 정책을 기반으로 특정 애플리케이션의 실행을 차단하며, 맞춤형 허용 애플리케이션 목록을 생성
- AMP for Endpoints 관리 콘솔을 사용하여 악성 코드의 영향을 완화하도록 지원 관리 콘솔은 AMP for Endpoints 구축의 모든 부분을 제어하고 침투의 모든 단계를 관리할 수 있는 강력하고 유연한 웹 인터페이스를 제공합니다.

AMP for Endpoints에 대한 자세한 내용은 다음을 참조하십시오.

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html.

- AMP for Endpoints 관리 콘솔의 온라인 도움말.
- http://docs.amp.cisco.com에서 구할 수 있는 AMP for Endpoints 설명서.

악성코드 방지 비교: Firepower 대 AMP for Endpoints

표 *113:* 탐지 제품별 고급 악성코드 방지 차이점

기능	Firepower 악성코드 방지(AMP for Networks)	AMP for Endpoints
파일 유형 탐지 및 차단 방법(파일 제어)	네트워크 트래픽에서 액세스 제어 및 파일 정책 사용	지원되지 않음
악성코드 탐지 및 차단 방법	네트워크 트래픽에서 액세스 제어 및 파일 정책 사용	개별 엔드포인트(최종 사용자 컴퓨터 및 모바일 디바이스)에서 AMP 클라우드와 통신하는 커넥터 사용
검사되는 네트워크 트래픽	매니지드 디바이스를 통과하는 트래픽	없음, 엔드포인트에 설치된 커넥터가 파일을 직접 검사
악성코드 인텔리전스 데이터 소스	AMP 클라우드(퍼블릭 또는 프라이빗)	AMP 클라우드(퍼블릭 또는 프라이빗)
악성코드 탐지 견고성	제한된 파일 유형	모든 파일 유형
악성코드 분석 선택	FMC기반 및 AMP 클라우드 내 분석 기반	FMC및 AMP for Endpoints 관리 콘솔의 추가 옵션
악성코드 완화	네트워크 트래픽에서 악성코드 차단, FMC에서 위협 요소 제거 시작	AMP for Endpoints 기반 격리 및 침투 제어 옵션 FMC에서 위협 요소 제거 시작
생성되는 이벤트	파일 이벤트, 캡처된 파일, 악성코드 이벤트, 회귀적 악성코드 이벤트	악성코드 이벤트
악성코드 이벤트의 정보	기본적인 악성코드 이벤트 정보 및 연결 데이터(IP 주소, 포트, 애플리케이션 프로토콜)	심층적인 악성코드 이벤트 정보, 연결 데이터 없음
네트워크 파일 경로	FMC기반	FMC 및 AMP for Endpoints 관리 콘솔에는 각각 네트워크 파일 경로 분석이 있습니다. 두 가지 모두 유용합니다.
필수 라이선스 또는 서브스크립션	파일 제어를 수행하는 데 필요한 라이선스 및 AMP for Networks	AMP for Endpoints 서브스크립션. AMP for Endpoints 데이터를 FMC로 가져오는 데는 라이선스가 필요하지 않습니다.

Firepower와 AMP for Endpoints 통합 정보

조직이 AMP for Endpoints를 구축한 경우, 필요하다면 해당 제품을 Firepower 구축에 통합할 수 있습니다.

AMP for Endpoints와의 통합에는 전용 Firepower 라이선스가 필요하지 않습니다.

Firepower와 AMP for Endpoints 통합의 이점

AMP for Endpoints 구축을 Firepower 시스템과 통합하면 다음과 같은 이점이 있습니다.

-
- 시스템은 AMP for Endpoints가 탐지한 악성코드 이벤트를 Firepower Management Center로 가져올 수 있으므로 사용자는 Firepower 시스템에 의해 생성된 악성코드 이벤트와 함께 이러한 이벤트를 관리할 수 있습니다. 이러한 이벤트에 대해 가져온 데이터에는 스캔, 악성코드 탐지, 격리, 차단된 실행, 클라우드 리콜 및 FMC가 모니터링하는 호스트에 대해 표시하는 IOC(Indications of Compromise)가 포함됩니다.

  자세한 내용은 AMP for Endpoints를 사용한 악성코드 이벤트 분석, 2966 페이지를 참고하십시오.

중요 Cisco AMP Private Cloud를 사용하는 경우, AMP for Endpoints 및 AMP Private Cloud, 1898 페이지에서 제한 사항을 참조하십시오.

AMP for Endpoints 및 AMP Private Cloud

엔드포인트 커넥터에 대 한 모든 AMP 데이터를 해당 데이터를 전달 하는 프라이빗 클라우드를 보낼 네트워크에서 AMP 엔드포인트 데이터를 수집 하려면 Cisco AMP 프라이빗 클라우드를 구성 하는 경우는 Firepower Management Center합니다. 프라이빗 클라우드는 외부 연결을 통해 엔드포인트 데이터를 공유하지 않습니다.

필요한 용량을 지원하기 위해 여러 프라이빗 클라우드를 구성할 수 있습니다.

Firepower와 AMP for Endpoints 통합

조직이 Cisco의 AMP for Endpoints 제품을 구축한 경우, 해당 제품을 Firepower와 통합하여 Firepower와 AMP for Endpoints 통합의 이점, 1898 페이지에 설명된 이점을 얻을 수 있습니다.

AMP for Endpoints와 통합한다면, AMP for Networks (AMP for Firepower) 연결을 구성했다 하더라도 AMP for Endpoints 연결을 구성해야 합니다. 여러 AMP for Endpoints 클라우드 연결을 구성해도 됩니다.

주의 다중 도메인 구축에서는, 특히 리프 도메인에 겹치는 IP 공간이 있다면 AMP for Endpoints 연결은 리프 수준에서만 구성해야 합니다. 여러 서브도메인에 IP-MAC 주소 쌍이 동일한 호스트가 있는 경우, 시스템은 AMP for Endpoints가 생성하는 악성코드 이벤트를 잘못된 리프 도메인에 저장하거나 IOC를 잘못된 호스트에 연결할 수 있습니다.

하지만 연결마다 별도의 AMP for Endpoints 계정을 사용한다면 어떤 도메인 수준에서도 AMP for Endpoints 연결을 구성할 수 있습니다. 예를 들어 MSSP의 각 클라이언트에는 자체 AMP for Endpoints 구축이 있을 수 있습니다.

참고 성공적으로 등록되지 않은 AMP for Endpoints 연결은 AMP for Networks 에 영향을 미치지 않습니다.

시작하기 전에

- 이 작업을 수행하려면 관리자 사용자여야 합니다.
- 구축에서 Cisco AMP 프라이빗 클라우드를 사용하는 경우, AMP for Endpoints 및 AMP Private Cloud, 1898 페이지에서 제한 사항을 참조하십시오.
- AMP for Endpoints가 설정되고 네트워크에서 정상적으로 작동해야 합니다.
- Firepower Management Center이 인터넷에 직접 액세스할 수 있어야 합니다.
- FMC와 AMP for Endpoints가 서로 통신할 수 있는지 확인합니다. 보안, 인터넷 액세스 및 통신 포트, 3107 페이지의 항목을 참조하십시오.
- Firepower Management Center를 공장 기본값으로 복원하거나 이전 버전으로 되돌린 후 AMP 클라우드에 연결하는 경우, AMP for Endpoints 관리 콘솔을 사용하여 이전 연결을 제거합니다.
- 이 절차 도중 AMP for Endpoints 콘솔에 로그인하려면 AMP for Endpoints 자격 증명이 필요합니다.

프로시저

단계 **1** **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** **Add AMP Cloud Connection(AMP** 클라우드 연결 추가**)**를 클릭합니다.

단계 **3** **Cloud Name(**클라우드 이름**)** 드롭다운 목록에서 사용할 클라우드를 선택합니다.

- Firepower Management Center의 지리적 위치에 가장 가까운 AMP 클라우드를 선택합니다.

  APJC는 아시아/태평양/일본/중국입니다.

- AMP 프라이빗 클라우드(AMPv)의 경우, **Private Cloud(**프라이빗 클라우드**)**를 선택하고 Cisco AMP Private Cloud, 1874 페이지에 설명된 대로 진행합니다.

단계 **4** AMP for Networks 와 AMP for Endpoints 모두에 클라우드를 사용하려면, **Use for AMP for Firepower(AMP for Firepower**에 사용**)** 확인란을 선택합니다.

AMP for Networks (AMP for Firepower) 통신을 처리할 다른 클라우드를 구성한 경우에는 이 확인란 선택을 취소할 수 있지만 이것이 유일한 AMP 클라우드 연결이라면 선택을 취소할 수 없습니다.

다중 도메인 구축에서 이 확인란은 전역 도메인에만 표시됩니다. 각 Firepower Management Center에는 하나의 AMP for Networks 연결만 있을 수 있습니다.

단계 **5** **Register(**등록**)**를 클릭합니다.

회전하는 상태 아이콘은 연결이 보류 중(예를 들어 Firepower Management Center에서 연결을 구성한 후 AMP for Endpoints 관리 콘솔을 사용하여 권한을 부여하기 전)임을 나타냅니다. 거부됨( )은 클라우드가 연결을 거부했거나 다른 이유로 연결이 실패했음을 나타냅니다.

단계 **6** 계속해서 AMP for Endpoints 관리 콘솔로 이동한다고 확인한 다음 관리 콘솔에 로그인합니다.

단계 **7** 관리 콘솔을 사용하여 AMP 클라우드가 AMP for Endpoints 데이터를 Firepower Management Center에 전송하도록 권한을 부여합니다.

단계 **8** FMC가 수신하는 데이터를 제한하려면 정보를 수신할 조직 내 특정 그룹을 선택합니다.

기본적으로 AMP 클라우드는 모든 그룹에 대해 데이터를 전송합니다. 그룹을 관리하려면 AMP for Endpoints 관리 콘솔에서 **Management** > **Groups(**관리 그룹**)**를 선택합니다. 자세한 내용은 관리 콘솔 온라인 도움말을 참조하십시오.

단계 **9** 연결을 활성화하고 데이터 전송을 시작하려면 **Allow(**허용**)**를 클릭합니다.

Deny(거부**)**를 클릭하면 Firepower Management Center로 되돌아가며, 여기서는 연결이 거부된 것으로 표시됩니다. AMP for Endpoints 콘솔의 Applications(애플리케이션) 페이지에서 다른 곳으로 이동하고 연결을 거부하지도 허용하지도 않는 경우, 연결은 Firepower Management Center의 웹 인터페이스에서 보류 중으로 표시됩니다. 이런 상황에서는 상태 모니터가 연결 실패를 알리지 않습니다. 나중에 AMP 클라우드에 연결하려면 실패하거나 보류 중인 연결을 삭제한 다음 다시 생성하십시오.

AMP for Endpoints 연결의 등록이 완료되지 않아도 AMP for Networks 연결은 비활성화되지 않습니다.

단계 **10** 연결이 올바로 구성되어 있는지 확인하려면,

a) **AMP** > **AMP Management(AMP** 관리**)** 페이지의 **Cisco AMP Solution Type(Cisco AMP** 솔루션 유형**)** 열에서 **`AMP for Endpoints`**를 포함하는 클라우드 이름을 선택합니다.
b) 표시되는 AMP for Endpoints 콘솔 창에서 **Accounts(**계정**) > Applications(**애플리케이션**)**를 선택합니다.
c) Firepower Management Center가 목록에 있는지 확인합니다.
d) AMP for Endpoints 콘솔 창에서 **Manage(**관리**) > Computers(**컴퓨터**)**를 선택합니다.
e) Firepower Management Center가 목록에 있는지 확인합니다.

다음에 수행할 작업

- AMP for Endpoints 콘솔 창에서 필요에 따라 설정을 구성합니다. 예를 들어 관리 센터의 그룹 구성원 자격을 정의하고 정책을 할당합니다. 자세한 내용은 AMP for Endpoints 온라인 도움말이나 기타 설명서를 참조하십시오.
- 기본 상태 정책은 성공적인 초기 연결 후 Firepower Management Center가 AMP for Endpoints 포털에 연결할 수 없거나 연결이 등록 취소된 경우, AMP 포털을 사용하여 사용자에게 경고합니다.

  System(시스템**) > Health(**상태**) > Policy(**정책**)** 아래에서 **AMP for Endpoints Status(AMP for Endpoints** 상태**)** 모니터가 활성화되어 있는지 확인합니다.

파일 정책 및 악성코드 보호 히스토리

기능	버전	세부 사항
장 개편	6.4 기간에서 변경이 이루어졌지만 다시 게시되는 모든 버전에 표시됩니다.	혼란을 줄이기 위해 이 장의 내용을 개편했습니다. 파일/악성코드 이벤트 및 네트워크 파일 경로 분석, 2963 페이지을 위해 일부 내용을 장에 포함하거나 장에서 제외했습니다.
URL 필터링 정보를 새로운 URL 필터링 장으로 이동	6.3	URL 필터링을 위한 클라우드 통신 구성에 대한 정보를 이 새로운 URL 필터링 장으로 이동 이와 관련하여 이 장의 Cisco CSI 주제의 구조를 변경

76 장

파일 및 악성코드 탐지 성능 및 저장 조정

다음 주제에서는 파일 및 악성코드 검사 성능과 저장을 구성하는 방법을 설명합니다.

- 파일 및 악성코드 탐지 성능 및 저장 옵션, 1903 페이지
- 파일 및 악성코드 탐지 성능 및 저장 조정, 1905 페이지

파일 및 악성코드 탐지 성능 및 저장 옵션

파일 크기를 늘리면 시스템의 성능에 영향을 미칠 수 있습니다.

표 ***114:*** 고급 액세스 제어 파일 및 ***AMP for Networks*** 옵션

필드	설명	지침 및 제한 사항
파일 유형 탐지 중에 검사되는 바이트 수 제한	파일 유형 탐지를 수행할 때 검사되는 바이트 수를 지정합니다.	0-4294967295(4GB) 0은 제한을 제거합니다. 기본값은 TCP 패킷의 최대 세그먼트 크기입니다(1460바이트). 대부분의 경우 시스템은 첫 번째 패킷을 사용하여 공용 파일 유형을 확인할 수 있습니다. ISO 파일을 탐지하려면 36870보다 큰 값을 입력합니다.
악성코드 차단을 위한 클라우드 조회가 다음보다 오래 걸리는 경우 파일 허용(초)	악성코드 클라우드 조회가 이루어지는 동안 **Block Malware**(악성코드 차단) 규칙과 일치하고 캐시된 속성이 없는 파일의 최종 바이트가 시스템에 유지되는 기간을 지정합니다. 시스템이 속성을 보유하지 못하고 시간이 경과하면, 파일은 통과됩니다. 사용할 수 없는 속성은 캐시되지 않습니다.	0-30초 지원 팀에 문의하지 않고 이 옵션을 0으로 설정하지 마십시오. Cisco는 연결 실패로 인한 트래픽 차단을 방지하기 위해 기본값을 사용할 것을 권장합니다.

필드	설명	지침 및 제한 사항
(바이트**)**보다 큰 파일의 **SHA-256** 해시 값을 계산하지 마십시오**.**	맞춤형 탐지 목록에 추가된 경우, 시스템이 특정 크기보다 큰 파일을 저장하거나 파일에 대한 클라우드 조회를 하거나 파일을 차단하지 않도록 합니다.	0-4294967295(4GB) 0은 제한을 제거합니다. 이 값은 **Maximum file size to store (bytes)** 및 **Maximum file size for dynamic analysis testing (bytes)**보다 크거나 같아야 합니다.
Minimum file size for advanced file inspection and storage (bytes)	이러한 설정은 다음을 지정합니다. • 시스템이 다음 탐지기를 사용하여 검사할 수 있는 파일 크기: • Spero 분석 • 샌드박싱 및 사전 분류 • 로컬 악성코드 분석/ClamAV • 아카이브 검사 • 시스템이 파일 규칙을 사용하여 저장할 수 있는 파일 크기.	0 - 10485760(10MB) 0은 파일 스토리지를 비활성화합니다. **Maximum file size to store (bytes)** 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.
Maximum file size for advanced file inspection and storage (bytes)		0 - 10485760(10MB) 0은 파일 스토리지를 비활성화합니다. **Minimum file size to store (bytes)**보다 크거가 같고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.
Minimum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 AMP 클라우드에 제출할 수 있는 최소 파일 크기를 지정합니다.	0 -10485760(10MB) **Maximum file size for dynamic analysis testing (bytes)** 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다. 동적 분석을 위한 파일 크기는 파일 분석의 최소 및 최대 설정에서 정의된 한도 이내여야 합니다. Firepower 5.x 버전을 실행하는 장치를 구축하는 경우, 시스템은 15360보다 작은 모든 값을 15360으로 변경합니다. 시스템은 제출할 수 있는 최소 파일 크기에 대한 업데이트를 AMP 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최소 크기가 현재 값보다 큰 경우, 현재 값이 새 최소값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.

필드	설명	지침 및 제한 사항
Maximum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 AMP 클라우드에 제출할 수 있는 최대 파일 크기를 지정합니다.	0-10485760(10MB) **Minimum file size for dynamic analysis testing (bytes)** 보다 크거나 같고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다. 동적 분석을 위한 파일 크기는 파일 분석의 최소 및 최대 설정에서 정의된 한도 이내여야 합니다. Firepower 버전 5.x를 실행하는 장치를 구축하는 경우, 시스템은 2097152보다 큰 모든 값을 2097152로 변경합니다. 시스템은 제출할 수 있는 최대 파일 크기에 대한 업데이트를 AMP 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최대 크기가 현재 값보다 작은 경우, 현재 값이 새 최대값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.

파일 및 악성코드 탐지 성능 및 저장 조정

이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자 사용자여야 합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **Files and Malware Settings(**파일 및 악성코드 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** 파일 및 악성코드 탐지 성능 및 저장 옵션, 1903 페이지에 설명된 옵션을 설정합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Snort® 재시작 시나리오, 505 페이지

XVII 부

TID 인텔리전스 및 위협 분석

• Cisco Threat Intelligence Director(TID), 1909 페이지

77 장

Cisco Threat Intelligence Director(TID)

이 장의 주제에서는 Firepower System에서 TID를 구성하고 사용하는 방법을 설명합니다.

- Cisco Threat Intelligence Director(TID) 개요, 1909 페이지
- TID(Threat Intelligence Director) 요구 사항 및 사전 요건, 1912 페이지
- 설정 방법 Cisco Threat Intelligence Director(TID), 1914 페이지
- TID 인시던트 및 관찰 데이터 분석, 1924 페이지
- Cisco Threat Intelligence Director(TID) 구성 보기 및 변경, 1936 페이지
- 문제 해결 Cisco Threat Intelligence Director(TID), 1952 페이지
- 기록Cisco Threat Intelligence Director(TID), 1955 페이지

Cisco Threat Intelligence Director(TID) 개요

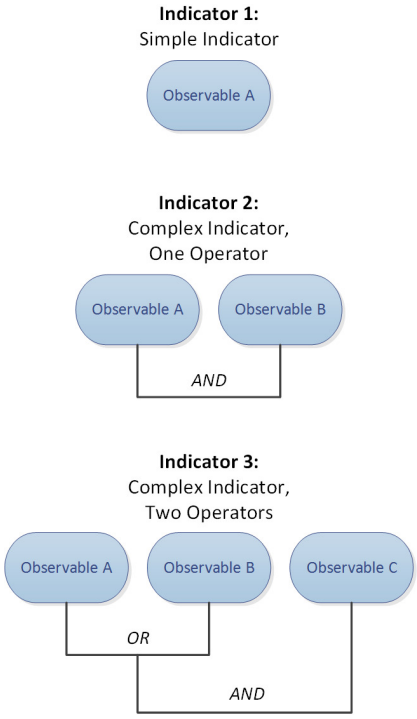
Cisco Threat Intelligence Director(TID)는 위협 인텔리전스 데이터를 운용하여 인텔리전스 데이터 집계, 방어 작업 구성, 환경 내 위협 분석에 도움이 됩니다. 이 기능은 다른 Firepower 기능을 보완하기 위한 것이며, 위협에 대한 추가 방어선을 제공합니다.

호스팅 플랫폼에 구성할 경우, TID는 위협 인텔리전스 소스에서 데이터를 수집하여 구성된 모든 매니지드 디바이스(요소)에 게시합니다. 호스팅 플랫폼과 이 릴리스에서 지원되는 요소에 대한 자세한 내용은 플랫폼, 요소 및 라이선스 요구 사항, 1912 페이지를 참조하십시오.

소스에는 관찰 가능 개체를 포함하는 지표가 포함됩니다. 지표는 위협과 관련된 모든 특성을 전달하고, 개별적인 관찰 가능 개체는 위협과 관련된 개별적 특성(예: SHA-256 값)을 나타냅니다. 간단한 지표에는 하나의 관찰 가능 개체가 포함되고 복잡한 지표에는 둘 이상의 관찰 가능 개체가 포함됩니다.

관찰 가능 개체와 관찰 가능 개체 사이의 AND/OR 연산자는 다음 예에서 보듯 지표의 패턴을 형성합니다.

그림 *68:* 예*:* 지표 패턴



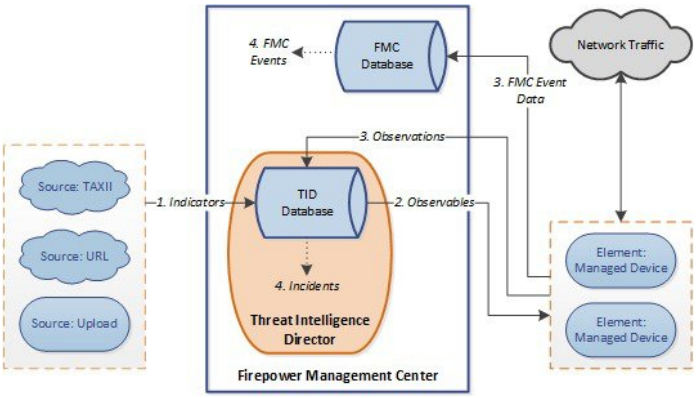
관찰 가능 개체가 요소에 게시된 후 요소는 시스템이 트래픽에서 관찰 가능 개체를 식별할 때 트래픽을 모니터링하여 관찰 가능 개체를 Firepower Management Center에 보고합니다.

Firepower Management Center는 모든 요소에서 관찰을 수집하고, TID 지표를 기준으로 관찰을 평가하며, 관찰 가능 개체의 상위 지표에 연결된 인시던트를 생성하거나 업데이트합니다.

인시던트는 지표의 패턴이 처리될 때 완전히 실현됩니다. 트래픽이 지표의 관찰 가능 개체 하나 이상과는 일치하지만 전체 패턴과는 일치하지 않는 경우, 인시던트가 부분적으로 실현됩니다. 자세한 내용은 관찰 및 사고 생성, 1924 페이지를 참고하십시오.

다음 다이어그램은 샘플 Firepower System 구성에서의 데이터 흐름을 보여줍니다.

그림 *69: Firepower Management Center* 데이터 흐름



TID가 완전히 또는 부분적으로 실현되면 시스템은 구성된 작업(모니터링, 차단, 부분적으로 차단 또는 작업 없음)을 수행합니다. 자세한 내용은 수행하는 작업에 영향을 미치는 요소, 1932 페이지를 참조하십시오.

TID 및 보안 인텔리전스

액세스 제어 정책의 일환으로 보안 인텔리전스는 평판 인텔리전스를 사용하여 IP 주소, URL, 도메인과의 연결을 신속하게 차단합니다. 보안 인텔리전스는 업계를 선도하는 Cisco Talos Intelligence Group(Talos)의 위협 인텔리전스에 대한 고요한 액세스를 제공합니다. Security Intelligence(보안 인텔리전스)에 대한 자세한 내용은 보안 인텔리전스 정보, 1695 페이지를 참고하십시오.

TID 다음과 같이 서드파티 소스의 보안 인텔리전스에 따라 연결을 차단하는 시스템의 기능을 강화합니다.

- **TID**는 추가 트래픽 필터링 기준을 지원합니다 - 보안 인텔리전스를 사용하여 IP 주소, URL 및 (DNS 정책이 활성화된 경우) 도메인 이름을 기반으로 트래픽을 필터링할 수 있습니다. TID는 또한 이러한 기준에 따른 필터링을 지원하며 SHA-256 해시 값에서의 필터링에 대한 지원을 추가합니다.
- **TID**는 추가 인텔리전스 수집 방법을 지원합니다 - 보안 인텔리전스와 TID를 모두 사용하면 플랫 파일을 수동으로 업로드하거나 서드파티 호스트에서 플랫 파일을 검색하도록 시스템을 구성하여 위협 인텔리전스를 시스템으로 가져올 수 있습니다. TID는 이러한 플랫 파일 관리의 유연성을 높입니다. 또한 TID는 STIX™(Structured Threat Information eXpression) 형식으로 제공되는 인텔리전스를 검색하고 수집할 수 있습니다.
- **TID**는 필터링 작업의 세분화된 제어를 제공합니다 - 보안 인텔리전스를 사용하여 네트워크, URL 또는 DNS 개체별로 필터링 기준을 지정할 수 있습니다. 보안 인텔리전스 개체(특히 목록 및 피드)는 여러 IP 주소, URL 또는 DNS 도메인 이름을 포함할 수 있지만 개체의 개별 요소가 아닌 전체 개체를 기준으로 차단 또는 차단 금지할 수 있습니다. TID를 사용하여 개별 기준(즉, 단순한 지표 또는 개별 관찰 가능 개체)의 필터링 작업을 구성할 수 있습니다.
- **TID** 구성 변경에는 재구축이 필요 없습니다 - 액세스 제어 정책에서 보안 인텔리전스 설정을 수정한 후에는 변경된 구성을 매니지드 디바이스에 다시 구축해야 합니다. TID를 사용하면 액세스 제어 정책을 매니지드 디바이스에 처음 구축한 후 재구축 없이 소스, 지표, 관찰 가능 개체를 구성할 수 있으며, 시스템은 새로운 TID 데이터를 요소에 자동으로 게시합니다.

보안 인텔리전스 또는 TID가 특정 인시던트를 처리할 수 있을 때 시스템이 수행하는 작업에 대한 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 1933 페이지를 참조하십시오.

Threat Intelligence Director의 성능 영향

Firepower Management Center

경우에 따라 다음을 확인할 수 있습니다.

- 특별히 큰 STIX 소스를 수집하는 동안 시스템에 약간의 성능 문제가 발생할 수 있으며, 수집이 끝날 때까지 예상보다 시간이 더 걸릴 수 있습니다.

- 새롭거나 수정된 TID 데이터를 요소에 게시하는 데 최대 15분이 걸릴 수 있습니다.

매니지드 디바이스

특별한 성능상 영향은 없습니다. TID가 성능에 미치는 영향은 Firepower Management Center 보안 인텔리전스 기능과 동일합니다.

Cisco Threat Intelligence Director(TID) 및 고가용성 구성

고사용성 구성인 액티브 Firepower Management Center에서 TID을 호스팅하는 경우, 시스템은 TID 설정과 TID 데이터를 스탠바이 Firepower Management Center에 동기화하지 않습니다. 페일오버 후 데이터를 복구할 수 있도록 액티브 Firepower Management Center에서 정기적인 TID 데이터 백업을 수행하는 것을 권장합니다.

자세한 내용은 TID 데이터 백업 및 복구 정보, 1923 페이지를 참조하십시오.

TID(Threat Intelligence Director) 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

관리자

TID(Threat Intelligence Director) 사용자

추가 요구 사항

다음 주제에서는 Threat Intelligence Director를 사용하기 위한 추가 요구 사항에 대해 설명합니다.

플랫폼, 요소 및 라이선스 요구 사항

호스팅 플랫폼

물리적/가상 Firepower Management Center에서 TID를 호스팅할 수 있습니다.

- Firepower System 버전 6.2.2 이상 실행.
- 최소 15GB의 메모리로 구성.
- REST API 액세스가 활성화되도록 구성. REST API 액세스 활성화의 내용을 참조하십시오.

요소

Firepower System 버전 6.2.2 이상을 실행하는 Firepower Management Center 매니지드 디바이스는 TID 요소로 사용할 수 있습니다.

라이선싱

SHA-256 관찰 가능 개체 게시에 대한 파일 정책을 구성하려면 Firepower System에 악성코드 라이선스(기본 또는 스마트)가 필요합니다.

자세한 내용은 지원할 정책 구성 TID, 1915 페이지 및 Firepower 라이선스 정보, 157 페이지의 내용을 참조하십시오.

소스 요구 사항

소스 유형 요구 사항:

STIX

파일은 STIX 버전 1.0, 1.1, 1.1.1 또는 1.2여야 하며, STIX 설명서 (http://stixproject.github.io/documentation/suggested-practices/)의 지침을 준수해야 합니다.

STIX 파일에는 복잡한 지표가 포함될 수 있습니다.

URL 다운로드 또는 파일 업로드를 통해 설정할 경우, STIX 파일의 최대 크기는 40MB입니다. 이보다 큰 STIX 파일이 있으면 TAXII 서버를 사용하는 것이 좋습니다.

플랫 파일

파일은 행당 하나의 관찰 가능 개체가 있는 ASCII 텍스트 파일이어야 합니다.

플랫 파일에는 간단한 지표만 포함됩니다(지표당 하나의 관찰 가능 개체).

플랫 파일의 최대 크기는 500MB입니다.

TID는 다음을 지원하지 않습니다.

- 관찰 가능 개체 값을 구분하는 구분 기호 문자(예: `observable,`은 잘못되었습니다).
- 관찰 가능 개체 값 앞뒤에 오는 문자(예: `"observable"`은 잘못되었습니다).

각 파일에는 한 가지 유형의 콘텐츠만 포함되어야 합니다.

- `SHA-256` - SHA-256 해시 값.
- `Domain` - RFC 1035에서 정의된 도메인 이름.
- `URL` - RFC 1738에서 정의된 URL.

참고 TID 포트, 프로토콜 또는 인증 정보를 포함하는 모든 URL을 표준화하고 지표를 탐지할 때 표준화된 버전을 사용합니다. 예를 들어 TID는 다음 URL 중 하나를 표준화합니다.

```
http://example.com/index.htm
http://example.com:8080/index.htm
example.com:8080/index.htm
example.com/index.htm
```

주로 다룹니다.

```
example.com/index.htm
```

또는 예를 들어 TID는 다음 URL을 표준화합니다.

```
http://abc@example.com:8080/index.htm
```

as

```
abc@example.com/index.htm/
```

- `IPv4` - RFC 791에서 정의된 IPv4 주소.

  TID CIDR 블록을 허용하지 않습니다.

- `IPv6` - RFC 4291에서 정의된 IPv6 주소.

  TID 프리픽스 길이를 허용하지 않습니다.

설정 방법 Cisco Threat Intelligence Director(TID)

참고 TID 구성 또는 작업 도중 문제가 발생하면 문제 해결 Cisco Threat Intelligence Director(TID), 1952 페이지를 참조하십시오.

프로시저

단계 **1** 설치가 TID 실행을 위한 요구 사항을 충족하는지 확인합니다.

플랫폼, 요소 및 라이선스 요구 사항, 1912 페이지의 내용을 참조하십시오.

단계 **2** 매니지드 디바이스마다 TID 지원에 필요한 정책을 구성하고 이러한 정책을 디바이스에 구축합니다.

지원할 정책 구성 TID, 1915 페이지의 내용을 참조하십시오.

인텔리전스 데이터 소스를 수집하기 전이나 후에 요소를 구성할 수 있습니다.

단계 **3** TID가 수집할 인텔리전스 소스를 구성합니다.

소스 요구 사항, 1913 페이지과 데이터 소스 수집 옵션, 1916 페이지의 항목을 참조하십시오.

단계 **4** 아직 게시하지 않은 경우, 데이터를 요소에 게시합니다. 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지의 내용을 참조하십시오.

다음에 수행할 작업

- 정기적으로 예약된 백업에 TID를 포함시킵니다. TID 데이터 백업 및 복구 정보, 1923 페이지의 내용을 참조하십시오.

  Firepower Management Center 구축이 고가용성(HA) 구성인 경우, Cisco Threat Intelligence Director(TID) 및 고가용성 구성, 277 페이지도 참조하십시오.

- (선택 사항) 원하는 경우, TID 기능에 대한 관리자 액세스 권한을 부여합니다. TID 액세스 권한이 있는 사용자 역할, 1923 페이지 및 Firepower System 사용자 관리FMC의 사용자 계정, 49 페이지를 참조하십시오.

- 작업 중 필요에 따라 구성을 미세 조정합니다. 예를 들어 오탐 인시던트를 생성하는 관찰 가능 개체를 차단 금지 목록에 추가합니다. Cisco Threat Intelligence Director(TID) 구성 보기 및 변경, 1936 페이지의 내용을 참조하십시오.

지원할 정책 구성 TID

Firepower Management Center의 TID 데이터를 매니지드 디바이스(요소)에 게시하려면 액세스 제어 정책을 구성해야 합니다. 또한 관찰과 Firepower Management Center 이벤트 생성을 최대화하도록 액세스 제어 정책을 구성하는 것이 좋습니다.

TID를 지원할 매니지드 디바이스마다 아래의 단계를 수행하여 연결된 액세스 제어 정책을 구성합니다.

데이터가 게시된 후 TID를 사용하도록 구성된 요소는 현재 게시된 모든 관찰 가능 개체를 자동으로 수신합니다.

프로시저

단계 **1** 액세스 제어 정책의 **Advanced Settings(**고급 설정**)**에서 **Enable Threat Intelligence Director(Threat Intelligence Director** 활성화**)** 확인란이 선택되어 있는지 확인합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

자세한 내용은 액세스 제어 정책 고급 설정, 1637 페이지를 참고하십시오.

단계 **2** 규칙이 아직 없다면 액세스 제어 정책에 규칙을 추가합니다. TID에서는 액세스 제어 정책이 적어도 하나의 규칙을 지정해야 합니다.

자세한 내용은 기본 액세스 제어 정책 만들기, 1629 페이지를 참고하십시오.

단계 **3** **Intrusion Prevention(**침입 방지**)**을 액세스 제어 정책의 기본 작업으로 선택하고 TID 탐지를 위해 트래픽을 해독하려는 경우, SSL 정책을 액세스 제어 정책에 연결합니다(액세스 제어에 다른 정책 연결, 1641 페이지 참조).

단계 **4** `SHA-256` 관찰 가능 개체가 관찰 및 Firepower Management Center 이벤트를 생성하도록 하려면,

a) 하나 이상의 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙이 포함된 파일 정책을 생성합니다.

자세한 내용은 파일 정책 구성, 1868 페이지를 참고하십시오.

b) 이 파일 정책을 액세스 제어 정책의 하나 이상의 규칙과 연결합니다.

단계 **5** `IPv4`, `IPv6`, `URL` 또는 `Domain Name`(도메인 이름) 관찰이 연결 및 보안 인텔리전스 이벤트를 생성하도록 하려면 액세스 제어 정책에서 연결 및 보안 인텔리전스 로깅을 활성화합니다.

a) 파일 정책을 호출한 액세스 제어 규칙에서 **Log at End of Connection(**연결 종료 시 로깅**)** 및 **File Events: Log Files(**파일 이벤트**:** 로그 파일**)**를 활성화합니다(아직 활성화되지 않은 경우).

자세한 내용은 액세스 제어 규칙으로 연결 로깅, 2872 페이지를 참고하십시오.

b) 보안 인텔리전스 설정에서 기본 로깅**(DNS Policy(DNS** 정책**)**, **Networks(**네트워크**)**, **URLs(URL))** 이 활성화되어 있는지 확인합니다.

자세한 내용은 보안 인텔리전스로 연결 로깅, 2871 페이지를 참고하십시오.

단계 **6** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

다음에 수행할 작업

다음에서 나머지 항목 완료 설정 방법 Cisco Threat Intelligence Director(TID), 1914 페이지

데이터 소스 수집 옵션

사용하려는 데이터 유형 및 전달 메커니즘에 따라 구성 옵션을 선택합니다.

이러한 데이터 유형에 대한 자세한 내용은 소스 요구 사항, 1913 페이지를 참조하십시오.

표 115: 데이터 소스 수집 옵션

데이터 유형	수집 옵션
STIX	• TAXII 서버에서 STIX 피드 수집: 소스로 사용할 TAXII 피드 가져오기, 1917 페이지의 내용을 참조하십시오. • URL에서 STIX 데이터 다운로드: URL에서 소스 가져오기, 1918 페이지의 내용을 참조하십시오. • STIX 파일 업로드: 소스로 사용할 로컬 파일 업로드, 1920 페이지의 내용을 참조하십시오.
플랫 파일	• URL에서 데이터 다운로드: URL에서 소스 가져오기, 1918 페이지의 내용을 참조하십시오. • 플랫 파일 업로드: 소스로 사용할 로컬 파일 업로드, 1920 페이지의 내용을 참조하십시오.

소스로 사용할 TAXII 피드 가져오기

TID 구성 또는 작업 도중 문제가 발생하면 다음을 참조하십시오. 문제 해결 Cisco Threat Intelligence Director(TID), 1952 페이지

프로시저

단계 1 소스가 다음의 요구 사항을 충족하는지 확인합니다 소스 요구 사항, 1913 페이지

단계 2 **Intelligence(인텔리전스)** > **Sources(소스)**를 선택합니다.

단계 3 추가(+) 버튼을 클릭합니다.

단계 4 소스의 `Delivery(전달)` 방법으로 **TAXII**를 선택합니다.

단계 5 정보를 입력합니다.

- 호스트 서버가 암호화된 연결을 요구하는 경우, TID 소스의 TLS/SSL 설정 구성, 1921 페이지에 설명된 대로 **SSL Settings(SSL 설정)**를 구성합니다.
- TAXII 소스의 **Action(작업)** 선택 항목은 변경할 수 없습니다.

  `Block(차단)`은 TAXII 소스의 **Action(작업)** 옵션이 아닙니다. STIX 데이터에는 시스템이 차단할 수 없는 복잡한 지표가 포함될 수 있기 때문입니다. 디바이스(요소)는 단일 관찰 가능 개체를 저장하고 이에 기반하여 작업을 수행하며, 여러 관찰 가능 개체에 기반하여 작업을 수행할 수 없습니다.

하지만 수집 후에는 소스에서 얻은 개별 관찰 가능 개체와 간단한 지표를 차단할 수 있습니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참고하십시오.

- 피드 목록이 로드되려면 시간이 약간 걸릴 수 있습니다.
- **Update Every(**다음 간격으로 업데이트**)** 간격은 TID가 TAXII 소스에서 업데이트를 가져오는 빈도를 지정합니다.

  데이터 소스가 적절히 업데이트되는 업데이트 빈도를 설정하십시오. 예를 들어 소스가 하루에 3번 업데이트되는 경우, 최신 데이터를 정기적으로 캡처하려면 1440/3 또는 480분으로 업데이트 간격을 설정합니다.
- **TTL**로 지정한 일 수가 지나면 TID는 다음을 삭제합니다.
  - 후속 소스 업데이트에 포함되지 않은 소스의 모든 지표.
  - 남아 있는 지표가 참조하지 않는 모든 관찰 가능 개체.

단계 **6** 즉시 요소에 게시하려면 **Publish(**게시**)** 슬라이더( )가 활성화되어 있는지 확인합니다.

이 옵션이 활성화되면 시스템은 초기 소스 데이터 및 모든 후속 변경 사항을 자동으로 게시합니다.

자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지 섹션을 참조해 주십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- TAXII 피드에는 많은 양의 데이터가 포함될 수 있으므로 시스템이 모든 데이터를 수집하려면 시간이 걸릴 수 있습니다. 수집 상태를 보려면 Source(소스) 페이지를 새로 고칩니다.
- 이 소스에 대한 오류가 표시되면 마우스 포인터를 상태 아이콘 위로 가져가 세부 정보를 확인합니다.
- 초기 TID 구성을 수행하는 경우, 설정 방법 Cisco Threat Intelligence Director(TID), 1914 페이지로 돌아갑니다.

URL에서 소스 가져오기

TID가 호스트에서 파일을 가져오도록 하려면 URL 소스를 구성합니다.

TID 구성 또는 작업 도중 문제가 발생하면 다음을 참조하십시오. 문제 해결 Cisco Threat Intelligence Director(TID), 1952 페이지

프로시저

단계 1 소스가 다음의 요구 사항을 충족하는지 확인합니다 소스 요구 사항, 1913 페이지

단계 2 **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 3 추가(+) 버튼을 클릭합니다.

단계 4 소스의 `Delivery(전달)` 방법으로 **URL**을 선택합니다.

단계 5 양식을 작성합니다.

- 플랫 파일을 수집하는 경우, 소스에 포함된 데이터를 설명하는 **Type(**유형**)**을 선택합니다.
- 호스트 서버가 암호화된 연결을 요구하는 경우, TID 소스의 TLS/SSL 설정 구성, 1921 페이지에 설명된 대로 **SSL Settings(SSL** 설정**)**를 구성합니다.
- Name(이름): 지표에 기반한 인시던트 정렬 및 처리를 TID 단순화하려면 소스에서 일관된 명명 체계를 사용합니다. 예를 들어 <source>-<type>.

  소스 이름을 포함하면 추가 정보 또는 피드백을 위해 소스로 돌아가기가 단순화됩니다.

  이름을 일관되게 입력해야 합니다. 예를 들어 IPv4 주소가 있는 소스에는 항상 IPV4(IPv4 또는 ipv4 또는 IP_v4 또는 IP_V4 또는 ip-v4 또는 IP-v4, IP-V4 등이 아니라)를 사용할 수 있습니다.
- STIX 파일을 수집하는 경우, `Block(차단)`은 **Action(**작업**)** 옵션이 아닙니다. STIX 데이터에는 시스템이 차단할 수 없는 복잡한 지표가 포함될 수 있기 때문입니다. 디바이스(요소)는 단일 관찰 가능 개체를 저장하고 이에 기반하여 작업을 수행하며, 여러 관찰 가능 개체에 기반하여 작업을 수행할 수 없습니다.

  하지만 수집 후에는 소스에서 얻은 개별 관찰 가능 개체와 간단한 지표를 차단할 수 있습니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참고하십시오.
- 데이터 소스가 적절히 업데이트되는 업데이트 빈도를 설정하십시오. 예를 들어 소스가 하루에 3번 업데이트되는 경우, 최신 데이터를 정기적으로 캡처하려면 1440/3 또는 480분으로 업데이트 간격을 설정합니다.
- **TTL** 간격으로 지정한 일 수가 지나면 TID는 다음을 삭제합니다.
  - 후속 소스 업데이트에 포함되지 않은 소스의 모든 지표.
  - 남아 있는 지표가 참조하지 않는 모든 관찰 가능 개체.

단계 6 즉시 요소에 게시하려면 **Publish(**게시**)** 슬라이더( )가 활성화되어 있는지 확인합니다.

이 옵션이 활성화되면 시스템은 초기 소스 데이터 및 모든 후속 변경 사항을 자동으로 게시합니다.

자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지 섹션을 참조해 주십시오.

단계 7 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 수집 상태를 보려면 Source(소스) 페이지를 새로 고칩니다. 오류가 표시되면 마우스 포인터를 상태 아이콘 위로 가져가 세부 정보를 확인합니다.
- 초기 TID 구성을 수행하는 경우, 설정 방법 Cisco Threat Intelligence Director(TID), 1914 페이지로 돌아갑니다.

소스로 사용할 로컬 파일 업로드

이 절차는 로컬 파일의 일회성 수동 업로드에 사용하십시오.

STIX 파일을 수집할 때 TID는 STIX 파일의 콘텐츠에서 간단하거나 복잡한 지표를 생성합니다.

플랫 파일을 수집할 때 TID는 파일의 관찰 가능 개체 값마다 간단한 지표를 생성합니다.

TID 구성 또는 작업 도중 문제가 발생하면 문제 해결 Cisco Threat Intelligence Director(TID), 1952 페이지를 참조하십시오.

프로시저

단계 **1** 파일이 다음의 요구 사항을 충족하는지 확인합니다. 소스 요구 사항, 1913 페이지

단계 **2** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **3** 추가(➕) 버튼을 클릭합니다.

단계 **4** 소스의 `Delivery(전달)` 방법으로 **Upload(**업로드**)**를 선택합니다.

단계 **5** 양식을 작성합니다.

- 플랫 파일을 업로드하는 경우 소스에 포함된 데이터를 설명하는 **Type(**유형**)**을 선택합니다.
- Name(이름): 지표에 기반한 인시던트 정렬 및 처리를 TID 단순화하려면 소스에서 일관된 명명 체계를 사용합니다. 예를 들어 <source>-<type>.

  소스 이름을 포함하면 추가 정보 또는 피드백을 위해 소스로 돌아가기가 단순화됩니다.

  이름을 일관되게 입력해야 합니다. 예를 들어 IPv4 주소가 있는 소스에는 항상 IPV4(IPv4 또는 ipv4 또는 IP_v4 또는 IP_V4 또는 ip-v4 또는 IP-v4, IP-V4 등이 아니라)를 사용할 수 있습니다.
- STIX 파일을 업로드하는 경우, `Block(차단)`은 **Action(**작업**)** 옵션이 아닙니다. STIX 데이터에는 복잡한 지표가 포함될 수 있기 때문입니다. 디바이스(요소)는 단일 관찰 가능 개체를 저장하고 이에 기반하여 작업을 수행하며, 여러 관찰 가능 개체에 기반하여 작업을 수행할 수 없습니다.

  하지만 지표 또는 관찰 가능 개체 수준에서 간단한 지표를 차단할 수 있습니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참고하십시오.
- **TTL** 간격으로 지정한 일 수가 지나면 TID는 다음을 삭제합니다.
  - 후속 업로드에 포함되지 않은 소스의 모든 지표.
  - 남아 있는 지표가 참조하지 않는 모든 관찰 가능 개체.

단계 **6** 즉시 요소에 게시하려면 **Publish(**게시**)** 슬라이더( )가 활성화되어 있는지 확인합니다.

수집 시 소스를 게시하지 않으면 나중에 모든 소스를 한 번에 게시할 수 없으며, 대신 각 관찰 가능 개체를 개별적으로 게시해야 합니다. 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 수집 상태를 보려면 Source(소스) 페이지를 새로 고칩니다. 오류가 표시되면 마우스 포인터를 상태 아이콘 위로 가져가 세부 정보를 확인합니다.
- 초기 TID 구성을 수행하는 경우, 설정 방법 Cisco Threat Intelligence Director(TID), 1914 페이지로 돌아갑니다.

중복 표시기 처리

하나의 지표가 여러 소스에 포함된 경우, 다음과 같은 상황이 발생할 수 있습니다.

- 플랫 파일 소스의 지표 – 지표의 인스턴스마다 하나씩 인시던트를 생성하므로 특정 위협의 1회 발생으로 여러 인스턴스가 생성될 수 있습니다.
- STIX 소스의 지표 – 서로 다른 STIX 소스의 지표가 동일한 ID를 공유하는 경우, 이러한 지표를 포함하는 소스의 수에 상관없이 해당 지표에 대해 하나의 인시던트만 생성됩니다.

이후의 중복 인시던트를 방지하려면 중복된 지표 하나를 제외하고 모든 게시를 일시 중지하십시오. 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지의 내용을 참조하십시오.

TID 소스의 TLS/SSL 설정 구성

호스트 서버가 암호화된 연결을 요구하는 경우, **SSL Settings(SSL** 설정**)**를 구성합니다.

시작하기 전에

- 소스로 사용할 TAXII 피드 가져오기, 1917 페이지 또는 URL에서 소스 가져오기, 1918 페이지에 설명된 대로 `TAXII` 또는 `URL` 소스 구성을 시작합니다.

프로시저

단계 **1** **Edit Source(**소스 편집**)** 대화 상자에서 **SSL Settings(SSL** 설정**)** 섹션을 확장합니다.

단계 **2** 서버 인증서가 자체 서명된 경우:

a) **Self-Signed Certificate(**자체 서명 인증서**)**를 활성화합니다.

b) **SSL Hostname Verification(SSL** 호스트네임 확인**)** 방법을 선택합니다.

- Strict(엄격) - TID에서 소스 **URL**이 서버 인증서에서 제공된 호스트네임과 일치해야 합니다.

  호스트네임에 와일드카드가 포함된 경우, TID는 둘 이상의 서브도메인을 매칭할 수 없습니다.

- Browser Compatible(브라우저 호환) - TID에서 소스 **URL**이 서버 인증서에서 제공된 호스트네임과 일치해야 합니다.

  호스트네임에 와일드카드가 포함된 경우, TID는 모든 서브도메인을 매칭합니다.

- Allow All(모두 허용) - TID에서 소스 **URL**이 서버 인증서에서 제공된 호스트네임과 일치하지 않아도 됩니다.

예를 들어 subdomain1.subdomain2.cisco.com이 소스 **URL**이고 *.cisco.com이 서버 인증서에서 제공된 호스트네임인 경우:

- Strict(엄격) 호스트네임 확인이 실패합니다.
- Browser Compatible(브라우저 호환) 호스트네임 확인이 성공합니다.
- Allow All(모두 허용) 호스트네임 확인은 호스트네임 값을 완전히 무시합니다.

c) **Server Certificate(**서버 인증서**)**:

- PEM 인코딩된 자체 서명 서버 인증서에 액세스할 수 있는 경우, 텍스트 편집기에서 자체 서명 서버 인증서를 열고 BEGIN CERTIFICATE 및 END CERTIFICATE 행을 포함한 전체 텍스트 블록을 복사합니다. 이 전체 문자열을 필드에 입력합니다.
- 자체 서명 서버 인증서에 액세스할 수 없는 경우, 필드를 비워 둡니다. 소스를 저장한 후 TID는 서버에서 인증서를 검색합니다.

단계 **3** 서버가 사용자 인증서를 요구하는 경우:

a) **User Certificate(**사용자 인증서**)**를 입력합니다.

텍스트 편집기에서 PEM 인코딩된 인증서를 열고 BEGIN CERTIFICATE 및 END CERTIFICATE 행이 포함된 전체 텍스트 블록을 복사합니다. 이 전체 문자열을 필드에 입력합니다.

b) **User Private Key(**사용자 개인 키**)**를 입력합니다.

텍스트 편집기에서 개인 키 파일을 열고 BEGIN RSA PRIVATE KEY 및 END RSA PRIVATE KEY 행이 포함된 전체 텍스트 블록을 복사합니다. 이 전체 문자열을 필드에 입력합니다.

다음에 수행할 작업

- 인증서의 만료 날짜를 적어 둡니다. 현재 인증서가 만료된 후 새 서버 인증서를 입력하도록 일정 알림을 설정하는 것이 좋습니다.
- 계속 소스를 구성합니다.

• 소스로 사용할 TAXII 피드 가져오기, 1917 페이지
• URL에서 소스 가져오기, 1918 페이지

TID 액세스 권한이 있는 사용자 역할

Firepower Management Center 사용자 계정을 사용하여 TID 메뉴 및 페이지에 액세스할 수 있습니다.

- **Admin** 또는 **Threat Intelligence Director User** 사용자 역할이 있는 계정.
- **Intelligence** 권한을 포함하는 맞춤형 사용자 역할이 있는 계정.

또한 **Admin**, **Access Admin** 또는 **Network Admin** 사용자 역할이 있는 Firepower Management Center 사용자 계정을 사용하여 액세스 제어 정책에서 TID를 활성화하거나 비활성화할 수 있습니다.

사용자 계정에 대한 자세한 내용은 Firepower System 사용자 관리FMC의 사용자 계정, 49 페이지를 참조하십시오.

TID 데이터 백업 및 복구 정보

Firepower Management Center를 사용하여 TID에 필요한 모든 데이터(요소 데이터, 보안 인텔리전스 이벤트, 연결 이벤트, TID 구성 및 TID 데이터)를 백업하고 복구할 수 있습니다. 자세한 내용은 백업 및 복원, 203 페이지의 내용을 참고하십시오.

참고 고가용성 컨피그레이션인 활성 Firepower Management Center에서 TID를 호스팅하는 경우, 시스템은 TID 구성과 TID 데이터를 대기 Firepower Management Center에 동기화하지 않습니다. 페일오버 후 데이터를 복구할 수 있도록 활성 Firepower Management Center에서 정기적인 TID 데이터 백업을 수행하는 것을 권장합니다.

표 ***116: TID***-관련된 파일 백업 및 복구 내용

TID-관련된 파일 내용	선택 항목 백업	선택 항목 복구
요소 데이터	구성 백업	구성 데이터 복구
Firepower Management Center 이벤트 날짜	이벤트 백업	이벤트 데이터 복원
TID 구성 및 TID 데이터	**Threat Intelligence Director** 백업	**Threat Intelligense Director** 데이터 복구

TID 인시던트 및 관찰 데이터 분석

TID 요소에 의해 생성된 인시던트 및 관찰 데이터를 분석하려면 Incident(인시던트) 테이블 및 Incident Details(인시던트 세부 사항) 페이지를 사용합니다.

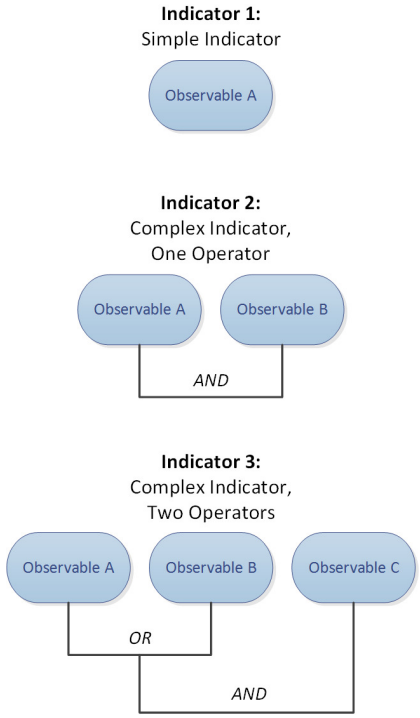
관찰 및 사고 생성

TID 지표의 첫 번째 관찰 가능 개체를 트래픽에서 볼 때 인시던트를 생성합니다. 간단한 지표는 단일 관찰 후 완전히 실현됩니다. 복잡한 지표는 하나 이상의 추가 관찰이 패턴을 충족할 때까지는 부분적으로 실현됩니다. 복잡한 지표는 단일 트랜잭션 도중에 반드시 충족될 필요는 없습니다. 각 관찰 가능 개체는 시간이 지나면서 서로 다른 트랜잭션에 의해 별도로 충족될 수 있습니다.

참고 지표의 패턴을 평가할 때 TID은 지원되지 않고 유효하지 않은 개체 그리고 Do Not Block(차단 금지) 리스트에 추가된 관찰 가능 개체는 무시합니다.

인시던트가 완전히 실현된 후 후속 관찰이 새로운 인시던트를 트리거합니다.

그림 *70:* 예*:* 지표 패턴



TID가 위의 예에서 관찰 가능 개체를 수집했고 관찰 가능 개체가 순서대로 보인 경우, 인시던트 생성은 다음과 같이 진행됩니다.

1. 시스템이 트래픽에서 관찰 가능 개체 A를 식별하는 경우, TID:

- 지표 1의 완전히 실현된 인시던트를 생성합니다.
- 지표 2 및 지표 3의 부분적으로 실현된 인시던트를 생성합니다.

2. 시스템이 트래픽에서 관찰 가능 개체 B를 식별하는 경우, TID:
   - 패턴이 충족되었기 때문에 인시던트를 지표 2의 완전 실현으로 업데이트합니다.
   - 인시던트를 지표 3의 부분적 실현으로 업데이트합니다.
3. 시스템이 트래픽에서 관찰 가능 개체 C를 식별하는 경우, TID:
   - 패턴이 충족되었기 때문에 인시던트를 지표 3의 완전 실현으로 업데이트합니다.
4. 시스템이 관찰 가능 개체 A를 두 번째 식별하는 경우, TID:
   - 지표 1의 완전히 실현된 새 인시던트를 생성합니다.
   - 지표 2 및 지표 3의 부분적으로 실현된 인시던트를 생성합니다.

특정 지표가 여러 소스에 존재하는 경우, 중복된 인시던트를 볼 수 있습니다. 자세한 내용은 문제 해결 Cisco Threat Intelligence Director(TID), 1952 페이지를 참고하십시오.

인시던트는 실제 트래픽에 의해서만 생성됩니다. URL B에 대한 관찰 가능 개체가 있고 사용자가 URL B에 대한 링크를 표시하는 URL A를 방문하는 경우, 사용자가 URL B 링크를 클릭하지 않는 한 인시던트가 발생하지 않습니다.

사고 보기 및 관리

Incidents(인시던트) 페이지에는 TID에 대한 요약 정보가 표시됩니다(사고 요약 정보, 1926 페이지 참조).

시작하기 전에

- 설정 방법 Cisco Threat Intelligence Director(TID), 1914 페이지에 설명된 대로 기능을 구성합니다.
- 관찰 및 사고 생성, 1924 페이지에 설명된 대로 관찰 및 인시던트 생성을 이해합니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Incidents(**인시던트**)**를 선택합니다.

단계 **2** 인시던트 보기:

- 하나 이상의 필터를 추가하려면 필터(🔍)을 클릭합니다. 기본 필터는 6시간입니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 1945 페이지를 참고하십시오.
- TID에 의해 인시던트가 마지막으로 업데이트된 날짜와 시간을 보려면 **Last Updated(**마지막 업데이트**)** 열의 값 위에 마우스 커서를 올려놓습니다.

- 인시던트에 연결된 지표에 대한 자세한 정보를 보려면 **Indicator Name(**지표 이름**)** 열의 텍스트를 클릭합니다(지표 보기 및 관리, 1940 페이지 참조).

단계 **3** **Incident ID(**인시던트 **ID)** 열의 값을 클릭하여 추가 세부 정보를 봅니다.

표시되는 세부 정보에 대한 설명은 사고 세부 사항, 1927 페이지를 참조하십시오.

- 지표 세부 정보를 보려면 창 하단 섹션의 **Indicator(**지표**)** 제목 아래에서 지표 값(예: IP 주소 또는 SHA-256 값)을 클릭합니다.
- 관찰 세부 정보를 보려면 **Observations(**관찰**)** 제목 바로 아래 있는 관찰 왼쪽 화살표를 클릭합니다.
- Security Intelligence Events(보안 인텔리전스 이벤트) 페이지에서 이 인시던트를 보려면 관찰 세부 정보 섹션에서 **Events(**이벤트**)** 링크를 클릭합니다.

단계 **4** (선택 사항) 인시던트 세부 정보 페이지에서 설명 정보를 입력합니다.

팁: 아래 옵션의 일관성과 효용성을 최대화하려면 명명 규칙, 카테고리 선택, 신뢰도 기준을 미리 계획하고 문서화하십시오.

- **Name(**이름**)**, **Description(**설명**)**, **Category(**카테고리**)** 필드에 원하는 값을 입력합니다.
- **Confidence(**신뢰도**)**의 등급 레벨을 클릭합니다.
- **Status(**상태**)** 필드의 드롭다운 목록에서 값을 선택하여 인시던트에 대한 조사 상태를 표시합니다.

사고 요약 정보

Incident(인시던트) 페이지에는 모든 TID 인시던트의 요약 정보가 표시됩니다.

표 ***117:*** 사고 요약 정보

필드	설명
Last Updated(마지막 업데이트 날짜**)**	시스템 또는 사용자가 인시던트를 마지막으로 업데이트한 후 경과한 일 수입니다. 업데이트 날짜와 시간을 보려면 이 열의 값 위에 마우스 커서를 올려놓습니다.

필드	설명
인시던트 **ID**	인시던트의 고유 식별자입니다. 이 ID는 다음 형식을 갖습니다. `<type>-<date>-<number>` • `<type>` - 인시던트에 관련된 지표 또는 관찰 가능 개체의 유형. 간단한 지표의 경우, 이 값은 관찰 가능 개체 유형(`IP`(IPv4 또는 IPv6), `URL`(URL), `DOM`(도메인) 또는 `SHA`(SHA-256))을 나타냅니다. 복잡한 지표의 경우, 이 값은 `COM`입니다. • `<date>` - 인시던트가 생성된 날짜(*yyyymmdd*). • `<number>` - 일일 인시던트 번호, 즉 인시던트의 일일 발생 시퀀스 중 어디에서 인시던트가 발생하는지 지정하는 번호입니다. 이 시퀀스는 0부터 시작됩니다. 예를 들어 `DOM-20170828-10`은 해당 날짜에 생성된 11번째 인시던트입니다. 시스템은 식별자 옆에 인시던트가 부분적으로 실현되는지 완전히 실현되는지 보여주는 아이콘을 표시합니다. 자세한 내용은 관찰 및 사고 생성, 1924 페이지를 참고하십시오.
지표 이름	인시던트에 관련된 지표의 이름입니다. 지표에 대한 추가 정보를 보려면 이 열의 값을 클릭합니다(지표 보기 및 관리, 1940 페이지 참조).
유형	인시던트에 관련된 지표의 유형입니다. • 단일 관찰 가능 개체를 포함하는 지표는 데이터 유형(`URL`, `SHA-256` 등)을 표시합니다. • 둘 이상의 관찰 가능 개체를 포함하는 지표는 `Complex`로 표시됩니다.
수행한 작업	인시던트와 관련하여 시스템에서 수행한 작업입니다. 자세한 내용은 사고 세부 사항, 1927 페이지를 참고하십시오.
상태	인시던트에 대한 조사의 상태입니다. 자세한 내용은 사고 세부 사항, 1927 페이지를 참고하십시오.
삭제( )	인시던트를 영구적으로 삭제하려면 이 아이콘을 클릭합니다.

사고 세부 사항

Indicdent Details(인시던트 세부 사항) 창에는 단일 TID 인시던트에 대한 정보가 표시됩니다. 이 창은 2개의 섹션으로 나뉩니다.

- 인시던트 세부 사항: 기본 정보, 1927 페이지
- 사고 세부 사항: 지표 및 관찰, 1929 페이지

인시던트 세부 사항: 기본 정보

Incident Details(인시던트 세부 사항) 창의 상단 섹션은 아래에 설명된 정보를 제공합니다.

표 *118: Basic Incident Information(*기본 인시던트 정보*)* 필드

필드	설명
Partially-Realized *IncidentID* 또는 **Fully-Realized** *IncidentID*	인시던트의 고유 식별자 외에 인시던트의 상태(부분적으로 실현 또는 완전히 실현)를 나타내는 아이콘입니다. 참고 인시던트의 상태를 확인할 때 TID는 지원되지 않으며 유효하지 않은 관찰 가능 개체와 차단 안 함 목록의 관찰 가능 개체를 무시합니다.
열림	인시던트를 마지막으로 업데이트한 날짜와 시간입니다.
이름	사용자가 직접 입력하는 선택적인 맞춤형 인시던트 이름입니다. 팁: Description(설명) 필드(창의 하단)에 소스의 정보가 있는 경우, 해당 필드의 정보를 사용하여 인시던트의 이름을 지정합니다.
설명	사용자가 직접 입력하는 선택적인 맞춤형 인시던트 설명입니다. 팁: Description(설명) 필드(창의 하단)에 소스의 정보가 있는 경우, 해당 필드의 정보를 사용하여 인시던트를 설명합니다.
감시	인시던트 내의 관찰 횟수입니다.
확신	인시던트의 상대적 중요성을 표시하기 위해 직접 선택할 수 있는 선택적 등급입니다.
수행한 작업	`Monitored(모니터링됨)`, `Blocked(차단됨)` 또는 `Partially Blocked(부분적으로 차단됨)`와 같이 시스템이 수행한 작업입니다. `Partially Blocked(부분적으로 차단됨)`는 인시던트에 `Monitored(모니터링됨)` 관찰과 `Blocked(차단됨)` 관찰이 모두 포함됨을 나타냅니다. 참고 **Action Taken(**수행한 작업**)**은 반드시 TID에서 선택한 작업이 아니라 시스템이 수행한 작업을 나타냅니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 1933 페이지를 참고하십시오.
카테고리	사용자가 인시던트에 직접 추가하는 선택적 맞춤형 태그 또는 키워드입니다.
상태	인시던트 분석의 현재 상태를 나타내는 값입니다. **Status(**상태**)**를 처음 변경하기 전까지 모든 인시던트는 `New(신규)`입니다. 이 필드는 선택 항목입니다. 조직의 요구 사항에 따라 다음과 같은 상태 값을 사용하는 것이 좋습니다. • `New(신규)` - 인시던트에 조사가 필요하지만 조사를 아직 시작하지 않았습니다. • `Open(열림)` - 현재 인시던트를 조사하고 있습니다. • `Closed(닫힘)` - 인시던트를 조사했고 조치를 취했습니다. • `Rejected(거부됨)` - 인시던트를 조사했고 취할 조치가 없다고 결정했습니다.

필드	설명
삭제( )	이 아이콘을 클릭하면 이 인시던트가 영구적으로 삭제됩니다.

사고 세부 사항: 지표 및 관찰

Incident Details(인시던트 세부 사항) 창의 하단 섹션은 지표 및 관찰 정보의 자세한 보기를 제공합니다. 이 정보는 **Indicator(**지표**)** 필드, 지표 패턴, **Observations(**관찰**)** 필드로 구성됩니다.

지표 섹션

처음으로 지표 세부 정보를 볼 때 이 섹션에는 지표 이름만 표시됩니다.

Indicator(지표) 페이지에서 지표를 보려면 지표 이름을 클릭합니다.

지표에서 나가지 않고 더 많은 지표 세부 정보를 보려면 지표 이름 옆의 아래쪽 화살표를 클릭합니다. 세부 사항 필드에는 다음이 포함됩니다.

표 ***119:*** 지표 필드

필드	설명
설명	소스에서 제공하는 지표 설명입니다.
소스	지표가 포함된 소스입니다. 전체 소스 세부 사항에 액세스하려면 이 링크를 클릭합니다.
만료	소스의 **TTL** 값에 따라 인시던트가 만료되는 날짜와 시간입니다.
조치	지표와 관련된 조치입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참고하십시오.
게시	지표의 게시 설정입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참고하십시오.
STIX 다운로드	소스 유형이 `STIX`인 경우, 이 버튼을 클릭하여 STIX 파일을 다운로드합니다.

지표 패턴

지표 패턴은 지표를 구성하는 관찰 가능 개체와 연산자를 그림으로 나타낸 것입니다. 연산자는 지표 내에서 관찰 가능 개체를 연결합니다. AND 관계는 **AND** 연산자로 표시됩니다. OR 관계는 **OR** 연산자로 또는 여러 관찰 가능 개체를 밀접히 그룹화하여 표시됩니다.

패턴의 관찰 가능 개체가 이미 보인 경우, 관찰 가능 개체 상자는 흰색입니다. 관찰 가능 개체가 아직 보이지 않은 경우, 관찰 가능 개체 상자는 회색입니다.

지표 패턴에서,

- **Whitelist(**화이트리스트**)** 버튼을 클릭하여 차단 안 함 목록에 관찰 가능 개체를 추가합니다. 이 아이콘은 흰색 및 회색 관찰 가능 개체 상자에 있습니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 1951 페이지를 참고하십시오.
- 흰색 관찰 가능 개체 상자 위에 커서를 올려놓으면 **Observations(**관찰**)** 섹션에서 관련 관찰이 강조 표시됩니다.
- 흰색 관찰 가능 개체 상자를 클릭하면 시스템은 **Observations(**관찰**)** 섹션에서 관련 관찰을 강조 표시하고, 해당 관찰을 보기로 스크롤하며(여러 관찰이 있는 경우), 해당 관찰의 상세한 표시를 확장합니다.
- 지표 패턴에서 회색 관찰 가능 개체 상자 위에 커서를 올려놓거나 클릭하면 **Observations(**관찰**)** 섹션에 아무 변화도 없습니다. 관찰 가능 개체가 보이지 않으므로 아직 표시할 관찰 세부 정보가 없습니다.

관찰 섹션

기본적으로 **Observations(**관찰**)** 섹션에는 다음을 포함한 요약 정보가 표시됩니다.

- 관찰을 트리거한 관찰 가능 개체의 유형(예를 들어 도메인)
- 관찰 가능 개체를 구성하는 데이터
- 관찰이 첫 번째 관찰인지 후속 관찰인지 여부(예를 들어 첫 번째 또는 세 번째)

참고 단일 관찰 가능 개체가 세 번 이상 보인 경우, TID는 첫 번째 및 마지막 관찰 세부 사항을 표시합니다. 중간 관찰에 대한 세부 사항은 사용할 수 없습니다.

- 관찰 날짜 및 시간
- 관찰 가능 개체에 대해 구성된 작업

Observations(관찰**)** 섹션에서 관찰 위에 커서를 올려놓으면 지표 패턴에서 관련된 관찰 가능 개체가 강조 표시됩니다.

Observations(관찰**)** 섹션에서 관찰을 클릭하면 시스템은 지표 패턴에서 관련된 관찰 가능 개체를 강조 표시하고 첫 번째 관련 가능 개체를 보기로 스크롤합니다(여러 관찰 가능 개체가 있는 경우). 관찰을 클릭하면 **Observations(**관찰**)** 섹션에서 관찰의 세부 사항이 확장됩니다.

관찰 세부 사항에는 다음 필드가 포함됩니다.

표 ***120:*** 관찰 세부 정보 필드

필드	설명
소스	관찰을 트리거한 트래픽의 소스 IP 주소와 포트입니다.

필드	설명
대상	관찰을 트리거한 트래픽의 대상 IP 주소와 포트입니다.
추가 정보	관찰을 트리거한 트래픽과 관련된 DNS 및 인증 정보입니다.
Events(이벤트)	클릭 가능한 이 링크에는 관찰이 연결, 보안 인텔리전스, 파일 또는 악성코드 이벤트를 생성했는지 표시됩니다. Firepower Management Center 이벤트 테이블의 이벤트를 보려면 링크를 클릭합니다(연결 이벤트 정보, 2875 페이지 참조).

TID 관찰에 대한 이벤트 보기

TID 관찰이 생성하는 Firepower Management Center 이벤트에 대한 자세한 내용은 Firepower Management Center 이벤트의 TID 관찰, 1931 페이지를 참조하십시오.

TID 관련 이벤트에 대해 로깅되는 시스템 작업은 TID와 다른 Firepower Management Center 기능의 상호 작용에 따라 달라질 수 있습니다. 작업 우선 순위에 대한 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 1933 페이지를 참조하십시오.

시작하기 전에

- 설정 방법 Cisco Threat Intelligence Director(TID), 1914 페이지에 설명된 대로 기능을 구성합니다.
- 지원할 정책 구성 TID, 1915 페이지에 설명된 대로 TID에 필요한 이벤트 로깅을 활성화했는지 확인합니다.

프로시저

단계 **1** **Intelligence(인텔리전스)** > **Incidents(인시던트)**를 선택합니다.

단계 **2** 인시던트의 **Incident ID(인시던트 ID)** 값을 클릭합니다.

단계 **3** 관찰 상자를 표시하려면 **Indicator(지표)** 섹션에서 관찰을 클릭합니다.

단계 **4** 관찰 상자 왼쪽 상단 모서리에 있는 화살표를 클릭하여 관찰 상자를 확장합니다.

단계 **5** 관찰 정보에서 **Events(이벤트)** 링크를 클릭합니다. 보안 인텔리전스 표시에 대한 자세한 내용은 연결 이벤트 정보, 2875 페이지를 참조하십시오.

Firepower Management Center 이벤트의 TID 관찰

액세스 제어 정책을 완전히 구성하면 TID 관찰은 다음 Firepower Management Center 이벤트를 생성합니다.

표 *121: Firepower Management Center* 관찰이 생성하는 이벤트

관찰 콘텐츠	연결 이벤트 테이블	보안 인텔리전스 이벤트 테이블	파일 이벤트 테이블	악성코드 이벤트 테이블
SHA-256	예	아니요	예	예, 속성이 악성코드 또는 맞춤형 탐지인 경우.
도메인 이름, **URL** 또는 **IPv4/IPv6**	Yes(예) TID 관련 연결 이벤트는 TID 관련 보안 인텔리전스 카테고리 값으로 식별됩니다.	Yes(예) TID 관련 보안 인텔리전스 이벤트는 TID 관련 보안 인텔리전스 카테고리 값으로 식별됩니다.	아니요	아니요

수행하는 작업에 영향을 미치는 요소

TID 관찰 가능 개체와 일치하는 트래픽이 탐지될 때 시스템이 수행하는 작업과 작업을 수행하는 시기는 여러 요인이 결정합니다.

- 보안 인텔리전스와 같은 기능은 TID 전에 작업을 수행합니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 1933 페이지 섹션을 참조해 주십시오.
- 일반적으로는 관찰 가능 개체에 대해 구성된 작업(상위 지표 또는 소스에 대해 구성된 작업과 다를 수 있음)이 수행됩니다.
- STIX 소스에는 복잡한 지표가 포함될 수 있으므로 소스에 대한 작업 설정은 Monitor(모니터링)으로만 설정할 수 있습니다. 하지만 STIX 피드 또는 파일에 포함된 개별적인 간단한 지표 또는 관찰 가능 개체는 Block(차단)으로 설정할 수 있습니다.
- 지표 및 관찰 가능 개체에 대한 작업 설정은 상속되거나 상속을 재정의하도록 개별적으로 구성될 수 있습니다. TID 구성의 상속, 1945 페이지 및 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참조하십시오.
- 아니면 실행 가능한 트래픽이 차단 안 함 목록에 있을 수 있습니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가, 1951 페이지 섹션을 참조해 주십시오.
- 부분적으로 실현된 인시던트 및 완전히 실현된 인시던트에 대해 구성된 작업이 수행됩니다.
- 복잡한 지표에 기반하는 인시던트는 부분적으로 차단될 수 있습니다. 이는 지표에 모니터링되는 관찰과 차단된 관찰이 모두 포함된 경우에 발생할 수 있습니다.
- 게시를 일시 중지하면 시스템이 수행하는 작업에 영향을 미칩니다. 게시 일시 중지 정보, 1948 페이지 및 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참조하십시오.
- TID 기능을 일시 중지하면 모든 작업이 수행되지 않습니다. 기능을 다시 시작한 후 실행 가능한 데이터가 전과 다를 수 있습니다. 자세한 내용은 TID 일시 중지 및 요소에서 TID 데이터 제거, 1949 페이지를 참조하십시오.

TID-Firepower Management Center 작업 우선 순위

TID 관찰 가능 개체 작업이 Firepower Management Center 정책 작업과 충돌하는 경우, 시스템은 다음과 같이 작업 우선 순위를 지정합니다.

- 보안 인텔리전스 차단 금지
- TID 차단
- 보안 인텔리전스 차단
- TID 모니터링
- 보안 인텔리전스 모니터링

구체적으로,

표 ***122: TID URL*** 관찰 가능 개체 작업 대 보안 인텔리전스 작업

설정: 보안 인텔리전스 작업	설정: **TID** 관찰 가능 개체 작업	**TID** 인시던트 필드: 수행한 작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
화이트리스트	`Monitor(모니터링)` 또는 `Block(차단)`	TID 인시던트 없음	보안 인텔리전스 이벤트 없음		
차단	모니터링	차단됨	차단	시스템 분석에서 결정. 다음 참조. 보안 인텔리전스 카테고리, 1702 페이지	`URL 차단`
	차단	차단됨	차단	`TID URL 차단`	`URL 차단`
모니터링	모니터링	모니터링됨	보안 인텔리전스 및 TID 후에 처리되는 액세스 제어 규칙에 의해 결정됩니다.	`TID URL 모니터링`	`URL 모니터링`
	차단	차단됨	차단	`TID URL 차단`	`URL 차단`

표 ***123: TID IPv4/IPv6*** 관찰 가능 개체 작업 대 보안 인텔리전스 작업

설정: 보안 인텔리전스 작업	설정: **TID** 관찰 가능 개체 작업	**TID** 인시던트 필드: 수행한 작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
화이트리스트	Monitor(모니터링) 또는 Block(차단)	TID 인시던트 없음	보안 인텔리전스 이벤트 없음		
차단	모니터링	TID 인시던트 없음	차단	시스템 분석에서 결정. 다음 참조. 보안 인텔리전스 카테고리, 1702 페이지	IP 차단
	차단	차단됨	차단	TID IPv4 차단 TID IPv6 차단	IP 차단
모니터링	모니터링	모니터링됨	보안 인텔리전스 및 TID 후에 처리되는 액세스 제어 규칙에 의해 결정됩니다.	TID IPv4 모니터링 TID IPv6 모니터링	IP Monitor
	차단	차단됨	차단	TID IPv4 차단 TID IPv6 차단	IP 차단

표 ***124: TID*** 도메인 이름 관찰 가능 개체 작업 대 ***DNS*** 정책 작업

설정: **DNS** 정책 작업	설정: **TID** 도메인 이름 관찰 가능 개체 작업	**TID**인시던트필드:수행한 작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
화이트리스트	Monitor(모니터링) 또는 Block(차단)	TID 인시던트 없음	보안 인텔리전스 이벤트 없음		
삭제, 도메인을 찾을 수 없음 싱크 홀 - 로그 싱크 홀 - 차단 및 로그	모니터링	차단됨	차단	시스템 분석에서 결정. 다음 참조. 보안 인텔리전스카테고리,1702페이지	DNS 차단
	차단	차단됨	차단	TID 도메인 이름 차단	DNS 차단

설정: **DNS** 정책 작업	설정: **TID** 도메인 이름 관찰 가능 개체 작업	**TID**인시던트 필드:수행한 작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
모니터링	모니터링	모니터링됨	보안 인텔리전스 및 TID 후에 처리되는 액세스 제어 규칙에 의해 결정됩니다.	TID 도메인 이름 모니터링	DNS 모니터링
	차단	차단됨	차단	TID 도메인 이름 차단	DNS 차단

표 ***125: TID SHA-256*** 관찰 가능 개체 작업 대 악성코드 클라우드 조회 파일 정책

파일 속성	**TID SHA-256** 관찰 가능 개체 작업	**TID** 인시던트의 수행한 작업	파일 이벤트의 작업	악성코드 이벤트의 작업
정상	Monitor(모니터링) 또는 Block(차단)	모니터링됨	악성코드 클라우드 조회	해당 없음
악성코드	Monitor(모니터링) 또는 Block(차단)	모니터링됨	악성코드 클라우드 조회	해당 없음
Custom	Monitor(모니터링) 또는 Block(차단)	모니터링됨	• 악성코드 클라우드 조회, SHA-256이 맞춤형 탐지 목록에 없는 경우. • 맞춤형 탐지, SHA-256이 맞춤형 탐지 목록에 있는 경우.	• 악성코드 클라우드 조회, SHA-256이 맞춤형 탐지 목록에 없는 경우. • 맞춤형 탐지, SHA-256이 맞춤형 탐지 목록에 있는 경우.
알 수 없음	Monitor(모니터링) 또는 Block(차단)	모니터링됨	악성코드 클라우드 조회	해당 없음

참고 TID 매칭은 시스템이 동적 분석을 위해 파일을 전송하기 전에 이루어집니다.

표 ***126: TID SHA-256*** 관찰 가능 개체 작업 대 악성코드 파일 차단 정책

파일 속성	**TID SHA-256** 관찰 가능 개체 작업	**TID** 인시던트의 수행한 작업	파일 이벤트의 작업	악성코드 이벤트의 작업
Clean(안전) 또는 Unknown(알 수 없음)	모니터링	모니터링됨	악성코드 클라우드 조회	해당 없음
	차단	차단됨	• TID 차단, SHA-256이 맞춤형 탐지 목록에 없는 경우. 수정된 파일 속성은 Custom(맞춤형) 입니다. • 맞춤형 탐지 차단, SHA-256이 맞춤형 탐지 목록에 있는 경우.	TID 차단 수정된 파일 속성은 Custom(맞춤형) 입니다.
Malware(악성코드) 또는 Custom(맞춤형)	모니터링	차단됨	악성코드 차단	악성코드 차단
	차단	차단됨	• TID 차단, SHA-256이 맞춤형 탐지 목록에 없는 경우. 수정된 파일 속성은 Custom(맞춤형) 입니다. • 맞춤형 탐지 차단, SHA-256이 맞춤형 탐지 목록에 있는 경우.	TID 차단 수정된 파일 속성은 Custom(맞춤형) 입니다.

Cisco Threat Intelligence Director(TID) 구성 보기 및 변경

다음 정보를 사용하여 구성을 검토하고 필요에 따라 미세 조정합니다.

요소(매니지드 디바이스)의 TID 상태 보기

Firepower Management Center에 매니지드 디바이스로 등록된 모든 디바이스는 Elements(요소) 페이지에 자동으로 표시됩니다. 올바로 구성된 모든 요소(지원할 정책 구성 TID, 1915 페이지에 지정된 대로)는 요소가 추가되기 전에 수집된 관찰 가능 개체를 포함하여 현재 게시된 모든 관찰 가능 개체를 수신합니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Elements(**요소**)**를 선택합니다.

단계 **2** 요소가 연결되어 있고 TID이(가) 활성화되어 있는지 확인하려면 요소 이름 옆에 있는 아이콘 위에 마우스를 올려 놓습니다.

참고 구축 후 적용된 액세스 제어 정책 및 TID 활성화 여부를 포함하여 이 페이지의 정보가 업데이트되는 데 최대 5분이 걸릴 수 있습니다.

소스 보기 및 관리

Source(소스) 페이지에는 구성된 모든 소스에 대한 요약 정보가 표시됩니다(소스 요약 정보, 1938 페이지 참조).

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **2** 소스 보기:

- 페이지에 표시된 소스를 필터링하려면 필터( )을 클릭합니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 1945 페이지를 참고하십시오.
- 자세한 수집 상태를 보려면 **Status(**상태**)** 열에 있는 텍스트 위에 커서를 올려놓습니다. 자세한 내용은 소스 상태 세부 사항, 1939 페이지를 참고하십시오.

단계 **3** 소스 관리:

- **Action(**작업**)** 설정을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참조하십시오. 작업이 고정되어 있다면 그것이 소스 **Type(**유형**)**에 대해 지원되는 유일한 작업입니다.
- **Publish(**게시**)** 설정을 수정하려면 슬라이더( )를 클릭합니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참고하십시오.

- 소스 TID 업데이트를 일시 중지하거나 재개하려면 **Pause Updates(**업데이트 일시 중지**)** 또는 **Resume Updates(**업데이트가 재개**)**를 클릭합니다. 업데이트를 일시 중지하면 업데이트는 일시 중지되지만 기존 지표와 관찰 가능 개체는 TID에 남아 있습니다.
- 소스를 삭제하려면 삭제( )을 클릭합니다. 소스가 여전히 처리 중이면 아이콘이 회색으로 표시됩니다. 소스를 삭제하면 해당 소스에 연결된 모든 지표가 삭제됩니다. 연결된 관찰 가능 개체도 삭제될 수 있지만 시스템에 남아 있는 지표와 연결된 경우에는 보존됩니다.

소스 요약 정보

Source(소스) 페이지에는 구성된 모든 소스의 요약 정보가 표시됩니다. 아래 표에는 요약 표시의 필드에 대한 간략한 설명이 나와 있습니다. 이러한 필드에 대한 자세한 내용은 소스와 관련된 구성 항목의 설명을 참조하십시오(데이터 소스 수집 옵션, 1916 페이지 참조).

표 ***127:*** 소스 요약 정보

필드	설명
이름	소스 이름입니다.
유형	소스의 데이터 형식입니다(`STIX` 또는 `플랫 파일`).
전달	TID가 소스 검색에 사용하는 방법입니다.
조치	이 소스 내에 포함된 데이터와 일치하는 트래픽에 대해 시스템이 수행하도록 구성된 작업(`Block(차단)` 또는 `Monitor(모니터링)`)입니다. 가용성, 상속, 상속 재정의 등 TID 작업에 대한 자세한 내용은 수행하는 작업에 영향을 미치는 요소, 1932 페이지를 참조하십시오.
게시	TID가 소스의 데이터를 등록된 요소(TID를 지원하도록 구성된 매니지드 디바이스)에 게시하는지 여부를 지정하는 `켜기` 또는 `끄기` 토글입니다. 지표는 상위 소스로부터 **Publish(**게시**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(**게시**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 1945 페이지를 참고하십시오.
Last Updated(마지막 업데이트 날짜**)**	TID가 소스를 마지막으로 업데이트한 날짜와 시간입니다.

필드	설명
상태	소스의 현재 상태: • **New(**신규**)** - 소스가 새로 생성되었습니다. • **Scheduled(**예약됨**)** - 초기 다운로드 또는 후속 업데이트가 예약되었지만 아직 진행 중이 아닙니다. • **Downloading(**다운로드 중**)** - TID가 초기 다운로드 또는 업데이트 새로 고침을 수행 중입니다. • **Parsing(**구문 분석 중**)** 또는 **Processing(**처리 중**)** - TID가 소스를 수집하고 있습니다. • **Completed(**완료**)** - TID가 소스 수집을 완료했습니다. • **Completed with Errors(**오류와 함께 완료**)** - TID가 소스 수집을 완료했지만, 일부 관측 가능 개체가 지원되지 않거나 잘못되었습니다. • **Error(**오류**)** - TID에 문제가 발생했습니다. 소스가 **Update Frequency(**업데이트 빈도**)**가 지정된 TAXII 또는 URL 소스이고 업데이트가 일시 중지되지 않은 경우, TID는 예약된 다음 업데이트에서 다시 시도합니다. 상태를 업데이트하려면 페이지를 새로 고칩니다.
수정( )	이 아이콘을 클릭하면 소스에 대한 설정을 수정할 수 있습니다.
삭제( )	이 아이콘을 클릭하면 소스가 영구적으로 삭제됩니다.

소스 상태 세부 사항

Sources(소스) 요약 페이지에서 소스의 **Status(**상태**)** 값에 커서를 올려놓으면 TID에서 아래 설명된 추가 세부 정보를 제공합니다.

데이터	설명
상태 메시지	소스의 현재 상태를 간략하게 설명합니다.
마지막 업데이트 날짜	TID가 소스를 마지막으로 업데이트한 날짜와 시간을 지정합니다.
다음 업데이트	TAXII 및 URL 소스의 경우, 이 값은 TID가 다음에 소스를 업데이트할 시기를 지정합니다.

데이터	설명
지표	지표 개수를 지정합니다. • **Consumed(사용됨)** - 가장 최근 소스 업데이트 중에 TID가 처리한 지표 수입니다. 이 숫자는 수집 또는 삭제 여부에 상관없이 업데이트에 포함된 모든 지표를 나타냅니다. • **Discarded(삭제됨)** - 가장 최근 업데이트 중에 시스템이 TID에 추가하지 않은 잘못된 형식의 지표 수입니다. 참고 TAXII 소스의 경우, TAXII 업데이트는 기존 데이터를 교체하지 않고 증분 데이터를 추가하기 때문에 TID에서는 별도의 **Last Update(마지막 업데이트)** 및 **Total(총)** 지표 개수를 제공합니다. 다른 소스 유형의 지표는 소스가 기존 데이터 세트를 완전히 대체하므로 TID는 **Last Update(마지막 업데이트)** 개수만 제공합니다. 지표의 모든 관찰 가능 개체가 **Invalid(잘못됨)**인 경우, TID는 지표를 삭제합니다.
관찰 가능 항목	관찰 가능 개체 개수를 지정합니다. • **Consumed(사용됨)** - 가장 최근 소스 업데이트 중에 TID가 처리한 관찰 가능 개체 수입니다. 이 숫자는 수집 또는 삭제 여부에 상관없이 업데이트에 포함된 모든 관찰 가능 개체를 나타냅니다. • **Unsupported(지원되지 않음)** - 가장 최근 업데이트 중에 시스템이 TID에 추가하지 않은 지원되지 않는 관찰 가능 개체 수입니다. 지원되는 관찰 가능 개체 유형에 대한 자세한 내용은 소스 요구 사항, 1913 페이지의 콘텐츠 유형에 대한 정보를 참조하십시오. • **Invalid(유효하지 않음)** - 가장 최근 업데이트 중에 시스템이 TID에 추가하지 않은 유효하지 않은 관찰 가능 개체 수입니다. 유효하지 않은 관찰 가능 개체는 잘못 구성된 관찰 가능 개체입니다. 예를 들어 `10.10.10.10.123`는 유효한 IPv4 주소가 아닙니다. 참고 TAXII 소스의 경우, TAXII 업데이트는 기존 데이터를 교체하지 않고 증분 데이터를 추가하기 때문에 TID에서는 별도의 **Last Update(마지막 업데이트)** 및 **Total(총)** 관찰 가능 개체 개수를 제공합니다. 다른 소스 유형의 관찰 가능 개체는 소스가 기존 데이터 세트를 완전히 대체하므로 TID는 **Last Update(마지막 업데이트)** 개수만 제공합니다.

지표 보기 및 관리

지표는 수집된 소스에서 자동으로 생성됩니다. 이 페이지의 정보에 대한 자세한 내용은 지표 요약 정보, 1941 페이지를 참조하십시오.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **2** **Indicators(**지표**)**를 클릭합니다.

단계 **3** 현재 지표 보기:

- 페이지에 표시된 지표를 필터링하려면 필터( )을 클릭합니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 1945 페이지를 참고하십시오.
- 지표(연결된 관찰 가능 개체 포함)에 대한 추가 세부 정보를 보려면 지표 이름을 클릭합니다. 자세한 내용은 지표 세부사항, 1942 페이지를 참고하십시오.
- **Incidents(**인시던트**)** 열에서 번호를 클릭하여 지표에 연결된 인시던트에 대한 정보를 보거나 인시던트 위에 커서를 올려놓아 인시던트가 완전히 실현되었는지 부분적으로 실현되었는지 확인합니다.
- TID가 소스로부터 지표 수집을 완료했는지 확인하려면 **Status(**상태**)** 열을 보십시오.

단계 **4** 현재 지표 관리:

- **Action(**작업**)**을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참조하십시오. 작업이 고정되어 있다면 그것이 소스 **Type(**유형**)**에 대해 지원되는 유일한 작업입니다.
- **Publish(**게시**)** 설정을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참조하십시오.
- 지표의 관찰 가능 개체 하나 이상을 차단 안 함 목록에 추가하려면 지표 이름을 클릭하여 Indicator Details(지표 세부 사항) 페이지에 액세스합니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 1951 페이지를 참고하십시오.

지표 요약 정보

Indicators(지표) 페이지에는 구성된 소스에 연결된 모든 지표에 대한 요약 정보가 표시 됩니다.

표 ***128:*** 지표 요약 정보

필드	설명
유형	• 단일 관찰 가능 개체를 갖는 지표는 해당 관찰 가능 개체의 데이터 유형(URL, SHA-256 등)을 나열합니다. • 둘 이상의 관찰 가능 개체를 포함하는 지표는 `Complex`로 나열됩니다. 특정 관찰 가능 개체를 보려면 유형 위에 커서를 올려놓습니다.
이름	지표 이름입니다.

필드	설명
소스	지표가 포함된 소스입니다(상위 소스).
인시던트	지표와 연결된 인시던트에 대한 정보: • 인시던트가 부분적으로 실현되는지 완전히 실현되는지 지정하는 아이콘 • 지표에 연결된 인시던트 수
조치	지표와 관련된 조치입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참고하십시오. 지표는 상위 소스로부터 **Action(**작업**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Action(**작업**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 1945 페이지를 참고하십시오.
게시	지표의 게시 설정입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참고하십시오. 지표는 상위 소스로부터 **Publish(**게시**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(**게시**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 1945 페이지를 참고하십시오.
Last Updated(마지막 업데이트 날짜**)**	TID가 지표를 마지막으로 업데이트한 날짜와 시간입니다.
상태	지표의 현재 상태: • **Pending(**보류 중**)** - TID가 지표의 관찰 가능 개체를 수집하는 중입니다. • **Completed(**완료**)** - TID가 지표의 모든 관찰 가능 개체를 성공적으로 수집했습니다. • **Completed With Errors(**오류와 함께 완료**)** - TID가 지표 수집을 완료했지만 일부 관측 가능 개체가 지원되지 않거나 유효하지 않습니다.

지표 세부사항

Indicator Details(지표 세부 사항) 페이지에는 인시던트의 지표 및 관찰 가능 개체가 표시됩니다.

표 ***129:*** 지표 세부 사항 정보

필드	설명
이름	지표 이름입니다.
설명	소스에서 제공하는 지표 설명입니다.

필드	설명
소스	지표가 포함된 소스입니다.
만료	소스의 **TTL** 값에 따라 지표가 만료되는 날짜와 시간입니다.
조치	지표와 관련된 조치입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참고하십시오. 지표는 상위 소스로부터 **Action(**작업**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Action(**작업**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 1945 페이지를 참고하십시오.
게시	지표의 게시 설정입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참고하십시오. 지표는 상위 소스로부터 **Publish(**게시**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(**게시**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 1945 페이지를 참고하십시오.
지표 패턴	지표의 패턴을 구성하는 관찰 가능 개체와 연산자입니다. 연산자는 지표 내에서 관찰 가능 개체를 연결합니다. AND 관계는 **AND** 연산자로 표시됩니다. OR 관계는 **OR** 연산자로 또는 여러 관찰 가능 개체를 밀접히 그룹화하여 표시됩니다. 필요에 따라 **Whitelist(**화이트리스트**)** 버튼을 클릭하여 차단 안 함 목록에 관찰 가능 개체를 추가합니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 1951 페이지를 참고하십시오.

관찰 가능 개체 보기 및 관리

Observables(관찰 가능 개체) 페이지에는 성공적으로 수집된 모든 관찰 가능 개체가 표시됩니다(관찰 가능 개체 요약 정보, 1944 페이지 참조).

시작하기 전에

- 소스로 사용할 TAXII 피드 가져오기, 1917 페이지, URL에서 소스 가져오기, 1918 페이지, 또는 소스로 사용할 로컬 파일 업로드, 1920 페이지에 설명된 대로 하나 이상의 소스를 구성합니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **2** 관찰 가능 개체를 클릭 합니다.

단계 **3** 현재 관찰 가능 개체 보기:

- 페이지에 표시된 관찰 가능 개체를 필터링하려면 필터( )을 클릭합니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 1945 페이지를 참고하십시오.

- **Value(값)** 열의 정보가 잘린 경우, 값 위에 커서를 올려놓습니다.
- 관찰 가능 개체를 포함하는 지표를 보려면 **Indicators(지표)** 열에서 숫자를 클릭합니다. 관찰 가능 개체 값을 필터로 하여 Incident(인시던트) 페이지가 열립니다. 자세한 내용은 지표 보기 및 관리, 1940 페이지를 참고하십시오.

단계 **4** 현재 관찰 가능 개체 관리:

- **Action(작업)**을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참조하십시오.
- 관찰 가능 개체의 **Publish(게시)** 설정을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참조하십시오.
- 관찰 가능 개체의 만료 날짜를 변경하려면 상위 소스의 **TTL**을 수정합니다. 자세한 내용은 소스 보기 및 관리, 1937 페이지를 참고하십시오.
- **Whitelist(화이트리스트)** 버튼을 클릭하여 차단 금지 목록에 관찰 가능 개체를 추가합니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 1951 페이지를 참고하십시오.

관찰 가능 개체 요약 정보

관찰 가능 개체 페이지에는 모든 수집 된 관찰 가능 개체에 대 한 요약 정보가 표시 됩니다.

표 ***130:*** 관찰 가능 개체 요약 정보

필드	설명
유형	관찰 가능 개체 데이터 유형: `SHA-256`, 도메인, `URL`, `IPv4`또는 `IPv6`.
값	관찰 가능 개체를 구성하는 데이터입니다.
지표	관찰 가능 개체를 포함하는 상위 지표의 수입니다.
조치	관찰 가능 개체에 대해 구성된 작업입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지를 참고하십시오. 지표는 상위 소스로부터 **Action(작업)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Action(작업)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 1945 페이지를 참고하십시오.
게시	관찰 가능 개체의 게시 설정입니다(소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지 참조). 지표는 상위 소스로부터 **Publish(게시)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(게시)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 1945 페이지를 참고하십시오.

필드	설명
업데이트 위치:	TID가 관찰 가능 개체를 마지막으로 업데이트한 날짜와 시간입니다.
만료	관찰 가능 개체가 상위 지표의 **TTL**에 따라 TID에서 자동으로 제거될 날짜입니다.
화이트리스트 버튼	이 버튼을 클릭하면 차단 안 함 목록에 관찰 가능 항목이 추가됩니다. 차단 금지 목록에 TID 관찰 가능 항목 추가 , 1951 페이지의 내용을 참조하십시오.

테이블 보기에서 TID 데이터 필터링

프로시저

단계 **1** 다음 TID 테이블 보기 중 하나를 선택합니다.

- **Intelligence(**인텔리전스**)** > **Incidents(**인시던트**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Indicators(**지표**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Observables(**관찰 가능 개체**)**

단계 **2** 필터( )을 클릭하고 필터 속성을 선택합니다.

단계 **3** 해당 필터 속성의 값을 선택하거나 입력합니다.

필터는 대/소문자를 구분합니다.

단계 **4** (선택 사항) 여러 속성을 필터링하려면 필터( )을 클릭하고 2단계와 3단계를 반복합니다.

단계 **5** 필터를 마지막으로 적용한 이후의 변경 사항을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

단계 **6** 필터를 적용하여 테이블을 새로 고치려면 **Apply(**적용**)**를 클릭합니다.

단계 **7** 필터 속성을 개별적으로 제거하려면 필터 속성 옆에 있는 제거( )을 클릭하고 **Apply(**적용**)**를 클릭하여 테이블을 새로 고칩니다.

TID 구성의 상속

TID는 소스로부터 인텔리전스 데이터를 수집할 때 해당 소스의 하위 개체로 지표와 관찰 가능 개체를 생성합니다. 이러한 하위 개체는 생성될 때 상위 구성에서 **Action(**작업**)** 및 **Publish(**게시**)** 설정을 상속합니다

지표는 상위 소스에서 이러한 설정을 상속합니다. 지표는 하나의 상위 소스만 가질 수 있습니다.

관찰 가능 개체는 상위 지표에서 이러한 설정을 상속합니다. 관찰 가능 개체는 여러 상위 지표를 가질 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- 여러 상위에서 TID 설정 상속, 1946 페이지
- 상속된 TID 설정 재정의 정보, 1946 페이지

여러 상위에서 TID 설정 상속

관찰 가능 개체에 여러 상위 지표가 있는 경우, 시스템은 모든 상위 항목에서 상속한 설정을 비교하여 가장 안전한 옵션을 관찰 가능 개체에 할당합니다. 그 결과는 다음과 같습니다.

- **Action(작업)**: `Block(차단)`이 `Monitor(모니터링)`보다 안전합니다
- **Publish(게시)**: `On`가 `Off`보다 안전합니다

예를 들어 SourceA는 IndicatorA 및 관련 ObservableA에 기여할 수 있습니다.

설정	SourceA	IndicatorA	ObservableA
조치	차단	차단	차단
게시	`Off`	`Off`	`Off`

SourceB가 ObservableA도 포함하는 IndicatorB에 나중에 기여하는 경우, 시스템은 ObservableA를 다음과 같이 수정합니다.

설정	SourceB	IndicatorB	ObservableA
조치	모니터링	모니터링	`Block(차단)` (IndicatorA에서 상속)
게시	켜기	켜기	`On` (IndicatorB에서 상속)

이 예에서 ObservableA에는 두 가지 상위 항목이 있습니다. **Action(작업)** 설정의 상위 항목 하나와 **Publish(게시)** 설정의 상위 항목 하나입니다. 관찰 가능 개체의 설정을 수동으로 편집한 다음 설정을 되돌리면 시스템은 **Action(작업)** 설정을 IndicatorA 값으로, **Publish(게시)** 설정을 IndicatorB 값으로 설정합니다.

상속된 TID 설정 재정의 정보

상속된 설정을 재정의하려면 하위 수준에서 설정을 변경합니다(소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 1947 페이지 및 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지 참조). 상속된 설정을 재정의하면 하위 개체는 상위 개체의 변경에도 불구하고 해당 설정을 유지합니다.

예를 들어 재정의 없이 다음과 같은 원래 설정으로 시작할 수 있습니다.

설정	SourceA	IndicatorA	ObservableA1	ObservableA2
게시	끄기	끄기	끄기	끄기

IndicatorA에 대한 설정을 재정의하는 경우, 설정은 다음과 같습니다.

설정	SourceA	IndicatorA	ObservableA1	ObservableA2
게시	끄기	켜기	켜기	켜기

이 경우, SourceA의 **Publish(**게시**)** 설정 변경은 더 이상 자동으로 IndicatorA로 캐스케이딩되지 않습니다. 하지만 IndicatorA에서 ObservableA1 및 ObservableA2로의 상속은 계속되는데, 현재 관찰 가능 개체 설정이 값을 재정의하도록 설정되어 있지 않기 때문입니다.

나중에 ObservableA1에 대한 설정을 재정의하는 경우:

설정	SourceA	IndicatorA	ObservableA1	ObservableA2
게시	끄기	켜기	끄기	켜기

IndicatorA의 **Publish(**게시**)** 설정 변경은 더 이상 자동으로 ObservableA1으로 캐스케이딩되지 않습니다. 하지만 이러한 변경 사항은 계속해서 ObservableA2로 캐스케이딩됩니다. 값을 재정의하도록 설정되어 있지 않기 때문입니다.

관찰 가능 개체 수준에서는 재정의 설정에서 상속된 설정으로 되돌릴 수 있으며, 시스템은 설정 변경을 상위 지표에서 해당 관찰 가능 개체로 자동으로 캐스케이딩하는 작업을 재개합니다.

소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정

참고:

- 상위 항목의 작업을 수정하면 모든 하위 항목의 작업이 설정됩니다. 소스 수준에서 작업을 수정하면 소스의 모든 지표의 작업이 설정됩니다. 지표 수준에서 작업을 수정하면 지표의 모든 관찰 가능 개체의 작업이 설정됩니다.
- 하위 항목의 작업을 수정하면 상속이 중단됩니다. 지표 수준에서 작업을 수정하고 이후에 소스 수준에서 수정하면 개별 지표의 작업을 수정할 때까지 지표의 작업은 보존됩니다. 관찰 가능 개체 수준에서 작업을 수정하고 이후에 지표 수준에서 수정하면 개별 관찰 가능 개체의 작업을 수정할 때까지 관찰 가능 개체의 작업은 보존됩니다. 관찰 가능 개체 수준에서는 상위 지표의 작업으로 자동으로 되돌릴 수 있습니다. 상속에 대한 자세한 내용은 TID 구성의 상속, 1945 페이지를 참조하십시오.

다른 수행하는 작업에 영향을 미치는 요소, 1932 페이지도 검토하는 것이 좋습니다.

프로시저

단계 **1** 다음 중 하나를 선택합니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)**

참고 TID 소스 수준에서 TAXII 소스 차단을 지원하지 않습니다. TAXII 소스에 간단한 지표가 포함된 경우, 지표 또는 관찰 가능 개체 수준에서 차단할 수 있습니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Indicators(**지표**)**

  참고 TID 복잡한 지표의 차단를 지원하지 않습니다. 대신 복잡한 지표 내의 개별적 관찰 가능 개체를 차단합니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Observables(**관찰 가능 개체**)**

단계 **2** **Action(**작업**)** 드롭다운을 사용하여 `Monitor(모니터링)`(모니터( ))) 또는 `Block(차단)`(차단( ))을 선택합니다.

단계 **3** (관찰 가능 개체만 해당) 상위 지표로부터의 작업 설정 상속을 재개하려면 관찰 가능 개체의 **Action(**작업**)** 설정 옆에 있는 되돌리기를 클릭합니다.

게시 일시 중지 정보

- 기능 수준에서 게시를 일시 중지하면 시스템은 요소에 저장된 모든 TID 관찰 가능 개체를 제거합니다. 즉, TID는 위협을 탐지하거나 모니터링하거나 차단할 수 없습니다. 시스템의 다른 보안 기능은 영향을 받지 않습니다.
- 소스, 지표 또는 관찰 가능 개체 수준에서 게시를 일시 중지하는 경우, 시스템은 일시 중지된 TID 관찰 가능 개체를 요소에서 제거하므로 트래픽과의 매칭이 방지됩니다.
- 상위 항목의 게시를 일시 중지하면 모든 하위 항목이 일시 중지됩니다. 소스 수준에서 게시를 일시 중지하면 모든 해당 지표의 게시가 일시 중지됩니다. 지표 수준에서 게시를 일시 중지하면 모든 해당 관찰 가능 개체의 게시가 일시 중지됩니다.
- 하위 항목의 게시를 일시 중지하면 상속이 중단됩니다. 지표 수준에서 게시를 일시 중지하고 이후에 소스 수준에서 게시하면 지표의 개별 설정을 변경할 때까지 지표의 게시가 계속 일시 중지됩니다. 관찰 가능 개체 수준에서 게시를 일시 중지하고 이후에 지표 수준에서 게시하면 관찰 가능 개체의 개별 설정을 변경할 때까지 관찰 가능 개체의 게시가 계속 일시 중지됩니다. 관찰 가능 개체 수준에서는 상위 지표의 게시 상태로 자동으로 되돌릴 수 있습니다. 상속에 대한 자세한 내용은 TID 구성의 상속, 1945 페이지를 참조하십시오.
- 업로드된 소스의 게시는 지표 수준에서만 일시 중지할 수 있습니다.
- 관찰 가능 대상에 대한 게시 일시 중지와 관찰 가능 항목을 차단 안 함 목록에 추가하는 것에 대한 비교는 차단 금지 목록에 TID 관찰 가능 항목 추가 , 1951 페이지의 내용을 참조하십시오.
- 개별 관찰 가능 개체 또는 지표의 게시/일시 중지 설정을 지정했다면 소스 업데이트에 동일한 관찰 가능 개체 또는 지표가 포함된 경우, 소스 업데이트는 해당 설정을 변경하지 않습니다.
- 게시는 개체 관리 페이지에서 비활성화할 수 있습니다. 관찰 가능 개체 게시 빈도 수정, 1950 페이지의 내용을 참조하십시오.

- Source(소프) 페이지의 업데이트 일시 중지 옵션은 데이터를 요소에 게시하는 것과 관련이 없고, 피드의 Firepower Management Center에서의 소스 업데이트에 적용됩니다.

TID 일시 중지 및 요소에서 TID 데이터 제거

주의 이 설정은 모든 요소에 대한 게시를 일시 중지하고, 요소에 저장된 모든 TID 관찰 가능 개체를 제거하며, TID 기능을 사용하여 트래픽 검사를 중지합니다.

더 세부적인 수준에서 관찰 가능 개체를 비활성화하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지를 참조하십시오.

관리 센터의 데이터(기존 인시던트 및 구성된 소스, 지표, 관찰 가능 개체 및 소스 수집)는 이 설정의 영향을 받지 않습니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Settings(**설정**)**를 선택합니다.

단계 **2** **Pause(**일시 중지**)**를 클릭합니다.

다음에 수행할 작업

요소에서의 TID 데이터 동기화와 관찰 생성을 재개할 준비가 되면 이 페이지에서 수동으로 게시를 재개합니다. 관리 센터의 기존 관찰 가능 개체가 모든 요소에 게시됩니다.

소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시

소스 수준에서 게시가 활성화되면 시스템은 초기 소스 데이터 및 다음을 포함한 모든 후속 변경 사항을 자동으로 게시합니다.

- 주기적 소스 새로 고침에 따른 변경 사항
- 시스템 작업(예를 들어 **TTL** 만료)에서 발생하는 변경 사항
- 사용자가 시작한 변경(예: 지표 또는 관찰 가능 개체의 **Action(**작업**)** 설정 변경)

참고 디바이스(요소)에서 한 번에 모든 TID 관찰 가능 개체를 제거하려면 TID 일시 중지 및 요소에서 TID 데이터 제거, 1949 페이지를 참조하십시오.

시작하기 전에

게시를 일시 중지하기 전에 게시 일시 중지 정보, 1948 페이지에 설명된 영향을 이해하십시오.

프로시저

단계 **1** 다음 중 하나를 선택합니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Indicators(**지표**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Observables(**관찰 가능 개체**)**

단계 **2** **Publish(**게시**)** 슬라이더( )를 찾고 이를 사용해서 게시를 요소로 전환합니다.

단계 **3** (관찰 가능 개체만 해당) 상위 지표로부터의 게시 설정 상속을 재개하려면 관찰 가능 개체의 **Publish(**게시**)** 설정 옆에 있는 **Revert(**되돌리기**)**를 클릭합니다.

다음에 수행할 작업

- 요소가 변경 사항을 수신하도록 10분 이상 기다립니다. 큰 소스와 관련된 변경 사항은 이보다 시간이 더 걸립니다.
- (선택 사항) 관찰 가능 개체 수준에서 TID 데이터의 게시 빈도를 변경합니다(관찰 가능 개체 게시 빈도 수정, 1950 페이지 참조).

관찰 가능 개체 게시 빈도 수정

기본적으로 시스템은 5분마다 관찰 가능 개체를 TID 요소에 게시합니다. 이 절차를 사용하여 이 간격을 다른 값으로 설정하십시오.

시작하기 전에

- 관찰 가능 개체 수준에서 TID 데이터 게시를 활성화합니다(소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 1949 페이지 참조).

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **Security Intelligence(**보안 인텔리전스**)** > **Network Feeds and Lists(**네트워크 목록 및 피드**)**를 선택합니다.

단계 **3** **Cisco-TID-Feed**옆에 있는 수정 아이콘을 클릭합니다.

단계 **4** **Update Frequency(**업데이트 빈도**)** 드롭다운 목록에서 값을 선택합니다.

- 요소에 대한 관찰 가능 개체 데이터 게시를 중지하려면 **Disable(**비활성화**)**을 선택합니다.
- 관찰 가능 개체 게시 간격을 설정하려면 다른 값을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

차단 금지 목록에 TID 관찰 가능 항목 추가

간단한 지표의 관찰 가능 개체를 지정된 **Action(**작업**)**에서 제외하려면(모니터링 또는 차단 없이 트래픽이 통과하도록 하려면) 해당 관찰 가능 개체를 차단 금지 목록에 추가할 수 있습니다.

복잡한 지표에서 TID는 트래픽을 평가할 때 차단 금지 목록에 추가된 관찰 가능 개체를 무시하지만 해당 지표의 다른 관찰 가능 개체는 여전히 평가됩니다. 예를 들어 지표에 AND 연산자로 연결된 Observable 1과 Observable 2가 포함되어 있고 Observable 1을 차단 금지 목록에 추가하려는 경우, TID는 Observable 2가 보일 때 완전히 실현된 인시던트를 생성합니다.

이에 비해 동일한 복잡한 지표에서 Observable 1을 차단 금지 목록에 추가하는 대신 Observable 1의 게시를 비활성화하면 TID는 Observable 2가 보일 때 부분적으로 실현된 인시던트를 생성합니다.

화이트리스트 버튼(☑)은 지표 세부 사항 페이지 및 관찰 가능 개체 페이지에 표시됩니다. 차단 금지 목록에 관찰 가능 항목을 추가하려면 해당 아이콘을 클릭합니다.

참고 관찰 가능 개체를 차단 금지 목록에 추가하는 경우, 관찰 가능 개체의 **Action(**작업**)** 설정이 상속된 값이건 재정의 값이건 상관없이 차단 금지 목록이 해당 설정에 우선합니다.

소스 업데이트에 동일한 관찰 가능 개체가 포함된 경우 해당 업데이트는 개별 관찰 가능 개체의 차단 금지 목록 설정에 영향을 주지 않습니다.

차단 금지 목록에 TID 관찰 가능 항목 추가

차단 안 함 목록 사용에 대한 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 1951 페이지의 내용을 참조하십시오.

팁 "차단 안 함 목록에 추가" 버튼(☑)은 웹 인터페이스 여러 위치에 표시될 수 있습니다. 이러한 위치 어디서나 이 버튼을 클릭하여 관찰 가능 개체를 차단 안 함 목록에 추가할 수 있습니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**) > Sources(**소스**) > Observables(**관찰 가능 개체**)**를 클릭합니다.

단계 **2** 허용하려는 관찰 가능 개체로 이동합니다.

단계 **3** 해당 관찰 가능 개체에 대해 (**Whitelist(**화이트리스트**)**)를 클릭합니다.

다음에 수행할 작업

(선택 사항) 차단 안 함 목록에서 관찰 가능 개체를 제거해야 하는 경우, 버튼을 다시 클릭합니다.

STIX 소스 파일 보기

프로시저

단계 **1** **Intelligence(**인텔리전스**) > Sources(**소스**) > Indicators(**지표**)**를 선택합니다.
단계 **2** 지표 이름을 클릭합니다.
단계 **3** **Download STIX(STIX** 다운로드**)**를 클릭합니다.
단계 **4** 텍스트 편집기에서 파일을 엽니다.

문제 해결 Cisco Threat Intelligence Director(TID)

다음 섹션에서는 일반적인 TID 문제의 가능한 해결책과 완화 방법을 설명합니다.

플랫 파일 소스 가져오기 또는 업로드에서 오류 발생

시스템이 플랫 파일 소스를 가져오지 못하거나 업로드하지 못하는 경우, 플랫 파일의 데이터가 **Intelligence(**인텔리전스**) > Sources(**소스**)** 페이지의 **Type(**유형**)** 열과 일치하는지 확인합니다.

TAXII 또는 **URL** 소스 업데이트에서 오류 발생

TAXII 또는 URL 소스 업데이트에서 소스 상태 오류가 발생하는 경우, 서버 인증서가 만료되지 않았는지 확인합니다. 인증서가 만료된 경우, TID가 새 인증서를 검색할 수 있도록 새 서버 인증서를 입력하거나 기존 서버 인증서를 삭제합니다. 자세한 내용은 TID 소스의 TLS/SSL 설정 구성, 1921 페이지를 참고하십시오.

지표 또는 소스에 **"**차단**"** 작업을 사용할 수 없고 **"**모니터링**"**만 사용 가능

지표 또는 소스에서 개별 관찰 가능 개체의 작업을 변경할 수 있습니다.

TID 테이블 보기가 **"**결과 없음**"**을 반환

테이블 보기에는 **Sources(**소스**)**, **Indicators(**지표**)**, **Observables(**관찰 가능 개체**)**, **Incidents(**인시던트**)** 페이지가 포함됩니다.

TID 테이블 보기 중 하나에서 데이터가 보이지 않는 경우:

- 테이블 필터를 확인하고 **Last Updated(**마지막 업데이트**)** 필터 속성의 기간을 확장하는 것이 좋습니다(테이블 보기에서 TID 데이터 필터링, 1945 페이지 참조).
- 소스를 올바르게 구성했는지 확인합니다(데이터 소스 수집 옵션, 1916 페이지 참조).
- 액세스 제어 정책 및 관련 정책이 TID를 지원하도록 구성되었는지 확인합니다(지원할 정책 구성 TID, 1915 페이지 참조). 예를 들어 SHA-256 관찰 가능 개체가 관찰을 생성하지 않는 경우, 구축된 액세스 제어 정책에 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 정책을 호출하는 하나 이상의 액세스 제어 규칙이 포함되어 있는지 확인합니다.
- TID 지원 액세스 제어 정책과 관련 정책을 요소에 구축했는지 확인합니다(컨피그레이션 변경 사항 구축, 498 페이지 참조).
- 기능 수준에서 TID 데이터 게시를 일시 중지하지 않았는지 확인합니다(TID 일시 중지 및 요소에서 TID 데이터 제거, 1949 페이지 참조).

시스템이 느려지거나 성능 저하

성능에 미치는 영향에 대한 자세한 내용은 Threat Intelligence Director의 성능 영향, 1911 페이지를 참조하십시오.

Firepower Management Center 테이블 보기에 **TID** 데이터가 표시되지 않음

관찰 가능 개체를 요소에 게시하지만 연결, 보안 인텔리전스, 파일 또는 악성코드 이벤트 테이블에 TID 데이터가 표시되지 않는 경우, 요소에 구축된 액세스 제어 및 파일 정책을 확인합니다. 자세한 내용은 지원할 정책 구성 TID, 1915 페이지를 참고하십시오.

하나 이상의 요소가 **TID** 데이터에 압도됨

TID 데이터가 하나 이상의 디바이스를 압도하는 경우, TID 게시를 일시 중지하고 요소에 저장된 데이터를 제거하는 것이 좋습니다. 자세한 내용은 TID 일시 중지 및 요소에서 TID 데이터 제거, 1949 페이지를 참고하십시오.

시스템은 **TID** 차단 대신 악성코드 클라우드 조회를 수행

이것은 의도적인 것입니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 1933 페이지를 참고하십시오.

시스템은 **TID** 작업 대신 보안 인텔리전스 또는 **DNS** 정책 작업을 수행

이것은 의도적인 것입니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 1933 페이지를 참고하십시오.

TID가 비활성화됨

- 어플라이언스에 메모리를 추가합니다. Threat Intelligence Director는 메모리가 15GB 이상인 어플라이언스에서만 사용할 수 있습니다.

- Firepower Management Center에 대한 REST API 액세스를 활성화합니다. 자세한 내용은 REST API 액세스 활성화를 참고하십시오.

시스템이 예상대로 **TID** 인시던트를 생성하지 않거나 **TID** 작업을 수행하지 않음

- 모든 매니지드 디바이스가 TID에 대해 적절히 활성화 및 구성되었는지 확인합니다. 요소(매니지드 디바이스)의 TID 상태 보기, 1937 페이지 및 지원할 정책 구성 TID, 1915 페이지를 참조하십시오.
- 변경 사항이 요소에 게시되려면 적어도 5~10분이 걸리며, 많은 데이터 피드를 게시하는 경우에는 더 오래 걸릴 수 있습니다.
- 관찰 가능 개체에 대한 작업 설정을 확인합니다. 관찰 가능 개체 보기 및 관리, 1943 페이지의 내용을 참조하십시오.
- 시스템이 수행하는 TID 작업에 영향을 미치는 다른 요인의 목록은 수행하는 작업에 영향을 미치는 요소, 1932 페이지를 참조하십시오.
- 요소(매니지드 디바이스)에 있어야 할 위협 데이터가 없을 수 있습니다. 게시 일시 중지 정보, 1948 페이지의 내용을 참조하십시오.

특정 위협 **1**회 발생에서 여러 인시던트가 생성

이것은 하나의 지표가 여러 소스에 포함된 경우에 발생할 수 있습니다.

자세한 내용은 중복 표시기 처리, 1921 페이지를 참조하십시오.

기록Cisco Threat Intelligence Director(TID)

기능	버전	세부 사항
작업 우선순위 변경	6.5	

기능	버전	세부 사항

		이 변경 사항은 둘 이상의 Firepower 기능이 특정 관찰 가능 개체에 적용할 수 있을 때 적용됩니다.
		
		TID 차단/모니터링 관찰 가능 작업이 보안 인텔리전스로 인한 차단/모니터링에 우선하도록 변경되었습니다.
		
		중요 시스템은 예전과 같은 방식으로 트래픽을 효율적으로 처리합니다. 이전에 차단된 트래픽은 계속 차단되고, 모니터링되는 트래픽은 계속 모니터링됩니다. 이렇게 하면 이벤트에 보고된 구성 요소가 작업을 담당하는 것으로 변경됩니다. 더 많은 TID 인시던트가 생성될 수도 있습니다.
		
		• 트래픽이 보안 인텔리전스 차단 작업과 일치하더라도 TID 관찰 가능 개체 차단 작업을 설정하는 경우:
		  • 연결 이벤트의 보안 인텔리전스 범주는 TID 블록의 변형입니다.
		  • 시스템은 차단된 작업으로 TID 인시던트를 생성합니다.
		
		• 트래픽이 보안 인텔리전스 모니터 규칙과도 일치하더라도 TID 관찰 가능 개체 모니터 작업을 설정하는 경우:
		  • 연결 이벤트의 보안 인텔리전스 범주는 TID 모니터링의 변형입니다.
		  • 시스템은 모니터링된 작업으로 TID 인시던트를 생성합니다.
		
		이전에는 이러한 경우 시스템에서 분석별로 범주를 보고하지만, TID 인시던트를 생성하지는 않았습니다.

기능	버전	세부 사항
Cisco Threat Intelligence Director(TID)	6.2.2	도입된 기능: 외부 소스의 위협 인텔리전스를 사용하여 위협을 식별하고 처리할 수 있습니다. 새로운 화면: 여러 탭이 포함된 새로운 최상위 **Intelligence(**인텔리전스**)** 메뉴. 지원되는 플랫폼: Firepower Management Center

XVIII 부

침입 탐지 및 방지

- 침입 탐지 및 방지 개요, 1961 페이지
- 침입 및 네트워크 분석 정책의 레이어, 1979 페이지
- 침입 정책 시작하기, 1995 페이지
- 규칙을 사용하여 침입 정책 조정, 2007 페이지
- 네트워크 자산에 대한 침입 방지 맞춤화, 2037 페이지
- 민감한 데이터 탐지, 2043 페이지
- 침입 이벤트 로깅 글로벌 제한, 2057 페이지
- 침입 규칙 편집기, 2063 페이지
- 침입 방지 성능 조정, 2185 페이지

78 장

침입 탐지 및 방지 개요

다음 주제에서는 네트워크 분석 및 침입 정책의 개요를 제공합니다.

- 네트워크 분석 및 침입 정책 기본 사항, 1961 페이지
- 정책이 트래픽에서 침입을 검토하는 방법, 1962 페이지
- 시스템 제공 및 맞춤형 네트워크 분석 및 침입 정책, 1967 페이지
- 네트워크 분석 및 침입 정책에 대한 라이선스 요건, 1974 페이지
- 네트워크 분석 및 침입 정책 요구 사항 및 사전 요건, 1974 페이지
- 탐색 패널: 네트워크 분석 및 침입 정책, 1974 페이지
- 충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

네트워크 분석 및 침입 정책 기본 사항

네트워크 분석 및 침입 정책은 Firepower System의 침입 탐지 및 방지 기능의 일환으로 함께 작동합니다.

- 침입 탐지란 용어는 일반적으로 네트워크 트래픽에서 잠재적인 침입을 수동적으로 모니터링 및 분석하고 보안 분석을 위한 공격 데이터를 저장하는 프로세스를 말합니다. 'IDS'라고 하기도 합니다.
- 침입 방지란 용어에는 침입 탐지의 개념이 포함되지만, 악성 트래픽이 네트워크를 통과할 때 이를 차단 또는 변경하는 기능이 추가됩니다. 'IPS'라고 하기도 합니다.

침입 방지 구축에서 시스템이 패킷을 검토할 때:

- 네트워크 분석 정책은 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽을 향후에 평가할 수 있도록 트래픽을 해독하고 전처리하는 방법을 제어합니다.
- 침입 정책은 침입 및 전처리 규칙(집합적으로 침입 규칙이라고도 함)을 사용하여 패턴 기반의 공격에 대한 디코딩된 패킷을 검사합니다. 침입 정책은 변수 집합과 페어링되는데, 이를 통해 네트워크 환경을 올바르게 반영하는 지정된 값을 사용할 수 있습니다.

네트워크 분석과 침입 정책 모두 상위 액세스 제어 정책에 의해 호출되지만 그 시점은 다릅니다. 시스템이 트래픽을 분석하기 때문에, 네트워크 분석(디코딩 및 전처리) 단계는 침입 방지(추가 전처리 및 침입 규칙) 단계보다 이전에 또는 별도로 발생합니다. 네트워크 분석 및 침입 정책은 폭넓고 심층

적인 패킷 검사를 제공합니다. 이 둘을 함께 사용하면 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성을 위협할 수 있는 네트워크 트래픽을 탐지하고 알리고 방지할 수 있습니다.

Firepower System에서는 상호 보완하고 함께 작동하는 비슷한 이름의 여러 네트워크 분석 및 침입 정책(예: Balanced Security and Connectivity)을 제공합니다. 시스템이 제공하는 정책을 사용하면 Cisco Talos Intelligence Group(Talos)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 전처리기 규칙 상태를 설정할 뿐만 아니라 전처리기 및 다른 고급 설정에 대한 초기 구성을 제공합니다.

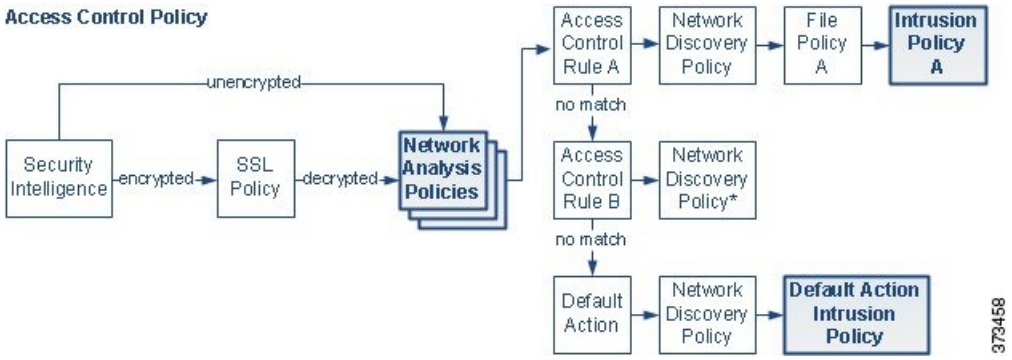
또한 사용자 지정 네트워크 분석 및 침입 정책을 만들 수 있습니다. 사용자 지정 정책의 설정을 조정하여 가장 중요하다고 생각되는 방식으로 트래픽을 검사할 수 있으며, 따라서 매니지드 디바이스의 성능과 디바이스가 생성하는 이벤트에 효과적으로 대응하는 능력 모두를 향상시킬 수 있습니다.

웹 인터페이스에서 유사한 정책 편집기를 사용하여 네트워크 분석 및 침입 정책을 생성, 수정, 저장 및 관리합니다. 정책 유형 중 하나를 수정할 때 탐색 패널이 웹 인터페이스의 왼쪽에 표시되며, 오른쪽에는 다양한 구성 페이지가 표시됩니다.

정책이 트래픽에서 침입을 검토하는 방법

시스템이 액세스 제어 배포의 일부로 트래픽을 분석할 때, 네트워크 분석(디코딩 및 전처리) 단계는 침입 방지(침입 규칙 및 고급 설정) 단계보다 이전에 또는 별도로 발생합니다.

다음 다이어그램은 인라인, 침입 방지 및 AMP for Networks 구축에서 트래픽 분석의 순서를 간소화된 형식으로 보여줍니다. 또한 액세스 제어 정책이 다른 정책을 호출하여 트래픽을 검토하는 방법 및 그러한 정책이 호출되는 순서를 보여줍니다. 네트워크 분석 및 침입 정책 선택 단계는 강조 표시됩니다.



인라인 구축(즉, 관련 설정을 라우팅, 스위칭 또는 투명한 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 디바이스에 구축하는 경우)의 경우, 시스템은 예시된 프로세스의 거의 모든 단계에서 추가 검사 없이 트래픽을 차단할 수 있습니다. 보안 인텔리전스, SSL 정책, 네트워크 분석 정책, 파일 정책 및 침입 정책은 모두 트래픽을 삭제 또는 수정할 수 있습니다. 수동으로 패킷을 검사하는 네트워크 검색 정책만으로는 트래픽의 흐름에 영향을 줄 수 없습니다.

마찬가지로 프로세스의 각 단계에서 패킷은 시스템이 이벤트를 생성하도록 할 수 있습니다. 침입 및 프리프로세서 이벤트(침입 이벤트로 총칭)는 패킷 또는 패킷의 내용에 보안 위험 있음을 나타내는 것입니다.

팁 다이어그램에는 SSL 검사 설정에서 암호화 트래픽의 통과를 허용하는 경우 또는 SSL 검사를 설정하지 않은 경우, 액세스 제어 규칙이 암호화 트래픽을 처리한다는 점이 반영되어 있지 않습니다. 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

단일 연결의 경우, 다이어그램에 나타난 것처럼 시스템은 액세스 제어 규칙에 앞서 네트워크 분석 정책을 선택하지만, 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후에 발생한다는 점에 유의하십시오. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방식에 영향을 주지 않습니다.

복호화, 정규화 및 전처리: 네트워크 분석 정책

프로토콜 차이가 패턴 일치를 불가능하게 할 수 있으므로 디코딩과 전처리가 없으면 시스템은 침입 탐지를 위해 트래픽을 제대로 평가할 수 없습니다. 네트워크 분석 정책은 이러한 트래픽 처리 작업을 제어합니다.

- 보안 인텔리전스에 의해 트래픽이 필터링된 후
- 암호화된 트래픽이 선택적인 SSL 정책에 의해 해독된 후
- 트래픽을 파일 또는 침입 정책으로 검사할 수 있기 전

네트워크 분석 정책은 처리 단계에서 패킷을 제어합니다. 먼저 시스템이 첫 세 개 TCP/IP 레이어를 통해 패킷을 디코딩한 다음, 프로토콜 이상 징후를 표준화하고, 전처리하며, 계속해서 탐지합니다.

- 패킷 디코더는 패킷 헤더 및 페이로드를 전처리기에서 쉽게 사용할 수 있는 형식으로, 그리고 추후 침입 규칙에서 쉽게 사용할 수 있는 형식으로 변환합니다. TCP/IP 스택의 각 레이어는 데이터링크 레이어로 시작하여 계속해서 네트워크 및 전송 레이어를 통해 차례로 디코딩됩니다. 패킷 디코더는 또한 패킷 헤더의 다양하고 변칙적인 작업을 탐지합니다.
- 인라인 배포에서, 인라인 표준화 전처리기는 공격자가 탐지를 우회하는 가능성을 최소화하기 위해 트래픽을 새로 포맷합니다(표준화합니다). 이는 다른 전처리기 및 침입 규칙에 따라 패킷이 검사될 수 있도록 준비하고, 시스템이 처리하는 패킷이 사용자 네트워크 호스트에서 수신된 패킷과 동일한지 확인할 수 있도록 지원합니다.

  참고 패시브 구축의 경우, Cisco는 네트워크 분석 수준에서 인라인 표준화를 구성하는 대신 액세스 제어 정책 수준에서 적응형 프로파일을 구성하고 할 것을 권장합니다.

- 다양한 네트워크 및 전송 레이어 전처리기는 IP 조각을 이용한 익스플로잇을 탐지하고 체크섬 유효성 검증을 수행하며, TCP와 UDP 세션 전처리를 수행합니다.

일부 고급 전송 및 네트워크 전처리기 설정은 액세스 제어 정책의 대상 디바이스에서 처리된 모든 트래픽에 전역으로 적용된다는 점에 유의하십시오. 이러한 설정은 네트워크 분석 정책보다는 액세스 제어 정책에서 구성합니다.

- 다양한 애플리케이션 레이어 프로토콜 디코더는 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화합니다. 애플리케이션 레이어 프로토콜 인코딩을 정규화함으로써 시스템에서는 데이터가 다르게 표현된 패킷에 동일한 콘텐츠 관련 침입 규칙을 효과적으로 적용하고 의미 있는 결과를 얻을 수 있습니다.
- Modbus, DNP3, CIP 및 s7commplus SCADA 전처리기는 트래픽의 비정상적인 상태를 탐지하고 침입 규칙에 데이터를 제공합니다. Supervisory Control(감시 제어) 및 Data Acquisition(데이터 획득. SCADA) 프로토콜은 제조, 생산, 정수 처리, 배전, 공항 및 배송 시스템 등과 같은 산업, 인프라 및 설비의 데이터를 모니터링하고, 제어하며, 획득합니다.
- 여러 전처리기는 사용자가 Back Orifice, portscans, SYN floods 및 기타 속도 기반 공격과 같은 특정 위협을 탐지하도록 합니다.

  침입 정책에서 ASCII 텍스트의 신용카드 번호 및 주민등록번호/사회보장번호 같은 민감한 데이터를 탐지하는 민감한 데이터 프리프로세서를 구성할 수 있습니다.

새로 만든 액세스 제어 정책에서 하나의 기본 네트워크 분석 정책은 동일한 상위 액세스 제어 정책에 의해 호출된 모든 침입 정책에 대한 모든 트래픽에 대해 전처리를 제어합니다. 먼저, 시스템은 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책을 기본값으로 사용하지만, 기타 시스템이 제공하는 네트워크 분석 정책 또는 사용자 지정 네트워크 분석 정책으로 변경할 수 있습니다. 더 복잡한 구축에서 고급 사용자는 일치하는 트래픽을 전처리하는 다양한 맞춤형 네트워크 분석 정책을 할당하여 특정 보안 영역, 네트워크, VLAN에 트래픽 전처리 옵션을 맞출 수 있습니다.

액세스 제어 규칙: 침입 정책 선택

초기 전처리 후, (있는 경우) 액세스 제어 규칙이 트래픽을 평가합니다. 대부분의 경우 패킷과 일치하는 첫 번째 액세스 제어 규칙이 트래픽을 처리하는 규칙입니다. 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용할 수 있습니다.

액세스 제어 규칙을 통해 트래픽을 허용할 경우, 시스템은 트래픽에서 데이터 검색, 악성코드, 금지 파일 및 침입을 순서대로 검사할 수 있습니다. 액세스 제어 규칙과 일치하지 않는 트래픽은 검색 데이터와 침입을 검사할 수 있는 액세스 제어 정책의 기본 작업에 의해 처리됩니다.

참고 어느 네트워크 분석 정책이 패킷을 전처리하는지에 상관없이 모든 패킷은 구성된 액세스 제어 규칙에 일치되며 따라서 하향식 순서로 침입 정책에 의한 잠재적 검사의 대상이 됩니다.

정책이 트래픽에서 침입을 검토하는 방법, 1962 페이지의 다이어그램은 다음과 같이 인라인, 침입 방지 및 AMP for Networks 구축에서 디바이스를 통한 트래픽 흐름을 보여줍니다.

- Access Control Rule A는 일치하는 트래픽의 진행을 허용합니다. 그런 다음 트래픽은 네트워크 검색 정책에 의해 검색 데이터가, File Policy A에 의해 금지 파일 및 악성코드가 검사된 다음 Intrusion Policy A에 의해 침입이 검사됩니다.

- Access Control Rule B 역시 일치하는 트래픽을 허용합니다. 그러나 이 시나리오에서는 트래픽에서 침입(또는 파일이나 악성코드)이 검사되지 않으므로 규칙과 연결된 침입 또는 파일 정책이 없습니다. 기본적으로 진행을 허용하는 트래픽은 네트워크 검색 정책에 의해 검사되며 이것은 구성할 필요가 없습니다.
- 이 시나리오에서 액세스 제어 정책의 기본 작업은 일치하는 트래픽을 허용하는 것입니다. 다음으로 트래픽은 네트워크 검색 정책으로 그리고 침입 정책의 검사를 받습니다. 침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 때 다른 침입 정책을 사용할 수 있습니다(그러나 반드시 그렇게 해야 할 필요는 없음).

시스템은 차단된 트래픽 또는 신뢰할 수 있는 트래픽은 검사하지 않으므로 다이어그램의 예에는 차단 또는 신뢰 규칙이 포함되어 있지 않습니다.

침입 검사: 침입 정책, 규칙 및 변수 집합

침입 방지는 트래픽이 목적지로 들어가기 전 시스템의 최후의 방어선으로 사용할 수 있습니다. 침입 정책은 보안 위반 확인을 위해 시스템이 인라인 배포에서 트래픽을 검사하는 방식을 제어하며, 악성 트래픽을 차단하거나 변경할 수 있습니다. 침입 정책의 주요 기능은 어느 침입 및 전처리기 규칙이 활성화되는지와 이들이 구성되는 방식을 관리하는 것입니다.

침입 및 전처리기 규칙

침입 규칙은 네트워크의 취약성을 이용하려는 시도를 탐지하는 키워드 및 논쟁의 지정된 집합이며, 시스템은 침입 규칙을 사용하여 네트워크 트래픽을 분석하고, 규칙의 기준과 일치하는지를 확인합니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하며, 패킷 데이터가 규칙에 지정된 모든 조건에 일치하는 경우 규칙이 트리거됩니다.

시스템에는 Cisco Talos Intelligence Group(Talos)가 생성한 다음 유형의 규칙이 포함됩니다.

- 공유 개체 침입 규칙. 이는 컴파일된 것이며 수정할 수 없습니다(소스 및 대상 포트, IP 주소와 같은 규칙 헤더 정보 제외)
- 표준 텍스트 침입 규칙. 이는 규칙의 새 사용자 지정 인스턴스로 저장되며 수정할 수 있습니다.
- 전처리기 규칙. 이는 네트워크 분석 정책에서 전처리기 및 패킷 디코더 탐지 옵션과 관련된 규칙입니다. 전처리기 규칙을 복사하거나 수정할 수 없습니다. 대부분의 전처리기 규칙은 기본적으로 비활성화됩니다. 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.에 전처리기를 사용하려면 이들을 활성화해야 합니다.

시스템이 침입 정책에 따라 패킷을 처리할 때, 먼저 규칙 최적화기가 다음과 같은 기준에 근거하여 하위 집합 내 모든 활성화된 규칙을 분류합니다. 전송 레이어, 애플리케이션 프로토콜, 보호된 네트워크로 오가는 방향 등. 다음으로, 침입 규칙 엔진은 각 패킷에 적용하기 위해 적절한 규칙 하위 집합을 선택합니다. 마지막으로 다중 규칙 검색 엔진은 세 가지 검색 유형을 사용하여 트래픽이 규칙과 일치하는지 확인합니다.

- 프로토콜 필드 검색은 애플리케이션 프로토콜 내 특정 필드에서 일치 항목을 검색합니다.
- 일반적인 콘텐츠 검색은 패킷 페이로드의 ASCII 또는 이진 바이트 일치 항목을 검색합니다.

- 패킷 이상 징후 검색은 특정 내용을 포함하기보다는 잘 알려진 프로토콜을 위반하는 패킷 헤더 및 페이로드를 검색합니다.

사용자 지정 침입 정책에서 규칙을 활성화 및 비활성화하고 사용자 고유의 표준 텍스트 규칙을 작성 및 추가하여 탐지를 설정할 수 있습니다. Firepower 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결할 수도 있습니다.

변수 집합

시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 변수 집합을 사용합니다. 집합 내 대부분의 변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책 내 변수를 사용하여 규칙 삭제 및 동적 규칙 상태의 IP 주소를 나타낼 수 있습니다.

시스템은 단일 기본 변수 집합을 제공하는데, 이는 미리 정의된 기본 변수로 구성되어 있습니다. 대부분의 시스템이 제공하는 공유 개체 규칙과 표준 텍스트 규칙은 미리 정의된 이러한 기본 변수를 사용하여 네트워크와 포트 번호를 정의합니다. 예를 들어, 대부분의 규칙은 `$HOME_NET` 변수를 사용하여 보호된 네트워크를 지정하고 `$EXTERNAL_NET` 변수를 사용하여 보호되지 않은(또는 외부) 네트워크를 지정합니다. 또한, 전문 규칙은 종종 미리 정의된 다른 변수를 사용합니다. 예를 들어, 웹 서버에 대한 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

팁 시스템에서 제공한 침입 정책을 사용하는 경우에도 Cisco는 기본 변수 집합의 주요 기본 변수를 수정할 것을 강력하게 권장합니다. 올바르게 네트워크 환경을 반영하는 변수를 사용할 때, 처리는 최적화되고 시스템은 의심스러운 활동에 대해 관련 시스템을 모니터링할 수 있습니다. 고급 사용자는 하나 이상의 사용자 지정 침입 정책으로 페어링을 위한 사용자 지정 변수 집합을 만들고 사용할 수 있습니다.

관련 항목

사전 정의된 기본 변수, 582 페이지

침입 이벤트 생성

시스템은 가능한 침입을 식별하면 침입 또는 전처리기 이벤트(총칭하여 침입 이벤트라고도 함)를 생성합니다. 매니지드 디바이스는 Firepower Management Center에 자체 이벤트를 전송합니다. 여기서는 집계된 데이터를 보고 네트워크 자산에 대한 공격을 더 잘 이해할 수 있습니다. 인라인 구축에서 매니지드 디바이스는 유해한 것으로 알려진 패킷을 삭제 또는 교체할 수도 있습니다.

데이터베이스의 각 침입 이벤트는 이벤트 헤더를 포함하며, 이벤트 이름 및 분류에 관한 정보를 포함합니다. 여기에는 소스 및 대상 IP 주소, 포트, 이벤트를 생성한 프로세스, 이벤트의 날짜 및 시간, 그리고 공격의 출처 및 공격 대상에 대한 컨텍스트 관련 정보 등이 있습니다. 패킷 기반 이벤트의 경우, 시스템은 또한 해독된 패킷 헤더 및 패킷의 페이로드 또는 이벤트를 시작한 패킷의 복사본을 로깅합니다.

패킷 디코더, 전처리기 및 침입 규칙 엔진은 모두 시스템이 이벤트를 생성하도록 할 수 있습니다. 예를 들면 다음과 같습니다.

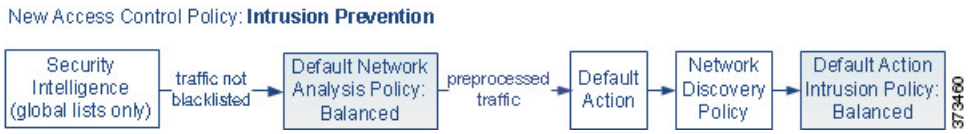
- (네트워크 분석 정책에서 구성된) 패킷 디코더가 어떤 옵션 또는 페이로드도 없는 IP 데이터그램의 크기인 20바이트보다 작은 IP 패킷을 수신한 경우, 디코더는 이를 이상 트래픽으로 해석합니다. 나중에, 패킷을 검토하는 침입 정책에서 관련 디코더 규칙이 활성화된 경우, 시스템은 전처리기 이벤트를 생성합니다.
- IP 조각 모음 전처리기에 중복되는 일련의 IP 조각이 발생할 경우, 전처리기는 이를 잠재적인 공격으로 해석하며, 관련 전처리기 규칙이 활성화된 경우 시스템은 전처리기 이벤트를 생성합니다.
- 패킷에 의해 트리거될 때 침입 이벤트를 생성할 수 있도록 침입 규칙 엔진 내에서 대부분의 표준 텍스트 규칙 및 공유 개체 규칙이 작성됩니다.

데이터베이스에 침입 이벤트가 누적됨에 따라 잠재적인 공격의 분석을 시작할 수 있습니다. 시스템은 침입 이벤트를 검토하고 네트워크 환경 및 보안 정책의 컨텍스트에서 중요성을 띠는지 여부를 평가하는 데 필요한 도구를 제공합니다.

시스템 제공 및 맞춤형 네트워크 분석 및 침입 정책

새로운 액세스 제어 정책을 생성하는 것이 Firepower System을 사용하여 트래픽 플로우를 관리하는 첫 단계 중 하나입니다. 기본적으로, 새로 만든 액세스 제어 정책은 트래픽을 검토하기 위해 시스템 제공 네트워크 분석 및 침입 정책을 호출합니다.

다음 다이어그램은 인라인 침입 방지 배포에서 새로 만든 액세스 제어 정책이 트래픽을 초반에 처리하는 방식을 보여줍니다. 전처리 및 침입 방지 단계는 강조 표시됩니다.



다음 방식을 참고하십시오.

- 기본 네트워크 분석 정책이 액세스 제어 정책에서 처리된 모든 트래픽의 전처리를 제어하는 방식. 초기에는 시스템이 제공한 *Balanced Security and Connectivity*(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본값입니다.
- 액세스 제어 정책의 기본 작업은 시스템이 제공한 *Balanced Security and Connectivity*(균형 잡힌 보안 및 연결성)에 의해 결정된 대로 모든 비 악성 트래픽을 허용합니다. 기본 작업에서 트래픽 통과를 허용하므로 침입 정책이 악성 트래픽을 검사하고 잠재적으로 차단하기 전에 검색 기능이 트래픽에서 호스트, 애플리케이션, 사용자 데이터를 검사할 수 있습니다.
- 정책은 기본 보안 인텔리전스 옵션(전역 차단 및 차단 금지 목록)을 사용하고, SSL 정책 내에서 암호화된 트래픽을 해독하지 않으며, 액세스 제어 규칙을 사용하여 네트워크 트래픽의 특수 처리 및 검사를 수행하지 않습니다.

침입 방지 배포를 조정하기 위해 취할 수 있는 간단한 조치는 시스템 제공 네트워크 분석 및 침입 정책의 서로 다른 집합을 기본값으로 사용하는 것입니다. Cisco는 Firepower System에서 이러한 정책의 여러 쌍을 제공합니다.

또는, 사용자 지정 정책을 생성하고 사용하여 침입 방지 배포를 맞춤화할 수 있습니다. 전처리기 옵션, 침입 규칙 및 이 정책에 구성된 기타 고급 설정이 네트워크의 보안 요구를 충족하지 않음을 알게 될 수도 있습니다. 네트워크 분석 및 침입 정책을 설정하여 시스템이 침입 탐지를 위해 네트워크에서 트래픽을 처리하고 검사하는 방식을 매우 세부적으로 구성할 수 있습니다.

시스템 제공 네트워크 분석 및 침입 정책

Cisco는 Firepower System에서 네트워크 분석 정책과 침입 정책의 여러 쌍을 제공합니다. 시스템이 제공하는 네트워크 분석 및 침입 정책을 사용하여 Cisco Talos Intelligence Group(Talos)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 전처리기 규칙 상태뿐 아니라 전처리기의 초기 구성과 기타 고급 설정을 제공합니다.

모든 네트워크 프로파일, 트래픽 혼합 또는 방어 태세를 포괄하는 시스템 제공 정책은 없습니다. 각각은 잘 조정된 방어 정책의 시작점을 제공하는 일반적인 사례와 네트워크 설정을 다룹니다. 시스템에서 제공하는 정책을 그대로 사용해도 되지만 Cisco는 사용자의 네트워크에 맞게 조정하는 맞춤형 정책의 기반으로 사용할 것을 강력하게 권장합니다.

팁 시스템에서 제공한 네트워크 분석 및 침입 정책을 사용하고 있는 경우에도 자신의 네트워크 환경을 정확하게 반영할 수 있도록 시스템의 침입 변수를 구성해야 합니다. 최소한 기본값 집합의 주요 기본 변수는 수정하시기 바랍니다.

새로운 취약성이 알려지면 Talos에서 침입 규칙 업데이트(*Snort Rule Updates(Snort* 규칙 업데이트*)*라고도 함)를 릴리스합니다. 이 규칙 업데이트는 모든 시스템 제공 네트워크 분석 또는 침입 정책을 수정할 수 있고 새롭게 업데이트된 침입 규칙 및 전처리기 규칙, 기존 규칙을 위한 수정된 상태, 그리고 수정된 기본 정책 설정을 제공할 수 있습니다. 규칙 업데이트는 또한 시스템 제공 정책에서 규칙을 삭제할 수 있고, 새로운 규칙 카테고리를 제공할 수 있으며, 기본 변수 집합을 수정할 수 있습니다.

규칙 업데이트가 구축에 영향을 미치는 경우, 웹 인터페이스에는 영향을 받는 침입 및 네트워크 분석 정책은 물론 해당 상위 액세스 제어 정책도 최신이 아닌 것으로 표시됩니다. 변경 사항이 적용되려면 업데이트된 정책을 다시 구축해야 합니다.

편의상 규칙 업데이트를 구성하여 영향을 받는 침입 정책을 단독으로 또는 영향을 받는 액세스 제어 정책과 조합하여 자동으로 다시 구축할 수 있습니다. 이를 통해 쉽고 자동적으로 사용자 배포를 최신 상태로 유지하여 최근 발견된 침입 및 익스플로잇으로부터 보호할 수 있습니다.

전처리 설정을 최신으로 유지하려면 반드시 액세스 제어 정책을 다시 구축해야 합니다. 그러면 현재 실행 중인 것과 다른 모든 관련 SSL, 네트워크 분석 및 파일 정책이 다시 적용되며, 고급 전처리 및 성능 옵션의 기본값도 업데이트할 수 있습니다.

Cisco는 Firepower System에서 다음 네트워크 분석 및 침입 정책을 제공합니다.

Balanced Security and Connectivity(보안과 연결의 균형 유지**)** 네트워크 분석 및 침입 정책

이 정책은 속도 및 탐지 모두에 구축됩니다. 이들은 함께 사용되며, 대다수 조직 및 배포 유형을 위해 좋은 시작점의 역할을 합니다. 시스템은 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 정책 및 설정을 대부분의 경우 기본값으로 사용합니다.

Connectivity Over Security(연결이 보안에 우선함**)** 네트워크 분석 및 침입 정책

이 정책은 (모든 리소스에 접근할 수 있는) 연결성이 네트워크 인프라 보안에 우선하는 조직을 위해 구축됩니다. 침입 정책은 Security Over Connectivity(보안이 연결에 우선함)에서 활성화된 것보다 훨씬 더 적은 규칙을 활성화합니다. 트래픽을 차단하는 가장 중요한 규칙만 사용 설정됩니다.

Security Over Connectivity(보안이 연결에 우선함**)** 네트워크 분석 및 침입 정책

이 정책은 네트워크 인프라 보안이 사용자 편의에 우선하는 조직을 위해 구축됩니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다.

Maximum Detection(최대 탐지**)** 네트워크 분석 및 침입 정책

이러한 정책은 Security over Connectivity(연결보다 보안 우선) 정책보다 네트워크 인프라 보안이 더 강조되는 조직에 구축되며, 운영에 더 큰 영향을 미칠 수 있습니다. 예를 들어 이 침입 정책에서는 악성코드, 익스플로잇 킷, 오래된 일반적인 취약성, 통제되지 않은 알려진 익스플로잇 등 다수의 위협 범주에서 규칙을 활성화합니다.

No Rules Active(활성 규칙 불가**)** 침입 정책

No Rules Active(활성 규칙 불가) 침입 정책에서는 모든 침입 규칙 및 침입 규칙 임계값을 제외한 모든 고급 설정이 비활성화됩니다. 이 정책은 다른 시스템 제공 정책 중 하나에서 활성화된 규칙에 근거를 두는 것을 대신하여 사용자 고유의 침입 정책 생성을 원할 경우 시작점이 됩니다.

참고 선택한 시스템 제공 기본 정책에 따라 정책 설정은 달라집니다. 정책 설정을 보려면 정책 옆에 있는 수정 아이콘을 클릭하고 **Manage Base Policy(**기본 정책 관리**)** 링크를 클릭합니다.

맞춤형 네트워크 분석 및 침입 정책의 이점

전처리기 옵션, 침입 규칙 및 시스템 제공 네트워크 분석 또는 침입 정책에 구성된 기타 고급 설정이 조직의 보안 요구를 완전히 충족하지 않음을 확인할 수도 있습니다.

사용자 지정 정책을 구축하는 것은 사용자 환경에서 시스템의 성능을 개선할 수 있으며, 사용자 네트워크에서 일어나는 악의적인 트래픽 및 정책 위반을 집중적으로 살펴볼 수 있도록 할 수 있습니다. 사용자 지정 정책을 생성하고 설정함에 따라 사용자는 시스템이 침입 탐지를 위해 네트워크에서 트래픽을 처리하고 검사하는 방식을 매우 세부적으로 구성할 수 있습니다.

모든 사용자 정책에는 기본 정책이 있으며, 이는 기본 레이어라고도 하는데, 정책의 모든 구성에 대한 기본 설정을 정의합니다. 레이어는 여러 네트워크 분석 또는 침입 정책을 효율적으로 관리하는 데 사용할 수 있는 구성 요소입니다.

대부분의 경우, 사용자 지정 정책은 시스템 제공 정책을 기반으로 하지만, 다른 사용자 지정 정책을 사용할 수 있습니다. 하지만, 사용자 지정 정책은 시스템 제공 정책을 정책 체인의 궁극적인 기반으로 둡니다. 사용자 지정 정책을 사용자 기반으로 사용하는 경우 규칙 업데이트는 시스템 제공 정책을 변경할 수 있으며, 규칙 업데이트를 가져오는 것이 사용자에게 영향을 미칠 수 있습니다. 규칙 업데

이트가 구축에 영향을 미치는 경우, 웹 인터페이스는 영향받는 정책을 최신 상태가 아닌 것으로 표시합니다.

맞춤형 네트워크 분석 정책의 이점

기본적으로 하나의 네트워크 분석 정책이 액세스 제어 정책에서 다루는 모든 암호화되지 않은 트래픽을 전처리합니다. 이는 모든 패킷이 나중에 이들을 검토하는 침입 정책(따라서 침입 규칙 집합)에 관계없이 동일한 설정에 따라 디코딩 및 전처리된다는 것을 의미합니다.

초기에는 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본값입니다. 전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다.

사용 가능한 옵션 조정은 전처리기에 따라 다르지만, 전처리기 및 디코더를 조정할 수 있는 일부 방법은 다음을 포함합니다:

- 모니터링하는 트래픽에 적용하지 않는 전처리를 비활성화할 수 있습니다. 예를 들어, HTTP Inspect(HTTP 검사) 전처리기는 HTTP 트래픽을 표준화합니다. 네트워크에 Microsoft IIS(Internet Information Services)를 사용하는 웹 서버가 없는 것이 확실하면 IIS 관련 트래픽을 검색하는 전처리기 옵션을 비활성화하여 시스템 처리 오버헤드를 줄일 수 있습니다.

참고 맞춤형 네트워크 분석 정책에서 전처리기를 비활성화했지만 시스템이 나중에 해당 전처리기를 사용하여 활성화된 침입 또는 전처리기 규칙에 대해 패킷을 평가해야 하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 전처리기를 자동으로 활성화하여 사용합니다.

- 적절하다고 판단되는 경우, 포트를 지정하여 특정 전처리기 활동에 집중합니다. 예를 들어 DNS 서버 응답이나 암호화된 SSL 세션을 모니터링하기 위한 추가 포트 또는 텔넷, HTTP 및 RPC 트래픽을 해독하는 포트를 식별할 수 있습니다.

복합적인 배포를 사용하는 고급 사용자의 경우, 다수의 네트워크 분석 정책을 생성할 수 있는데, 각각은 트래픽을 다르게 전처리하기 위해 조정된 것입니다. 그런 다음 이러한 정책을 사용하도록 시스템을 구성하여 서로 다른 보안 영역, 네트워크 또는 VLAN을 사용하는 트래픽의 전처리를 제어할 수 있습니다 (ASA FirePOWER 모듈은 VLAN에 의한 전처리를 제한할 수 없습니다.)

참고 사용자 지정 네트워크 분석 정책, 특히 다중 네트워크 분석 정책을 사용하여 전처리를 조작하는 것은 고급 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 반드시 주의하여 서로 보완하는 단일 패킷을 검토하는 네트워크 분석 및 침입 정책을 허용해야 합니다.

사용자 지정 침입 정책의 이점

처음에 침입 방지를 수행하도록 구성된 새로 만든 액세스 제어 정책에서 기본 작업은 모든 트래픽을 허용하지만, 먼저 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입

정책으로 이를 검사합니다. 액세스 제어 규칙을 추가하거나 기본 작업을 변경하지 않는 한 모든 트래픽은 해당 침입 정책에 의해 검사됩니다.

침입 방지 배포를 사용자 정의하려면 여러 침입 정책을 만들 수 있는데, 각각은 트래픽을 검사하기 위해 서로 다르게 지정됩니다. 다음으로 어떤 정책이 어떤 트래픽을 검사하는지를 지정하는 규칙으로 액세스 제어 정책을 구성합니다. 액세스 제어 규칙은 간단하거나 복잡할 수 있으며, 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL 및 사용자를 포함하는 여러 기준을 사용하여 트래픽과 일치시키고 검사합니다.

침입 정책의 주요 기능은 어느 침입 및 전처리기 규칙이 활성화되는지와 다음과 같이 이들이 구성되는 방식을 관리하는 것입니다.

- 각 침입 정책 내에서 사용자의 환경에 적용 가능한 모든 규칙이 활성화되어 있음을 확인해야 하며, 환경에 적용할 수 없는 규칙은 비활성화하여 성능을 향상시켜야 합니다. 인라인 배포에서, 악성 패킷을 삭제하거나 수정할 규칙을 지정할 수 있습니다.
- Firepower 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결할 수 있습니다.
- 필요에 따라 기존 규칙을 수정하고 새 표준 텍스트 규칙을 작성하여 새로운 익스플로잇을 포착하거나 보안 정책을 적용할 수 있습니다.

침입 정책에 만들 수 있는 다른 사용자 지정은 다음을 포함합니다.

- 중요한 데이터 전처리기는 신용 카드 번호 및 ASCII 문자로 표시된 Social Security numbers(사회보장 번호)와 같은 중요한 데이터를 탐지합니다. Back Orifice 공격, 몇몇 포트스캔 유형 및 과도한 트래픽으로 네트워크의 무력화를 시도하는 속도 기반 공격 등 특정 위협을 탐지하는 그 밖의 전처리기는 네트워크 분석 정책에서 구성됩니다.
- 전역 임계값은 침입 규칙과 일치하는 트래픽이 얼마나 많이 지정된 기간 내 특정 주소 또는 주소 범위를 대상으로 하거나 특정 주소 또는 주소 범위로부터 발생하는지에 근거하여 시스템이 이벤트를 생성하도록 합니다. 이를 통해 많은 수의 이벤트로 인해 시스템이 마비되는 것을 방지할 수 있습니다.
- 침입 이벤트 알림을 차단하고 개별 규칙 또는 전체 침입 정책에 대한 임계값을 설정하여 많은 수의 이벤트로 인해 시스템이 마비되는 것을 방지할 수 있습니다.
- 웹 인터페이스 내 침입 이벤트다양한 보기 이외에도, syslog 기능에 로깅을 활성화하거나 SNMP 트랩 서버에 이벤트 데이터를 보낼 수 있습니다. 정책별로 침입 이벤트 알림 제한을 지정하고, 외부 로깅 기능에 침입 이벤트 알림을 설정하며, 침입 이벤트에 외부 응답을 구성할 수 있습니다. 이러한 정책 단위 경고 컨피그레이션 외에도 각 규칙이나 규칙 그룹에 대해 침입 이벤트의 이메일 경고를 전역적으로 활성화 또는 비활성화할 수 있습니다. 어떤 침입 정책이 패킷을 처리하는지와 상관없이 이메일 경고 설정이 사용됩니다.

사용자 지정 정책의 한계

전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 반드시 주의하여 구성이 서로 보완하는 단일 패킷을 처리하고 검토하는 네트워크 분석 및 침입 정책을 허용할 수 있도록 해야 합니다.

기본적으로, 시스템은 단일 액세스 제어 정책을 사용하여 매니지드 디바이스에서 처리된 모든 트래픽을 전처리하도록 하나의 네트워크 분석 정책을 사용합니다. 다음 다이어그램은 인라인 침입 방지 배포에서 새로 만든 액세스 제어 정책이 트래픽을 초반에 처리하는 방식을 보여줍니다. 전처리 및 침입 방지 단계는 강조 표시됩니다.

기본 네트워크 분석 정책이 액세스 제어 정책에서 처리된 모든 트래픽의 전처리를 제어하는 방식에 유의하십시오. 초기에는 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본값입니다.

전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다. 그러나 맞춤형 네트워크 분석 정책에서 전처리기를 비활성화했지만 시스템이 활성화된 침입 또는 전처리기 규칙에 대해 전처리된 패킷을 평가해야 하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 전처리기를 자동으로 활성화하여 사용합니다.

참고 전처리기를 비활성화하는 성능 이점을 가져오려면, 반드시 전처리기를 요구하는 규칙을 활성화한 침입 정책이 없음을 확인해야 합니다.

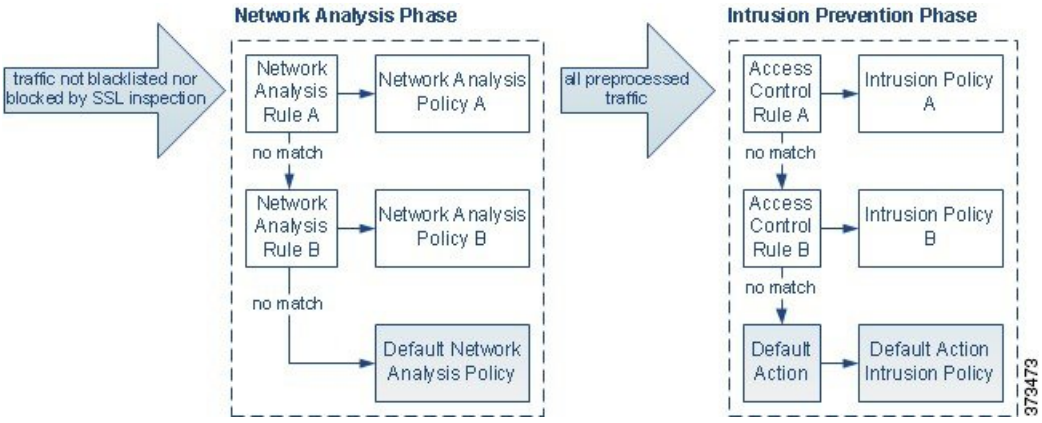
여러 사용자 지정 네트워크 분석 정책을 사용하는 경우 추가 문제가 발생합니다. 복잡한 구축을 수행하는 고급 사용자의 경우, 일치하는 트래픽을 전처리하는 맞춤형 네트워크 분석 정책을 할당하여 특정 보안 영역, 네트워크, VLAN에 맞게 전처리를 조정할 수 있습니다. (ASA FirePOWER은 VLAN에 의한 전처리를 제한할 수 없는 점에 유의하십시오.) 이를 수행하려면, 액세스 제어 정책에 사용자 지정 네트워크 분석 규칙을 추가합니다. 각 규칙에 규칙과 일치하는 트래픽의 전처리를 관리하는 연결된 네트워크 정책 분석이 있습니다.

팁 액세스 제어 정책의 고급 설정으로 네트워크 분석 규칙을 구성합니다. Firepower System의 다른 규칙 유형과는 달리 네트워크 분석 규칙은 네트워크 분석 정책에 포함되지 않고 네트워크 분석 정책을 호출합니다.

시스템은 규칙 번호로 하향식 순서로 구성된 모든 네트워크 분석 규칙에 패킷을 일치시킵니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다. 이는 사용자에게 트래픽을 전처리하는 데 있어 많은 유연성을 제공하지만, 어느 네트워크 분석 정책이 패킷을 전처리했는지에 상관없이 모든 패킷은 고유의 프로세스에서 순차적으로 액세스 제어 규칙에 일치되므로 침입 정책에 의해 잠재적인 검사에도 일치된다는 점에 유의하십시오. 즉, 특정 네트워크 분석 정책을 통해 패킷을 전처리하면 해당 패킷이 특정 침입 정책으로 검토된다고 보장되지 않습니다. 반드시 신중하게 액세스 제어 정책을 구성하여 특정 패킷을 평가하는 올바른 네트워크 분석 및 침입 정책을 호출하도록 해야 합니다.

다음 다이어그램은 네트워크 분석 정책 (전처리) 선택 단계가 어떻게 해서 침입 방지 (규칙) 단계 전에 또는 별도로 발생하는지를 집중적으로 자세히 보여줍니다. 간소화를 위해 다이어그램은 탐색 및

파일/악성코드 검사 단계를 포함하지 않습니다. 이는 또한 기본 네트워크 분석 및 기본 작업 침입 정책을 강조 표시합니다.



이 시나리오에서 액세스 제어 정책은 두 개의 네트워크 분석 규칙 및 기본 네트워크 분석 정책으로 구성됩니다.

- Network Analysis Rule A(네트워크 분석 규칙 A)는 Network Analysis Policy A(네트워크 분석 규칙 A)로 일치하는 트래픽을 전처리합니다. 나중에 이 트래픽을 Intrusion Policy A(침입 정책 A)로 검사할 수 있습니다.
- Network Analysis Rule B(네트워크 분석 규칙 B)는 Network Analysis Policy B(네트워크 분석 규칙 B)로 일치하는 트래픽을 전처리합니다. 나중에 이 트래픽을 Intrusion Policy B(침입 정책 B)로 검사할 수 있습니다.
- 나머지 모든 트래픽은 기본 네트워크 분석 정책으로 전처리됩니다. 나중에, 이 트래픽을 액세스 제어 정책의 기본 작업과 관련된 침입 정책에 따라 검사할 수 있습니다.

시스템은 트래픽을 전처리한 후, 침입 탐지를 위해 트래픽을 검토할 수 있습니다. 다이어그램은 두 개의 액세스 제어 규칙 및 기본 작업으로 액세스 제어 정책을 보여 줍니다.

- Access Control Rule A(액세스 제어 규칙 A)가 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 Intrusion Policy A(침입 정책 A)로 검사됩니다.
- Access Control Rule B(액세스 제어 규칙 B)가 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 Intrusion Policy B(침입 정책 B)로 검사됩니다.
- 액세스 제어 정책의 기본 작업이 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 기본 작업의 침입 정책에 의해 검사됩니다.

각 패킷의 처리는 네트워크 분석 정책과 침입 정책 쌍에 의해 제어되지만, 시스템이 사용자를 대신하여 쌍을 조정하는 것은 아닙니다. Network Analysis Rule A(네트워크 분석 규칙 A) 및 Access Control Rule A(액세스 제어 규칙 A)가 동일한 트래픽을 처리하지 않도록 액세스 제어 정책을 잘못 설정한 시나리오를 고려하십시오. 예를 들어, 특정 보안 영역에서 트래픽 처리를 제어하기 위해 페어링된 정책을 의도할 수 있지만 두 규칙의 조건에서 서로 다른 영역을 잘못 사용하는 것입니다. 그러면 트래픽이 잘못 전처리될 수 있습니다. 따라서, 네트워크 분석 규칙 및 사용자 지정 정책을 사용하여 전처리를 조작하는 것은 고급 작업입니다.

단일 연결의 경우, 시스템은 액세스 제어 규칙에 앞서 네트워크 분석 정책을 선택하지만, 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후에 발생한다는 점에 유의하십시오. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방식에 영향을 주지 않습니다.

네트워크 분석 및 침입 정책에 대한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

네트워크 분석 및 침입 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

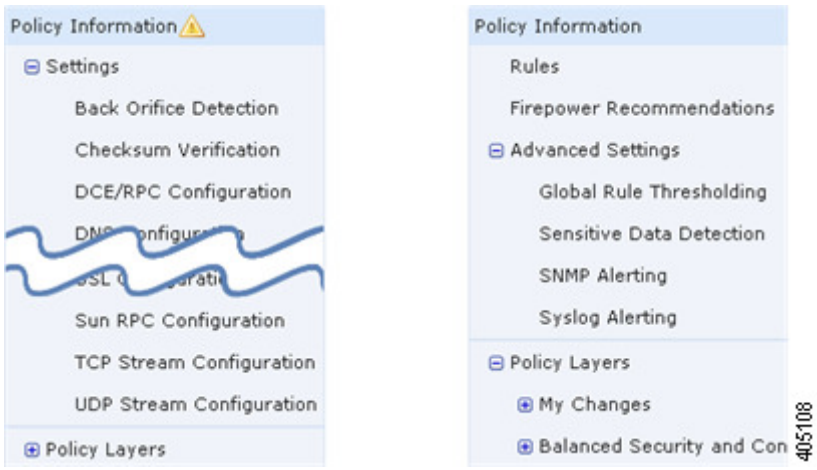
사용자 역할

- 관리자
- 침입 관리자

탐색 패널: 네트워크 분석 및 침입 정책

네트워크 분석 정책과 침입 정책은 비슷한 웹 인터페이스를 사용하여 구성을 수정하고 변경 사항을 저장합니다.

탐색 패널은 두 정책 유형 중 하나를 수정할 때 웹 인터페이스의 왼쪽에 나타납니다. 다음 그래픽은 네트워크 분석 정책(왼쪽) 및 침입 정책(오른쪽) 탐색 패널을 표시합니다.



분계선이 정책 설정으로 연결되는 링크로 탐색 패널을 분리합니다. 정책 설정은 정책 레이어와의 직접 상호 작용이 있는 것(아래) 또는 해당 상호 작용이 없는 것(위)으로 구성할 수 있습니다. 모든 설정 페이지로 이동하려면 탐색 패널에서 해당 이름을 클릭합니다. 탐색 패널에서 항목을 어둡게 하는 것은 현재 설정 페이지를 강조 표시합니다. 예를 들어, Policy Information(정책 정보) 위에 있는 그림에서 페이지는 탐색 패널의 오른쪽에 표시됩니다.

정책 정보

Policy Information(정책 정보) 페이지는 일반적으로 사용되는 설정을 위한 구성 옵션을 제공합니다. 위에 표시된 네트워크 분석 정책 패널의 그림과 같이, 정책이 저장되지 않은 변경 사항을 포함할 때 정책 변경 아이콘이 탐색 패널의 **Policy Information(**정책 정보**)** 옆에 나타납니다. 변경 사항을 저장하면 아이콘은 사라집니다.

규칙**(**침입 정책만**)**

침입 정책의 Rules(규칙) 페이지에서 공유 개체 규칙, 표준 텍스트 규칙, 전처리 규칙의 규칙 상태 및 기타 설정을 구성할 수 있습니다.

Firepower 권장 사항**(**침입 정책만 해당**)**

침입 정책의 Firepower Recommendations(Fireppower 권장 사항) 페이지에서는 네트워크에서 탐지되는 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산 보호를 위해 특별히 작성된 침입 규칙과 연결할 수 있습니다. 이렇게 하면 모니터링되는 네트워크의 특정 요구에 맞게 침입 정책을 맞춤화할 수 있습니다.

설정**(**네트워크 분석 정책**)** 및 고급 설정**(**침입 정책**)**

네트워크 분석 정책에서 Settings(설정) 페이지를 통해 전처리기를 활성화하거나 비활성화하고 전처리기 구성 페이지에 액세스할 수 있습니다. **Settings(**설정**)** 링크를 확장하여 정책의 모든 활성화된 전처리기를 위한 개별 구성 페이지로 연결되는 하위 링크를 표시합니다.

침입 정책에서 Advanced Settings(고급 설정) 페이지를 통해 고급 설정 및 해당 고급 설정을 위한 액세스 구성 페이지를 활성화하거나 비활성화할 수 있습니다. **Advanced Settings(**고급 설정**)** 링크를 확장

하여 정책에서 활성화된 모든 고급 설정을 위한 개별 구성 페이지로 연결되는 하위 링크를 표시합니다.

정책 레이어

Policy Layers(정책 레이어) 페이지는 네트워크 분석 또는 침입 정책을 구성하는 레이어에 대한 요약을 표시합니다. Policy Layers(정책 레이어) 페이지를 확장하여 정책의 레이어를 위한 요약 페이지로 연결되는 하위 링크를 표시합니다. 각 레이어 하위 링크를 확장하면 레이어에서 활성화된 모든 규칙, 전처리기 또는 고급 설정에 대한 구성 페이지로 연결되는 하위 링크를 표시합니다.

충돌 및 변경: 네트워크 분석 및 침입 정책

네트워크 분석 또는 침입 정책을 편집하면 탐색 패널의 **Policy Information(**정책 정보**)** 옆에 정책 변경 아이콘이 나타나 저장되지 않은 변경 사항이 정책에 포함되어 있음을 표시합니다. 시스템에서 변경 내용을 인식하기 전에 변경 내용을 저장(또는 커밋)해야 합니다.

참고 저장한 후에는 변경 사항을 적용하기 위해 네트워크 분석 또는 침입 정책을 배포해야 합니다. 저장하지 않고 정책을 배포했다면 가장 최근에 저장된 구성을 사용하십시오.

수정 문제 해결

네트워크 분석 정책 페이지(**Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**))**와 침입 정책 페이지(**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**))**는 각 정책이 저장되지 않은 변경 사항을 가지고 있는지 여부와 현재 정책을 편집하고 있는 사람에 대한 정보를 표시합니다. Cisco는 한 번에 한 명만 정책을 편집할 것을 권장합니다. 동시 편집을 수행하는 경우 그 결과는 다음과 같습니다.

- 네트워크 분석 또는 침입 정책을 동시에 편집하거나 다른 사용자가 동일한 정책을 편집하는 경우 다른 사용자가 변경 내용을 정책에 저장하면 다른 사용자의 변경 내용을 덮어쓸 것이라는 주의를 받습니다.
- 여러 웹 인터페이스 인스턴스를 통해 동일한 사용자와 동일한 네트워크 분석 또는 침입 정책을 편집하는 경우 한 인스턴스에 대한 변경 내용을 저장하면 다른 인스턴스에 대한 변경 내용을 저장할 수 없습니다.

구성 종속성 해결

특정 분석을 수행하기 위해, 많은 전처리기와 침입 규칙은 트래픽이 특정 방법으로 먼저 디코딩되거나 전처리되도록, 또는 다른 종속성을 갖도록 요청합니다. 네트워크 분석 또는 침입 정책을 저장하면, 시스템은 자동으로 필수 설정을 활성화하거나 다음과 같이 비활성화된 설정은 트래픽에 영향을 미치지 못함을 경고합니다.

- SNMP 알림 규칙을 추가했지만 SNMP 경고를 구성하지 않은 경우 침입 정책을 저장할 수 없습니다. SNMP 경고를 설정하거나 규칙 경고를 비활성화한 후 다시 저장해야 합니다.

- 침입 정책이 활성화된 중요한 데이터를 포함하지만 중요한 데이터 전처리를 활성화하지 않은 경우 침입 정책을 저장할 수 없습니다. 시스템이 전처리를 활성화하고 정책을 저장할 수 있도록 하거나, 규칙을 비활성화하고 다시 저장할 수 있도록 해야 합니다.
- 네트워크 분석 정책에 필요한 전처리기를 비활성화한 경우에도, 여전히 정책을 저장할 수 있습니다. 그러나 시스템은 웹 인터페이스에서 전처리기가 비활성화된 상태로 유지되더라도 현재 설정으로 비활성화된 전처리기를 자동으로 사용합니다.
- 네트워크 분석 정책에서 인라인 모드를 비활성화하지만 Inline Normalization(인라인 표준화) 전처리기를 활성화한 경우, 여전히 정책을 저장할 수 있습니다. 그러나 시스템은 표준화 설정이 무시될 것임을 경고합니다. 인라인 모드를 비활성화해도 전처리기가 트래픽을 수정하거나 차단할 수 있는 다른 설정을 시스템이 무시하는 결과를 야기하며, 여기에는 체크섬 유효성 검증 및 속도 기반 공격 방지가 포함됩니다.

정책 변경 커밋, 삭제 및 캐싱

네트워크 분석 또는 침입 정책을 수정할 때 변경 사항을 저장하지 않고 정책 편집기를 종료할 경우, 시스템은 해당 변경 사항을 캐시합니다. 변경 사항은 시스템에서 로그아웃하거나 시스템 충돌이 발생할 때도 캐시됩니다. 시스템 캐시는 사용자 당 네트워크 분석 하나와 침입 정책 하나에 대한 저장되지 않은 변경 사항을 저장할 수 있습니다. 동일한 유형의 다른 정책을 수정하려면 먼저 변경 사항을 커밋하거나 삭제해야 합니다. 시스템은 변경 내용을 처음 정책에 저장하지 않고 다른 정책을 수정할 때 또는 침입 규칙 업데이트를 가져올 때 캐시된 변경 사항을 삭제합니다.

네트워크 분석 또는 침입 정책 편집기의 정책 정보 페이지에서 정책 변경을 커밋하거나 취소할 수 있습니다.

에 Firepower Management Center 컨피그레이션을 제어할 수 있습니다.

- 네트워크 분석 또는 침입 정책 변경 사항을 커밋할 때 코멘트를 표시할지 여부를 묻거나 필수인 경우
- 여부 변경 및 메모는 감사 로그 기록

관련 항목

네트워크 분석 정책 환경설정
침입 정책 환경설정

네트워크 분석 또는 침입 정책 종료

프로시저

네트워크 분석 또는 침입 정책 고급 편집기를 종료하려면 다음 중에서 선택할 수 있습니다.

- 캐시 - 정책을 종료하고 변경 사항을 캐시하려면 아무 메뉴 또는 다른 페이지 경로를 선택합니다. 종료 시 메시지가 표시되면 **Leave page(**페이지에서 나가기**)**를 클릭하거나 고급 편집기에 남으려면 **Stay on page(**페이지에 남기**)**를 클릭합니다.

- 취소 - 저장되지 않은 변경 사항을 취소하려면 Policy Information(정책 정보 페이지)에서 **Discard Changes(**변경 취소**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.
- 저장 - 정책 변경 사항을 저장하려면 Policy Information(정책 정보) 페이지에서 **Commit Changes(**변경 적용**)**를 클릭합니다. 메시지가 표시되면 코멘트를 입력하고 **OK(**확인**)**를 클릭합니다.

79 장

침입 및 네트워크 분석 정책의 레이어

다음 주제에서는 침입 및 네트워크 분석 정책에서 레이어를 사용하는 방법을 설명합니다.

- 레이어 기본 사항, 1979 페이지
- 네트워크 분석 및 침입 정책 레이어를 위한 라이선스 요건, 1979 페이지
- 네트워크 분석 및 침입 정책 레이어에 대한 요구 사항 및 사전 요건, 1980 페이지
- 레이어 스택, 1980 페이지
- 레이어 관리, 1985 페이지

레이어 기본 사항

관리되는 디바이스가 많은 좀 더 큰 조직에는 여러 부서, 사업부 또는 경우에 따라 여러 회사의 고유한 요구를 지원하기 위한 다수의 침입 정책 및 네트워크 분석 정책이 있을 수 있습니다. 두 정책 유형의 구성은 여러 정책을 효율적으로 관리하기 위해 사용할 수 있는 레이어라는 구성 요소에 포함됩니다.

침입 및 네트워크 분석 정책의 레이어는 기본적으로 동일한 방식으로 작동합니다. 의식적으로 레이어를 사용하지 않고 각 정책 유형을 만들고 수정할 수 있습니다. 정책 구성을 수정할 수 있으며, 정책에 사용자 레이어를 추가하지 않은 경우 시스템은 초기 이름이 *My Changes(*내 변경 사항*)*인 구성 가능한 단일 레이어에 변경 사항을 자동으로 포함합니다. 또한, 최대 200개의 레이어를 추가할 수 있으며 이러한 레이어에서 설정의 조합을 구성할 수도 있습니다. 사용자 레이어를 복사, 병합, 이동 및 삭제할 수 있으며 가장 중요한 기능으로는 개별 사용자 레이어를 동일한 유형의 다른 정책과 공유할 수 있다는 점입니다.

네트워크 분석 및 침입 정책 레이어를 위한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

네트워크 분석 및 침입 정책 레이어에 대한 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

레이어 스택

레이어 스택은 다음으로 구성됩니다.

사용자 레이어

사용자가 구성 가능한 레이어입니다. 사용자 구성 가능한 레이어를 복사, 병합, 이동 또는 삭제할 수 있으며, 사용자 구성 가능한 모든 레이어를 동일한 유형의 다른 정책과 공유할 수 있습니다. 이 레이어에는 처음에 My Changes라는 이름이 지정되는 자동 생성된 레이어가 포함됩니다.

기본 제공 레이어

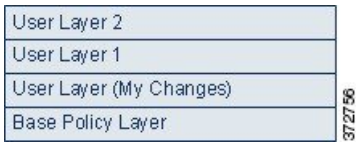
읽기 전용 기본 정책 레이어입니다. 이 레이어의 정책은 시스템 제공 정책 또는 사용자가 생성하는 맞춤형 정책일 수 있습니다.

기본적으로 네트워크 분석 또는 침입 정책에는 기본 정책 레이어 및 My Changes 레이어가 포함됩니다. 필요에 따라 사용자 레이어를 추가할 수 있습니다.

각 정책 레이어에는 네트워크 분석 정책의 모든 프리프로세서에 대한 또는 침입 정책의 모든 침입 규칙 및 고급 설정에 대한 완전한 구성이 포함되어 있습니다. 최하위 기반 정책 레이어에는 정책 생성 시 선택한 기반 정책의 모든 설정이 포함되어 있습니다. 상위 레이어의 설정이 하위 레이어의 동일한 설정에 비해 우선권을 갖습니다. 레이어에 명시적으로 설정되지 않은 기능은 명시적으로 설정된 다음 최상위 레이어에서 설정을 상속합니다. 시스템은 레이어를 병합합니다. 즉, 네트워크 트래픽을 처리할 때 모든 설정의 누적된 효과만 적용합니다.

팁 전적으로 기반 정책의 기본 설정에 기반하는 침입 또는 네트워크 분석 정책을 생성할 수 있습니다. 침입 정책의 경우에는 모니터링되는 네트워크의 특정 요구 사항에 맞게 침입 정책을 조정하려는 경우, Firepower 규칙 상태 권장 사항을 사용할 수도 있습니다.

다음 그림은 레이어 스택의 예를 보여줍니다. 여기에는 기본 정책 레이어 및 초기 My Changes 레이어 외에 두 개의 사용자 구성 가능한 레이어인 *User Layer 1* 및 *User Layer 2*가 포함되어 있습니다. 이 그림에서, 추가하는 사용자 구성 가능한 각 레이어는 처음에 스택의 최상위 레이어에 배치됩니다. 따라서 그림의 User Layer 2는 스택에서 가장 마지막에 추가된 것이며 최상위 레이어입니다.



규칙 업데이트가 정책을 수정하도록 허용하는지와 상관없이, 규칙 업데이트의 변경 사항은 레이어에서 사용자가 수행한 변경 사항을 재정의하지 않습니다. 이는 규칙 업데이트의 변경 사항이 기반 정책에서 이루어지며, 이것이 기반 정책 레이어의 기본 설정을 결정하기 때문입니다. 사용자 변경 사항은 항상 상위 레이어에서 이루어지므로, 규칙 업데이트가 기반 정책에 대해 수행하는 모든 변경 사항을 재정의합니다.

기본 레이어

침입 또는 네트워크 분석 정책의 기반 레이어(기반 정책이라고도 함)는 정책의 모든 구성에 대한 기본 설정을 정의하며 정책에서 최하위 레이어입니다. 새 정책을 생성할 때 새 레이어를 추가하지 않은 채 설정을 변경하면 변경 사항은 My Changes(내 변경 사항) 레이어에 저장되며 기반 정책의 설정을 재정의합니다(그러나 변경하지는 않음).

시스템 제공 기반 정책

Firepower System은 여러 쌍의 네트워크 분석 정책과 침입 정책을 제공합니다. 시스템이 제공하는 네트워크 분석 및 침입 정책을 사용하여 Cisco Talos Intelligence Group(Talos)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 전처리기 규칙 상태뿐 아니라 전처리기의 초기 구성과 기타 고급 설정을 제공합니다. 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다.

시스템이 제공하는 정책을 기반으로 사용할 경우, 규칙 업데이트를 가져오면 기반 정책의 설정을 수정할 수 있습니다. 하지만 시스템이 시스템 제공 기반 정책을 자동으로 변경하지 않도록 맞춤형 정책을 구성할 수 있습니다. 이를 통해 규칙 업데이트와는 별개의 일정에 따라 시스템 제공 기본 정책을 수동으로 업데이트할 수 있습니다. 어떤 경우든, 규칙 업데이트가 기반 정책에 대해 수행하는 변경 사항은 My Changes(내 변경 사항) 또는 다른 레이어의 설정을 변경하거나 재정의하지 않습니다.

시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다.

맞춤형 기본 정책

맞춤형 정책을 기반으로 사용할 수 있습니다. 사용자 지정 정책의 설정을 조정하여 가장 중요하다고 생각되는 방식으로 트래픽을 검사할 수 있으며, 이에 따라 관리되는 디바이스의 성능과 디바이스가 생성하는 이벤트에 효과적으로 대응하는 능력 모두를 향상시킬 수 있습니다.

다른 정책의 기반으로 사용하는 맞춤형 정책을 변경하면 해당 변경 사항은 기반을 사용하는 정책의 기본 설정으로 자동으로 사용됩니다.

또한 모든 정책에는 정책 체인의 궁극적인 기반으로 시스템 제공 정책이 있기 때문에 맞춤형 기본 정책을 사용하는 경우에도 규칙 업데이트가 정책에 영향을 미칠 수 있습니다. 체인 내 첫 번째 사용자 지정 정책(시스템이 제공하는 정책을 기본으로 사용하는 것)은 규칙 업데이트가 해당 기본 정책을 수정하는 것을 허용하며, 사용자 정책에도 영향을 줄 수 있습니다.

기본 정책을 변경하는 방법에 상관없이(규칙 업데이트로 변경하거나 기본 정책으로 사용하는 맞춤형 정책을 수정하면서 변경하거나) 이러한 변경은 My Changes 또는 다른 레이어의 설정을 변경하거나 재정의하지 않습니다.

규칙 업데이트가 기본 정책에 미치는 영향

규칙 업데이트를 가져올 때 시스템은 시스템에서 제공한 침입, 액세스 제어, 네트워크 분석 정책을 수정합니다. 규칙 업데이트에는 다음이 포함될 수 있습니다.

- 수정된 네트워크 분석 전처리기 설정
- 침입 및 액세스 제어 정책의 수정된 고급 설정
- 신규 및 업데이트된 침입 규칙
- 기존 규칙의 수정된 상태
- 새 규칙 카테고리와 기본 변수

규칙 업데이트는 시스템 제공 정책에서 기존 규칙을 삭제할 수도 있습니다.

기본 변수 및 규칙 카테고리를 변경하면 시스템 수준에서 처리됩니다.

시스템 제공 정책을 침입 또는 네트워크 분석 기본 정책으로 사용하는 경우, 규칙 업데이트가 기본 정책(이 경우, 시스템 제공 정책의 복사본)을 수정하도록 허용할 수 있습니다. 규칙 업데이트가 기본 정책을 업데이트하는 것을 허용할 경우, 새로운 규칙 업데이트는 기본 정책으로 사용하는 시스템 제공 정책에 대한 변경 사항과 동일하게 기본 정책을 변경합니다. 해당 설정을 수정하지 않은 경우 기반 정책의 설정이 현재 정책의 설정을 결정합니다. 그러나 규칙 업데이트는 현재 정책에서 수행하는 변경 사항을 재정의하지 않습니다.

규칙 업데이트가 기본 정책을 수정하도록 허용하지 않는 경우, 하나 이상의 규칙 업데이트를 가져온 후 기본 정책을 수동으로 업데이트할 수 있습니다.

침입 정책의 규칙 상태와 상관없이 또는 규칙 업데이트가 기본 침입 정책을 업데이트하도록 허용하는지 여부와 상관없이, 규칙 업데이트는 Talos가 삭제하는 침입 규칙을 항상 삭제합니다.

변경 사항을 네트워크 트래픽에 다시 구축할 때까지 현재 구축된 침입 정책의 규칙은 다음과 같이 작동합니다.

- 비활성화된 침입 규칙은 비활성화 상태를 유지합니다.
- **Generate Events(**이벤트 생성**)**로 설정된 규칙은 트리거될 때 계속해서 이벤트를 생성합니다.
- **Drop and Generate Events(**이벤트 삭제 및 생성**)**로 설정된 규칙은 트리거될 때 계속해서 이벤트를 생성하고 위반 패킷을 삭제합니다.

규칙 업데이트는 다음 조건이 모두 충족되지 않으면 사용자 지정 기본 정책을 수정하지 않습니다.

- 규칙 업데이트를 통해 상위 정책의 시스템이 제공하는 기본 정책, 즉 사용자 지정 기본 정책을 생성한 정책을 수정할 수 있습니다.
- 상위 기본 정책 내 해당 설정을 대체하는 상위 정책을 변경하지 않았습니다.

두 조건이 충족된 경우, 상위 정책을 저장하면 규칙 업데이트 내 변경 사항이 하위 정책, 즉, 사용자 지정 기본 정책을 사용하는 정책에 전달됩니다.

예를 들어 규칙 업데이트가 이전에 비활성화된 침입 규칙을 활성화하여 상위 침입 정책의 규칙 상태를 수정하지 않은 경우, 상위 정책을 저장하면 수정된 규칙 상태가 기반 정책에 전달됩니다.

마찬가지로, 규칙 업데이트가 기본 프리프로세서 설정을 수정하고 상위 네트워크 분석 정책에서 설정을 수정하지 않은 경우, 상위 정책을 저장하면 수정된 설정이 기반 정책에 전달됩니다.

기반 정책 변경

다른 시스템 제공 정책 또는 맞춤형 정책을 기본 정책으로 선택할 수 있습니다.

최대 다섯 개의 사용자 지정 정책을 묶을 수 있는데, 다섯 중 넷은 이전에 만들어진 다른 넷 중 하나를 기본 정책으로 사용하는 것이며, 다섯 번째는 반드시 시스템이 제공하는 정책을 기본 정책으로 사용해야 합니다.

프로시저

단계 **1** 정책을 수정하는 동안 탐색 패널에서 **Policy Information(**정책 정보**)**을 클릭합니다.

단계 **2** 다음 옵션을 구성할 수 있습니다.

- 기본 정책 선택 - **Base Policy(**기본 정책**)** 드롭다운 목록에서 선택합니다.
- 규칙 업데이트가 기본 정책을 수정하도록 허용 - **Manage Base Policy(**기본 정책 관리**)**를 클릭한 다음 **Update when a new Rule Update is installed(**새 규칙 업데이트가 설치되면 업데이트**)** 확인란을 선택합니다.

  팁 확인란을 선택 취소하고 정책을 저장한 다음 규칙 업데이트를 가져오면 Base Policy(기반 정책) 요약 페이지에 **Update Now(**지금 업데이트**)**가 나타나고, 페이지의 상태 메시지가 업데이트되어 정책이 최신 상태가 아님을 알립니다. 가장 최근에 가져온 규칙 업데이트의 변경 사항으로 기본 정책을 업데이트하려면 **Update Now(**지금 업데이트**)**를 클릭합니다.

단계 **3** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

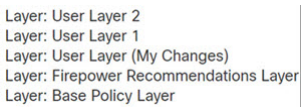
관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

Firepower Recommendations 레이어

침입 정책에서 규칙 상태 권장 사항을 생성할 때 권장 사항을 기반으로 규칙 상태를 자동으로 수정할지 여부를 선택할 수 있습니다.

다음 그림에서 보듯 권장 규칙 상태를 사용하면 읽기 전용 기본 제공 Firepower Recommendations 레이어가 기반 레이어 바로 위에 삽입됩니다.



이 레이어는 침입 정책에 고유합니다.

나중에 권장 규칙 상태를 사용하지 않기로 선택하면 시스템은 Firepower Recommendations 레이어를 제거합니다. 이 레이어는 수동으로 삭제할 수 없지만 권장 규칙 상태의 사용 여부를 선택하여 추가하고 삭제할 수 있습니다.

Firepower Recommendations 레이어를 추가하면 탐색 패널의 Policy Layers(정책 레이어) 아래에 Firepower Recommendations 링크가 추가됩니다. 이 링크를 클릭하면 Firepower Recommendations 레이어 페이지의 읽기 전용 보기가 나타납니다. 여기에서 Rules(규칙) 페이지의 권장 사항으로 필터링된 보기에 읽기 전용 모드로 액세스할 수 있습니다.

권장 규칙 상태를 사용하면 탐색 패널의 Firepower Recommendations 링크 아래에 Rules(규칙) 하위 링크도 추가됩니다. Rules(규칙) 하위 링크를 클릭하면 Firepower Recommendations 레이어에서 Rules(규칙) 페이지의 읽기 전용 표시에 액세스할 수 있습니다. 이 보기에서 다음에 유의하십시오.

- 상태 열에 규칙 상태 아이콘이 없으면 해당 상태는 기본 정책에서 상속된 것입니다.
- 이 보기 또는 다른 Rules(규칙) 페이지 보기의 Firepower Recommendations 열에 규칙 상태 아이콘이 없으면 이 규칙에 대한 권장 사항이 없는 것입니다.

관련 항목

네트워크 자산에 대한 침입 방지 맞춤화, 2037 페이지

레이어 관리

Policy Layers(정책 레이어) 페이지는 네트워크 분석 또는 침입 정책에 대한 완전한 레이어 스택을 요약하는 단일 페이지를 제공합니다. 이 페이지에서 공유 및 비공유 레이어를 추가하고, 레이어를 복사, 병합, 이동 및 삭제하고, 각 레이어의 요약 페이지에 액세스하고, 각 레이어 내에서 활성화, 비활성화 및 재정의된 구성에 대한 구성 페이지에 액세스할 수 있습니다.

각 레이어에 대해 다음 정보를 볼 수 있습니다.

- 레이어가 기본 제공 레이어인지, 공유된 사용자 레이어인지, 공유되지 않은 사용자 레이어인지 여부
- 가장 높은(효과적인) 프리프로세서 또는 고급 설정 구성이 포함되어 있는 레이어(기능 이름별)
- 침입 정책에서, 상태가 레이어에 설정되어 있고 각 규칙 상태에 대해 규칙 수가 설정된 침입 규칙의 수

Policy Layers(정책 레이어) 페이지는 또한 활성화된 모든 전처리기(네트워크 분석) 또는 고급 설정(침입), 침입 정책, 침입 규칙의 최종 효과에 대한 요약을 제공합니다.

각 레이어의 요약에 있는 기능 이름은 어떤 구성이 레이어에서 활성화, 비활성화, 재정의 또는 상속되었는지를 다음과 같이 나타냅니다.

기능 상태	기능 이름
레이어에서 활성화됨	일반 텍스트로 작성됨
레이어에서 비활성화됨	삭제됨
상위 레이어에서 구성에 의해 대체됨	기울임 꼴 텍스트로 작성됨
하위 레이어에서 상속됨	없음

네트워크 분석 또는 침입 정책에 최대 200개의 레이어를 추가할 수 있습니다. 레이어를 추가하면 정책에서 최상위 레이어로 나타납니다. 초기 상태는 모든 기능에 대한 Inherit(상속) 상태이며, 침입 정책에 이벤트 필터링, 동적 상태 또는 알림 규칙 작업이 설정되어 있지 않습니다.

레이어를 정책에 추가할 때 사용자 구성 가능한 레이어에 고유한 이름을 지정합니다. 나중에 이름을 변경할 수 있으며, 원하는 경우, 레이어를 수정할 때 표시되는 설명을 추가하거나 수정할 수 있습니다.

레이어를 복사하거나 User Layers(사용자 레이어) 페이지 영역 내에서 레이어를 위 또는 아래로 이동하거나 초기 My Changes 레이어를 포함한 사용자 레이어를 삭제할 수 있습니다. 다음과 같은 고려 사항을 참고하십시오,

- 레이어를 복사하면 복사본이 최상위 레이어로 나타납니다.
- 공유 레이어를 복사하면 처음에는 공유되지 않고 나중에 원하는 경우 공유할 수 있는 레이어가 생성됩니다.

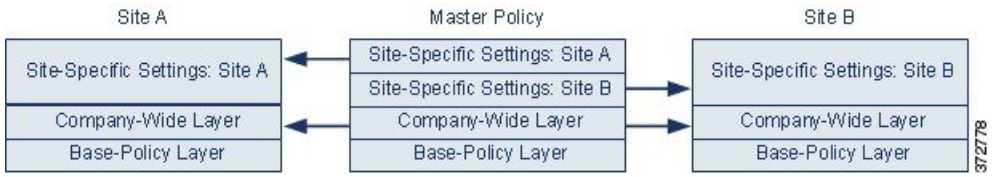
- 공유 레이어는 삭제할 수 없습니다. 공유가 활성화되었지만 다른 정책과 공유되지 않은 레이어는 공유 레이어가 아닙니다.

사용자 구성 가능 레이어를 바로 아래의 다른 사용자 구성 가능 레이어와 병합할 수 있습니다. 병합된 레이어는 각 레이어의 고유한 설정을 모두 보유하며, 두 레이어 모두 동일한 프리프로세서에 대한 설정, 침입 규칙 또는 고급 설정을 포함한 경우 상위 레이어의 설정을 수용합니다. 병합된 레이어는 하위 레이어의 이름을 유지합니다. 다른 정책에 추가할 수 있는 공유 가능 레이어를 생성하는 정책에서 공유 가능 레이어 바로 위의 비공유 레이어는 공유 가능 레이어와 병합할 수 있지만 공유 가능 레이어를 아래 있는 비공유 레이어와 병합할 수 없습니다. 또 다른 정책에서 생성한 공유 레이어를 추가하는 정책에서는 공유 레이어를 바로 아래에 있는 비공유 레이어와 병합할 수 있으며 이 경우 그 결과 레이어는 더 이상 공유되지 않습니다. 비공유 레이어는 그 아래에 있는 공유 레이어와 병합할 수 없습니다.

공유 레이어

공유 레이어는 공유를 허용하는 다른 정책에서 레이어를 생성한 후 정책에 추가 하는 레이어입니다. 공유 가능 레이어는 공유를 허용하는 레이어입니다.

다음 그림은 전사적 레이어와 사이트 A 및 B를 위한 사이트별 레이어를 생성하고 이를 공유하도록 허용하는 마스터 정책의 예를 보여줍니다. 그런 다음 이를 사이트 A 및 B에 대한 정책에 공유 레이어로 추가합니다.



마스터 정책의 전사적 레이어에는 사이트 A와 B에 적용할 수 있는 설정이 포함됩니다. 사이트별 레이어에는 각 사이트에 한정된 설정이 포함됩니다. 예를 들어 네트워크 분석 정책의 경우 Site A(사이트 A)에는 모니터링되는 네트워크에 웹 서버가 없을 수 있으며 HTTP Inspect 프리프로세서의 보호 또는 처리 오버헤드가 필요하지 않을 수 있지만, 두 사이트에 모두 TCP 스트림 전처리가 필요할 수 있습니다. 두 사이트 모두와 공유하는 전사적 레이어에서 TCP 스트림 프로세싱을 활성화할 수 있고, Site A(사이트 A)와 공유하는 사이트별 레이어에서 HTTP Inspect 프리프로세서를 비활성화할 수도 있으며, Site B(사이트 B)와 공유하는 사이트별 레이어에서 HTTP Inspect 프리프로세서를 활성화할 수도 있습니다. 또한 구성 조정에 필요한 경우 사이트별 정책의 상위 레이어에서 구성을 수정하여 각 사이트에 대한 정책을 추가적으로 조정할 수도 있습니다.

마스터 정책 예에서 합병된 최종 설정이 트래픽 모니터링에 유용할 것이라고 말할 수는 없지만, 사이트별 정책의 구성 및 업데이트에서 절약되는 시간을 고려하면 정책 레이어를 유용하게 응용하는 예라고 할 수 있습니다.

다른 많은 레이어 구성도 가능합니다. 예를 들어 회사, 부서, 네트워크, 심지어 사용자 단위로도 정책 레이어를 정의할 수 있습니다. 침입 정책의 경우 한 레이어에는 고급 설정을 포함하고 다른 레이어에는 규칙 설정을 포함할 수도 있습니다.

사용자 구성 가능한 레이어를 동일한 유형의 다른 정책(침입 또는 네트워크 분석)과 공유할 수 있습니다. 공유 가능 레이어 내에서 구성을 수정한 다음 변경 사항을 커밋하면 시스템은 레이어를 공유하

는 모든 정책을 업데이트하고 영향을 받는 모든 정책의 목록을 제공합니다. 레이어를 생성한 정책에 있는 기능 구성만 변경할 수 있습니다.

다른 정책에서 추가한 레이어에 대해서는 공유를 비활성화할 수 없습니다. 먼저 다른 정책에서 레이어를 삭제하거나 다른 정책을 삭제해야 합니다.

공유하고자 하는 레이어가 생성된 사용자 지정 정책이 기본 정책인 경우 정책에 공유 레이어를 추가할 수 없습니다. 이렇게 하면 정책에 순환 종속성이 부여됩니다.

다중 도메인 구축에서는 상위 정책의 공유 레이어를 하위 도메인의 정책에 추가할 수 있습니다.

레이어 관리

프로시저

단계 **1** 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다.

단계 **2** Policy Layers(정책 레이어) 페이지에서 다음 관리 작업을 수행할 수 있습니다.

- 다른 정책에서 공유 레이어 추가 - User Layers(사용자 레이어) 옆에 있는 Add Shared Layer(공유 레이어 추가) 아이콘(추가( ))을 클릭하고 **Add Shared Layer(**공유 레이어 추가**)** 드롭다운 목록에서 레이어를 선택한 다음 **OK(**확인**)**를 클릭합니다.
- 비공유 레이어 추가 - User Layers(사용자 레이어) 옆에 있는 Add Layer(레이어 추가) 아이콘(추가( ))을 클릭하고 **Name(**이름**)**을 입력한 다음 **OK(**확인**)**를 클릭합니다.
- 레이어 설명 추가 또는 변경 - 레이어 옆에 있는 수정( )을 클릭한 다음 **Description(**설명**)**을 추가하거나 변경합니다.
- 레이어를 다른 정책과 공유하도록 허용 - 레이어 옆에 있는 수정( )을 클릭한 다음 **Sharing(**공유**)** 확인란의 선택을 취소합니다.
- 레이어 이름 변경 - 레이어 옆에 있는 수정( )을 클릭한 다음 **Name(**이름**)**을 변경합니다.
- 레이어 복사 - 레이어의 복사 ( )를 클릭합니다.
- 레이어 삭제 - 레이어의 삭제( )를 클릭한 다음 **OK(**확인**)**를 클릭합니다.
- 두 레이어 병합 - 두 레이어 중 위 레이어의 병합( )를 클릭한 다음**OK(**확인**)**를 클릭합니다.
- 레이어 이동 - 레이어 요약에서 빈 영역을 클릭하고 위치 화살표가 레이어를 이동하려는 레이어 위나 아래에 있는 선을 가리킬 때까지 끕니다.

단계 **3** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

레이어 탐색

프로시저

단계 **1** 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다.

단계 **2** 다음 작업을 수행하여 레이어 간에 이동할 수 있습니다.

- 전처리기 또는 고급 설정 페이지에 액세스 - 레이어 수준 전처리기 또는 고급 설정 구성 페이지에 액세스하려면 해당 레이어 행에서 기능 이름을 클릭합니다. 구성 페이지는 기본 정책 및 공유 레이어에 있는 읽기 전용 페이지입니다.
- 규칙 페이지 액세스 - 규칙 상태 유형으로 필터링된 레이어 수준 규칙 설정 페이지에 액세스하려면 레이어 요약에서 **Drop and Generate Events(**이벤트 삭제 및 생성**)**, **Generate Events(**이벤트 생성**)** 또는 **Disabled(**비활성화**)**를 클릭합니다. 선택한 규칙 상태로 설정된 규칙이 레이어에 포함되지 않는 경우 규칙이 표시되지 않습니다.
- Policy Information(정책 정보) 페이지 표시 - Policy Information(정책 정보) 페이지를 표시 하려면 탐색 패널에서 **Policy Summary(**정책 요약**)**를 클릭합니다.
- 레이어 요약 페이지 표시 - 레이어 요약 페이지를 표시하려면 레이어 행에서 레이어 이름을 클릭하거나 사용자 레이어 옆에 있는 수정( )을 클릭합니다. 공유 레이어에 대한 읽기 전용 요약 페이지에 액세스하려면 보기 ( )를 클릭할 수도 있습니다.

단계 **3** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

레이어 내 침입 규칙

레이어에 대한 Rules(규칙) 페이지에서 개별 레이어 설정을 볼 수도 있고, Rules(규칙) 페이지의 정책 보기에서 모든 설정의 최종 효과를 볼 수도 있습니다. Rules(규칙) 페이지의 정책 보기에서 규칙 설정을 수정할 경우 정책에서 사용자 구성 가능한 최상위 레이어를 수정하게 됩니다. Rules(규칙) 페이지의 레이어 드롭다운 목록을 사용하여 다른 레이어로 전환할 수 있습니다.

다음 표에서는 여러 레이어에서 동일한 설정 유형을 구성하는 효과에 대해 설명합니다.

표 ***131:*** 레이어 규칙 설정

설정 수	설정 유형	목적
하나	규칙 상태	하위 레이어의 규칙에 대해 설정된 규칙 상태를 재정의하고, 하위 레이어에서 구성된 해당 규칙에 대한 모든 임계값, 억제, 등급 기반 규칙 상태 및 알림을 무시합니다. 규칙이 기반 정책 또는 하위 레이어에서 상태를 상속하도록 하려면 규칙 상태를 Inherit(상속)로 설정합니다. 침입 정책 Rules(규칙) 페이지에서 작업하는 경우, 침입 정책 Rules(규칙) 페이지는 모든 규칙 설정의 기본 효과의 중첩 보기이기 때문에 규칙 상태를 Inherit(상속)로 설정할 수 없습니다.
하나	임계값 SNMP 알림	하단 레이어의 규칙에 대해 동일한 유형의 설정을 무시합니다. 임계값을 설정하여 레이어에서 규칙에 대한 기존 임계값을 모두 덮어쓴다는 점을 참고하십시오.
하나 이상	억제등급 기반 규칙 상태	규칙 상태가 설정되어 있는 첫 번째 레이어까지 각각의 선택한 규칙에 대한 동일한 유형의 설정을 중첩적으로 결합합니다. 규칙 상태가 설정되어 있는 레이어 아래의 설정은 무시됩니다.
하나 이상	코멘트	규칙에 코멘트를 추가합니다. 코멘트는 정책이나 레이어별이 아니라 규칙별로 추가됩니다. 모든 레이어의 규칙에 하나 이상의 코멘트를 추가할 수 있습니다.

예를 들어, 규칙 상태를 한 레이어에서는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정하고 상위 레이어에서는 Disabled(비활성화)로 설정할 경우, 침입 정책 Rules(규칙) 페이지는 규칙이 비활성화되었음을 나타냅니다.

다른 예로, 한 레이어에서는 규칙에 대한 소스 기반 삭제를 192.168.1.1로 설정하고, 다른 레이어에서는 규칙에 대한 대상 기반 삭제를 192.168.1.2로 설정하는 경우, Rules(규칙) 페이지는 소스 주소 192.168.1.1 및 대상 주소 192.168.1.2에 대한 이벤트를 삭제하는 것이 중첩 효과임을 보여줍니다. 억제 및 등급 기반 규칙 상태 설정은 선택한 각 규칙에 대해 동일한 유형의 설정을 규칙에 대해 규칙 상태가 설정된 첫 번째 레이어까지 아래로 누적 결합합니다. 규칙 상태가 설정되어 있는 레이어 아래의 설정은 무시됩니다.

특정 레이어의 각 Rules(규칙) 페이지에서 색상 구분은 다음과 같이 유효 상태가 상위 레이어, 하위 레이어 또는 현재 레이어 중 어디에 있는지 나타냅니다.

- 빨간색 - 유효 상태가 상위 레이어에 있습니다
- 노란색 - 유효 상태가 하위 레이어에 있습니다
- 음영 처리되지 않음 - 유효 상태가 현재 레이어에 있습니다

침입 정책 Rules(규칙) 페이지는 모든 규칙 설정의 기본 효과에 대한 중첩 보기이므로, 규칙 상태는 이 페이지에서 색으로 지정되지 않습니다.

레이어에서 침입 규칙 구성

침입 정책에서 사용자 구성 가능한 레이어의 규칙에 대해 규칙 상태, 이벤트 필터링, 동적 상태, 알림, 규칙 코멘트를 설정할 수 있습니다. 변경하려는 레이어에 액세스한 후 침입 정책 Rules(규칙) 페이지에서 하듯 레이어에 대한 Rules(규칙) 페이지에서 설정을 추가합니다.

프로시저

단계 **1** 침입 정책을 수정할 때 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 확장합니다.

단계 **2** 수정할 정책 레이어를 확장합니다.

단계 **3** 수정할 정책 레이어 바로 아래에 있는 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 규칙을 사용하여 침입 정책 조정, 2007 페이지에서 설명하는 설정을 수정합니다.

팁 수정 가능한 레이어에서 개별 설정을 삭제하려면 레이어의 Rules(규칙) 페이지에서 규칙 메시지를 두 번 클릭하여 규칙 세부 정보를 표시합니다. 삭제할 설정 옆에 있는 **Delete**를 클릭한 다음 **OK**를 두 번 클릭합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

다중 레이어에서 규칙 설정 제거

침입 정책의 여러 레이어에서 특정 유형의 이벤트 필터, 동적 상태 또는 알림을 동시에 제거할 수 있습니다. 시스템은 선택한 설정을 제거하고 정책에서 수정 가능한 최고 레이어에 규칙에 대한 나머지 설정을 복사합니다.

시스템은 모든 설정을 제거하거나 규칙 상태가 설정되어 있는 레이어를 발견할 때까지 설정된 각 레이어를 통해 설정 유형을 아래로 제거합니다. 후자의 경우, 시스템은 해당 레이어에서 설정을 제거하고 설정 유형 제거를 중지합니다.

시스템이 기본 정책 또는 공유 레이어에서 설정 유형을 발견할 때, 그리고 정책 내 최고 레이어가 수정 가능한 경우, 시스템은 규칙에 대한 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어에 복사합니다. 또는 정책 내 최고 레이어가 공유 레이어인 경우, 시스템은 공유 레이어 위에 수정 가능한 새 레이어를 만들고 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어에 복사합니다.

참고 공유 레이어 또는 기본 정책에서 파생된 규칙 설정을 제거하면 하단 레이어 또는 기본 정책에서 이 규칙에 대한 모든 변경이 무시됩니다. 하단 레이어 또는 기본 정책에서 변경 사항 무시를 중지하려면, 최상위 레이어의 요약 페이지에서 규칙 상태를 **Inherit(**상속**)**로 설정합니다.

프로시저

단계 **1** 침입 정책을 수정하는 동안 탐색 패널에서 **Policy Information(**정책 정보**)** 바로 아래에 있는 **Rules(**규칙**)**를 클릭합니다.

팁 또한 레이어의 Rules(규칙) 페이지에 있는 레이어 드롭다운 목록에서 **Policy(**정책**)**를 선택하거나 Policy Information(정책 정보) 페이지에서 **Manage Rules(**규칙 관리**)**를 선택할 수 있습니다.

단계 **2** 여러 설정을 제거할 하나 이상의 규칙을 선택합니다.

- 특정 규칙 선택 - 특정 규칙을 선택하려면 각 규칙 옆에 있는 확인란을 선택합니다.
- 모든 규칙 선택 - 현재 목록에서 모든 규칙을 선택하려면 열 맨위의 확인란을 선택합니다.

단계 **3** 다음 옵션 중 하나를 선택합니다.

- **Event Filtering(**이벤트 필터링**)** > **Remove Thresholds(**임계값 제거**)**
- **Event Filtering(**이벤트 필터링**)** > **Remove Suppressions(**억제 제거**)**
- **Dynamic State(**동적 상태**)** > **Remove Rate-Based Rule States(**등급 기반 상태 제거**)**
- **Alerting(**알림**)** > **Remove SNMP Alerts(SNMP** 알림 제거**)**

  참고 공유 레이어 또는 기본 정책에서 파생된 규칙 설정을 제거하면 하단 레이어 또는 기본 정책에서 이 규칙에 대한 모든 변경이 무시됩니다. 하단 레이어 또는 기본 정책에서 변경 사항 무시를 중지하려면, 최상위 레이어의 요약 페이지에서 규칙 상태를 **Inherit(**상속**)**로 설정합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

사용자 지정 기본 정책에서 규칙 변경 허용하기

레이어를 추가하지 않은 사용자 지정 네트워크 분석 또는 침입 정책이 다른 사용자 지정 정책을 기본 정책으로 사용할 때, 다음과 같은 경우 해당 규칙 상태를 상속할 규칙을 설정해야 합니다.

- 기본 정책에서 규칙에 설정된 이벤트 필터, 동적 상태 또는 SNMP 알림을 삭제하는 경우 및
- 해당 규칙이 기본 정책으로 사용하는 다른 사용자 지정 정책에서 사용자가 차후에 변경하는 사항을 허용하기를 원하는 경우

프로시저

단계 **1** 침입 정책을 수정할 때 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 확장합니다.

단계 **2** **My Changes(**내 변경 사항**)**를 확장합니다.

단계 **3** **My Changes(**내 변경 사항**)** 바로 아래에 있는 **Rules(**규칙**)** 링크를 클릭합니다.

단계 **4** 설정을 수용하려는 하나 이상의 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙 선택 - 특정 규칙을 선택하려면 각 규칙 옆에 있는 확인란을 선택합니다.
- 모든 규칙 선택 - 현재 목록에서 모든 규칙을 선택하려면 열 맨위의 확인란을 선택합니다.

단계 **5** **Rule State(**규칙 상태**)** 드롭다운 목록에서 **Inherit(**상속**)**를 선택합니다.

단계 **6** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

레이어의 사전 처리기 및 고급 설정

침입 정책의 네트워크 분석 및 고급 설정에서 전처리기를 구성하기 위해 유사한 메커니즘을 사용합니다. 네트워크 분석 Settings(설정) 페이지에서 전처리기 및 침입 정책 Advanced Settings(고급 설정) 페이지에서 침입 정책 고급 설정을 활성화 및 비활성화할 수 있습니다. 이 페이지는 또한 모든 관련 기능에 대한 효과적인 상태의 개요를 제공합니다. 예를 들어, 네트워크 분석 SSL 전처리기가 한 레이어에서 비활성화되고 상위 레이어에서 활성화된 경우 Settings(설정) 페이지에서는 활성화된 것으로 보여줍니다. 이 페이지에서 변경된 사항은 정책의 상단 레이어에 나타납니다. Back Orifice 전처리기에는 사용자 구성 가능한 옵션이 없습니다.

또한 전처리기나 고급 설정을 활성화하거나 비활성화할 수 있으며, 사용자 구성 가능한 레이어에 대한 요약 페이지에서 해당 구성 페이지에 액세스할 수 있습니다. 이 페이지에서 레이어 이름 및 설명을 변경하고 동일한 유형의 다른 정책과 레이어를 공유할지 여부를 구성할 수 있습니다. 탐색 패널에서 **Policy Layers(**정책 레이어**)** 아래 레이어 이름을 선택하여 다른 레이어에 대한 요약 페이지로 전환할 수 있습니다.

전처리기 또는 고급 설정을 활성화하면 탐색 패널에서 레이어 이름 아래에 해당 기능에 대한 구성 페이지에 하위 링크가 나타나고, 레이어에 대한 요약 페이지의 기능 옆에 수정( )이 나타납니다. 이는 레이어의 기능을 비활성화하거나 Inherit(상속)로 설정하면 사라집니다.

전처리기 또는 고급 설정의 상태(활성화 또는 비활성화)를 설정하면 하단 레이어에서 해당 기능의 상태 및 구성 설정을 무시합니다. 기본 정책 또는 하단 레이어에서 전처리기 또는 고급 설정이 상태와 구성을 상속하는 것을 원하는 경우, 규칙 상태를 **Inherit(**상속**)**로 설정합니다. Settings(설정) 또는 Advanced Settings(고급 설정) 페이지에서 작업하는 경우 Inherit(상속)을 선택할 수 없다는 점에 유의하십시오. 현재 활성화된 기능을 상속하는 경우, 탐색 패널의 하위 링크와 구성 페이지의 수정 아이콘이 더 이상 표시되지 않습니다.

시스템은 기능이 활성화된 가장 높은 레이어에서 구성을 사용합니다. 명시적으로 구성을 수정하지 않은 경우, 시스템은 기본 구성을 사용합니다. 예를 들어, 한 레이어에서 네트워크 분석 DCE/RPC 전처리기를 활성화하고 수정하는 경우, 그리고 상위 레이어에서는 그것을 활성화하지만 변경하지 않는 경우, 시스템은 상위 레이어의 기본 구성을 사용합니다.

각 레이어 요약 페이지에서 색상 구분은 다음과 같이 유효 구성이 상위 레이어, 하단 레이어 또는 현재 레이어 중 어디에 있는지 나타냅니다.

- 빨간색 - 유효한 구성이 상위 레이어에 있음
- 노란색 - 유효한 구성이 하위 레이어에 있음
- 음영 처리되지 않음 - 유효 상태가 현재 레이어에 있음

Settings(설정) 및 Advanced Settings(고급 설정) 페이지는 관련된 모든 설정의 복합적인 보기이므로, 이 페이지는 효과적인 구성의 위치를 나타내는 색상 구분을 사용하지 않습니다.

레이어 내 전처리기 및 고급 설정 구성

프로시저

단계 **1** 정책을 수정할 때, 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 확장한 후 수정할 레이어 이름을 클릭합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 레이어 **Name(**이름**)**을 변경합니다.
- **Description(**설명**)**을 추가하거나 변경합니다.
- 다른 정책과 레이어를 공유할 수 있는지 지정하려면 **Sharing(**공유**)** 확인란을 선택하거나 선택 취소합니다.
- 활성화된 전처리기/고급 설정의 구성 페이지에 액세스하려면 수정( ) 또는 기능 하위 링크를 클릭합니다.
- 현재 레이어에서 전처리기/고급 설정을 비활성화하려면 기능 옆에 있는 **Disabled(**비활성화**)**를 클릭합니다.
- 현재 레이어에서 전처리기/고급 설정을 활성화하려면 기능 옆에 있는 **Enabled(**활성화**)**를 클릭합니다.
- 현재 레이어 아래 최상위 레이어의 설정에서 전처리기/고급 설정 상태 및 구성을 상속하려면 **Inherit(**상속**)**를 클릭합니다.

단계 **3** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

80 장

침입 정책 시작하기

다음 주제에서는 침입 정책을 시작하는 방법을 설명합니다.

- 침입 정책 기본 사항, 1995 페이지
- 침입 정책을 위한 라이선스 요건, 1997 페이지
- 침입 정책 요구 사항 및 사전 요건, 1997 페이지
- 침입 정책 관리, 1997 페이지
- 맞춤형 침입 정책 생성, 1998 페이지
- Snort 2 침입 정책 편집, 1999 페이지
- 침입 방지를 수행하는 액세스 제어 규칙 설정, 2001 페이지
- 인라인 구축의 삭제 작업, 2002 페이지
- 이중 시스템 구축의 삭제 작업, 2003 페이지
- 침입 정책 고급 설정, 2004 페이지
- 침입 탐지 및 방지에 대한 성능 최적화, 2005 페이지

침입 정책 기본 사항

침입 정책은 트래픽에서 보안 위반을 검사하고 인라인 구축에서 악성 트래픽을 차단 또는 변경할 수 있는 침입 탐지 및 방지 구성의 정의된 집합입니다. 침입 정책은 액세스 제어 정책에 따라 호출되며, 트래픽이 목적지에 허가되기 전 시스템의 마지막 방어선입니다.

각 침입 정책의 핵심에는 침입 규칙이 있습니다. 활성화된 규칙은 시스템이 규칙과 일치하는 트래픽의 침입 이벤트를 생성하도록 (하거나 선택적으로 차단하도록) 합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다.

Firepower System은 Cisco Talos Intelligence Group(Talos)의 경험을 활용할 수 있는 여러 기본 침입 정책을 제공합니다. Talos는 이 정책에 대해 침입 및 전처리기 규칙 상태(활성화 또는 비활성화)를 설정할 뿐 아니라 다른 고급 설정의 초기 구성을 제공합니다.

팁 시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다.

사용자 지정 침입 정책을 생성하는 경우, 다음을 수행할 수 있습니다.

- 규칙 활성화/비활성화 및 고유의 규칙 작성과 추가를 통해 탐지 기능을 조정할 수 있습니다.
- Firepower 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결합니다.
- 외부 경고, 민감한 데이터 전처리 및 전역 규칙 임계값과 같은 다양한 고급 설정을 구성합니다.
- 효율적으로 여러 침입 정책을 관리하기 위해 레이어를 구성 요소로 사용합니다.

인라인 배포에서 침입 정책은 트래픽을 차단하고 수정할 수 있습니다.

- 삭제 규칙은 일치하는 패킷을 삭제하고 침입 이벤트를 생성할 수 있습니다. 침입 또는 전처리기 삭제 규칙을 구성하려면 해당 상태를 Drop and Generate Events(이벤트 삭제 및 생성)로 설정합니다.
- 침입 규칙은 `replace` 키워드를 사용하여 악성 콘텐츠를 교체할 수 있습니다.

침입 규칙이 트래픽에 영향을 주려면 삭제 규칙 및 콘텐츠를 교체하는 규칙을 올바르게 구성해야 하며, 매니지드 디바이스를 인라인으로(즉, 인라인 인터페이스 집합으로) 올바르게 구축해야 합니다. 마지막으로, 침입 정책의 삭제 작업을 활성화하거나 **Drop when Inline(**인라인 시 삭제**)** 설정을 활성화해야 합니다.

침입 정책을 조정할 경우, 특히 규칙을 활성화하고 추가할 경우, 일부 침입 규칙에서는 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 합니다. 침입 정책이 패킷을 검토하기 전에, 패킷은 네트워크 분석 정책 내 구성에 따라 전처리됩니다. 필수 전처리기를 비활성화하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

주의 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다.

사용자 지정 침입 정책을 구성한 후, 하나 이상의 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 침입 정책을 연결함으로써 액세스 제어 구성의 일부로 사용할 수 있습니다. 이는 트래픽이 최종 목적지로 전달되기 전에 허용되는 특정 트래픽을 검토하기 위해 시스템이 침입 정책을 강제로 사용하도록 합니다. 침입 정책과 페어링된 변수 집합을 통해 홈 네트워크 및 외부 네트워크와 사용자 네트워크의 서버를 적절하게 반영할 수 있습니다.

기본적으로 시스템은 암호화된 페이로드의 침입 검사를 비활성화합니다. 이는 암호화 연결이 침입 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

침입 정책을 위한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

침입 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 정책 관리

Intrusion Policy(침입 정책) 페이지(**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**)에서 다음 정보와 함께 현재의 맞춤형 침입 정책을 볼 수 있습니다.

- 정책이 최종 수정된 시간과 날짜(로컬 시간) 및 정책을 수정한 사용자
- **Drop When Inline(**인라인 시 삭제**)** 설정의 활성화 여부. 이는 인라인 배포에서 트래픽을 삭제하고 수정할 수 있도록 합니다
- 트래픽을 검사하기 위해 침입 정책을 사용하는 액세스 제어 정책 및 디바이스의 유형
- 정책에 저장되지 않은 변경 사항이 있는지 여부 및 현재 정책을 수정하고 있는 사람에 관한 정보
- 다중 도메인 구축에서 정책이 생성된 도메인

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 침입 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교, 514 페이지를 참조하십시오.
- 생성 - **Create Policy(**정책 생성**)**를 클릭합니다(맞춤형 침입 정책 생성, 1999 페이지 참조).
- 삭제 - 삭제하려는 정책 옆에 있는 삭제( )를 클릭합니다. 다른 사용자가 정책 변경 사항을 저장하지 않은 경우, 시스템은 확인하라는 메시지를 표시하고 사용자에게 알립니다. **OK(**확인**)**를 클릭하여 확인합니다.

  컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 수정 - 편집하려는 정책 옆에 있는 수정( )을 클릭합니다. Snort 2 침입 정책 편집, 1999 페이지의 내용을 참조하십시오.

  보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 내보내기 - 다른 Firepower Management Center에서 가져올 침입 정책을 내보내려면 **YouTube EDU(**)을 클릭합니다. 컨피그레이션 내보내기, 240 페이지을 참조하십시오.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- 보고서 - 보고서( )을(를) 클릭합니다. 현재 정책 보고서 생성, 515 페이지의 내용을 참조하십시오.

맞춤형 침입 정책 생성

새로운 침입 정책을 만드는 경우, 사용자는 반드시 고유한 이름을 제공하고, 기본 정책을 지정하며, 삭제 작업을 지정해야 합니다.

기본 정책은 침입 정책의 기본 설정을 정의합니다. 새로운 정책에서 구성을 변경하면 기본 정책 설정을 대체하지만 변경하지는 않습니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다.

침입 정책의 삭제 작업 또는 **Drop When Inline(**인라인 시 삭제**)** 설정은 시스템이 삭제 규칙(규칙 상태가 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있는 침입 또는 전처리 규칙) 및 트래

픽에 영향을 미치는 다른 침입 정책 구성을 처리하는 방식을 결정합니다. 악성 패킷을 삭제하거나 교체하기를 원할 때 인라인 배포에서 삭제 작업을 활성화해야 합니다. 수동 배포에서, 시스템은 삭제 작업에 관계없이 트래픽 흐름에 영향을 줄 수 없습니다.

맞춤형 침입 정책 생성

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다. 다른 정책에 저장되지 않은 변경 사항이 있는 경우, Intrusion Policy(침입 정책) 페이지로 돌아가라는 메시지가 나타나면 **Cancel(**취소**)**을 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력하고, 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **4** 최초 **Base Policy(**기본 정책**)**를 선택합니다.

시스템 제공 정책 또는 다른 맞춤형 정책을 기본 정책으로 사용할 수 있습니다.

단계 **5** 인라인 배포에서 삭제 작업 설정하기, 2003 페이지에 설명된 대로 인라인 구축에서 시스템의 삭제 동작을 설정합니다.

단계 **6** 다음과 같이 정책을 생성합니다.

- 새 정책을 생성하고 Intrusion Policy 페이지로 돌아가려면 **Create Policy**를 클릭합니다. 새로운 정책의 설정은 기본 정책의 설정과 같습니다.
- **Create and Edit Policy(**정책 생성 및 수정**)**를 클릭하여 정책을 만들고 고급 침입 정책 편집기에서 이를 열어 수정합니다(침입 정책 변경, 2000 페이지 참고).

관련 항목

레이어 내 침입 규칙, 1988 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

Snort 2 침입 정책 편집

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택합니다.

단계 **2** 구성하려는 침입 정책 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 정책 수정:

- 기본 정책 변경 - **Base Policy(**기본 정책**)** 드롭다운 목록에서 기본 정책을 선택합니다(기반 정책 변경, 1983 페이지 참조).
- 고급 설정 구성 - 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다(침입 정책 고급 설정, 2004 페이지 참조).
- Firepower 권장 침입 규칙 구성 - 탐색 패널에서 **Firepower Recommendations(Firepower** 권장 사항**)**를 클릭합니다(Firepower 추천 생성 및 적용, 2040 페이지 참조).
- 인라인 구축의 삭제 동작 - **Drop when Inline(**인라인 시 삭제**)**을 선택하거나 선택 취소합니다(인라인 배포에서 삭제 작업 설정하기, 2003 페이지 참조).
- 권장 규칙 상태에 따라 규칙 필터링 - 권장 사항을 생성한 후 각 권장 사항 유형 옆에 있는 **View(**보기**)**를 클릭합니다. 모든 권장 사항을 보려면 **View Recommended Changes(**권장 변경 사항 보기**)**를 클릭합니다.
- 현재 규칙 상태에 따라 규칙 필터링 - 각 규칙 상태 유형(이벤트 생성, 이벤트 삭제 및 생성) 옆에 있는 **View(**보기**)**를 클릭합니다(침입 정책의 침입 규칙 필터, 2015 페이지 참조).
- 정책 레이어 관리 - 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다(레이어 관리, 1985 페이지 참조).
- 침입 규칙 관리 - **Manage Rules(**규칙 관리**)**를 클릭합니다(침입 정책의 침입 규칙 보기, 2009 페이지 참조).
- 기본 정책의 설정 보기 - **Manage Base Policy(**기본 정책 관리**)**를 클릭합니다(기본 레이어, 1981 페이지 참조).

단계 **4** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Firepower 추천 생성 및 적용, 2040 페이지
레이어에서 침입 규칙 구성, 1990 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

침입 정책 변경

새 침입 정책을 생성할 때, 기본 정책과 동일한 침입 규칙 및 고급 설정을 갖습니다.

시스템은 사용자당 하나의 침입 정책을 캐시합니다. 침입 정책을 수정하는 동안 메뉴를 선택하거나 다른 페이지로 이동하는 다른 경로를 선택하는 경우, 해당 페이지에서 나가더라도 변경 사항이 시스템 캐시에 남아 있습니다.

침입 방지를 수행하는 액세스 제어 규칙 설정

액세스 제어 정책에는 침입 정책과 관련된 여러 액세스 제어 규칙이 포함될 수 있습니다. 모든 Allow or Interactive Block(허용 또는 인터랙티브 차단) 액세스 제어 규칙에 대해 침입 검사를 구성할 수 있습니다. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크 상에 있는 다양한 유형의 트래픽에 대해 다양한 침입 검사 프로파일과 맞춰볼 수 있습니다.

시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 변수 집합을 사용합니다. 집합의 변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책 내 변수를 사용하여 규칙 삭제 및 동적 규칙 상태의 IP 주소를 나타낼 수 있습니다.

팁 시스템에서 제공한 침입 정책을 사용하더라도 Cisco는 네트워크 환경을 정확하게 반영할 수 있도록 시스템의 침입 변수를 구성할 것을 강력히 권장합니다. 최소한 기본값 집합의 기본 변수라도 수정하시기 바랍니다.

시스템이 제공하는 침입 정책 및 사용자 정의 침입 정책의 이해

Cisco는 Firepower System에서 여러 침입 정책을 제공합니다. 시스템이 제공하는 침입 정책을 사용하여 Cisco Talos Intelligence Group(Talos)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 전처리 규칙 상태를 설정할 뿐만 아니라 고급 설정의 초기 구성을 제공합니다. 사용자는 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다. 맞춤형 정책을 구축하면 사용자 환경에서 시스템의 성능을 개선할 수 있으며, 사용자 네트워크에서 발생하는 악의적인 트래픽 및 정책 위반을 집중적으로 확인할 수 있습니다.

연결 및 침입 이벤트 로깅

액세스 제어 규칙에 의해 호출된 침입 정책이 침입을 탐지하고 침입 이벤트를 생성할 경우, 해당 이벤트는 Firepower Management Center에 저장됩니다. 시스템은 또한 액세스 제어 규칙의 로깅 구성에 관계없이 침입이 발생한 연결의 종료를 Firepower Management Center 데이터베이스에 자동으로 로깅합니다.

관련 항목

사전 정의된 기본 변수, 582 페이지

액세스 제어 규칙 설정 및 침입 정책

단일한 액세스 제어 정책에서 사용할 수 있는 고유한 침입 정책의 수는 대상 디바이스의 모델에 따라 다르며, 성능이 뛰어난 디바이스일수록 더 많은 정책을 처리할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다. 다양한 침입 정책-변수 집합 쌍을 Allow(허용) 및 Interactive Block(인터랙티브 차단) 규칙(및 기본 작업)에 연결할 수 있지만 대상 디바이스에 구성된 대로 검사를 수행할 수 있는 리소스가 부족한 경우, 액세스 제어 정책을 구축할 수 없습니다.

침입 방지 수행을 위한 액세스 제어 규칙 구성

이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자 여야합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 새 규칙을 만들거나 기존 규칙을 편집합니다. 액세스 제어 규칙 구성 요소, 1648 페이지 참조.

단계 **2** 규칙 작업이 **Allow(**허용**)**, **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 초기화**)**으로 설정되어 있는지 확인합니다.

단계 **3** 클릭합니다. 선택합니다.

단계 **4** 시스템이 제공하는 정책 또는 맞춤형 **Intrusion Policy(**침입 정책**)**를 선택하거나 **None(**없음**)**을 선택하여 액세스 제어 규칙과 일치하는 트래픽에 대한 침입 검사를 비활성화합니다.

단계 **5** 침입 정책에 관련된 변수 집합을 변경하려면 **Variable Set(**변수 집합**)** 드롭다운 목록에서 값을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

변수 집합, 580 페이지
Snort® 재시작 시나리오, 505 페이지

인라인 구축의 삭제 작업

인라인 구축에서 트래픽에 실제로 영향을 주지 않고 구성이 어떻게 작동하는지(즉, 관련 구성이 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 디바이스에 구축되는지) 평가하려면 삭제 동작을 비활성화합니다. 이 경우, 시스템은 침입 이벤트를 생성하지만 삭제 규칙을 트리거하는 패킷을 삭제하지는 않습니다. 결과에 만족하는 경우, 삭제 작업을 활성화할 수 있습니다.

수동 배포에서 또는 탭 모드의 인라인 배포에서, 시스템은 삭제 작업에 관계없이 트래픽에 영향을 줄 수 없습니다. 즉 수동 배포에서 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙은 Generate Events(이벤트 생성)로 설정된 규칙과 동일하게 작동합니다. 말하자면 시스템은 침입 이벤트를 생성하지만 패킷을 삭제하지는 않습니다.

참고 FTP를 통한 악성코드의 전송을 차단하려면 AMP for Networks 를 올바르게 구성하는 것은 물론 액세스 제어 정책의 기본 침입 정책에서 **Drop when Inline(**인라인 시 삭제**)**을 활성화해야 합니다.

침입 이벤트를 볼 때, 워크플로는 인라인 결과를 포함할 수 있는데, 이는 트래픽이 실제로 삭제되었는지 여부 또는 단지 트래픽이 삭제되었을 가능성이 있는지 여부를 나타냅니다.

인라인 배포에서 삭제 작업 설정하기

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 정책의 삭제 작업을 설정합니다.

- 침입 규칙이 트래픽에 영향을 미치고 이벤트를 생성할 수 있게 하려면 **Drop When Inline(**인라인 시 삭제**)** 확인란을 선택합니다.
- 이벤트는 계속 생성하면서 침입 규칙이 트래픽에 영향을 미치지 못하도록 하려면 **Drop when Inline(**인라인 시 삭제**)** 확인란 선택을 취소합니다.

단계 **4** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

이중 시스템 구축의 삭제 작업

네트워크에 직접 연결된 두 시스템이 있는 경우, 첫 번째 시스템이 이벤트를 삭제하고 두 번째 시스템에서 삭제 또는 "would have dropped(삭제했을)" 이벤트를 기록하는 것은 정상입니다. 첫 번째 시스템은 파일의 마지막 패킷을 스캔할 때까지 패킷을 삭제하기로 결정하고, 두 번째 시스템 역시 트래픽을 검사하고 트래픽을 "to be dropped(삭제될)" 트래픽으로 식별합니다.

예를 들어 첫 번째 패킷이 규칙을 트리거하는 5패킷 HTTP GET 요청은 첫 번째 시스템에 의해 차단되고 마지막 패킷만 삭제됩니다. 두 번째 시스템은 4패킷만 수신하고 연결은 삭제되지만 두 번째 시스템은 세션을 잘라내는 동안 최종적으로 부분적 GET 요청을 플러싱할 때 인라인 결과와 동일한 "would have dropped(삭제했을)"가 있는 규칙을 트리거합니다.

침입 정책 고급 설정

침입 정책의 고급 설정을 구성하려면 특정한 전문성이 필요합니다. 침입 정책에 대한 기본 정책은 기본적으로 활성화되는 고급 설정 및 각각에 대한 기본 구성을 결정합니다.

침입 정책의 탐색 패널에 있는 **Advanced Settings(**고급 설정**)**를 선택하는 경우, 정책은 유형별 고급 설정을 나열합니다. Advanced Settings(고급 설정) 페이지에서 침입 정책의 고급 설정을 활성화하거나 비활성화할 수 있으며, 고급 설정 구성 페이지에 액세스할 수도 있습니다. 고급 설정은 구성할 수 있도록 활성화되어 있어야 합니다.

고급 설정을 비활성화하면 하위 링크 및 **Edit(**수정**)** 링크는 더 이상 표시되지 않지만, 구성은 유지됩니다. 일부 침입 정책 구성(침입 규칙에 대한 중요한 데이터 규칙, SNMP 경고)은 활성화되고 고급 설정을 정확하게 구성해야 합니다.

고급 설정에서 구성을 수정하는 데는 수정하고 있는 구성과 네트워크에 미칠 잠재적 영향에 대한 이해가 필요합니다.

특정 위협 탐지

중요한 데이터 전처리기는 신용 카드 번호 및 ASCII 문자로 표시된 Social Security numbers(사회 보장 번호)와 같은 중요한 데이터를 탐지합니다.

Back Orifice 공격, 몇몇 포트스캔 유형 및 과도한 트래픽으로 네트워크의 무력화를 시도하는 속도 기반 공격 등 특정 위협을 탐지하는 그 밖의 전처리기는 네트워크 분석 정책에서 구성됩니다.

침입 규칙 임계값

전역 규칙 임계값은 임계값을 사용하여 시스템이 로깅하고 침입 이벤트를 표시하는 횟수를 제한할 수 있도록 하여 많은 이벤트로 인해 시스템이 마비되는 것을 방지합니다.

외부 응답

웹 인터페이스 내의 다양한 침입 이벤트 보기 외에도 시스템 로그(syslog) 기능에 로깅을 활성화하거나 SNMP 트랩 서버에 이벤트 데이터를 보낼 수 있습니다. 정책별로 침입 이벤트 알림 제한을 지정하고, 외부 로깅 기능에 침입 이벤트 알림을 설정하며, 침입 이벤트에 외부 응답을 구성할 수 있습니다.

이러한 정책 단위 경고 컨피그레이션 외에도 각 규칙이나 규칙 그룹에 대해 침입 이벤트의 이메일 경고를 전역적으로 활성화 또는 비활성화할 수 있습니다. 어떤 침입 정책이 패킷을 처리하는지와 상관없이 이메일 경고 설정이 사용됩니다.

관련 항목

민감한 데이터 탐지 기본 사항, 2043 페이지
전역 규칙 임계값 기본 사항, 2057 페이지

침입 탐지 및 방지에 대한 성능 최적화

Firepower System이 침입 탐지 및 방지를 수행하도록 하되 검색 데이터를 활용할 필요가 없는 경우, 아래 설명처럼 새 검색을 비활성화하여 성능을 최적화할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 다음 사용자 역할 중 하나를 보유해야 합니다.

- 액세스 제어를 위한 관리자, 액세스 관리자 또는 네트워크 관리자
- 네트워크 검색을 위한 관리자 또는 검색 관리자

프로시저

단계 **1** 대상 디바이스에 구축된 액세스 제어 정책과 연결된 규칙을 수정하거나 삭제합니다. 해당 디바이스에 연결된 액세스 규칙에는 사용자, 애플리케이션 또는 URL 조건이 있을 수 없습니다(액세스 제어 규칙 생성 및 수정, 1651 페이지 참조).

단계 **2** 대상 디바이스의 네트워크 검색 정책에서 모든 규칙을 삭제합니다(네트워크 검색 규칙 구성, 2540 페이지 참조).

단계 **3** 변경된 구성을 대상 디바이스에 구축합니다(컨피그레이션 변경 사항 구축, 498 페이지 참조).

81 장

규칙을 사용하여 침입 정책 조정

다음 주제에서는 규칙을 사용하여 침입 정책을 조정하는 방법을 설명합니다.

- 침입 규칙 조정 기본 사항, 2007 페이지
- 침입 규칙 유형, 2008 페이지
- 침입 규칙 라이선스 요구 사항, 2009 페이지
- 침입 규칙 요구 사항 및 사전 요건, 2009 페이지
- 침입 정책의 침입 규칙 보기, 2009 페이지
- 침입 정책의 침입 규칙 필터, 2015 페이지
- 침입 규칙 상태, 2023 페이지
- 침입 정책의 침입 이벤트 알림 필터, 2025 페이지
- 동적 침입 규칙 상태, 2032 페이지
- 침입 규칙 설명 추가, 2035 페이지

침입 규칙 조정 기본 사항

침입 정책의 Rules(규칙) 페이지를 사용하여 공유 개체 규칙, 표준 텍스트 규칙, 전처리기 규칙의 규칙 상태 및 기타 설정을 구성할 수 있습니다.

규칙 상태를 Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정하여 규칙을 활성화합니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 이벤트를 생성합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다. 인라인 구축에서 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙이 일치하는 트래픽에 대해 이벤트를 생성하거나 해당 트래픽을 삭제하도록 침입 정책을 설정할 수도 있습니다. 수동 배포에서, Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙은 일치 트래픽에만 이벤트를 생성합니다.

하위 집합을 표시하도록 규칙을 필터링하면 규칙 상태 또는 규칙 설정을 변경하고자 하는 정확한 규칙 집합을 선택할 수 있습니다.

침입 규칙 또는 규칙 인수에 비활성화된 전처리기가 필요한 경우, 네트워크 분석 정책의 웹 인터페이스에서 전처리기가 비활성화 상태로 남아 있더라도 시스템은 자동으로 전처리기를 현재 구성으로 사용합니다.

침입 규칙 유형

침입 규칙은 시스템이 네트워크에서 취약점을 익스플로잇하려는 시도를 탐지하는 데 사용하는 키워드와 인수의 지정된 집합입니다. 시스템에서 네트워크 트래픽을 분석하면서 각 규칙에 지정된 조건과 패킷을 비교하고 데이터 패킷이 규칙에 지정된 모든 조건을 충족하는 경우 규칙을 트리거합니다.

침입 정책에는 다음이 포함됩니다.

- 침입 규칙(공유 개체 규칙 및 표준 텍스트 규칙으로 세분화됨)
- 패킷 디코더의 탐지 옵션 또는 Firepower 시스템에 포함된 전처리기 중 하나와 연결된 전처리기 규칙

다음 표에는 이러한 규칙 유형의 속성이 요약되어 있습니다.

표 ***132:*** 침입 규칙 유형

유형	**GID(generator ID)**	**Snort ID SID**	소스	복사 가능 여부	편집 가능 여부
공유 객체 규칙	3	1000000 미만	Cisco Talos Intelligence Group(Talos)	예	limited(제한적)
표준 텍스트 규칙	1 (전역 도메인 또는 레거시 GID)	1000000 미만	Talos	예	limited(제한적)
	1000 - 2000 (하위 도메인)	1000000 이상	사용자가 생성하거나 가져옴	예	예
전처리기 규칙	디코더 또는 전처리기별	1000000 미만	Talos	아니요	아니요
		1000000 이상	옵션 구성 중 시스템에서 생성	아니요	아니요

Talos에서 생성한 규칙의 변경 사항은 저장할 수 없지만 맞춤형 규칙으로 수정된 규칙의 복사본은 저장할 수 있습니다. 규칙 또는 규칙 헤더 정보(예: 소스 및 대상 포트와 IP 주소)에 사용되는 변수 중 하나를 수정할 수 있습니다. 다중 도메인 구축에서 Talos에 의해 생성된 규칙은 전역 도메인에 속합니다. 하위 도메인의 관리자는 규칙의 로컬 복사본을 저장한 다음 편집할 수 있습니다.

Talos은 생성하는 규칙마다 각 기본 침입 정책에서 기본 규칙 상태를 할당합니다. 대부분의 전처리기 규칙은 기본적으로 비활성화되어 있으며, 시스템에서 전처리기 규칙을 위한 이벤트를 생성하고 인라인 구축에서 문제가 되는 패킷을 삭제하도록 하려면 활성화해야 합니다.

침입 규칙 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

침입 규칙 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 정책의 침입 규칙 보기

침입 정책에서 규칙이 표시되는 방법을 조정할 수 있으며, 여러 기준으로 규칙을 정렬할 수 있습니다. 또한 규칙 설정, 규칙 문서 및 기타 규칙 사양을 보려면 특정 규칙에 대한 세부사항을 표시할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 규칙을 보면서 다음을 수행할 수 있습니다.

- 침입 정책에서 규칙 필터 설정, 2022 페이지에 설명된 대로 규칙을 필터링합니다.
- 정렬하려는 열의 상단에서 제목을 클릭하여 규칙을 정렬합니다.
- 침입 규칙 세부 사항 보기, 2011 페이지에 설명된 대로 침입 규칙의 세부 정보를 봅니다.
- **Policy(**정책**)** 드롭다운 목록에서 레이어를 선택하여 다른 정책 레이어의 규칙을 봅니다.

침입 규칙 페이지 열

침입 규칙 페이지는 메뉴 바와 열 헤더에서 동일한 아이콘을 사용합니다. 예를 들어, Rule State(규칙 상태) 메뉴는 규칙 목록의 Rule State(규칙 상태) 열과 동일한 **Generate Events(**이벤트 생성**)**를 사용합니다.

표 ***133:*** 규칙 페이지 열

제목	설명
GID	규칙의 GID(Generator ID)를 나타내는 정수.
SID	Snort ID(SID)를 나타내는 정수로, 규칙의 고유한 식별자 역할을 합니다. 맞춤형 규칙의 경우, SID는 1000000 이상입니다.
메시지	규칙 이름으로도 작동하는 이 규칙에서 생성된 이벤트에 포함된 메시지.
이벤트 생성	규칙의 규칙 상태: • 이벤트 삭제 및 생성 • 이벤트 생성 • **Disabled** 비활성화된 규칙의 아이콘은 트래픽 삭제 없이 이벤트를 생성하도록 설정된 규칙의 아이콘이 흐리게 표시된 버전입니다. 또한 규칙의 규칙 상태 아이콘을 클릭하면 규칙 상태를 변경할 수 있습니다.
Firepower 권장 규칙 상태	Firepower가 권장하는 규칙의 규칙 상태
이벤트 필터	규칙에 적용된 이벤트 임계값 및 이벤트 삭제를 포함하는 이벤트 필터.
동적 상태	특정 속도 이상이 발생한 경우 효과를 나타내는 규칙을 위한 동적 상태 규칙.
오류( )	규칙에 구성된 알림(현재는 SNMP 알림만 해당됨)
코멘트( )	규칙에 추가된 코멘트.

또한 레이어 드롭다운 목록을 사용하여 침입 정책의 다른 레이어에 대한 Rules(규칙) 페이지로 전환할 수 있습니다. 정책에 레이어를 추가하지 않는 한, 드롭다운 목록에 나열되는 수정 가능한 보기는 정책 Rules(규칙) 페이지 및 정책 레이어에 대한 Rules(규칙) 페이지(원래 이름은 `My Changes`)뿐입니다. 이 두 보기 중 하나에서 변경하는 것은 다른 보기에서 변경하는 것과 동일합니다. 드롭다운 목록에는 읽기 전용 기본 정책을 위한 Rules(규칙) 페이지도 나열됩니다.

침입 규칙 세부 사항

Rule Detail(규칙 세부 사항) 보기에서 규칙 문서, Firepower 권장 사항 및 규칙 오버헤드를 볼 수 있습니다. 또한 규칙 특정 기능을 보고 추가할 수 있습니다.

표 ***134:*** 규칙 세부사항

항목	설명
요약	규칙 요약. 규칙 기반 이벤트의 경우, 규칙 문서에 요약 정보가 포함되어 있으면 이 행이 나타납니다.
규칙 상태	해당 규칙에 대한 현재 규칙 상태. 규칙 상태가 설정된 레이어를 나타내기도 합니다.
Firepower 권장 사항	Firepower 권장 사항이 생성된 경우, 권장 규칙 상태를 나타내는 아이콘(침입 규칙 페이지 열, 2010 페이지 참조). 권장 사항이 규칙 활성화인 경우, 시스템은 권장 사항을 트리거한 네트워크 자산 또는 구성도 표시합니다.
규칙 오버헤드	시스템 성능에 대한 규칙의 잠재적 영향력 및 규칙이 오탐을 생성할 가능성. 취약성에 매핑되지 않는 한 로컬 규칙에는 할당된 오버헤드가 없습니다.
임계값	현재 이 규칙에 설정된 임계값이자 해당 규칙에 대해 임계값을 추가하는 기능
삭제	현재 이 규칙에 설정된 삭제 설정이자 해당 규칙에 대해 삭제를 추가하는 기능
동적 상태	현재 이 규칙에 설정된 등급 기반 규칙 상태 및 해당 규칙의 동적 규칙 상태를 추가하는 기능.
알림	이 규칙에 설정된 SNMP 알림 및 해당 규칙에 대한 알림을 추가하는 기능.
코멘트	이 규칙에 추가된 코멘트이자 해당 규칙에 대해 코멘트를 추가하는 기능
설명서	Cisco Talos Intelligence Group(Talos)가 제공한 현재 규칙의 규칙 문서. 원하는 경우, 더 구체적인 규칙 세부 사항을 보려면 **Rule Documentation(**규칙 문서**)**을 클릭합니다.

침입 규칙 세부 사항 보기

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 창에서 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 규칙 세부 사항을 보려는 규칙을 클릭한 다음 페이지 하단에서 **Show Details(**세부 정보 표시**)**를 클릭합니다.
침입 규칙 세부 사항, 2011 페이지에 설명된 대로 규칙 세부 사항이 표시됩니다.

단계 **5** 규칙 세부 사항에서 다음을 구성할 수 있습니다.

- 알림 - 침입 규칙에 대한 SNMP 알림 설정, 2014 페이지 참조.
- 코멘트 - 침입 규칙에 설명 추가, 2015 페이지 참조.
- 동적 규칙 상태 - 규칙 세부 사항 페이지에서 동적 규칙 상태 설정, 2013 페이지 참조.
- 임계값 - 침입 규칙에 대한 임계값 설정, 2012 페이지 참조.
- 억제 - 침입 규칙에 대한 삭제 설정, 2013 페이지 참조.

침입 규칙에 대한 임계값 설정

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 단일 임계값을 설정할 수 있습니다. 임계값을 추가하여 규칙에 대한 기존 임계값을 덮어씁니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 이를 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워 둡니다.

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Thresholds(**임계값**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Type(**유형**)** 드롭다운 목록에서 설정하려는 임계값 유형을 선택합니다.

- **Limit(**제한**)**를 선택하여 기간당 지정된 이벤트 인스턴스 수로 알림을 제한합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold(**임계값**)**를 선택합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both(**모두**)**를 선택합니다.

단계 **3** 이벤트 인스턴스를 소스 IP 주소로 추적할지 대상 IP 주소로 추적할지 나타내려면 **Track By(**추적 기준**)** 드롭다운 목록에서 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택합니다.

단계 **4** 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(**카운트**)** 필드에 입력합니다.

단계 **5** 이벤트 인스턴스를 추적할 기간(초 단위)을 지정하는 숫자를 **Seconds(**초**)** 필드에 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 이벤트 필터 개수가 표시됩니다.

침입 규칙에 대한 삭제 설정

침입 규칙에서 규칙에 하나 이상의 억제를 설정할 수 있습니다.

유효하지 않은 값을 입력하면 **Revert(**되돌리기**)**가 이 필드에 나타난다는 점에 유의하십시오. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Suppressions(**억제**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Suppression Type(**억제 유형**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 선택한 규칙에 대한 이벤트를 완전히 억제하려면 **Rule(**규칙**)**을 선택합니다.
- 지정된 소스 IP 주소에서 시작되는 패킷에 의해 생성된 이벤트를 억제하려면 **Source(**소스**)**를 선택합니다.
- 지정된 대상 IP 주소로 이동하는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination(**대상**)**을 선택합니다.

단계 **3** 억제 유형으로 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택한 경우, **Network(**네트워크**)** 필드에 IP 주소, 주소 블록 또는 이러한 항목의 조합으로 구성된 쉼표로 구분된 목록을 입력합니다.

침입 정책이 액세스 제어 정책의 기본 작업과 연결된 경우 기본 작업 변수 집합의 네트워크 변수를 지정하거나 나열할 수도 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

팁 시스템은 억제된 규칙 옆의 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 필터 위의 숫자는 이벤트 필터의 수를 나타냅니다.

규칙 세부 사항 페이지에서 동적 규칙 상태 설정

규칙에 하나 이상의 동적 규칙 상태를 설정할 수 있습니다. 나열된 첫 번째 동적 규칙 상태의 우선 순위가 가장 높습니다. 2개의 동적 규칙 상태가 충돌하면 첫 번째 상태의 작업이 수행됩니다.

동적 규칙 상태는 정책에 따라 다릅니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 이를 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워 둡니다.

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Dynamic State(**동적 상태**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Track By(**추적 기준**)** 드롭다운 목록에서 옵션을 선택해 규칙 일치를 추적할 방법을 나타냅니다.

- 특정 소스 또는 소스 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Source(**소스**)**를 선택합니다.
- 특정 대상 또는 대상 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Destination(**대상**)**을 선택합니다.
- 해당 규칙의 모든 일치를 추적하려면 **Rule(**규칙**)**을 선택합니다.

단계 **3** **Track By(**추적 기준**)**를 **Source(**소스**)** 또는 **Destination(**대상**)**으로 설정하는 경우, **Network (**네트워크**)** 필드에 추적하려는 각 호스트의 IP 주소를 입력합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 공격 속도를 설정하려면 **Rate(**속도**)** 옆에 기간당 규칙 일치 수를 지정합니다.

- 임계값으로 사용할 규칙 일치의 수를 **Count(**카운트**)** 필드에서 지정합니다.
- **Seconds(**초**)** 필드에서 공격을 추적할 기간을 구성하는 시간(초)을 지정합니다.

단계 **5** **New State(**새로운 상태**)** 드롭다운 목록에서 조건이 충족되면 취할 새로운 작업을 선택합니다.

단계 **6** **Timeout(**시간 제한**)** 필드에 값을 입력합니다.

시간 제한이 발생한 후, 규칙은 원래 상태로 돌아갑니다. 새로운 작업이 시간 초과되는 것을 방지하려면 `0`을 입력합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Dynamic State(동적 상태) 열의 규칙 옆에 동적 상태( )를 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가한 경우, 필터 위의 숫자는 필터 수를 나타냅니다.

침입 규칙에 대한 **SNMP** 알림 설정

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 SNMP 알림을 설정할 수 있습니다.

프로시저

침입 규칙의 세부 사항에서 **Alerts(**알림**)** 옆에 있는 **Add SNMP Alert(SNMP** 알림추가**)**를 클릭합니다.

팁 시스템은 Alerting(알림) 열의 규칙 옆에 알림 아이콘(오류( ))을 표시합니다. 규칙에 여러 알림을 추가하는 경우 알림 개수가 표시됩니다.

침입 규칙에 설명 추가

프로시저

단계 **1** 침입 규칙의 세부 사항에서 **Comments(**코멘트**)** 옆에 있는 **Add(**추가**)**를 클릭합니다.

단계 **2** **Comments(**코멘트**)** 필드에 규칙 코멘트를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Comments(코멘트) 열의 규칙 옆에 코멘트( )를 표시합니다. 규칙에 여러 코멘트를 추가하는 경우, 코멘트 위의 숫자는 코멘트 수를 나타냅니다.

단계 **4** 규칙 코멘트를 삭제하려면 규칙 코멘트 섹션에서 **Delete(**삭제**)**를 클릭합니다. 커밋되지 않은 침입 정책 변경 사항과 함께 코멘트가 캐시된 경우에만 코멘트를 삭제할 수 있습니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

침입 정책의 침입 규칙 필터

Rules(규칙) 페이지에 표시된 규칙을 단일 기준 또는 여러 기준의 조합으로 필터링할 수 있습니다.

규칙 필터 키워드를 사용하면 규칙 설정(예: 규칙 상태 또는 이벤트 필터)을 적용할 규칙을 쉽게 찾을 수 있습니다. 키워드로 필터링하고 동시에 Rules(규칙) 페이지 필터 패널에서 원하는 인수를 선택하여 키워드에 대한 인수를 선택할 수 있습니다.

침입 규칙 필터 참고 사항

구성한 필터가 Filter(필터) 텍스트 상자에 표시됩니다. 필터 패널에서 키워드 및 키워드 인수를 클릭하여 필터를 구성할 수 있습니다. 여러 키워드를 선택하면 시스템에서 AND 논리로 키워드를 통합하여 복합 검색 필터를 생성합니다. 예를 들어 **Category(**카테고리**)** 아래에서 **preprocessor(**전처리기**)**를 선택한 다음 **Rule Content(**규칙 콘텐츠**)** > **GID**를 선택하고 `116`을 입력하면 `Category: “preprocessor” GID:”116”` 필터가 생성됩니다. 이 필터는 전처리기 규칙이고 GID가 116인 규칙을 모두 검색합니다.

Category(카테고리), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Platform Specific(플랫폼 특징), Preprocessor(전처리기) 및 Priority(우선 순위) 필터 그룹을 통해 키워드를 위한 1개 이상의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어 **Category(**카테고리**)**에서 **os-linux** 및 **os-windows**를 선택하면 `Category:"os-windows,os-linux"` 필터를 생성할 수 있습니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리에 속하는 모든 규칙을 검색합니다.

필터 패널을 표시하려면 표시 아이콘을 클릭합니다.

필터 패널을 숨기려면, 숨기기 아이콘을 클릭합니다.

침입 정책 규칙 필터 구성 가이드라인

대부분의 경우, 필터를 작성할 때 침입 정책의 Rules(규칙) 페이지 왼쪽에 있는 필터 패널을 사용하여 원하는 키워드/인수를 선택할 수 있습니다.

Rule(규칙) 필터는 필터 패널의 규칙 필터 그룹으로 그룹화됩니다. 많은 규칙 필터 그룹에 하위 기준이 포함되어 있어서 원하는 특정 규칙을 손쉽게 찾을 수 있습니다. 일부 규칙 필터에는 개별 규칙으로 드릴다운하기 위해 확장할 수 있는 여러 레벨이 있습니다.

필터 패널의 항목은 때로는 필터 유형 그룹, 때로는 키워드, 그리고 때로는 키워드에 대한 인수를 나타냅니다. 다음에 유의하십시오.

- 키워드(Rule Configuration(규칙 구성), Rule Content(규칙 콘텐츠), Platform Specific(플랫폼별) 및 Priority(우선순위)가 아닌 필터 유형 그룹 제목을 선택하면 확장되어 사용 가능한 키워드가 나열됩니다.

  기준 목록의 노드를 클릭하여 키워드를 선택하면 팝업 창이 나타나는데, 여기에서 필터링할 인수를 제공합니다.

  해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

  예를 들어 필터 패널에서 **Rule Configuration(**규칙 구성**)** > **Recommendation(**권장 사항**)** 아래에 있는 **Drop and Generate Events(**이벤트 삭제 및 생성**)**를 클릭하는 경우, 필터 텍스트 상자에 `Recommendation: "Drop and Generate Events"`가 추가됩니다. 그런 다음 **Rule Configuration(**규칙 구성**)** > **Recommendation(**권장 사항**)** 아래에 있는 **Generate Events(**이벤트 생성**)**를 클릭하는 경우, 필터가 `Recommendation:"Generate Events"`로 변경됩니다.

- 키워드(Category(카테고리), Classifications(분류), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Priority(우선 순위) 및 Rule Update(규칙 업데이트))인 필터 유형 그룹 제목을 선택하면 사용 가능한 인수가 나열됩니다.

  이 그룹 유형에서 항목을 선택하면 항목이 적용하는 인수와 키워드가 필터에 즉시 추가됩니다. 키워드가 필터에 이미 있는 경우, 그룹에 해당하는 키워드에 대한 기존 인수를 교체합니다.

  예를 들어 필터 패널에서 **Category(**카테고리**)** 아래의 **os Linux**를 클릭할 경우, 필터 텍스트 상자에 `Categoy:"os-linux"`가 추가됩니다. 그런 다음 **Category(**카테고리**)** 아래에서 **os-windows**를 클릭하면 필터가 `Category:"os-windows"`로 변경됩니다.

- Rule Content(규칙 콘텐츠) 아래의 참조는 키워드이며, 그 아래에 나열된 참조 ID 유형도 마찬가지입니다. 참조 키워드를 선택하면 팝업 창이 나타납니다. 여기서 인수를 제공하면 기존 필터에 키워드가 추가됩니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우, 새로 제공하는 인수가 기존 인수를 교체합니다.

  예를 들어, 필터 패널에서 **Rule Content(**규칙 내용**)** > **Reference(**참조**)** > **CVE ID**를 클릭하면 팝업 창에 CVE ID를 입력하라는 메시지가 표시됩니다. `2007`을 입력한 경우, 다음 `CVE: “2007”`이 필터 텍스트 상자에 추가됩니다. 예를 들어 필터 패널에서 **Rule Content(**규칙 내용**)** > **Reference(**참조**)**를 클릭하면 팝업 창에 참조를 입력하라는 메시지가 표시됩니다. `2007`을 입력한 경우, `Reference:”2007”`이 필터 텍스트 상자에 추가됩니다.

- 서로 다른 그룹에서 규칙 필터 키워드를 선택하면 각 필터 키워드가 필터에 추가되며 기존 키워드는 유지됩니다(동일한 키워드의 새 값으로 덮어쓰지 않는 한).

  예를 들어 필터 패널에서 **Category(**카테고리**)** 아래의 **os Linux**를 클릭할 경우, 필터 텍스트 상자에 `Categoy:"os-linux"`가 추가됩니다. **Microsoft Vulnerabilities(Microsoft** 취약성**)** 아래의 **MS00-006**을 클릭할 경우, 필터는 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`으로 변경됩니다.

- 여러 키워드를 선택하면 시스템에서 AND 논리로 키워드를 통합하여 복합 검색 필터를 생성합니다. 예를 들어 **Category(**카테고리**)** 아래에서 **preprocessor(**전처리기**)**를 선택한 다음 **Rule Content(**규칙 콘텐츠**)** > **GID**를 선택하고 `116`을 입력하면 `Category: “preprocessor” GID:”116”` 필터가 생성됩니다. 이 필터는 전처리기 규칙이고 GID가 116인 규칙을 모두 검색합니다.

- Category(카테고리), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Platform Specific(플랫폼 특징) 및 Priority(우선 순위) 필터 그룹을 통해 키워드를 위한 하나 이상의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어 **Category(**카테고리**)**에서 **os-linux** 및 **os-windows**를 선택하면 `Category:"os-windows,app-detect"` 필터를 생성할 수 있습니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리에 속하는 모든 규칙을 검색합니다.

둘 이상의 필터 키워드/인수 쌍으로 동일한 규칙을 검색할 수 있습니다. 예를 들어, 규칙이 **dos** 카테고리에서 필터링될 경우, 그리고 **High(**높은**)** 우선 순위로 필터링할 경우 DOS Cisco 시도 규칙(SID 1545)이 나타납니다.

참고 Cisco Talos Intelligence Group(Talos)는 규칙 업데이트 메커니즘을 사용하여 규칙 필터를 추가 및 제거할 수 있습니다.

Rules(규칙) 페이지에 있는 규칙은 공유 개체 규칙(generator ID 3) 또는 표준 텍스트 규칙(generator ID 1, Global domain or legacy GID; 1000 - 2000, descendant domains)일 수 있습니다. 다음 표는 다양한 규칙 필터에 대해 설명합니다.

표 ***135:*** 규칙 필터 그룹

필터 그룹	설명	다중 인수 지원 여부	제목	목록 내 항목
규칙 컨피그레이션	규칙의 구성에 따라 규칙을 찾습니다.	아니요	그룹화	키워드
규칙 콘텐츠	규칙의 내용에 따라 규칙을 찾습니다.	아니요	그룹화	키워드
카테고리	규칙 편집기에 사용되는 규칙 카테고리에 따라 규칙을 찾습니다. 로컬 규칙은 로컬 하위 그룹에 나타납니다.	예	키워드	인수

필터 그룹	설명	다중 인수 지원 여부	제목	목록 내 항목
분류	규칙에 의해 생성된 이벤트의 패킷 표시에 나타나는 공격 분류에 따라 규칙을 찾습니다.	아니요	키워드	인수
Microsoft 취약성	Microsoft 게시판 번호에 따라 규칙을 찾습니다.	예	키워드	인수
Microsoft 웜	Microsoft Windows 호스트에 영향을 미치는 특정 웜에 따라 규칙을 찾습니다.	예	키워드	인수
플랫폼별	특정 운영 체제 버전에 대한 연관성에 따라 규칙을 찾습니다. 규칙 하나가 둘 이상의 운영 체제 또는 둘 이상의 운영 체제 버전에 영향을 미칠 수 있습니다. 예를 들어, SID 2260을 활성화하면 Mac OS X, IBM AIX 및 기타 운영 체제의 모든 버전에 영향을 줍니다.	예	키워드	인수 하위 목록의 항목 중 하나를 선택한 경우, 인수에 수정자가 추가됩니다.
전처리기	개별 전처리기에 대한 규칙을 찾습니다. 전처리기가 활성화되었을 때 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 전처리기 옵션에 연결된 전처리기 규칙을 활성화해야 합니다.	예	그룹화	하위 그룹화

필터 그룹	설명	다중 인수 지원 여부	제목	목록 내 항목
우선순위	높음, 중간, 낮음 우선순위에 따라 규칙을 찾습니다. 규칙에 할당된 분류가 우선순위를 결정합니다. 이 그룹은 규칙 카테고리로 심화 그룹화됩니다. 로컬 규칙(즉, 사용자가 가져오거나 생성하는 규칙)은 우선순위 그룹에 나타나지 않습니다.	예	키워드	인수 하위 목록의 항목 중 하나를 선택한 경우, 인수에 수정자가 추가됩니다.
규칙 업데이트	특정 규칙 업데이트를 통해 추가 또는 수정된 규칙을 찾습니다. 각 규칙 업데이트에 대해 모든 규칙을 보거나, 가져온 규칙만 보거나, 업데이트에 의해 변경된 기존 규칙만 볼 수 있습니다.	아니요	키워드	인수

침입 규칙 설정 필터

Rules(규칙) 페이지에 나열되는 규칙을 여러 규칙 컨피그레이션 설정으로 필터링할 수 있습니다. 예를 들어 규칙 상태가 권장 규칙 상태에 일치하지 않는 규칙 집합을 보려는 경우, **Does not match recommendation(**권장 규칙 상태에 일치하지 않음**)**을 선택하여 규칙 상태를 필터링할 수 있습니다.

기준 목록의 노드를 클릭하여 키워드를 선택하면 필터링할 인수를 입력할 수 있습니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

예를 들어 필터 패널에서 **Rule Configuration(**규칙 구성**) > Recommendation(**권장 사항**)** 아래에 있는 **Drop and Generate Events(**이벤트 삭제 및 생성**)**를 클릭하는 경우, 필터 텍스트 상자에 `Recommendation: "Drop and Generate Events"`가 추가됩니다. 그런 다음 **Rule Configuration(**규칙 구성**) > Recommendation(**권장 사항**)** 아래에 있는 **Generate Events(**이벤트 생성**)**를 클릭하는 경우, 필터가 `Recommendation:"Generate Events"`로 변경됩니다.

침입 규칙 콘텐츠 필터

Rules(규칙) 페이지에 나열되는 규칙을 여러 규칙 콘텐츠 항목별로 필터링할 수 있습니다. 예를 들어, 규칙의 SID를 검색하여 규칙을 빠르게 검색할 수 있습니다. 또한 특정 목적지 포트로 가는 트래픽을 검사하는 모든 규칙을 찾을 수 있습니다.

기준 목록의 노드를 클릭하여 키워드를 선택하면 필터링할 인수를 입력할 수 있습니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

예를 들어 필터 패널의 **Rule Content(**규칙 콘텐츠**)**에서 **SID**를 클릭하면 SID를 입력하라는 팝업 창이 나타납니다. `1045`를 입력하면 `SID:"1045"`가 필터 텍스트 상자에 추가됩니다. 그런 다음 **SID**를 다시 클릭하여 SID 필터를 `1044`로 변경하면 필터가 `SID:"1044"`로 바뀝니다.

표 ***136:*** 규칙 콘텐츠 필터

이 필터는**...**	다음과 같은 규칙을 찾습니다**.**
Message	메시지 필드에 제공된 문자열을 포함합니다.
SID	지정된 SID가 있습니다.
GID	지정된 GID가 있습니다.
참조	참조 필드에 제공된 문자열을 포함합니다. 특정 참조 유형과 제공된 문자열을 기준으로 필터링할 수도 있습니다.
조치	`Alerts(알림)` 또는 `pass(통과)`로 시작합니다.
프로토콜	선택한 프로토콜을 포함합니다.
Direction(방향)	표시된 방향 설정이 규칙에 포함되어 있는지 여부에 기반합니다.
Source IP(소스 IP)	규칙에서 소스 IP 주소 지정에 특정 주소나 변수를 사용합니다. 유효한 IP 주소, CIDR 블록/접두사 길이로 필터링하거나 `$HOME_NET` 또는 `$EXTERNAL_NET` 같은 변수를 사용하여 필터링할 수 있습니다.
Destination IP(목적지 IP)	규칙에서 소스 IP 주소 지정에 특정 주소나 변수를 사용합니다. 유효한 IP 주소, CIDR 블록/접두사 길이로 필터링하거나 `$HOME_NET` 또는 `$EXTERNAL_NET` 같은 변수를 사용하여 필터링할 수 있습니다.
소스 포트	지정된 소스 포트를 포함합니다. 포트 값은 1과 65535 사이의 정수이거나 포트 변수여야 합니다.
대상 포트	지정된 대상 포트를 포함합니다. 포트 값은 1과 65535 사이의 정수이거나 포트 변수여야 합니다.
규칙 오버헤드	선택한 규칙 오버 헤드가 있습니다.
메타데이터	일치하는 키 값 쌍을 포함하는 메타데이터가 있습니다. 예를 들어, HTTP 애플리케이션 프로토콜과 관련된 메타데이터로 규칙을 찾으려면 `metadata:"service http"`를 입력합니다.

침입 규칙 카테고리

Firepower System은 규칙이 탐지하는 트래픽 유형에 따라 카테고리에 규칙을 배치합니다. Rules(규칙) 페이지에서 규칙 카테고리로 필터링하여, 한 카테고리의 모든 규칙에 대해 규칙 속성을 설정할 수 있습니다. 예를 들어 네트워크에 Linux 호스트가 없는 경우, **os-linux** 카테고리로 필터링한 다음 표시되는 모든 규칙을 비활성화하여 전체 **os-linux** 카테고리를 비활성화할 수 있습니다.

마우스 포인터를 카테고리 이름 위로 이동하면 해당 카테고리의 규칙 수가 표시됩니다.

참고 Cisco Talos Intelligence Group(Talos)는 규칙 업데이트 메커니즘을 사용하여 카테고리를 추가 및 제거할 수 있습니다.

침입 규칙 필터 구성 요소

필터 패널에서 필터를 클릭할 때 제공되는 특수 키워드 및 해당 인수를 변경하려면 필터를 수정할 수 있습니다. Rules(규칙) 페이지의 사용자 지정 필터 규칙은 규칙 편집기에서 사용되는 것처럼 기능하지만 필터 패널을 통해 필터를 선택할 때 표시되는 구문을 사용하여 Rules(규칙) 페이지 필터에 제공된 모든 키워드를 사용할 수 있습니다. 나중에 사용할 키워드를 결정하려면 필터 패널 오른쪽에서 적절한 인수를 클릭합니다. 필터 텍스트 상자에 필터 키워드와 인수 구문이 나타납니다. 키워드에 대한 쉼표로 구분된 여러 인수는 Category(카테고리) 및 Priority(우선 순위) 필터 유형에만 지원된다는 점을 기억하십시오.

키워드와 인수, 문자 문자열, 따옴표의 리터럴 문자 문자열을 사용할 수 있으며 여러 필터 조건을 공백으로 구분할 수 있습니다. 필터에는 정규 표현식, 와일드카드 문자 또는 부정 문자(!), 보다 큼 기호(>), 보다 작음 기호(<)와 같은 특별 연산자를 포함할 수 없습니다. 키워드 없이, 키워드의 첫 글자 대문자 없이 또는 인수 앞뒤의 따옴표 없이 검색할 용어를 입력하면 검색은 문자열 검색으로 처리되며, 지정된 용어가 카테고리, 메시지 및 SID 필드에서 검색됩니다.

`gid` 및 `sid` 키워드를 제외한, 모든 인수 및 문자열은 부분 문자열로 처리됩니다. `gid` 및 `sid`의 인수는 정확히 일치하는 것만 반환합니다.

각 규칙 필터의 형식에는 하나 이상의 키워드를 포함할 수 있습니다.

keyword:"*argument*"

키워드가 침입 규칙 필터 그룹의 키워드 중 하나이고 인수가 큰 따옴표로 둘러싸여 있으며 특정 필드 또는 키워드 관련 필드에서 검색할 단일 대소문자 구분 영숫자 문자열인 경우입니다. 키워드의 첫 글자는 대문자로 입력해야 합니다.

`gid` 및 `sid`를 제외한 모든 키워드에 대한 인수는 부분 문자열로 처리됩니다. 예를 들어, 인수 `123`은 `"12345"`, `"41235"`, `"45123"` 등을 반환합니다. `gid` 및 `sid`의 인수는 정확하게 일치하는 경우에만 반환됩니다. 예를 들어, `sid:3080`은 `SID 3080`만 반환합니다.

각 규칙 필터는 또한 하나 이상의 영숫자 문자 문자열을 포함할 수 있습니다. 문자열은 규칙 Message(메시지) 필드, Snort ID(SID) 및 생성자 ID(GID)를 검색합니다. 예를 들어, 문자열 `123`은 규칙 메시지에서 문자열 `"Lotus123"`, `"123mania"` 등을 반환하며, 또한 `SID 6123`, `SID 12375` 등을 반환합니다. 하나 이상의 문자열로 필터링하여 부분 SID를 검색할 수 있습니다.

모든 문자열은 대소문자를 구분하지 않으며 부분 문자열로 처리됩니다. 예를 들어, 문자열 `ADMIN`, `admin` 또는 `Admin`은 모두 `"admin"`, `"CFADMIN"`, `"Administrator"` 등을 반환합니다.

정확히 일치하는 항목을 반환하기 위해 인용구에서 문자열을 묶을 수 있습니다. 예를 들어, 인용구 내 문자열 `"overflow attempt"`는 정확한 문자열만 반환하지만, 인용구가 없는 두 개의 문자열 `overflow` 및 `attempt`로 구성된 필터는 `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"` 등을 반환합니다.

키워드, 문자열 또는 둘 다로 이루어진 스페이스로 구분된 문자열의 조합을 입력하여 필터링 결과를 좁힐 수 있습니다. 결과는 필터링 조건과 일치하는 모든 규칙을 포함합니다.

순서에 상관없이 여러 필터 상태를 입력할 수 있습니다. 예를 들어, 다음 필터 각각은 동일한 규칙을 반환합니다.

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

침입 규칙 필터 사용

침입 정책의 Rules(규칙) 페이지 왼쪽에 있는 필터 패널에서 사전 정의된 필터 키워드를 선택할 수 있습니다. 필터를 선택하면 페이지에 모든 일치하는 규칙이 표시되거나 일치하는 규칙이 없음이 표시됩니다.

추가로 제한하려면 필터에 키워드를 추가할 수 있습니다. 입력한 모든 필터는 전체 규칙 데이터베이스를 검색하고 일치하는 규칙을 모두 반환합니다. 페이지가 계속 이전 검색 결과를 표시하고 있는데 필터를 입력하는 경우, 페이지는 이를 지우고 새 필터의 결과로 돌아갑니다.

필터를 선택할 때 제공된 동일한 키워드 및 인수 구문을 사용하여 필터를 입력할 수도 있고, 선택한 후 필터에서 인수 값을 수정할 수도 있습니다. 키워드 없이, 키워드의 첫 글자 대문자 없이 또는 인수 앞뒤의 따옴표 없이 검색할 용어를 입력하면 검색은 문자열 검색으로 처리되며, 지정된 용어가 카테고리, 메시지 및 SID 필드에서 검색됩니다.

침입 정책에서 규칙 필터 설정

규칙의 하위 집합을 표시하려면 Rule(규칙) 페이지에서 규칙을 필터링할 수 있습니다. 그런 다음 컨텍스트 메뉴에서 사용 가능한 기능 선택을 포함하여 원하는 페이지 기능을 사용할 수 있습니다. 이 기능은 예를 들어 특정 카테고리의 모든 규칙에 대해 임계값을 설정하고자 할 때 유용할 수 있습니다. 필터링된 목록이나 필터링되지 않은 목록의 규칙과 같은 기능을 사용할 수 있습니다. 예를 들어 필터링된 목록 또는 필터링되지 않은 목록에서 규칙에 새 규칙 상태를 적용할 수 있습니다.

모든 키워드, 키워드 인수 및 문자열은 대소문자를 구분하지 않습니다. 필터에 이미 있는 키워드에 대한 인수를 클릭하면 기존 인수가 교체됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** **Rules(**규칙**)**를 클릭합니다.

단계 **4** 다음 방법을 개별적으로 사용하거나 조합하여 필터를 구성합니다.

- **Filter(**필터**)** 텍스트 상자에 값을 입력하고 Enter를 누릅니다.
- 미리 정의된 키워드를 확장합니다. 예를 들어 **Rule Configuration(**규칙 구성**)**을 클릭합니다.
- 키워드를 클릭하고 메시지가 표시되면 인수 값을 지정합니다. 예를 들면 다음과 같습니다.
  - **Rule Configuration(**규칙 구성**)** 아래에서 **Rule State(**규칙 상태**)**를 클릭하고 드롭다운 목록에서 `Generate Events(이벤트 생성)`를 클릭한 다음 **OK(**확인**)**를 클릭합니다.
  - **Rule Configuration(**규칙 구성**)** 아래에서 **Comment(**코멘트**)**를 클릭하고 필터링할 코멘트 텍스트 문자열을 입력한 다음 **OK(**확인**)**를 클릭할 수 있습니다.
  - **Category(**카테고리**)**에서 시스템이 인수 값으로 사용하는 **app-detect**를 클릭할 수 있습니다.
- 키워드를 확장하고 인수 값을 클릭합니다. 예를 들어 **Rule State(**규칙 상태**)**를 확장하고 **Generate Events(**이벤트 생성**)**를 클릭합니다.

침입 규칙 상태

침입 규칙 상태를 통해 개별 침입 정책 내에서 규칙을 활성화하거나 비활성화할 수 있을 뿐 아니라 모니터링된 조건이 규칙을 트리거하는 경우, 시스템이 수행하는 작업을 지정할 수도 있습니다.

Cisco Talos Intelligence Group(Talos)는 각 기본 정책에서 각 침입 및 전처리기 규칙의 기본 상태를 설정합니다. 예를 들어 규칙은 Security Over Connectivity(연결성보다 보안 우선) 기본 정책에서 활성화되고 Connectivity Over Security(보안보다 연결성 우선) 기본 정책에서 비활성화될 수 있습니다. Talos는 경우에 따라 규칙 업데이트를 사용하여 기본 정책에서 하나 이상의 규칙 상태를 변경할 수 있습니다. 규칙 업데이트가 기반 정책을 업데이트하도록 허용하면, 정책을 생성하기 위해 사용한 기본 정책(또는 기반으로 하는 기본 정책)에서 기본 상태가 변경될 때 정책에 있는 규칙의 기본 상태를 변경하는 것도 허용됩니다. 그러나 규칙 상태를 변경한 경우 규칙 업데이트가 변경 사항을 재정의하지 않습니다.

침입 규칙을 생성하면 침입 정책은 정책 생성에 사용되는 기본 정책에 있는 규칙의 기본 상태를 상속합니다.

침입 규칙 상태 옵션

침입 정책에서 규칙의 상태를 다음 값으로 설정할 수 있습니다.

이벤트 생성

시스템이 일치하는 트래픽을 찾으면 특정 침입 시도를 탐지하고 침입 이벤트를 생성하도록 하려는 경우에 설정합니다. 악의적인 패킷이 네트워크를 이동하여 규칙을 트리거하면 규칙이 목적지로 전송되고 시스템이 침입 이벤트를 생성합니다. 악의적인 패킷이 대상에 도달하지만 이벤트 로깅을 통해 알림이 전송됩니다.

이벤트 삭제 및 생성

시스템이 일치하는 트래픽을 찾으면 특정 침입 이벤트를 탐지하고, 공격을 포함하는 패킷을 삭제하고, 침입 이벤트를 생성하도록 하려는 경우에 설정합니다. 악성 패킷은 대상에 도달하지 못하며 이벤트 로깅을 통해 알림이 전송됩니다.

7000 또는 8000 Series 디바이스 인라인 인터페이스 집합이 탭 모드인 구축을 포함한 패시브 구축에서 이 규칙 상태로 설정된 규칙 집합은 이벤트를 생성하지만 패킷을 삭제하지는 않습니다. 시스템에서 패킷을 삭제하려면 침입 정책에서 **Drop when Inline(**인라인 시 삭제**)**를 활성화(기본 설정)하고 디바이스 인라인으로 구축해야 합니다.

Disable

시스템이 일치하는 트래픽을 평가하지 않도록 하려면 설정합니다.

참고 **Generate Events(**이벤트 생성**)** 또는 **Drop and Generate Events(**이벤트 삭제 및 생성**)** 옵션을 선택하면 규칙이 활성화됩니다. **Disable(**비활성화**)**를 선택하면 규칙이 비활성화됩니다.

Cisco는 침입 정책 내 침입 규칙을 모두 활성화하지 않을 것을 강력히 권장합니다. 모든 규칙이 활성화될 경우 관리되는 디바이스의 성능이 저하될 수 있습니다. 대신 네트워크 환경과 가능한 한 일치하도록 규칙 설정을 조정하십시오.

침입 규칙 상태 설정

침입 규칙 상태는 정책별로 다릅니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

팁 이 페이지에는 활성화된 총 규칙 수, Generate Events(이벤트 생성)로 설정된 활성화된 총 규칙 수, Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 총 수가 표시됩니다. 또한 수동 배포에서는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙만 이벤트를 생성한다는 점에 유의하십시오.

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 규칙 상태를 설정할 규칙을 선택합니다.

단계 **5** 다음 중 하나를 선택합니다.

- **Rule State(**규칙 상태**)** > **Generate Events(**이벤트 생성**)**
- **Rule State(**규칙 상태**)** > **Drop and Generate Events(**이벤트 삭제 및 생성**)**
- **Rule State(**규칙 상태**)** > **Disable(**비활성화**)**

단계 **6** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

침입 정책의 침입 이벤트 알림 필터

침입 이벤트의 중요성은 발생 빈도 또는 소스/대상 IP 주소를 기준으로 결정될 수 있습니다. 어떤 경우에는 특정 횟수가 발생할 때까지 이벤트에 대해 신경 쓰지 않아도 됩니다. 예를 들어, 어떤 사용자가 서버에 로그인을 시도하는 경우 특정 횟수만큼 실패할 때까지는 염려하지 않아도 됩니다. 다른 경우에는 소수의 발생 상황만 확인해도 광범위한 문제의 존재 여부를 파악할 수 있습니다. 예를 들어 웹 서버에 대해 DoS 공격이 시작된 경우, 상황을 해결해야 하는지를 파악하려면 침입 이벤트의 발생 상황을 몇 번만 확인해보면 됩니다. 동일한 이벤트를 수백 번 확인하면 시스템에 부담을 줄 뿐입니다.

침입 이벤트 임계값

지정된 기간 내 이벤트 생성 횟수를 기반으로 시스템이 침입 이벤트를 로깅 및 표시하는 횟수를 제한하도록 침입 정책당 개별 규칙에 대한 임계값을 설정할 수 있습니다. 이를 통해 많은 수의 동일한 이벤트로 인해 마비되는 것을 방지할 수 있습니다. 공유 개체 규칙, 표준 텍스트 규칙 또는 전처리기 규칙별 임계값을 설정할 수 있습니다.

침입 이벤트 임계값 설정

임계값을 설정하려면 먼저 임계값 설정 유형을 지정합니다.

표 ***137:*** 임계값 설정 옵션

옵션	설명
Limit(제한)	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(count 인수로 지정)에 대한 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Limit(**제한**)**로, **Count(**카운트**)**는 10으로, 그리고 **Seconds(**초**)**는 60으로 설정하고 14개의 패킷이 규칙을 트리거하는 경우, 시스템은 동일한 시간(분) 내 발생한 첫 10개의 패킷을 표시한 후 규칙의 이벤트 로깅을 중단합니다.
Threshold(임계값)	지정된 기간 중 지정된 패킷 수(count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅하고 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅하면 시간에 대한 카운터가 다시 시작됩니다. 예를 들어, 유형은 **Threshold(**임계값**)**로, **Count(**카운트**)**는 10으로, 그리고 **Seconds(**초**)**는 60으로 설정하면 규칙은 33초에 10번 트리거됩니다. 시스템은 하나의 이벤트를 생성한 다음, Seconds(초) Count(카운트) 카운터를 0으로 재설정합니다. 그런 다음 규칙은 다음 25초 안에 다시 10번 트리거됩니다. 카운터가 33초에 0으로 재설정되어 있기 때문에 시스템은 다른 이벤트를 로깅합니다.
Both(모두)	지정된 수(카운트)의 패킷이 규칙을 트리거한 후 특정 시기 동안 한 번에 하나의 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Both(**모두**)**로, **Count(**카운트**)**는 2로, 그리고 **Seconds(**초**)**는 10으로 설정하면, 다음과 같이 이벤트가 계산됩니다. • 규칙이 10초 안에 한 번 트리거되는 경우, 시스템은 어떤 이벤트도 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초 안에 두 번 트리거되는 경우, 시스템은 하나의 이벤트를 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

다음으로 이벤트 임계값이 소스 IP 주소별로 계산되는지 대상 IP 주소별로 계산되는지 결정하는 추적을 지정합니다.

표 *138:* 임계값 설정 *IP* 옵션

옵션	설명
소스	소스 IP 주소당 이벤트 인스턴스 수를 계산합니다.
대상	대상 IP 주소당 인스턴스 이벤트 수를 계산합니다.

마지막으로, 임계값을 정의하는 기간 및 인스턴스 수를 지정합니다.

표 *139:* 임계값 설정 인스턴스/시간 옵션

옵션	설명
개수	임계값 충족에 필요한 추적 IP 주소당 지정된 기간의 이벤트 인스턴스 수.
시간(초)	카운트가 재설정되기 전에 경과된 시간(초). 임계값 유형을 **limit(**제한**)**로, 추적을 **Source IP(**소스 **IP)**로, **count(**카운트**)**를 `10`으로, 그리고 **seconds(**초**)**를 `10`으로 설정한 경우, 시스템은 주어진 소스 포트에서 10초 안에 발생한 첫 10개의 이벤트를 로깅하고 표시합니다. 첫 10초 안에 7개의 이벤트만 발생한 경우, 시스템은 이를 모두 로깅하고 표시하며, 첫 10초 안에 40개의 이벤트가 발생한 경우, 시스템은 10개를 로깅하고 표시한 후 10초의 시간이 경과한 시점에서 다시 카운팅을 시작합니다.

침입 이벤트 임계값 설정을 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 삭제와 조합하여 사용할 수도 있습니다.

팁 침입 이벤트의 패킷 보기 내에서 임계값을 추가할 수도 있습니다.

관련 항목

detection_filter 키워드, 2167 페이지
패킷 보기 내 임계값 옵션 설정, 2942 페이지

침입 이벤트 임계값 추가 및 수정

침입 정책에서 하나 이상의 특정 규칙의 임계값을 설정할 수 있습니다. 별도로 또는 동시에 기존 임계값 설정을 수정할 수도 있습니다. 각각에 대해 단일 임계값을 설정할 수 있습니다. 임계값을 추가하여 규칙에 대한 기존 임계값을 덮어씁니다.

또한 침입 정책에 연결된 모든 규칙 및 전처리기 생성 이벤트에 기본적으로 적용되는 전역 임계값을 수정할 수 있습니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없으면 필드를 비워 둡니다.

팁 다중 CPU를 가진 매니지드 디바이스에서 전역 또는 개별 임계값은 예상보다 많은 수의 이벤트를 야기할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 창에서 **Policy Information(**정책 정보**)** 바로 아래의 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 임계값을 설정할 규칙을 찾습니다.

단계 **5** **Event Filtering(**이벤트 필터링**)** > **Threshold(**임계값**)**를 선택합니다.

단계 **6** **Type(**유형**)** 드롭다운 목록에서 임계값 유형을 선택합니다.

단계 **7** **Track By(**추적 기준**)** 드롭다운 목록에서 이벤트 인스턴스를 **Source(**소스**)** IP 주소로 추적할지 **Destination(**대상**)** IP 주소로 추적할지 선택합니다.

단계 **8** **Count(**카운트**)** 필드에 값을 입력합니다.

단계 **9** **Seconds(**초**)** 필드에 값을 입력합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우, 필터 위의 숫자는 이벤트 필터의 수를 나타냅니다.

단계 **11** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

전역 규칙 임계값 기본 사항, 2057 페이지

침입 이벤트 임계값 보기 및 삭제

규칙의 기존 임계값 설정을 보거나 삭제하고자 할 수 있습니다. 임계값에 대해 구성된 설정을 표시하여 시스템에 적절한지 확인하려면 Rules Details(규칙 세부 사항) 보기를 사용할 수 있습니다. 적절하지 않은 경우 새 임계값을 추가하여 기존 값을 덮어쓸 수 있습니다.

또한 침입 정책이 로깅한 모든 규칙 및 전처리기 생성 이벤트에 기본적으로 적용되는 전역 임계값을 수정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 창에서 **Policy Information(**정책 정보**)** 바로 아래의 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 보거나 삭제할 구성된 임계값이 있는 규칙을 선택합니다.

단계 **5** 선택한 각 규칙에 대한 임계값을 제거하려면 **Event Filtering(**이벤트 필터링**)** > **Remove Thresholds(**임계값 제거**)**를 선택합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

전역 규칙 임계값 기본 사항, 2057 페이지

침입 정책 삭제 설정

특정 IP 주소 또는 특정 범위의 IP 주소가 특정 규칙 또는 전처리기를 트리거하면 침입 이벤트 알림을 삭제할 수 있습니다. 이렇게 하면 오탐을 없애는 데 도움이 됩니다. 예를 들어 특정 익스플로잇처럼 보이는 패킷을 전송하는 메일 서버가 있는 경우, 메일 서버에 의해 이벤트가 트리거될 때 해당 이벤트에 대한 이벤트 알림을 억제할 수 있습니다. 규칙은 모든 패킷에 대해 트리거되지만, 기준에 맞는 공격에 대한 이벤트만 표시됩니다.

침입 정책 삭제 유형

침입 이벤트 억제를 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 임계값 설정과 조합하여 사용할 수도 있습니다.

팁 침입 이벤트의 패킷 보기 내에서 억제를 추가할 수도 있습니다. 침입 규칙 편집기 페이지(**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**) 및 침입 이벤트 페이지(이벤트가 침입 규칙에 의해 트리거된 경우)에서 마우스 오른쪽 버튼을 클릭하면 나타나는 컨텍스트 메뉴를 사용하여 억제 설정에 액세스할 수도 있습니다.

관련 항목

detection_filter 키워드, 2167 페이지
패킷 보기 내 임계값 옵션 설정, 2942 페이지

침입 규칙에 대한 침입 이벤트 삭제

침입 정책에서 규칙에 대한 침입 이벤트 알림을 억제할 수 있습니다. 규칙에 대한 알림이 삭제되면, 규칙은 트리거되지만 이벤트는 생성되지 않습니다. 규칙에 하나 이상의 삭제를 설정할 수 있습니다. 나열된 첫 번째 삭제가 가장 높은 우선 순위를 갖습니다. 2개의 억제가 충돌하면 첫 번째 억제의 작업이 수행됩니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 이를 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 억제 조건을 구성할 하나 이상의 규칙을 선택합니다.

단계 **5** **Event Filtering(**이벤트 필터링**)** > **Suppression(**억제**)**을 선택합니다.

단계 **6** **Suppression Type(**억제 유형**)**을 선택합니다.

단계 **7** 억제 유형으로 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택한 경우, **Network(**네트워크**)** 필드에 소스 또는 대상 IP 주소로 지정할 IP 주소, 주소 블록 또는 변수를 입력하거나 이러한 항목의 조합을 포함하는 쉼표로 구분된 목록을 입력합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

팁 시스템은 억제된 규칙 옆의 Event Filtering(이벤트 필터링) 열의 규칙 옆에 **Event Filter(**이벤트 필터**)**를 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우, 필터 위의 숫자는 이벤트 필터의 수를 나타냅니다.

단계 **9** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

삭제 조건 보기 및 삭제

기존 삭제 조건을 보거나 삭제하려고 할 수 있습니다. 예를 들어, 메일 서버는 일반적으로 익스플로잇처럼 보이는 패킷을 전송하므로 메일 서버 IP 주소에서 시작되는 패킷에 대한 이벤트 알림을 억제할 수 있습니다. 그리고 해당 메일 서버를 폐쇄하고 다른 호스트에 IP 주소를 다시 할당할 경우, 해당 소스 IP 주소에 대한 삭제 조건을 삭제해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 억제를 보거나 삭제할 규칙을 선택합니다.

단계 **5** 다음 옵션을 이용할 수 있습니다.

- 규칙에 대한 모든 억제를 제거하려면 **Event Filtering(**이벤트 필터링**)** > **Remove Suppressions(**억제 제거**)**를 선택합니다.
- 특정 억제 설정을 제거하려면 규칙을 클릭한 다음 **Show details(**세부 정보 보기**)**를 클릭합니다. 삭제 설정을 확장하고 제거할 삭제 설정 옆에 있는 **Delete(**삭제**)**를 클릭합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

동적 침입 규칙 상태

속도 기반 공격은 네트워크 또는 호스트에 과도한 트래픽을 전송하여 네트워크 또는 호스트를 마비시켜 느려지게 하거나 적법한 요청을 거부하도록 시도하는 것입니다. 속도 기반 차단을 사용하여 특정 규칙에 대한 과도한 규칙 일치에 대응하여 규칙 작업을 변경할 수 있습니다.

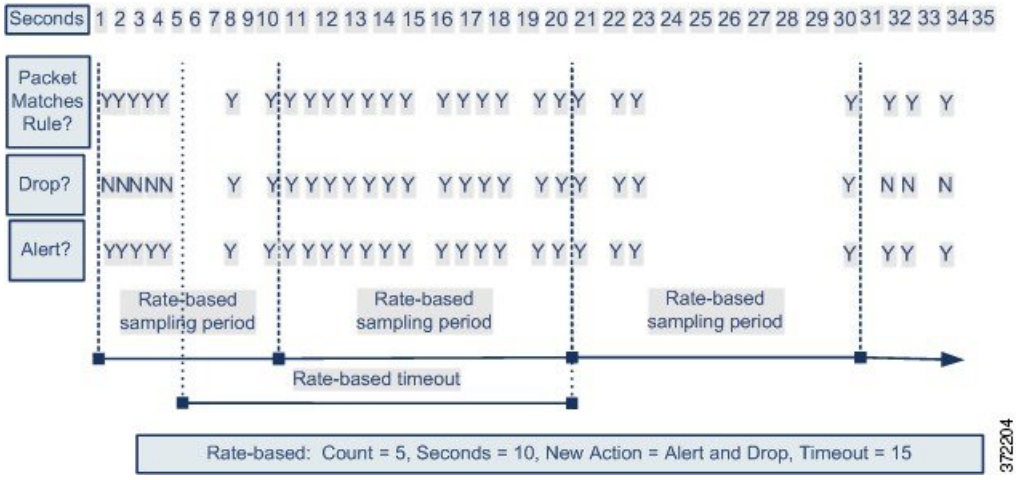
지정된 기간에 규칙에 대해 너무 많은 일치가 발생할 때 이를 탐지하는 속도 기반 필터를 포함하도록 침입 정책을 구성할 수 있습니다. 인라인으로 구축된 매니지드 디바이스에서 이 기능을 사용하여 지정된 시간 동안 속도 기반 공격을 차단한 후 규칙 일치를 통해 이벤트만 생성하고 트래픽을 삭제하지는 않는 규칙 상태로 돌아갈 수 있습니다.

속도 기반 공격 방지는 비정상적 트래픽 패턴을 식별하고 해당 트래픽이 정당한 요청에 미치는 영향을 최소화하려 시도합니다. 특정 대상 IP 주소로 이동하거나 특정 소스 IP 주소에서 오는 트래픽에서의 과도한 규칙 일치를 식별할 수 있습니다. 탐지된 모든 트래픽에서 특정 규칙에 대해 발생하는 과도한 일치에 대응할 수도 있습니다.

규칙과 일치하는 모든 패킷을 삭제하지는 않을 것이지만 지정된 시간에 특정 일치 속도가 발생하면 규칙과 일치하는 패킷을 삭제하려는 경우, 규칙을 Drop and Generate Events(이벤트 삭제 및 생성) 상태로 설정하지 않을 수 있습니다. 동적 규칙 상태를 사용하면 규칙에 대한 작업에서 변경을 트리거하는 속도, 속도가 충족될 때 작업에서 변경해야 할 내용, 새 작업의 지속 시간 등을 구성할 수 있습니다.

다음 다이어그램은 공격자가 호스트에 액세스하기 위해 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지가 구성된 규칙을 트리거합니다. 속도 기반 설정은 10초 범위 안에 규칙 일치가 다섯 번 발생하면 규칙 속성을 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 새로운 규칙 속성은 15초 후 시간 초과됩니다.

시간이 초과되더라도 패킷은 이어지는 속도 기반 샘플링 기간 내에 여전히 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 Generate Events(이벤트 생성)로 돌아갑니다.



동적 침입 규칙 상태 설정

침입 정책에서 침입 또는 전처리기 규칙에 대해 속도 기반 필터를 구성할 수 있습니다. 속도 기반 필터에는 다음과 같은 3개의 구성 요소가 포함되어 있습니다.

- 특정 초 이내 규칙 일치의 계수로 구성한 규칙 일치 비율
- 속도를 초과할 경우 다음 3개의 사용 가능한 작업과 함께 취할 새로운 작업: Generate Events(이벤트 생성), Drop and Generate Events(이벤트 삭제 및 생성), Disable(비활성화)
- 시간 제한 값으로 설정한 작업 기간

시작한 경우, 속도가 해당 기간 동안 구성된 속도까지 떨어지더라도 시간 제한에 도달할 때까지 새로운 작업이 발생한다는 점에 유의하십시오. 시간 제한에 도달하면, 속도가 임계값 아래로 떨어진 경우, 규칙 작업은 규칙에 처음 설정된 작업으로 돌아갑니다.

인라인 구축에서 속도 기반 공격 차단을 구성하여 일시적으로 또는 영구적으로 공격을 차단할 수 있습니다. 속도 기반 구성 없이 Generate Events(이벤트 생성)로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙에 대한 패킷을 삭제하지 않습니다. 하지만 속도 기반 기준이 구성되어 있는 규칙이 공격 트래픽과 일치하는 경우, 해당 규칙이 처음에는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있지 않더라도 속도 작업은 속도 작업이 활성화된 기간 동안 패킷이 삭제되도록 할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나 비활성화된 규칙에 일치하는 트래픽을 삭제할 수 없습니다.

동일한 규칙에서 다중 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 나열된 첫 번째 필터의 우선 순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌하면 첫 번째 속도 기반 필터의 작업이 수행됩니다.

규칙 페이지에서 동적 규칙 상태 설정

규칙에 하나 이상의 동적 규칙 상태를 설정할 수 있습니다. 나열된 첫 번째 동적 규칙 상태의 우선 순위가 가장 높습니다. 2개의 동적 규칙 상태가 충돌하면 첫 번째 상태의 작업이 수행됩니다.

동적 규칙 상태는 정책에 따라 다릅니다.

잘못된 값을 입력하면 **Revert(**되돌리기**)**가 필드에 나타납니다. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없으면 필드를 지웁니다.

참고 동적 규칙 상태는 비활성화된 규칙을 활성화하거나, 비활성화된 규칙과 일치하는 트래픽을 삭제할 수 없습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 창에서 **Policy Information(**정책 정보**)** 바로 아래의 **Rules(**규칙**)**를 클릭합니다.

단계 **4** 동적 규칙 상태를 추가할 규칙을 선택합니다.

단계 **5** **Dynamic State(**동적 상태**)** > **Add Rate-Based Rule State(**속도 기반 규칙 상태 추가**)**를 선택합니다.

단계 **6** **Track By(**추적 기준**)** 드롭다운 목록에서 값을 선택합니다.

단계 **7** **Track By**를 **Source** 또는 **Destination**으로 설정하는 경우 추적하려는 각 호스트의 주소를 **Network** 필드에 입력합니다. 단일 IP 주소, 주소 블록, 변수 또는 이들 조합으로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **8** 공격 속도를 설정하려면 **Rate(**속도**)** 옆에 기간당 규칙 일치 수를 지정합니다.

- **Count(**카운트**)** 필드에 값을 입력합니다.
- **Seconds(**초**)** 필드에 값을 입력합니다.

단계 **9** **New State(**새로운 상태**)** 드롭다운 목록에서 조건이 충족되면 수행할 새로운 작업을 지정합니다.

단계 **10** **Timeout(**시간 제한**)** 필드에 값을 입력합니다.

시간 제한이 발생한 후, 규칙은 원래 상태로 돌아갑니다. 새 작업의 시간 초과를 금지하려면 0을 지정하거나 **Timeout** 필드를 비워둡니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Dynamic State(동적 상태) 열의 규칙 옆에 **Dynamic State(**동적 상태**)**를 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가한 경우, 필터 위의 숫자는 필터 수를 나타냅니다.

팁 규칙 집합에 대한 모든 동적 규칙 설정을 삭제하려면 Rules(규칙) 페이지에서 규칙을 선택한 후 **Dynamic State(**동적 상태**)** > **Remove Rate-Based States(**속도 기반 상태 제거**)**를 선택합니다. 규칙을 선택하고 **Show details(**세부 정보 보기**)**를 클릭한 후 제거할 속도 기반 필터 옆에 있는 **Delete(**삭제**)**를 클릭하여 규칙의 규칙 세부 정보에서 개별 속도 기반 규칙 상태 필터를 삭제할 수도 있습니다.

단계 **12** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

침입 규칙 설명 추가

침입 정책에서 규칙에 코멘트를 추가할 수 있습니다. 이렇게 추가되는 코멘트는 해당 정책에 한정됩니다. 즉, 한 침입 정책에서 규칙에 추가하는 코멘트는 다른 침입 정책에서는 표시되지 않습니다. 추가하는 코멘트는 해당 침입 정책 Rules(규칙) 페이지의 Rule Details(규칙 세부 사항) 보기에서 볼 수 있습니다.

코멘트가 포함된 침입 정책 변경 사항을 커밋한 후에는 또한 규칙 Edit(수정) 페이지에서 **Rule Comment(**규칙 코멘트**)**를 클릭하여 코멘트를 볼 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정 아이콘(수정( ))을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색창의 **Policy Information(**정책 정보**)** 아래에서 **Rules(**규칙**)**를 즉시 클릭합니다.

단계 **4** 코멘트를 추가하고자 하는 규칙을 선택합니다.

단계 **5** **Comments(**코멘트**)** > **Add Rule Comment(**규칙 코멘트 추가**)**를 선택합니다.

단계 **6** **Comments(**코멘트**)** 필드에 규칙 코멘트를 입력합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

팁 시스템은 Comments(코멘트) 열의 규칙 옆에 코멘트( )를 표시합니다. 규칙에 여러 코멘트를 추가하는 경우, 코멘트 위의 숫자는 코멘트 수를 나타냅니다.

단계 **8** 원하는 경우, 코멘트 옆의 **Delete(**삭제**)**를 클릭하여 규칙 코멘트를 삭제합니다.

커밋되지 않은 침입 정책 변경 사항과 함께 코멘트가 캐시된 경우에만 코멘트를 삭제할 수 있습니다. 침입 정책 변경 사항이 커밋되면 규칙 코멘트는 영구적입니다.

단계 **9** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

82 장

네트워크 자산에 대한 침입 방지 맞춤화

다음 주제에서는 Firepower 권장 규칙을 사용하는 방법을 설명합니다.

- Firepower 권장 규칙 정보, 2037 페이지
- Firepower 추천 기본 설정, 2038 페이지
- Firepower 추천 고급 설정, 2039 페이지
- Firepower 추천 생성 및 적용, 2040 페이지

Firepower 권장 규칙 정보

Firepower 침입 규칙 권장사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 자산을 보호하기 위해 특별히 작성된 규칙과 연결할 수 있습니다. 침입 정책을 모니터링되는 네트워크의 특정 요구를 조정할 수 있게 합니다.

시스템에서 각 IPS 정책 대 한 권장 사항 개별 집합을 만듭니다. 일반적으로 표준 텍스트 규칙 및 공유 개체 규칙에 대 한 규칙 상태 변경을 권장합니다. 그러나, 전처리기 및 디코더 규칙에 대 한 변경 사항을 추천해 합니다.

규칙 상태 권장 사항을 생성할 때에 기본 설정을 사용 하 여 수도 있고 고급 설정을 구성할 수 있습니다. 고급 설정을 수행할 수 있습니다.

- 취약성에 대 한 네트워크에 있는 호스트 시스템 모니터링 재정의
- 규칙 오버 헤드에 따라 시스템이 권장 규칙에 영향을
- 규칙을 비활성화 하기 위한 권장 생성을 활성화할지 지정

권장 되는 즉시 사용 또는 권장 사항 (및 영향을 받는 규칙)을 수락 하기 전에 검토 선택할 수도 있습니다.

권장 규칙 상태를 사용하도록 선택하면 읽기 전용 Firepower 권장 사항 계층이 침입 정책에 추가되고 이후 권장 규칙 상태를 사용하지 않기로 선택하면 계층이 제거됩니다.

침입 정책에서 가장 최근에 저장된 구성 설정에 따라 자동으로 권장 사항을 생성하도록 태스크를 예약할 수 있습니다.

시스템은 수동으로 설정한 규칙 상태를 변경하지 않습니다.

- 권장 사항을 생성하기 전에 지정된 규칙의 상태를 수동으로 설정하면 시스템이 향후 해당 규칙의 상태를 수정할 수 없게 됩니다.
- 권장 사항을 생성한 후 수동으로 지정된 규칙의 상태를 설정하면 해당 규칙의 권장 상태가 재정의됩니다.

팁 침입 정책 리포트는 권장 상태와 다른 규칙 상태를 가진 규칙 목록을 포함할 수 있습니다.

권장 필터링된 규칙 페이지를 표시하는 동안 또는 탐색 패널 또는 정책 정보 페이지에서 직접 규칙 페이지에 액세스한 후 규칙 상태를 수동으로 설정하고 규칙을 정렬하고 규칙 페이지에서 사용할 수 있는 다른 작업(예: 규칙 억제, 규칙 임계값 설정 등)을 수행할 수 있습니다.

참고 Cisco Talos Intelligence Group(Talos) 시스템 제공 정책에서 각 규칙의 적절한 상태를 결정합니다. 시스템 제공 정책을 사용 하 여 기본 정책으로 시스템 Firepower 권장 규칙 상태에 규칙을 설정 하도록 허용 하는 경우 네트워크 자산 대 한 Cisco에서 권장 하는 설정을 IPS 정책 규칙에 일치 합니다.

권장된 규칙 및 멀티 테 넌 시

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 상위 도메인의 침입 정책에서 이 기능을 활성화하면 모든 하위 리프 도메인의 데이터를 사용하여 권장 사항이 생성됩니다. 이로 인해 일부 리프 도메인에는 없는 자산에 맞게 조정된 침입 규칙이 활성화되어 성능에 영향을 줄 수 있습니다.

Firepower 추천 기본 설정

Firepower 권장 사항을 생성하면 시스템은 네트워크 자산과 연결된 취약성으로부터 보호하는 규칙의 기본 정책을 검색하고 기본 정책에서 규칙의 현재 상태를 식별합니다. 그런 다음 시스템은 규칙 상태를 추천하며, 사용자가 선택하면 규칙을 권장 상태로 설정합니다.

시스템은 다음과 같은 기본 분석을 수행하여 권장 사항을 생성합니다.

표 ***140:*** 취약성을 기준으로 한 규칙 상태 권장 사항

규칙이 검색된 자산을 보호합니까**?**	기본 정책 규칙 상태	권장 규칙 상태
예	비활성화	이벤트 생성
	이벤트 생성	이벤트 생성
	이벤트 삭제 및 생성	이벤트 삭제 및 생성
아니요	모든 상태	비활성화

테이블에서 다음에 유의하십시오.

- 규칙이 기본 정책에서 비활성화되어 있거나 Generate Events(이벤트 생성)로 설정된 경우, 권장 상태는 항상 Generate Events(이벤트 생성)입니다.

  예를 들어 기본 정책이 모든 규칙이 비활성화되는 No Rules Active(활성 규칙 없음)인 경우, Drop and Generate Events(이벤트 삭제 및 생성) 권장 사항은 없습니다.

- Drop and Generate Events(이벤트 삭제 및 생성)은 기본 정책에서 이미 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙의 경우에만 권장됩니다.

  규칙을 Drop and Generate events(이벤트 삭제 및 생성)으로 설정하려 하고 해당 규칙이 기본 정책에서 비활성화되어 있거나 Generate Events(이벤트 생성)로 설정된 경우, 규칙 상태를 수동으로 재설정해야 합니다.

Firepower 권장 규칙의 고급 설정을 변경하지 않고 권장 사항을 생성하면 시스템은 검색된 전체 네트워크의 모든 호스트에 대해 규칙 상태를 변경하도록 권장합니다.

시스템은 기본적으로 오버헤드가 낮거나 중간인 규칙에 대해서만 권장 사항을 생성하며, 규칙을 비활성화하라는 권장 사항을 생성합니다.

시스템은 Impact Qualification 기능을 사용하여 비활성화하는 취약성에 기반한 침입 규칙에 대해 규칙 상태를 권장하지 않습니다.

시스템은 항상 호스트에 매핑된 서드파티 취약성에 연결된 로컬 규칙을 활성화하도록 권장합니다.

시스템은 매핑되지 않은 로컬 규칙에 대해서는 상태 권장 사항을 만들지 않습니다.

관련 항목

개별 취약성 비활성화, 3027 페이지
서드파티 제품 매핑, 2407 페이지

Firepower 추천 고급 설정

정책 보고서에 권장 사항과 규칙 상태의 모든 차이를 포함합니다

기본적으로 침입 정책 보고서는 정책의 활성화된 규칙, 즉 Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙을 나열합니다. **Include all differences(**모든 차이점 포함**)** 옵션을 활성화하면 권장 상태가 저장된 상태와 다른 규칙도 나열됩니다. 정책 보고서에 대해서는 정책 보고서, 515 페이지를 참조하십시오.

검사할 네트워크

권장 사항을 위해 검사할 모니터링되는 네트워크 또는 개별 호스트를 지정합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 하나 또는 둘 다로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.

지정하는 호스트 내 주소의 목록은 부정을 제외하고 OR 연산으로 연결되며, 모든 OR 연산이 계산되면 AND 연산으로 연결됩니다.

호스트 정보를 기반으로 특정 패킷에 대해 활성 규칙 프로세싱을 동적으로 수정하려면 적응형 프로파일을 활성화할 수도 있습니다.

권장 사항 임계값(규칙 오버 헤드별)

사용자가 선택하는 임계값보다 오버헤드가 높은 침입 규칙을 시스템이 권장하거나 자동으로 활성화하는 것을 방지합니다.

오버헤드는 규칙이 시스템 성능에 미칠 수 있는 영향과 규칙이 오탐을 생성할 가능성에 기반합니다. 오버헤드가 더 높은 규칙을 허용하면 일반적으로 권장 사항은 늘어나지만 시스템 성능에 영향이 있을 수 있습니다. 침입 Rules(규칙) 페이지의 규칙 세부 사항 보기에서 규칙의 오버헤드 등급을 볼 수 있습니다.

시스템은 규칙을 비활성화하라는 권장 사항에 대해서는 규칙 오버헤드를 고려하지 않습니다. 또한 서드파티 취약성에 매핑되지 않는 한 로컬 규칙은 오버 헤드가 없는 것으로 간주됩니다.

특정 설정의 오버헤드 등급이 있는 규칙에 대한 권장 사항을 생성할 경우, 오버헤드가 다른 권장 사항을 생성한 다음 원래 오버헤드 설정에 대해 권장 사항을 다시 생성하는 것이 차단되지 않습니다. 권장 사항의 생성 횟수 또는 생성에 사용하는 오버헤드 설정의 수와 상관없이 동일한 규칙 집합에 대해 권장 사항을 생성할 때마다 각 오버헤드 설정에 대해 동일한 규칙 상태 권장 사항을 얻게 됩니다. 예를 들면 오버헤드를 medium으로, 그 다음에는 high로, 그런 다음 마지막으로 다시 medium으로 설정하여 권장 사항을 생성할 수 있습니다. 네트워크의 호스트와 애플리케이션이 변경되지 않은 경우, 오버헤드가 medium으로 설정된 권장 사항의 두 집합은 해당 규칙 집합에 대해 동일합니다.

규칙을 비활성화하라는 권장 사항 수락

시스템은 Firepower 권장 사항을 기반으로 하는 침입 규칙을 비활성화 여부를 지정 합니다.

규칙을 비활성화하라는 권장 사항을 수용하면 규칙 적용 범위가 제한됩니다. 규칙을 비활성화하라는 권장 사항을 생략하면 규칙 적용 범위가 증가합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지
적응형 프로파일 및 Firepower 권장 규칙, 2372 페이지

Firepower 추천 생성 및 적용

Firepower 권장 사항 사용을 시작하거나 중지하려면 네트워크 및 침입 규칙 집합의 크기에 따라 몇 분 정도 걸릴 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 상위 도메인의 침입 정책에서 이 기능을 활성화하면 모든 하위 리프 도메인의 데이터를 사용하여 권장 사항이 생성됩니다. 이로 인해 일부 리프 도메인에는 없는 자산에 맞게 조정된 침입 규칙이 활성화되어 성능에 영향을 줄 수 있습니다.

시작하기 전에

Firepower 권장 사항에는 다음 요구 사항이 있습니다.

- FTD 라이센스—위협
- 기본 라이선스—보호
- 사용자 역할—관리자 또는 침입 관리자

프로시저

단계 **1** 침입 정책 편집기의 탐색창에서 **Firepower Recommendations(Firepower** 권장 사항**)**를 클릭합니다.

단계 **2** (선택 사항) 고급 설정을 구성합니다(Firepower 추천 고급 설정, 2039 페이지 참조).

단계 **3** 권장 사항을 생성하고 적용합니다.

- 권장 사항 생성 및 사용 - 권장 사항을 생성하고 일치하도록 규칙 상태를 변경합니다. 권장 사항을 생성한 적이 없는 경우에만 사용할 수 있습니다.
- 권장 사항 생성 - 권장 사항을 사용 중인지 여부에 상관없이 새로운 권장 사항을 생성하지만 일치하도록 규칙 상태를 변경하지는 않습니다.
- 권장 사항 업데이트 - 권장 사항을 사용 중인 경우, 권장 사항을 생성하고 일치하도록 규칙 상태를 변경합니다. 그렇지 않은 경우, 규칙 상태를 변경하지 않고 새 권장 사항을 생성합니다.
- 권장 사항 사용 - 구현되지 않은 권장 사항과 일치하도록 규칙 상태를 변경합니다.
- 권장 사항 사용 안 함 - 권장 사항 사용을 중지합니다. 권장 사항을 적용하기 전에 규칙의 상태를 수동으로 변경한 경우, 규칙 상태는 사용자가 부여한 값으로 돌아갑니다. 그렇지 않은 경우, 규칙 상태는 기본값으로 돌아갑니다.

권장 사항을 생성할 때 시스템은 권장 변경 사항의 요약을 표시합니다. 시스템이 상태 변경을 권장하는 규칙의 목록을 보려면 새로 제안된 규칙 상태 옆에 있는 **View(**보기**)**를 클릭합니다.

단계 **4** 구현한 권장 사항을 평가하고 조정합니다.

대부분의 Firepower 권장 사항을 수락하는 경우에도 규칙 상태를 수동으로 설정하여 개별 권장 사항을 재정의할 수 있습니다(침입 규칙 상태 설정, 2024 페이지 참조).

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Firepower 추천 자동화, 256 페이지

83 장

민감한 데이터 탐지

다음 주제에서는 민감한 데이터 탐지 및 그 구성 방법을 설명합니다.

- 민감한 데이터 탐지 기본 사항, 2043 페이지
- 전역 민감한 데이터 탐지 옵션, 2044 페이지
- 개별 민감한 데이터 유형 옵션, 2045 페이지
- 시스템 제공 민감한 데이터 유형, 2046 페이지
- 민감한 데이터 탐지 라이선스 요건, 2047 페이지
- 민감한 데이터 탐지 요구 사항 및 사전 요건, 2048 페이지
- 민감한 데이터 탐지 구성, 2048 페이지
- 모니터링된 애플리케이션 프로토콜 및 민감한 데이터, 2050 페이지
- 모니터링할 애플리케이션 프로토콜 선택, 2050 페이지
- 특별 케이스: FTP 트래픽에서 민감한 데이터 탐지, 2051 페이지
- 맞춤형 민감한 데이터 유형, 2052 페이지

민감한 데이터 탐지 기본 사항

사회 보장 번호, 신용카드 번호, 운전면허증 번호 같은 민감한 정보가 인터넷에 고의적으로 또는 실수로 유출될 수 있습니다. 이 시스템에서는 ASCII 텍스트로 된 민감한 데이터에 대한 이벤트를 탐지하고 생성할 수 있는 민감한 데이터 전처리기를 제공하며, 이는 실수로 인한 데이터 유출을 탐지할 때 특히 유용합니다.

전역 민감한 데이터 전처리기 옵션은 전처리기가 작용하는 방법을 제어합니다. 다음을 지정하는 전역 옵션을 변경할 수 있습니다.

- 시작하는 패킷에서 전처리기가 신용 카드 번호 또는 사회 보장 번호의 마지막 네 자리를 제외한 모든 것을 대체하는지 여부
- 네트워크에서 민감한 데이터에 대해 모니터링하는 대상 호스트의 종류
- 단일 세션에서 단일 이벤트로 귀결되는 모든 데이터 유형의 총 발생 횟수

개별 데이터 유형은 지정된 대상 네트워크에서 이벤트를 탐지하고 생성할 수 있는 민감한 데이터를 식별합니다. 다음을 지정하는 데이터 유형 옵션에 대한 기본 설정을 변경할 수 있습니다.

- 탐지된 데이터 유형이 단일한 세션별 이벤트를 생성하려면 충족해야 하는 임계값
- 각 데이터 유형을 모니터링할 대상 포트
- 각 데이터 유형을 모니터링할 애플리케이션 프로토콜

사용자 지정 데이터 유형을 만들고 수정하여 지정하려는 데이터 패턴을 탐지할 수 있습니다. 예를 들어, 병원이 환자 번호를 보호하기 위해 데이터 유형을 만들 수 있으며 대학이 고유 번호 패턴이 있는 학생 수를 탐지하기 위해 데이터 유형을 만들 수도 있습니다.

시스템에서는 개별 데이터 유형을 트래픽과 일치시켜 TCP 세션당 민감한 데이터를 탐지합니다. 사용자 침입 정책에서 모든 데이터 유형에 적용되는 전역 옵션 및 각 데이터 유형에 대한 기본 설정을 수정할 수 있습니다. Firepower System는 일반적으로 사용되는 미리 정의된 데이터 유형을 제공합니다. 또한 사용자 지정 데이터 유형을 만들 수 있습니다.

민감한 데이터 전처리기 규칙은 각 데이터 유형과 연결됩니다. 각 데이터 유형의 전처리기 규칙을 활성화하여 각 데이터 유형에 대한 민감한 데이터 탐지 및 이벤트 생성을 활성화할 수 있습니다. 구성 페이지 링크를 통해 Rules(규칙) 페이지에서 민감한 데이터를 필터링하여 볼 수 있는데, 여기서 규칙을 활성화/비활성화하고 다른 규칙 속성을 구성할 수 있습니다.

데이터 유형과 관련된 규칙이 활성화되고 민감한 데이터 탐지가 비활성화된 경우, 침입 정책에 변경 사항을 저장하면, 자동으로 민감한 데이터 전처리기를 활성화하는 옵션이 제공됩니다.

팁 민감한 데이터 전처리기는 FTP 또는 HTTP를 사용하여 업로드되고 다운로드된 암호화되지 않은 Microsoft에서 민감한 데이터를 탐지할 수 있습니다. Word 파일이 ASCII 텍스트 및 서식 설정 명령을 별도로 분류하는 방식 때문에 이것이 가능합니다.

시스템에서는 암호화되거나 위장된 형태의 민감한 데이터나 압축 또는 인코딩된 형식(예: Base64 인코딩 이메일 첨부 파일)의 민감한 데이터를 탐지하지 않습니다. 예를 들어 시스템은 전화 번호 (555)123-4567은 탐지하지만 (5 5 5) 1 2 3 - 4 5 6 7과 같이 공백으로 각 번호가 분리되어 있거나 (555)-123-4567과 같이 HTML 코드가 끼어 있는 애매한 버전은 탐지하지 못합니다. 하지만 시스템은 중간 코드가 번호 패턴을 방해하지 않는 HTML 코드 번호 (555)-123-4567은 탐지합니다.

전역 민감한 데이터 탐지 옵션

전역 민감한 데이터 옵션은 정책 단위이며 모든 데이터 유형에 적용됩니다.

마스크

시작하는 패킷에서 신용 카드 번호 또는 사회 보장 번호의 마지막 네 자리를 제외한 모든 것을 X로 대체합니다. 마스크 처리된 번호는 웹 인터페이스의 침입 이벤트 보기 및 다운로드한 패킷에 표시됩니다.

네트워크

민감한 데이터를 위해 모니터링할 대상 호스트를 지정합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 시스템은 비어 있는 필드를 모든으로 해석하며, 모든 대상 IP 주소를 의미합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

전역 임계값

전처리기가 전역 임계값 이벤트를 생성하기 전에 모든 조합에서 탐지해야 하는 단일 세션 동안 모든 데이터 유형의 모든 항목 수를 지정합니다. 1부터 65535까지 지정할 수 있습니다.

Cisco는 이 옵션 값을 정책에서 활성화한 모든 개별 데이터 유형의 가장 높은 임계값보다 높게 설정할 것을 권장합니다.

전역 임계값에 관해 다음 사항에 유의하십시오.

- 조합된 데이터 유형 발생에서 이벤트를 탐지 및 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 전처리기 규칙 139:1을 활성화해야 합니다.
- 전처리기는 세션당 하나의 전역 임계값 이벤트를 생성합니다.
- 전역 이벤트 임계값은 개별 데이터 유형 이벤트와 상관없습니다. 즉 전처리기는 모든 개별 데이터 유형에 대한 이벤트 임계값에 도달했는지에 관계없이, 그리고 그 반대의 경우에도 그에 관계없이, 전역 임계값에 도달했을 때 이벤트를 생성합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

개별 민감한 데이터 유형 옵션

최소한 각 맞춤형 데이터 유형은 이벤트 임계값 및 모니터링할 하나 이상의 포트 또는 애플리케이션 프로토콜을 지정해야 합니다.

시스템이 제공하는 각각의 데이터 유형은 다른 경우에는 액세스할 수 없는 `sd_pattern` 키워드를 사용하여 트래픽에서 탐지할 내장형 데이터 패턴을 정의합니다. 또한 간단한 정규 표현식을 사용하여 사용자 고유의 데이터 패턴을 지정할 수 있는 사용자 지정 데이터 유형을 생성할 수도 있습니다.

민감한 데이터 유형은 Senstivie Data Detection(민감한 데이터 탐지)가 활성화된 모든 침입 정책에 표시됩니다. 시스템에서 제공한 데이터 유형은 읽기 전용으로 표시됩니다. 맞춤형 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 민감한 데이터 유형을 표시하며, 이 데이터 유형은 수정할 수 있습니다. 상위 도메인에서 생성된 데이터 유형도 표시되며, 이 데이터 유형은 제한적 방법으로 수정할 수 있습니다. 상위 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

표 ***141:*** 개별 데이터 유형 옵션

옵션	설명
데이터 유형	데이터 유형의 고유한 이름을 지정합니다.
임계값	시스템이 이벤트를 생성할 때 데이터 유형 발생 수를 지정합니다. 1부터 255까지 지정할 수 있습니다. 전처리기는 세션당 탐지한 데이터 유형에 대한 1가지 이벤트를 생성한다는 점에 유의하십시오. 전역 이벤트 임계값은 개별 데이터 유형 이벤트와 상관없습니다. 즉 전처리기는 전역 이벤트 임계값에 도달했는지 여부와 그 반대의 경우에도 관계없이, 데이터 유형 이벤트 임계값에 도달했을 때 이벤트를 생성합니다.
대상 포트	각 데이터 유형을 모니터링할 대상 포트를 지정합니다. 단일 포트나 쉼표로 구분된 포트 목록 또는 모든 대상 포트를 뜻하는 `any`(모든)를 지정할 수 있습니다.
애플리케이션 프로토콜	데이터 유형에 대해 모니터링하기 위해 최대 8개의 애플리케이션 프로토콜을 지정합니다. 모니터링할 애플리케이션 프로토콜을 식별하려면 애플리케이션 탐지기를 활성화해야 합니다. 기본 디바이스의 경우, 이 기능에는 제어 라이선스가 필요합니다.
패턴	탐지할 패턴을 지정합니다. 이 필드는 맞춤형 데이터 유형에만 있습니다.

관련 항목

탐지기 활성화 및 비활성화, 2456 페이지

시스템 제공 민감한 데이터 유형

각 침입 정책은 대시가 있거나 없는 신용 카드 번호, 전자 메일 주소, 미국 전화 번호 및 미국 사회 보장 번호와 같은 일반적으로 사용되는 데이터 패턴 탐지를 위한 시스템 제공 데이터 유형을 포함합니다.

각각의 시스템 제공 데이터 유형은 생성기 ID(GID) 138을 가진 단일 민감한 데이터 전처리기 규칙과 연결됩니다. 정책에서 사용할 각 데이터 유형에 대해 연결된 민감한 데이터 규칙을 침입 정책에서 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.해야 합니다.

다음 표에서는 각 데이터 유형을 설명하고 해당 전처리기 규칙을 나열합니다.

표 ***142:*** 시스템 제공 민감한 데이터 유형

데이터 유형	설명	전처리기 규칙 **GID:SID**
신용 카드 번호	표준 구분 대시나 공백을 사용하거나 사용하지 않고 Visa®, MasterCard®, Discover® 및 American Express® 15/16자리 신용 카드 번호를 매칭합니다. 또한 Luhn 알고리즘을 사용하여 신용 카드 확인 번호를 확인합니다.	138:2
이메일 주소	이메일 주소에 일치합니다.	138:5
미국 전화 번호	패턴 `(\d{3}) ?\d{3}-\d{4}`를 준수하는 미국 전화 번호를 매칭합니다.	138:6
대시 없는 미국 사회 보장 번호	유효한 3자리 지역 번호와 유효한 2자리 그룹 번호가 있으며 대시를 포함하지 않는 9자리 미국 사회 보장 번호를 매칭합니다.	138:4
대시 있는 미국 사회 보장 번호	유효한 3자리 지역 번호와 유효한 2자리 그룹 번호가 있으며 대시를 포함하는 9자리 미국 사회 보장 번호를 매칭합니다.	138:3

사회 보장 번호 외의 9자리 번호에서 오탐을 줄이기 위해 전처리기는 각 사회 보장 번호에서 4자리 일련 번호 앞에 오는 3자리 지역 번호와 2자리 그룹 번호를 검증하는 알고리즘을 사용합니다. 전처리기는 2009년 11월까지 사회 보장 그룹 번호를 승인합니다.

민감한 데이터 탐지 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호 또는 절차에 나와 있습니다.

민감한 데이터 탐지 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

민감한 데이터 탐지 구성

민감한 데이터 탐지는 Firepower System의 성능에 큰 영향을 미칠 수 있으므로 Cisco에서는 다음 지침을 따를 것을 권장합니다.

- 기본 침입 정책으로 No Rules Active(활성 규칙 불가) 기본 정책을 선택합니다.
- 해당 네트워크 분석 정책에서 다음 구성이 활성화되어 있는지 확인하십시오.
  - **Application Layer Preprocessors(**애플리케이션 레이어 전처리기**)** 아래의 **FTP and Telnet Configuration(FTP** 및 텔넷 구성**)**
  - **Transport/Network Layer Preprocessors(**전송/네트워크 레이어 전처리기**)** 아래의 **IP Defragmentation(IP** 조각 모음**)** 및 **TCP Stream Configuration(TCP** 스트림 컨피그레이션**)**

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

시작하기 전에

클래식 디바이스의 경우, 이 절차에는 보호 또는 제어 라이선스가 필요합니다.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 수정( )을(를) 클릭합니다.

단계 **6** 다음 옵션을 이용할 수 있습니다.

- 전역 민감한 데이터 탐지 옵션, 2044 페이지에 설명된 대로 전역 설정을 수정합니다.
- **Targets(**대상**)** 섹션에서 데이터 유형을 선택하고 개별 민감한 데이터 유형 옵션, 2045 페이지에 설명된 대로 데이터 유형 구성을 수정합니다.
- 맞춤형 민감한 데이터를 검사하려면 맞춤형 데이터 유형을 생성합니다(맞춤형 민감한 데이터 유형, 2052 페이지 참조).

단계 **7** 데이터 유형을 모니터링할 애플리케이션 프로토콜을 추가 또는 제거합니다(모니터링된 애플리케이션 프로토콜 및 민감한 데이터, 2050 페이지 참조).

참고 FTP 트래픽에서 민감한 데이터를 탐지하려면 `Ftp data` 애플리케이션 프로토콜을 추가해야 합니다.

단계 **8** 원하는 경우, 민감한 데이터 전처리기 규칙을 표시하려면 **Configure Rules for Sensitive Data Detection(**민감한 데이터 탐지 규칙 구성**)**을 클릭합니다.

나열된 규칙 중 원하는 항목을 활성화 또는 비활성화할 수 있습니다. 또한 Rules(규칙) 페이지에서 규칙 억제, 속도 기반 공격 방지 등과 같은 사용 가능한 다른 작업에 대한 민감한 데이터 규칙을 구성할 수 있습니다. 자세한 내용은 침입 규칙 유형, 2008 페이지를 참고하십시오.

단계 **9** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

민감한 데이터 탐지를 활성화하지 않고 정책에서 민감한 데이터 전처리기 규칙을 활성화한 경우, 정책에 변경 사항을 저장하면 민감한 데이터 탐지를 활성화하라는 메시지가 표시됩니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 생성하려면 민감한 데이터 탐지 규칙 138:2, 138:3, 138:4, 138:5, 138:6, 138:>999999 또는 139:1을 활성화합니다. 자세한 내용은 침입 규칙 상태, 2023 페이지, 전역 민감한 데이터 탐지 옵션, 2044 페이지, 시스템 제공 민감한 데이터 유형, 2046 페이지, 맞춤형 민감한 데이터 유형, 2052 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

특별 케이스: FTP 트래픽에서 민감한 데이터 탐지, 2051 페이지

모니터링된 애플리케이션 프로토콜 및 민감한 데이터

각 데이터 유형에 대해 모니터링하기 위해 최대 8개의 애플리케이션 프로토콜을 지정할 수 있습니다. 선택한 각 애플리케이션 프로토콜에 대해 하나 이상의 탐지기가 활성화되어야 합니다. 기본적으로 모든 시스템 제공 탐지기는 활성화되어 있습니다. 애플리케이션 프로토콜에 활성화된 탐지기가 없는 경우, 시스템은 해당 애플리케이션의 모든 시스템 제공 탐지기를 자동으로 활성화합니다. 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 해당 애플리케이션의 맞춤형 탐지기를 활성화합니다.

각 데이터 유형에 대해 모니터링하기 위해 최소 1개의 애플리케이션 프로토콜 또는 포트를 지정해야 합니다. 그러나 FTP 트래픽에서 민감한 데이터 탐지를 원하는 경우를 제외하고 Cisco는 완벽한 적용을 위해 애플리케이션 프로토콜을 지정할 때 해당 포트를 지정할 것을 권장합니다. 예를 들어 HTTP를 지정하는 경우, 잘 알려진 HTTP 포트 80도 구성할 수 있습니다. 네트워크의 새 호스트가 HTTP를 구현하면, 시스템은 새 HTTP 애플리케이션 프로토콜을 검색하는 사이에 포트 80을 모니터링합니다.

FTP 트래픽에서 민감한 데이터를 탐지하려는 경우, `FTP data` 애플리케이션 프로토콜을 지정해야 합니다. 포트 번호 지정에는 이점이 없습니다.

관련 항목

탐지기 활성화 및 비활성화, 2456 페이지
특별 케이스: FTP 트래픽에서 민감한 데이터 탐지, 2051 페이지

모니터링할 애플리케이션 프로토콜 선택

시스템에서 제공하는 민감한 데이터 유형 및 맞춤형 민감한 데이터 유형에서 모니터링할 애플리케이션 프로토콜을 지정할 수 있습니다. 선택하는 애플리케이션 프로토콜은 정책별로 다릅니다.

시작하기 전에

클래식 디바이스의 경우 이 절차에는 제어 라이선스가 필요합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**을(를) 선택합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Data Types(**데이터 유형**)**에서 데이터 유형 이름을 클릭합니다.

단계 **7** **Application Protocols(**애플리케이션 프로토콜**)** 필드 옆의 수정( )을 클릭합니다.

단계 **8** 다음 옵션을 이용할 수 있습니다.

- 모니터링할 애플리케이션 프로토콜을 추가하려면 **Available(**사용 가능**)** 목록에서 하나 이상의 애플리케이션 프로토콜을 선택한 다음 오른쪽 화살표(>) 버튼을 클릭합니다. 모니터링할 최대 8개의 애플리케이션 프로토콜을 추가할 수 있습니다.
- 애플리케이션 프로토콜을 모니터링에서 제거하려면 **Enabled(**활성화**)** 목록에서 선택한 다음 왼쪽 화살표(<) 버튼을 클릭합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 탐색 창에서 **Policy Information(**정책 정보**)**을 클릭하고 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

특별 케이스: FTP 트래픽에서 민감한 데이터 탐지, 2051 페이지

특별 케이스: FTP 트래픽에서 민감한 데이터 탐지

어떤 트래픽에서 민감한 데이터를 모니터링할지를 결정할 때에는 일반적으로 모니터링할 포트를 지정하거나 구축에서 애플리케이션 프로토콜을 지정합니다.

그러나, 포트 또는 애플리케이션 프로토콜을 지정하는 것은 FTP 트래픽의 민감한 데이터를 탐지하는 데 충분하지 않습니다. FTP 트래픽 내 민감한 데이터가 FTP 애플리케이션 프로토콜의 트래픽에서 발견되는 일이 간헐적으로 발생하는데, 일시적 포트 번호를 사용하여 탐지하는 것을 어렵게 만듭니다. FTP 트래픽에서 민감한 데이터를 검색하려면 반드시 구성에 다음을 포함해야 합니다.

- FTP 트래픽에서 민감한 데이터 탐지를 활성화하려면 `FTP data` 애플리케이션 프로토콜을 지정합니다.

  FTP 트래픽에서 민감한 데이터를 탐지하는 특정 케이스의 경우 `FTP data` 애플리케이션 프로토콜을 지정해도 탐지되지 않습니다. 대신, 이는 FTP/텔넷 처리기의 신속한 처리를 통해 FTP 트래픽에서 민감한 데이터를 탐지하도록 합니다.

- FTP Data 탐지기(기본적으로 활성화됨)가 활성화되었는지 확인합니다.
- 민감한 데이터에 대해 모니터링하는 최소 1개의 포트가 구성에 포함되어 있는지 확인합니다.

FTP 트래픽에서 민감한 데이터에 대해 탐지만 원하는 가능성이 낮은 경우를 제외하면 FTP 포트를 지정할 필요가 없다는 점에 유의하십시오. 대부분의 민감한 데이터 구성은 HTTP 또는 이메일 포트와 같은 다른 포트를 포함합니다. 모니터링을 위해 1개의 FTP 포트만 지정하고 다른 포트는 지정하지 않을 경우, Cisco는 FTP 명령 포트 23을 지정할 것을 권장합니다.

관련 항목

FTP/텔넷 디코더, 2244 페이지
탐지기 활성화 및 비활성화, 2456 페이지
민감한 데이터 탐지 구성, 2048 페이지

맞춤형 민감한 데이터 유형

맞춤형 데이터 유형을 생성할 때마다 생성기 ID(GID) 138과 1000000 이상의 Snort ID(SID), 즉 로컬 규칙의 SID를 갖는 단일한 민감한 데이터 전처리기 규칙도 생성됩니다.

연결된 민감한 데이터 규칙을 활성화하여 정책에서 사용할 각 맞춤형 데이터 유형에 대한 탐지 및 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.을 활성화해야 합니다.

민감한 데이터 규칙의 활성화에 도움이 되도록 구성 페이지의 링크를 통해 모든 시스템 제공 및 맞춤형 민감한 데이터 규칙을 표시하는 침입 정책 Rules(규칙) 페이지의 필터링된 보기로 이동할 수 있습니다. 또한 침입 정책 Rules(규칙) 페이지에서 로컬 필터링 카테고리를 선택하여 모든 로컬 맞춤형 지정 규칙과 함께 맞춤형 민감한 데이터 규칙을 표시할 수 있습니다. 맞춤형 민감한 데이터 규칙은 규칙 편집기 페이지(**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**)에 나열되지 않습니다.

생성한 맞춤형 데이터 유형은 시스템의 모든 침입 정책 또는 다중 도메인 구축의 경우에는 현재 도메인에서 활성화할 수 있습니다. 맞춤형 데이터 유형을 활성화하려면 해당 맞춤형 데이터 유형 탐지에 사용할 정책에서 연결된 민감한 데이터 규칙을 활성화해야 합니다.

맞춤형 민감한 데이터 유형의 데이터 패턴

다음으로 구성된 정규식 단순 집합을 사용하여 사용자 지정 데이터 유형에 대한 데이터 패턴을 정의합니다.

- 3개의 메타 문자
- 메타 문자를 문자로 사용할 수 있도록 하는 이스케이프된 문자
- 6개의 문자 클래스

메타 문자는 정규 표현식에서 특정 의미가 있는 리터럴 문자입니다.

표 ***143:*** 민감한 데이터 패턴 메타 문자

메타 문자	설명	예
?	앞선 문자 또는 이스케이프 시퀀스에 0회 또는 1회 발생에 일치합니다. 즉, 앞선 문자 또는 이스케이프 시퀀스는 선택 사항입니다.	colou?r는 color 또는 colour에 일치합니다.
{n}	앞선 문자 또는 이스케이프 시퀀스에 n회 일치합니다.	예를 들어\d{2}는 55, 12 등과 일치하고, \l{3}은 AbC, www 등과 일치하며, \w{3}은 a1B, 25C 등과 일치하고, x{5}는 xxxxx와 일치합니다.
\	메타 문자를 실제 문자로 사용할 수 있으며, 미리 정의된 문자 클래스를 지정하는 데 사용할 수도 있습니다.	\?는 물음표와 일치하고, \\는 백슬래시에 일치하며, \d는 숫자 등과 일치합니다.

민감한 데이터 전처리기가 일부 문자를 리터럴 문자로 정확하게 해석하려면 백슬래시를 사용하여 해당 문자를 이스케이프해야 합니다.

표 ***144:*** 이스케이프된 민감한 데이터 패턴 문자

사용할 이스케이프된 문자	나타낼 문자
\?	?
\{	{
\}	}
\\	\

맞춤형 민감한 데이터 패턴을 정의할 때 문자 클래스를 사용할 수 있습니다.

표 ***145:*** 민감한 데이터 패턴 문자 클래스

문자 클래스	설명	문자 클래스 정의
\d	모든 숫자 ASCII 문자 0-9와 일치합니다.	0-9
\D	숫자 ASCII 문자가 아닌 모든 바이트와 일치합니다.	0-9 아님
\l(소문자 “ell")	모든 ASCII 문자와 일치합니다.	a-zA-Z
\L	ASCII 문자가 아닌 모든 바이트와 일치합니다.	a-zA-Z 아님

문자 클래스	설명	문자 클래스 정의
\w	모든 ASCII 영숫자 문자와 일치합니다. PCRE 정규식과는 달리, 이는 밑줄(_)을 포함하지 않는다는 점에 유의하십시오.	a-zA-Z0-9
\W	ASCII 영숫자 문자가 아닌 모든 바이트와 일치합니다.	a-zA-Z0-9 아님

전처리기는 직접 입력한 문자를 정규식의 일부 대신 문자로 처리합니다. 예를 들어, 데이터 패턴 1234는 `1234`에 일치합니다.

다음 데이터 패턴 예제는 시스템이 제공한 민감한 데이터 규칙 138:4에서 사용되는데, 미국 전화 번호를 검색하기 위해 이스케이프된 디지트 문자 클래스, 승수 및 옵션 지정자 메타 문자, 그리고 문자 대시(-) 및 좌우 괄호() 문자를 사용합니다.

```
(\d{3}) ?\d{3}-\d{4}
```

사용자 지정 데이터 패턴을 만들 때 주의를 기울이십시오. 올바른 구문을 사용하지만 많은 잘못된 긍정을 야기할 수도 있는 전화 번호 탐지를 위해 다음 데이터 패턴을 고려하십시오.

```
(?\d{3})? ?\d{3}-?\d{4}
```

두 번째 예제는 괄호(선택 사항), 스페이스(선택 사항) 및 대시(선택 사항)를 조합하므로 다음과 같은 원하는 패턴의 전화 번호를 탐지합니다.

- `(555)123-4567`
- `555123-4567`
- `5551234567`

그러나, 두 번째 예제 패턴은 또한 잘못된 긍정을 야기하는 다음과 같은 유효하지 않은 잠재적인 패턴을 탐지합니다.

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

마지막으로 이해를 돕기 위해 소규모 회사 네트워크에서 모든 대상 트래픽의 낮은 이벤트 임계값을 사용하여 소문자 `a`를 탐지하는 데이터 패턴을 생성하는 극단적인 예를 고려하십시오. 이러한 데이터 패턴은 단지 몇 분 만에 사용자 시스템을 수백 만개의 이벤트로 마비시킬 수 있습니다.

맞춤형 민감한 데이터 유형 설정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 민감한 데이터 유형을 표시하며, 이 데이터 유형은 수정할 수 있습니다. 상위 도메인에서 생성된 데이터 유형도 표시되며, 이 데이터 유형은 제

한적 방법으로 수정할 수 있습니다. 상위 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

침입 정책에서 데이터 유형에 대한 민감한 데이터 규칙이 활성화된 경우에는 해당 데이터 유형을 삭제할 수 없습니다.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Data Types(**데이터 유형**)** 옆에 있는 추가( )를 클릭합니다.

단계 **7** 데이터 유형의 이름을 입력합니다.

단계 **8** 이 데이터 유형으로 탐지할 패턴을 입력합니다(맞춤형 민감한 데이터 유형의 데이터 패턴, 2052 페이지 참조).

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** 원하는 경우, 데이터 유형 이름을 클릭하고 개별 민감한 데이터 유형 옵션, 2045 페이지에 설명된 옵션을 수정합니다.

단계 **11** 필요에 따라 삭제( )를 클릭하여 사용자 지정 데이터 유형을 삭제한 다음 **OK(**확인**)**를 클릭하여 확인합니다.

참고 침입 정책에서 해당 데이터 유형에 대한 민감한 데이터 규칙이 활성화된 경우에는 해당 데이터 유형을 삭제할 수 없다고 시스템이 경고합니다. 삭제를 다시 시도하려면 먼저 영향을 받는 정책에서 민감한 데이터 규칙을 비활성화해야 합니다(침입 규칙 상태 설정, 2024 페이지 참조).

단계 **12** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 해당 데이터 유형을 사용하려는 각 정책에서 연결된 맞춤형 민감한 데이터 전처리 규칙을 활성화합니다(침입 규칙 상태 설정, 2024 페이지 참조).

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

맞춤형 민감한 데이터 유형 수정, 2056 페이지

맞춤형 민감한 데이터 유형 수정

맞춤형 민감한 데이터 유형의 모든 필드를 편집할 수 있습니다. 하지만 이름 또는 패턴 필드를 수정하는 경우, 시스템의 모든 침입 정책에서 이러한 설정이 변경됩니다. 다른 옵션은 정책별 값으로 설정할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 민감한 데이터 유형을 표시하며, 이 데이터 유형은 수정할 수 있습니다. 상위 도메인에서 생성된 데이터 유형도 표시되며, 이 데이터 유형은 제한적 방법으로 수정할 수 있습니다. 상위 데이터 유형의 경우, 이름 및 패턴 필드가 읽기 전용으로 표시되지만 다른 옵션은 정책별 값으로 설정할 수 있습니다.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Sensitive Data Detection(**민감한 데이터 탐지**)**이 비활성화되었다면 **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Sensitive Data Detection(**민감한 데이터 탐지**)** 옆에 있는 **Edit(**편집**)**를 클릭 합니다.

단계 **6** **Targets(**대상**)** 섹션에서 맞춤형 데이터 유형의 이름을 클릭합니다.

단계 **7** **Edit Data Type Name and Pattern(**데이터 유형 이름 및 패턴 수정**)**을 클릭합니다.

단계 **8** 데이터 유형 이름 및 패턴을 수정합니다(맞춤형 민감한 데이터 유형의 데이터 패턴, 2052 페이지 참조).

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** 나머지 옵션은 정책별 값으로 설정합니다(개별 민감한 데이터 유형 옵션, 2045 페이지 참조).

단계 **11** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 탐색창에서 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

84 장

침입 이벤트 로깅 글로벌 제한

다음 주제에서는 침입 이벤트 로깅을 전역 제한하는 방법을 설명합니다.

- 전역 규칙 임계값 기본 사항, 2057 페이지
- 전역 규칙 임계값 옵션, 2058 페이지
- 전역 임계값에 대한 라이선스 요건, 2060 페이지
- 전역 임계값 요구 사항 및 사전 요건, 2060 페이지
- 전역 임계값 구성, 2061 페이지
- 전역 임계값 비활성화, 2062 페이지

전역 규칙 임계값 기본 사항

전역 규칙 임계값은 침입 정책에 의한 이벤트 로깅에 대해 제한을 설정합니다. 모든 트래픽에 해당되는 글로벌 규칙 임계값을 설정하여 정책이 지정된 기간당 특정 소스 또는 대상의 이벤트를 로깅하고 표시하는 빈도를 제한할 수 있습니다. 또한, 정책에서 공유 객체 규칙, 표준 텍스트 규칙 또는 전처리기 규칙당 임계값도 설정할 수 있습니다. 글로벌 임계값을 설정하면 해당 임계값은 정책 내에서 특정 임계값을 재정의하지 않는 각 규칙에 적용됩니다. 임계값을 사용하면 이벤트 수가 너무 많아서 혼란스러워지는 상황을 피할 수 있습니다.

각 침입 정책은 모든 침입 규칙 및 전처리기 규칙에 기본적으로 적용되는 기본 글로벌 규칙 임계값을 포함합니다. 이 기본 임계값은 대상에 방문하는 트래픽의 이벤트 수를 60초당 하나로 제한합니다.

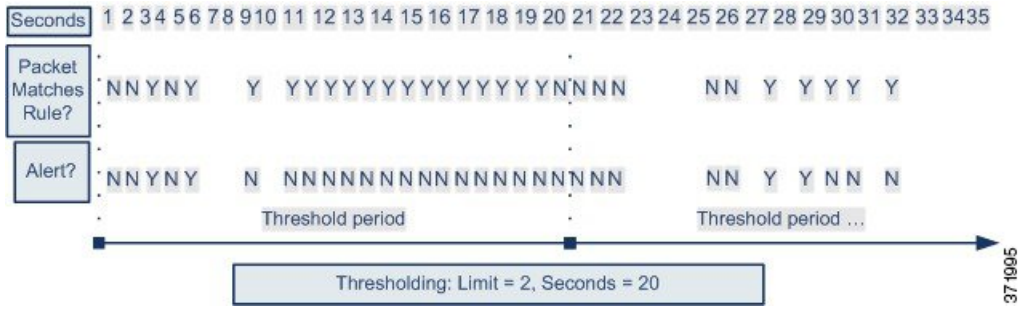
다음 작업을 수행할 수 있습니다.

- 전역 임계값을 변경합니다.
- 전역 임계값을 비활성화합니다.
- 특정 규칙의 개별 임계값을 설정하여 전역 임계값을 재정의합니다.

  예를 들어 전역 제한 임계값은 60초당 이벤트 5회이지만, SID 1315에 대해서는 60초당 이벤트 10회의 특정 임계값을 설정할 수 있습니다. 다른 모든 규칙은 60초당 생성되는 이벤트가 5회를 넘지 않지만 SID 1315의 경우, 시스템은 60초당 이벤트를 최대 10회 생성합니다.

팁 다중 CPU를 가진 매니지드 디바이스에서 전역 또는 개별 임계값은 예상보다 많은 수의 이벤트를 야기할 수 있습니다.

다음 다이어그램은 전역 규칙 임계값 설정의 작동 방식을 보여줍니다. 이 예에서는 공격이 특정 규칙에 대해 진행 중입니다. 전역 제한 임계값은 각 규칙의 이벤트 생성을 20초당 2회로 제한하도록 설정되어 있습니다. 기간은 1초에 시작하여 21초에 끝납니다. 기간이 끝나면 주기가 다시 시작되고 다음 두 규칙 일치가 이벤트를 생성하며, 시스템은 해당 기간 중에 더 이상 이벤트를 생성하지 않습니다.



전역 규칙 임계값 옵션

기본 임계값은 각 규칙에 대한 이벤트 생성을 동일한 대상으로 향하는 트래픽에서 매 60초당 하나의 이벤트로 제한합니다. 전역 규칙 임계값 설정 옵션의 기본값은 다음과 같습니다.

- **Type(**유형**)** — 제한
- **Track By(**추적 방법**)** — 대상
- **Count(**카운트**)** — 1
- **Seconds(**초**)** — 60

이러한 기본값은 다음과 같이 수정할 수 있습니다.

표 ***146:*** 임계값 설정 유형

옵션	설명
Limit(제한)	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(count 인수로 지정)에 대한 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Limit(**제한**)**로, **Count(**카운트**)**는 `10`으로, 그리고 **Seconds(**초**)**는 `60`으로 설정하고 14개의 패킷이 규칙을 트리거하는 경우, 시스템은 동일한 시간(분) 내 발생한 첫 10개의 패킷을 표시한 후 규칙의 이벤트 로깅을 중단합니다.

옵션	설명
Threshold(임계값)	지정된 기간 중 지정된 패킷 수(count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅하고 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅하면 시간에 대한 카운터가 다시 시작됩니다. 예를 들어, 유형은 **Threshold(**임계값**)**로, **Count(**카운트**)**는 10으로, 그리고 **Seconds(**초**)**는 60으로 설정하면 규칙은 33초에 10번 트리거됩니다. 시스템은 하나의 이벤트를 생성한 다음, Seconds(초) Count(카운트) 카운터를 0으로 재설정합니다. 그런 다음 규칙은 다음 25초 안에 다시 10번 트리거됩니다. 33초에 카운터가 0으로 재설정되므로 시스템은 또 다른 이벤트를 로깅합니다.
Both(모두)	지정된 수(카운트)의 패킷이 규칙을 트리거한 후 특정 시기 동안 한 번에 하나의 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Both(**모두**)**로, **Count(**카운트**)**는 2로, 그리고 **Seconds(**초**)**는 10으로 설정하면, 다음 이벤트가 결과를 카운트합니다. • 규칙이 10초 안에 한 번 트리거되는 경우, 시스템은 어떤 이벤트도 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초 안에 두 번 트리거되는 경우, 시스템은 하나의 이벤트를 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

Track By(추적 기준**)** 옵션은 이벤트 인스턴스 카운트가 소스 IP 주소별로 계산되는지 대상 IP 주소별로 계산되는지 결정합니다.

다음과 같이 임계값을 정의하는 인스턴스 수와 기간도 지정할 수 있습니다.

표 ***147:*** 임계값 설정 인스턴스/시간 옵션

옵션	설명
Count	**Limit(**제한**)** 임계값의 경우, 임계값 충족에 필요한 IP 주소 또는 주소 범위 추적별로 지정된 기간별 이벤트 인스턴스의 수. **Threshold(**임계값**)** 임계값의 경우, 임계값으로 사용할 규칙 일치의 수.

옵션	설명
Seconds	**Limit** 임계값의 경우, 공격이 추적되는 기간을 구성하는 초 단위의 시간. **Threshold** 임계값의 경우, 카운트가 재설정되기까지 경과하는 초 단위의 시간. 임계값 유형을 **Limit(**제한**)**로, 추적을 **Source(**소스**)**로, **Count(**카운트**)**를 10으로, 그리고 **Seconds(**초**)**를 10으로 설정한 경우, 시스템은 주어진 소스 포트에서 10초 안에 발생한 첫 10개의 이벤트를 로깅하고 표시합니다. 첫 10초 안에 일곱 개의 이벤트만 발생한 경우, 시스템은 이를 모두 로깅하고 표시하며, 첫 10초 안에 40개의 이벤트가 발생한 경우, 시스템은 10개를 로깅하고 표시한 후, 10초의 시간이 경과한 시점에서 다시 카운팅을 시작합니다.

관련 항목

전역 임계값 구성, 2061 페이지
침입 이벤트 임계값, 2025 페이지

전역 임계값에 대한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

전역 임계값 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

전역 임계값 구성

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Intrusion Rule Thresholds(**침입 규칙 임계값**)**에서 **Global Rule Thresholding(**전역 규칙 임계값 설정**)**이 비활성화된 경우, **Enabled(**활성화**)**를 클릭합니다.

단계 **5** **Global Rule Thresholding(**전역 규칙 임계값**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Type(**유형**)**을 사용하여 **Seconds(**초**)** 필드에서 지정하는 시간 동안 적용할 임계값 유형을 지정합니다.

단계 **7** **Track By(**추적 기준**)**을 사용하여 추적 방법을 지정합니다.

단계 **8** **Count(**카운트**)** 필드에 값을 입력합니다.

단계 **9** **Seconds(**초**)** 필드에 값을 입력합니다.

단계 **10** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

전역 규칙 임계값 옵션, 2058 페이지
레이어에서 침입 규칙 구성, 1990 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

전역 임계값 비활성화

임계값 설정을 모든 규칙에 기본적으로 적용하지 않고 특정 규칙에 대한 이벤트 임계값을 설정하려는 경우, 최상위 정책 레이어에서 전역 임계값 설정을 비활성화할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 선택 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **4** **Intrusion Rule Thresholds(**침입 규칙 임계값**)** 아래 **Global Rule Thresholding(**전역 규칙 임계값 설정**)** 옆에서 **Disabled(**비활성화**)**를 클릭합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지
레이어에서 침입 규칙 구성, 1990 페이지

85 장

침입 규칙 편집기

다음 주제에서는 침입 규칙 편집기를 사용하는 방법을 설명합니다.

- 침입 규칙 수정 소개, 2063 페이지
- 침입 규칙 편집기 라이선스 요구 사항, 2064 페이지
- 침입 규칙 편집기 요구 사항 및 사전 요건, 2064 페이지
- 규칙 구조, 2065 페이지
- 맞춤형 규칙 생성, 2077 페이지
- 규칙 검색, 2083 페이지
- 침입 규칙 편집기 페이지에서 규칙 필터링, 2085 페이지
- 침입 규칙의 키워드 및 인수, 2088 페이지

침입 규칙 수정 소개

침입 규칙은 시스템이 네트워크에서 취약성을 익스플로잇하려는 시도를 탐지하는 데 사용하는 키워드와 인수의 집합입니다. 시스템은 네트워크 트래픽을 분석하면서 패킷을 각 규칙에 지정된 조건과 비교합니다. 패킷 데이터가 규칙에 지정된 모든 조건과 일치하는 경우, 규칙이 트리거됩니다. 규칙이 알림 규칙인 경우, 침입 이벤트를 생성합니다. 규칙이 전달 규칙인 경우, 트래픽을 무시합니다. 인라인 구축의 삭제 규칙의 경우, 시스템은 패킷을 삭제하고 이벤트를 생성합니다. Firepower Management Center 웹 인터페이스에서 침입 이벤트를 보고 평가할 수 있습니다.

Firepower System은 공유 개체 규칙과 표준 텍스트 규칙이라는 두 가지 유형의 침입 규칙을 제공합니다. Cisco Talos Intelligence Group(Talos)는 공유 개체 규칙을 사용하여 기존의 표준 텍스트 규칙에서는 불가능한 방식으로 취약성에 대한 공격을 탐지할 수 있습니다. 공유 객체 규칙은 생성할 수 없습니다. 자체 침입 규칙을 작성하는 경우, 표준 텍스트 규칙을 생성합니다.

맞춤형 표준 텍스트 규칙을 작성하여 보게 될 이벤트 유형을 조정할 수 있습니다. 이 설명서는 특정 익스플로잇 탐지를 목표로 하는 규칙을 설명하고 있지만, 가장 성공적인 규칙은 알려진 특정 익스플로잇보다는 알려진 취약성을 공격하려고 시도하는 트래픽을 대상으로 합니다. 규칙을 작성하고 규칙의 이벤트 메시지를 지정하여, 공격 및 정책 회피를 나타내는 트래픽을 더욱 쉽게 확인할 수 있습니다.

사용자 지정 침입 정책에서 사용자 지정 표준 텍스트 규칙을 활성화하는 경우, 트래픽이 특정 방법으로 먼저 디코딩 또는 전처리되는 것을 일부 규칙 키워드 및 인수가 요구한다는 점에 유의하십시오.

이 챕터에서는 전처리를 제어하는 네트워크 분석 정책에서 구성해야 하는 옵션을 설명합니다. 필수 전처리기를 비활성화하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

주의 제어 네트워크 환경을 사용하여 프로덕션 환경에서 규칙을 사용하기 전에 작성하는 모든 침입 규칙을 테스트하도록 하십시오. 잘못 작성한 침입 규칙은 시스템의 성능에 심각한 영향을 줄 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 규칙을 표시하며 이러한 규칙은 수정할 수 있습니다. 상위 도메인에서 생성된 규칙도 표시되지만, 이러한 규칙은 수정할 수 없습니다. 하위 도메인에서 생성된 규칙을 보고 수정하려면 해당 도메인으로 전환하십시오. 시스템 제공 침입 규칙은 전역 도메인에 속합니다. 하위 도메인의 관리자는 이러한 시스템 규칙의 편집 가능한 로컬 복사본을 만들 수 있습니다.

침입 규칙 편집기 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

침입 규칙 편집기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

규칙 구조

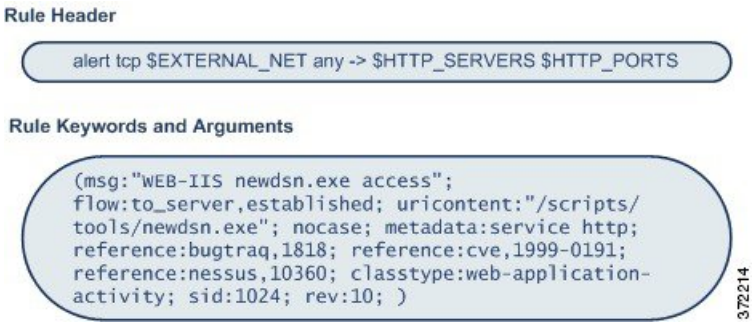
모든 표준 텍스트 규칙은 두 개의 논리적 섹션인 규칙 헤더 및 규칙 옵션을 포함합니다. 규칙 헤더에는 다음이 포함됩니다.

- 규칙의 상태 또는 유형
- 프로토콜
- 소스와 대상 IP 주소 및 넷마스크
- 소스에서 대상에 이르는 트래픽의 흐름을 보여 주는 방향 표시기
- 소스 및 대상 포트

규칙 옵션 섹션에는 다음이 포함됩니다.

- 이벤트 메시지
- 키워드와 매개 변수 및 인수
- 규칙을 트리거하기 위해 패킷 페이로드가 일치해야 하는 패턴
- 규칙 엔진이 패킷의 어느 부분을 검사해야 하는지에 관한 설명서

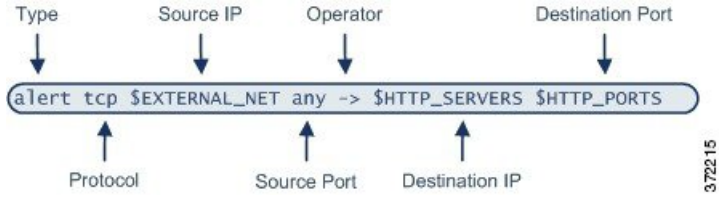
다음 다이어그램은 규칙의 일부를 설명합니다.



규칙의 옵션 섹션은 괄호로 둘러싸인 섹션이라는 점에 유의하십시오. 침입 규칙 편집기는 표준 텍스트 규칙을 구축할 수 있도록 사용하기 쉬운 인터페이스를 제공합니다.

침입 규칙 헤더

모든 표준 텍스트 규칙 및 공유 개체 규칙에는 매개변수와 인수를 포함하는 규칙 헤더가 있습니다. 다음은 규칙 헤더의 일부를 설명합니다.



다음 표는 위에 표시된 규칙 헤더의 각 부분을 나타냅니다.

표 ***148:*** 규칙 헤더 값

규칙 헤더 구성 요소	예제 값	값
작업	`Alert(긴급 경고)`	침입 이벤트가 트리거되면 이를 생성합니다.
프로토콜	`tcp`	TCP 트래픽만 테스트합니다.
소스 IP 주소	`$EXTERNAL_NET`	내부 네트워크에 없는 모든 호스트에서 나오는 트래픽을 테스트합니다.
소스 포트	`any`	시작 호스트의 모든 포트에서 나오는 트래픽을 테스트합니다.
연산자	`->`	(네트워크 웹 서버로 가는) 외부 트래픽을 테스트합니다.
대상 IP 주소	`$HTTP_SERVERS`	내부 네트워크에서 웹 서버로 지정된 모든 호스트에 인도되는 트래픽을 테스트합니다.
대상 포트	`$HTTP_PORTS`	내부 네트워크에서 HTTP 포트에 인도되는 트래픽을 테스트합니다.

참고 이전 예제는 대부분의 침입 규칙과 같이 기본 변수를 사용합니다.

관련 항목

변수 집합, 580 페이지

침입 규칙 헤더 작업

각 규칙 헤더는 패킷이 규칙을 트리거할 때 시스템이 취할 작업을 지정하는 매개 변수를 포함합니다. 경고로 설정된 작업을 가진 규칙은 규칙을 트리거한 패킷에 대해 침입 이벤트를 생성하고 해당 패킷의 세부 사항을 로깅합니다. 통과로 설정된 작업을 가진 규칙은 규칙을 트리거한 패킷에 대해 이벤트를 생성하거나 해당 패킷의 세부 사항을 로깅하지 않습니다.

참고 인라인 배포에서 *Drop and Generate Events(*이벤트 삭제 및 생성*)*로 설정된 상태의 규칙은 규칙을 트리거한 패킷에 대해 침입 이벤트를 생성합니다. 또한 수동 배포에서 삭제 규칙을 적용할 경우, 규칙은 알림 규칙으로 작동합니다.

기본적으로, 통과 규칙은 경고 규칙을 대체합니다. 특정 상황에서 경고 규칙을 비활성화하는 대신 알림 규칙을 트리거하여 전달 규칙에 정의된 기준을 충족하는 패킷을 방지하는 전달 규칙을 만들 수 있습니다. 예를 들어, "익명" 사용자로 FTP 서버에 로그인을 시도하는 규칙이 활성 상태로 유지되기를 원할 수 있습니다. 하지만, 네트워크에 하나 이상의 적정 익명 FTP 서버가 있는 경우, 특정 서버의 경우, 익명 사용자는 원래 규칙을 트리거하지 않도록 지정하는 규칙을 작성하고 활성화할 수 있습니다.

침입 규칙 편집기 내 **Action(**작업**)** 목록에서 규칙 유형을 선택합니다.

침입 규칙 헤더 프로토콜

각 규칙 헤더에서, 규칙이 검사하는 트래픽의 프로토콜을 지정해야 합니다. 분석을 위해 다음 네트워크 프로토콜을 지정할 수 있습니다.

- ICMP(Internet Control Message Protocol)
- IP(인터넷 프로토콜)

  참고 프로토콜이 `ip`로 설정되면 시스템은 침입 규칙 헤더의 포트 정의를 무시합니다.

- TCP(Transmission Control Protocol)
- UDP(User Datagram Protocol)

IP를 프로토콜 유형으로 사용하여 TCP, UDP, ICMP, IGMP 및 더 많은 수를 포함하는 IANA에 의해 할당된 모든 프로토콜을 검토합니다.

참고 지금은 IP 페이로드에서 다음 헤더(예를 들어, TCP 헤더)의 패턴과 일치하는 규칙을 작성할 수 없습니다. 대신, 일치하는 콘텐츠는 마지막 디코딩된 프로토콜과 함께 시작됩니다. 해결 방법으로, 규칙 옵션을 사용하여 TCP 헤더에서 패턴을 일치시킬 수 있습니다.

침입 규칙 편집기 내 **Protocol(**프로토콜**)** 목록에서 프로토콜 유형을 선택합니다.

관련 항목

침입 규칙 헤더 프로토콜, 2067 페이지

침입 규칙 헤더 방향

규칙 헤더 내에서, 규칙이 패킷을 검사할 수 있도록 패킷이 이동해야 하는 방향을 지정할 수 있습니다. 다음 표는 이러한 옵션에 대해 설명합니다.

표 ***149:*** 규칙 헤더의 방향 옵션

사용 환경	테스트 대상
방향	특정 소스 IP 주소에서 특정 대상 IP 주소로 이동하는 트래픽에 한정
양방향	특정 소스 및 대상 IP 주소 간에 이동하는 모든 트래픽

침입 규칙 헤더 소스 및 대상 **IP** 주소

특정 IP 주소에서 시작하거나 특정 IP 주소를 대상으로 한 패킷 검사를 제한하면 시스템이 실행해야 하는 패킷 검사량이 줄어듭니다. 이는 또한 규칙을 보다 구체적으로 만들고 소스와 대상 IP 주소가 의심스러운 작업을 표시하지 않는 패킷에 대해 트리거된 규칙 가능성을 제거하여 잘못된 긍정을 줄입니다.

팁 시스템은 IP 주소만 인식하고 소스 또는 대상 IP 주소의 호스트 이름을 수락하지 않습니다.

규칙 편집기의 **Source IPs(**소스 **IP)** 및 **Destination IPs(**대상 **IP)** 필드에서 소스 및 대상 IP 주소를 지정합니다.

표준 텍스트 규칙을 작성할 때 필요에 따라 다양한 방법으로 IPv4 및 IPv6 주소를 지정할 수 있습니다. 단일 IP 주소, `any`(모두), IP 주소 목록, CIDR 표기법, 프리픽스 길이 또는 네트워크 변수를 지정할 수 있습니다. 또한, 특정 IP 주소 또는 IP 주소의 집합을 제외할지 여부를 나타낼 수 있습니다. IPv6 주소를 지정할 때, RFC 4291에 정의된 주소 지정 규칙을 사용할 수 있습니다.

침입 규칙 내 **IP** 주소 구문

다음 표에서는 소스 및 대상 IP 주소를 지정할 수 있는 다양한 방법을 요약합니다.

표 ***150:*** 소스**/**대상 ***IP*** 주소 구문

지정 대상	사용 환경	예
모든 IP 주소	`any`	`any`
특정 IP 주소	해당 IP 주소 동일한 규칙에서 IPv4 및 IPv6 소스와 대상 주소를 혼용하지 않는다는 점에 유의하십시오.	`192.168.1.1` `2001:db8::abcd`
IP 주소 목록	IP 주소를 둘러싸는 괄호(`[]`) 및 IP 주소를 구분하는 쉼표	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`

지정 대상	사용 환경	예
IP 주소 블록	IPv4 CIDR 블록 또는 IPv6 주소 접두사 코멘트	`192.168.1.0/24` `2001:db8::/32`
특정 IP 주소 또는 주소 집합을 제외한 모든 주소	IP 주소 또는 무효화를 원하는 주소 앞에 있는 `!` 문자	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
하나 이상의 특정 IP 주소를 제외한 IP 주소의 블록 내 모든 주소	무효화된 주소 또는 블록 목록이 뒤따르는 주소 블록	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
네트워크 변수에 정의된 IP 주소	`$`로 시작하는 대문자로 된 변수 이름 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다.	`$HOME_NET`
IP 주소 변수에 의해 정의된 주소를 제외한 모든 IP 주소	`!$`로 시작하는 대문자로 된 변수 이름	`!$HOME_NET`

다음 설명은 일부 IP 주소 입력 방법에 대한 추가 정보를 제공합니다.

모든 **IP** 주소

모든 IPv4 또는 IPv6 주소를 나타내는 규칙 소스 또는 대상 IP 주소로 `any`라는 단어를 지정할 수 있습니다.

예를 들어, 다음 규칙은 **Source IPs(**소스 **IP)** 및 **Destination IPs(**대상 **IP)** 필드의 인수 **any**를 사용하며 모든 IPv4 또는 IPv6 소스와 대상 주소로 패킷을 평가합니다.

```
alert tcp any any -> any any
```

또한 `::`을 지정하여 모든 IPv6 주소를 나타낼 수 있습니다.

여러 **IP** 주소

IP 주소를 쉼표로 구분하여 개별 IP 주소를 나열할 수 있습니다. 원하는 경우, 다음 예에 나온 것처럼 부정되지 않은 목록을 대괄호로 감쌀 수도 있습니다.

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4와 IPv6는 다음의 예시에서처럼 개별적으로 또는 조합하여 나열할 수 있습니다.

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

이전 소프트웨어 릴리스에서는 괄호로 IP 주소 목록을 포함하는 것이 필요하지만 여기서는 필요하지 않다는 점에 유의하십시오. 선택 사항으로, 각 쉼표 앞이나 뒤에 스페이스로 목록을 입력할 수 있다는 점도 참고하십시오.

참고 무효화된 목록을 괄호로 묶어야 합니다.

또한 IPv4 CIDR(Classless Inter-Domain Routing: 클래스리스 도메인 간 라우팅) 표기법 또는 IPv6 프리픽스 길이를 사용하여 주소 블록을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- 192.168.1.0/24는 서브넷 마스크 255.255.255.0, 즉, 192.168.1.255를 통한 192.168.1.0으로 192.168.1.0 네트워크에서 IPv4 주소를 지정합니다.
- 2001:db8::/32는 2001:db8:: 네트워크에서 32비트의 접두사 길이로 IPv6 주소를 지정하는데, 이는, 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff를 통한 2001:db8::입니다.

팁 IP 주소 블록을 지정해야 하지만 CIDR 또는 접두사 길이 표기를 사용하여 이를 표시할 수 없는 경우, CIDR 블록 및 IP 주소 내 접두사 길이를 사용할 수 있습니다.

IP 주소 부정

느낌표(!)를 사용하여 지정된 IP 주소를 무효화할 수 있습니다. 즉, 지정된 IP 주소 또는 주소를 제외한 모든 IP 주소와 일치할 수 있습니다. 예를 들어, `! 192.168.1.1`은 192.168.1.1 이외의 모든 IP 주소를 지정하고, `! 2001: db8: ca2e:: fa4c`는 2001: db8: ca2e:: fa4c. 이외의 모든 IP 주소를 지정합니다.

IP 주소 목록을 무효화하려면 괄호로 묶은 IP 주소의 목록 앞에 !를 표시하십시오. 예를 들어, `![192.168.1.1,192.168.1.5]`는 192.168.1.1 또는 192.168.1.5. 이외의 모든 IP 주소를 정의합니다.

참고 IP 주소 목록을 무효화하기 위해서는 괄호를 사용해야 합니다.

IP 주소 목록과 함께 무효화 문자를 사용할 때는 주의하십시오. 예를 들어, 192.168.1.1 또는 192.168.1.5가 아닌 모든 주소를 일치시키기 위해 `[!192.168.1.1,!192.168.1.5]`를 사용하는 경우,시스템은 이 구문을 "192.168.1.1이 아닌 모든 주소, 또는 192.168.1.5가 아닌 모든 주소"로 해석합니다.

192.168.1.5는 192.168.1.1이 아니고 192.168.1.1은 192.168.1.5가 아니므로, 두 IP 주소 모두 IP 주소 `[!192.168.1.1,!192.168.1.5]` 값에 일치하며, 이는 본질적으로 "`any(모두)`"를 사용하는 것과 동일합니다.

이보다는 `![192.168.1.1,192.168.1.5]`를 사용하십시오. 시스템은 이를 "192.168.1.1이 아니며 192.168.1.5도 아닌 주소"로 해석하며, 이는 괄호 사이에 나열된 IP 주소를 제외한 모든 IP 주소에 일치하는 것입니다.

논리적으로 `any(모두)`와 무효화를 함께 사용할 수 없다는 점에 유의하십시오. 함께 사용하는 경우 무효화되면 어떤 주소도 나타내지 못하게 됩니다.

관련 항목

변수 집합, 580 페이지

침입 규칙 헤더 소스 및 대상 포트

규칙 편집기의 **Source Port(**소스 포트**)** 및 **Destination Port(**대상 포트**)** 필드에서 소스 포트와 대상 포트를 지정합니다.

침입 규칙 내 포트 구문

Firepower System은 규칙 헤더에 사용되는 포트 번호를 정의하기 위해 특정 유형의 구문을 사용합니다.

참고 프로토콜이 `ip`로 설정되면 시스템은 침입 규칙 헤더의 포트 정의를 무시합니다.

다음의 예시에서와 같이 쉼표로 포트를 구분하여 나열할 수 있습니다.

```
80, 8080, 8138, 8600-9000, !8650-8675
```

또는, 다음의 예시는 괄호로 포트 목록을 묶는 방법을 보여주는데, 이는 이전의 소프트웨어 버전에서는 필요했지만 더 이상 필요하지 않습니다.

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

다음의 예시에서처럼 무효화된 포트 목록을 반드시 괄호로 묶어야 한다는 점에 유의하십시오.

```
![20, 22, 23]
```

다음 표는 사용 가능한 구문을 요약한 것입니다.

표 ***151:*** 소스/대상 포트 구문

지정 대상	사용 환경	예
모든 포트	`any`	`any`
특정 포트	포트 번호	`80`
포트 범위	범위 내 첫 번째 및 마지막 포트 번호 사이의 대시	`80-443`
특정 포트보다 작거나 같은 모든 포트	포트 번호 앞의 대시	`-21`
특정 포트보다 같거나 큰 모든 포트	포트 번호 다음의 대시	`80-`

지정 대상	사용 환경	예
특정 포트 또는 특정 범위의 포트를 제외한 모든 포트	무효화를 원하는 포트, 포트 목록 또는 범위의 포트 앞의 !문자 논리적으로는 any(모두)를 제외한 모든 포트 지정에 부정을 사용할 수 있다는 점에 유의하십시오. any가 부정되는 경우에는 *no port(*포트 없음*)*가 표시됩니다.	`!20`
포트 변수에 의해 정의된 모든 포트	$로 시작하는 대문자로 된 변수 이름	`$HTTP_PORTS`
포트 변수에 의해 정의된 포트를 제외한 모든 포트	!$로 시작하는 대문자로 된 변수 이름	`!$HTTP_PORTS`

침입 이벤트 세부 정보

표준 텍스트 규칙을 구성할 때 규칙이 익스플로잇 시도에서 탐지하는 취약성을 설명하는 컨텍스트 정보를 포함할 수 있습니다. 또한 취약성 데이터베이스에 외부 참조를 포함하고 사용자 조직에서 이벤트가 가지고 있는 우선 순위를 정의할 수 있습니다. 분석가가 이벤트를 볼 때, 그들은 우선 순위, 공격, 즉시 사용 가능한 알려진 위협 완화에 대한 정보를 가지게 됩니다.

Message

규칙이 트리거될 때 메시지로 표시되는 의미 있는 텍스트를 지정할 수 있습니다. 메시지는 규칙이 공격 시도를 탐지하게 되는 취약성의 속성에 대한 즉각적인 통찰력을 제공해 줍니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다. 시스템은 메시지를 완전히 묶고 있는 따옴표를 떼어버립니다.

팁 규칙 메시지를 지정해야 합니다. 또한, 공백, 하나 이상의 따옴표, 하나 이상의 아포스트로피 또는 공백, 따옴표, 아포스트로피로의 조합만으로는 메시지를 구성할 수 없습니다.

침입 규칙 편집기에서 이벤트 메시지를 정의하려면 **Message(**메시지**)** 필드에 이벤트 메시지를 입력합니다.

분류

각 규칙에, 이벤트의 패킷 표시에 나타나는 공격 분류를 지정할 수 있습니다. 다음 표에서는 각 분류의 이름과 번호를 나열합니다.

표 ***152:*** 규칙 분류

번호	분류 이름	설명
1	not-suspicious	의심스럽지 않은 트래픽
2	unknown	알 수 없는 트래픽

번호	분류 이름	설명
3	bad-unknown	잠재적인 악성 트래픽
4	attempted-recon	정보 유출 시도
5	successful-recon-limited	정보 유출
6	successful-recon-largescale	대규모 정보 유출
7	attempted-dos	서비스 거부 시도
8	successful-dos	서비스 거부
9	attempted-user	사용자 권한 획득 시도
10	unsuccessful-user	사용자 권한 획득 실패
11	successful-user	사용자 권한 획득 성공
12	attempted-admin	관리자 권한 획득 시도
13	successful-admin	관리자 권한 획득 성공
14	rpc-portmap-decode	RPC 쿼리 디코드
15	shellcode-detect	실행 가능한 코드가 탐지됨
16	string-detect	의심스러운 문자열이 탐지됨
17	suspicious-filename-detect	의심스러운 파일 이름이 탐지됨
18	suspicious-login	의심스러운 사용자 이름을 사용한 로그인 시도가 탐지됨
19	system-call-detect	시스템 호출이 탐지됨
20	tcp-connection	TCP 연결이 탐지됨
21	trojan-activity	네트워크 트로이 목마가 탐지됨
22	unusual-client-port-connection	클라이언트가 비정상적인 포트를 사용하고 있음
23	network-scan	네트워크 스캔이 탐지됨
24	denial-of-service	DoS(Denial-of-Service) 공격이 탐지됨
25	non-standard-protocol	비표준 프로토콜 또는 이벤트가 탐지됨
26	protocol-command-decode	일반적인 프로토콜 명령 디코드
27	web-application-activity	잠재적으로 취약한 웹 애플리케이션에 액세스

번호	분류 이름	설명
28	web-application-attack	웹 애플리케이션 공격
29	misc-activity	기타 활동
30	misc-attack	기타 공격
31	icmp-event	일반 ICMP 이벤트
32	inappropriate-content	부적절한 콘텐츠가 발견됨
33	policy-violation	잠재적인 기업 개인 정보 보호 위반
34	default-login-attempt	기본 사용자 이름 및 비밀번호로 로그인 시도
35	sdf	중요한 데이터
36	malware-cnc	알려진 악성코드 명령 및 제어 트래픽
37	client-side-exploit	알려진 클라이언트 측 공격 시도
38	file-format	알려진 악성 파일 또는 파일 기반 익스플로잇

맞춤형 분류

사용자가 정의하는 규칙에서 생성된 이벤트의 패킷 표시 설명을 위한 더 많은 맞춤형 콘텐츠를 원할 경우, 맞춤형 분류를 생성할 수 있습니다.

인수	설명
분류 이름	분류의 이름입니다. 40개 이상의 문자를 사용하는 경우, 페이지를 읽기가 어렵습니다. 다음 문자는 지원되지 않습니다: `<> () \ ‘“&$;` 및 공백 문자.
분류 설명	분류의 설명입니다. 영숫자와 공백을 사용할 수 있습니다. `<> () \ ‘“&$;` 문자는 지원되지 않습니다.
Priority(우선순위)	높음, 중간 또는 낮음.

맞춤형 우선 순위

기본적으로, 규칙의 우선 순위는 규칙에 대한 이벤트 분류에서 파생됩니다. 하지만 규칙에 `priority` 키워드를 추가하고 high(높음), medium(중간) 또는 low(낮음) 우선 순위를 선택하여 규칙의 분류 우선 순위를 재정의할 수 있습니다. 예를 들어 웹 애플리케이션 공격을 탐지하는 규칙에 high(높음) 우선 순위를 할당하려면 `priority` 키워드를 규칙에 추가하고 우선 순위로 **high(**높음**)**를 선택합니다.

맞춤형 참조

reference 키워드를 사용하여 외부 웹사이트에 참조를 추가하고 이벤트에 대한 자세한 내용을 추가할 수 있습니다. 참조를 추가하면 패킷이 규칙을 트리거한 이유에 대한 확인을 돕기 위해 분석가에게 즉시 사용 가능한 리소스를 제공합니다. 다음 표는 알려진 악성 공격에 관한 데이터를 제공하는 몇 가지 외부 시스템 나열합니다.

표 ***153:*** 외부 공격 식별 시스템

시스템 **ID**	설명	예시 **ID**
bugtraq	Bugtraq 페이지	8550
cve	일반 취약점 및 노출 ID	2020-9607
mcafee	McAfee 페이지	98574
url	웹사이트 참조	www.example.com?exploit=14
msb	Microsoft 보안 공지	MS11-082
nessus	Nessus 페이지	10039
secure-url	보안 웹사이트 참조(https://...)	intranet/exploits/exploit=14 모든 보안 웹사이트로 secure-url을 함께 사용할 수 있다는 점을 참고하십시오.

다음과 같이 참조 값을 입력하여 참조를 지정합니다.

```
id_system,id
```

여기서 id_system은 프리픽스로 사용되고 있는 시스템이고 id는 CVE ID 번호, Arachnids ID 또는 URL(http:// 없음)입니다.

예를 들어 CVE-2020-9607에 설명되어 있는 Adobe Acrobat 및 Reader 문제를 지정하려면 다음 값을 입력합니다.

```
cve,2020-9607
```

규칙에 참조 사항을 추가할 때 다음에 유의하십시오.

- 쉼표 뒤에 스페이스를 사용하지 마십시오.
- 시스템 ID에 대문자를 사용하지 마십시오.

관련 항목

맞춤형 분류 추가, 2076 페이지
이벤트 우선 순위 정의, 2076 페이지

이벤트 참조 정의, 2077 페이지

맞춤형 분류 추가

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 분류를 표시하며, 사용자는 이러한 분류의 우선 순위를 설정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 분류도 표시되지만 사용자는 이러한 분류의 우선 순위를 설정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 분류를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 규칙을 만들거나 수정할 때 **Classification(**분류**)** 드롭다운 목록에서 **Edit Classifications(**분류 수정**)**을 선택합니다.

View Classifications(분류 보기**)**가 대신 표시되는 경우, 구성이 상위 도메인에 속하거나 구성을 수정할 권한이 없는 것입니다.

단계 **2** 침입 이벤트 세부 정보, 2072 페이지에 설명된 대로 **Classification Name(**분류 이름**)**과 **Classification Description(**분류 설명**)**을 입력합니다.

단계 **3** **Priority(**우선 순위**)** 드롭다운 목록에서 분류의 우선 순위를 선택합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 새 규칙 작성, 2078 페이지 또는 기존 규칙 수정, 2079 페이지를 참고하십시오.

관련 항목

맞춤형 규칙 생성, 2077 페이지

이벤트 우선 순위 정의

프로시저

단계 **1** 규칙을 만들거나 수정할 때 **Detection Options(**탐지 옵션**)** 드롭다운 목록에서 `priority(우선 순위)`를 선택합니다.

단계 **2** **Add Option(**옵션 추가**)**을 클릭합니다.

단계 **3** **priority(**우선 순위**)** 드롭다운 목록에서 값을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 새 규칙 작성, 2078 페이지 또는 기존 규칙 수정, 2079 페이지를 참고하십시오.

관련 항목

맞춤형 규칙 생성, 2077 페이지

이벤트 참조 정의

프로시저

단계 **1** 규칙을 만들거나 수정할 때 **Detection Options(**탐지 옵션**)** 드롭다운 목록에서 `reference(참조)`를 선택합니다.

단계 **2** **Add Option(**옵션 추가**)**을 클릭합니다.

단계 **3** 침입 이벤트 세부 정보, 2072 페이지에 설명된 대로 **reference(**참조**)** 필드에 값을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 새 규칙 작성, 2078 페이지 또는 기존 규칙 수정, 2079 페이지를 참고하십시오.

관련 항목

맞춤형 규칙 생성, 2077 페이지

맞춤형 규칙 생성

다음 방법으로 맞춤형 침입 규칙을 만들 수 있습니다.

- 자체 표준 텍스트 규칙 생성
- 기존 표준 텍스트 규칙을 새로 저장
- 시스템에서 제공한 공유 개체 규칙을 새로 저장
- 다중 도메인 구축에서 하위 도메인에 상위 도메인 규칙을 새로 저장
- 로컬 규칙 파일 가져오기

시스템은 규칙 생성에 사용된 방법에 상관없이 맞춤형 규칙을 로컬 규칙 카테고리에 저장합니다.

맞춤형 침입 규칙을 만들 때 시스템은 `GID: SID: Rev`형식의 고유한 규칙 번호를 규칙에 할당합니다. 이 번호의 요소는 다음과 같습니다.

GID

생성자 ID입니다. 모든 표준 텍스트 규칙의 경우, 이 값은 1(전역 도메인 또는 레거시 GID) 또는 1000 - 2000(하위 도메인)입니다. 새로운 규칙으로 저장하는 모든 공유 개체 규칙의 경우, 이 값은 1입니다.

SID

Snort ID. 규칙이 시스템 규칙의 로컬 규칙인지 여부를 나타냅니다. 새 규칙을 만들 때 시스템은 로컬 규칙에 사용 가능한 다음 SID를 할당합니다.

로컬 규칙의 SID 번호는 1000000에서 시작하며 각 새 로컬 규칙의 SID는 1씩 증가합니다.

Rev

수정 번호. 새 규칙의 경우, 수정 번호는 1입니다. 사용자 지정 규칙을 변경할 때마다 수정 번호가 하나씩 증가합니다.

맞춤형 표준 텍스트 규칙에서 헤더 설정과 규칙 키워드 및 인수를 설정합니다. 규칙 헤더 설정을 사용하면 특정 프로토콜을 사용하며 특정 IP 주소 또는 포트를 오가는 트래픽만을 매칭하도록 규칙의 범위를 좁힐 수 있습니다.

맞춤형 시스템 제공 표준 텍스트 규칙 또는 공유 개체 규칙에서는 소스/대상 포트 및 IP 주소와 같은 규칙 헤더 정보를 수정하는 것으로 제한됩니다. 규칙 키워드 또는 인수를 수정할 수 없습니다.

공유 개체 규칙의 헤더 정보를 수정하고 변경 사항을 저장하면 생성자 ID(GID) 1(전역 도메인) 또는 1000 - 2000(하위 도메인) 및 맞춤형 규칙에 사용 가능한 다음 SID로 규칙의 새 인스턴스가 생성됩니다. 시스템은 공유 개체 규칙의 새 인스턴스를 예약된 `soid` 키워드에 연결하는데, 이 경우 사용자가 생성한 규칙이 Cisco Talos Intelligence Group(Talos)에 의해 생성된 규칙에 매핑됩니다. 생성하는 공유 개체 규칙의 인스턴스를 삭제할 수 있지만 Talos에 의해 생성된 공유 개체 규칙은 삭제할 수 없습니다.

새 규칙 작성

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 침입 규칙에 액세스합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택하고 **Intrusion Rules(**침입 규칙**)**를 클릭합니다.
- **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**을(를) 선택합니다.

단계 **2** **Create Rule(**규칙 생성**)**을 클릭합니다.

단계 **3** **Message(**메시지**)** 필드에 값을 입력합니다.

단계 **4** 다음 각 드롭다운 목록에서 값을 선택합니다.

- 분류
- 조치
- 프로토콜

- 방향

단계 **5** 다음 필드에 값을 입력합니다.

- 소스 **IP**
- 대상 **IP**
- **Source Port(**소스 포트**)**
- **Destination Port(**목적지 포트**)**

이러한 필드의 값을 지정하지 않으면 시스템은 `any(모든)` 값을 사용합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **6** **Detection Options(**탐지 옵션**)** 드롭다운 목록에서 값을 선택합니다.

단계 **7** **Add Option(**옵션 추가**)**을 클릭합니다.

단계 **8** 추가한 키워드의 모든 인수를 입력합니다.

단계 **9** 필요한 경우, 6~8 단계를 반복합니다.

단계 **10** 여러 키워드를 추가한 경우, 다음을 수행할 수 있습니다.

- 키워드 다시 정렬 - 이동하려는 키워드 옆의 위쪽 또는 아래쪽 화살표를 클릭합니다.
- 키워드 삭제 - 해당 키워드 옆에 있는 **X**를 클릭합니다.

단계 **11** **Save As New(**새 이름으로 저장**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 침입 정책 내에서 새로운 규칙이나 변경된 규칙을 활성화합니다(침입 정책의 침입 규칙 보기, 2009 페이지 참조).
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

기존 규칙 수정

맞춤형 침입 규칙을 수정할 수 있습니다. 다중 도메인 구축에서는 현재 도메인에 속한 맞춤형 침입 규칙만 수정할 수 있습니다.

시스템 제공 규칙과 상위 도메인에 속한 규칙은 로컬 규칙 카테고리에 새로운 맞춤형 규칙으로 저장한 다음 수정할 수 있습니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 침입 규칙에 액세스합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택하고 **Intrusion Rules(**침입 규칙**)**를 클릭합니다.
- **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**을(를) 선택합니다.

단계 **2** 수정할 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 폴더를 통해 규칙으로 이동합니다.
- 규칙을 검색합니다(규칙 검색, 2083 페이지 참조).
- 규칙이 속한 그룹을 필터링합니다(규칙 필터링, 2087 페이지 참조).

단계 **3** 규칙 옆에 있는 수정( )을 클릭하거나 검색 결과에서 규칙 메시지를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 규칙 유형에 적절하게 규칙을 수정합니다.

참고 공유 개체 규칙에 대한 프로토콜을 수정하지 마십시오. 이를 삭제하면 규칙이 무효화됩니다.

단계 **5** 다음 옵션을 이용할 수 있습니다.

- 맞춤형 규칙을 수정하고 해당 규칙의 현재 버전을 재정의하려는 경우, **Save(**저장**)**를 클릭합니다.
- 시스템 제공 규칙 또는 상위 도메인에 속한 규칙을 수정하거나 맞춤형 규칙을 수정하고 변경 사항을 새 규칙으로 저장하려는 경우, **Save As New(**새로 저장**)**를 클릭합니다.

다음에 수행할 작업

- 시스템 제공 규칙 대신 로컬에서 수정한 규칙을 사용하려면 침입 규칙 상태, 2023 페이지의 절차를 사용하여 시스템 제공 규칙을 비활성화하고 로컬 규칙을 활성화합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

규칙 검색, 2083 페이지
침입 규칙 편집기 페이지에서 규칙 필터링, 2085 페이지

규칙 문서 보기

Rule Edit(규칙 편집) 페이지에서 Cisco Talos Intelligence Group(Talos)가 제공하는 규칙 설명서를 볼 수 있습니다. 규칙 문서를 보는 동안 **Rule Documentation(**규칙 설명서**)** 및 기타 외부 참조를 클릭하여 Talos가 제공하는 추가 정보를 볼 수 있습니다. **Context Explorer(**컨텍스트 탐색기**)**를 클릭하면 규칙에 의해 생성된 이벤트의 컨텍스트 정보를 볼 수도 있습니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 침입 규칙에 액세스합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택하고 **Intrusion Rules(**침입 규칙**)**를 클릭합니다.
- **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**을(를) 선택합니다.

단계 **2** 보려는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 폴더를 통해 규칙으로 이동합니다.
- 규칙을 검색합니다(규칙 검색, 2083 페이지 참조).
- 규칙이 속한 그룹을 필터링합니다(규칙 필터링, 2087 페이지 참조).

단계 **3** 규칙 옆에 있는 수정( )을 클릭하거나 검색 결과에서 규칙 메시지를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** **View Documentation(**설명서 보기**)**을 클릭합니다.

단계 **5** 원하는 경우, 다음 링크 중 하나를 클릭합니다.

- **Rule Documentation(**규칙 설명서**)** - 자세한 규칙 세부 정보를 볼 수 있습니다.
- Other external references(기타 외부 참조) - 사용 가능한 외부 참조에 대한 정보를 보려면 키워드 필터링, 2085 페이지 및 침입 이벤트 세부 정보, 2072 페이지의 *Custom Reference(*맞춤형 참조*)*를 참조하십시오.
- **Context Explorer(**컨텍스트 탐색기**)** - 컨텍스트 탐색기에서 규칙의 컨텍스트 데이터 보기에 대한 정보는 침입 정보 섹션, 2710 페이지를 참조하십시오.

팁 외부 링크를 선택하면 설명서 팝업 창이 닫힙니다. 규칙을 수정하지 않고 규칙 편집 페이지에서 나가려면 아무 메뉴 경로나 선택합니다.

침입 규칙에 코멘트 추가

모든 침입 규칙에 코멘트를 추가할 수 있습니다. 이러한 코멘트는 규칙 및 규칙이 식별하는 익스플로잇 또는 정책 위반에 대한 컨텍스트 및 추가 정보를 제공하는 데 유용할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 코멘트를 표시하며 이러한 코멘트는 수정할 수 있습니다. 상위 도메인에서 생성된 코멘트도 표시되지만 이러한 코멘트는 삭제할 수 없습니다. 하위 도메인에서 생성된 코멘트를 보려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 침입 규칙에 액세스합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택하고 **Intrusion Rules(**침입 규칙**)**를 클릭합니다.
- **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**을(를) 선택합니다.

단계 **2** 코멘트를 달고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 폴더를 통해 규칙으로 이동합니다.
- 규칙을 검색합니다(규칙 검색, 2083 페이지 참조).
- 규칙이 속한 그룹을 필터링합니다(규칙 필터링, 2087 페이지 참조).

단계 **3** 규칙 옆에 있는 수정( )을 클릭하거나 검색 결과에서 규칙 메시지를 클릭합니다.

규칙 옆에 보기 ( )가 대신 표시되는 경우에는 해당 규칙이 상위 정책에 속하거나 규칙을 수정할 권한이 없는 것입니다.

단계 **4** **Rule Comment(**규칙 코멘트**)**를 클릭합니다.

단계 **5** 입력란에 코멘트를 입력합니다.

단계 **6** **Add Comment(**코멘트 추가**)**를 클릭합니다.

팁 침입 이벤트의 패킷 보기에서 규칙 코멘트를 추가하고 볼 수도 있습니다.

다음에 수행할 작업

- 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 새 규칙 작성, 2078 페이지 또는 기존 규칙 수정, 2079 페이지를 참고하십시오.

관련 항목

규칙 검색, 2083 페이지
이벤트 정보 필드, 2937 페이지

사용자 지정 규칙 삭제

침입 정책에서 현재 활성화되지 않은 맞춤형 규칙을 삭제할 수 있습니다. 시스템이 제공하는 표준 텍스트 규칙 또는 공유 개체 규칙은 삭제할 수 없습니다. 다중 도메인 구축에서는 현재 도메인에서 생성된 로컬 규칙만 삭제할 수 있습니다.

시스템은 삭제된 카테고리에 삭제된 규칙을 저장하며, 사용자는 삭제한 규칙을 새로운 규칙의 기준으로 사용할 수 있습니다. 침입 정책의 Rules(규칙) 페이지가 삭제된 카테고리를 표시하지 않으므로, 삭제된 사용자 지정 규칙을 사용할 수 없습니다.

팁 맞춤형 규칙에는 수정된 헤드 정보와 함께 저장하는 공유 개체 규칙이 포함됩니다. 시스템은 또한 이러한 규칙을 로컬 규칙 카테고리에 저장하고 GID 1(전역 도메인 또는 레거시 GID) 또는 1000 - 2000(하위 도메인)을 사용해 나열합니다. 공유 개체 규칙의 수정된 버전은 삭제할 수 있지만 원본 공유 개체 규칙은 삭제할 수 없습니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 침입 규칙에 액세스합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택하고 **Intrusion Rules(**침입 규칙**)**를 클릭합니다.
- **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**을(를) 선택합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 모든 로컬 규칙 삭제 - **Delete Local Rules(**로컬 규칙 삭제**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.
- 단일 규칙 삭제 - **Group Rules By(**규칙 그룹화 기준**)** 드롭다운 목록에서 `Local Rules(로컬 규칙)`를 선택하고 삭제할 규칙 옆에 있는 삭제( )을 클릭한 다음 **OK(**확인**)**를 클릭하여 삭제를 확인합니다.

관련 항목

침입 규칙 상태, 2023 페이지

규칙 검색

Firepower System은 수천 개의 표준 텍스트 규칙을 제공하며, Cisco Talos Intelligence Group(Talos)는 새로운 취약성과 익스플로잇이 발견됨에 따라 계속 규칙을 추가합니다. 특정 규칙을 손쉽게 검색하여 활성화, 비활성화 또는 수정할 수 있습니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 침입 규칙에 액세스합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택하고 **Intrusion Rules(**침입 규칙**)**를 클릭합니다.
- **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**을(를) 선택합니다.

단계 **2** 툴바에서 **Search(**검색**)**를 클릭합니다.

단계 **3** 검색 기준을 추가합니다.

단계 **4** **Search(**검색**)**를 클릭합니다.

다음에 수행할 작업

- 찾은 규칙(시스템 규칙인 경우 규칙의 복사본)을 보거나 수정하려면 하이퍼링크가 있는 규칙 메시지를 클릭합니다. 자세한 내용은 새 규칙 작성, 2078 페이지 또는 기존 규칙 수정, 2079 페이지를 참고하십시오.

침입 규칙에 대한 검색 기준

다음 표에서는 사용 가능한 검색 옵션에 대해 설명합니다.

표 ***154:*** 규칙 검색 기준

옵션	설명
Signature ID	Snort ID(SID)를 기반으로 단일 규칙을 검색하려면 SID 번호를 입력합니다. 여러 규칙을 검색하려면 쉼표로 구분된 SID 번호 목록을 입력합니다. 이 필드의 문자 제한은 80자입니다.
생성자 ID	표준 텍스트 규칙을 검색하려면 **1**을 선택합니다. 공유 개체 규칙을 검색하려면 **3**을 선택합니다.
Message	특정 메시지가 있는 규칙을 검색하려면 규칙 메시지의 한 단어를 **Message(**메시지**)** 필드에 입력합니다. 예를 들어 DNS 익스플로잇을 검색하려면 `DNS`를, 버퍼 오버플로 익스플로잇을 검색하려면 `overflow`를 입력합니다.
프로토콜	특정 프로토콜의 트래픽을 평가하는 규칙을 검색하려면 프로토콜을 선택합니다. 프로토콜을 선택하지 않으면 검색 결과에 모든 프로토콜에 대한 규칙이 포함됩니다.
소스 포트	지정된 포트에서 오는 패킷을 검사하는 규칙을 검색하려면 소스 포트 번호 또는 포트 관련 변수를 입력합니다.
대상 포트	특정 포트로 향하는 패킷을 검사하는 규칙을 검색하려면 대상 포트 번호 또는 포트 관련 변수를 입력합니다.
Source IP(소스 IP)	지정된 IP 주소에서 오는 패킷을 검사하는 규칙을 검색하려면 소스 IP 주소 또는 IP 주소 관련 변수를 입력합니다.
Destination IP(목적지 IP)	지정된 IP 주소로 향하는 패킷을 검사하는 규칙을 검색하려면 대상 IP 주소 또는 IP 주소 관련 변수를 입력합니다.
키워드	특정 키워드를 검색하려면 키워드 검색 옵션을 사용할 수 있습니다. 키워드를 선택하고 검색할 키워드 값을 입력합니다. 키워드 값 앞에 느낌표(`!`)를 입력하면 지정된 값 이외의 모든 값을 매칭할 수도 있습니다.
카테고리	특정 카테고리의 규칙을 검색하려면 **Category(**카테고리**)** 목록에서 카테고리를 선택합니다.
분류	특정 분류가 있는 규칙을 검색하려면 **Classification(**분류**)** 목록에서 분류를 선택합니다.
규칙 상태	특정 정책 및 규칙 상태 내의 규칙을 검색하려면 첫 번째 **Rule State(**규칙 상태**)** 목록에서 정책을 선택하고 두 번째 목록에서 상태를 선택해 **Generate Events(**이벤트 생성**)**, **Drop and Generate Events(**이벤트 삭제 및 생성**)** 또는 **Disabled(**비활성화**)**로 설정된 규칙을 검색합니다.

침입 규칙 편집기 페이지에서 규칙 필터링

침입 규칙 편집기 페이지에서 규칙을 필터링해 규칙의 하위 집합을 표시할 수 있습니다. 예를 들어, 규칙을 수정하거나 상태를 변경하기를 원하지만 수천 개의 규칙 중에서 이를 찾는 데 어려움이 있는 경우, 이는 유용할 수 있습니다.

필터를 입력하면, 페이지는 적어도 하나의 일치하는 규칙을 포함하는 모든 폴더를 표시하거나, 규칙이 하나도 일치하지 않을 때는 메시지를 표시합니다.

필터링 가이드라인

필터는 특수 키워드 및 해당 인수, 문자열 및 텍스트 문자열, 그리고 여러 필터 상태를 분리하는 스페이스를 포함할 수 있습니다. 필터에는 정규 표현식, 와일드카드 문자 또는 부정 문자(!), 보다 큼 기호(>), 보다 작음 기호(<)와 같은 특별 연산자를 포함할 수 없습니다.

모든 키워드, 키워드 인수 및 문자열은 대소문자를 구분하지 않습니다. `gid` 및 `sid` 키워드를 제외한, 모든 인수 및 문자열은 부분 문자열로 처리됩니다. `gid` 및 `sid`의 인수는 정확히 일치하는 것만 반환합니다.

필터링되지 않은 원래 페이지에서 폴더를 확장할 수 있으며, 후속 필터가 해당 폴더에서 일치 항목을 반환하면 폴더는 확장된 상태로 유지됩니다. 이는 찾고자 하는 규칙이 많은 규칙을 포함하는 폴더에 있을 때 유용할 수 있습니다.

후속 필터로 필터를 제한할 수 없습니다. 입력한 모든 필터는 전체 규칙 데이터베이스를 검색하고 일치하는 규칙을 모두 반환합니다. 페이지가 계속 이전 검색 결과를 표시하고 있는데 필터를 입력하는 경우, 페이지는 이를 지우고 새 필터의 결과로 돌아갑니다.

필터링된 목록이나 필터링되지 않은 목록의 규칙과 같은 기능을 사용할 수 있습니다. 예를 들어 침입 규칙 편집기 페이지에서 필터링된 목록이나 필터링되지 않은 목록의 규칙을 수정할 수 있습니다. 또한 해당 페이지에 대해 상황에 맞는 메뉴에서 모든 옵션을 사용할 수 있습니다.

팁 모든 하위 그룹의 규칙을 포함한 총 규칙 수가 클 경우 규칙이 여러 카테고리에 나타날 수 있기 때문에 고유한 총 규칙 수가 훨씬 적더라도 필터링에 상당한 시간이 소요될 수 있습니다.

키워드 필터링

각 규칙 필터의 형식에는 하나 이상의 키워드를 포함할 수 있습니다.

```
keyword:argument
```

여기서 keyword는 다음 표에 있는 키워드 중 하나이며, argument는 키워드와 관련된 하나 이상의 특정 필드에서 검색할, 대소문자를 구분하지 않는 단일 영숫자 문자열입니다.

`gid` 및 `sid`를 제외한 모든 키워드에 대한 인수는 부분 문자열로 처리됩니다. 예를 들어, 인수 `123`은 `"12345"`, `"41235"`, `"45123"` 등을 반환합니다. `gid` 및 `sid`의 인수는 정확하게 일치하는 경우에만 반환됩니다. 예를 들어, `sid:3080`은 SID 3080만 반환합니다.

팁 하나 이상의 문자열로 필터링하여 부분 SID를 검색할 수 있습니다.

다음 표는 규칙을 필터링하는 데 사용할 수 있는 인수 및 특정 필터링 키워드를 나타냅니다.

표 ***155:*** 규칙 필터링 키워드

키워드	설명	예
`arachnids`	규칙 참조에서 Arachnids ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`arachnids:181`
`bugtraq`	규칙 참조에서 Bugtraq ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`bugtraq:2120`
`cve`	규칙 참조에서 CVE 번호의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`cve:2003-0109`
`gid`	인수 `1`은 표준 텍스트 규칙을 반환합니다. 인수 `3`은 공유 개체 규칙을 반환합니다.	`gid:3`
`mcafee`	규칙 참조에서 McAfee ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`mcafee:10566`
`msg`	이벤트 메시지로도 알려진 규칙 Message(메시지) 필드의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`msg:chat`
`nessus`	규칙 참조에서 Nessus ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`nessus:10737`
`ref`	규칙 참조 또는 규칙 Message(메시지) 필드에서 단일 영숫자 문자열의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`ref:MS03-039`
`sid`	정확한 Snort ID가 있는 규칙을 반환합니다.	`sid:235`
`url`	규칙 참조에서 URL의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다.	`url:faqs.org`

관련 항목

이벤트 참조 정의, 2077 페이지
침입 이벤트 세부 정보, 2072 페이지
전처리기 생성기 ID, 2928 페이지

문자열 필터링

각 규칙 필터는 하나 이상의 영숫자 문자열을 포함할 수 있습니다. 문자열은 규칙 **Message(**메시지**)** 필드, Snort ID(SID) 및 생성자 ID(GID)를 검색합니다. 예를 들어, 문자열 `123`은 규칙 메시지에서 문자열 `"Lotus123"`, `"123mania"` 등을 반환하며, 또한 SID 6123, SID 12375 등을 반환합니다.

모든 문자열은 대소문자를 구분하지 않으며 부분 문자열로 처리됩니다. 예를 들어, 문자열 `ADMIN`, `admin` 또는 `Admin`은 모두 `"admin"`, `"CFADMIN"`, `"Administrator"` 등을 반환합니다.

정확히 일치하는 항목을 반환하기 위해 인용구에서 문자열을 묶을 수 있습니다. 예를 들어, 인용구 내 문자열 `"overflow attempt"`는 정확한 문자열만 반환하지만, 인용구가 없는 두 개의 문자열 `overflow` 및 `attempt`로 구성된 필터는 `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"` 등을 반환합니다.

관련 항목

침입 이벤트 세부 정보, 2072 페이지
전처리기 생성기 ID, 2928 페이지

키워드 및 문자열 조합 필터링

키워드, 문자열 또는 둘 다로 이루어진 스페이스로 구분된 문자열의 조합을 입력하여 필터링 결과를 좁힐 수 있습니다. 결과는 필터링 조건과 일치하는 모든 규칙을 포함합니다.

순서에 상관없이 여러 필터 상태를 입력할 수 있습니다. 예를 들어, 다음 필터 각각은 동일한 규칙을 반환합니다.

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

규칙 필터링

Intrusion Rules(침입 규칙) 페이지에서 규칙을 하위 집합으로 필터링하면 특정 규칙을 더 쉽게 찾을 수 있습니다. 그런 다음 컨텍스트 메뉴에서 사용 가능한 기능 선택을 포함하여 원하는 페이지 기능을 사용할 수 있습니다.

규칙 필터링은 수정할 규칙을 찾을 때 특히 유용할 수 있습니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 침입 규칙에 액세스합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**를 선택하고 **Intrusion Rules(**침입 규칙**)**를 클릭합니다.
- **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**을(를) 선택합니다.

단계 **2** 필터링 전에 다음 옵션을 이용할 수 있습니다.

- 확장할 규칙 그룹을 확장합니다. 일부 규칙 그룹에도 확장할 수 있는 하위 그룹이 있습니다.

  필터링되지 않은 원래 페이지에서 그룹을 확장하면 해당 그룹에 규칙이 있을 것으로 예상되는 경우 유용할 수 있습니다. 후속 필터가 해당 폴더와 일치할 때, 그리고 필터 지우기( )을 클릭하여 원래의 필터링되지 않은 페이지로 돌아온 경우 해당 그룹은 확장된 채로 유지됩니다.

- **Group Rules By(**규칙 분류 기준**)** 드롭다운 목록에서 다른 그룹화 방법을 선택합니다.

단계 **3** **Group Rules By(**규칙 그룹화 기준**)** 목록 아래 필터( ) 옆에 있는 입력란에 필터 제약 조건을 입력합니다.

단계 **4** Enter를 누릅니다.

참고 지우기( )을 클릭하여 필터링된 현재 목록을 삭제합니다.

침입 규칙의 키워드 및 인수

규칙 언어를 사용하여 키워드를 결합함으로써 규칙 작업을 지정할 수 있습니다. 키워드 및 관련 값(일명 인수)은 규칙 엔진이 테스트하는 패킷 및 패킷 관련 값을 시스템이 평가하는 방법을 지시합니다. Firepower System은 현재 콘텐츠 매칭, 프로토콜별 패턴 매칭, 상태별 매칭 등의 검사 기능을 수행할 수 있는 키워드를 지원합니다. 키워드당 최대 100개의 인수를 정의할 수 있고, 매우 특정한 규칙을 만들기 위해 호환성 키워드를 얼마든지 통합할 수 있습니다. 이는 잘못된 긍정 및 잘못된 부정의 가능성을 줄이고 사용자가 수신하는 침입 정보에 집중하는 데 도움을 줍니다.

또한 패시브 구축에서 적응형 프로파일을 사용하여 규칙 메타데이터와 호스트 정보에 따라 특정 패킷에 대한 활성 규칙 처리를 동적으로 조정할 수 있습니다.

이 섹션에 설명된 키워드는 규칙 편집기에서 Detection Options(탐지 옵션) 아래 나열됩니다.

관련 항목

적응형 프로파일 정보, 2371 페이지

content 및 protected_content 키워드

패킷에서 탐지할 내용을 지정하려면 `content` 키워드 또는 `protected_content` 키워드를 사용합니다.

사용자는 거의 항상 `content` 또는 `protected_content` 키워드를 따라야 합니다. 이 키워드는 콘텐츠를 어디에서 검색해야 할지, 검색에 있어 대소문자 구분이 필요한지 여부, 그리고 다른 옵션을 나타내는 수식어 옆에 있습니다.

모든 콘텐츠 일치는 이벤트를 트리거하는 규칙에 대해 참이어야 한다는 점, 즉, 각 콘텐츠 일치는 다른 항목과 AND 관계를 가지고 있다는 점에 유의하십시오.

또한, 인라인 배포에서 악성 콘텐츠와 일치하고 이를 동일한 길이의 자체 문자열로 대체하는 규칙을 설정할 수 있다는 점에 유의하십시오.

content

content 키워드를 사용하면, 규칙 엔진이 해당 문자열에 대한 패킷 페이로드 또는 스트림을 검색합니다. 예를 들어, content 키워드 중 하나의 값으로 /bin/sh를 입력하면, 규칙 엔진은 문자열 /bin/sh에 대한 패킷 페이로드를 검색합니다.

ASCII 문자열, 16진수 콘텐츠(이진 바이트 코드) 또는 이 둘의 조합 중 하나를 사용하여 콘텐츠에 일치시킵니다. 키워드 값에서 파이프 문자(|)로 16진수 콘텐츠를 묶습니다. 예를 들어, |90C8 C0FF FFFF|/bin/sh와 같은 형태를 사용하여 16진수 콘텐츠 및 ASCII 콘텐츠를 섞을 수 있습니다.

단일 규칙에서 여러 콘텐츠 일치를 지정할 수 있습니다. 이를 위해, content 키워드의 추가 인스턴스를 사용합니다. 각 콘텐츠 일치의 경우, 규칙이 트리거되려면 패킷 페이로드 또는 스트림에서 콘텐츠 일치를 찾아야 한다는 것을 나타낼 수 있습니다.

⚠

주의 content 키워드가 하나만 포함된 규칙을 생성하고 키워드에 대해 **Not** 옵션을 선택한 경우 침입 정책을 무효화할 수 있습니다.

protected_content

protected_content 키워드를 사용하면 규칙 인수를 구성하기 전에 검색 내용 문자열을 인코딩할 수 있습니다. 원래 규칙 작성자는 키워드를 구성하기 전에 문자열을 인코딩하기 위해 해시 함수(SHA-512, SHA-256 또는 MD5)를 사용합니다.

content 키워드 대신 protected_content 키워드를 사용하면, 규칙 엔진이 해당 문자열 및 예상한 대로 대부분 키워드 옵션에 대해 패킷 페이로드 또는 스트림을 검색하는 방법은 변경되지 않습니다. 다음 표에는 예외가 요약되어 있습니다. 여기서 protected_content 키워드 옵션은 content 키워드 옵션과 다릅니다.

표 ***156: protected_content*** 옵션 예외

옵션	설명
해시 유형	protected_content 규칙 키워드에 대한 새로운 옵션.
대소문자 구분 안 함	지원되지 않음
내부	지원되지 않음
수준	지원되지 않음
길이	protected_content 규칙 키워드에 대한 새로운 옵션.
빠른 패턴 매처 사용	지원되지 않음
빠른 패턴 매처 한정	지원되지 않음
빠른 패턴 매처 오프셋 및 길이	지원되지 않음

Cisco는 `protected_content` 키워드를 포함하는 규칙에 최소 하나의 `content` 키워드를 포함할 것을 권장합니다. 이렇게 하면 규칙 엔진이 빠른 패턴 매처를 사용하여 처리 속도를 높이고 성능을 향상시킬 수 있습니다. 규칙에서 `protected_content` 키워드 앞에 콘텐츠 `keyword`를 배치합니다. 규칙에 최소 하나의 `content` 키워드가 포함될 때, `content` 키워드 Use Fast Pattern Matcher(빠른 패턴 매처 사용) 인수를 활성화했는지 여부에 상관없이 규칙 엔진이 빠른 패턴 매처를 사용한다는 점에 유의하십시오.

주의 `protected_content` 키워드가 하나만 포함된 규칙을 생성하고 키워드에 대해 **Not** 옵션을 선택한 경우 침입 정책을 무효화할 수 있습니다.

관련 항목

맞춤형 규칙 생성, 2077 페이지
기본 content 또는 protected_content 키워드 인수, 2090 페이지
replace 키워드, 2101 페이지

기본 **content** 또는 **protected_content** 키워드 인수

`content` 또는 `protected_content` 키워드를 수정하는 파라미터로 콘텐츠 검색 위치 및 대소문자 구분 여부를 제한할 수 있습니다. `content` 또는 `protected_content` 키워드를 수정하여 검색할 내용을 지정할 수 있는 옵션을 구성합니다.

대소문자 구분 안 함

참고 `protected_content` 키워드를 구성할 때 이 옵션은 지원되지 않습니다.

ASCII 문자열의 콘텐츠 일치를 검색할 때 대소문자 구분을 무시하기 위해 규칙 엔진을 검사할 수 있습니다. 검색에서 대소문자를 구분하도록 하려면 콘텐츠 검색을 지정할 때 **Case Insensitive(**대소문자 구분 안 함**)**를 선택합니다.

해시 유형

참고 이 옵션은 `protected_content` 키워드에 한정하여 구성 가능합니다.

Hash Type(해시 유형**)** 드롭다운을 사용하여 검색 문자열을 인코딩하는 데 사용한 해시 함수를 확인합니다. 시스템은 `protected_content` 검색 문자열에 대해 SHA-512, SHA-256 및 MD5 해싱을 지원합니다. 선택한 해시 유형이 해시된 콘텐츠의 길이와 일치하지 않을 경우, 시스템은 규칙을 저장하지 않습니다.

시스템은 Cisco가 설정한 기본값을 자동으로 선택합니다. **Default(**기본값**)**를 선택하면 규칙에 특정 해시 함수가 기록되지 않으며 시스템은 SHA-512를 해시 함수로 가정합니다.

Raw Data

Raw Data(원시 데이터**)** 옵션은 (네트워크 분석 정책에서 디코딩된) 표준화된 페이로드 데이터를 분석하기 전에 원래 패킷 페이로드를 규칙 엔진이 분석하도록 지시하며, 인수 값을 사용하지 않습니다. 텔넷 트래픽을 분석할 때 이 키워드를 사용하여 표준화 전 페이로드에서 텔넷 협상 옵션을 선택할 수 있습니다.

Raw Data 옵션은 동일한 `content` 또는 `protected_content` 키워드에서 HTTP content 옵션과 함께 사용할 수 없습니다.

팁 HTTP 검사 전처리기 **Client Flow Depth(**클라이언트 흐름 수준**)** 및 **Server Flow Depth(**서버 흐름 수준**)** 옵션을 구성하여 원시 데이터가 HTTP 트래픽에서 검사되는지 여부 및 검사할 원시 데이터의 양을 결정할 수 있습니다.

Not

지정된 내용과 일치하지 않는 콘텐츠를 검색하려면 **Not(**아님**)** 옵션을 선택합니다. **Not** 옵션을 선택한 상태로 `content` 또는 `protected_content` 키워드가 포함된 규칙을 생성하는 경우, **Not** 옵션을 선택하지 않은 상태로 하나 이상의 `content` 또는 `protected_content` 키워드를 규칙에 포함해야 합니다.

주의 **Not** 옵션을 선택한 경우 `content` 또는 `protected_content` 키워드가 하나만 포함된 규칙을 생성해서는 안 됩니다. 침입 정책을 무효화할 수 있습니다.

예를 들어 SMTP rule 1:2541:9에는 세 개의 `content` 키워드가 포함되어 있으며, 그중 하나에 대해서만 **Not** 옵션이 선택되어 있습니다. **Not** 옵션이 선택된 하나를 제외하고 모든 `content` 키워드를 제거하면 이 규칙을 기반으로 하는 맞춤형 규칙은 무효가 됩니다. 침입 정책에 이러한 규칙을 추가하면 정책을 무효화할 수 있습니다.

팁 동일한 `content` 키워드에서 **Not(**아님**)** 체크 박스와 **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)** 체크 박스를 모두 선택할 수는 없습니다.

content 또는 protected_content 키워드 검색 위치

위치 검색 옵션을 사용하여 지정된 콘텐츠 검색을 시작할 위치 및 검색 범위를 지정할 수 있습니다.

허용된 조합**: content** 검색 위치 인수

두 개의 `content` 위치 쌍 중 하나를 사용하여 지정된 콘텐츠 검색을 시작할 위치 및 검색 범위를 다음과 같이 지정할 수 있습니다.

- **Offset(**오프셋**)** 및 **Depth(**수준**)**를 함께 사용하여 패킷 페이로드의 시작과 관련된 항목을 검색합니다.
- **Distance(**영역**)** 및 **Within(**내부**)**을 함께 사용하여 현재 검색 위치와 관련된 항목을 검색합니다.

한 쌍만 지정할 때, 쌍에서 다른 옵션의 기본값이 가정됩니다.

Offset(오프셋**)** 및 **Depth(**수준**)** 옵션을 **Distance(**영역**)** 및 **Within(**내부**)** 옵션과 함께 사용할 수 없습니다. 예를 들어 **Offset** 및 **Within** 쌍은 사용할 수 없습니다. 규칙에서 위치 옵션을 얼마든지 사용할 수 있습니다.

위치가 지정되지 않으면 **Offset** 및 **Depth**의 기본값이 사용됩니다. 즉, 내용 검색은 패킷 페이로드의 처음부터 시작되고 패킷의 끝까지 계속됩니다.

기존의 `byte_extract` 변수를 사용하여 위치 옵션에 대한 값을 지정할 수 있습니다.

팁 규칙에서 위치 옵션을 얼마든지 사용할 수 있습니다.

관련 항목

byte_extract 키워드, 2106 페이지

허용되는 조합: **protected_content** 검색 위치 인수

지정된 내용에 대한 검색을 어디에서 시작할지, 어디까지 계속해야 할지를 지정하려면 다음과 같이 필수 **Length** `protected_content` 위치 옵션을 **Offset** 또는 **Distance** 위치 옵션 중 하나와 함께 사용하십시오.

- **Length(**길이**)**와 **Offset(**오프셋**)**을 함께 사용하여 패킷 페이로드의 시작과 관련된 보호된 문자열을 검색합니다.
- **Length(**길이**)**와 **Distance(**영역**)**를 함께 사용하여 현재 검색 위치와 관련된 보호된 문자열을 검색합니다.

팁 단일 키워드 구성에서 **Offset(**오프셋**)**과 **Distance(**영역**)** 옵션을 함께 사용할 수 없지만, 규칙에서 위치 옵션은 얼마든지 사용할 수 있습니다.

어떤 위치도 지정하지 않은 경우, 기본값이 가정됩니다. 즉, 패킷 페이로드가 시작될 때 콘텐츠 검색이 시작되며, 패킷이 종료될 때까지 계속됩니다.

기존의 `byte_extract` 변수를 사용하여 위치 옵션에 대한 값을 지정할 수 있습니다.

관련 항목

byte_extract 키워드, 2106 페이지

content 및 **protected_content** 검색 위치 인수

깊이

참고 이 옵션은 `content` 키워드를 구성할 때만 지원됩니다.

최대 콘텐츠 검색 수준을 오프셋 값의 시작부터 바이트 단위로 지정하거나 오프셋이 구성되어 있지 않은 경우 패킷 페이로드의 시작부터 지정합니다.

예를 들어 content 값 `cgi-bin/phf`, `offset` 값 `3`, `depth` 값 `22`의 규칙에서는 규칙 헤더에 지정된 매개 변수를 충족하는 패킷에서 `cgi-bin/phf` 문자열에 대한 일치 검색이 3바이트에서 시작되고 22바이트를 처리한 후(25바이트에서) 중지됩니다.

최대 65535바이트의 지정된 콘텐츠의 길이와 같거나 큰 값을 지정해야 합니다. 값으로 0을 지정할 수 없습니다.

기본 수준은 패킷 끝까지 검색하는 것입니다.

거리

이전의 성공적인 콘텐츠 일치 후에 지정한 바이트 수가 나타나는 다음 콘텐츠 일치를 규칙 엔진이 확인하도록 지시합니다.

영역 카운터가 0바이트에서 시작하므로, 마지막 성공적인 콘텐츠 일치보다 앞으로 이동하기를 원하는 바이트 수보다 하나 적은 수를 지정합니다. 예를 들어, 4를 지정한 경우, 검색은 다섯 번째 바이트에서 시작됩니다.

-65535에서 65535까지 바이트 값을 지정할 수 있습니다. 마이너스 `Distance(영역)` 값을 지정한 경우, 사용자가 찾기 시작한 바이트가 패킷의 초기에 범위 밖으로 밀려날 수 있습니다. 검색은 패킷의 첫 번째 바이트에서 시작하지만, 패킷 외부 바이트를 모두 고려합니다. 예를 들어 패킷의 현재 위치가 5번째 바이트이고 다음 내용 규칙 옵션에서 `Distance` 값 -10이며 `Within` 값이 20이면, 검색은 페이로드의 처음부터 시작되며 `Within` 옵션은 15로 조정됩니다.

기본값이 0인 것은 마지막 콘텐츠 일치 다음의 패킷 내 현재 위치를 의미합니다.

길이

참고 이 옵션은 `protected_content` 키워드를 구성할 때만 지원됩니다.

Length(길이**)** `protected_content` 키워드 옵션은 해시되지 않은 검색 문자열의 길이를 바이트 단위로 나타냅니다.

예를 들어 안전한 해시를 생성하기 위해 내용 `Sample1` 을 사용한 경우 **Length** 값에 `7`을 사용하십시오. 반드시 이 필드에 값을 입력해야 합니다.

Offset(오프셋**)**

패킷 페이로드의 어느 위치에서 패킷 페이로드의 시작과 관련된 콘텐츠 검색을 시작할지 바이트 단위로 지정합니다. -65535에서 65535까지 바이트 값을 지정할 수 있습니다.

오프셋 카운터가 0바이트에서 시작하므로, 패킷 페이로드의 시작에서 앞으로 이동하기를 원하는 바이트 수보다 하나 적은 수를 지정합니다. 예를 들어, 7을 지정한 경우, 검색은 여덟 번째 바이트에서 시작됩니다.

기본 오프셋은 0으로, 패킷의 시작을 의미합니다.

내부

참고 이 옵션은 `content` 키워드를 구성할 때만 지원됩니다.

Within(내부**)** 옵션은 규칙을 트리거하려면 다음 콘텐츠 일치가 마지막 콘텐츠 일치 종료 후 지정한 바이트 수 안에 발생해야 한다는 것을 나타냅니다. 예를 들어 **Within** 값으로 `8`을 지정하면 다음 내용 일치는 패킷 페이로드의 다음 8바이트 이내에 발생해야 합니다. 그렇지 않으면 규칙 트리거 기준이 충족되지 않습니다.

최대 65535바이트의 지정된 콘텐츠의 길이와 같거나 큰 값을 지정할 수 있습니다.

Within의 기본값은 패킷의 끝까지 검색하는 것입니다.

개요: **HTTP content** 및 **protected_content** 키워드 인수

HTTP `content` 또는 `protected_content` 키워드 옵션으로 인해 HTTP 검사 전처리기에서 디코딩된 HTTP 메시지 안에서 콘텐츠 일치를 검색할 위치를 지정할 수 있습니다.

두 가지 옵션은 HTTP 응답의 상태 필드를 검색합니다.

- **HTTP** 상태 코드
- **HTTP** 상태 메시지

규칙 엔진이 원시, 비정규 상태 필드를 검색하더라도 다른 원시 HTTP 필드 및 표준화된 HTTP 필드가 결합되면 이 옵션은 고려해야 할 제한 조건 하에서 설명을 간소화하기 위해 여기에 별도로 나열된다는 점에 유의하십시오.

다섯 가지 옵션은 적절한 수준에서 HTTP 요청이나 응답 또는 둘 다에서 표준화된 필드를 검색합니다.

- **HTTP URI**
- **HTTP** 메서드
- **HTTP** 헤더
- **HTTP** 쿠키
- **HTTP** 클라이언트 본문

세 가지 옵션은 적절한 수준에서 HTTP 요청이나 응답 또는 둘 다에서 원시(표준화되지 않은) 비상태 필드를 검색합니다.

- **HTTP** 원시 **URI**
- **HTTP** 원시 헤더
- **HTTP** 원시 쿠키

HTTP `content` 옵션을 선택할 때 다음 지침을 사용하십시오.

- HTTP `content` 옵션은 TCP 트래픽에만 적용됩니다.
- 성능에 부정적인 영향을 방지하려면, 지정된 내용이 표시될 수 있는 메시지의 해당 부분만 선택합니다.

  예를 들어, 쇼핑 카트 메시지에서처럼 트래픽이 규모가 큰 쿠키를 포함할 가능성이 높을 경우, HTTP 헤더에서 지정된 콘텐츠를 검색할 수 있지만 HTTP 쿠키에서는 검색할 수 없습니다.

- HTTP 검사 전처리기 표준화를 이용하고 성능을 향상시키려면, 사용자가 생성한 모든 HTTP 관련 규칙에 **HTTP URI**, **HTTP Method(HTTP** 메서드**)**, **HTTP Header(HTTP** 헤더**)** 또는 **HTTP Client Body(HTTP** 클라이언트 본문**)** 옵션이 선택된 최소한 하나의 `content` 또는 `protected_content` 키워드가 포함되어야 합니다.

- `replace` 키워드를 HTTP `content` 또는 `protected_content` 키워드 옵션과 함께 사용할 수 없습니다.

단일 표준화된 HTTP 옵션 또는 상태 필드를 지정하거나, 표준화된 HTTP 옵션 및 상태 필드를 어떤 조합에서나 사용하여 일치하는 콘텐츠 영역을 대상으로 할 수 있습니다. 그러나 HTTP 필드 옵션을 사용할 경우, 다음 제한 사항을 참고하십시오.

- **Raw Data** 옵션은 동일한 `content` 또는 `protected_content` 키워드에서 HTTP 옵션과 함께 사용할 수 없습니다.
- 원시 HTTP 필드 옵션(**HTTP Raw URI**, **HTTP Raw Header** 또는 **HTTP Raw Cookie**)을 동일한 `content` 또는 `protected_content` 키워드에서 해당 표준화 옵션(각각 **HTTP URI**, **HTTP Header** 또는 **HTTP Cookie**)과 함께 사용할 수 없습니다.
- 하나 이상의 다음 HTTP 필드 옵션과 함께 **Use Fast Pattern Matcher**를 선택할 수 없습니다.

  HTTP Raw URI(HTTP 원시 **URI)**, **HTTP Raw Header(HTTP** 원시 헤더**)**, **HTTP Raw Cookie(HTTP** 원시 쿠키**)**, **HTTP Cookie(HTTP** 쿠키**)**, **HTTP Method(HTTP** 메서드**)**, **HTTP Status Message(HTTP** 상태 메시지**)** 또는 **HTTP Status Code(HTTP** 상태 코드**)**

  그러나 다음의 표준화 필드 중 하나를 검색하는 데 역시 fast pattern matcher를 사용하는 `content` 또는 `protected_content` 키워드에는 위의 옵션을 포함할 수 있습니다.

  HTTP URI, **HTTP Header(HTTP** 헤더**)** 또는 **HTTP Client Body(HTTP** 클라이언트 본문**)**

  예를 들어, **HTTP Cookie(HTTP** 쿠키**)**, **HTTP** 헤더**(HTTP Header)**, 및 **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)**를 선택한 경우, 규칙 엔진은 HTTP 쿠키 및 HTTP 헤더 모두에서 콘텐츠를 검색하지만 빠른 패턴 매처는 HTTP 헤더에만 적용되고 HTTP 쿠키에는 적용되지 않습니다.

- 제한 옵션과 비제한 옵션을 결합하면 fast pattern matcher는 사용자가 지정한 비제한 필드만 검색하여, 제한된 필드에 대한 평가를 비롯한 완전한 평가를 위해 침입 규칙 편집기로 규칙을 전달할지 여부를 테스트합니다.

관련 항목

content 키워드 빠른 패턴 매처 인수, 2098 페이지

HTTP content 및 protected_content 키워드 인수

HTTP URI

이 옵션을 선택하여 표준화된 요청 URI 필드에서 콘텐츠 일치를 검색합니다.

같은 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP URI (U) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오.

참고 파이프라인 방식 HTTP 요청 패킷은 여러 URI를 포함합니다. **HTTP URL**을 선택하여 규칙 엔진이 파이프라인 방식 HTTP 요청 패킷을 탐지하면, 규칙 엔진은 콘텐츠 일치를 위해 패킷 내 모든 URI를 검색합니다.

HTTP 원시 URI

이 옵션을 선택하여 표준화된 요청 URI 필드에서 콘텐츠 일치를 검색합니다.

같은 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP URI (U) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오.

참고 파이프라인 방식 HTTP 요청 패킷은 여러 URI를 포함합니다. **HTTP URL**을 선택하여 규칙 엔진이 파이프라인 방식 HTTP 요청 패킷을 탐지하면, 규칙 엔진은 콘텐츠 일치를 위해 패킷 내 모든 URI를 검색합니다.

HTTP 메서드

이 옵션을 선택하여 요청 메서드 필드에서 콘텐츠 일치를 검색하는데, 이는 URI에서 식별된 리소스를 사용하는 GET 및 POST와 같은 작업을 확인합니다.

HTTP 헤더

이 옵션을 선택하여 표준화된 헤더 필드의 콘텐츠 일치를 검색하는데, HTTP 요청에서는 쿠키를 제외합니다. 또한 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션이 활성화된 응답에서도 쿠키를 제외합니다.

동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 헤더 (H) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오.

HTTP 원시 헤더

이 옵션을 선택하여 원시 헤더 필드의 콘텐츠 일치를 검색하는데, HTTP 요청에서는 쿠키를 제외합니다. 또한 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션이 활성화된 응답에서도 쿠키를 제외합니다.

동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 원시 헤더(D) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오.

HTTP 쿠키

표준화된 HTTP 클라이언트 요청 헤더에서 식별된 쿠키에서, 그리고 HTTP Inspect 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션이 활성화되었을 때 응답 set-cookie 데이터에서 내용 일치를 검색하려면 이 옵션을 선택합니다. 시스템이 본문 내용으로서의 메시지 본문에 포함되는 쿠키를 처리한다는 점에 유의하십시오.

반드시 HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)** 옵션을 활성화하여 일치하는 쿠키만 검색해야 합니다. 그렇지 않을 경우, 규칙 엔진은 쿠키를 포함하는 전체 헤더를 검색합니다.

다음 사항을 참고하십시오.

- 동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 쿠키 (C) 옵션과 조합하여 사용할 수 없습니다.
- `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.

HTTP 원시 쿠키

표준화된 HTTP 클라이언트 요청 헤더에서 식별된 쿠키에서, 그리고 HTTP Inspect 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션이 활성화되었을 때 응답 set-cookie 데이터에서 내용 일치를 검색하려면 이 옵션을 선택합니다. 시스템은 메시지 본문에 포함된 쿠키를 본문 내용으로 취급합니다.

반드시 HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)** 옵션을 활성화하여 일치하는 쿠키만 검색해야 합니다. 그렇지 않을 경우, 규칙 엔진은 쿠키를 포함하는 전체 헤더를 검색합니다.

다음 사항을 참고하십시오.

- 동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 원시 쿠키 (K) 옵션과 조합하여 사용할 수 없습니다.
- `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.

HTTP 클라이언트 본문

이 옵션을 선택하여 HTTP 클라이언트 요청에서 메시지 본문의 콘텐츠 일치를 검색합니다.

이 옵션이 작동하도록 하려면, HTTP 검사 전처리기 **HTTP Client Body Extraction Depth(HTTP** 클라이언트 본문 추출 수준**)** 옵션에 대해 0에서 65535까지의 값을 지정해야 합니다.

HTTP 상태 코드

HTTP 응답의 3자리 상태 코드에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션이 일치를 되돌릴 수 있도록 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션을 활성화해야 합니다.

HTTP 상태 메시지

이 옵션을 선택하여 HTTP 응답의 상태 코드에 동반되는 본문 설명에서 콘텐츠 일치를 검색합니다.

이 옵션이 일치를 되돌릴 수 있도록 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션을 활성화해야 합니다.

관련 항목

pcre 수식자 옵션, 2112 페이지
서버 레벨 HTTP 정상화 옵션, 2254 페이지

개요: **content** 키워드 빠른 패턴 매처

참고 `protected_content` 키워드를 구성할 때 이 옵션은 지원되지 않습니다.

빠른 패턴 매처는 패킷을 규칙 엔진에 전달하기 전에 평가할 규칙을 신속하게 결정합니다. 이 초기 결정은 패킷 평가에 사용되는 규칙의 수를 크게 줄여 성능을 개선합니다.

기본적으로, 빠른 패턴 매처는 규칙에 지정된 가장 긴 콘텐츠를 위한 패킷을 검색합니다. 이는 규칙의 필요 없는 평가를 최대한 제거하기 위한 것입니다. 다음의 예제 규칙 조각을 고려하십시오.

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

거의 모든 HTTP 클라이언트 요청은 `GET` 콘텐츠를 포함하지만, `/exploit.cgi` 콘텐츠를 포함하는 요청은 거의 없습니다. 빠른 패턴 콘텐츠로 `GET`을 사용하는 것은 대부분의 경우 규칙 엔진이 이 규칙을 평가하도록 하며 일치로 귀결되는 경우가 거의 없도록 합니다. 그러나 대부분의 클라이언트 `GET` 요청은 `/exploit.cgi`를 사용하여 평가되지 않을 것이므로 성능이 증가할 것입니다.

빠른 패턴 매처가 지정된 콘텐츠를 탐지하는 경우에만 규칙 엔진이 규칙에 대해 패킷을 평가합니다. 예를 들어, 규칙 내 하나의 `content` 키워드가 콘텐츠를 `short`로 지정하는데, 다른 키워드는 `longer`로 지정하고, 세 번째 키워드는 `longest`로 지정하는 경우, 빠른 패턴 매처는 `longest` 콘텐츠를 사용하며, 규칙 엔진이 페이로드에서 `longest`로 평가된 경우에만 규칙이 평가됩니다.

content 키워드 빠른 패턴 매처 인수

빠른 패턴 매처 사용

사용할 빠른 패턴 매처에 더 짧은 검색 패턴을 지정하려면 이 옵션을 사용합니다. 원칙적으로, 지정한 패턴은 패킷 내에서 발견될 가능성이 가장 긴 패턴보다 낮으므로 표적 공격을 더욱 구체적으로 식별합니다.

Use Fast Pattern Matcher 및 동일한 `content` 키워드의 다른 옵션을 선택할 때는 다음 제한 사항에 유의하십시오.

- 규칙당 한 번만 **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)**를 지정할 수 있습니다.
- **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)**를 **Not(**아님**)**과 함께 선택하는 경우 **Distance(**영역**)**, **Within(**내부**)**, **Offset(**오프셋**)** 또는 **Depth(**수준**)**를 사용할 수 없습니다.

- Use Fast Pattern Matcher(빠른 패턴 매처 사용)는 다음 HTTP 필드 옵션 중 어느 것과도 조합하여 선택할 수 없습니다.

  HTTP Raw URI(HTTP 원시 **URI)**, **HTTP Raw Header(HTTP** 원시 헤더**)**, **HTTP Raw Cookie(HTTP** 원시 쿠키**)**, **HTTP Cookie(HTTP** 쿠키**)**, **HTTP Method(HTTP** 메서드**)**, **HTTP Status Message(HTTP** 상태 메시지**)** 또는 **HTTP Status Code(HTTP** 상태 코드**)**

  그러나 다음의 표준화 필드 중 하나를 검색하는 데 역시 fast pattern matcher를 사용하는 `content` 키워드에는 위의 옵션을 포함할 수 있습니다.

  HTTP URI, **HTTP Header(HTTP** 헤더**)** 또는 **HTTP Client Body(HTTP** 클라이언트 본문**)**

  예를 들어, **HTTP Cookie(HTTP** 쿠키**)**, **HTTP** 헤더**(HTTP Header)**, 및 **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)**를 선택한 경우, 규칙 엔진은 HTTP 쿠키 및 HTTP 헤더 모두에서 콘텐츠를 검색하지만 빠른 패턴 매처는 HTTP 헤더에만 적용되고 HTTP 쿠키에는 적용되지 않습니다.

  원시 HTTP 필드 옵션(**HTTP Raw URI**, **HTTP Raw Header** 또는 **HTTP Raw Cookie**)을 동일한 `content` 키워드에서 해당 표준화 옵션(각각 **HTTP URI**, **HTTP Header** 또는 **HTTP Cookie**)과 함께 사용할 수 없습니다.

  제한 옵션과 무제한 옵션을 결합할 때, 빠른 패턴 매처는 사용자가 지정하는 무제한 필드만을 검색하여 제한된 필드의 평가를 포함하는 전체 평가를 위한 규칙 엔진으로 패킷을 전달할지 여부를 테스트합니다.

- 선택적으로, **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)**를 선택하면, **Fast Pattern Matcher Only(**빠른 패턴 매처 한정**)** 또는 **Fast Pattern Matcher Offset and Length(**빠른 패턴 매처 오프셋 및 길이**)** 중 하나를 선택할 수 있지만 둘 다 선택할 수는 없습니다.
- Base64 데이터를 검사할 때는 빠른 패턴 매처를 사용할 수 없습니다.

빠른 패턴 매처 한정

이 옵션을 선택하면 `content` 키워드를 규칙 옵션이 아니라 빠른 패턴 매처 옵션으로만 사용할 수 있습니다. 지정된 콘텐츠의 규칙 엔진 평가가 필요하지 않은 경우 이 옵션을 사용하여 리소스를 유지할 수 있습니다. 예를 들어, 콘텐츠 `12345`가 페이로드 안에서 어디든 있어야 한다고만 요구하는 규칙의 경우를 생각해 보십시오. 빠른 패턴 매처가 패턴을 탐지하면, 패킷이 규칙의 추가 키워드에 대해 평가될 수 있습니다. 패턴 `12345`를 포함하는지 확인하기 위해 패킷을 재평가하는 규칙 엔진은 없어도 됩니다.

규칙이 지정된 콘텐츠에 연결된 다른 조건을 포함할 때는 이 옵션을 사용하지 않습니다. 예를 들어, `abcd`가 `1234` 앞에 나타나는지를 다른 규칙 조건이 확인하는 경우 `1234` 내용을 검색하기 위해 이 옵션을 사용하지 않을 수 있습니다. 이 경우 규칙 엔진은 상대적인 위치를 파악할 수 없습니다. **Fast Pattern Matcher Only**를 지정하면 규칙 엔진은 지정된 내용을 검색하지 않기 때문입니다.

이 옵션을 사용할 때 다음 사항에 유의하십시오:

- 지정된 내용은 위치와 무관합니다. 즉, 페이로드 어디에서나 발생할 수 있습니다. 따라서 위치 옵션(**Distance(**영역**)**, **Within(**내부**)**, **Offset(**오프셋**)**, **Depth(**수준**)**, 또는 **Fast Pattern Matcher Offset and Length(**빠른 패턴 매처 오프셋 및 길이**)**)을 사용할 수 없습니다.
- 이 옵션을 **Not(**아님**)**과 조합하여 사용할 수 없습니다.

- 이 옵션을 **Fast Pattern Matcher Offset and Length(**빠른 패턴 매처 오프셋 및 길이**)**와 조합하여 사용할 수 없습니다.
- 모든 패턴이 빠른 패턴 매처에 대소문자 구분 없이 삽입되므로 지정된 내용에서는 대소문자가 구분되지 않습니다. 이는 자동으로 처리되므로 이 옵션을 선택할 때 **Case Insensitive(**대소문자 구분 안 함**)**를 선택할 필요가 없습니다.
- 사용자는 즉시 다음 키워드와 **Fast Pattern Matcher Only(**빠른 패턴 매처 한정**)** 옵션을 함께 사용하는 `content` 키워드를 따르지 말아야 하며, 이는 현재 검색 위치에 관련된 검색 위치를 설정하는 것입니다.
  - `isdataat`
  - `pcre`
  - **Distance(**영역**)** 또는 **Within(**내부**)**을 선택한 경우 `content`
  - **HTTP URI**를 선택한 경우 `content`
  - `asn1`
  - `byte_jump`
  - `byte_test`
  - `byte_extract`
  - `base64_decode`

빠른 패턴 매처 오프셋 및 길이

Fast Pattern Matcher Offset and Length(빠른 패턴 매처 오프셋 및 길이**)** 옵션을 사용하면 검색할 콘텐츠의 일부를 지정할 수 있습니다. 이는 패턴이 너무 길어 패턴의 일부만으로도 규칙을 가능한 일치로 확인하기에 충분한 경우 메모리 사용량을 줄일 수 있습니다. 규칙이 빠른 패턴 매처에서 선택되면, 규칙에 대해 전체 패턴이 평가됩니다.

다음 구문을 사용하여 검색을 시작할 위치(오프셋) 및 검색 범위(길이)를 바이트 단위로 지정함으로써 빠른 패턴 매처의 일부를 사용하기로 결정합니다.

```
offset,length
```

예를 들어, 다음과 같은 콘텐츠의 경우:

```
1234567
```

오프셋과 길이 바이트 수를 다음과 같이 지정할 경우:

```
1,5
```

빠른 패턴 매처가 콘텐츠 `23456`만 검색합니다.

이 옵션을 **Fast Pattern Matcher Only(**빠른 패턴 매처 한정**)**와 함께 사용할 수 없습니다.

관련 항목

개요: HTTP content 및 protected_content 키워드 인수, 2094 페이지
base64_decode 및 base64_data 키워드, 2181 페이지

replace 키워드

인라인 구축에서 `replace` 키워드를 사용하여 지정된 내용을 교체할 수 있습니다.

참고 `replace` 키워드를 사용하여 Cisco SSL Appliance가 탐지한 SSL 트래픽에서 내용을 교체할 수 없습니다. 교체 데이터가 아니라 원래 암호화된 데이터가 전송됩니다. 자세한 내용은 *Cisco SSL Appliance Administration and Deployment Guide(Cisco SSL Appliance* 관리 및 구축 가이드*)*를 참고하십시오.

`replace` 키워드를 사용하려면 `content` 키워드를 사용하여 특정 문자열을 찾는 맞춤형 표준 텍스트 규칙을 작성합니다. `replace` 키워드를 사용하여 콘텐츠를 대체할 문자열을 지정합니다. 대체 값 및 콘텐츠 값은 동일한 길이여야 합니다.

참고 `protected_content` 키워드 내 해시된 콘텐츠를 대체하기 위해 `replace` 키워드를 사용할 수 없습니다.

원하는 경우, 이전 Firepower System 소프트웨어 버전과의 호환을 위해 교체 문자열을 따옴표로 묶을 수 있습니다. 따옴표를 포함하지 않은 경우, 따옴표는 규칙에 자동으로 추가되므로 규칙은 구문적으로 정확합니다. 교체 텍스트의 일부로 앞뒤 따옴표를 포함하려면, 다음의 예시에서 볼 수 있듯이, 백슬래시를 사용하여 이스케이프해야 합니다.

```
"replacement text plus \"quotation\" marks""
```

규칙은 여러 `replace` 키워드를 포함할 수 있지만, `content` 키워드 하나당 하나만 포함됩니다. 규칙에서 찾은 콘텐츠의 첫 번째 인스턴스만 대체됩니다.

다음은 `replace` 키워드의 사용 예에 대한 설명입니다.

- 시스템이 공격을 포함한 수신 패킷을 탐지하는 경우, 악성 문자열을 무해한 것으로 바꿀 수 있습니다. 때때로 이 기술은 단순히 문제를 일으키는 패킷을 중단하는 것보다 더욱 성공적입니다. 일부 공격 시나리오에서, 공격자는 삭제된 패킷이 네트워크 방어를 무시하거나 네트워크를 초과할 때까지 다시 보냅니다. 패킷을 삭제하는 대신 다른 문자열로 한 문자열을 대체하여, 취약하지 않았던 대상에 대해 공격이 개시되었다고 공격자가 믿도록 속일 수 있습니다.
- 예를 들어, 취약한 버전의 웹 서버를 실행하고 있는지 여부를 알기 위해 시도하는 정찰 공격이 우려되는 경우, 발신 패킷을 탐지하고 본인의 텍스트로 배너를 바꿀 수 있습니다.

참고 대체 규칙을 사용하려는 인라인 침입 정책에서 규칙 상태를 Generate Events(이벤트 생성)로 설정했는지 확인합니다. 규칙을 Drop and Generate events(이벤트 중단 및 생성)로 설정하면 패킷이 중단될 수 있고, 이는 콘텐츠를 대체하는 것을 방지합니다.

문자열 교체 프로세스의 일부로서, 대상 호스트가 패킷을 오류 없이 받을 수 있도록 시스템은 자동으로 패킷 체크섬을 업데이트합니다.

`replace` 키워드를 HTTP 요청 메시지 `content` 키워드 옵션과 함께 사용할 수 없다는 점에 유의하십시오.

관련 항목

content 및 protected_content 키워드, 2088 페이지
개요: HTTP content 및 protected_content 키워드 인수, 2094 페이지

byte_jump 키워드

`byte_jump` 키워드는 지정된 바이트 세그먼트에서 정의된 바이트 수를 계산한 후 지정하는 옵션에 따라 지정된 바이트 세그먼트의 끝 또는 패킷 페이로드의 시작 또는 마지막 콘텐츠 일치와 관련된 지점에서부터 앞으로 패킷 내 바이트 수를 건너뜁니다. 이는 특정 세그먼트 바이트가 패킷 내 변수 데이터에 포함된 바이트 수를 설명하는 패킷에 유용합니다.

다음 표에서는 `byte_jump` 키워드에 필요한 인수에 대해 설명합니다.

표 ***157:*** 필수 ***byte_jump*** 인수

인수	설명
바이트	패킷에서 추출할 바이트 수입니다. DCE/RPC 없이 사용하는 경우, 허용되는 값은 1 ~ 10이며 다음 제한 사항이 적용됩니다. • • 1, 2 또는 4 이외의 바이트 수를 지정하는 경우, 숫자 유형(16진수, 8진수 또는 10진수)을 지정해야 합니다. DCE/RPC와 함께 사용하는 경우, 허용되는 값은 1, 2, 4입니다.
Offset	처리를 시작할 페이로드에 들어가는 바이트 수. `offset` 카운터는 0바이트부터 시작되므로, `offset` 값을 계산할 때는 패킷 페이로드의 처음부터 또는 마지막으로 성공한 내용 일치로부터 앞으로 이동하려는 바이트 수에서 1을 빼야 합니다. -65535에서 65535까지 바이트를 지정할 수 있습니다. 기존의 `byte_extract` 변수를 사용하여 이 인수의 값을 지정할 수도 있습니다.

다음 표에서는 시스템이 필수 인수에 지정한 값을 해석하는 방식을 정의하는 데 사용할 수 있는 옵션을 설명합니다.

표 *158:* 추가 선택 ***byte_jump*** 인수

인수	설명
Relative	오프셋이 마지막으로 성공한 콘텐츠 일치에 포함된 마지막 패턴에 연결되도록 합니다.
Align	변환된 바이트의 수를 다음 32비트 경계로 반올림합니다.
Multiplier	규칙 엔진이 최종 `byte_jump` 값을 얻기 위해 패킷에서 얻은 `byte_jump` 값에 곱해야 하는 값을 나타냅니다. 즉 규칙 엔진은 지정된 바이트 세그먼트에서 정의한 바이트 수를 건너뛰는 대신, Multiplier 인수로 지정한 정수로 곱해진 바이트 수를 건너뜁니다.
Post Jump Offset	다른 `byte_jump` 인수를 적용한 후 앞이나 뒤로 건너뛸 -63535~63535 범위의 바이트 수입니다. 양수 값은 앞으로 건너뛰고 음수 값은 뒤로 건너뜁니다. 필드를 비워 두거나 `0`을 입력하여 비활성화합니다. **DCE/RPC** 인수를 선택할 경우, 일부 `byte_jump` 인수가 적용되지 않습니다.
From Beginning	규칙 엔진이 패킷의 현재 위치부터가 아니라 패킷 페이로드의 처음부터 시작하는 페이로드 내 지정된 바이트 수를 건너뛰어야 한다고 표시합니다.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

`byte_jump` 키워드가 바이트를 계산하는 방법을 정의하려는 경우, 다음 표에 설명된 인수 중에서 선택할 수 있습니다. 바이트 순서 인수를 선택하지 않으면 규칙 엔진은 Big Endian 바이트 순서를 사용합니다.

표 *159:* 바이트 순서 ***byte_jump*** 인수

인수	설명
Big Endian	빅 엔디언 바이트 순서의 프로세스 데이터. 기본 네트워크 바이트 순서입니다.
Little Endian	리틀 엔디언 순서의 프로세스 데이터
DCE/RPC	DCE/RPC 전처리기에서 처리된 트래픽에 `byte_jump` 키워드를 지정합니다. DCE/RPC 전처리기는 빅 엔디언 또는 리틀 엔디언 바이트 순서를 결정하고, **Number Type** 및 **Endian** 인수는 적용되지 않습니다. 이 인수를 활성화하면, `byte_jump`를 다른 DCE/RPC 특정 키워드와 함께 사용할 수 있습니다.

시스템이 다음 표에 있는 인수 중 하나를 사용하여 패킷 내 문자열을 보는 방식을 정의합니다.

표 160: 번호 유형 인수

인수	설명
Hexadecimal String	변환된 문자열 데이터를 16진수 형태로 나타냅니다.
Decimal String	변환된 문자열 데이터를 십진수 형태로 나타냅니다.
Octal String	변환된 문자열 데이터를 8진수 형태로 나타냅니다.

예를 들어 byte_jump에 대해 설정한 값이 다음과 같으면

- Bytes = 4
- Offset = 12
- Relative 활성화
- Align 활성화

규칙 엔진은 마지막으로 성공한 콘텐츠 일치 후 13바이트를 나타내는 4개의 바이트로 표시된 수를 계산하고, 패킷 내 해당 수의 바이트를 건너뜁니다. 예를 들어, 특정 패킷 내 4개의 계산된 바이트가 00 00 00 1F인 경우, 규칙 엔진은 이를 31로 환산합니다. 엔진에 다음 32비트 경계로 이동하도록 지시하는 align이 지정되었으므로 규칙 엔진은 패킷에서 32바이트 앞으로 건너뜁니다.

또는 byte_jump에 대해 설정한 값이 다음과 같으면

- Bytes = 4
- Offset = 12
- From Beginning 활성화
- Multiplier = 2

규칙 엔진은 패킷의 시작 후 13바이트를 나타내는 4개의 바이트로 표시된 수를 계산합니다. 다음, 엔진은 이 수에 2를 곱하여 건너뛸 총 바이트 수를 얻습니다. 예를 들어, 특정 패킷 내 4개의 계산된 바이트가 00 00 00 1F인 경우, 규칙 엔진은 이를 31로 환산한 후 2를 곱하여 62를 얻습니다. From Beginning이 활성화되어 있으므로, 규칙 엔진은 패킷의 처음 63바이트를 건너뜁니다.

관련 항목

byte_extract 키워드, 2106 페이지
DCE/RPC 키워드, 2139 페이지

byte_test 키워드

byte_test 키워드는 Value 인수 및 연산자에 대해 지정된 바이트 세그먼트를 테스트합니다.

다음 표에서는 byte_test 키워드에 필요한 인수에 대해 설명합니다.

표 161: 필수 byte_test 인수

인수	설명
바이트	패킷에서 계산할 바이트 수. DCE/RPC 없이 사용하는 경우, 허용되는 값은 1 ~ 10입니다. 하지만 1, 2 또는 4 이외의 바이트 수를 지정하는 경우, 숫자 유형(16진수, 8진수 또는 10진수)을 지정해야 합니다. DCE/RPC와 함께 사용하는 경우, 허용되는 값은 1, 2, 4입니다.
Value	해당 연산자를 포함하여 테스트할 값입니다. 지원되는 연산자: <, >, =, !, &, ^, !>, !<, !=, !& 또는 !^. 예를 들어 `!1024`를 지정하면 `byte_test`는 지정된 숫자를 변환하고, 이 숫자가 1024와 같지 않으면 이벤트를 생성합니다(다른 모든 키워드 파라미터가 일치하는 경우). !와 !=는 같다는 점에 유의하십시오. 기존의 `byte_extract` 변수를 사용하여 이 인수의 값을 지정할 수도 있습니다.
Offset	처리를 시작할 페이로드에 들어가는 바이트 수. `offset` 카운터는 0바이트부터 시작되므로, `offset` 값을 계산할 때는 패킷 페이로드의 처음부터 또는 마지막으로 성공한 내용 일치로부터 앞으로 이동하려는 바이트 수에서 1을 빼야 합니다. 기존의 `byte_extract` 변수를 사용하여 이 인수의 값을 지정할 수 있습니다.

시스템에서 다음 표에 설명된 인수와 함께 `byte_test` 인수를 사용하는 방법을 더 정의할 수 있습니다.

표 162: 추가 선택 byte_test 인수

인수	설명
Relative	오프셋이 마지막으로 성공한 패턴 일치와 연결되도록 합니다.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

`byte_test` 키워드가 테스트할 바이트를 계산하는 방법을 정의하려면, 다음 표의 인수 중에서 선택합니다. 바이트 순서 인수를 선택하지 않으면 규칙 엔진은 Big Endian 바이트 순서를 사용합니다.

표 163: 바이트 순서 byte_test 인수

인수	설명
Big Endian	빅 엔디언 바이트 순서의 프로세스 데이터. 기본 네트워크 바이트 순서입니다.
Little Endian	리틀 엔디언 순서의 프로세스 데이터

인수	설명
DCE/RPC	DCE/RPC 전처리기에서 처리된 트래픽에 byte_test 키워드를 지정합니다. DCE/RPC 전처리기는 빅 엔디언 또는 리틀 엔디언 바이트 순서를 결정하고, **Number Type** 및 **Endian** 인수는 적용되지 않습니다. 이 인수를 활성화하면, byte_test를 다른 DCE/RPC 특정 키워드와 함께 사용할 수 있습니다.

시스템이 다음 표에 있는 인수 중 하나를 사용하여 패킷 내 문자열 데이터를 보는 방식을 정의할 수 있습니다.

표 ***164:*** 번호 유형 ***byte-test*** 인수

인수	설명
Hexadecimal String	변환된 문자열 데이터를 16진수 형태로 나타냅니다.
Decimal String	변환된 문자열 데이터를 십진수 형태로 나타냅니다.
Octal String	변환된 문자열 데이터를 8진수 형태로 나타냅니다.

예를 들어, byte_test에 대한 값이 다음과 같이 지정된 경우:

- Bytes = 4
- Operator 및 Value > 128
- Offset = 8
- Relative 활성화

규칙 엔진은 마지막으로 성공한 내용 일치에서 9바이트 떨어진 곳에 나타나는 4바이트에 설명된 숫자를 계산하고, 계산된 숫자가 128바이트보다 크면 규칙을 트리거합니다.

관련 항목

byte_extract 키워드, 2106 페이지
DCE/RPC 키워드, 2139 페이지

byte_extract 키워드

byte_extract 키워드를 사용하여 패킷에서 지정한 바이트 수를 변수로 읽을 수 있습니다. 해당 변수는 나중에 동일한 규칙에서 다른 특정 검색 키워드 내 특정 인수에 대한 값으로 사용할 수 있습니다.

예를 들면, 이는 특정 세그먼트 바이트가 패킷 내 데이터에 포함된 바이트 수를 나타내는 패킷에서 데이터 크기를 추출하는 데 유용합니다. 예를 들어, 특정 세그먼트 바이트는 후속 데이터가 4바이트로 구성되어 있다고 표시할 수 있습니다. 사용자는 사용자 변수 값으로 사용하기 위해 4바이트의 데이터 크기를 추출할 수 있습니다.

byte_extract를 사용하여 규칙에서 최대 두 개의 개별 변수를 동시에 만들 수 있습니다. 몇 번이든 byte_extract 변수를 재정의할 수 있습니다. 동일한 변수 이름 및 기타 변수 정의를 새로운 byte_extract 키워드와 함께 입력하면 해당 변수의 이전 정의를 덮어씁니다.

다음 표에서는 byte_extract 키워드에 필요한 인수에 대해 설명합니다.

표 ***165:*** 필수 ***byte_extract*** 인수

인수	설명
Bytes to Extract	패킷에서 추출할 바이트 수. 1, 2 또는 4 이외의 바이트 수를 지정하는 경우, 숫자 유형(16진수, 8진수 또는 10진수)을 지정해야 합니다.
Offset	데이터 추출을 시작할 페이로드 내 바이트 수. -65535에서 65535까지 바이트를 지정할 수 있습니다. 오프셋 카운터는 0바이트에서 시작하므로, 계산에 넣으려는 바이트 수에서 1을 빼 오프셋 값을 계산합니다. 예를 들어, 8바이트를 계산에 넣으려면 7을 지정합니다. 규칙 엔진은 패킷의 페이로드의 처음부터 계산에 넣거나 사용자가 또한 **Relative(**연결**)**를 지정한 경우, 마지막으로 성공한 콘텐츠 일치 후에 계산에 넣습니다. 음수는 **Relative**를 지정한 경우에만 지정할 수 있습니다.
Variable Name	다른 탐지 키워드에 대한 인수에 사용할 변수 이름입니다. 영숫자 문자열이 반드시 문자로 시작되도록 지정할 수 있습니다.

시스템이 추출할 데이터를 찾는 방식을 더욱 자세히 정의하려면 다음 표에 설명된 인수를 사용할 수 있습니다.

표 ***166:*** 추가 옵션 ***byte_extract*** 인수

인수	설명
Multiplier	패킷에서 추출된 값에 대한 승수입니다. 0에서 65535를 지정할 수 있습니다. 승수를 지정하지 않은 경우, 기본값은 1입니다.
Align	추출된 값을 가장 가까운 2바이트 또는 4바이트 경계로 반올림합니다. 또한 **Multiplier**를 선택하는 경우, 시스템은 정렬 전에 승수를 적용합니다.
Relative	**Offset**이 페이로드의 시작 대신 마지막으로 성공한 콘텐츠 일치의 끝에 연결되도록 합니다.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

byte_extract 키워드가 테스트할 바이트를 계산하는 방법을 정의하려면, 다음 표의 인수 중에서 선택합니다. 바이트 순서 인수를 선택하지 않으면 규칙 엔진은 Big Endian 바이트 순서를 사용합니다.

표 ***167:*** 바이트 순서 ***byte_extract*** 인수

인수	설명
Big Endian	빅 엔디언 바이트 순서의 프로세스 데이터. 기본 네트워크 바이트 순서입니다.
Little Endian	리틀 엔디언 순서의 프로세스 데이터
DCE/RPC	DCE/RPC 전처리기에서 처리된 트래픽에 `byte_extract` 키워드를 지정합니다. DCE/RPC 전처리기는 빅 엔디언 또는 리틀 엔디언 바이트 순서를 결정하고, **Number Type** 및 **Endian** 인수는 적용되지 않습니다. 이 인수를 활성화하면, `byte_extract`를 다른 DCE/RPC 특정 키워드와 함께 사용할 수도 있습니다.

데이터를 ASCII 문자열로 읽으려면 숫자 유형을 지정할 수 있습니다. 다음 표에 있는 인수 중 하나를 선택하여 패킷 내 문자열 데이터를 보는 방식을 정의할 수 있습니다.

표 ***168:*** 번호 유형 ***byte_extract*** 인수

인수	설명
Hexadecimal String	추출된 문자열 데이터를 16진수 형태로 읽습니다.
Decimal String	추출된 문자열 데이터를 십진수 형태로 읽습니다.
Octal String	추출된 문자열 데이터를 8진수 형태로 읽습니다.

예를 들어, `byte_extract`에 대한 값이 다음과 같이 지정된 경우

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative = 활성화

규칙 엔진은 마지막으로 성공한 콘텐츠 일치(에 연결)에서 9바이트 떨어져서 나타나는 네 개의 바이트에 설명된 번호를 `var`로 명명된 변수로 읽는데, 이는 나중에 규칙에서 특정 키워드 인수에 대한 값으로 지정할 수 있습니다.

다음 표는 `byte_extract` 키워드에 정의된 변수를 지정할 수 있는 키워드 인수를 나열합니다.

표 ***169: byte_extract*** 변수를 받아들이는 인수

키워드	인수
content	Depth, Offset, Distance, Within
byte_jump	Offset(오프셋)

키워드	인수
byte_test	Offset, Value
isdataat	Offset(오프셋)

관련 항목

DCE/RPC 전처리기, 2228 페이지
DCE/RPC 키워드, 2139 페이지
기본 content 또는 protected_content 키워드 인수, 2090 페이지
byte_jump 키워드, 2102 페이지
byte_test 키워드, 2104 페이지
패킷 특성, 2163 페이지

개요: pcre 키워드

`pcre` 키워드를 사용하면 PCRE(Perl-compatible regular expression)를 사용하여 패킷 페이로드에서 지정된 내용을 검사할 수 있습니다. PCRE를 사용하여 동일한 콘텐츠의 약간의 차이에 따라 일치하는 여러 규칙을 작성하는 것을 방지할 수 있습니다.

정규 표현식은 다양한 방법으로 표시할 수 있는 콘텐츠를 검색할 때 유용합니다. 콘텐츠는 패킷의 페이로드에서 메시지를 찾는 시도에서 고려할 다른 특성을 가질 수 있습니다.

침입 규칙에서 사용되는 정규 표현식 구문은 전체 정규 표현식의 하위 집합이며, 전체 라이브러리의 지침에 사용되는 구문에서 어느 정도 변경된다는 점에 유의하십시오. 규칙 편집기를 사용하여 `pcre` 키워드를 추가할 경우, 전체 값을 다음 형식으로 입력합니다.

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

여기에서 각 항목은 다음을 나타냅니다.

- !는 선택적 무효화입니다(정규 표현식에 일치하지 않는 패턴에 일치시키기를 원할 때 이를 사용합니다).
- /pcre/는 Perl 호환 정규 표현식입니다.
- `ismxAEGRBUIPHDMCKSY` 수식자 옵션의 모든 조합입니다.

패킷 페이로드에서 특정 콘텐츠를 검색하기 위해 PCRE에서 이들을 사용할 때 규칙 엔진이 정확하게 해석할 수 있도록 하려면 다음 표에 나열된 문자를 이스케이프해야 한다는 점에 유의하십시오.

표 ***170:*** 이스케이프된 ***PCRE*** 문자

이스케이프 대상	백슬래시	헥사 코드
#(해시 부호)	\#	\x23
;(세미콜론)	\;	\x3B

이스케이프 대상	백슬래시	헥사 코드
|(세로 선)	|	\x7C
:(콜론)	\:	\x3A

또한 /가 아닌 ?가 구분 문자일 때 `m?regex?`를 사용할 수 있습니다. 정규 표현식에서 슬래시와 일치해야 하는 상황에서 이를 사용하고자 할 수도 있지만 백슬래시로 이스케이프하지 않습니다. 예를 들어 `m?`regex`? ismxAEGRBUIPHDMCKSY`를 사용할 수 있습니다. 여기서 regex는 Perl 호환 정규 표현식이고 `ismxAEGRBUIPHDMCKSY`는 수식자 옵션의 임의의 조합입니다.

팁 원하는 경우, Perl 호환 정규 표현식을 따옴표로 묶을 수 있습니다(예: pcre_expression 또는 “pcre_expression“). 따옴표 사용 옵션은 따옴표가 선택 사항이 아닌 필수인 경우 이전 버전에 익숙한 기존 사용자에게 제공됩니다. 침입 규칙 편집기는 보고서를 저장한 후 규칙을 표시할 때 따옴표를 표시하지 않습니다.

pcre 구문

`pcre` 키워드는 표준 Perl 호환 정규 표현식(PCRE) 구문을 허용합니다. 다음 섹션에서는 각 구문에 대해 설명합니다.

팁 이 섹션은 PCRE에 사용할 수 있는 기본 구문을 설명하지만, 더 많은 고급 정보를 Perl(펄) 및 PCRE에 할애하는 온라인 참조 또는 도서를 참고할 수 있습니다.

메타 문자

메타 문자는 정규 표현식에서 특정 의미가 있는 리터럴 문자입니다. 정규 표현식에서 이를 사용할 때, 이들 앞에 백슬래시를 두어 "이스케이프"해야 합니다.

다음 표에서는 PCRE에 사용할 수 있는 메타 문자를 설명하고 각각의 예를 제공합니다.

표 ***171: PCRE*** 메타 문자

메타 문자	설명	예
.	줄 바꿈을 제외한 모든 문자와 일치합니다. `s`가 수정 옵션으로 사용되는 경우, 이는 또한 줄 바꿈 문자를 포함합니다.	`abc.`는 `abcd`, `abc1`, `abc#` 등에 일치시킵니다.
*	0 이상의 문자 또는 표현이 나타나는 것에 일치시킵니다.	`abc*`는 `abc`, `abcc`, `abccc`, `abcccccc` 등에 일치시킵니다.
?	0 또는 하나의 문자/표현이 나타나는 것에 일치시킵니다.	`abc?`는 `abc`에 일치시킵니다.

메타 문자	설명	예
+	하나 이상의 문자 또는 표현이 나타나는 것에 일치시킵니다.	abc+는 abc, abcc, abccc, abcccccc 등에 일치시킵니다.
()	표현을 그룹화합니다.	(abc)+는 abc, abcabc, abcabcabc 등에 일치시킵니다.
{}	문자 또는 표현에 일치하는 수에 대한 한계를 지정합니다. 상한 및 하한을 설정하고자 하는 경우, 쉼표로 상한 및 하한을 구분합니다.	a{4,6}은 aaaa, aaaaa 또는 aaaaaa에 일치시킵니다. (ab){2}는 abab에 일치시킵니다.
[]	문자 클래스를 정의하도록 허용하며, 집합에 설명된 문자의 조합 또는 모든 문자에 일치시킵니다.	[abc123]은 a 또는 b 또는 c 등에 일치시킵니다.
^	문자열의 시작 지점에 있는 콘텐츠에 일치시킵니다. 문자 클래스 내에서 사용되는 경우에도 무효화에 사용됩니다.	^in은 info 내 "in"에 일치하지만, bin에서는 일치하지 않습니다. [^a]은 a를 포함하지 않는 모든 문자열에 일치합니다.
$	문자열이 끝나는 지점에 있는 콘텐츠에 일치시킵니다.	ce$는 announce 내 "ce"에 일치하지만, cent에서는 일치하지 않습니다.
|	또는(OR) 표현을 나타냅니다.	(MAILTO|HELP)는 MAILTO 또는 HELP에 일치시킵니다.
\	메타 문자를 실제 문자로 사용할 수 있으며, 미리 정의된 문자 클래스를 지정하는 데 사용할 수도 있습니다.	\.는 기간에 일치하고, *는 별표에 일치하며, \\는 백슬래시에 일치합니다. \d는 숫자에 일치하며, \w는 영숫자에 일치합니다.

문자 클래스

문자 클래스는 알파벳 문자, 영숫자, 숫자 및 공백 문자를 포함합니다. 괄호 안에서 자체 문자 클래스를 만들 수도 있지만 다른 유형의 문자 유형에 대한 바로 가기로 사전 정의된 클래스를 사용할 수도 있습니다. 추가 수식자 없이 사용할 경우, 문자 클래스는 한 자릿수 또는 문자와 일치됩니다.

다음 표에서는 PCRE가 수용한 사전 정의된 문자 클래스의 예를 설명하고 제공합니다.

표 ***172: PCRE*** 문자 클래스

문자 클래스	설명	문자 클래스 정의
\d	숫자 문자("디지트")에 일치합니다.	[0-9]
\D	숫자 문자가 아닌 모든 문자에 일치합니다.	[^0-9]
\w	영숫자 문자("단어")에 일치합니다.	[a-zA-Z0-9_]
\W	영숫자 문자가 아닌 모든 문자에 일치합니다.	[^a-zA-Z0-9_]

문자 클래스	설명	문자 클래스 정의
\s	공백, 복귀, 탭, 줄 바꿈 및 서식 이송을 포함하여 공백 문자에 일치시킵니다.	[\r\t\n\f]
\S	공백 문자가 아닌 모든 문자에 일치시킵니다.	[^ \r\t\n\f]

pcre 수식자 옵션

pcre 키워드 값의 정규 표현식 구문을 지정한 후 변경 옵션을 사용할 수 있습니다. 이러한 수정자는 Perl, PCRE 및 Snort 관련 처리 기능을 수행합니다. 수식자는 언제나 PCRE 값의 끝에 표시되며, 다음과 같은 형식으로 표시됩니다.

```
/pcre/ismxAEGRBUIPHDMCKSY
```

이 경우 ismxAEGRBUPHMC가 다음 표에 나타나는 모든 수정 옵션을 포함할 수 있습니다.

팁 또는, 정규 표현식 및 모든 수정 옵션을 따옴표로 둘러쌀 수 있습니다(예: "/pcre/ismxAEGRBUIPHDMCKSY"). 따옴표 사용 옵션은 따옴표가 선택 사항이 아닌 필수인 경우 이전 버전에 익숙한 기존 사용자에게 제공됩니다. 침입 규칙 편집기는 보고서를 저장한 후 규칙을 표시할 때 따옴표를 표시하지 않습니다.

다음 표에서는 사용자가 Perl 처리 기능을 수행하는 데 사용할 수 있는 옵션을 설명합니다.

표 ***173: Perl*** 관련 게시물 정규 표현식 옵션

옵션	설명
i	정규 표현식에서 대소문자를 구분하지 않도록 합니다.
s	점 문자(.)는 줄 바꿈 또는 \n 문자를 제외한 모든 문자를 설명합니다. "s" 를 옵션으로 사용하여 이를 무시할 수 있으며, 점 문자가 줄 바꿈 문자를 포함한 모든 문자에 일치하도록 할 수 있습니다.
m	기본적으로, 문자열은 문자의 단선으로 처리되며, ^ 및 $는 특정 문자열의 시작 및 끝 지점에 일치됩니다. "m"을 옵션으로 사용할 때, ^ 및 $는 버퍼의 시작 또는 끝부분뿐만 아니라 버퍼에서 모든 줄 바꿈 문자 바로 앞 또는 바로 뒤 콘텐츠에 일치시킵니다.
x	패턴에 나타날 수 있는 공백 데이터 문자를 무시합니다. 이스케이프 되었을 때(앞에 백슬래시가 있을 때) 또는 문자 클래스 안에 포함되었을 때는 제외합니다.

다음 표에서는 정규 표현식 뒤에 사용할 수 있는 PCRE 수식자를 설명합니다.

표 ***174: PCRE*** 관련 게시물 정규 표현식 옵션

옵션	설명
A	패턴은 문자열의 시작 지점과 일치해야 합니다(정규 표현식의 ^를 사용하는 것과 동일).
E	$가 제목 문자열 끝에만 일치하도록 설정합니다. (마지막 문자가 줄바꿈인 경우 E가 없는 $는 또한 마지막 문자 바로 앞에 일치하지만 다른 모든 줄바꿈 문자 앞에서는 일치하지 않습니다).
G	기본적으로, * + 및 ?는 "최대값에 일치"시킵니다. 이는 두 개 이상의 일치가 발견되는 경우, 가장 긴 일치 항목을 선택한다는 것을 의미합니다. 이를 변경하려면 G 문자를 사용하며, 이는 그 뒤에 물음표 문자(?)가 나오지 않는 한 이 문자들이 항상 첫 번째 일치 항목을 선택하도록 하기 위한 것입니다. 예를 들면 *? +? 및 ??는 G 수식자를 사용하는 구조에서 최대값에 일치시킵니다. 그리고 추가적인 물음표가 없는 *, + 또는 ?의 모든 예는 최대값에 일치시키지 않습니다.

다음 표에서는 정규 표현식 뒤에 사용할 수 있는 Snort 특정 수식자를 설명합니다.

.

표 ***175: Snort*** 특정 게시물 정규 표현식 수식자

옵션	설명
R	규칙 엔진으로 발견된 마지막 일치 끝부분과 관련된 일치하는 콘텐츠를 검색합니다.
B	전처리기에서 해독하기 전에 데이터 내의 내용을 검색합니다(이 옵션은 Raw Data 인수와 content 또는 protected_content 키워드를 함께 사용하는 것과 유사합니다).
U	HTTP 검사 전처리기에서 해독된 표준화된 HTTP 요청 메시지에 대해 URI 내의 콘텐츠를 검색합니다. 이 옵션은 content 또는 protected_content 키워드 **HTTP URI** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 파이프라인된 HTTP 요청 패킷에는 여러 URI가 포함되어 있습니다. U 옵션을 포함하는 PCRE 표현은 규칙 엔진이 파이프라인 방식 HTTP 요청 패킷의 첫 URI에서만 콘텐츠 일치를 검색하도록 합니다. 패킷의 모든 URI를 검색하려면 U 옵션을 사용하는 동반 PCRE 식의 유무와 상관없이 content 또는 protected_content 키워드와 함께 **HTTP URI**를 선택하십시오.
I	HTTP 검사 전처리기에서 해독된 원시 HTTP 요청 메시지에 대해 URI 내의 콘텐츠를 검색합니다. 이 옵션은 content 또는 protected_content 키워드 **HTTP Raw URI** 옵션과 조합하여 동일한 내용을 검색하는 데 사용할 수 없습니다.
P	HTTP 검사 전처리기에서 해독된 표준화된 HTTP 요청 메시지에 대해 본문 내의 콘텐츠를 검색합니다.

옵션	설명
H	HTTP 검사 전처리기에서 해독된 HTTP 요청 또는 응답 메시지의 헤더 내 콘텐츠를 검색합니다. 쿠키는 제외합니다. 이 옵션은 `content` 또는 `protected_content` 키워드 **HTTP Header** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다.
D	HTTP 검사 전처리기에서 해독된 원시 HTTP 요청 또는 응답 메시지의 헤더 내 콘텐츠를 검색합니다. 쿠키는 제외합니다. 이 옵션은 `content` 또는 `protected_content` 키워드 **HTTP Raw Header** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다.
M	HTTP 검사 전처리기에서 해독된 표준화된 HTTP 요청 메시지의 메서드 필드에서 콘텐츠를 검색합니다. 메서드 필드는 URI에서 식별된 리소스를 만들기 위해 GET, PUT, CONNECT 등의 작업을 식별합니다.
C	HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)** 옵션이 활성화되면 HTTP 요청 헤더의 모든 쿠키 내 표준화된 콘텐츠를 검색합니다. 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션이 활성화되면 HTTP 응답 헤더의 모든 set-cookie 내 표준화된 콘텐츠도 검색합니다. **Inspect HTTP Cookies(HTTP** 쿠키 검사**)**가 활성화되지 않은 경우, 쿠키 또는 set-cookie 데이터를 포함한 전체 헤더를 검색합니다. 다음 사항을 참고하십시오. • 메시지 본문에 포함된 쿠키는 본문 콘텐츠로 처리됩니다. • 이 옵션은 `content` 또는 `protected_content` 키워드 **HTTP Cookie** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. • `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.

옵션	설명
K	HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)** 옵션이 활성화되면 HTTP 요청 헤더의 모든 쿠키 내의 원시 콘텐츠를 검색합니다. 전처리기 **Inspect HTTP Responses(HTTP** 응답 검사**)** 옵션이 활성화되면 HTTP 응답 헤더의 모든 set-cookie 내 표준화된 콘텐츠를 검색합니다. **Inspect HTTP Cookies(HTTP** 쿠키 검사**)**가 활성화되지 않은 경우, 쿠키 또는 set-cookie 데이터를 포함한 전체 헤더를 검색합니다. 다음 사항을 참고하십시오. • 메시지 본문에 포함된 쿠키는 본문 콘텐츠로 처리됩니다. • 이 옵션은 `content` 또는 `protected_content` 키워드 **HTTP Raw Cookie** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. • `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.
S	HTTP 응답에서 3자리 상태 코드를 검색합니다.
Y	HTTP 응답의 상태 코드를 동반하는 텍스트 설명을 검색합니다.

참고 U 옵션을 R 옵션과 함께 사용하지 마십시오. 이는 성능 문제를 야기할 수 있습니다. 또한, U 옵션을 다른 HTTP 콘텐츠 옵션(I, P, H, D, M, C, K, S, 또는 Y)과 함께 사용하지 마십시오.

관련 항목

개요: HTTP content 및 protected_content 키워드 인수, 2094 페이지

pcre 예시 키워드 값

다음의 예시는 일치하는 각 예의 설명과 함께 `pcre`에 입력할 수 있는 값을 보여줍니다.

- **`/feedback[(\d{0,1})]?\.cgi/U`**

이 예는 feedback 뒤에 0 또는 1개의 숫자 문자와 `.cgi`가 차례로 나오며 URI 데이터에만 위치하는 `feedback`에 대한 패킷 페이로드를 검색합니다.

이 예는 다음에 일치됩니다.

- `feedback.cgi`
- `feedback1.cgi`
- `feedback2.cgi`
- `feedback3.cgi`

이 예는 다음과 일치되지 않습니다.

- `feedbacka.cgi`
- `feedback11.cgi`
- `feedback21.cgi`
- `feedbackzb.cgi`

- **`/^ez(\w{3,5})\.cgi/iU`**

이 예제는 패킷 페이로드에서 문자열의 처음에 나오는 `ez`, 그 뒤에 3~5개의 문자로 구성된 단어, 그리고 그 뒤에 `.cgi`를 검색합니다. 검색은 대소문자를 구분하지 않으며 URI 데이터만 검색합니다.

이 예는 다음에 일치됩니다.

- `EZBoard.cgi`
- `ezman.cgi`
- `ezadmin.cgi`
- `EZAdmin.cgi`

이 예는 다음과 일치되지 않습니다.

- `ezez.cgi`
- `fez.cgi`
- `abcezboard.cgi`
- `ezboardman.cgi`

- **`/mail(file|seek)\.cgi/U`**

이 예는 mail 뒤에 `file` 또는 `seek`이 나오며 URI 데이터에 있는 `mail`에 대한 패킷 페이로드를 검색합니다.

이 예는 다음에 일치됩니다.

- `mailfile.cgi`
- `mailseek.cgi`

이 예는 다음과 일치되지 않습니다.

- `MailFile.cgi`
- `mailfilefile.cgi`

- **`m?http\\x3a\x2f\x2f.*(\n|\t)+?U`**

이 예는 HTTP 요청의 탭 또는 줄 바꿈 문자에 대한 URI 콘텐츠의 패킷 페이로드를 검색하며, 어떤 수의 문자가 앞에 와도 됩니다. 이 예는 `m?`regex`?`를 사용하여 표현식에서 `http\:\/\/`를 사용하는 것을 방지합니다. 콜론은 백슬래시 앞에 위치한다는 점을 참고하십시오.

이 예는 다음에 일치됩니다.

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

이 예는 다음과 일치되지 않습니다.

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

이 예에서는 등호 및 모든 수의 문자를 포함하는 파이프 문자 또는 공백이 뒤따르는 줄 바꿈을 포함하는 모든 문자 수와 함께 URL에 대한 패킷 페이로드를 검색합니다. 이 예는 `m?`regex`?`를 사용하여 표현식에서 `http\:\/\/`를 사용하는 것을 방지합니다.

이 예는 다음에 일치됩니다.

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

이 예는 다음과 일치되지 않습니다.

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

이 예는 MAC 주소에 대한 패킷 페이로드를 검색합니다. 백슬래시로 콜론 문자를 이스케이프한다는 점에 유의하십시오.

metadata 키워드

`metadata` 키워드를 사용하여 규칙에 자체 설명 정보를 추가할 수 있습니다. `metadata` 키워드를 `service` 인수와 함께 사용하여 네트워크 트래픽에서 애플리케이션과 포트를 식별할 수도 있습니다. 추가하는 정보를 사용하여 필요에 맞게 규칙을 구성하거나 식별할 수 있고, 추가하는 정보와 `service` 인수를 규칙에서 검색할 수 있습니다.

시스템은 인수 형식을 기반으로 메타데이터를 검증합니다.

key value

*key*와*value*가 스페이스로 구분된 결합 설명을 제공합니다. 이것은 Cisco에서 제공하는 규칙에 메타데이터를 추가하기 위해 Cisco Talos Intelligence Group(Talos)에서 사용하는 형식입니다.

또는, 다음 형식을 사용할 수 있습니다.

key = *value*

예를 들어 *key value* 형식에서 다음과 같이 카테고리 및 하위 카테고리를 사용하여 작성자와 날짜별로 규칙을 식별할 수 있습니다.

```
author SnortGuru_20050406
```

규칙에서 여러 `metadata` 키워드를 사용할 수 있습니다. 다음 예에 나온 것처럼 쉼표를 사용하여 단일 `metadata` 키워드에서 여러 *key value* 인수를 구분할 수 있습니다.

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003,
revised_by SnortUser1_20070123
```

key value 또는 *key*=*value* 형식만 사용하도록 제한되지 않습니다. 그러나 이러한 형식 기반의 검증에서 오는 제한 사항에 대해 알고 있어야 합니다.

피해야 할 제한된 문자

다음과 같은 문자 제한 사항을 참고하십시오.

- 세미콜론(;) 또는 콜론(:)을 사용하지 마십시오.
- 시스템은 쉼표를 여러 *key value* 또는 *key*=*value* 인수의 구분자로 해석합니다. 예를 들면 다음과 같습니다.

  key value, *key value*, *key value*

- 시스템은 등호(=) 문자 또는 공백 문자를 *key* 와 *value* 사이의 구분자로 해석합니다. 예를 들면 다음과 같습니다.

  key value

  key=*value*

다른 모든 문자는 허용됩니다.

피해야 할 예약된 메타데이터

다음 단어는 Talos에서 사용하도록 예약되어 있으므로 `metadata` 키워드에서 단일 인수나 *key value* 인수의 *key*로 사용하지 마십시오.

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

참고 예상과 다르게 기능했을 수도 있는 로컬 규칙에 제한된 메타데이터를 추가하는 것에 관한 도움을 받으려면 Support(지원부)에 연락하십시오.

영향 레벨 **1**

`metadata` 키워드에서 다음의 예약된 *key value* 인수를 사용할 수 있습니다.

```
impact_flag red
```

key value 인수는 가져온 로컬 규칙 또는 침입 규칙 편집기를 사용하여 생성한 맞춤형 규칙에 대해 영향 플래그를 red(레벨 1)로 설정합니다.

Talos가 Cisco에서 제공하는 규칙에 `impact_flag red` 인수를 포함하는 경우, 규칙을 트리거한 패킷이 소스 또는 대상 호스트가 바이러스, 트로이 목마 또는 기타 악성 소프트웨어에 의해 손상되었을 가능성이 있음을 나타내는 것이라고 Talos에서 판단한 것입니다.

관련 항목

로컬 침입 규칙 가져오기 모범 사례, 190 페이지
침입 이벤트 클립보드, 2951 페이지

서비스 메타데이터

시스템은 네트워크에 있는 호스트에서 실행 중인 애플리케이션을 탐지하고 애플리케이션 프로토콜 정보를 네트워크 트래픽에 삽입합니다. 시스템은 검색 정책의 구성에 관계없이 이 작업을 수행합니다. TCP 또는 UDP 규칙에서 `metadata` 키워드 `service` 인수를 사용하여 네트워크 트래픽에서 애플리케이션 프로토콜 및 포트를 매칭할 수 있습니다. 규칙의 하나 이상의 `service` 애플리케이션 인수를 단일 포트 인수와 조합할 수 있습니다.

서비스 애플리케이션

`metadata` 키워드를 `service`와 함께 *key*로 사용하고 애플리케이션을 *value*로 사용하여 패킷을 식별된 애플리케이션 프로토콜과 매칭할 수 있습니다. 예를 들어 다음 `metadata` 키워드 안의 *key value* 인수는 HTTP 트래픽과 규칙을 연결합니다.

```
service http
```

쉼표로 구분된 여러 애플리케이션을 식별할 수 있습니다. 예를 들면 다음과 같습니다.

```
service http, service smtp, service ftp
```

주의 침입 규칙이 서비스 메타데이터를 사용하려면 적응형 프로파일 구성, 2374 페이지에 설명된 대로 적응형 프로파일링이 반드시 활성화되어야 합니다.

다음 표에서는 `service` 키워드와 함께 사용되는 가장 일반적인 애플리케이션 값을 설명합니다.

참고 표에 없는 애플리케이션 식별에 어려움이 있다면 지원 부서에 문의하십시오.

표 ***176:*** 서비스 값

값	설명
cvs	Concurrent Versions System
dcerpc	분산 컴퓨팅 환경/원격 절차 호출 시스템
dns	Domain Name System
finger	핑거 사용자 정보 프로토콜
ftp	파일 전송 프로토콜
ftp-data	파일 전송 프로토콜(데이터 채널)
http	Hypertext Transfer Protocol
imap	Internet Message Access Protocol
isakmp	Internet Security Association and Key Management Protocol
mysql	My Structured Query Language
netbios-dgm	NETBIOS 데이터그램 서비스
netbios-ns	NETBIOS 이름 서비스
NetBIOS ssn	NETBIOS 세션 서비스
nntp	Network News Transfer Protocol
oracle	Oracle Net Services
셸	OS 셸
pop2	포스트 오피스 프로토콜, 버전 2
POP3	포스트 오피스 프로토콜, 버전 3
smtp	간단한 메일 전송 프로토콜
snmp	Simple Network Management Protocol
ssh	Secure Shell 네트워크 프로토콜
sunrpc	Sun Remote Procedure Call Protocol
telnet	텔넷 네트워크 프로토콜

값	설명
`tftp`	Trivial File Transfer Protocol
`x11`	X 윈도우 시스템

서비스 포트

`metadata` 키워드를 `service`와 함께 ***key***로, 지정된 포트 인수를 ***value***로 사용하여 규칙이 애플리케이션과 조합된 포트를 매칭하는 방법을 정의할 수 있습니다.

아래 표에서 규칙당 하나씩 포트 값을 지정할 수 있습니다.

표 ***177:*** 서비스 포트 값

값	설명
`else-ports` 또는 `unknown`	다음 조건 중 하나가 충족되는 경우 시스템이 규칙을 적용합니다. • 패킷 애플리케이션이 알려져 있고 규칙 애플리케이션과 일치합니다. • 패킷 애플리케이션이 알려져 있지 않고 패킷 포트가 규칙 포트와 일치합니다. `else-ports` 및 `unknown` 값은 `service`가 포트 수식자 없는 애플리케이션 프로토콜을 지정할 때 시스템이 사용하는 기본 동작을 생성합니다.
`and-ports`	시스템은 패킷 애플리케이션이 알려져 있고 규칙 애플리케이션과 일치하며 패킷 포트가 규칙 헤더의 포트와 일치하는 경우, 규칙을 적용합니다. 애플리케이션을 지정하지 않는 규칙에서는 `and-ports`를 사용할 수 없습니다.
`or-ports`	다음 조건 중 하나가 충족되는 경우 시스템이 규칙을 적용합니다. • 패킷 애플리케이션이 알려져 있고 규칙 애플리케이션과 일치합니다. • 패킷 애플리케이션이 알려져 있지 않고 패킷 포트가 규칙 포트와 일치합니다. • 패킷 애플리케이션이 규칙 애플리케이션과 일치하지 않고 패킷 포트가 규칙 포트와 일치합니다. • 규칙이 애플리케이션을 지정하지 않고 패킷 포트가 규칙 포트와 일치합니다.

다음에 유의하십시오.

- `service` 애플리케이션 인수와 함께 `service and-ports` 인수를 포함해야 합니다.
- 규칙이 위의 표의 값 중 둘 이상을 지정하는 경우, 시스템은 규칙에 표시되는 마지막 값을 적용합니다.
- 포트 인수와 애플리케이션 인수의 순서는 상관없습니다.

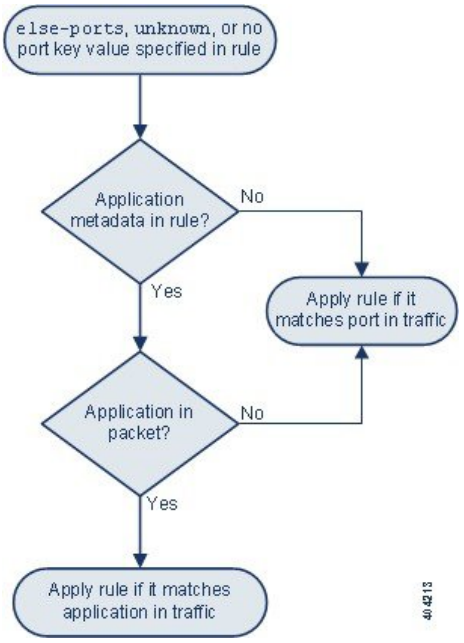
`and-ports` 값을 제외하고 하나 이상의 `service` 애플리케이션 인수와 함께 또는 없이 `service` 포트 인수를 포함시킬 수 있습니다. 예를 들면 다음과 같습니다.

```
service or-ports, service http, service smtp
```

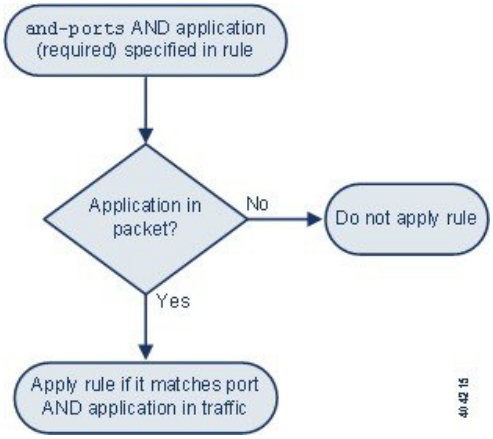
트래픽의 애플리케이션 및 포트

아래 다이어그램은 침입 규칙이 지원하는 애플리케이션 및 포트 조합과 이러한 규칙 제약 조건을 패킷 데이터에 적용한 결과를 보여줍니다.

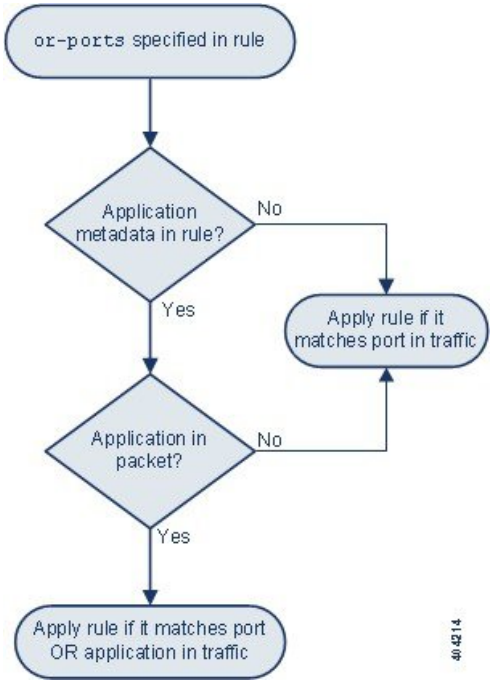
호스트 애플리케이션 프로토콜 **else source/destination** 포트**:**



호스트 애플리케이션 프로토콜 **and source/destination** 포트**:**



호스트 애플리케이션 프로토콜 **or source/destination** 포트**:**



예제 일치

`metadata` 키워드와 함께 `service` 인수를 사용하는 다음 샘플 규칙은 일치하는 데이터 및 일치하지 않는 데이터의 예와 함께 표시되어 있습니다.

- `alert tcp any any -> any [80,8080] (metadata:service and-ports, service http, service smtp;)`

예제 일치	비일치 예
• TCP 포트 80을 통한 HTTP 트래픽 • TCP 포트 8080을 통한 HTTP 트래픽 • TCP 포트 80을 통한 SMTP 트래픽 • TCP 포트 8080을 통한 SMTP 트래픽	• 포트 80 또는 8080의 POP3 트래픽 • 포트 80 또는 8080의 알 수 없는 애플리케이션 트래픽 • 9999 포트의 HTTP 트래픽

- `alert tcp any any -> any [80,8080] (metadata:service or-ports, service http;)`

예제 일치	비일치 예
• 모든 포트의 HTTP 트래픽 • 포트 80의 SMTP 트래픽 • 포트 8080의 SMTP 트래픽 • 포트 80과 8080의 알 수 없는 애플리케이션 트래픽	• 80 또는 8080 외의 포트의 비HTTP 및 비SMTP 트래픽

- 다음 규칙 중 하나:
  - `alert tcp any any -> any [80,8080] metadata:service else-ports, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service unknown, service http;)`
  - `alert tcp any any -> any [80,8080] metadata:service http;)`

예제 일치	비일치 예
• 모든 포트의 HTTP 트래픽 • 패킷 애플리케이션을 알 수 없는 경우 포트 80 • 패킷 애플리케이션을 알 수 없는 경우 포트 8080	• 포트 80 또는 8080의 SMTP 트래픽 • 포트 80 또는 8080의 POP3 트래픽

메타데이터 검색 가이드라인

`metadata` 키워드를 사용하는 규칙을 검색하려면 규칙 Search(검색) 페이지에서 `metadata` 키워드를 선택하고, 선택적으로 메타데이터의 일부를 입력합니다. 예를 들어 다음을 입력할 수 있습니다.

- `search`를 입력하면 *key*에 `search`를 사용한 모든 규칙이 표시됩니다.
- `search http`를 입력하면 *key*에 `search`를 사용하고 *value*에 `http`를 사용한 모든 규칙이 표시됩니다.
- `author snortguru`를 입력하면 *key*에 `author`를 사용하고 *value*에 `SnortGuru`를 사용한 모든 규칙이 표시됩니다.
- `author s`를 입력하면 *key*에 `author`를 사용하고, *value*에 `SnortGuru` 또는 `SnortUser1` 또는 `SnortUser2` 같은 용어를 사용한 모든 규칙이 표시됩니다.

팁 *key*와 *value*를 모두 검색하는 경우, 검색에서 규칙의 *key value* 인수에 사용되는 것과 동일한 연결 연산자(등호[=] 또는 공백 문자)를 사용하십시오. *key* 뒤에 등호(=)를 사용하는지 공백 문자를 사용하는지에 따라 검색에서 다른 결과가 반환됩니다.

메타데이터를 추가하는 데 사용하는 형식과 상관없이 시스템은 메타데이터 검색 용어를 *key value* 또는 *key=value* 인수의 전체 또는 일부로 해석합니다. 예를 들어 다음은 *key value* 또는 *key=value* 형식을 따르지 않는 유효한 메타데이터일 수 있습니다.

```
ab cd ef gh
```

그러나 시스템은 예제의 각 공백을 *key*와 *value* 사이의 구분 기호로 해석합니다. 따라서 병렬 용어 및 단일 용어에 대해 다음 검색 중 하나를 사용하여 예제 메타데이터를 포함하는 규칙을 성공적으로 찾을 수 있습니다.

```
cd ef
ef gh
ef
```

그러나 다음 검색을 사용하면 규칙을 찾을 수 없습니다. 시스템이 이를 단일 *key value* 인수로 해석하기 때문입니다.

```
ab ef
```

관련 항목

규칙 검색, 2083 페이지

IP 헤더 값

키워드를 사용하여 패킷의 IP 헤더 내 가능한 공격 또는 보안 정책 위반을 식별할 수 있습니다.

fragbits

`fragbits` 키워드는 IP 헤더의 단편 및 예약 비트를 검사합니다. Reserved Bit(예약 비트), More Fragments bit(추가 단편 비트)에서 각 패킷을 확인할 수 있으며, 어떤 조합에서나 Don't Fragment bit(단편화 금지 비트)를 확인할 수 있습니다.

표 ***178:*** 단편 비트 인수 값

인수	설명
R	예약 비트
M	추가 단편 비트
D	단편화 금지 비트

`fragbits` 키워드를 사용하여 규칙을 개선하기 위해 규칙에서 인수 값 다음에 다음 표에 설명된 모든 연산자를 지정할 수 있습니다.

표 ***179:*** 단편 비트 연산자

연산자	설명
더하기 기호(+)	패킷은 모든 지정된 비트와 일치해야 합니다.

연산자	설명
별표(*)	패킷은 모든 지정된 비트에 일치할 수 있습니다.
느낌표(!)	지정된 비트가 하나도 설정되지 않은 경우 패킷은 기준을 충족합니다.

예를 들어, 설정된 Reserved Bit(예약 비트) (및 가능한 다른 모든 비트)가 있는 패킷에 대한 이벤트를 생성하려면, `fragbits` 값으로 `R+`를 사용합니다.

id

`ID` 키워드는 키워드의 인수에 지정된 값에 대한 IP 헤더 단편 ID 필드를 테스트합니다. 일부 서비스 거부 툴 및 스캐너는 이 필드를 탐지하기 쉬운 특정 번호로 설정합니다. 예를 들어, Synscan 포트스캔을 탐지하는 SID 630에서는 `ID` 값이 스캐너에서 전송하는 패킷에 ID 번호로 사용된 정적 값 `39426`으로 설정됩니다.

참고 `ID`의 값은 숫자여야 합니다.

ipopts

`IPopts` 키워드를 사용하면 지정된 IP 헤더 옵션을 위한 패킷을 검색할 수 있습니다. 다음 표에는 사용 가능한 인수 값이 나열되어 있습니다.

표 ***180: IPoption*** 인수

인수	설명
rr	레코드 경로
eol	목록 끝
nop	무연산
ts	타임 스탬프
sec	IP 보안 옵션
lsrr	느슨한 소스 라우팅
ssrr	엄격한 소스 라우팅
satid	스트림 식별자

분석가가 가장 자주 살펴보는 것은 엄격한 소스 라우팅과 느슨한 소스 라우팅입니다. 그 이유는 이 옵션이 도용된 소스 IP 주소를 나타낼 수 있기 때문입니다.

ip_proto

ip_proto 키워드를 사용하면 키워드 값으로 지정된 IP 프로토콜을 통해 패킷을 식별할 수 있습니다. 0에서 255까지의 번호로 IP 프로토콜을 지정할 수 있습니다. 이 번호를 <, >, 또는 ! .연산자와 결합할 수 있습니다. 예를 들어, ICMP가 아닌 모든 프로토콜을 통해 트래픽을 검사하려면, ip_proto 키워드에 대한 값으로 !1을 사용합니다. 또한 단일 규칙에서 ip_proto 키워드를 여러 번 사용할 수 있습니다. 하지만, 규칙 엔진은 키워드의 여러 인스턴스를 Boolean AND 관계를 갖는 것으로 해석한다는 점에 유의하십시오. 예를 들어, ip_proto:!3; ip_proto:!6을 포함하는 규칙을 생성하는 경우, 규칙은 GGP 프로토콜 및 TCP 프로토콜을 사용하는 트래픽을 무시합니다.

tos

일부 네트워크는 서비스 유형(ToS) 값을 사용하여 네트워크로 이동하는 패킷의 우선 순위를 설정합니다. tos 키워드는 키워드의 인수로 지정한 값에 대한 패킷의 IP 헤더 ToS 값을 테스트합니다. tos 키워드를 사용하는 규칙은 해당 ToS가 특정 값으로 설정된 패킷과 규칙에서 제시된 기준의 나머지 부분을 충족하는 패킷에서 트리거됩니다.

참고 tos의 인수 값은 숫자여야 합니다.

ToS 필드는 IP 헤더 프로토콜에서 더 이상 사용되지 않으며 DSCP(Differentiated Services Code Point) 필드로 대체되었습니다.

ttl

패킷의 ttl(time-to-live) 값은 삭제되기 전에 만들 수 있는 홉의 수를 나타냅니다. ttl 키워드를 사용하여 키워드의 인수로 지정한 값 또는 값 범위에 대한 패킷의 IP 헤더 ttl 값을 테스트할 수 있습니다. 낮은 TTL 값은 때로 traceroute 또는 침입 회피 시도를 표시하므로 ttl 키워드 매개 변수를 0이나 1과 같은 낮은 값으로 설정하는 것이 도움이 될 수 있습니다. (하지만 이 키워드에 대한 적절한 값은 매니지드 디바이스 배치 및 네트워크 토폴로지에 따라 다르다는 점을 참고하십시오.) 다음과 같이 구문을 사용합니다.

- 0에서 255 사이의 정수를 사용하여 TTL 값으로 특정 값을 설정합니다. 또한 등호(=)로 값을 입력할 수 있습니다(예를 들어 5 또는 =5를 지정할 수 있습니다).
- 하이픈(-)을 사용하여 TTL 값의 범위를 지정합니다(예를 들어, 0-2 는 0에서 2까지의 모든 값을, -5는 0에서 5까지의 모든 값을, 그리고 5-는 5에서 255까지의 모든 값을 지정합니다).
- 부등호(>)를 사용하여 특정 값보다 큰 TTL 값을 지정합니다(예를 들어, >3은 3보다 큰 모든 값을 지정합니다).
- 크거나 같음 기호(>=)를 사용하여 특정 값보다 크거나 같은 TTL 값을 지정합니다(예를 들어, >=3은 3보다 크거나 같은 모든 값을 지정합니다).
- 부등호(<)를 사용하여 특정 값보다 작은 TTL 값을 지정합니다(예를 들어, <3은 3보다 작은 모든 값을 지정합니다).
- 작거나 같음 기호(<=)를 사용하여 특정 값보다 작거나 같은 TTL 값을 지정합니다(예를 들어, <=3은 3보다 작거나 같은 모든 값을 지정합니다).

ICMP 헤더 값

Firepower System은 ICMP 패킷의 헤더에서 공격 및 보안 정책 위반을 식별하는 데 사용할 수 있는 키워드를 지원합니다. 하지만 대부분의 ICMP 유형 및 코드를 탐지하는 사전 정의된 규칙이 존재한다는 점을 참고하십시오. 기존 규칙을 활성화하거나 기존 규칙에 기반한 로컬 규칙을 생성하는 것을 고려하십시오. ICMP 규칙을 처음부터 구축하면 요구를 충족시키는 규칙을 더욱 신속하게 찾을 수 있습니다.

icmp_id 및 icmp_seq

ICMP ID 및 시퀀스 번호는 ICMP 응답과 ICMP 요구를 연결하는 데 도움이 됩니다. 일반적인 트래픽에서 이 값은 패킷에 동적으로 할당됩니다. 일부 은닉 채널 및 분산서비스거부(DDoS) 프로그램은 정적 ICMP ID 및 시퀀스 값을 사용합니다. 다음 키워드를 사용하면 정적 값으로 ICMP 패킷을 확인할 수 있습니다.

키워드	정의
icmp_id	ICMP 에코 요청 또는 회신 패킷의 ICMP ID 번호를 검사합니다. `icmp_id` 키워드에 대한 인수로 ICMP ID 번호에 해당하는 숫자를 사용합니다.
icmp_seq	`icmp_seq` 키워드는 ICMP 에코 요청 또는 회신 패킷의 ICMP 시퀀스를 검사합니다. `icmp_seq` 키워드에 대한 인수로 ICMP 시퀀스 번호에 해당하는 숫자를 사용합니다.

itype

특정 ICMP 메시지 유형 값으로 패킷을 검색하려면 `itype` 키워드를 사용합니다. 유효한 ICMP 유형 값 또는 유효하지 않은 ICMP 유형 값을 지정하여 다양한 트래픽 유형을 테스트할 수 있습니다. 예를 들어, 공격자는 범위에서 서비스 거부 및 플러딩 공격을 야기할 사정 거리 밖의 ICMP 유형 값을 설정할 수 있습니다.

보다 작음(<) 및 보다 큼(>)을 사용하여 `itype` 인수 값의 범위를 지정할 수 있습니다.

예를 들면 다음과 같습니다.

- <35
- >36
- 3<>55

icode

ICMP 메시지는 때로 목적지에 도달할 수 없는 경우 정보를 제공하는 코드 값을 포함합니다.

특정 ICMP 코드 값으로 패킷을 확인하려면 `icode` 키워드를 사용할 수 있습니다. 유효한 ICMP 코드 값 또는 유효하지 않은 ICMP 코드 값을 지정하여 다양한 트래픽 유형을 테스트할 수 있습니다.

보다 작음(<) 및 보다 큼(>)을 사용하여 `icode` 인수 값의 범위를 지정할 수 있습니다.

예를 들면 다음과 같습니다.

- 35보다 작은 값을 찾으려면, `<35`를 지정합니다.
- 36보다 큰 값을 찾으려면, `>36`을 지정합니다.
- 3에서 55 사이의 값을 찾으려면, `3<>55`를 지정합니다.

팁 `icode` 및 `itype` 키워드를 사용하여 둘 다에 일치하는 트래픽을 식별할 수 있습니다. 예를 들어, ICMP Destination Unreachable(목적지 도달 불가) 코드 유형과 ICMP Port Unreachable(포트 연결 불가) 코드 유형을 포함하는 ICMP 트래픽을 식별하려면 Destination Unreachable(목적지 도달 불가)에 대한 3의 값과 함께 `itype` 키워드를, Port Unreachable(포트 연결 불가)에 대한 3의 값과 함께 `icode` 키워드를 사용합니다.

TCP 헤더 값 및 스트림 크기

Firepower System은 패킷의 TCP 헤더와 TCP 스트림 크기를 사용하여 시도된 공격을 식별하도록 설계된 키워드를 지원합니다.

ack

패킷의 TCP 확인 응답 수에 대한 값을 비교하려면 `ack` 키워드를 사용할 수 있습니다. `ack` 키워드에 지정된 값이 패킷의 TCP 확인 응답 수에 일치하는 경우 규칙이 트리거됩니다.

`ack`의 인수 값은 숫자여야 합니다.

flags

`flags` 키워드를 사용하여 검사한 패킷에 지정되었을 때, 규칙이 트리거되도록 하는 TCP 플래그의 조합을 지정할 수 있습니다.

참고 관례상 `flags` 값으로 `A+`를 사용할 경우, `established` 값으로 `flow` 키워드를 사용해야 합니다. 일반적으로 모든 플래그 조합 탐지를 확인하기 위해 플래그를 사용하는 경우, `stateless` 값으로 `flow` 키워드를 사용해야 합니다.

`flag` 키워드에 대해 다음 표에 설명한 값을 확인하거나 무시할 수 있습니다.

표 ***181:*** 플래그 인수

인수	**TCP** 플래그
Ack	데이터를 확인합니다.
Psh	데이터는 이 패킷에 보내야 합니다.
Syn	새로운 연결입니다.

인수	TCP 플래그
Urg	패킷은 긴급한 데이터를 포함합니다.
Fin	닫힌 연결입니다.
Rst	중지된 연결입니다.
CWR	ECN 정체 창이 줄었습니다. 이는 이전에 R1 인수였으며 하위 호환성을 위해 계속 지원됩니다.
ECE	ECN 에코입니다. 이는 이전에 R2 인수였으며 하위 호환성을 위해 계속 지원됩니다.

`flags` 키워드를 사용할 때에는 여러 플래그를 기준으로 시스템이 매칭을 수행하는 방법을 나타내기 위해 연산자를 사용할 수 있습니다. 다음 표에서 이 연산자를 설명합니다.

표 ***182:*** 플래그와 함께 사용되는 연산자

연산자	설명	예
all	패킷은 모든 지정된 플래그를 포함해야 합니다.	`Urg` 및 `all`을 선택하여 패킷이 Urgent(긴급) 플래그를 포함해야 하며 다른 모든 플래그를 포함하도록 지정합니다.
any	패킷은 지정된 플래그를 모두 포함할 수 있습니다.	`Ack`, `Psh` 및 `any`를 선택하여 `Ack` 및 `Psh` 플래그 둘 중 하나 또는 둘 다 규칙을 트리거할 수 있도록 설정되어야 하며 모든 플래그가 하나의 패킷에도 설정될 수 있도록 지정합니다.
not	패킷은 지정된 플래그 집합을 포함할 수 없습니다.	`Urg`와 `not`을 선택하여 Urgent(긴급) 플래그가 이 규칙을 트리거하는 패킷에 설정되지 않도록 지정합니다.

flow

`flow` 키워드를 사용하여 세션 특징에 기반한 규칙에 따라 검사를 위한 패킷을 선택할 수 있습니다. `flow` 키워드를 사용하면 클라이언트 흐름 또는 서버 흐름에 규칙을 적용하여 규칙이 적용된 트래픽 흐름의 방향을 지정할 수 있습니다. `flow` 키워드가 패킷을 검사하는 방법을 지정하려면, 분석을 원하는 트래픽의 방향과 검사된 패킷의 상태, 그리고 패킷이 재구축된 스트림의 일부인지 여부를 설정할 수 있습니다.

규칙을 처리할 때 패킷의 상태 저장 검사가 이루어집니다. TCP 규칙이 상태 비저장 트래픽(설정된 세션 컨텍스트가 없는 트래픽)을 무시하기를 원하는 경우, 규칙에 `flow` 키워드를 추가하고 키워드의 **Established** 인수를 선택해야 합니다. UDP 규칙이 스테이트리스 트래픽을 무시하도록 하려면 규칙에 `flow` 키워드를 추가하고 **Established** 인수나 방향 인수 또는 둘 모두를 선택해야 합니다. 이것은 TCP 또는 UDP 규칙이 패킷의 상태 저장 검사를 수행하도록 합니다.

방향 인수를 추가하면, 규칙 엔진은 지정된 방향과 일치하는 흐름과 함께 설정한 상태가 있는 해당 패킷만 검사합니다. TCP 또는 UDP 연결이 탐지되었을 때 트리거되는 규칙에 `established` 인수 및 `From Client` 인수와 함께 `flow` 키워드를 추가하는 경우, 규칙 엔진은 클라이언트에서 전송된 패킷만 검사합니다.

팁 최대 성능을 위해, TCP 규칙 또는 UDP 세션 규칙에서 항상 `flow` 키워드를 포함합니다.

다음 표에서는 `flow` 키워드에 대해 지정할 수 있는 스트림 관련 인수를 설명합니다.

표 ***183:*** 상태 관련 흐름 인수

인수	설명
Established	연결이 설정된 경우 트리거됩니다.
Stateless	스트림 프로세서의 상태에 상관없이 트리거됩니다.

다음 표에서는 `flow` 키워드에 대해 지정할 수 있는 방향 옵션을 설명합니다.

표 ***184:*** 흐름 방향 인수

인수	설명
To Client	서버 응답 시 트리거됩니다.
To Server	클라이언트 응답 시 트리거됩니다.
From Client	클라이언트 응답 시 트리거됩니다.
From Server	서버 응답 시 트리거됩니다.

`From Server` 및 `To Client`는 같은 기능을 수행하며, `To Server` 및 `From Client`도 같은 기능을 수행한다는 점에 유의하십시오. 이 옵션은 규칙에 컨텍스트 및 가독성을 추가하기 위해 존재합니다. 예를 들어 서버에서 클라이언트에 취해지는 공격을 탐지하기 위해 설계된 규칙을 작성하는 경우, `From Server`를 사용하십시오. 하지만 클라이언트에서 서버에 취해지는 공격을 탐지하기 위해 설계된 규칙을 작성하는 경우, `From Client`를 사용합니다.

다음 표에서는 `flow` 키워드에 대해 지정할 수 있는 스트림 관련 인수를 설명합니다.

표 ***185:*** 스트림 관련 흐름 인수

인수	설명
Ignore Stream Traffic	재작성한 스트림 패킷에서 트리거되지 않습니다.
Only Stream Traffic	재작성된 스트림 패킷에서만 트리거됩니다.

예를 들어, 스트림 프리프로세서에 의해 리어셈블된, 설정된 세션에서 클라이언트에서 서버로 이동하는 트래픽을 탐지하려면 `flow` 키워드에 대해 `To Server, Established, Only Stream Traffic`을 사용할 수 있습니다.

seq

seq 키워드로 정적 시퀀스 번호 값을 지정할 수 있습니다. 시퀀스 번호가 특정 인수에 일치하는 패킷은 키워드를 포함하는 규칙을 트리거합니다. 이 키워드는 거의 사용되지 않지만 정적 시퀀스 번호로 생성된 패킷을 사용한 스캔 네트워크와 공격 식별에 도움이 됩니다.

window

window 키워드를 사용하여 관심 있는 TCP 창 크기를 지정할 수 있습니다. 이 키워드를 포함하는 규칙은 지정된 TCP 창 크기의 패킷이 발생할 때마다 트리거됩니다. 이 키워드는 거의 사용되지 않지만 정적 TCP 창 크기로 생성된 패킷을 사용한 스캔 네트워크와 공격 식별에 도움이 됩니다.

stream_size

다음 형식을 사용하여 stream_size 키워드를 TCP 스트림 바이트의 크기를 결정하는 스트림 전처리기와 함께 사용할 수 있습니다.

```
direction,operator,bytes
```

bytes가 바이트 수인 경우. 쉼표(,)로 인수의 각 옵션을 구분해야 합니다.

다음 표에서는 stream_size 키워드에 대해 지정할 수 있는 대소문자를 구분하지 않는 방향 옵션을 설명합니다.

표 ***186: stream_size*** 키워드 방향 인수

인수	설명
client	지정된 스트림 크기와 일치하는 클라이언트의 스트림에서 트리거됩니다.
server	지정된 스트림 크기와 일치하는 서버의 스트림에서 트리거됩니다.
both	클라이언트 트래픽 및 지정된 스트림 크기와 일치하는 서버의 트래픽 모두에서 트리거됩니다. 예를 들어, `both, >, 200` 인수는 클라이언트 발신 트래픽이 200바이트보다 큰 경우 및 서버 발신 트래픽이 200바이트보다 큰 경우에 트리거됩니다.
either	무엇이 먼저 발생하든 지정된 스트림 크기와 일치하는 클라이언트 또는 서버의 트래픽에서 트리거됩니다. 예를 들어, `either, >, 200` 인수는 클라이언트 발신 트래픽이 200바이트보다 큰 경우 또는 서버 발신 트래픽이 200바이트보다 큰 경우에 트리거됩니다.

다음 표에서는 stream_size 키워드와 함께 사용할 수 있는 연산자를 설명합니다.

표 ***187: stream_size*** 키워드 인수 연산자

연산자	설명
=	같음

연산자	설명
!=	같지 않음
>	보다 큼
<	보다 작음
>=	보다 크거나 같음
<=	보다 작거나 같음

예를 들어, `client, >=, 5001216`을 `stream_size` 키워드의 인수로 사용하여 클라이언트에서 5001216 바이트와 같거나 큰 서버로 이동하는 TCP 스트림을 탐지할 수 있습니다.

stream_reassembly 키워드

`stream_reassemble` 키워드를 사용하여 연결 시 검사된 트래픽이 규칙 조건에 일치할 때 단일 연결에 대한 TCP 스트림 리어셈블리를 활성화 및 비활성화할 수 있습니다. 또는, 규칙에서 이러한 키워드를 여러 번 사용할 수 있습니다.

스트림 리어셈블리를 활성화하거나 비활성화하려면 다음 구문을 사용합니다.

```
enable|disable, server|client|both, option, option
```

다음 표에서는 `stream_reassemble` 키워드와 함께 사용할 수 있는 선택적 인수를 설명합니다.

표 ***188: stream_reassemble*** 선택적 인수

인수	설명
noalert	규칙에 지정된 다른 모든 탐지 옵션에 관계없이 어떤 이벤트도 생성하지 않습니다.
fastpath	일치할 때 연결 트래픽의 나머지 부분을 무시합니다.

예를 들어 다음 규칙은 HTTP 응답에서 200 OK 상태 코드가 탐지된 연결에 대해 이벤트를 생성하지 않은 채 TCP 클라이언트 측 스트림 리어셈블리를 비활성화합니다.

```
alert tcp any 80 -> any any (flow:to_client, established; content: “200 OK”;
stream_reassemble:disable, client, noalert
```

SSL 키워드

SSL 규칙 키워드를 사용하여 SSL(Secure Sockets Layer) 전처리기를 호출할 수도 있고 암호화된 세션에서 패킷으로부터 SSL 버전 및 세션 상태에 관한 정보를 추출할 수 있습니다.

클라이언트와 서버가 SSL 또는 TLS(전송 레이어 보안)를 사용하여 암호화된 세션을 설정하기 위해 통신할 때 핸드쉐이크 메시지를 교환합니다. 세션에서 전송되는 데이터는 암호화되지만, 핸드쉐이크 메시지는 그렇지 않습니다.

SSL 전처리기는 특정 핸드쉐이크 필드의 상태 및 버전 정보를 추출합니다. 핸드쉐이크 내 두 필드는 핸드쉐이크의 세션 및 단계를 암호화하는 데 사용된 SSL 또는 TLS 버전을 나타냅니다.

ssl_state

`ssl_state` 키워드는 암호화된 세션에 대한 상태 정보를 비교하는 데 사용될 수 있습니다. 동시에 사용된 2개 이상의 SSL 버전을 확인하려면, 규칙에서 여러 `ssl_version` 키워드를 사용합니다.

규칙이 `ssl_state` 키워드를 사용하면, 규칙 엔진은 SSL 전처리기를 호출하여 SSL 상태 정보에 대한 트래픽을 확인하도록 합니다.

예를 들어, 너무 긴 챌린지 길이 및 너무 많은 데이터를 가진 `ClientHello` 메시지를 보내 서버에 버퍼 오버플로를 일으키는 공격자의 시도를 검색하려면, `client_hello`와 함께 `ssl_state` 키워드를 인수로 사용한 후 비정상적으로 규모가 큰 패킷을 확인할 수 있습니다.

쉼표로 구분된 목록을 사용하여 SSL 상태에 대한 여러 인수를 지정합니다. 여러 인수를 나열할 경우, 시스템은 OR 연산자를 사용하여 이를 평가합니다. 예를 들어, 인수로 `client_hello` 및 `server_hello`를 지정한 경우, 시스템은 `client_hello` 또는 `server_hello`가 있는 트래픽에 대한 규칙을 평가합니다.

또한 모든 인수를 무효화할 수 있습니다. 예를 들면 다음과 같습니다.

```
!client_hello, !unknown
```

연결이 각 상태 집합에 도달했음을 확인하려면 ssl_state 규칙 옵션을 사용하는 여러 규칙이 사용되어야 합니다. `ssl_state` 키워드는 다음 식별자를 인수로 취합니다.

표 ***189: ssl_state*** 인수

인수	목적
`client_hello`	메시지 유형이 `ClientHello`인 핸드셰이크 메시지에 대해 매칭합니다. 여기서 클라이언트는 암호화된 세션을 요청합니다.
`server_hello`	메시지 유형이 `ServerHello`인 핸드셰이크 메시지에 대해 매칭합니다. 여기서 서버는 암호화된 세션에 대한 클라이언트의 요청에 응답합니다.
`client_keyx`	메시지 유형으로 `ClientKeyExchange`를 가진 핸드쉐이크 메시지와 비교하며, 서버로부터 키를 수신했음을 확인하기 위해 클라이언트가 서버에 키를 전송합니다.
`server_keyx`	메시지 유형으로 `serverKeyExchange`를 가진 핸드쉐이크 메시지와 비교하며, 서버로부터 키를 수신했음을 확인하기 위해 클라이언트가 서버에 키를 전송합니다.
`unknown`	모든 핸드쉐이크 메시지 유형과 비교합니다.

ssl_version

ssl_version 키워드는 암호화된 세션의 버전 정보와 일치시키는 데 사용될 수 있습니다. 규칙이 ssl_version 키워드를 사용하면, 규칙 엔진은 SSL 전처리기를 호출하여 SSL 버전 정보에 대한 트래픽을 확인하도록 합니다.

예를 들어 SSL 버전 2에 버퍼 오버플로 취약성이 있음을 알고 있는 경우, SSL의 해당 버전을 사용하는 트래픽을 식별하려면 ssl_version 키워드와 sslv2 인수를 사용할 수 있습니다.

쉼표로 구분된 목록을 사용하여 SSL 버전에 대한 여러 인수를 지정합니다. 여러 인수를 나열할 경우, 시스템은 OR 연산자를 사용하여 이를 평가합니다. 예를 들어, SSLv2를 사용하지 않는 모든 암호화된 트래픽을 식별하고자 한다면 규칙에 ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2를 추가할 수 있습니다. 규칙은 SSL 버전 3, TLS 버전 1.0, TLS 버전 1.1, 또는 TLS 버전 1.2를 사용하여 모든 트래픽을 평가합니다.

ssl_version 키워드는 다음 SSL/TLS 버전 식별자를 인수로 취합니다.

표 ***190: ssl_version*** 인수

인수	목적
sslv2	SSL(Secure Sockets Layer) 버전 2를 사용하여 인코딩된 트래픽과 비교합니다.
sslv3	SSL(Secure Sockets Layer) 버전 3을 사용하여 인코딩된 트래픽과 비교합니다.
tls1.0	TLS(전송 레이어 보안) 버전 1.0을 사용하여 인코딩된 트래픽과 비교합니다.
tls1.1	TLS(전송 레이어 보안) 버전 1.1을 사용하여 인코딩된 트래픽과 비교합니다.
tls1.2	TLS(전송 레이어 보안) 버전 1.2를 사용하여 인코딩된 트래픽과 비교합니다.

appid 키워드

appid 키워드를 사용하여 패킷에서 애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 웹 애플리케이션을 식별할 수 있습니다. 예를 들어 특정 취약성의 영향을 받기 쉬운 특정 애플리케이션을 대상으로 할 수 있습니다.

침입 규칙의 appid 키워드 내에서 **Configure AppID(AppID** 구성**)**를 클릭하여 탐지할 하나 이상의 애플리케이션을 선택합니다.

사용 가능한 애플리케이션 탐색

조건 만들기를 처음 시작할 때 **Available Application(**사용 가능한 애플리케이션**)** 목록은 제한되지 않은 상태이며 시스템에서 탐지되는 모든 애플리케이션이 페이지당 100개씩 표시됩니다.

- 애플리케이션 페이지를 넘기려면 목록 아래의 화살표를 클릭합니다.
- 애플리케이션의 특성에 대한 요약 정보와 찾아갈 수 있는 인터넷 검색 링크가 포함된 팝업 창을 표시하려면 애플리케이션 옆의 정보() 을 클릭합니다.

애플리케이션 필터 사용

매칭할 애플리케이션을 찾으려면, 다음과 같은 방법으로 **Available Applications** 목록을 제한할 수 있습니다.

- 애플리케이션을 검색하려면 **Search by name** 프롬프트를 클릭한 다음 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 애플리케이션을 표시합니다.
- 필터를 적용하여 애플리케이션을 제한하려면 **Application Filters(**애플리케이션 필터**)** 목록을 사용합니다. 필터를 적용하면 **Available Applications** 목록이 업데이트됩니다. 사용자의 편의를 위해 시스템은 잠금 취소 아이콘을 사용하여 암호화 트래픽이나 암호화되지 않은 트래픽이 아닌 해독된 트래픽에서만 식별할 수 있는 애플리케이션을 표시합니다.

참고 Application Filters(애플리케이션 필터) 목록에서 하나 이상의 필터를 선택하고 **Available Applications(**사용 가능한 애플리케이션**)** 목록도 검색하는 경우 선택한 항목 및 검색을 통해 필터링한 **Available Applications(**사용 가능한 애플리케이션**)** 목록이 AND 연산을 사용하여 조합됩니다.

애플리케이션 선택

단일 애플리케이션을 선택하려면 애플리케이션을 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다. 현재의 제한된 보기에서 모든 애플리케이션을 선택하려면 마우스 오른쪽 버튼으로 클릭하고 **Select All(**모두 선택**)**을 선택합니다.

애플리케이션 레이어 프로토콜 값

전처리기가 애플리케이션 레이어 프로토콜 값의 표준화 및 검사 작업 대부분을 수행하지만 사용자는 다양한 전처리기 옵션을 사용하여 계속해서 애플리케이션 레이어 값을 검사할 수 있습니다.

RPC 키워드

`rpc` 키워드는 TCP 또는 UDP 패킷에서 ONC RPC(Open Network Computing Remote Procedure Call) 서비스를 식별합니다. 이를 통해 호스트에서 RPC 프로그램을 확인하려는 시도를 탐지할 수 있습니다. 침입자는 RPC 포트매퍼를 사용하여 네트워크에서 실행되는 RPC 서비스가 공격받을 가능성이 있는지 결정할 수 있습니다. 이들은 포트매퍼를 사용하지 않고 RPC를 실행하는 다른 포트에 액세스를 시도할 수도 있습니다. 다음 표에서는 `rpc` 키워드가 수용하는 인수를 나열합니다.

표 ***191: rpc*** 키워드 인수

인수	설명
application	RPC 애플리케이션 번호
procedure	호출된 RPC 절차
version	RPC 버전

`rpc` 키워드에 대한 인수를 지정하려면, 다음 구문을 사용합니다.

```
application,procedure,version
```

application(이 RPC 애플리케이션 번호인 경우, procedure는 RPC 절차 번호이며, version은 RPC 버전 번호입니다. `rpc` 키워드에 대한 모든 인수를 지정해야 합니다. 인수 중 하나를 지정할 수 없는 경우, 별표(`*`)로 교체합니다.

예를 들어, 모든 절차 또는 버전으로 RPC 포트매퍼를 검색하려면(번호 100000으로 표시된 RPC 애플리케이션), `100000,*,*`를 인수로 사용합니다.

ASN.1 키워드

`asn1` 키워드를 사용하면 패킷 또는 패킷의 일부를 해독하여 다양한 악성 인코딩을 찾을 수 있습니다.

다음 표에서는 `asn1` 키워드의 인수에 대해 설명합니다.

표 ***192: asn.1*** 키워드 인수

인수	설명
Bitstring Overflow	원격으로 공격 가능한 유효하지 않은 비트 스트링 인코딩을 탐지합니다.
Double Overflow	표준 버퍼보다 큰 이중 ASCII 인코딩을 탐지합니다. 이것은 Microsoft Windows에서 악용 가능한 기능으로 알려져 있지만 현재로서는 어떤 서비스가 악용 가능한지 알 수 없습니다.
Oversize Length	제공된 인수보다 큰 ASN.1 유형 길이를 탐지합니다. 예를 들어, Oversize Length로 500을 설정한 경우, 500보다 큰 모든 ASN.1 유형이 규칙을 트리거합니다.
Absolute Offset	패킷 페이로드의 시작 지점으로부터 절대적 오프셋을 설정합니다. (오프셋 카운터가 0바이트부터 시작한다는 점에 유의하십시오.) 예를 들어, SNMP 패킷을 해독할 경우, Absolute Offset은 0으로 설정하고 Relative Offset은 설정하지 않습니다. Absolute Offset은 양수이거나 음수일 수 있습니다.
Relative Offset	이것은 마지막으로 성공한 콘텐츠 일치로부터의 상대적 오프셋이며, `pcre` 또는 `byte_jump`입니다. 콘텐츠 "foo" 바로 다음에 있는 ASN.1 시퀀스를 해독하려면, Relative Offset은 0으로 설정하고 Absolute Offset은 설정하지 않습니다. Relative Offset은 양수이거나 음수일 수 있습니다. (오프셋 카운터가 0바이트부터 시작한다는 점에 유의하십시오.)

예를 들어, 버퍼 오버플로를 만드는 Microsoft ASN.1 라이브러리에는 알려진 취약성이 있는데, 공격자가 특별히 만들어진 인증 패킷으로 조건을 공격하도록 허용합니다. 시스템이 asn.1 데이터를 해독할 때 패킷의 익스플로잇 코드가 시스템 수준 권한이 있는 호스트에서 실행되거나 DoS 조건을 일으킬 수 있습니다. 다음 규칙은 `asn1` 키워드를 사용하여 이 취약성을 이용하려는 시도를 탐지합니다.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|";
nocase; offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length 100,
relative_offset 54;)
```

위 규칙은 포트 445를 사용하여 $EXTERNAL_NET 변수에 정의된 모든 IP 주소, 모든 포트로부터 $HOME_NET 변수에 정의된 모든 IP 주소로 이동하는 TCP 트래픽에 대한 이벤트를 생성합니다. 또한, 서버로 연결된 TCP 연결에만 규칙을 수행합니다. 규칙은 다음으로 특정 위치에서 특정 내용을 테스트합니다. 마지막으로, 규칙은 `asn1` 키워드를 사용하여 비트 스트링 인코딩 및 이중 ASCII 인코딩을 탐지하고, 마지막으로 성공한 콘텐츠 일치의 끝 지점에서 55바이트 길이부터 100바이트 이상의 길이를 가진 asn.1 유형을 식별합니다. (오프셋 카운터가 0바이트부터 시작한다는 점에 유의하십시오.)

urilen 키워드

`urilen` 키워드를 HTTP 검사 전처리기와 함께 사용하여 최대 길이보다는 작고 최소 길이보다는 크며, 특정 범위 안에 있는 특정 길이 URI의 HTTP 트래픽을 검사할 수 있습니다.

HTTP 검사 전처리기가 패킷을 표준화하고 검사한 후, 규칙 엔진은 규칙에 대한 패킷을 평가하고, `urilen` 키워드가 지정한 길이 상태에 URI가 일치하는지 결정합니다. 이 키워드를 사용하여 URI 길이 취약성을 이용하려고 하는 익스플로잇을 탐지할 수 있습니다. 예를 들면 공격자가 DoS 조건을 야기하거나 시스템 수준 권한이 있는 호스트에서 코드를 실행할 수 있는 버퍼 오버플로를 생성하는 것입니다.

`urilen` 키워드를 규칙에서 사용할 때 다음 사항에 유의하십시오.

- 실전에서는 항상 `urilen` 키워드와 `flow:established` 키워드 및 하나 이상의 다른 키워드를 조합하여 사용합니다.
- 규칙 프로토콜은 항상 TCP입니다.
- 대상 포트는 항상 HTTP 포트입니다.

십진수로 나타낸 바이트 수와 보다 작음(<) 또는 보다 큼(>)을 사용하여 URI 길이를 지정합니다.

예를 들면 다음과 같습니다.

- 5바이트 길이의 URI를 탐지하려면 `5`를 지정합니다.
- 5바이트 길이보다 짧은 URI를 탐지하려면 `< 5`(스페이스 문자 하나로 분리)를 지정합니다.
- 5바이트 길이보다 긴 URI를 탐지하려면 `> 5`(스페이스 문자 하나로 분리)를 지정합니다.
- 길이가 3에서 5바이트 사이에 들어가는 URI를 탐지하려면 `3 <> 5`(<> 전후에 스페이스 문자 하나씩 표시)를 지정합니다.

예를 들어, eDirectory 버전 8.8과 함께 제공된 Novell의 서버 모니터링 및 진단 유틸리티 iMonitor 버전 2.4에는 알려진 취약성이 있습니다. 과도하게 긴 URI을 포함하는 패킷은 버퍼 오버플로를 생성하며 이로 인해 공격자가 시스템 수준 권한으로 호스트에서 실행하거나 DoS 조건을 야기할 수 있는 특수하게 조작된 패킷이 포함된 조건을 악용할 수 있습니다. 다음 규칙은 `urilen` 키워드를 사용하여 이 취약성을 악용하려는 시도를 탐지합니다.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt"; flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

위 규칙은 $HTTP_PORTS 변수에 정의된 포트를 사용하여 $EXTERNAL_NET 변수에 정의된 모든 IP 주소, 모든 포트로부터 $HOME_NET 변수에 정의된 모든 IP 주소로 이동하는 TCP 트래픽에 대한 이벤트를 생성합니다. 또한, 패킷은 서버로 설정된 TCP 연결에서만 규칙에 대해 평가됩니다. 규칙은 `urilen` 키워드를 사용하여 길이가 8192바이트 이상인 모든 URI를 탐지합니다. 마지막으로 규칙은 URI에서 대소문자를 구분하지 않는 특정 콘텐츠 `/nds/`를 검색합니다.

관련 항목

침입 규칙 헤더 프로토콜, 2067 페이지
침입 규칙 헤더 소스 및 대상 포트, 2071 페이지
사전 정의된 기본 변수, 582 페이지

DCE/RPC 키워드

다음 표에 설명된 3개의 DCE/RPC 키워드를 사용하여 DCE/RPC 세션 트래픽에서 익스플로잇을 모니터링할 수 있습니다. 시스템이 이 키워드로 규칙을 처리할 때, DCE/RPC 전처리기를 호출합니다.

표 ***193: DCE/RPC*** 키워드

사용 키워드	사용 방법	탐지 대상
`dce_iface`	단독으로	특정 DCE/RPC 서비스를 식별하는 패킷
`dce_opnum`	`dce_iface`가 앞에 오는 경우	특정 DCE/RPC 서비스 작업을 식별하는 패킷
`dce_stub_data`	`dce_iface` + `dce_opnum`이 앞에 오는 경우	특정 작업 요청 또는 응답을 정의하는 스텁 데이터

표에서 `dce_opnum` 및 `dce_iface`가 항상 앞에 와야 한다는 점과 `dce_stub_data` 및 `dce_iface` + `dce_opnum`이 항상 앞에 와야 한다는 점에 유의하시기 바랍니다.

DCE/RPC 키워드를 다른 규칙 키워드와 조합하여 사용할 수 있습니다. DCE/RPC 규칙의 경우, `byte_jump`, `byte_test`, and `byte_extract` 키워드를 선택한 **DCE/RPC** 인수와 함께 사용합니다.

Cisco는 DCE/RPC 키워드를 포함하는 규칙에 최소 하나의 `content` 키워드를 포함할 것을 권장합니다. 이는 규칙 엔진이 빠른 패턴 매처를 사용하도록 하는 것인데, 이는 처리 속도를 높이고 성능을 향상시킵니다. 규칙에 최소 하나의 `content` 키워드가 포함될 때, `content` 키워드 **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)** 인수를 활성화했는지 여부에 상관없이 규칙 엔진이 빠른 패턴 매처를 사용한다는 점에 유의하십시오.

다음의 경우 일치 내용으로 DCE/RPC 버전 및 연속되는 헤더 정보를 사용할 수 있습니다.

- 규칙은 다른 `content` 키워드를 포함하지 않습니다
- 규칙은 다른 `content` 키워드를 포함하지만, DCE/RPC 버전 및 연속된 정보는 다른 콘텐츠보다 고유한 패턴을 나타냅니다

  예를 들어, DCE/RPC 버전 및 연속되는 정보는 단일 바이트의 콘텐츠보다 고유할 가능성이 더 높습니다.

다음 버전 중 하나 및 연속되는 정보 콘텐츠 일치로 자격 심사 규칙을 종료해야 합니다.

- 연결 지향 DCE/RPC 규칙은 주요 버전 05, 비주요 버전 00, 요청 PDU(프로토콜 데이터 장치) 유형 00에 대해 콘텐츠 `|05 00 00|`을 사용합니다.
- 연결 없는 DCE/RPC 규칙은 버전 04, 요청 PDU 유형 00에 대해 콘텐츠 `|04 00|`을 사용합니다.

어떤 경우든 DCE/RPC 프리프로세서에 의해 이미 완료된 처리를 반복하지 않고 fast pattern matcher를 호출하려면 버전 및 인접 정보에 대한 `content` 키워드를 규칙의 마지막 키워드로 배치하십시오. `content` 키워드를 규칙의 끝에 두는 것은 fast pattern matcher를 호출하기 위한 디바이스로 사용되는 버전 내용에 적용되며, 규칙의 다른 내용 일치에는 적용할 필요가 없습니다.

관련 항목

DCE/RPC 전처리기, 2228 페이지
content 및 protected_content 키워드, 2088 페이지
content 키워드 빠른 패턴 매처 인수, 2098 페이지
개요: byte_jump 및 byte_test 키워드
byte_extract 키워드, 2106 페이지

dce_iface

`dce_if ace` 키워드를 사용하여 특정 DCE/RPC 서비스를 확인할 수 있습니다.

선택적으로, `dce_opnum` 및 `dce_stub_data` 키워드와 조합하여 `dce_iface`를 사용해 검사해야 할 DCE/RPC 트래픽을 추가로 제한할 수 있습니다.

고정된 16바이트 UUID(Universally Unique Identifier) 식별자는 각 DCE/RPC 서비스에 할당된 애플리케이션 인터페이스를 식별합니다. 예를 들어 UUID 4b324fc8-670-01d3-1278-5a47bf6ee188은 피어 투 피어 프린터, 파일 및 SMB 명명된 파이프 등을 위한 다양한 관리 기능을 제공하는 DCE/RPC lanmanserver 서비스(srvsvc 서비스라고도 함)를 식별합니다. DCE/RPC 전처리기는 UUID 및 DCE/RPC 세션을 추적하기 위한 관련 헤더 값을 사용합니다.

인터페이스 UUID는 하이픈으로 구분된 5개의 16진수 문자열로 구성됩니다.

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

넷로그온 인터페이스에 대해 다음 UUID에 표시된 대로 하이픈을 포함하는 전체 UUID를 입력하여 인터페이스를 지정합니다.

```
12345678-1234-abcd-ef00-01234567cffb
```

빅 엔디언 바이트 순서로 UUID에 처음 3개 문자열을 지정해야 한다는 점에 유의하십시오. 게시된 인터페이스 목록 및 프로토콜 분석기는 일반적으로 UUID를 정확한 바이트 순서로 정렬하지만 이를 입력하기 전에 UUID 바이트 순서를 다시 정렬해야 할 수 있습니다. 경우에 따라 리틀 엔디언 바이트 순서로 처음 3개 문자열과 함께 원시 ASCII 텍스트로 표시될 수 있으므로 다음 메신저 서비스를 보여진 UUID로 생각하십시오.

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

다음과 같이 하이픈을 삽입하고 처음 3개 문자열을 빅 엔디언 바이트 순서로 나열함으로써 `dce_iface` 키워드에 동일한 UUID를 지정합니다.

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

DCE/RPC 세션이 여러 인터페이스에 요청을 포함할 수 있지만, 한 규칙에서 한 개의 `dce_iface` 키워드만 포함해야 합니다. 추가 인터페이스를 검색하려면 추가 규칙을 만듭니다.

DCE/RPC 애플리케이션 인터페이스에는 또한 인터페이스 버전 번호가 있습니다. 선택적으로 동일한 버전, 동일하지 않은 버전, 특정 값보다 적거나 큰 버전을 나타내는 연산자와 인터페이스 버전을 지정할 수 있습니다.

TCP 세그멘테이션 또는 IP 프래그먼트화 외에도 연결 지향 DCE/RPC 및 연결 없는 DCE/RPC를 모두 프래그먼트화할 수 있습니다. 일반적으로, 첫 번째 이외의 다른 DCE/RPC 조각을 지정된 인터페이스와 연결하는 것은 유용하지 않고, 이렇게 하면 그 결과로 많은 양의 잘못된 긍정을 얻을 수 있습니다. 그러나, 유연성을 위해 지정된 인터페이스에 대한 모든 조각을 선택적으로 평가할 수 있습니다.

다음 표에는 `dce_iface` 키워드 인수가 요약되어 있습니다.

표 ***194: dce_iface*** 인수

인수	설명
Interface UUID	하이픈을 포함하는 UUID는 사용자가 DCE/RPC 트래픽에서 탐지할 특정 서비스의 애플리케이션 인터페이스를 식별합니다. 특정 인터페이스에 연결된 모든 요청은 인터페이스 UUID에 일치됩니다.
Version	또는, 0에서 65535까지의 애플리케이션 인터페이스 버전 번호 및 특정 값보다 큰(>), 작은(<), 같은(=), 같지 않은(!) 버전을 탐지할지 여부를 나타내는 연산자.
All Fragments	또는, 모든 관련 DCE/RPC 조각의 인터페이스와 일치하는 것을 가능하게 합니다. 지정되어 있는 경우, 인터페이스 버전에서도 가능합니다. 이 인수는 기본적으로 비활성화되어 있는데, 첫 번째 조각 또는 조각화되지 않은 전체 패킷이 특정 인터페이스와 연결되어 있는 경우에만 키워드 일치를 나타냅니다. 이 인수를 활성화하면 잘못된 긍정을 얻을 수 있다는 점에 유의하십시오.

dce_opnum 키워드

`dce_opnum` 키워드를 DCE/RPC 전처리기와 함께 사용하여 DCE/RPC 서비스가 제공하는 하나 이상의 특정 작업을 확인하는 패킷을 탐지할 수 있습니다.

클라이언트 함수 호출은 특정 서비스 함수를 요구하는데, 이는 DCE/RPC 사양에서 작업으로 참조됩니다. 작업 번호(opnum)는 DCE/RPC 헤더에서 특정 작업을 식별합니다. 공격이 특정 작업을 대상으로 할 가능성이 높습니다.

예를 들어, UUID 12345678-1234-abcd-ef00-01234567cffb는 여러 다양한 작업을 제공하는 넷로그온 서비스에 대한 인터페이스를 식별합니다. 그중 하나는 작업 6의 NetrServerPasswordSet 작업입니다.

작업을 위한 서비스를 식별하려면 `dce_iface` 키워드 다음에 `dce_opnum` 키워드를 입력해야 합니다.

단일 십진수 0에서 65535를 지정하여 특정 작업, 하이픈으로 구분된 작업의 범위 또는 쉼표로 구분된 작업 및 범위의 목록을 어떤 순서로도 나타낼 수 있습니다.

다음의 예시 중 하나를 통해 유효한 넷로그온 작업 번호를 지정합니다.

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data 키워드

dce_stub_data 키워드를 DCE/RPC 전처리기와 함께 사용하여 다른 규칙 옵션에 관계없이 스텁 데이터 시작 시 규칙 엔진이 검사를 시작하도록 지정할 수 있습니다. dce_stub_data 키워드를 따르는 패킷 페이로드 규칙 옵션은 스텁 데이터 버퍼에 관련하여 적용됩니다.

DCE/RPC 스텁 데이터는 DCE/RPC 중심의 서비스와 루틴을 제공하는 메커니즘인 클라이언트 절차 호출과 DCE/RPC 런타임 시스템 간 인터페이스를 제공합니다. DCE/RPC 공격은 DCE/RPC 패킷의 스텁 데이터 부분에 표시됩니다. 스텁 데이터는 특정 작업 또는 함수 호출에 연결되어 있으므로, 관련 서비스 및 작업을 식별하려면 dce_stub_data에 앞에 항상 dce_iface 및 dce_opnum을 입력해야 합니다.

dce_stub_data 키워드는 인수를 갖지 않습니다.

SIP 키워드

4개의 SIP 키워드를 사용하면 SIP 세션 트래픽을 모니터링하여 공격을 탐지할 수 있습니다.

SIP 프로토콜은 서비스 거부(DoS) 공격에 취약하다는 점을 참고하십시오. 이러한 공격을 해결할 규칙은 속도 기반 공격 방지를 활용할 수 있습니다.

sip_header 키워드

sip_header 키워드를 사용하여 추출된 SIP 요청 또는 응답 헤더 시작에서 검사를 시작하고 헤더 필드로 검사를 제한할 수 있습니다.

sip_header 키워드는 인수를 갖지 않습니다.

다음의 예제 규칙 조각 SIP 헤더를 가리키고 CSeq 헤더 필드에 일치됩니다.

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

관련 항목

동적 침입 규칙 상태, 2032 페이지
속도 기반 공격 방지, 2359 페이지

sip_body 키워드

sip_body 키워드를 사용하여 추출된 SIP 요청 또는 응답 메시지 본문 시작 지점에서 검사를 시작하고 검사를 메시지 본문 검사로 제한할 수 있습니다.

sip_body 키워드는 인수를 갖지 않습니다.

다음의 예제 규칙 조각은 SIP 메시지 본문을 가리키고 추출된 SDP 데이터의 c(연결 정보) 필드에서 특정 IP 주소에 일치됩니다.

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

규칙은 SDP 내용을 검색하는 것에 제한되지 않습니다. SIP 전처리기는 전체 메시지 본문을 추출하고 이를 규칙 엔진이 사용할 수 있도록 합니다.

sip_method 키워드

각 SIP 요청의 *method* 필드는 요청의 목적을 확인합니다. `sip_method` 키워드를 사용하여 특정 메서드에 대한 SIP 요청을 테스트할 수 있습니다. 메서드가 여러 개인 경우 쉼표로 구분하십시오.

다음 중 하나로 현재 정의된 SIP 메서드를 지정할 수 있습니다.

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

메서드는 대소문자를 구분하지 않습니다. 쉼표로 여러 방법을 분리할 수 있습니다.

새로운 SIP 방법은 향후에 정의될 수도 있기 때문에, 사용자는 또한 사용자 지정 방법, 즉, 현재 정의된 SIP 방법이 아닌 방법을 지정할 수 있습니다. 수락된 필드 값은 RFC 2616에서 정의되는데, `=`, `(`, 및 `}`와 같은 제어 문자 및 구분 기호를 제외한 모든 문자를 허용합니다. 제외되는 구분 기호의 전체 목록을 보려면 RFC 2616을 참고하십시오. 시스템은 트래픽의 지정된 사용자 지정 메서드가 발생할 경우, 패킷 헤더를 검사하지만 메시지는 검사하지 않습니다.

시스템은 최대 32개의 메서드까지 지원하는데, 최근 정의된 메서드 21개에 메서드 11개를 추가한 것입니다. 시스템은 사용자가 구성할 수 있는 정의되지 않은 모든 메서드를 무시합니다. 총 32개의 메서드는 SIP 전처리기 옵션을 **Methods to Check(**확인하는 메서드**)**를 사용하여 지정된 방법을 포함한다는 점에 유의하십시오.

무효화를 사용하면 단 한 개의 방법만 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
!invite
```

그러나 규칙 내 여러 `sip_method` 키워드는 **AND** 작업으로 연결되어 있다는 점을 참고하십시오. 예를 들어 `invite` 및 `cancel` 외의 모든 추출된 메서드를 테스트하려면 두 개의 부정 `sip_method` 키워드를 사용할 수 있습니다.

```
sip_method: !invite
sip_method: !cancel
```

Cisco는 `sip_method` 키워드를 포함하는 규칙에 최소 하나의 `content` 키워드를 포함할 것을 권장합니다. 이는 규칙 엔진이 빠른 패턴 매처를 사용하도록 하여 처리 속도를 높이고 성능을 향상시키기 위함입니다. 규칙에 최소 하나의 `content` 키워드가 포함될 때, `content` 키워드 **Use Fast Pattern Matcher(**빠른 패턴 매처 사용**)** 인수를 활성화했는지 여부에 상관없이 규칙 엔진이 빠른 패턴 매처를 사용한다는 점에 유의하십시오.

관련 항목

SIP 전처리기 옵션, 2271 페이지
content 및 protected_content 키워드, 2088 페이지
content 키워드 빠른 패턴 매처 인수, 2098 페이지

sip_stat_code 키워드

각 SIP 응답에 있는 세 자리의 상태 코드는 요청된 작업의 결과를 나타냅니다. `sip_stat_code` 키워드를 사용하여 특정 상태 코드에 대한 SIP 응답을 테스트할 수 있습니다.

한 자리 응답 유형 번호 1-9, 특정 세 자리 번호 100-999 또는 둘의 어느 조합으로도 쉼표로 구분된 목록을 지정할 수 있습니다. 목록은 목록의 단일 번호가 SIP 응답의 코드에 일치하는 경우 일치합니다.

다음 표에서는 지정할 수 있는 SIP 상태 코드 값을 나타냅니다.

표 ***195: sip_stat_code*** 값

탐지 대상	지정 대상	예시	탐지 대상
특정 상태 코드	3자리 상태 코드	189	189
지정한 단일 숫자로 시작되는 3자리 코드	단일 디지트	1	1xx. 즉, 100, 101, 102 등
값 목록	쉼표로 구분된 특정 코드 및 단일 숫자의 모든 조합	222, 3	222 + 300, 301, 302 등

규칙에 `content` 키워드가 포함되었는지 여부와 상관없이, 규칙 엔진은 `sip_stat_code` 키워드로 지정한 값을 검색하는 데 fast pattern matcher를 사용하지 않습니다.

GTP 키워드

세 개의 GTP(GSRP 터널링 프로토콜) 키워드를 통해 GTP 버전, 메시지 유형 및 정보 요소에 대한 GTP 명령 계통을 검사할 수 있습니다. GTP 키워드는 다른 침입 규칙 키워드(예: `content` 또는 `byte_jump`)와 함께 사용할 수 없습니다. `gtp_info` 또는 `gtp_type` 키워드를 사용하는 각 규칙에서 `gtp_version` 키워드를 사용해야 합니다.

gtp_version 키워드

GTP 버전 0, 1, 2를 위한 GTP 컨트롤 메시지를 검사하려면 `gtp_version` 키워드를 사용할 수 있습니다.

GTP 버전마다 정의하는 메시지 유형 및 정보 요소가 다르기 때문에 `gtp_type` 또는 `gtp_info` 키워드를 사용할 때 반드시 `gtp_version`을 사용해야 합니다. 값 0, 1, 2를 지정할 수 있습니다.

gtp_type 키워드

각 GTP 메시지는 숫자 값 및 문자열 모두로 구성된 메시지 유형으로 식별됩니다. `gtp_type` 키워드를 사용하여 트래픽에서 특정 GTP 메시지 유형을 검사할 수 있습니다. GTP 버전마다 정의하는 메시지 유형 및 정보 요소가 다르기 때문에 `gtp_type` 또는 `gtp_info` 키워드를 사용할 때 반드시 `gtp_version`도 사용해야 합니다.

다음 예에 나온 것처럼 메시지 유형에 대해 정의된 10진수 값, 정의된 문자열, 둘 중 하나 또는 둘 모두의 쉼표로 구분된 조합의 목록을 지정할 수 있습니다.

```
10, 11, echo_request
```

시스템은 OR 연산자를 사용하여 사용자가 나열하는 각 값 또는 문자열에 일치시킵니다. 사용자가 값 및 문자열을 표시하는 순서는 상관없습니다. 목록의 단일 값 또는 문자열과 키워드를 일치시킵니다. 인식되지 않은 문자열 또는 외부 범위 값을 포함하는 규칙을 저장하려고 하는 경우 오류 메시지가 표시됩니다.

동일한 메시지 유형을 위한 서로 다른 값을 사용하는 다양한 GTP 버전이 표에 있다는 점에 유의하십시오. 예를 들어, `sgsn_context_request` 메시지 유형은 GTPv0 및 GTPv1에서 50의 값을 갖지만, GTPv2에서는 130의 값을 갖습니다.

패킷의 버전 번호에 따라 `gtp_type` 키워드는 서로 다른 값에 일치합니다. 위의 예제에서, 키워드는 GTPv0 또는 GTPv1 패킷의 메시지 유형 값 50 및 GTPv2 패킷의 값 130에 일치합니다. 패킷의 메시지 유형 값이 패킷에 지정된 버전에 대해 알려진 값이 아닌 경우 패킷이 키워드에 일치하지 않습니다.

메시지 유형을 위해 정수를 지정한 경우, 키워드의 메시지 유형이 GTP 패킷의 값에 일치하는 경우, 패킷에 지정된 버전에 관계없이 키워드는 일치합니다.

다음 표에서는 각 GTP 메시지 유형에 대해 시스템에서 인식하는 정의된 값 및 문자열을 나열합니다.

표 ***196: GTP*** 메시지 유형

값	버전 **0**	버전 **1**	버전 **2**
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	해당 없음
5	node_alive_response	node_alive_response	해당 없음
6	redirection_request	redirection_request	해당 없음
7	redirection_response	redirection_response	해당 없음
16	create_pdp_context_request	create_pdp_context_request	해당 없음
17	create_pdp_context_response	create_pdp_context_response	해당 없음
18	update_pdp_context_request	update_pdp_context_request	해당 없음
19	update_pdp_context_response	update_pdp_context_response	해당 없음
20	delete_pdp_context_request	delete_pdp_context_request	해당 없음
21	delete_pdp_context_response	delete_pdp_context_response	해당 없음
22	create_aa_pdp_context_request	init_pdp_context_activation_request	해당 없음
23	create_aa_pdp_context_response	init_pdp_context_activation_response	해당 없음
24	delete_aa_pdp_context_request	해당 없음	해당 없음
25	delete_aa_pdp_context_response	해당 없음	해당 없음
26	error_indication	error_indication	해당 없음

값	버전 **0**	버전 **1**	버전 **2**
27	pdu_notification_request	pdu_notification_request	해당 없음
28	pdu_notification_response	pdu_notification_response	해당 없음
29	pdu_notification_reject_request	pdu_notification_reject_request	해당 없음
30	pdu_notification_reject_response	pdu_notification_reject_response	해당 없음
31	해당 없음	supported_ext_header_notification	해당 없음
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	해당 없음	해당 없음	change_notification_request
39	해당 없음	해당 없음	change_notification_response
48	identification_request	identification_request	해당 없음
49	identification_response	identification_response	해당 없음
50	sgsn_context_request	sgsn_context_request	해당 없음
51	sgsn_context_response	sgsn_context_response	해당 없음
52	sgsn_context_ack	sgsn_context_ack	해당 없음
53	해당 없음	forward_relocation_request	해당 없음
54	해당 없음	forward_relocation_response	해당 없음
55	해당 없음	forward_relocation_complete	해당 없음
56	해당 없음	relocation_cancel_request	해당 없음
57	해당 없음	relocation_cancel_response	해당 없음
58	해당 없음	forward_srns_contex	해당 없음
59	해당 없음	forward_relocation_complete_ack	해당 없음
60	해당 없음	forward_srns_contex_ack	해당 없음

값	버전 0	버전 1	버전 2
64	해당 없음	해당 없음	modify_bearer_command
65	해당 없음	해당 없음	modify_bearer_failure_indication
66	해당 없음	해당 없음	delete_bearer_command
67	해당 없음	해당 없음	delete_bearer_failure_indication
68	해당 없음	해당 없음	bearer_resource_command
69	해당 없음	해당 없음	bearer_resource_failure_indication
70	해당 없음	ran_info_relay	downlink_failure_indication
71	해당 없음	해당 없음	trace_session_activation
72	해당 없음	해당 없음	trace_session_deactivation
73	해당 없음	해당 없음	stop_paging_indication
95	해당 없음	해당 없음	create_bearer_request
96	해당 없음	mbms_notification_request	create_bearer_response
97	해당 없음	mbms_notification_response	update_bearer_request
98	해당 없음	mbms_notification_reject_request	update_bearer_response
99	해당 없음	mbms_notification_reject_response	delete_bearer_request
100	해당 없음	create_mbms_context_request	delete_bearer_response
101	해당 없음	create_mbms_context_response	delete_pdn_request
102	해당 없음	update_mbms_context_request	delete_pdn_response
103	해당 없음	update_mbms_context_response	해당 없음
104	해당 없음	delete_mbms_context_request	해당 없음
105	해당 없음	delete_mbms_context_response	해당 없음
112	해당 없음	mbms_register_request	해당 없음
113	해당 없음	mbms_register_response	해당 없음
114	해당 없음	mbms_deregister_request	해당 없음
115	해당 없음	mbms_deregister_response	해당 없음
116	해당 없음	mbms_session_start_request	해당 없음

값	버전 **0**	버전 **1**	버전 **2**
117	해당 없음	mbms_session_start_response	해당 없음
118	해당 없음	mbms_session_stop_request	해당 없음
119	해당 없음	mbms_session_stop_response	해당 없음
120	해당 없음	mbms_session_update_request	해당 없음
121	해당 없음	mbms_session_update_response	해당 없음
128	해당 없음	ms_info_change_request	identification_request
129	해당 없음	ms_info_change_response	identification_response
130	해당 없음	해당 없음	sgsn_context_request
131	해당 없음	해당 없음	sgsn_context_response
132	해당 없음	해당 없음	sgsn_context_ack
133	해당 없음	해당 없음	forward_relocation_request
134	해당 없음	해당 없음	forward_relocation_response
135	해당 없음	해당 없음	forward_relocation_complete
136	해당 없음	해당 없음	forward_relocation_complete_ack
137	해당 없음	해당 없음	forward_access
138	해당 없음	해당 없음	forward_access_ack
139	해당 없음	해당 없음	relocation_cancel_request
140	해당 없음	해당 없음	relocation_cancel_response
141	해당 없음	해당 없음	configuration_transfer_tunnel
149	해당 없음	해당 없음	detach
150	해당 없음	해당 없음	detach_ack
151	해당 없음	해당 없음	cs_paging
152	해당 없음	해당 없음	ran_info_relay
153	해당 없음	해당 없음	alert_mme
154	해당 없음	해당 없음	alert_mme_ack
155	해당 없음	해당 없음	ue_activity

값	버전 0	버전 1	버전 2
156	해당 없음	해당 없음	ue_activity_ack
160	해당 없음	해당 없음	create_forward_tunnel_request
161	해당 없음	해당 없음	create_forward_tunnel_response
162	해당 없음	해당 없음	suspend
163	해당 없음	해당 없음	suspend_ack
164	해당 없음	해당 없음	resume
165	해당 없음	해당 없음	resume_ack
166	해당 없음	해당 없음	create_indirect_forward_tunnel_request
167	해당 없음	해당 없음	create_indirect_forward_tunnel_response
168	해당 없음	해당 없음	delete_indirect_forward_tunnel_request
169	해당 없음	해당 없음	delete_indirect_forward_tunnel_response
170	해당 없음	해당 없음	release_access_bearer_request
171	해당 없음	해당 없음	release_access_bearer_response
176	해당 없음	해당 없음	downlink_data
177	해당 없음	해당 없음	downlink_data_ack
179	해당 없음	해당 없음	pgw_restart
180	해당 없음	해당 없음	pgw_restart_ack
200	해당 없음	해당 없음	update_pdn_request
201	해당 없음	해당 없음	update_pdn_response
211	해당 없음	해당 없음	modify_access_bearer_request
212	해당 없음	해당 없음	modify_access_bearer_response
231	해당 없음	해당 없음	mbms_session_start_request
232	해당 없음	해당 없음	mbms_session_start_response
233	해당 없음	해당 없음	mbms_session_update_request
234	해당 없음	해당 없음	mbms_session_update_response
235	해당 없음	해당 없음	mbms_session_stop_request

값	버전 0	버전 1	버전 2
236	해당 없음	해당 없음	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	해당 없음
241	data_record_transfer_response	data_record_transfer_response	해당 없음
254	해당 없음	end_marker	해당 없음
255	pdu	pdu	해당 없음

gtp_info 키워드

GTP 메시지는 여러 요소 정보를 포함할 수 있는데, 이들 각각은 정의된 숫자 값 및 정의된 문자열 모두에서 확인됩니다. `gtp_info` 키워드를 사용하여 지정된 정보 요소의 시작 부분에서 검사를 시작하고 지정된 정보 요소로 검사를 제한할 수 있습니다. GTP 버전마다 정의하는 메시지 유형 및 정보 요소가 다르기 때문에 이 키워드를 사용할 때 `gtp_version`도 사용해야 합니다.

정보 요소에 대해 정의된 십진수 또는 정의된 문자열을 지정할 수 있습니다. 단일 값 또는 문자열을 지정할 수 있고, 규칙 안에서 여러 `gtp_info` 키워드를 사용하여 여러 요소 정보를 검사할 수 있습니다.

메시지가 동일한 유형의 여러 요소 정보를 포함할 때, 모두가 일치 여부를 위해 검사됩니다. 정보 요소가 잘못된 순서대로 발생하는 경우, 마지막 인스턴스만 검사됩니다.

동일한 정보 요소에 대해 서로 다른 값을 사용하는 다양한 GTP 버전이 있다는 점에 유의하십시오. 예를 들어, `cause` 정보 요소는 GTPv0 및 GTPv1에서 1의 값을 갖지만, GTPv2에서는 2의 값을 갖습니다.

패킷의 버전 번호에 따라 `gtp_info` 키워드는 서로 다른 값에 일치합니다. 위의 예제에서, 키워드는 GTPv0 또는 GTPv1 패킷의 정보 요소 값 1 및 GTPv2 패킷의 값 2에 일치합니다. 패킷의 정보 요소 값이 패킷에 지정된 버전에 대해 알려진 값이 아닌 경우 패킷이 키워드에 일치하지 않습니다.

정보 요소 값에 정수를 지정한 경우, 키워드의 메시지 유형이 GTP 패킷의 값에 일치하는 경우, 패킷에 지정된 버전에 관계없이 키워드에 일치합니다.

다음 표에서는 각 GTP 정보 요소에 대해 시스템에서 인식하는 값 및 문자열을 나열합니다.

표 ***197: GTP*** 정보 요소

값	버전 0	버전 1	버전 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	해당 없음
5	p_tmsi	p_tmsi	해당 없음

값	버전 0	버전 1	버전 2
6	qos	해당 없음	해당 없음
8	recording_required	recording_required	해당 없음
9	authentication	authentication	해당 없음
11	map_cause	map_cause	해당 없음
12	p_tmsi_sig	p_tmsi_sig	해당 없음
13	ms_validated	ms_validated	해당 없음
14	recovery	recovery	해당 없음
15	selection_mode	selection_mode	해당 없음
16	flow_label_data_1	teid_1	해당 없음
17	flow_label_signalling	teid_control	해당 없음
18	flow_label_data_2	teid_2	해당 없음
19	ms_unreachable	teardown_ind	해당 없음
20	해당 없음	nsapi	해당 없음
21	해당 없음	ranap	해당 없음
22	해당 없음	rab_context	해당 없음
23	해당 없음	radio_priority_sms	해당 없음
24	해당 없음	radio_priority	해당 없음
25	해당 없음	packet_flow_id	해당 없음
26	해당 없음	charging_char	해당 없음
27	해당 없음	trace_ref	해당 없음
28	해당 없음	trace_type	해당 없음
29	해당 없음	ms_unreachable	해당 없음
71	해당 없음	해당 없음	apn
72	해당 없음	해당 없음	ambr
73	해당 없음	해당 없음	ebi
74	해당 없음	해당 없음	ip_addr

값	버전 **0**	버전 **1**	버전 **2**
75	해당 없음	해당 없음	mei
76	해당 없음	해당 없음	msisdn
77	해당 없음	해당 없음	indication
78	해당 없음	해당 없음	pco
79	해당 없음	해당 없음	paa
80	해당 없음	해당 없음	bearer_qos
80	해당 없음	해당 없음	flow_qos
82	해당 없음	해당 없음	rat_type
83	해당 없음	해당 없음	serving_network
84	해당 없음	해당 없음	bearer_tft
85	해당 없음	해당 없음	tad
86	해당 없음	해당 없음	uli
87	해당 없음	해당 없음	f_teid
88	해당 없음	해당 없음	tmsi
89	해당 없음	해당 없음	cn_id
90	해당 없음	해당 없음	s103pdf
91	해당 없음	해당 없음	s1udf
92	해당 없음	해당 없음	delay_value
93	해당 없음	해당 없음	bearer_context
94	해당 없음	해당 없음	charging_id
95	해당 없음	해당 없음	charging_char
96	해당 없음	해당 없음	trace_info
97	해당 없음	해당 없음	bearer_flag
99	해당 없음	해당 없음	pdn_type
100	해당 없음	해당 없음	pti
101	해당 없음	해당 없음	drx_parameter

값	버전 0	버전 1	버전 2
103	해당 없음	해당 없음	gsm_key_tri
104	해당 없음	해당 없음	umts_key_cipher_quin
105	해당 없음	해당 없음	gsm_key_cipher_quin
106	해당 없음	해당 없음	umts_key_quin
107	해당 없음	해당 없음	eps_quad
108	해당 없음	해당 없음	umts_key_quad_quin
109	해당 없음	해당 없음	pdn_connection
110	해당 없음	해당 없음	pdn_number
111	해당 없음	해당 없음	p_tmsi
112	해당 없음	해당 없음	p_tmsi_sig
113	해당 없음	해당 없음	hop_counter
114	해당 없음	해당 없음	ue_time_zone
115	해당 없음	해당 없음	trace_ref
116	해당 없음	해당 없음	complete_request_msg
117	해당 없음	해당 없음	guti
118	해당 없음	해당 없음	f_container
119	해당 없음	해당 없음	f_cause
120	해당 없음	해당 없음	plmn_id
121	해당 없음	해당 없음	target_id
123	해당 없음	해당 없음	packet_flow_id
124	해당 없음	해당 없음	rab_contex
125	해당 없음	해당 없음	src_rnc_pdcp
126	해당 없음	해당 없음	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id

값	버전 **0**	버전 **1**	버전 **2**
130	pdp_context	pdp_context	해당 없음
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	해당 없음	qos	node_type
136	해당 없음	authentication_qu	fqdn
137	해당 없음	tft	ti
138	해당 없음	target_id	mbms_session_duration
139	해당 없음	utran_trans	mbms_service_area
140	해당 없음	rab_setup	mbms_session_id
141	해당 없음	ext_header	mbms_flow_id
142	해당 없음	trigger_id	mbms_ip_multicast
143	해당 없음	omc_id	mbms_distribution_ack
144	해당 없음	ran_trans	rfsp_index
145	해당 없음	pdp_context_pri	uci
146	해당 없음	addi_rab_setup	csg_info
147	해당 없음	sgsn_number	csg_id
148	해당 없음	common_flag	cmi
149	해당 없음	apn_restriction	service_indicator
150	해당 없음	radio_priority_lcs	detach_type
151	해당 없음	rat_type	ldn
152	해당 없음	user_loc_info	node_feature
153	해당 없음	ms_time_zone	mbms_time_to_transfer
154	해당 없음	imei_sv	throttling
155	해당 없음	camel	arp

값	버전 0	버전 1	버전 2
156	해당 없음	mbms_ue_context	epc_timer
157	해당 없음	tmp_mobile_group_id	signalling_priority_indication
158	해당 없음	rim_routing_addr	tmgi
159	해당 없음	mbms_config	mm_srvcc
160	해당 없음	mbms_service_area	flags_srvcc
161	해당 없음	src_rnc_pdcp	nmbr
162	해당 없음	addi_trace_info	해당 없음
163	해당 없음	hop_counter	해당 없음
164	해당 없음	plmn_id	해당 없음
165	해당 없음	mbms_session_id	해당 없음
166	해당 없음	mbms_2g3g_indicator	해당 없음
167	해당 없음	enhanced_nsapi	해당 없음
168	해당 없음	mbms_session_duration	해당 없음
169	해당 없음	addi_mbms_trace_info	해당 없음
170	해당 없음	mbms_session_repetition_num	해당 없음
171	해당 없음	mbms_time_to_data	해당 없음
173	해당 없음	bss	해당 없음
174	해당 없음	cell_id	해당 없음
175	해당 없음	pdu_num	해당 없음
177	해당 없음	mbms_bearer_capab	해당 없음
178	해당 없음	rim_routing_disc	해당 없음
179	해당 없음	list_pfc	해당 없음
180	해당 없음	ps_xid	해당 없음
181	해당 없음	ms_info_change_report	해당 없음
182	해당 없음	direct_tunnel_flags	해당 없음
183	해당 없음	correlation_id	해당 없음

값	버전 **0**	버전 **1**	버전 **2**
184	해당 없음	bearer_control_mode	해당 없음
185	해당 없음	mbms_flow_id	해당 없음
186	해당 없음	mbms_ip_multicast	해당 없음
187	해당 없음	mbms_distribution_ack	해당 없음
188	해당 없음	reliable_inter_rat_handover	해당 없음
189	해당 없음	rfsp_index	해당 없음
190	해당 없음	fqdn	해당 없음
191	해당 없음	evolved_allocation1	해당 없음
192	해당 없음	evolved_allocation2	해당 없음
193	해당 없음	extended_flags	해당 없음
194	해당 없음	uci	해당 없음
195	해당 없음	csg_info	해당 없음
196	해당 없음	csg_id	해당 없음
197	해당 없음	cmi	해당 없음
198	해당 없음	apn_ambr	해당 없음
199	해당 없음	ue_network	해당 없음
200	해당 없음	ue_ambr	해당 없음
201	해당 없음	apn_ambr_nsapi	해당 없음
202	해당 없음	ggsn_backoff_timer	해당 없음
203	해당 없음	signalling_priority_indication	해당 없음
204	해당 없음	signalling_priority_indication_nsapi	해당 없음
205	해당 없음	high_bitrate	해당 없음
206	해당 없음	max_mbr	해당 없음
251	charging_gateway_addr	charging_gateway_addr	해당 없음
255	private_extension	private_extension	private_extension

SCADA 키워드

규칙 엔진은 Modbus, DNP3, CIP 및 S7Commplus 규칙을 사용하여 특정 프로토콜 필드에 액세스합니다.

Modbus 키워드

Modbus 키워드는 단독으로 또는 `content` 및 `byte_jump`와 같은 다른 키워드와 조합하여 사용할 수 있습니다.

modbus_data

`modbus_data` 키워드를 사용하여 Modbus(모드버스) 요청 또는 응답 내 Data(데이터) 필드의 시작 부분을 나타낼 수 있습니다.

modbus_func

`modbus_func` 키워드를 사용하여 Modbus 애플리케이션 레이어 요청 또는 응답 헤더의 Function Code 필드에 일치시킬 수 있습니다. Modbus(모드버스) 기능 코드에 대해 단일 정의된 십진수 또는 단일 정의된 문자열을 지정할 수 있습니다.

다음 표에서는 Modbus(모드버스) 기능 코드를 위한 시스템에서 인식하는 정의된 값 및 문자열을 나열합니다.

표 ***198:*** 모드버스 기능 코드

값	문자열
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id

값	문자열
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

modbus_unit

`modbus_unit` 키워드를 사용하여 Modbus(모드버스) 요청 또는 응답 헤더에 Unit ID(장치 ID) 필드에 대한 단일 십진수와 일치시킬 수 있습니다.

DNP3 키워드

DNP3 키워드는 단독으로 또는 다른 키워드(예: `content` 또는 `byte_jump`)와 함께 사용할 수 있습니다.

dnp3_data

리어셈블된 DNP3 애플리케이션 레이어 조각의 시작 부분을 나타낼 때 `dnp3_data` 키워드를 사용할 수 있습니다.

DNP3 전처리기는 연결 레이어 프레임을 애플리케이션 레이어 조각으로 리어셈블합니다. `dnp3_data` 키워드는 각 애플리케이션 레이어 조각의 시작 부분을 나타냅니다. 다른 규칙 옵션은 데이터를 구분하고 16바이트마다 체크섬을 추가할 필요 없이 단편 내 리어셈블된 데이터를 일치시킬 수 있습니다.

dnp3_func

`dnp3_func` 키워드를 사용하여 DNP3 애플리케이션 레이어 요청 또는 응답 헤더의 Function Code(기능 코드) 필드에 일치시킬 수 있습니다. DNP3 기능 코드에 대해 단일 정의된 십진수 또는 단일 정의된 문자열을 지정할 수 있습니다.

다음 표에서는 DNP3 기능 코드의 시스템에서 인식하는 정의된 값 및 문자열을 나열합니다.

표 ***199: DNP3*** 기능 코드

값	문자열
0	confirm
1	read
2	write
3	select
4	operate

값	문자열
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req

값	문자열
33	authenticate_err
129	대응
130	unsolicited_response
131	authenticate_resp

dnp3_ind

`dnp3_ind` 키워드를 사용하여 DNP3 애플리케이션 레이어 응답 헤더의 Internal Indications(내부 표시) 필드의 플래그에 일치시킬 수 있습니다.

다음 예와 같이 알려진 단일 플래그 또는 쉼표로 구분된 플래그 목록에 대한 문자열을 지정할 수 있습니다.

```
class_1_events, class_2_events
```

여러 플래그를 지정할 때, 키워드는 목록의 모든 플래그에 일치시킵니다. 플래그 조합을 검색하려면, 규칙에서 `dnp3_ind` 키워드를 여러 번 사용합니다.

다음 목록은 정의된 DNP3 내부 표시 플래그를 시스템에서 인식하는 문자열 구문을 제공합니다.

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

dnp3_obj

`dnp3_obj` 키워드를 사용하여 요청 또는 응답의 DNP3 개체 헤더에 일치시킬 수 있습니다.

DNP3 데이터는 아날로그 입력 및 이진 입력 등과 같은 다양한 유형의 일련의 DNP3 개체로 구성됩니다. 각 유형은 아날로그 입력 그룹, 이진 입력 그룹과 같이 그룹으로 식별되는데, 이들 각각은 십진수 값으로 식별됩니다. 각 그룹의 개체는 16비트 정수, 32비트 정수, 짧은 부동 소수점 등과 같은 개체 변수에 의해 추가 식별되며 이들 각각은 개체의 데이터 형식을 지정합니다. 각 유형의 개체 변수는 또한 십진수로 식별할 수 있습니다.

개체 헤더 그룹 유형에 대한 십진수 및 개체 변수 유형에 대한 십진수를 지정하여 개체 헤더를 식별합니다. 이 둘의 조합은 DNP3 개체의 특정 유형을 정의합니다.

CIP 및 ENIP 키워드

다음 키워드를 단독으로 또는 함께 사용하여 CIP 전처리기에 의해 식별된 CIP 및 ENIP 트래픽에 대해 공격을 식별하는 맞춤형 침입 규칙을 생성할 수 있습니다. 구성 가능한 키워드의 경우, 허용되는 범위 내에서 단일 정수를 지정합니다. 자세한 내용은 CIP 전처리기, 2305 페이지를 참조하십시오.

표 ***200:***

키워드	일치 항목	범위
`cip_attribute`	CIP 메시지의 개체 클래스/인스턴스 속성 필드입니다. 정의된 단일 정수 값을 지정합니다.	0 - 65535
`cip_class`	CIP 메시지의 개체 클래스 필드입니다. 정의된 단일 정수 값을 지정합니다.	0 - 65535
`cip_conn_path_class`	연결 경로의 개체 클래스입니다. 단일 정수 값을 지정합니다.	0 - 65535
`cip_instance`	CIP 메시지의 인스턴스 ID 필드입니다. 단일 정수 값을 지정합니다.	0 - 4284927295
`cip_req`	서비스 요청 메시지입니다.	해당 없음
`cip_rsp`	서비스 응답 메시지입니다.	해당 없음
`cip_service`	CIP 서비스 요청 메시지의 서비스 필드입니다. 단일 정수 값을 지정합니다.	0 - 127
`cip_status`	CIP 서비스 응답 메시지의 상태 필드입니다. 단일 정수 값을 지정합니다.	0 - 255
`enip_command`	EthNet/IP 헤더의 명령 코드입니다. 단일 정수 값을 지정합니다.	0 - 65535
`enip_req`	EthNet/IP 요청 메시지입니다.	해당 없음
`enip_rsp`	EthNet/IP 응답 메시지입니다.	해당 없음

S7Commplus 키워드

S7Commplus 키워드를 단독으로 또는 함께 사용하여 CS7Commplus 전처리기에 의해 식별된 트래픽에 대해 공격을 식별하는 맞춤형 침입 규칙을 생성할 수 있습니다. 구성 가능한 키워드의 경우, 허용

되는 범위 내에서 단일 정수를 지정합니다. 자세한 내용은 S7Commplus 전처리기, 2309 페이지를 참고하십시오.

다음 사항을 참고하십시오.

- 동일한 규칙의 여러 S7commplus 키워드는 AND-ed입니다.
- 동일한 규칙에서 여러 `s7commplus_func` 또는 `s7commplus_opcode` 키워드를 사용하면 규칙이 무효화되며 트래픽과 일치하지 않습니다. 이러한 키워드로 여러 값을 검색하려면 여러 규칙을 생성합니다.

s7commplus_content

S7Commplus 침입 규칙에서 `content` 또는 `protected_content` 키워드를 사용하기 전에 `s7commplus_content` 키워드를 사용하여 패킷 페이로드의 시작 부분에 커서를 놓습니다. 자세한 내용은 content 및 protected_content 키워드, 2088 페이지를 참조하십시오.

s7commplus_func

`s7commplus_func` 키워드를 사용하여 S7Commplus 헤더의 다음 값 중 하나와 일치시킵니다.

- explore
- create object
- delete object
- setvariable
- getlink
- setmultivar
- getmultivar
- beginsequence
- endsequence
- invoke
- getvarsubstr
- 0x0 ~ 0xFFF

  숫자 식은 추가 값을 허용합니다.

s7commplus_opcode

`s7commplus_opcode` 키워드를 사용하여 S7Commplus 헤더의 다음 값 중 하나와 일치시킵니다.

- request
- response(대응)

- notification(알림)
- response2
- 0x0 ~ 0xFF

  숫자 식은 추가 값을 허용합니다.

패킷 특성

특정 패킷 특성을 가진 패킷에 대해서만 이벤트를 생성하는 규칙을 작성할 수 있습니다.

dsize

`dsize` 키워드는 패킷 페이로드 크기를 테스트합니다. 이 키워드와 보다 큼 연산자 및 보다 작음 연산자(<와 >)를 사용하여 값의 범위를 지정할 수 있습니다. 다음 구문을 사용하여 범위를 지정할 수 있습니다.

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

예를 들어, 400바이트보다 큰 패킷 크기를 나타내려면, `dtype` 값으로 `>400`을 사용합니다. 500바이트 미만의 패킷 크기를 나타내려면, `<500`을 사용합니다. 400바이트와 500바이트 사이의 모든 패킷에 대한 규칙 트리거를 포함하는 것으로 지정하려면, `400<>500`을 사용합니다.

⚠

주의 `dsize` 키워드는 모든 전처리기가 해독하기 전에 패킷을 테스트합니다.

isdataat

`isdataat` 키워드는 데이터가 페이로드의 특정 위치에 있다는 것을 규칙 엔진이 확인하도록 지시합니다.

다음 표에서는 `isdataat` 키워드와 함께 사용할 수 있는 인수를 나열합니다.

표 ***201: isdataat*** 인수

인수	유형	설명
Offset(오프셋)	필수	페이로드에서 특정 위치입니다. 예를 들어, 패킷 페이로드에서 데이터가 50바이트에 나타난다는 것을 테스트하려면, 오프셋 값으로 `50`을 지정합니다. `!` 수식자는 `isdataat` 테스트의 결과를 무효화합니다. 페이로드에 일정량의 데이터가 나타나지 않으면 경고합니다. 기존의 `byte_extract` 변수를 사용하여 이 인수의 값을 지정할 수도 있습니다.

인수	유형	설명
Relative	선택 사항	위치가 마지막으로 성공한 콘텐츠 일치와 연결되도록 합니다. 상대적 위치를 지정한 경우, 카운터가 0바이트에서 시작하므로, 계산하는 마지막으로 성공한 콘텐츠 일치에서 앞으로 이동할 바이트 수에서 1를 빼 위치를 계산한다는 점에 유의하십시오. 예를 들어, 데이터가 마지막으로 성공한 콘텐츠 일치 후 아홉 번째 바이트에 표시되도록 지정하려면, `8`의 상대적 오프셋을 지정합니다.
Raw Data	선택 사항	Firepower System 전처리기에서 암호 해독 또는 애플리케이션 레이어 표준화가 이루어지기 전에 데이터가 원래 패킷 페이로드에 위치하도록 지정합니다. 이전 콘텐츠 일치 항목이 원시 데이터 패킷에 있는 경우 이 인수를 **Relative(**연결**)**와 함께 사용할 수 있습니다.

예를 들어, 콘텐츠 `foo`를 검색하는 규칙에서 `isdataat`에 대한 값이 다음과 같이 지정될 경우

- Offset =!10
- Relative = 활성화

페이로드가 끝나기 전 `foo` 다음에 오는 10바이트를 규칙 엔진이 탐지하지 않는 경우 시스템에서 경고합니다.

sameip

`sameip` 키워드는 패킷의 소스와 대상 IP 주소가 동일한지 테스트합니다. 이 키워드는 인수를 취하지 않습니다.

fragoffset

`fragoffset` 키워드는 단편화된 패킷의 오프셋을 테스트합니다. 일부 익스플로잇(예: WinNuke DoS 공격)은 특정 오프셋이 있는, 수동으로 생성된 패킷 프래그먼트를 사용하므로 이 키워드가 유용합니다.

예를 들어, 단편화된 패킷의 오프셋이 31337바이트인지 여부를 테스트하려면, `fragoffset` 값으로 `31337`을 지정합니다.

`fragoffset` 키워드에 인수를 지정할 때 다음 연산자를 사용할 수 있습니다.

표 ***202: fragoffset*** 키워드 인수 연산자

연산자	설명
!	not
>	보다 큼
<	보다 작음

not 연산자(`!`)를 `<` 또는 `>`와 조합하여 사용할 수 없음에 유의하십시오.

cvs

`cvs` 키워드는 잘못된 형식의 CVS 항목에 대해 Concurrent Versions System(공동 버전 시스템, CVS) 트래픽을 테스트합니다. 공격자는 잘못된 형식의 항목을 사용하여 힙 오버플로를 강제하고 CSV 서버에서 악성 코드를 실행할 수 있습니다. 이 키워드는 두 개의 알려진 CVS 취약성에 대한 공격을 식별하는 데 사용될 수 있습니다. CVE-2004-0396(CVS 1.11 x~1.11.15, 1.12 x~1.12.7) 및 CVS-2004-0414(CVS 1.12 x~1.12.8, 1.11 x~1.11.16). `cvs` 키워드는 올바른 형식의 항목을 점검하고 잘못된 형식의 항목이 탐지되면 알림을 생성합니다.

사용자 규칙은 CVS 실행 포트를 포함해야 합니다. 또한, 트래픽이 발생할 수 있는 모든 포트는 CVS 세션을 위해 상태가 유지될 수 있도록 TCP 정책 내 스트림 리어셈블리에 대한 포트 목록에 추가해야 합니다. TCP 포트 2401(`pserver`) 및 514(`rsh`)는 스트림 리어셈블리가 발생하는 클라이언트 포트 목록에 포함됩니다. 그러나 사용자 서버가 `xinetd` 서버(즉, pserver)로 실행되는 경우, 이는 모든 TCP 포트에서 실행될 수 있다는 점에 유의하십시오. 스트림 리어셈블리 **Client Ports(**클라이언트 포트**)** 목록에 모든 비표준 포트를 추가합니다.

관련 항목

byte_extract 키워드, 2106 페이지
TCP 스트림 전처리 옵션, 2337 페이지

활성 응답 키워드

resp와 **react** 키워드는 활성 응답을 시작하는 2가지 방법을 제공합니다. 키워드 하나를 포함하는 침입 규칙은 패킷이 규칙을 트리거하면 단일 활성 응답을 시작합니다. 활성 응답 키워드는 트리거된 TCP 규칙에 대한 응답으로 TCP 연결을 종료하거나 트리거된 UDP 규칙에 대한 응답으로 UDP 세션을 닫는 활성 응답을 시작할 수 있습니다. 침입 삭제 규칙에서의 활성 응답, 2313 페이지의 내용을 참조하십시오. 활성 응답은 방화벽을 대신하지는 않습니다. 다양한 이유가 있는데, 대표적인 이유는 공격자가 활성 응답을 무시하거나 우회하도록 선택할 수 있다는 것입니다.

활성 응답은 (라우티드 또는 투명을 포함하는) 인라인 구축에서 지원됩니다. 예를 들어 인라인 배포의 `react` 키워드에 대한 응답으로, 시스템은 연결의 각 첨단 트래픽에 TCP 재설정(RST) 패킷을 직접 삽입할 수 있는데, 이는 보통 연결을 종료하게 합니다. 활성 응답은 패시브 구축에는 지원되지 않으며 적합하지도 않습니다.

활성 응답이 다시 라우팅될 수 있기 때문에, 시스템은 TCP 재설정이 TCP 재설정을 시작하도록 허용하지 않습니다. 이는 활성 응답의 무한 시퀀스를 방지합니다. 시스템은 또한 표준 관행에 따라 ICMP에서 연결할 수 없는 패킷이 ICMP에서 연결할 수 없는 패킷을 시작하도록 허용하지 않습니다.

침입 규칙이 활성 응답을 시작한 후 TCP 스트림 전처리기를 구성하여 TCP 연결에서 추가 트래픽을 탐지할 수 있습니다. 전처리기가 추가 트래픽을 탐지하면, 연결 또는 세션의 양쪽 끝에 지정된 최대 값까지 추가 활성 응답을 보냅니다. 고급 전송/네트워크 전처리기 옵션, 2314 페이지의 **Maximum Active Responses(**최대 활성 응답**)** 및 **Minimum Response Seconds(**최소 응답 시간**(**초**))**를 참조하십시오.

관련 항목

침입 삭제 규칙에서의 활성 응답, 2313 페이지

resp 키워드

규칙 헤더에서 TCP 또는 UDP 프로토콜 지정 여부에 따라 `resp` 키워드를 사용하여 TCP 연결 또는 UDP 세션에 적극적으로 응답할 수 있습니다.

키워드 인수를 통해 패킷 방향을 지정하고 TCP 재설정(RST) 패킷 또는 ICMP에서 연결할 수 없는 패킷을 활성 응답으로 사용할지 여부를 지정할 수 있습니다.

TCP 재설정(RST) 패킷 또는 ICMP에서 연결할 수 없는 패킷 중 무엇이든 사용하여 TCP 연결을 종료할 수 있습니다. UDP 세션을 종료하려면 ICMP에서 연결할 수 없는 인수만 사용해야 합니다.

다양한 TCP 재설정 인수를 통해 패킷 소스, 대상 또는 둘 다에 대한 활성 응답을 대상으로 할 수도 있습니다. 모든 ICMP에서 연결할 수 없는 인수는 패킷 소스를 대상으로 하며, 이러한 인수를 사용하여 ICMP 네트워크, 호스트, 포트에서 연결할 수 없는 패킷 또는 셋 모두를 사용할지 여부를 지정할 수 있습니다.

다음 표에는 규칙이 트리거될 때 Firepower System이 수행할 작업을 정확히 지정하기 위해 `resp` 키워드와 함께 사용할 수 있는 인수가 나열되어 있습니다.

표 ***203: resp*** 인수

인수	설명
reset_source	TCP 재설정 패킷을 규칙을 시작했던 패킷을 전송한 엔드 포인트에 보냅니다. 또는, 이전 버전과의 호환성을 위해 지원되는 `rst_snd`를 지정할 수 있습니다.
reset_dest	TCP 재설정 패킷을 규칙을 트리거한 패킷의 해당 대상 엔드 포인트에 보냅니다. 또는, 이전 버전과의 호환성을 위해 지원되는 `rst_rcv`를 지정할 수 있습니다.
reset_both	TCP 재설정 패킷을 전송 및 수신 엔드 포인트 모두에 보냅니다. 또는, 이전 버전과의 호환성을 위해 지원되는 `rst_all`을 지정할 수 있습니다.
icmp_net	ICMP 네트워크에서 연결할 수 없는 메시지를 발신자에게 보냅니다.
icmp_host	ICMP 호스트에서 연결할 수 없는 메시지를 발신자에게 보냅니다.
icmp_port	ICMP 포트에서 연결할 수 없는 메시지를 발신자에게 보냅니다. 이 인수는 UDP 트래픽을 종료하는 데 사용됩니다.
icmp_all	다음 ICMP 메시지를 발신자에게 보냅니다. • 네트워크에서 연결할 수 없음 • 호스트에서 연결할 수 없음 • 포트에서 연결할 수 없음

예를 들어 규칙이 트리거될 때 연결의 양쪽을 재설정하도록 규칙을 구성하려면 `resp` 키워드에 대한 값으로 `reset_both`를 사용합니다.

쉼표로 구분된 목록을 사용하여 다음과 같이 여러 인수를 지정할 수 있습니다.

```
argument,argument,argument
```

관련 항목

config response 명령

react 키워드

react 키워드를 사용하여 패킷이 규칙을 트리거할 때 TCP 연결 클라이언트에 기본 HTML 페이지를 보낼 수 있습니다. HTML 페이지를 보낸 후, 시스템은 TCP 재설정 패킷을 사용하여 연결 양쪽 끝에 활성 응답을 시작합니다. react 키워드는 UDP 트래픽에 대한 활성 응답을 시작하지 않습니다.

선택적으로, 다음 인수를 지정할 수 있습니다.

```
msg
```

패킷이 msg 인수를 사용하는 react 규칙을 트리거할 때, HTML 페이지는 규칙 이벤트 메시지를 포함합니다.

msg 인수를 지정하지 않으면 HTML 페이지에 다음 메시지가 포함됩니다.

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

참고 활성 응답이 다시 라우팅될 수 있으므로, HTML 페이지가 react 규칙을 시작하지 않도록 확인합니다. 이는 활성 응답의 무한 시퀀스를 방지합니다. Cisco는 프로덕션 환경에서 이를 활성화하기 전에 react 규칙을 광범위하게 테스트하는 것을 권장합니다.

관련 항목

규칙 구조, 2065 페이지

config response 명령

detection_filter 키워드

지정된 패킷 수가 지정된 시간 안에 규칙을 트리거하지 않는 한 detection_filter 키워드를 사용하여 이벤트 생성에서 규칙을 방지할 수 있습니다. 이를 통해 규칙이 조기에 이벤트를 생성하는 것을 중지할 수 있습니다. 예를 들어, 몇 초 동안 둘 또는 세 번의 로그인 실패는 예상된 작업일 수 있지만, 동일한 시간 동안 많은 시도가 있었다면 무차별 암호 대입 공격(brute force attack)을 나타낼 수 있습니다.

detection_filter 키워드에는 시스템이 소스 또는 대상 IP 주소를 추적하는지 여부, 이벤트를 트리거하기 전에 탐지 기준이 충족해야 하는 횟수, 횟수를 세는 기간을 정의하는 인수가 필요합니다.

이벤트 트리거를 연기하려면 다음 구문을 사용합니다.

```
track by_src/by_dst, count count, seconds number_of_seconds
```

track 인수는 규칙의 탐지 기준에 맞는 패킷 수를 셀 때 패킷의 소스 또는 대상 IP 주소를 사용할지 여부를 지정합니다. 시스템이 이벤트 인스턴스를 추적하는 방식을 지정하려면 다음 표에 설명된 인수 값에서 선택합니다.

표 ***204: detection_filter*** 추적 인수

인수	설명
by_src	소스 IP 주소로 세는 탐지 기준입니다.
by_dst	대상 IP 주소로 세는 탐지 기준입니다.

count 인수는 규칙이 이벤트를 생성하기 전에 지정된 시간 내에 지정된 IP 주소에 대한 규칙을 트리거해야 하는 패킷 수를 지정합니다.

seconds 인수는 규칙이 이벤트를 생성하기 전에 패킷의 지정된 수가 규칙을 트리거해야 하는 초를 지정합니다.

콘텐츠 foo에 대한 패킷을 검색하고 다음 인수와 함께 detection_filter 키워드를 사용하는 규칙의 사례를 고려해 보십시오.

```
track by_src, count 10, seconds 20
```

예제에서, 규칙이 특정 소스 IP 주소에서 20초 내에 10개 패킷에서 foo를 탐지할 때까지 이벤트를 생성하지 않습니다. 시스템이 처음 20초 내에 foo를 포함하는 패킷을 7개만 검색할 경우, 어떤 이벤트도 생성되지 않습니다. 그러나, 처음 20초 안에 foo가 40번 발생하면 규칙은 30개의 이벤트를 생성하고, 20초가 경과할 때 카운트가 다시 시작됩니다.

임계값과 **detection_filter** 키워드 비교

detection_filter 키워드는 더 이상 사용되지 않는 threshold 키워드를 대체합니다. threshold 키워드는 하위 버전 호환성을 계속 지원하며 침입 정책 안에서 설정한 임계값과 동일하게 실행합니다.

detection_filter 키워드는 패킷이 규칙을 트리거하기 전에 적용되는 탐지 기능입니다. 규칙은 지정된 패킷을 카운트하기 전에 탐지된 패킷 트리거에 대한 이벤트를 생성하지 않으며, 인라인 배포에서 규칙이 패킷을 삭제하도록 설정된 경우라도 해당 패킷을 삭제하지 않습니다. 반대로, 규칙은 규칙을 트리거하고 지정된 패킷 수 후에 발생하는 이벤트를 생성하며, 인라인 배포에서 규칙이 패킷을 삭제하도록 설정된 경우라면 해당 패킷을 삭제합니다.

임계값 설정은 탐지 작업으로 귀결되지 않는 이벤트 알림 기능입니다. 이는 패킷이 이벤트를 트리거한 후 적용됩니다. 인라인 배포에서 패킷을 삭제하도록 설정된 규칙은 규칙 임계값과는 별개로 규칙을 트리거하는 모든 패킷을 삭제합니다.

침입 정책에서 침입 이벤트 임계값 지정, 침입 이벤트 억제, 속도 기반 공격 방지 기능을 원하는 대로 조합하여 detection_filter 키워드를 사용할 수 있습니다. 또한 더 이상 사용되지 않는 threshold 키워드를 침입 정책의 침입 이벤트 임계값 설정 기능과 함께 사용하는, 가져온 로컬 규칙을 활성화한 경우 정책 인증이 실패할 수 있다는 점을 참고하십시오.

관련 항목

침입 이벤트 임계값, 2025 페이지
침입 정책 삭제 설정, 2029 페이지

규칙 페이지에서 동적 규칙 상태 설정, 2034 페이지
로컬 침입 규칙 가져오기 모범 사례, 190 페이지

tag 키워드

tag 키워드를 사용하여 시스템이 호스트 또는 세션에 대한 추가 트래픽을 로깅하도록 지시합니다. tag 키워드를 사용하여 캡처할 트래픽 유형 및 볼륨을 지정할 때 다음 구문을 사용합니다.

```
tagging_type, count, metric, optional_direction
```

다음 3개의 표에서는 사용 가능한 기타 인수를 설명합니다.

태그 지정의 2가지 유형을 선택할 수 있습니다. 다음 표에서는 태그 지정의 2가지 유형을 나타냅니다. 침입 규칙에 규칙 헤더 옵션만 구성한 경우 세션 태그 인수 유형은 다른 세션에서 가져온 것과 동일한 세션에서 가져온 패킷을 시스템이 로깅한다는 점에 유의하십시오. 동일한 세션에서 가져온 패킷을 그룹화하려면, 동일한 침입 규칙 내에서 하나 이상의 규칙 옵션(flag 키워드 또는 content 키워드)을 구성합니다.

표 ***205:*** 태그 인수

인수	설명
session	규칙을 트리거한 세션의 패킷을 로깅합니다.
host	규칙을 트리거한 패킷을 전송한 호스트의 패킷을 로깅합니다. 방향 수식자를 추가하여 호스트에서 가져오는 트래픽만 로깅(src)하거나 호스트로 이동하는 트래픽만 로깅(dst)할 수 있습니다.

트래픽을 얼마나 로깅할지 나타내려면 다음 인수를 사용합니다.

표 ***206: count*** 인수

인수	설명
count	규칙이 트리거된 후 로깅하려는 패킷 또는 시간(초)입니다. 이 측정 단위는 count 인수 다음에 오는 메트릭 인수로 지정됩니다.

다음 표에 설명된 메트릭 중 시간 단위나 트래픽 볼륨으로 로깅하려는 메트릭을 선택하십시오.

주의 높은 대역폭 네트워크는 초당 수천 개의 패킷을 볼 수 있고, 많은 수의 패킷을 태그하는 것은 성능에 심각한 영향을 미치게 될 수도 있으므로, 네트워크 환경에 맞춰 이 설정을 조정하십시오.

표 ***207:*** 로깅 메트릭 인수

인수	설명
packets	규칙이 트리거된 후 메트릭에 의해 지정된 패킷 수를 로깅합니다.

인수	설명
seconds	규칙이 트리거된 후 메트릭에 의해 지정된 시간(초)을 로깅합니다.

예를 들어, 다음 `tag` 키워드 값을 가진 규칙이 트리거되면

```
host, 30, seconds, dst
```

다음 30초 동안 클라이언트에서 호스트로 전송된 모든 패킷이 로깅됩니다.

flowbits 키워드

`flowbits` 키워드를 사용하여 세션에 상태 이름을 지정합니다. 이전에 표시된 상태에 따라 세션의 후속 패킷을 분석함으로써, 시스템은 단일 세션에서 여러 패킷을 포함하는 공격을 탐지하고 경고할 수 있습니다.

`flowbits` 상태 이름은 세션의 특정 부분에서 패킷에 할당된 사용자가 정의한 레이블입니다. 경고하기를 원하지 않는 패킷과 악성 패킷을 구별할 수 있도록 패킷 내용에 따라 상태 이름으로 패킷을 표시할 수 있습니다. 매니지드 디바이스 당 최대 1024개의 상태 이름을 정의할 수 있습니다. 예를 들어, 성공적인 로그인 후에만 발생하는 악성 패킷을 경고하려는 경우, `flowbits` 키워드를 사용하여 초기 로그인 시도를 구성하는 패킷을 제거할 수 있으므로 악성 패킷에만 집중할 수 있습니다. 먼저 `logged_in` 상태로 설정된 로그인이 있는 세션의 모든 패킷에 표시하는 규칙을 생성한 다음 `flowbits`가 첫 번째 규칙에 설정한 상태를 가진 패킷을 확인하고 해당 패킷에만 작동하는 두 번째 규칙을 생성하여 이 작업을 수행할 수 있습니다.

선택적 그룹 이름을 사용하면 상태 그룹에 상태 이름을 포함할 수 있습니다. 상태 이름은 여러 그룹에 속할 수 있습니다. 그룹과 연관되지 않은 상태는 상호 배타적이지 않으며, 따라서 그룹과 연관되지 않은 상태를 트리거하고 설정하는 규칙은 다른 현재 설정 상태에 영향을 주지 않습니다.

flowbits 키워드 옵션

다음 표에서는 `flowbits` 키워드에서 사용할 수 있는 연산자, 상태 및 그룹의 다양한 조합에 대해 설명합니다. 상태 이름은 영숫자 문자, 점(.), 밑줄(_), 대시(-)를 포함할 수 있습니다.

표 ***208: flowbits*** 옵션

연산자	상태 옵션	그룹	설명
`set`	`state_name`	선택 사항	패킷에 대해 지정된 상태를 설정합니다. 그룹이 정의된 경우 지정된 그룹의 상태를 설정합니다.
`set`	`state_name&state_name`	선택 사항	패킷에 대해 지정된 상태를 설정합니다. 그룹이 정의된 경우 지정된 그룹의 상태를 설정합니다.
`setx`	`state_name`	필수	패킷에 대해 지정된 그룹에서 지정한 상태를 설정하고, 그룹의 다른 모든 상태를 해제합니다.
`setx`	`state_name&state_name`	필수	패킷에 대해 지정된 그룹에서 지정한 상태를 설정하고, 그룹의 다른 모든 상태를 해제합니다.

연산자	상태 옵션	그룹	설명
`unset`	`state_name`	그룹 없음	패킷에 대해 지정된 상태를 해제합니다.
`unset`	`state_name&state_name`	그룹 없음	패킷에 대해 지정된 상태를 해제합니다.
`unset`	`all`	필수	지정된 그룹의 모든 상태를 해제합니다.
`toggle`	`state_name`	그룹 없음	설정된 경우 지정된 상태를 해제하고, 해제된 경우 지정된 상태를 설정합니다.
`toggle`	`state_name&state_name`	그룹 없음	설정된 경우 지정된 상태를 해제하고, 해제된 경우 지정된 상태를 설정합니다.
`toggle`	`all`	필수	지정된 그룹에 설정된 모든 상태를 해제하고, 지정된 그룹에서 해제된 모든 상태를 설정합니다.
`isset`	`state_name`	그룹 없음	지정된 상태가 패킷에서 설정되었는지 확인합니다.
`isset`	`state_name&state_name`	그룹 없음	지정된 상태가 패킷에서 설정되었는지 확인합니다.
`isset`	`state_name|state_name`	그룹 없음	지정된 상태 중 무엇이든 패킷에서 설정되었는지 확인합니다.
`isset`	`any`	필수	어느 상태든 지정된 그룹에서 설정되었는지 확인합니다.
`isset`	`all`	필수	모든 상태가 지정된 그룹에서 설정되었는지 확인합니다.
`isnotset`	`state_name`	그룹 없음	지정된 상태가 패킷에 설정되지 않았는지 확인합니다.
`isnotset`	`state_name&state_name`	그룹 없음	지정된 상태가 패킷에 설정되지 않았는지 확인합니다.
`isnotset`	`state_name|state_name`	그룹 없음	지정된 상태 중 무엇이든 패킷에 설정되지 않았는지 확인합니다.
`isnotset`	`any`	필수	어느 상태든 패킷에 설정되지 않았는지 확인합니다.
`isnotset`	`all`	필수	모든 상태가 패킷에 설정되지 않았는지 확인합니다.
`reset`	(상태 없음)	선택 사항	모든 패킷에 대한 모든 상태를 해제합니다. 그룹이 지정된 경우 그룹의 모든 상태를 해제합니다.
`noalert`	(상태 없음)	그룹 없음	이를 이벤트 발생을 억제할 다른 모든 연산자와 함께 사용합니다.

flowbits 키워드 사용 가이드라인

flowbits 키워드를 사용할 때 다음 사항에 유의하십시오.

- setx 연산자를 사용할 때, 지정된 상태는 지정된 그룹에만 속하며, 다른 그룹에는 속할 수 없습니다.
- setx 연산자는 여러 번 정의할 수 있으며, 각 인스턴스로 다른 상태와 동일 그룹을 지정합니다.
- setx 연산자를 사용하여 그룹을 지정할 때, 지정된 해당 그룹에서 set, toggle 또는 unset 연산자를 사용할 수 없습니다.
- isset 및 isnotset 연산자는 상태가 그룹 내에 있는지 여부에 상관없이 지정된 상태를 평가합니다.
- 침입 정책이 저장하는 동안 침입 정책은 다시 적용되며 액세스 제어 정책은 적용됩니다. (액세스 제어 정책이 하나의 침입 정책 또는 여러 침입 정책을 참조하는지 여부는 상관 없습니다.) 지정된 그룹 없이 isset 또는 isnotset 연산자를 포함하는 규칙을 활성화하고, 해당하는 상태 이름 및 프로토콜에 대한 flowbits 할당(set, setx, unset, toggle)에 영향을 주는 최소 하나의 규칙을 활성화하지 않는 경우, 해당하는 상태 이름의 flowbits 할당에 영향을 미치는 모든 규칙이 활성화됩니다.
- 침입 정책을 저장하고 침입 정책을 다시 적용하고 액세스 제어 정책을 적용하는 동안(액세스 제어 정책이 침입 정책 하나를 참조하든 여러 개를 참조하든 상관없이), 지정된 그룹과 함께 isset 또는 isnotset 연산자가 포함된 규칙을 활성화하면, flowbits 할당(set, setx, unset, toggle)에 영향을 주고 해당 그룹 이름을 정의하는 모든 규칙도 활성화됩니다.

flowbits 키워드 예시

이 섹션에서는 flowbits 키워드를 사용하는 세 가지 예를 제공합니다.

flowbits 키워드 예시: state_name을 사용한 설정

이것은 state_name을 사용한 flowbits 구성의 예입니다.

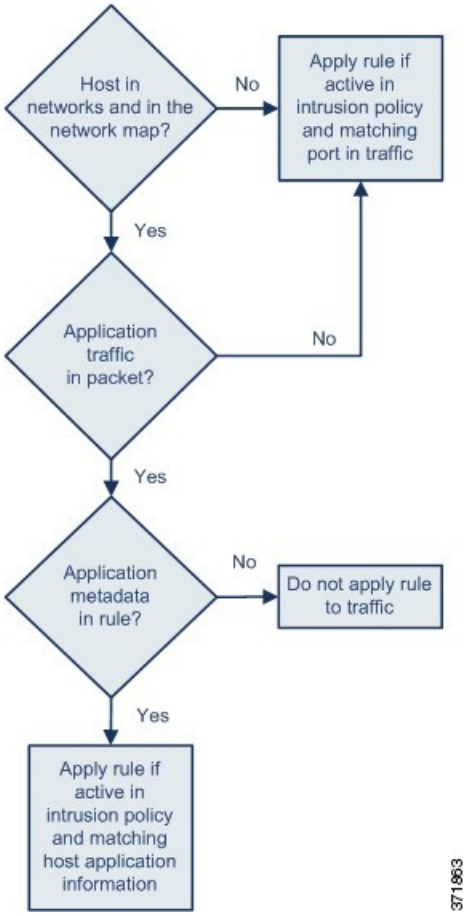
CVE ID 2000-0284에 설명된 IMAP 취약성을 고려하십시오. 이러한 취약성은 IMAP 구현에서 존재하는데, 특히 LIST, LSUB, RENAME, FIND 및 COPY 명령에 존재합니다. 그러나, 취약성을 사용하려면 공격자는 IMAP 서버에 로그인해야 합니다. IMAP 서버로부터의 LOGIN 확인 및 이를 따르는 익스플로잇은 서로 다른 패킷에 있어야 하므로 이러한 익스플로잇을 포착하는 비 플로우 기반(non-flow-based) 규칙을 작성하기는 어렵습니다. flowbits 키워드를 사용하여 사용자가 IMAP 서버에 로그인되어 있는지 여부를 추적하는 일련의 규칙을 구성할 수 있으며, 로그인되어 있는 경우, 공격 중 하나가 탐지되면 이벤트를 생성할 수 있습니다. 사용자가 로그인되어 있지 않은 경우, 공격은 취약성을 사용할 수 없고 어떤 이벤트도 생성되지 않습니다.

다음 두 가지 규칙 조각이 이 예를 보여줍니다. 첫 번째 규칙 조각은 IMAP 서버에서 IMAP 로그인 인증을 검색합니다.

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK

LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.



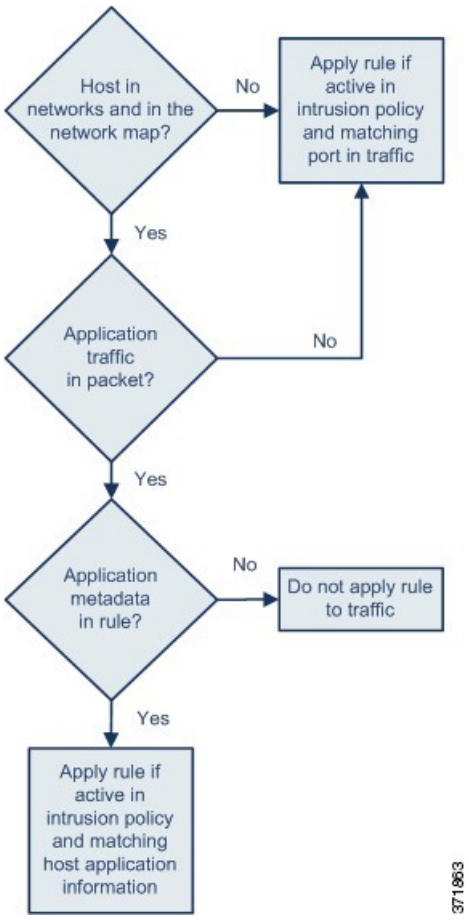
IMAP 서버에서 여러 무해한 로그인 세션을 볼 가능성이 크기 때문에 `flowbits:set`는 `logged_in`의 상태를 설정하는 반면, `flowbits:noalert`는 경고를 억제한다는 점에 유의하십시오.

logged_in 상태가 세션에서 일부의 이전 패킷의 결과로 설정되어 있지 않는 한 다음 규칙 조각은 LIST 문자열을 검색하지만 이벤트를 생성하지 않습니다:

```
alert tcp any any -> any 143 (msg:"IMAP LIST";

content:"LIST"; flowbits:isset,logged_in;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.



이 경우, 이전 패킷이 첫 번째 조각을 포함하는 규칙을 트리거하도록 야기하는 경우, 두 번째 조각을 포함하는 규칙이 트리거되고 이벤트를 생성합니다.

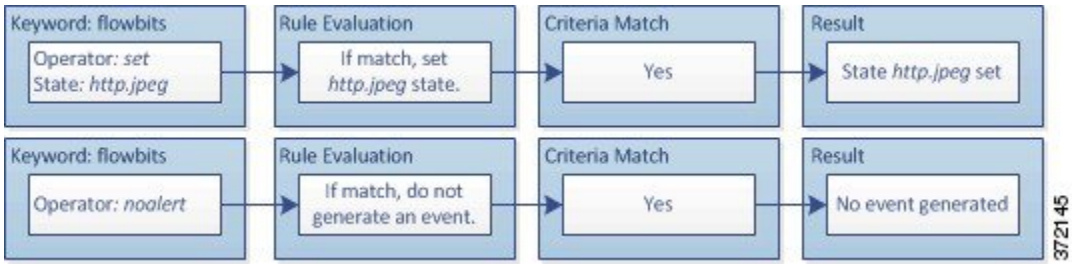
flowbits 키워드 예시: 오탐 이벤트의 설정 결과

그룹의 다양한 규칙에 설정된 여러 상태 이름을 포함하는 것은 뒤따르는 패킷의 콘텐츠가 더 이상 유효하지 않은 상태의 규칙에 일치할 때 발생할 가능성이 있는 잘못된 긍정 이벤트를 방지할 수 있습니다. 다음의 예제는 그룹의 여러 상태 이름을 포함하지 않을 때 잘못된 긍정을 얻을 수 있는 방법에 대해 설명합니다.

여기서 단일 세션 동안 표시된 다음 세 가지 규칙 조각이 순서대로 트리거하는 케이스를 고려해 보십시오.

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:set,http.jpeg; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

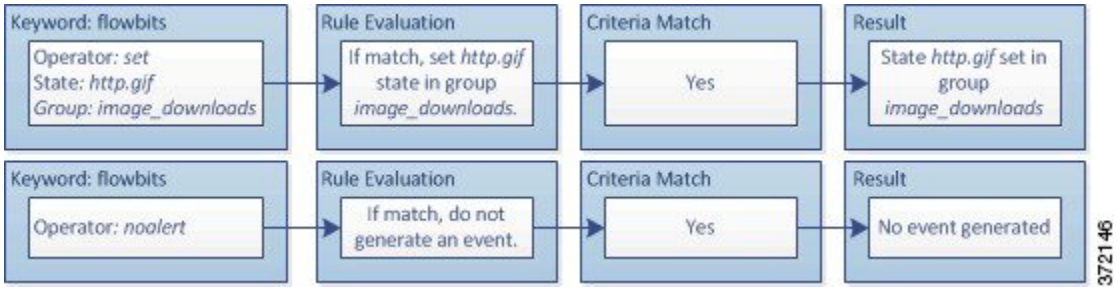


첫 번째 규칙 프래그먼트의 `content` 및 `pcre` 키워드는 JPEG 파일 다운로드를 매칭하고, `flowbits:set,http.jpeg`는 `http.jpeg flowbits` 상태를 설정하며, `flowbits:noalert`는 규칙의 이벤트 생성을 중지합니다. 규칙의 목적은 파일 다운로드를 탐지하고 `flowbits` 상태를 설정하는 것이며 하나 이상의 동반 규칙이 악성 콘텐츠와 조합된 상태 이름을 테스트하여 악성 콘텐츠가 탐지되면 이벤트를 생성할 수 있도록 하는 것이므로 어떤 이벤트도 생성되지 않습니다.

다음 규칙 조각은 위의 JPEG 파일 다운로드 다음에 일어나는 GIF 파일 다운로드를 탐지합니다.

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:set,http.jpg,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

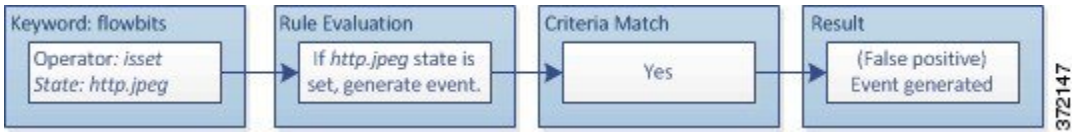


두 번째 규칙의 `content` 및 `pcre` 키워드는 GIF 파일 다운로드를 매칭하고, `flowbits:set,http.tif`는 `http.tif flowbits` 상태를 설정하며, `flowbits:noalert`는 규칙의 이벤트 생성을 중지합니다. 첫 번째 규칙 조각에 의해 설정된 `http.jpeg` 상태는 더 이상 필요 없더라도 여전히 설정되어 있다는 점에 유의하십시오. 이는 후속 GIF 다운로드가 발견되는 경우 JPEG 다운로드가 반드시 완료되어 있어야 하기 때문입니다.

세 번째 규칙 조각은 첫 번째 규칙 조각에 사용됩니다.

```
(msg:"JPEG exploit";?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"?/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.



세 번째 규칙 프래그먼트에서 `flowbits:isset,http.jpeg`는 이제 관련이 없는 `http.jpeg` 상태가 설정되었는지, 그리고 `content` 및 `pcre`가 JPEG 파일에서는 악성이지만 GIF 파일에서는 악성이 아닌 내용

과 일치하는지를 확인합니다. 세 번째 규칙 조각은 JPEG 파일에는 없는 공격을 위한 잘못된 긍정 이벤트로 귀결됩니다.

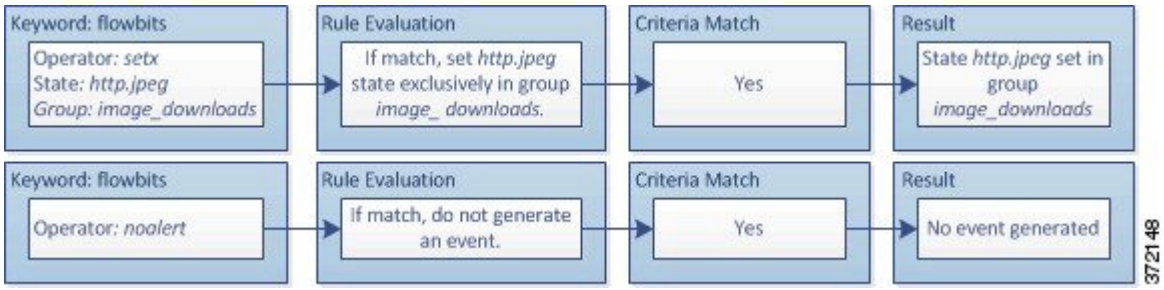
flowbits 키워드 예시: 오탐 이벤트 방지 설정

다음의 예시는 그룹에 상태 이름을 포함하고 `setx` 연산자를 사용하여 잘못된 긍정을 차단할 수 있는 방법에 대해 설명합니다.

이전 예와 동일한 경우를 고려하십시오. 이제는 동일한 상태 그룹에서 자신의 두 가지 상태 이름을 포함하는 처음 두 개의 규칙은 제외합니다.

```
(msg:"JPEG transfer";
content:"image/";pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
?flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

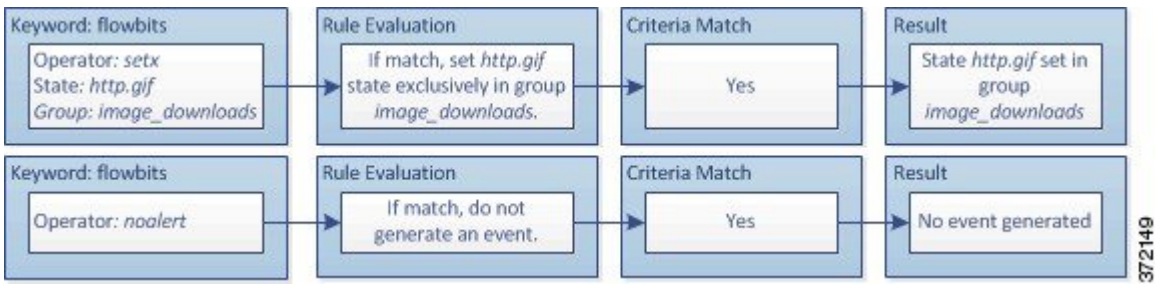


첫 번째 규칙 조각이 JPEG 파일 다운로드를 탐지하면, `flowbits:setx,http.jpeg,image_downloads` 키워드는 `flowbits` 상태를 `http.jpeg`로 설정하고 `image_downloads` 그룹의 상태를 포함합니다.

다음 규칙은 후속 GIF 파일 다운로드를 탐지합니다.

```
(msg:"GIF transfer"; content:"image/";
pcre:"/^Content-?Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
?flowbits:setx,http.jpg,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

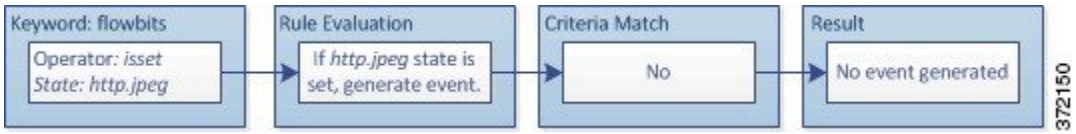


두 번째 규칙 프래그먼트가 GIF 다운로드와 일치하면 `flowbits:setx,http.tif,image_downloads` 키워드는 `http.jpg flowbits` 상태를 설정하고 그룹의 다른 상태인 `http.jpeg`를 설정 취소합니다.

세 번째 규칙 조각이 잘못된 긍정으로 귀결되지 않습니다.

```
(msg:"JPEG exploit"; ?flowbits:isset,http.jpeg;content:"|FF|";
pcre:"/?\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.



`flowbits:isset,http.jpeg`가 거짓이므로, 규칙 엔진은 규칙 처리를 중지하고 어떤 이벤트도 생성되지 않으며, 따라서 GIF 파일 내 콘텐츠가 JPEG 파일에 대한 공격 콘텐츠에 일치하는 경우에도 잘못된 긍정이 차단됩니다.

http_encode 키워드

`http_encode` 키워드를 사용하여 표준화 전에 HTTP 요청 또는 응답의 인코딩 유형에서 이벤트를 생성할 수 있습니다. HTTP URI, HTTP 헤더의 비쿠키 데이터, HTTP 요청 헤더의 쿠키 또는 HTTP 응답의 set-cookie 데이터 중 하나에서 가능합니다.

`http_encode` 키워드를 사용하여 규칙에 대한 일치 항목을 반환하는 HTTP 응답 및 HTTP 쿠키를 검사하는 HTTP Inspect(HTTP 검사) 전처리기를 구성해야 합니다.

또한 HTTP Inspect(HTTP 검사) 전처리기 구성에서 각 특정 인코딩 유형의 디코딩 및 알림 옵션을 활성화해야 침입 규칙의 `http_encode` 키워드가 해당 인코딩 유형에서 이벤트를 트리거할 수 있습니다.

다음 표에서는 이 옵션이 HTTP URI, 헤더, 쿠키 및 set-cookie에서 이벤트를 생성할 수 있는 인코딩 유형을 설명합니다.

표 ***209: http_encode*** 인코딩 유형

인코딩 유형	설명
utf8	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 UTF - 8 인코딩을 탐지합니다.
double_encode	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 이중 인코딩을 탐지합니다.
non_ascii	비ASCII 문자가 검색되었지만 탐지된 인코딩 유형이 활성화되지 않은 경우 지정된 위치에서 비ASCII 문자를 탐지합니다.
uencode	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 Microsoft %u 인코딩을 탐지합니다.
bare_byte	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 베어 바이트 인코딩을 탐지합니다.

관련 항목

HTTP 검사 전처리기, 2252 페이지
서버 레벨 HTTP 정상화 옵션, 2254 페이지

http_encode 키워드 구문

인코딩 위치

HTTP URI, 헤더 또는 집합 쿠키를 포함하는 쿠키에서 지정된 인코딩 유형을 검색할지 여부를 지정합니다.

인코딩 유형

다음 형식 중 하나를 사용하여 하나 이상의 인코딩 유형을 지정합니다.

```
encode_type
encode_type|encode_type|encode_type...
```

여기서 `encode_type`은 다음 중 하나입니다.

```
utf8
double_encode
non_ascii
uencode
bare_byte.
```

부정 연산자(!)와 OR 연산자(|)를 함께 사용할 수 없음에 유의하십시오.

http_encode 키워드 예시: 2개의 http_endcode 키워드를 사용하여 2개의 인코딩 검색

다음 예는 같은 규칙에서 2개의 `http_encode` 키워드를 사용하여 HTTP URI에서 UTF-8 AND Microsoft IIS %u 인코딩을 검색합니다.

첫 번째, `http_encode` 키워드:

- **Encoding Location(**인코딩 위치**)**: `HTTP URI`
- **Encoding Type(**인코딩 유형**)**: `utf8`

그런 다음 추가적인 `http_encode` 키워드:

- **Encoding Location(**인코딩 위치**)**: `HTTP URI`
- **Encoding Type(**인코딩 유형**)**: `uencode`

개요: file_type 및 file_group 키워드

`file_type` 및 `file_group` 키워드를 사용하면 FTP, HTTP, SMTP, IMAP, POP3, 그리고 해당 유형 및 버전에 따라 NetBIOS ssn(SMB)을 통해 전송되는 파일을 탐지할 수 있습니다. 단일 침입 규칙에서 하나 이상의 `file_type` 또는 `file_group` 키워드를 사용하지 마십시오.

팁 VDB(취약성 데이터베이스)를 업데이트하면 침입 규칙 편집기가 최신 파일 형식, 버전 및 그룹으로 채워집니다.

참고 시스템은 file_type 및 file_group 키워드를 수용하기 위해 전처리기를 자동으로 활성화하지 않습니다.

file_type 또는 file_group 키워드와 일치하는 트래픽에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.을 위해서는 특정 전처리기를 활성화해야 합니다.

표 ***210: file_type*** 및 ***file_group*** 침입 이벤트 생성

프로토콜	필수 전처리기 또는 전처리기 옵션
FTP	FTP/텔넷 전처리기 및 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 인라인 표준화 전처리기 옵션
HTTP	HTTP 트래픽에서 침입 이벤트를 생성하기 위한 HTTP 검사 전처리기
SMTP	HTTP 트래픽에서 침입 이벤트를 생성하기 위한 SMTP 전처리기
IMAP	IMAP 전처리기
POP3	POP 전처리기
Netbios-ssn(SMB)	DCE/RPC 전처리기 및 **SMB File Inspection(SMB** 파일 검사**)** DCE/RPC 전처리기 옵션

관련 항목

FTP/텔넷 디코더, 2244 페이지
인라인 정상화 전처리기, 2317 페이지
HTTP 검사 전처리기, 2252 페이지
SMTP 전처리기, 2283 페이지
IMAP 전처리기, 2277 페이지
POP 전처리기, 2280 페이지
DCE/RPC 전처리기, 2228 페이지

file_type 및 file_group 키워드

file_type

file_type 키워드를 사용하면 트래픽에서 탐지된 파일의 파일 유형 및 버전을 지정할 수 있습니다. 파일 유형 인수(예를 들어, **JPEG** 및 **PDF**)는 트래픽에서 찾을 파일의 형식을 식별합니다.

참고 file_type 키워드를 동일한 침입 규칙의 또 다른 file_type 또는 file_group 키워드와 사용해서는 안 됩니다.

시스템은 기본적으로 **Any Version(**모든 버전**)**을 선택하지만, 일부 파일 유형을 사용하면 트래픽에서 찾을 특정 파일 유형 버전을 식별할 수 있도록 버전 옵션을 선택할 수 있습니다(예를 들어, PDF 버전 **1.7**).

file_group

`file_group` 키워드를 사용하면 트래픽에서 Cisco가 정의한 비슷한 파일 유형 그룹을 선택할 수 있습니다(예를 들어 멀티미디어 또는 오디오). 파일 그룹은 또한 그룹 내 각 파일 유형에 대해 Cisco가 정의한 버전을 포함합니다.

참고 `file_group` 키워드를 동일한 침입 규칙의 또 다른 `file_group` 또는 `file_type` 키워드와 사용해서는 안 됩니다.

file_data 키워드

`file_data` 키워드는 `content`, `byte_jump`, `byte_test` 및 `pcre`와 같은 다른 키워드에 대해 사용 가능한 위치 인수를 위한 참고 사항으로 기능하는 포인터를 제공합니다. 탐지된 트래픽은 `file_data` 키워드가 나타내는 데이터 유형을 확인합니다. `file_data` 키워드를 사용하여 다음 페이로드 유형의 시작을 가리킬 수 있습니다.

- HTTP 응답 본문

  HTTP 응답 패킷을 검사하려면, HTTP Inspect(HTTP 검사) 전처리기를 활성화해야 하고 HTTP 응답을 검사하는 전처리기를 구성해야 합니다. HTTP Inspect(HTTP 검사) 전처리기가 HTTP 응답 본문 데이터를 탐지할 경우 `file_data` 키워드가 일치됩니다.

- 미압축 gzip 파일 데이터

  HTTP 응답 본문에서 압축되지 않은 gzip 파일을 검사하려면 HTTP Inspect(HTTP 검사) 전처리기를 활성화해야 하며, HTTP 응답을 검사하고 HTTP 응답 본문의 gzip 압축 파일을 압축 해제하도록 전처리기를 구성해야 합니다. 자세한 내용은 **Inspect HTTP Responses(HTTP** 응답 검사**)**와 **Inspect Compressed Data(**압축 데이터 검사**)** Server-Level HTTP Normalization(서버 수준 HTTP 표준화) 옵션을 참고하십시오. HTTP Inspect(HTTP 검사) 전처리기가 HTTP 응답 본문 내 미압축 gzip 데이터를 탐지할 경우 `file_data` 키워드가 일치됩니다.

- 표준화된 Javascript

  표준화된 Javascript 데이터를 검사하려면, HTTP Inspect(HTTP 검사) 전처리기를 활성화해야 하고 HTTP 응답을 검사하는 전처리기를 구성해야 합니다. HTTP Inspect(HTTP 검사) 전처리기가 HTTP 응답 본문 데이터 내 Javascript를 탐지할 경우 `file_data` 키워드가 일치됩니다.

- SMTP 페이로드

  SMTP 페이로드를 검사하려면, SMTP 전처리기를 활성화해야 합니다. `file_data` 키워드는 SMTP 프리프로세서가 SMTP 데이터를 탐지하는지 여부를 매칭합니다.

- SMTP, POP 또는 IMAP 트래픽의 인코딩된 이메일 첨부 파일

SMTP, POP 또는 IMAP 트래픽의 인코딩된 이메일 첨부 파일을 검사하려면 SMTP, POP 또는 IMAP 전처리기를 각각 활성화해야 하며 단독으로 또는 조합하여 활성화합니다. 다음, 각 활성화된 전처리기를 위해, 해독할 각 첨부 파일 인코딩 유형을 디코딩하기 위해 전처리기가 구성되어 있는지 확인해야 합니다. 사용자가 각 전처리기에 대해 구성할 수 있는 첨부 파일 디코딩 옵션은 다음과 같습니다: **Base64 Decoding Depth(**베이스**64** 디코딩 수준**)**, **7-Bit/8-Bit/Binary Decoding Depth(7**비트**/8**비트/이진 디코딩 수준**)**, **Quoted-Printable Decoding Depth(**발췌되어 인쇄 가능한 디코딩 수준**)** 그리고 **Unix-to-Unix Decoding Depth(**유닉스 투 유닉스 디코딩 수준**)**.

규칙에서 여러 `file_data` 키워드를 사용할 수 있습니다.

관련 항목

HTTP 검사 전처리기, 2252 페이지
서버 레벨 HTTP 정상화 옵션, 2254 페이지
SMTP 전처리기, 2283 페이지
IMAP 전처리기, 2277 페이지

pkt_data 키워드

`pkt_data` 키워드는 `content`, `byte_jump`, `byte_test` 및 `pcre`와 같은 다른 키워드에 대해 사용 가능한 위치 인수를 위한 참고 사항으로 기능하는 포인터를 제공합니다.

표준화된 FTP, 텔넷 또는 SMTP 트래픽이 발견되면, `pkt_data` 키워드는 표준화된 패킷 페이로드의 시작을 나타냅니다. 다른 트래픽이 발견되면 `pkt_data` 키워드는 원시 TCP 또는 UDP 페이로드의 시작을 나타냅니다.

다음 표준화 옵션은 시스템이 침입 규칙에 의한 검사를 위해 해당 트래픽을 표준화할 수 있도록 활성화되어야 합니다.

- 검사할 FTP 트래픽을 표준화하려면 FTP 및 텔넷 전처리기 **Detect Telnet Escape codes within FTP commands(FTP** 명령 내에서 텔넷 이스케이프 코드 탐지**)**를 활성화합니다.
- 검사할 텔넷 트래픽을 표준화하려면 FTP 및 텔넷 전처리기 **Normalize(**표준화**)** 텔넷 옵션을 활성화합니다.
- 검사할 SMTP 트래픽을 표준화하려면 SMTP 전처리기 **Normalize(**표준화**)** 옵션을 활성합니다.

규칙에서 여러 `pkt_data` 키워드를 사용할 수 있습니다.

관련 항목

클라이언트 레벨 FTP 옵션, 2249 페이지
텔넷 옵션, 2244 페이지
SMTP 전처리기 옵션, 2284 페이지

base64_decode 및 base64_data 키워드

`base64_decode` 및 `base64_data` 키워드를 함께 사용하여 규칙 엔진이 Base64 데이터로 지정된 데이터를 해독하고 검사하도록 지시할 수 있습니다. 이 방법은 예를 들면 HTTP PUT 및 POST 요청에서

Base64로 인코딩된 HTTP 인증 요청 헤더 및 Base64로 인코딩된 데이터를 검사하는 경우 유용할 수 있습니다.

이 키워드는 특히 HTTP 요청의 Base64 데이터를 해독하고 검사하는 데 유용합니다. 그러나, 또한 이 키워드를 여러 행 위의 길이가 긴 헤더 행을 확장하기 위해 HTTP가 스페이스 및 탭 문자를 사용하는 것과 같은 방식으로 이 문자를 사용하는 SMTP와 같은 모든 프로토콜과 함께 사용할 수 있습니다. 폴딩으로 알려진 이와 같은 행 확장이 이를 사용하는 프로토콜에 나타나지 않는 경우, 검사는 스페이스 또는 탭이 뒤따르지 않는 모든 복귀 또는 라인 피드에서 끝납니다.

base64_decode

`base64_decode` 키워드는 규칙 엔진이 패킷 데이터를 Base64 데이터로 해독하도록 지시합니다. 선택적 인수는 디코딩할 바이트 수와 디코딩을 시작할 데이터 내 위치를 지정하도록 합니다.

규칙에서 `base64_decode` 키워드를 한 번 사용할 수 있습니다. 이는 최소한 `base64_data` 키워드의 인스턴스 하나를 선행해야 합니다.

Base64 데이터를 해독하기 전에, 규칙 엔진은 여러 행을 가로질러 접힌 긴 헤더를 펼칩니다. 규칙 엔진에 다음이 발생할 때 디코딩은 종료됩니다.

- 헤더 행 끝
- 디코딩할 지정된 바이트 수
- 패킷 종료

다음 표에서는 `base64_decode` 키워드와 함께 사용할 수 있는 인수를 설명합니다.

표 ***211:*** 선택적 ***base64_*** 디코딩 인수

인수	설명
바이트	디코딩할 바이트 수를 지정합니다. 지정되지 않은 경우, 디코딩은 헤더 행 끝 또는 패킷 페이로드의 끝 중 먼저 오는 것까지 계속합니다. 0이 아닌 양수 값을 지정할 수 있습니다.
Offset	패킷 페이로드의 처음을 기준으로, 또는 **Relative**를 지정한 경우 현재 검사 위치를 기준으로 오프셋을 결정합니다. 0이 아닌 양수 값을 지정할 수 있습니다.
Relative	현재 검사 위치에 관련된 검사를 지정합니다.

base64_data

`base64_data` 키워드는 `base64_decode` 키워드를 사용하여 디코딩된 Base64 데이터 검사를 위한 참고 자료를 제공합니다. `base64_data` 키워드는 디코딩된 Base64 데이터 시작 시 검사가 시작되도록 설정합니다. 선택적으로, 검사할 위치를 추가로 지정하려면 `content` 또는 `byte_test`와 같은 기타 키워드에서 사용 가능한 위치 인수를 사용할 수 있습니다.

`base64_decode` 키워드를 사용한 후 `base64_data` 키워드를 최소한 한 번 사용해야 합니다. 선택적으로, `base64_data`를 여러 번 사용하여 디코딩된 Base64 데이터의 시작 부분으로 돌아갈 수 있습니다.

Base64 데이터를 검사할 때 다음에 유의하십시오.

- 빠른 패턴 매처를 사용할 수 없습니다.
- 개입하는 HTTP 콘텐츠 인수로 규칙에서 Base64 검사를 중지하는 경우, Base64 데이터의 상세 검사 전에 규칙에 다른 `base64_data` 키워드를 삽입해야 합니다.

관련 항목

개요: HTTP content 및 protected_content 키워드 인수, 2094 페이지
content 키워드 빠른 패턴 매처 인수, 2098 페이지

86 장

침입 방지 성능 조정

다음 주제에서는 침입 방지 성능을 개선하는 방법을 설명합니다.

- 침입 방지 성능 조정 정보, 2185 페이지
- 침입 방지 성능 조정 라이선스 요건, 2186 페이지
- 침입 방지 성능 조정 요구 사항 및 사전 요건, 2186 페이지
- 침입에 대한 패턴 일치 제한, 2186 페이지
- 침입 규칙용 정규식 제한 재정의, 2187 페이지
- 침입 규칙용 정규식 제한 재정의, 2188 페이지
- 패킷 침입당 이벤트 생성 제한, 2189 페이지
- 패킷당 생성되는 침입 이벤트 제한, 2189 페이지
- 패킷 및 침입 규칙 레이턴시 임계값 구성, 2190 페이지
- 침입 성능 통계 로깅 구성, 2196 페이지
- 침입 성능 통계 로깅 구성, 2197 페이지

침입 방지 성능 조정 정보

Cisco는 시스템이 시도된 침입의 트래픽을 분석할 때 시스템의 성능을 향상시키는 여러 기능을 제공합니다. 다음 작업을 수행할 수 있습니다.

- 이벤트 대기열에서 허용할 패킷의 수를 지정할 수 있습니다. 또한, 스트림 리어셈블리 전후에, 대형 스트림으로 재구축되는 패킷에 대한 검사를 활성화 또는 비활성화할 수 있습니다.
- 침입 규칙에서 사용되는 PCRE에 대한 기본 일치 및 재귀 한도를 재정의하여 패킷 페이로드 콘텐츠를 검사할 수 있습니다.
- 여러 이벤트가 생성될 때 규칙 엔진이 패킷 또는 패킷 스트림당 둘 이상의 이벤트를 로깅하도록 하여 보고된 이벤트 이상의 정보를 수집할 수 있습니다.
- 패킷 및 규칙 레이턴시 임계값으로 보안과 디바이스 레이턴시 유지 필요성 사이의 균형을 적절한 수준으로 유지할 수 있습니다.
- 디바이스가 자체 성능을 모니터링하고 보고하는 방법에 대한 기본 매개변수를 구성할 수 있습니다. 이를 통해 시스템이 디바이스에서 성능 통계를 업데이트하는 간격을 지정할 수 있습니다.

사용자는 액세스 제어 정책을 기반으로 한 성능 설정을 구성하고, 해당 상위 액세스 제어 정책에 의해 호출된 모든 침입 정책에 적용합니다.

침입 방지 성능 조정 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

침입 방지 성능 조정 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

침입에 대한 패턴 일치 제한

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Performance Settings(**성능 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Performance Settings(**성능 설정**)** 팝업 창에서 **Pattern Matching Limits(**패턴 일치 제한**)**를 클릭합니다.

단계 **4** **Maximum Pattern States to Analyze Per Packet(**패킷당 분석할 최대 패턴 상태**)** 필드에 대기열에 넣을 이벤트의 최대 수 값을 입력합니다.

단계 **5** 스트림 리어셈블리 전후에 대규모 데이터 스트림으로 재구축되는 패킷 검사를 비활성화하려면 **Disable Content Checks on Traffic Subject to Future Reassembly(**향후 리어셈블리 대상이 되는 트래픽에 대해 콘텐츠 확인 비활성화**)** 확인란을 선택합니다. 리어셈블리 전후의 검사에는 추가 프로세싱 오버헤드가 필요하므로 성능이 저하될 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

침입 규칙용 정규식 제한 재정의

기본 정규 표현식 제한은 최소 수준의 성능을 보장합니다. 이러한 제한을 재정의하면 보안을 강화할 수 있지만, 비효율 정규식에 대한 패킷 평가를 허용함으로써 성능에 중대한 영향을 미칠 수 있습니다.

⚠

주의 손상 패턴의 영향에 대한 지식이 있는 숙련된 침입 규칙 작성가가 아닌 이상 기본 PCRE 제한값을 재정의하지 마십시오.

표 ***212:*** 정규식 제약 조건 옵션

옵션	설명
일치 제한 상태	**Match Limit(**일치 제한**)** 재정의 여부를 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Match Limit(**일치 제한**)**에 대해 구성된 값을 사용하려면 **Default(**기본값**)**를 선택합니다. • 무제한 시도를 허용하려면 **Unlimited(**무제한**)**를 선택합니다. • **Custom**을 선택하여 **Match Limit**의 제한값을 1 이상으로 지정하거나, 0으로 지정하여 PCRE 매치 평가를 완전히 비활성화합니다.
일치 제한	PCRE 정규식에 정의된 패턴에 일치시키려는 시도의 횟수를 지정합니다.

옵션	설명
일치 반복 제한 상태	**Match Recursion Limit(**일치 반복 제한**)** 재정의 여부를 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Default**를 선택하여 **Match Recursion Limit**에 구성된 값을 사용합니다. • 무제한 반복을 허용하려면 **Unlimited(**무제한**)**를 선택합니다. • **Custom**을 선택하여 **Match Recursion Limit**의 제한값을 1 이상으로 지정하거나, 0으로 지정하여 PCRE 억제를 완전히 비활성화합니다. **Match Recursion Limit(**일치 반복 제한**)**가 작동하려면 반드시 **Match Limit(**일치 제한**)**보다 작아야 함을 참고하시기 바랍니다.
일치 반복 제한	패킷 페이로드에 대한 PCRE 정규식을 평가할 때 반복 수를 지정합니다.

관련 항목

개요: pcre 키워드, 2109 페이지

침입 규칙용 정규식 제한 재정의

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Performance Settings(**성능 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Performance Settings(**성능 설정**)** 팝업 창에서 **Regular Expression Limits(**정규 표현식 제한**)**을 클릭합니다.

단계 **4** 침입 규칙용 정규식 제한 재정의, 2187 페이지에서 설명한 모든 옵션을 수정할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

패킷 침입당 이벤트 생성 제한

침입 규칙 엔진은 규칙에 대한 트래픽을 평가할 때 주어진 패킷 또는 패킷 스트림에 대해 생성된 이벤트를 이벤트 대기열에 배치한 다음 대기열의 상위 이벤트를 사용자 인터페이스에 보고합니다. 침입 이벤트 로깅 제한을 구성할 때 대기열에 배치하고 로깅할 이벤트 수를 지정하고 대기열의 이벤트 순서를 결정할 기준을 선택할 수 있습니다.

표 ***213:*** 침입 이벤트 로깅 제한 옵션

옵션	설명
패킷당 저장된 최대 이벤트	주어진 패킷 또는 패킷 스트림에 대해 저장될 수 있는 최대 이벤트 수
패킷당 로깅된 최대 이벤트	주어진 패킷 또는 패킷 스트림에 대해 로깅될 수 있는 최대 이벤트 수. 이는 **Maximum Events Stored Per Packet(**패킷당 저장된 최대 이벤트**)** 값을 초과할 수 없습니다.
이벤트 로깅 우선 순위 지정 기준	이벤트 큐 내 이벤트 순서를 결정하는 데 사용되는 값. 최고 순위 이벤트는 사용자 인터페이스를 통해 보고됩니다. 사용자는 다음에서 선택할 수 있습니다. • `priority`. 이벤트 우선 순위에 따라 해당 큐에서 이벤트 순서를 결정하는 것. • `content_length`. 가장 긴 것으로 확인된 콘텐츠 일치에 따라 이벤트 순서를 결정하는 것. 이벤트가 콘텐츠 길이에 의해 순서가 정해질 때, 규칙 이벤트는 항상 디코더 및 전처리기 이벤트에 우선합니다.

패킷당 생성되는 침입 이벤트 제한

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Performance Settings(**성능 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Performance Settings(**성능 설정**)** 팝업 창에서 **Intrusion Event Logging Limits(**침입 이벤트 로깅 제한**)** 탭을 클릭합니다.

단계 **4** 패킷 침입당 이벤트 생성 제한, 2189 페이지의 모든 옵션을 수정할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

패킷 및 침입 규칙 레이턴시 임계값 구성

각 액세스 제어 정책은 지연 기반 설정으로 임계값을 사용해 패킷과 규칙 처리 성능을 관리합니다.

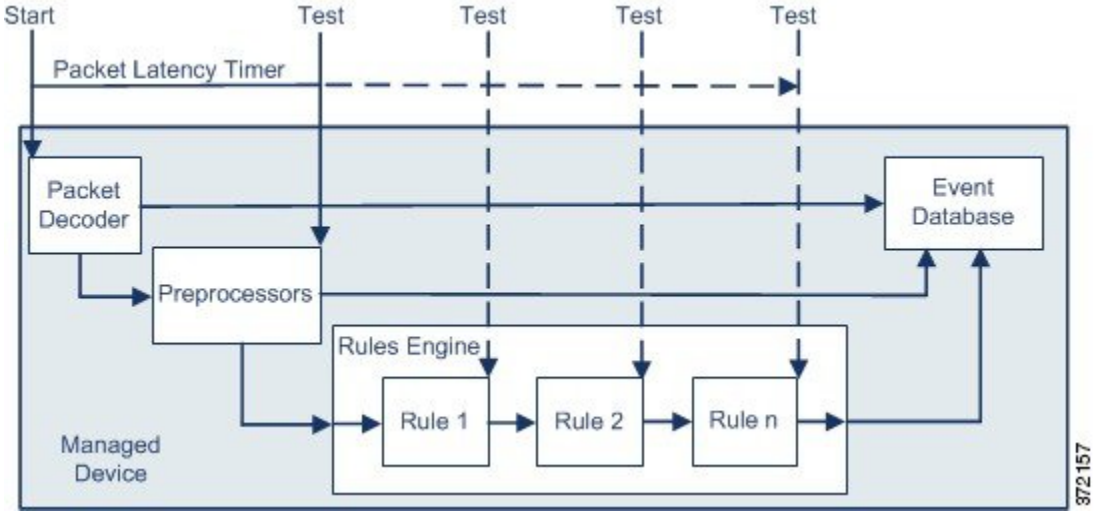
패킷 레이턴시 임계값은 처리 시간이 구성 가능한 임계값을 초과하는 경우 적용 가능한 디코더, 전처리기 및 규칙에 의해 패킷을 처리하는 데 드는 총 소요 시간을 측정합니다.

규칙 레이턴시 임계값은 각 규칙에서 개별 패킷을 처리하는 데 걸리는 시간을 측정하고, 처리 시간이 규칙 레이턴시 임계값(구성 가능한 연속 횟수)을 넘을 경우 위반 규칙 및 지정된 시간에 대한 관련 규칙 그룹을 동시에 중단하며, 일시 중단이 만료되면 해당 규칙을 복원합니다.

패킷 레이턴시 임계값

패킷 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반 레이턴시 구현입니다.

레이턴시 임계값에서 파생된 레이턴시 이점과 성능의 반대 급부는 검사하지 않은 패킷에 공격이 포함될 수 있다는 점입니다. 디코더가 프로세스를 시작할 때 각 패킷의 타이머가 시작됩니다. 타이밍은 패킷의 모든 처리가 종료되거나, 처리 시간이 타이밍 테스트 지점의 임계값을 초과할 때까지 계속됩니다.



위 그림에 표시된 것처럼, 패킷 레이턴시 타이밍은 다음과 같은 테스트 지점에서 테스트됩니다.

- 모든 디코더 및 전처리기의 처리가 완료된 이후 및 규칙 처리가 시작되기 이전
- 각 규칙에 따라 처리된 이후

처리 시간이 테스트 지점의 임계값을 초과할 경우, 패킷 검사가 중단됩니다.

팁 루틴 TCP 스트림 또는 IP 조각 리어셈블리 시간은 총 패킷 처리 시간에 포함되지 않습니다.

패킷 레이턴시 임계값은 디코더, 전처리기 또는 패킷 처리 규칙에 의해 시작된 이벤트에 대해서는 영향을 미치지 않습니다. 적용 가능한 디코더, 전처리기 또는 규칙은 보통 패킷이 완전히 처리될 때까지, 또는 레이턴시 임계값이 초과하여 패킷 처리가 끝날 때까지, 어느 쪽이든 먼저 될 때까지 작동합니다. 삭제 규칙이 인라인 배포에서 침입을 탐지하는 경우, 삭제 규칙은 이벤트를 시작하며 패킷은 삭제됩니다.

참고 패킷 레이턴시 임계값 위반으로 인해 해당 패킷 처리가 끝난 후 규칙에 반하여 평가되는 패킷은 없습니다. 이벤트를 시작했을 수도 있는 규칙은 해당 이벤트를 시작할 수 없으며, 삭제 규칙을 위해 패킷을 삭제할 수 없습니다.

패킷 레이턴시 임계값을 사용하면 과도한 처리 시간이 요구되는 패킷 검사를 중단함으로써 패시브 및 인라인 구축 시 시스템 성능을 향상하고, 인라인 구축 시 레이턴시를 줄일 수 있습니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 패시브 및 인라인 배포에서 과도한 시간을 들여 여러 규칙별 패킷 검사를 순차적으로 수행하는 경우
- 인라인 배포에서 네트워크 성능이 저하된 경우(예: 누군가 대용량 파일을 다운로드하여 패킷 처리 속도가 느려짐)

수동 배포에서 패킷의 처리를 중지하면 처리는 다음 패킷으로 간단하게 옮겨가므로 네트워크 성능 복구에 도움이 되지 않을 수도 있습니다.

패킷 레이턴시 임계값 참고 사항

기본적으로 패킷 처리에 대한 레이턴시 기반 성능 설정은 비활성화됩니다. 원한다면 활성화할 수도 있습니다. 그러나 Cisco에서는 임계값 설정 기본값 변경을 권장하지 않습니다.

아래 항목의 정보는 맞춤형 값을 지정하도록 선택하는 경우에만 적용됩니다.

표 ***214:*** 패킷 레이턴시 임계값 옵션

옵션	설명
임계값(마이크로초)	패킷의 검사가 중지될 때, 마이크로초로 시간을 지정합니다.

패킷 레이턴시 임계값 활성화

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 팝업 창에서 **Packet Handling(**패킷 처리**)**을 클릭합니다.

단계 **4** **Enable(**활성화**)** 확인란을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

패킷 레이턴시 임계값 구성

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 옆에 있는 수정( )을 클릭합니다.

System(시스템**)** > **Monitoring(**모니터링**)** > **Statistics(**통계**)**

단계 **3** 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **4** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 팝업 창에서 **Packet Handling(**패킷 처리**)**을 클릭합니다.

단계 **5** 맞춤형 값을 지정하려면

- **Enabled(**활성화**)** 확인란을 선택하고, 패킷 레이턴시 임계값 참고 사항, 2192 페이지에서 권장 최소 **Threshold(**임계값**)** 설정을 확인합니다.
- 패킷 처리 탭과 규칙 처리 탭 둘 다에서 맞춤형 값을 지정해야 합니다.

단계 **6** 권장 최소 임계값 설정은 패킷 레이턴시 임계값 참고 사항, 2192 페이지를 참조하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

Rule Latency Thresholding

규칙 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반 레이턴시 구현입니다.

레이턴시 임계값에서 파생된 레이턴시 이점과 성능의 반대 급부는 검사하지 않은 패킷에 공격이 포함될 수 있다는 점입니다. 타이머는 패킷이 규칙 그룹에 대해 처리될 때마다 처리 시간을 측정합니다. 규칙 처리 시간이 지정된 규칙 레이턴시 임계값을 초과하는 모든 경우, 시스템은 계수기를 증대합니다. 후속 임계값 위반 수가 지정된 수에 도달하는 경우, 시스템은 다음 작업을 수행합니다.

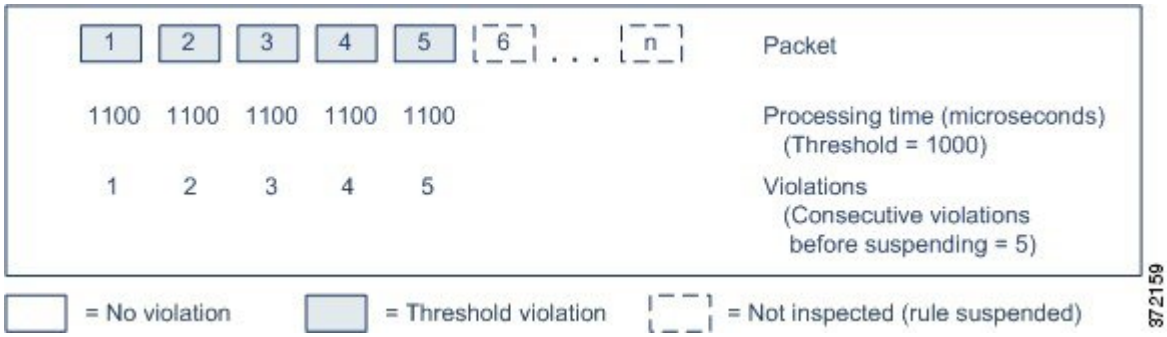
- 지정된 기간 동안 규칙을 중지합니다.
- 규칙이 중지되었음을 나타내는 이벤트를 시작합니다.
- 중지가 만료되면 규칙을 재활성화합니다.
- 규칙이 재활성화되었음을 나타내는 이벤트를 시작합니다.

그룹 규칙이 중지되거나 규칙 위반이 연속적이지 않은 경우 시스템은 계수기를 0에 맞춥니다. 규칙을 중지하기 전에 여러 개의 연속되는 위반을 허용하면 사용자는 가끔 일어나는 규칙 위반, 즉 성능에 미치는 영향이 무시할 만한 수준인 위반을 무시해버리고 사용자는 규칙 레이턴시 임계값을 반복적으로 초과하는 규칙에 미치는 더욱 중대한 영향력에 집중하게 됩니다.

다음의 예시는 규칙 중단으로 귀결되지 않는 다섯 가지의 연속 규칙 처리 시간을 보여줍니다.

위 예시에서, 처음 3개 패킷의 각각을 처리하는 데 필요한 시간은 1000마이크로초의 규칙 레이턴시 임계값을 위반하며, 각 위반과 함께 위반 계수기도 증대됩니다. 네 번째 패킷 처리는 임계값을 위반하지 않으며, 위반 계수기는 0으로 재설정됩니다. 다섯 번째 패킷은 임계값을 위반하며, 위반 계수기는 1에서 다시 시작합니다.

다음의 예시는 규칙 중단으로 귀결되는 다섯 가지의 연속 규칙 처리 시간을 보여줍니다.



두 번째 예에서, 다섯 개의 패킷 중 각각을 처리하는 데 필요한 시간은 1000마이크로초의 규칙 레이턴시 임계값을 위반합니다. 규칙 그룹은 각 패킷에 대한 1100마이크로초의 규칙 처리 시간이 명시된 5회 연속 위반 기간 동안 1000마이크로초의 임계값을 초과하므로 중지됩니다. 패킷 6 또는 그보다 큰 수(n)로 표시된 모든 후속 패킷은 중지가 만료될 때까지 중지된 규칙에 반해 검토되지 않습니다. 규칙이 재활성화된 후에 추가 패킷이 발생하는 경우, 위반 계수기는 0에서 다시 시작됩니다.

규칙 레이턴시 임계값은 패킷을 처리하는 규칙에 의해 시작된 침입 이벤트에는 어떤 영향도 미치지 않습니다. 규칙은 규칙 처리 시간이 임계값을 초과하는지 여부에 상관없이 패킷에서 탐지된 모든 침입에 대한 이벤트를 시작합니다. 침입을 탐지하는 규칙이 인라인 배포에서 삭제 규칙인 경우, 패킷은 삭제됩니다. 삭제 규칙이 패킷에서 규칙 중단으로 귀결되는 침입을 탐지하는 경우, 삭제 규칙은 침입 이벤트를 시작하고, 패킷은 삭제되며, 해당 규칙 및 모든 관련 규칙은 중지됩니다.

참고 패킷은 중단된 규칙에 반해 평가되지 않습니다. 이벤트를 시작했을 수도 있는 중지된 규칙은 해당 이벤트를 시작할 수 없으며, 삭제 규칙을 위해 패킷을 삭제할 수 없습니다.

규칙 레이턴시 임계값을 사용하면 대부분의 패킷 처리 시간을 관장하는 규칙을 중지함으로써 수동 배포 및 인라인 배포에 있어 시스템 성능을 향상하고, 인라인 배포 시 레이턴시를 줄일 수 있습니다. 패킷은 과부하된 디바이스에 복원할 수 있는 시간을 제공하면서 구성 가능한 시간이 만료될 때까지

중지된 규칙에 반해 다시 평가되지 않습니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 급히 쓰여진, 대개 테스트되지 않는 규칙에 과도한 양의 처리 시간이 필요한 경우
- 네트워크 성능이 저하된 경우(예: 누군가 대용량 파일을 다운로드하여 패킷 검사 속도가 느려짐)

규칙 레이턴시 임계값 참고

규칙 레이턴시 임계값은 시간 규칙이 **Consecutive Threshold Violations Before Suspending Rule(**규칙 중지 전 연속 임계값 위반**)**에 지정된 연속된 횟수 동안 **Threshold(**임계값**)**를 초과하는 패킷을 처리하기 시작할 때 **Suspension Time(**중지 시간**)**에 지정된 시간 동안 규칙을 중지합니다.

규칙이 중지되었을 때 규칙 134:1을 활성화하여 이벤트를 생성할 수 있고, 중지된 규칙이 활성화되었을 때는 규칙 134:2를 활성화하여 이벤트를 생성할 수 있습니다. 침입 규칙 상태 옵션, 2024 페이지의 내용을 참조하십시오.

표 ***215:*** 규칙 레이턴시 임계값 옵션

옵션	설명
임계값	패킷을 검토할 때 규칙이 초과해서는 안 되는 시간을 마이크로초로 지정합니다.
규칙 중지 전 연속 임계값 위반	**Threshold**에 대해 지정된 시간보다 오래 소요될 수 있는 연속 시간 횟수를 지정하여 규칙이 중단되기 전에 패킷을 검사할 수 있도록 합니다.
중단 시간	규칙 그룹을 중지하려면 초 단위 시간을 지정합니다.

규칙 레이턴시 임계값 구성

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 팝업 윈도우에서 **Rule Handling(**규칙 처리**)**를 선택합니다.

단계 **4** 규칙 레이턴시 임계값 참고, 2195 페이지에 있는 모든 옵션을 설정할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 이벤트를 생성하고 싶다면 레이턴시 규칙 134:1 및 134:2를 활성화합니다. 자세한 내용은 침입 규칙 상태 옵션, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

침입 성능 통계 로깅 구성

시간(초) 샘플링 및 패킷 수 최소화

성능 통계량 업데이트 사이에 지정된 시간(초)이 소요된 경우, 시스템은 패킷의 지정된 수를 분석했는지 확인합니다. 확인된 경우, 시스템은 성능 통계량을 업데이트합니다. 그렇지 않은 경우, 시스템은 패킷의 지정된 수를 분석할 때까지 기다립니다.

문제 해결 옵션: 로그 세션/프로토콜 배포

지원팀은 문제 해결 통화 중 사용자에게 프로토콜 배포, 패킷 길이 및 포트 통계량을 로깅할 것을 요청할 수 있습니다.

주의 지원팀이 지시할 때만 **Log Session/Protocol Distribution(**로그 세션/프로토콜 배포**)**을 활성화하십시오.

문제 해결 옵션: 요약

문제 해결 통화 중에 지원팀에서 Snort® 프로세스가 종료되거나 다시 시작된 경우에만 성능 통계를 계산하도록 시스템을 구성하라고 요청할 수 있습니다. 이 옵션을 활성화하려면, 또한 반드시 **Log Session/Protocol Distribution(**로그 세션/프로토콜 배포**)** 옵션을 선택합니다.

주의 지원팀이 지시할 때만 **Summary(**요약**)**를 활성화하십시오.

침입 성능 통계 로깅 구성

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭한 다음 **Performance Settings(**성능 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 표시되는 팝업 윈도우에서 **Performance Statistics(**성능 통계**)**를 클릭합니다.

단계 **3** 위에 설명된 대로 **Sample time(**샘플 시간**)** 또는 **Minimum number of packets(**패킷 최소 수**)**를 수정합니다.

단계 **4** 지원팀의 요청이 있는 경우에만 선택적으로, **Troubleshoot Options(**문제 해결 옵션**)** 섹션을 확장하고 해당 옵션을 수정합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

XIX 부

고급 네트워크 분석 및 전처리

- 네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정, 2201 페이지
- 네트워크 분석 정책 시작하기, 2209 페이지
- 애플리케이션 레이어 프리프로세서, 2227 페이지
- SCADA 프리프로세서, 2299 페이지
- 전송 및 네트워크 계층 전처리기, 2311 페이지
- 특정 위협 탐지, 2349 페이지
- 적응형 프로파일, 2371 페이지

87 장

네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정

다음 주제에서는 네트워크 분석 및 침입 정책에 대한 고급 설정 구성 방법을 설명합니다.

- 네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정 정보, 2201 페이지
- 네트워크 분석 및 침입 정책에 대한 고급 액세스 제어 설정 요구 사항 및 사전 요건, 2201 페이지
- 트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지
- 네트워크 분석 정책 고급 설정, 2203 페이지

네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정 정보

액세스 제어 정책의 고급 설정 대부분은 구성을 위한 특정 전문성을 요구하는 침입 탐지 및 방지 구성을 제어합니다. 고급 설정은 일반적으로 거의 또는 전혀 수정할 필요가 없으며 모든 배포에 공통적으로 적용하지는 않습니다.

네트워크 분석 및 침입 정책에 대한 고급 액세스 제어 설정 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

트래픽이 식별되기 전에 통과하는 패킷 검사

URL 필터링, 애플리케이션 탐지, 및 지능형 애플리케이션 우회를 비롯한 일부 기능의 경우, 연결을 설정하고 시스템에서 트래픽을 식별하고 어떤 액세스 제어 규칙(있을 경우)이 해당 트래픽을 처리할지 결정할 수 있도록 하려면 몇 개의 패킷이 통과해야 합니다.

액세스 제어 정책을 명시적으로 설정하여 이러한 패킷을 검사하고 패킷이 대상에 도달하는 것을 방지하고 이벤트를 생성해야 합니다. 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정, 2203 페이지의 내용을 참조하십시오.

시스템이 액세스 제어 규칙 또는 연결을 처리해야 하는 기본 작업을 확인하면, 연결의 나머지 패킷이 처리되고 그에 따라 검사됩니다.

트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례

- 액세스 제어 정책에 대해 지정된 기본 작업은 이러한 패킷에 적용되지 않습니다.
- 대신 다음 지침을 사용하여 액세스 제어 정책의 고급 설정에서 액세스 제어 규칙이 결정되기 전에 사용되는 침입 정책의 값을 선택합니다.
  - 시스템에서 생성한 정책 또는 맞춤형 침입 정책을 선택할 수 있습니다. 예를 들어 **Balanced Security and Connectivity(**균형 잡힌 보안 및 연결**)**를 선택할 수 있습니다.
  - 성능상의 이유로 특별한 이유가 없는 한 이 설정은 액세스 제어 정책에 대해 설정된 기본 작업과 일치해야 합니다.
  - 시스템이 침입 검사를 수행하지 않는 경우(예: 검색 전용 구축) **No Rules Active(**활성 규칙 없음**)**를 선택합니다. 시스템은 이러한 초기 패킷을 검사하지 않으며 통과할 수 있습니다.
  - 기본적으로 이 설정은 기본 변수 집합을 사용합니다. 이것이 용도에 적합한지 확인하십시오. 자세한 내용은 변수 집합, 580 페이지를 참조하십시오.
  - 처음으로 일치하는 네트워크 분석 규칙과 관련된 네트워크 분석 정책은 사용자가 선택하는 정책에 대한 트래픽을 사전 처리합니다. No 네트워크 분석 규칙 또는 none (없음)가 일치, 경우 기본 네트워크 분석 정책에 사용 됩니다.

트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정

참고 이 설정을 기본 침입 정책이라고도 합니다. (액세스 제어 정책에 대한 기본 작업과는 다릅니다.)

시작하기 전에

이러한 설정에 대한 모범 사례를 검토합니다. 트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례, 2202 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 **Network Analysis(**네트워크 분석**)**및 **Intrusion Policies(**침입 정책**)** 섹션 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** **Intrusion Policy used before Access Control rule is determined(**액세스 컨트롤 규칙이 결정되기 전에 사용된 침입 정책**)** 드롭다운 목록에서 침입 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, 수정( )을 클릭하여 새 창에서 정책을 편집할 수 있습니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 **3** **Intrusion Policy Variable Set(**침입 정책 변수 집합**)** 드롭다운 목록에서 다른 변수 집합을 선택하는 방법도 있습니다. 또는 변수 집합 옆에 있는 수정( )을 선택하여 변수 집합을 생성하고 편집해도 됩니다. 사용자가 변수 집합을 변경하지 않는 경우, 시스템은 기본 집합을 사용합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

변수 집합, 580 페이지

네트워크 분석 정책 고급 설정

네트워크 분석 정책은 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽을 향후에 평가할 수 있도록 트래픽을 해독하고 전처리하는 방법을 제어합니다. 이러한 트래픽 전처리는 보안 인텔리전스 매칭

및 트래픽 해독이 수행된 후 하지만 침입 정책이 패킷을 세부적으로 검사하기 전에 이루어집니다. 기본적으로, 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본 네트워크 정책이 됩니다.

팁 시스템이 제공하는 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트할 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다.

전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다. 복합적인 배포를 사용하는 고급 사용자의 경우, 다수의 네트워크 분석 정책을 생성할 수 있는데, 각각은 트래픽을 다르게 전처리하기 위해 조정된 것입니다. 그런 다음 이러한 정책을 사용하도록 시스템을 구성하여 서로 다른 보안 영역, 네트워크 또는 VLAN을 사용하는 트래픽의 전처리를 제어할 수 있습니다

이를 수행하려면, 액세스 제어 정책에 사용자 지정 네트워크 분석 규칙을 추가합니다. 네트워크 분석 규칙은 해당 자격과 일치하는 트래픽을 어떻게 전처리할지 단순히 지정한 일련의 구성과 조건입니다. 사용자는 기존의 액세스 제어 정책의 고급 옵션에서 네트워크 분석 규칙을 만들고 수정합니다. 각 규칙은 하나의 정책에만 속합니다.

각 규칙에는 다음이 포함되어 있습니다.

- 전처리하려는 특정 트래픽을 확인하는 일련의 규칙 조건
- 모든 규칙의 조건을 충족하는 트래픽을 전처리하는 데 사용하려는 결합된 네트워크 분석 정책

시스템이 트래픽을 전처리할 시간이 되면, 큰 규칙 번호에서 작은 번호 순서로 패킷을 네트워크 분석 규칙에 일치시킵니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.

기본 네트워크 분석 정책 설정

시스템에서 생성된 정책 또는 사용자가 생성한 정책을 선택할 수 있습니다.

참고 전처리기를 비활성화했지만 시스템이 활성화된 침입 또는 전처리기 규칙에 대해 전처리한 패킷을 평가해야 하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 비활성화 상태로 남아 있는 상태라 해도 시스템은 전처리기를 자동으로 활성화하여 사용합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 반드시 주의하여 서로 보완하는 단일 패킷을 검토하는 네트워크 분석 및 침입 정책을 허용해야 합니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** **Default Network Analysis Policy(**기본 네트워크 분석 정책**)** 드롭다운 목록에서 기본 네트워크 분석 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, 수정( )을 클릭하여 새 창에서 정책을 편집할 수 있습니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

사용자 지정 정책의 한계, 1971 페이지

네트워크 분석 규칙

액세스 제어 정책의 고급 설정에서, 네트워크 분석 규칙을 사용하여 네트워크 트래픽에 대한 전처리 구성을 맞춤화할 수 있습니다.

네트워크 분석 규칙은 1부터 번호가 지정됩니다. 시스템이 트래픽을 전처리할 시간이 되면, 오름차순 규칙 번호가 적어지는 순서로 패킷을 네트워크 분석 규칙에 일치시키며, 모든 규칙의 조건이 일치하는 첫 번째 규칙에 따라 트래픽을 전처리합니다.

규칙에 영역, 네트워크 및 VLAN 태그 조건을 추가할 수 있습니다. 규칙에 대해 특정 조건을 구성하지 않으면 시스템은 해당 기준에 따라 트래픽을 매칭하지 않습니다. 예를 들어, 네트워크 조건은 있지만 영역 조건이 없는 규칙의 경우 인그레스 또는 이그레스 인터페이스에 상관없이 소스 또는 대상 IP 주소에 따라 트래픽을 평가합니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.

네트워크 분석 규칙 설정

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

팁 **Network Analysis Policy List(**네트워크 분석 정책 목록**)**를 클릭해 기존 맞춤형 네트워크 분석 정책을 확인하고 편집합니다.

단계 **2** **Network Analysis Rules(**네트워크 분석 규칙**)** 옆에 있는 보유하고 있는 사용자 지정 규칙의 수를 표시하는 문장을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **4** 추가할 조건을 클릭해 규칙 조건을 설정합니다. 규칙 조건 유형, 525 페이지을 참조하십시오.

단계 **5** **Network Analysis(**네트워크 분석**)**을 클릭하고 이 규칙과 일치하는 트래픽을 전처리하는 데 사용할 **Network Analysis Policy(**네트워크 분석 정책**)**를 선택합니다.

수정( )을 클릭해 새 창에서 맞춤형 정책을 편집합니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 분석 규칙 관리

네트워크 분석 규칙은 해당 자격과 일치하는 트래픽을 어떻게 전처리할지 단순히 지정한 일련의 구성과 조건입니다. 사용자는 기존의 액세스 제어 정책의 고급 옵션에서 네트워크 분석 규칙을 만들고 수정합니다. 각 규칙은 하나의 정책에만 속합니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Advanced(**고급**)**을 클릭하고 Intrusion and Network Analysis Policies(침입 및 네트워크 분석 정책) 섹션 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** **Network Analysis Rules(**네트워크 분석 규칙**)** 옆에 있는 보유하고 있는 사용자 지정 규칙의 수를 표시하는 문장을 클릭합니다.

단계 **3** 사용자 지정 규칙을 수정합니다. 다음 옵션을 이용할 수 있습니다.

- 규칙 조건을 수정하거나 규칙에 의해 호출된 네트워크 분석 정책을 변경하기 위해서는 규칙 옆에 있는 수정( )을 클릭합니다.
- 규칙의 평가 순서를 변경하려면, 정확한 위치에 규칙을 클릭하여 끌어옵니다. 여러 규칙을 선택하려면 Shift와 Ctrl 키를 사용합니다.
- 규칙을 삭제하려면 규칙 옆에 있는 삭제( )을 클릭합니다.

팁 마우스 오른쪽 버튼으로 규칙을 클릭하면 새로운 네트워크 분석 규칙을 잘라내기, 복사, 붙여넣기, 편집, 삭제, 추가할 수 있는 콘텍스트 메뉴가 표시됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

88 장

네트워크 분석 정책 시작하기

다음 주제에서는 네트워크 분석 정책을 바탕으로 시작하는 방법을 설명합니다.

- 네트워크 분석 정책 기본 사항, 2209 페이지
- 네트워크 분석 정책에 대한 라이선스 요건, 2210 페이지
- 네트워크 분석 정책 요구 사항 및 사전 요건, 2210 페이지
- 네트워크 분석 정책 관리, 2210 페이지

네트워크 분석 정책 기본 사항

네트워크 분석 정책은 많은 트래픽 전처리 옵션을 관리하며, 액세스 제어 정책의 고급 설정에 의해 호출됩니다. 네트워크 분석 관련 전처리는 보안 인텔리전스 매칭 및 SSL 암호 해독 후, 그리고 액세스 제어 규칙이 패킷을 자세히 조사하기 전과 모든 침입 또는 파일 검사가 시작되기 전에 수행됩니다.

기본적으로, 시스템은 *Balanced Security and Connectivity(*균형 잡힌 보안 및 연결성*)* 네트워크 분석 정책을 사용하여 액세스 제어 정책에서 처리된 모든 트래픽을 전처리합니다. 그러나, 사용자는 이 전처리를 수행하는 기타 기본 네트워크 분석 정책을 선택할 수 있습니다. 사용자 편의를 위해, 시스템은 Cisco Talos Intelligence Group(Talos)이(가) 보안 및 연결의 특정 균형을 위해 조정한 변경할 수 없는 여러 네트워크 분석 정책 선택권을 제공합니다. 또한 맞춤형 전처리 설정이 있는 맞춤형 네트워크 분석 정책을 만들 수도 있습니다.

팁 시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다. 네트워크 분석 및 칩임 정책은 함께 작동해 트래픽을 검색합니다.

또한 여러 맞춤형 네트워크 분석 정책을 작성한 다음, 다른 트래픽을 전처리하도록 할당하여 특정 보안 영역, 네트워크 및 VLAN에 맞게 트래픽 전처리 옵션을 조정할 수도 있습니다. (ASA FirePOWER은 VLAN에 의한 전처리를 제한할 수 없는 점에 유의하십시오.)

네트워크 분석 정책에 대한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

네트워크 분석 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

네트워크 분석 정책 관리

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 네트워크 분석 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교, 514 페이지를 참조하십시오.
- Create(생성) - 새 네트워크 분석 정책을 생성하려면 **Create Policy(**정책 생성**)**를 클릭하고 Snort 2에 대한 맞춤형 네트워크 분석 정책 생성, 2220 페이지에서 설명하는 지침을 따릅니다.
- Delete(삭제) - 네트워크 분석 정책을 삭제하려면 삭제( )를 클릭하고 정책 삭제 여부를 확인합니다. 액세스 제어 정책이 네트워크 분석 정책을 참조하는 경우 이를 삭제할 수 없습니다.

  컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.
- Edit(편집) - 기존 네트워크 분석 정책을 편집하려면 수정( )을 클릭하고 네트워크 분석 정책 설정 및 캐시된 변경 사항, 2221 페이지에서 설명하는 지침을 따릅니다.

  보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 보고서 - 보고서( )을(를) 클릭합니다. 현재 정책 보고서 생성, 515 페이지의 내용을 참조하십시오.

Snort 3에 대한 맞춤형 네트워크 분석 정책 생성

기본 네트워크 분석 정책은 일반적인 네트워크 요구 사항 및 최적의 성능에 맞게 조정됩니다. 일반적으로 기본 네트워크 분석 정책은 대부분의 네트워크 요구 사항을 충족하므로 정책을 사용자 정의하지 않아도됩니다. 그러나 특정 네트워크 요구 사항이 있거나 성능 문제가 발생할 경우 기본 네트워크 분석 정책을 사용자 지정할 수 있습니다. 네트워크 분석 정책을 사용자 정의하는 것은 고급 사용자 또는 Cisco 지원만 수행해야 하는 고급 구성입니다.

Snort 3에서는 Snort 2보다 많은 수의 검사기(Snort 2의 전 처리기) 및 설정을 사용하여 기본 네트워크 분석 정책을 사용자 정의할 수 있습니다. 검사기 및 설정 수가 증가함에 따라 Snort 3의 네트워크 분석 정책을 더 잘 사용자 정의하고 네트워크 요구 사항에 맞게 성능을 조정하여 원하는 결과를 제공할 수 있습니다.

Snort 3 규칙 검사기는 규칙 및 설정이 구성되고 파일이 FMC에 업로드되는 JSON 파일입니다. JSON 편집기를 사용하여 사용자 정의 규칙을 작성하거나 기존 규칙을 재정의할 수 있습니다. 그러나 이러한 재정의는 여러 요인에 대해 스키마 파일에 의해 검증되며, 값이 합법적이거나 허용되는 범위 내에 있는 경우에만 파일을 FMC에 업로드할 수 있습니다. 또한 재정의를 추적하고 재정의를 기본값으로 쉽게 되돌릴 수 있습니다.

참고

- FMC를 7.0 릴리스로 업그레이드하는 동안 네트워크 분석 정책의 Snort 2 버전에서 수행된 변경 사항은 업그레이드 후에 Snort 3으로 마이그레이션되지 않습니다.
- 또한 침입 정책과 달리 Snort 2에 있던 변경 사항을 동기화하는 옵션은 네트워크 분석 정책에 사용할 수 없습니다. 그러나 네트워크 분석 정책을 수정하면 Snort 2 버전과 Snort 3 버전 모두에 업데이트가 적용됩니다.
- 네트워크 분석 정책의 Snort 2 버전은 업데이트되지 않으며 그대로 유지됩니다.

검사기 업데이트

Snort에서 새 검사기를 도입할 때마다 새 검사기는 일주일에 두 번 릴리스되는 LSP(Lightweight Security Package)의 일부로 포함됩니다. 또한 Snort가 기존 검사기 구성의 정수 범위를 수정하는 경우 LSP를 통해 업데이트된 정수 범위를 사용할 수 있습니다. LSP를 설치하고 나면 네트워크 분석 정책의 **Snort 3** 버전에서 **Inspector(**검사기**)** 아래에 새 검사기 및 업데이트된 범위를 사용할 수 있습니다.

바인더 검사기

바인더 검사기는 특정 검사기가 액세스하여 고려해야 하는 경우 흐름을 정의합니다. 트래픽이 바인더 검사기에 정의된 조건과 일치하면 해당 검사기의 값/구성만 적용됩니다.

예**: 1:**

dns 검사기의 경우, 바인더는 액세스해야 하는 다음 조건을 정의합니다. 조건:

- 포트가 53과 같습니다.
- 프로토콜이 *udp*와 같습니다.
- 역할이 서버와 같습니다.

이러한 조건이 충족되면 *dns* 유형을 사용합니다.

binder

Default Configuration (Maximum Detection)

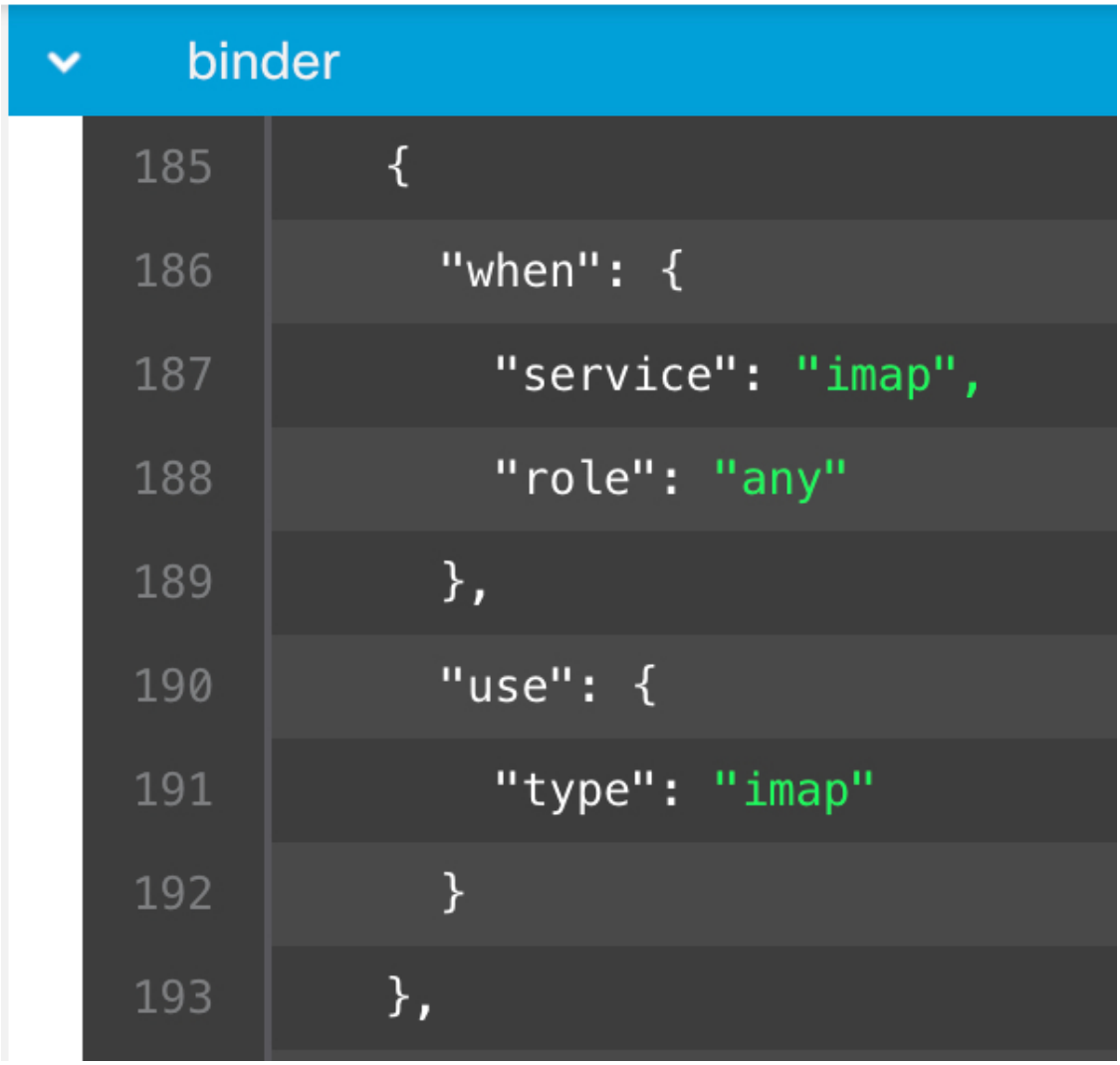
```
{
  "enabled": true,
  "type": "binder",
  "rules": [
    {
      "when": {
        "ports": "53",
        "proto": "udp",
        "role": "server"
      },
      "use": {
        "type": "dns"
      }
    },
```

예: 2:

imap 검사기의 경우 바인더는 액세스할 때 다음 조건을 정의합니다. 조건:

- 서비스가 imap와 같습니다.
- 역할이 any와 같습니다.

이러한 조건이 충족되면 imap 유형을 사용합니다.



싱글톤 검사기

싱글톤 검사기는 인스턴스를 포함하지 않습니다.

멀티톤 검사기

멀티톤 검사기에는 필요에 따라 구성할 수 있는 여러 인스턴스가 포함되어 있습니다. 멀티톤 검사기의 경우 재정의된 검사기 구성을 업로드할 때 JSON 파일의 각 인스턴스에 대해 일치하는 바인더 조건(검사기가 액세스 또는 사용되어야 하는 조건)도 포함/정의해야 합니다. 그렇지 않으면 업로드 오

류가 발생합니다. 새 인스턴스를 생성할 수도 있지만 오류를 방지하기 위해 생성하는 모든 새 인스턴스에 대해 바인더 조건을 포함해야 합니다.

네트워크 분석 정책 매핑

네트워크 분석 정책의 경우 Cisco Talos는 Snort 3 버전에 해당하는 Snort 2 버전의 정책을 찾는 데 사용되는 매핑 정보를 제공합니다.

이 매핑을 통해 Snort 3 버전의 정책이 동일한 Snort 2 버전을 사용할 수 있습니다. 그러나 이를 위해서는 몇 가지 고려 사항이 있을 수 있습니다. 예를 들어,

- Snort 2 버전과 Snort 3 버전 간의 정확한 규칙 매핑
- 하나의 Snort 2 규칙이 둘 이상의 Snort 3 규칙으로 분할될 수 있습니다.
- 둘 이상의 Snort 2 규칙을 하나의 Snort 3 규칙으로 변환할 수 있음

참고 일부 Snort 2 규칙은 Snort 3에 없을 수 있습니다. 이러한 경우 해당 규칙 재정의는 마이그레이션되지 않습니다.

네트워크 분석 정책 매핑 보기

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **NAP Mapping(NAP** 매핑**)**을 클릭합니다.

단계 **3** **View Mappings(**매핑 보기**)**의 화살표를 확장합니다.

Snort 2에 해당하는 정책에 자동으로 매핑되는 Snort 3 네트워크 분석 정책이 표시됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

네트워크 분석 정책 생성

기존의 모든 네트워크 분석 정책은 해당 Snort 2 및 Snort 3 버전과 함께 FMC에서 사용할 수 있습니다. 새 네트워크 분석 정책을 생성하면 Snort 2 버전 및 Snort 3 버전으로 생성됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Base Policy(**기본 정책**)**을 선택하고 **Save(**저장**)**를 클릭합니다.

새 네트워크 분석 정책을 생성하면 해당하는 **Snort 2** 버전 및 **Snort 3** 버전으로 생성됩니다.

네트워크 분석 정책 수정

네트워크 분석 정책을 수정하여 이름, 설명 또는 기본 정책을 변경할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.
단계 **2** **Edit(**편집**)**을 클릭하여 이름, 설명 또는 기본 정책을 변경합니다.
단계 **3** **Save(**저장**)**를 클릭합니다.

네트워크 분석 정책 사용자 정의

요구 사항에 따라 네트워크 분석 정책의 Snort 3 버전을 사용자 정의할 수 있습니다.

프로시저

단계 **1** 네트워크 분석 정책을 사용자 정의하려면 **Snort 3** 버전을 클릭합니다.
단계 **2** 다음에서 필요한 모드를 선택합니다.

- 방지
- 탐지

단계 **3** **Inspectors(**검사기**)**에서 기본 설정을 재정의할 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

검색 창에 관련 텍스트를 입력하여 검사기를 검색해야 할 수 있습니다.

단계 **4** **Settings(**설정**)** 버튼(오른쪽의 기어 아이콘)을 클릭합니다.

다음 옵션이 표시됩니다.

- 다운로드
  - Schema(스키마)
  - 샘플 파일/템플릿
  - 전체 설정
  - 재정의된 설정

- 업로드
  - 재정의된 설정

단계 **5** **Download(**다운로드**)**에서 다음 옵션을 사용하여 필요에 따라 스키마 파일, 샘플 파일, 전체 구성 또는 재정의된 구성을 다운로드할 수 있습니다.

이러한 옵션은 허용되는 값, 범위 및 패턴, 기존 및 기본 검사기 구성, 재정의된 검사기 구성에 대한 통찰력을 제공합니다.

a) **Schema(**스키마**)**를 클릭하여 스키마 파일을 다운로드합니다.

스키마 파일은 업로드하거나 다운로드하는 콘텐츠를 검증합니다. 스키마 파일을 다운로드하여 서드 파티 JSON 편집기를 사용하여 열 수 있습니다. 스키마 파일은 사용할 수 있는 허용되는 값, 범위 및 허용되는 패턴을 사용하여 검사기에 대해 구성할 수 있는 매개 변수를 식별하는 데 도움이 됩니다.

예를 들어 *arp_spoof_snort* 검사기의 경우 호스트를 구성할 수 있습니다. 호스트에는 *mac* 및 *ip* 주소 값이 포함됩니다. 스키마 파일에는 이러한 값에 대해 다음과 같은 허용 패턴이 표시됩니다.

- **mac** – 패턴**:** `^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **ip** – 패턴**:**
  `^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}(/[0-9]{1,2}){0,1})$`

검사기 구성을 성공적으로 재정의하려면 스키마 파일의 허용되는 패턴에 따라 값, 범위, 패턴을 제공해야합니다. 그렇지 않으면 오류 메시지가 표시됩니다.

b) **Sample File / Template(**샘플 파일 / 템플릿**)**을 클릭하여 예제 구성이 포함된 기존 템플릿을 사용하여 검사기를 구성하는 데 도움이 됩니다.

샘플 파일에 포함된 예제 구성을 참조하여 필요에 따라 변경할 수 있습니다.

c) 전체 검사기 구성을 단일 파일로 다운로드하려면 **Full Configuration(**전체 구성**)**을 클릭합니다.

따라서 검사기를 개별적으로 확장하는 대신 전체 구성을 다운로드하여 필요한 정보를 찾을 수 있습니다. 검사기 구성과 관련된 모든 정보를 이 파일에서 사용할 수 있습니다.

d) **Overrideden Configuration(**재정의된 구성**)**을 클릭하여 재정의된 관리자 구성을 다운로드합니다.

검사기 구성을 재정의하지 않은 경우 이 옵션은 비활성화됩니다. 검사기 구성을 재정의하면 이 옵션이 자동으로 활성화되어 다운로드할 수 있습니다.

단계 **6** 기존 구성을 재정의하려면

a) **Inspectors(**검사기**)**에서 기본 구성을 재정의할 필수 검사기를 확장합니다.

기본 구성이 왼쪽 열에 표시됩니다.

b) 기본 검사기 구성으로 JSON 파일을 생성합니다.

필요에 따라 **Sample File / Template(**샘플 파일 / 템플릿**)**을 사용할 수도 있습니다.

c) 필요에 따라 검사기 구성을 변경합니다.

변경 사항을 검증하고 스키마 파일을 준수하는지 확인합니다. 멀티톤 검사기의 경우 모든 인스턴스의 바인딩 조건이 JSON 파일에 포함되어 있는지 확인합니다. 자세한 내용은 멀티톤 검사기를 참조하십시오.

d) 재정의된 구성 파일을 시스템에 저장합니다.

단계 **7** **Upload(**업로드**)**에서 **Overrideden Configuration(**재정의된 구성**)**을 클릭하여 재정의된 구성이 포함된 JSON 파일을 업로드할 수 있습니다.

파일을 끌어다 놓거나 클릭하여 시스템에 저장된 재정의된 검사기 구성이 포함된 JSON 파일을 찾아볼 수 있습니다.

주의 재정의된 구성 파일을 업로드하면 현재 정책의 검사기를 덮어쓰며 되돌릴 수 없습니다. 구성을 재정의하기 전에 정보에 입각한 결정을 내리십시오.

단계 **8** **Import(**가져오기**)**를 클릭하여 재정의된 검사기 구성을 업로드합니다.

재정의된 검사기 구성을 업로드하면 검사기 옆에 재정의된 검사기임을 나타내는 주황색 원이 표시됩니다.

또한 검사기 아래의 **Overridden Configuration(**재정의된 구성**)** 열에 재정의된 값이 표시됩니다.

Search(검색) 표시줄 옆에 있는 **Show Overrides Only(**재정의 항목만 표시**)** 확인란을 사용하여 재정의된 모든 검사기를 볼 수도 있습니다.

참고 **Download(**다운로드**)** 아래에서 **Overrideden Configurations(**재정의된 구성**)**를 항상 다운로드한 다음 JSON 파일을 열고 이 파일의 검사기 구성에 새로운 변경/재정의를 추가합니다. 이 작업은 기존의 재정의된 구성을 잃지 않도록 하는 데 필요합니다.

단계 **9** (선택 사항) 재정의된 검사기(주황색 원으로 표시됨)에서 뒤로 화살표 아이콘을 클릭한 다음 **Revert(**되돌리기**)**를 클릭하여 재정의된 구성을 해당 검사기에 대해서만 기본 구성으로 되돌립니다.

Snort 2에 대한 맞춤형 네트워크 분석 정책 생성

새로운 네트워크 분석 정책을 생성하는 경우 고유한 이름 및 기본 정책을 지정하고 인라인 모드를 선택해야 합니다.

기본 정책은 네트워크 분석 정책의 기본 설정을 정의합니다. 새로운 정책에서 구성을 변경하면 기본 정책 설정을 대체하지만 변경하지는 않습니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다.

네트워크 분석 정책의 인라인 모드에서는 전처리기가 트래픽을 수정(표준화)하고 삭제하여 공격자가 탐지를 회피할 가능성을 최소화할 수 있습니다. 수동 배포에서는 시스템이 인라인 모드와 관계없이 트래픽 흐름에 영향을 줄 수 없다는 점에 유의하십시오.

관련 항목

기본 레이어, 1981 페이지
인라인 구축의 전처리기 트래픽 수정, 2224 페이지
사용자 지정 네트워크 분석 정책 만들기, 2220 페이지
네트워크 분석 정책 수정, 2222 페이지

사용자 지정 네트워크 분석 정책 만들기

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다. 다른 정책에 저장되지 않은 변경 사항이 있는 경우, **Network Analysis Policy(**네트워크 분석 정책**)** 페이지로 돌아가라는 메시지가 나타나면 **Cancel(**취소**)**을 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 정책 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 정책 이름과의 충돌을 식별할 수 있습니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** 최초 **Base Policy(**기본 정책**)**를 선택합니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다.

단계 **6** 인라인 구축에서 트래픽이 전처리기의 영향을 받게 하려면 **Inline Mode(**인라인 모드**)**를 활성화합니다.

단계 **7** 정책을 생성하려면:

- 새로운 정책을 만들고 **Network Analysis Policy(**네트워크 분석 정책**)**로 돌아가려면 **Create Policy(**정책 생성**)**를 클릭합니다. 새로운 정책의 설정은 기본 정책의 설정과 같습니다.
- **Create and Edit Policy(**정책 생성 및 편집**)**를 클릭하여 정책을 만들고 고급 네트워크 분석 정책 편집기에서 정책을 열어 편집합니다.

관련 항목

맞춤형 사용자 역할 생성
웹 인터페이스의 사용자 역할 맞춤화, 127 페이지

네트워크 분석 정책 관리

Network Analysis Policy(네트워크 분석 정책) 페이지(또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**(이)나 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**)에서 다음 정보와 함께 현재 맞춤형 네트워크 분석 정책을 볼 수 있습니다.

- 정책이 최종 수정된 시간과 날짜(로컬 시간) 및 정책을 수정한 사용자
- **Inline Mode** 설정의 활성화 여부(프리프로세서가 트래픽에 영향을 미치도록 허용)
- 트래픽을 전처리하는 데 네트워크 분석 정책을 사용하는 액세스 제어 정책 및 디바이스
- 정책에 저장되지 않은 변경 사항이 있는지 여부 및 현재 정책을 수정하고 있는 사람에 관한 정보

사용자가 생성하는 맞춤형 정책 이외에도 시스템은 두 개의 맞춤형 정책인, Initial Inline Policy(초기 인라인 정책)와 Initial Passive Policy(초기 수동 정책)를 제공합니다. 이 두 가지 네트워크 분석 정책은 Balanced Security and Connectivity(균형 보안 및 연결) 네트워크 분석 정책을 기반으로 사용합니다. 이 둘의 유일한 차이점은 인라인 모드에서는 전처리기가 인라인 정책의 트래픽에 영향을 미치도록 허용하고, 패시브 정책에서는 이를 비활성화한다는 점입니다. 시스템이 제공하는 이러한 맞춤형 정책을 편집하고 사용할 수 있습니다

Firepower System 사용자 계정 역할이 Intrusion Policy(침입 정책) 또는 Modify Intrusion Policy(침입 정책 수정)로 제한된 경우에만 네트워크 분석과 침입 정책을 생성 및 수정할 수 있습니다.

관련 항목

사용자 지정 네트워크 분석 정책 만들기, 2220 페이지
네트워크 분석 정책 수정, 2222 페이지

네트워크 분석 정책 설정 및 캐시된 변경 사항

새로운 네트워크 분석 정책을 생성하는 경우 해당 기본 정책의 설정과 동일합니다.

네트워크 분석 정책을 조정할 경우, 특히 전처리기를 비활성화할 경우, 일부 전처리기 및 침입 규칙은 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 필수 전처

리기를 비활성화하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

참고 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다.

시스템은 사용자당 1개의 네트워크 분석 정책을 캐시합니다. 네트워크 분석 정책을 수정하는 동안 모든 메뉴 또는 다른 페이지로 이동하는 다른 경로를 선택하는 경우, 해당 페이지를 벗어난다고 해도 변경 사항은 시스템 캐시에 유지됩니다.

관련 항목

정책이 트래픽에서 침입을 검토하는 방법, 1962 페이지
사용자 지정 정책의 한계, 1971 페이지

네트워크 분석 정책 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 구성하려는 네트워크 분석 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 네트워크 분석 정책 편집:

- 기본 정책 변경 - 기본 정책을 변경하려면 Policy Information(정책 정보) 페이지의 **Base Policy(**기본 정책**)** 드롭다운 목록에서 기본 정책을 선택합니다.
- 정책 레이어 관리 - 정책 레이어를 관리하려면 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다.
- 전처리기 수정 - 전처리기를 활성화, 비활성화 또는 편집하려면 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.
- 트래픽 수정 - 전처리기가 트래픽을 수정하거나 삭제하도록 허용하려면 Policy Information(정책 정보) 페이지에서 **Inline Mode(**인라인 모드**)** 확인란을 선택합니다.

- 설정 확인 - 기본 정책의 설정을 확인하려면 Policy Information(정책 정보) 페이지에서 **Manage Base Policy(**기본 정책 관리**)**를 클릭합니다.

단계 **4** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다. 변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 전처리기가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하도록 허용하려면, 전처리기에 대한 규칙을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

기본 레이어, 1981 페이지
기반 정책 변경, 1983 페이지
네트워크 분석 정책의 전처리기 설정, 2223 페이지
인라인 구축의 전처리기 트래픽 수정, 2224 페이지
레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

네트워크 분석 정책의 전처리기 설정

전처리기는 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비합니다. 전처리기는 패킷이 사용자가 구성한 전처리기 옵션을 트리거할 때 전처리기 이벤트를 생성합니다. 네트워크 분석 정책에 대한 기본 정책은 기본적으로 활성화되는 전처리기 및 각각에 대한 기본 구성을 결정합니다.

참고 대부분의 경우, 전처리기는 특정 전문가가 구성해야 하며 거의 수정이 필요하지 않습니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다.

전처리 구성을 수정하려면 구성 및 네트워크에 미치는 잠재적 영향에 대한 이해가 필요합니다.

일부 고급 전송 및 네트워크 전처리기 설정은 액세스 컨트롤 정책을 구축하는 모든 네트워크, 영역 및 VLAN에 전역적으로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다.

또한 침입 정책에서 ASCII 텍스트의 신용카드 번호 및 주민등록번호 같은 민감한 데이터를 탐지하는 민감한 데이터 전처리기를 구성할 수도 있습니다.

관련 항목

DCE/RPC 전처리기, 2228 페이지
DNP3 전처리기, 2302 페이지
DNS 전처리기, 2240 페이지
FTP/텔넷 디코더, 2244 페이지
GTP 전처리기, 2276 페이지
HTTP 검사 전처리기, 2252 페이지
IMAP 전처리기, 2277 페이지
인라인 정상화 전처리기, 2317 페이지
IP 조각 모음 전처리기, 2324 페이지
Modbus 전처리기, 2300 페이지
패킷 디코더, 2330 페이지
POP 전처리기, 2280 페이지
민감한 데이터 탐지 기본 사항, 2043 페이지
SIP 전처리기, 2270 페이지
SMTP 전처리기, 2283 페이지
SSH 전처리기, 2289 페이지
SSL 전처리기, 2294 페이지
Sun RPC 전처리기, 2269 페이지
TCP 스트림 전처리, 2334 페이지
UDP 스트림 전처리, 2346 페이지
사용자 지정 정책의 한계, 1971 페이지

인라인 구축의 전처리기 트래픽 수정

인라인 구축(즉 관련 설정을 라우팅, 스위칭 또는 투명 인터페이스나 인라인 인터페이스 쌍을 이용해 디바이스에 적용함)의 경우 일부 전처리기가 트래픽을 수정하거나 차단할 수 있습니다. 예를 들면 다음과 같습니다.

- 인라인 표준화 전처리기는 패킷을 정규화하여 다른 전처리기와 침입 규칙 엔진에 의한 분석을 위해 준비합니다. 또한 전처리기의 **Allow These TCP Options(**이러한 **TCP** 옵션 허용**)**와 **Block Unresolvable TCP Header Anomalies(**복구 불능 **TCP** 헤더 이상 징후 차단**)** 옵션을 사용하여 특정 패킷을 차단할 수도 있습니다.
- 시스템은 잘못된 체크섬이 포함된 패킷을 삭제할 수 있습니다.
- 시스템은 속도 기반 공격 방지 설정과 일치하는 패킷을 삭제할 수 있습니다.

네트워크 분석 정책에서 트래픽에 영향을 주도록 구성된 전처리기의 경우, 전처리기를 활성화하고 올바르게 구성해야 하며 매니지드 디바이스도 인라인으로 올바르게 구축해야 합니다. 마지막으로, 네트워크 분석 정책의 **Inline Mode(**인라인 모드**)** 설정을 활성화해야 합니다.

네트워크 분석 정책 참고 사항의 전처리기 설정

네트워크 분석 정책의 탐색 패널에 있는 **Settings(**설정**)**를 선택하는 경우, 정책은 유형 별 전처리기를 나열합니다. Settings(설정) 페이지에서 네트워크 분석 정책의 전처리기를 활성화 또는 비활성화할 수 있으며, 전처리기 구성 페이지에 액세스할 수도 있습니다.

이를 구성하려면 전처리기를 활성화해야 합니다. 전처리기를 활성화하면, 전처리기 구성 페이지로 연결되는 하위 링크가 탐색 패널의 **Settings(**설정**)** 링크 아래에 나타나고, Settings(설정) 페이지의 전처리기 옆에 구성 페이지로 연결되는 **Edit(**수정**)** 링크가 나타납니다.

팁 전처리기의 구성을 기본 정책의 설정으로 되돌리려면, 전처리기 구성 페이지에서 **Revert to Defaults(**기본값으로 되돌리기**)**를 클릭합니다. 메시지가 표시되면 복원할 것인지 확인합니다.

프리프로세서를 비활성화하면 하위 링크와 **Edit** 링크가 더 이상 나타나지 않지만 컨피그레이션은 그대로 유지됩니다. 특정 분석을 수행하려면 많은 전처리기와 침입 규칙에서 트래픽이 특정 방법으로 먼저 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 전처리기를 비활성화한 경우, 전처리기가 네트워크 분석 정책 웹 인터페이스에서 비활성화된 상태로 남아 있다고 해도, 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

구성이 인라인 배포에서 실제로는 트래픽을 수정하지 않으면서 어떻게 작동하는지 평가하려는 경우 인라인 모드를 비활성화하면 됩니다. 수동 구축에서 또는 탭 모드의 인라인 구축에서, 시스템은 인라인 모드에 관계없이 트래픽에 영향을 줄 수 없습니다.

참고 인라인 모드 비활성화는 침입 이벤트 성능 통계 그래프에 영향을 줄 수 있습니다. 인라인 구축에서 인라인 모드가 활성화된 경우 Intrusion Event Performance(침입 이벤트 성능) 페이지(**Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Performance(**침입 이벤트 성능**)**)에는 표준화 및 차단된 패킷을 나타내는 그래프가 표시됩니다. 인라인 모드를 비활성화하면(즉 패시브 구축에서는), 시스템이 표준화 또는 삭제했을 트래픽에 대한 데이터가 다수의 그래프에 표시됩니다.

참고 인라인 구축에서는 인라인 모드를 활성화하고 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화된 인라인 표준화 전처리기를 구성하는 것이 좋습니다. 수동 구축에서는 적응형 프로파일을 사용하는 것이 좋습니다.

관련 항목

고급 전송/네트워크 전처리기 설정, 2312 페이지
체크섬 확인, 2315 페이지
인라인 정상화 전처리기, 2317 페이지
침입 이벤트 성능 통계 그래프 유형, 2955 페이지

89 장

애플리케이션 레이어 프리프로세서

다음 주제에서는 애플리케이션 계층 전처리기와 전처리기 구성 방법을 설명합니다.

- 애플리케이션 계층 전처리기 소개, 2227 페이지
- 애플리케이션 계층 전처리기 라이선스 요구 사항, 2228 페이지
- 애플리케이션 계층 전처리기 요구 사항 및 사전 요건, 2228 페이지
- DCE/RPC 전처리기, 2228 페이지
- DNS 전처리기, 2240 페이지
- FTP/텔넷 디코더, 2244 페이지
- HTTP 검사 전처리기, 2252 페이지
- Sun RPC 전처리기, 2269 페이지
- SIP 전처리기, 2270 페이지
- GTP 전처리기, 2276 페이지
- IMAP 전처리기, 2277 페이지
- POP 전처리기, 2280 페이지
- SMTP 전처리기, 2283 페이지
- SSH 전처리기, 2289 페이지
- SSL 전처리기, 2294 페이지

애플리케이션 계층 전처리기 소개

애플리케이션 계층 프로토콜은 다양한 방법으로 동일한 데이터를 나타낼 수 있습니다. Firepower System은 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화하는 애플리케이션 계층 프로토콜 디코더를 제공합니다. 애플리케이션 계층 프로토콜 인코딩을 표준화하면 규칙 엔진이 동일한 콘텐츠 관련 규칙을 해당 데이터가 다르게 표시되는 패킷에 보다 효율적으로 적용할 수 있으며, 유익한 결과를 얻을 수 있습니다.

침입 규칙 또는 규칙 인수를 사용하려면 비활성화된 전처리기가 필요한 경우 네트워크 분석 정책 웹 인터페이스에서 비활성화 상태로 남아 있다고 해도, 시스템은 자동으로 전처리기를 현재 구성으로 사용한다는 점에 유의하십시오.

침입 정책에서 동반되는 전처리기 규칙을 활성화하지 않는 경우 대부분의 경우 전처리기는 이벤트를 생성하지 않는다는 점에 유의하십시오.

애플리케이션 계층 전처리기 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

애플리케이션 계층 전처리기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

DCE/RPC 전처리기

DCE/RPC 프로토콜을 사용하면 개별 네트워크 호스트에 있는 프로세스가 동일한 호스트에 있는 것처럼 통신할 수 있습니다. 이 프로세스 간 통신은 일반적으로 TCP 및 UDP를 통해 호스트 간에 전송됩니다. TCP 전송 내에서 DCE/RPC가 Windows SMB(Server Message Block) 프로토콜 또는 Samba로 더 캡슐화될 수 있습니다. Samba는 Windows와 UNIX 또는 Linux와 유사한 운영 체제로 구성된 혼합 환경에서 프로세스 간 통신에 사용되는 오픈 소스 SMB 구현입니다. 또한 네트워크의 Windows IIS 웹 서버는 방화벽을 통해 프록시 TCP 전송 DCE/RPC 트래픽에 분산 통신을 제공하는 IIS RPC over HTTP를 사용할 수도 있습니다.

DCE/RPC 전처리기 옵션 및 기능의 설명에는 MSRPC로 알려진 DCE/RPC의 Microsoft 구현이 포함됩니다. SMB 옵션 및 기능에 대한 설명은 SMB 및 Samba를 모두 나타냅니다.

대부분의 DCE/RPC 익스플로잇이 실제로 Windows 또는 Samba를 실행하는 네트워크의 모든 호스트가 될 수 있는 DCE/RPC 서버를 대상으로 하는 DCE/RPC 클라이언트 요청에서 발생하더라도, 익스플로잇은 서버 응답에서도 발생할 수 있습니다. DCE/RPC 전처리기는 RPC over HTTP 버전 1을 사용하는 TCP에서 전송되는 DCE/RPC를 포함하여 TCP, UDP 및 SMB 전송에서 캡슐화된 DCE/RPC 요청 및 응답을 탐지합니다. 전처리기는 DCE/RPC 데이터 스트림을 분석하고 이상 징후를 보이는 작업과

DCE/RPC 트래픽 내 회피 기술을 탐지합니다. 또한 SMB 데이터 스트림을 분석하고 SMB 이상 작업 및 회피 기술을 탐지합니다.

DCE/RPC 전처리기는 또한 IP 조각 모음 전처리기가 제공하는 IP 조각 모음 및 TCP 스트림 전처리기가 제공하는 TCP 스트림 리어셈블리에 더해 SMB의 분할을 해제하고 DCE/RPC 조각을 모읍니다.

마지막으로, DCE/RPC 전처리기는 규칙 엔진에 의한 처리를 위해 DCE/RPC 트래픽을 표준화합니다.

연결 없는 **DCE/RPC** 트래픽 및 연결 지향 **DCE/RPC** 트래픽

DCE/RPC 메시지는 DCE/RPC Protocol Data Units(프로토콜 데이터 단위, PDU)의 두 가지 명시적인 프로토콜 중 하나를 준수합니다.

연결 지향 **DCE/RPC PDU** 프로토콜

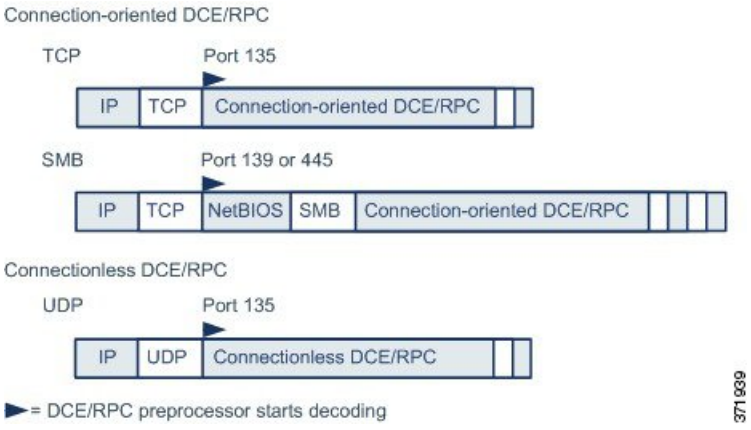
DCE/RPC 전처리기는 TCP, SMB 및 RPC over HTTP 전송에서 연결 지향 DCE/RPC를 탐지합니다.

연결 없는 **DCE/RPC PDU** 프로토콜

DCE/RPC 전처리기는 UDP 전송에서 연결 없는 DCE/RPC를 탐지합니다.

2개의 DCE/RPC PDU 프로토콜은 자체 고유한 헤더와 데이터 특성이 있습니다. 예를 들어 연결 지향 DCE/RPC 헤더 길이는 일반적으로 24바이트이며 연결 없는 DCE/RPC 헤더 길이는 80바이트로 고정됩니다. 또한 조각화된 연결 없는 DCE/RPC의 정확한 조각 순서는 연결 없는 전송으로 처리할 수 없으며, 연결 없는 DCE/RPC 헤더 값이어야 합니다. 반면 전송 프로토콜은 연결 지향 DCE/RPC의 정확한 조각 순서를 보장합니다. DCE/RPC 전처리기는 이와 그 외 기타 프로토콜 특정 특성을 이용하여 이상 징후 및 다른 회피 기술에 대한 프로토콜 모두를 모니터링하고, 트래픽을 규칙 엔진에 전달하기 전에 디코딩하고 조각 모음합니다.

다음 다이어그램은 DCE/RPC 전처리기가 여러 전송을 위해 DCE/RPC 트래픽을 처리하기 시작하는 시점에 대해 설명합니다.



그림에서 다음에 유의하십시오.

- 잘 알려진 TCP 또는 UDP 포트 135는 TCP와 UDP 전송에서 DCE/RPC 트래픽을 식별합니다.
- 그림은 RPC over HTTP를 포함하지 않습니다.

RPC over HTTP의 경우, 연결 지향 DCE/RPC는 그림에서처럼 HTTP를 통한 초기 구성 시퀀스 후 TCP에 직접 전송됩니다.

- DCE/RPC 전처리기는 일반적으로 NetBIOS 세션 서비스의 잘 알려진 TCP 포트 139 또는 이와 유사하게 구현된 잘 알려진 Windows 포트 445에서 SMB 트래픽을 수신합니다.

  SMB에는 DCE/RPC 전송 외에도 많은 기능이 있기 때문에 전처리기는 먼저 SMB 트래픽이 DCE/RPC 트래픽을 전달하는지 테스트한 다음, 전달하지 않는 경우 처리를 중지하고 전달하는 경우 처리를 계속 진행합니다.

- IP는 모든 DCE/RPC 전송을 캡슐화합니다.
- TCP는 모든 연결 지향 DCE/RPC를 전송합니다.
- UDP는 연결 없는 DCE/RPC를 전송합니다.

DCE/RPC 대상 기반 정책

Windows 및 Samba DCE/RPC 구현은 매우 다릅니다. 예를 들어, DCE/RPC 트래픽을 조각 모음할 때 Windows의 모든 버전은 첫 번째 조각에서 DCE/RPC 컨텍스트 ID를 사용하고, Samba의 모든 버전은 마지막 조각에서 컨텍스트 ID를 사용합니다. 다른 예로, 특정 함수 호출을 식별하기 위해 Windows Vista는 첫 번째 조각의 opnum(작업 번호) 헤더 필드를 사용하고, Samba 및 다른 모든 Windows 버전은 마지막 조각의 opnum 필드를 사용합니다.

또한 Windows 및 Samba SMB 구현에도 상당한 차이점이 있습니다. 예를 들어, 명명된 파이프로 작업할 때 Windows는 SMB OPEN 및 READ 명령을 인식하지만 Samba는 이러한 명령을 인식하지 않습니다.

DCE/RPC 전처리기를 활성화할 때는 기본 대상 기반 정책을 자동으로 활성화합니다. 필요에 따라 다른 Windows 또는 Samba 버전을 실행하는 다른 호스트를 대상으로 하는 대상 기반 정책을 추가할 수 있습니다. 기본 대상 기반 정책은 다른 대상 기반 정책에 포함되지 않는 모든 호스트에 적용됩니다.

각 대상 기반 정책에서 다음과 같이 할 수 있습니다.

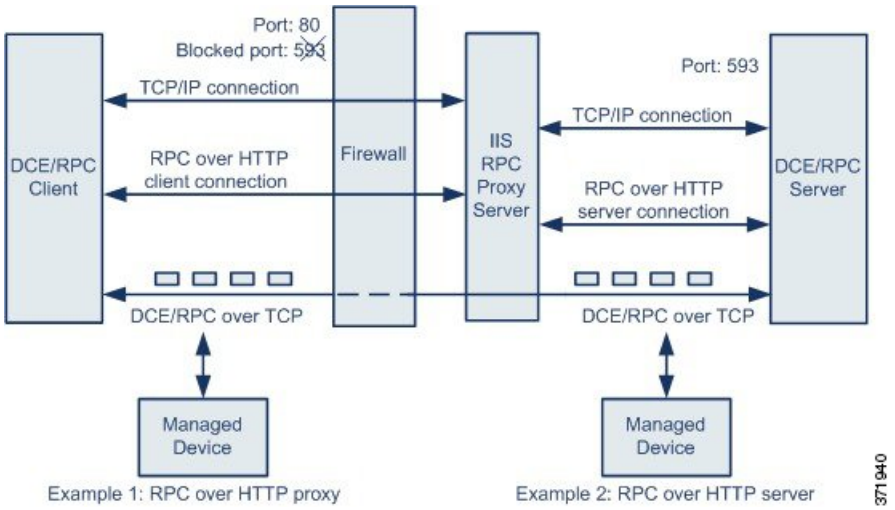
- 하나 이상의 전송을 활성화하고 각각에 대해 탐지 포트를 지정합니다.
- 자동 탐지 포트를 활성화하고 지정합니다.
- 사용자가 식별하는 하나 이상의 공유 SMB 리소스에 연결하려는 시도가 있는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다.
- SMB 트래픽의 파일을 탐지하고, 탐지한 파일에서 지정한 바이트 수를 검사하도록 전처리기를 구성할 수 있습니다.
- 또한 SMB 프로토콜 전문성을 가진 사용자만 변경할 수 있는 고급 옵션을 변경할 수 있습니다. 이 옵션을 통해 연속된 많은 SMB AndX 명령이 지정된 최대치를 초과하는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다.

DCE/RPC 전처리기 내 SMB 트래픽 파일 탐지를 활성화하는 것 외에도, 파일 정책을 구성하여 해당 파일을 선택적으로 수집 및 차단하거나 동적 분석을 위해 Cisco AMP 클라우드에 전송할 수 있습니다. 해당 정책 내에서 **Action(**작업**)**이 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)**며 **Application**

Protocol(애플리케이션 프로토콜**)**로 **Any(**모두**)** 또는 **NetBIOS-ssn(SMB)**을 선택한 파일 규칙을 생성해야 합니다.

RPC over HTTP 전송

HTTP 기반의 Microsoft RPC가 있으면 다음 다이어그램에서처럼 방화벽을 통해 DCE/RPC 트래픽을 터널링할 수 있습니다. DCE/RPC 전처리기는 HTTP 기반의 Microsoft RPC 버전 1을 탐지합니다.



Microsoft IIS 프록시 서버 및 DCE/RPC 서버는 동일한 호스트 또는 다른 호스트에 있을 수 있습니다. 개별 프록시와 서버 옵션은 두 경우 모두를 제공합니다. 그림에서 다음에 유의하십시오.

- DCE/RPC 서버는 DCE/RPC 클라이언트 트래픽에 대한 포트 593을 모니터링하지만, 방화벽은 포트 593을 차단합니다.

  방화벽은 일반적으로 포트 593을 기본값으로 차단합니다.

- RPC over HTTP는 방화벽이 허용할 가능성이 높은 잘 알려진 HTTP 포트 80을 사용하여 DCE/RPC over HTTP를 전송합니다.
- 예 1은 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 간 트래픽을 모니터링하기 위해 **RPC over HTTP proxy(RPC over HTTP** 프록시**)** 옵션을 선택하는 방법을 보여줍니다.
- 예 2는 Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 서로 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 **RPC over HTTP server(RPC over HTTP** 서버**)** 옵션을 선택하는 방법을 보여줍니다.
- 트래픽은 RPC over HTTP가 DCE/RPC 클라이언트와 서버 간의 프록시 설정을 완료한 후 연결 지향 DCE/RPC over TCP로만 구성됩니다.

DCE/RPC 전역 옵션

전역 DCE/RPC 전처리기 옵션은 전처리기가 작용하는 방법을 제어합니다. **Memory Cap Reached(**메모리 용량 도달**)** 및 **Auto-Detect Policy on SMB Session(SMB** 세션에서 자동 탐지 정책**)** 옵션을 제외한 경우, 이 옵션을 변경하면 성능 또는 탐지 기능에 부정적인 영향을 미칠 수 있다는 점에 유의하십

시오. 전처리기 및 전처리기와 활성화된 DCE/RPC 규칙 간의 상호 작용을 완벽하게 파악하지 않은 경우 이들을 변경할 수 없습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

최대 조각 크기

Enable Defragmentation(조각 모음 활성화**)**를 선택하면 허용된 최대 DCE/RPC 조각 길이를 지정합니다. 전처리기는 조각 모음 전에 처리를 위해 지정된 크기에 큰 조각을 자르지만 실제 패킷을 변경하지 않습니다. 빈 필드는 이 옵션을 비활성화합니다.

Maximum Fragment Size(최대 조각 크기**)** 옵션이 규칙이 탐지해야 하는 수준보다 크거나 동일한지 확인합니다.

리어셈블리 임계값

Enable Defragmentation(조각 모음 활성화**)**을 선택한 경우, 0은 이 옵션을 비활성화하고, 리어셈블된 패킷을 규칙 엔진으로 전송하기 전 프래그먼트된 DCE/RPC 바이트, 그리고 해당되는 경우 세그먼트된 SMB 바이트의 최소 수를 지정합니다. 낮은 값은 조기 검색 가능성을 증가시키지만 성능에 부정적인 영향을 미칠 수 있습니다. 이 옵션을 활성화하면 성능 영향을 테스트해야 합니다.

Reassembly Threshold(리어셈블리 임계값**)** 옵션이 규칙이 탐지해야 하는 수준보다 크거나 동일한지 확인합니다.

조각 모음 활성화

조각화된 DCE/RPC 트래픽을 조각 모음할지 여부를 지정합니다. 비활성화할 경우, 전처리기는 계속해서 이상 징후를 탐지하고 규칙 엔진에 DCE/RPC 데이터를 전송하지만, 조각화된 DCE/RPC 데이터에서 유실된 익스플로잇의 위험에 노출됩니다.

이 옵션을 사용하면 DCE/RPC 트래픽을 조각 모음하지 않는 유연성이 제공되지만, 대부분의 DCE/RPC 익스플로잇은 익스플로잇을 숨기기 위해 조각화를 이용하려고 시도합니다. 이 옵션을 비활성화하면 대부분의 알려진 익스플로잇을 우회하여 많은 수의 잘못된 부정이 야기됩니다.

메모리 용량 도달

전처리기에 할당된 최대 메모리 한도에 도달하거나 초과할 경우 이를 탐지합니다. 최대 메모리 용량에 도달하거나 초과할 경우, 전처리기는 메모리 용량 이벤트를 야기하고 해당 세션의 나머지 부분을 무시하는 세션과 관련된 보류 중인 모든 데이터를 비웁니다.

규칙 133:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

SMB 세션의 정책 자동 탐지

SMB `Session Setup AndX` 요청 및 응답에서 확인된 Windows 또는 Samba 버전을 탐지합니다. 탐지된 버전이 **Policy(**정책**)** 구성 옵션에 대해 구성된 Windows 또는 Samba 버전과 다른 경우, 탐지된 버전은 해당 세션만을 위해 구성된 버전을 대체합니다.

예를 들어 **Policy**를 Windows XP로 설정했는데 Windows Vista가 탐지된 경우, 프리프로세서는 해당 세션에 대해 Windows Vista 정책을 사용합니다. 다른 설정은 계속 적용됩니다.

DCE/RPC 전송이 SMB(즉, 전송이 TCP 또는 UDP인 경우)가 아닐 때는 버전을 탐지하고 정책을 자동으로 구성할 수 없습니다.

이 옵션을 활성화하려면 다음 드롭다운 목록 중 하나를 선택해야 합니다.

- **Client(**클라이언트**)**를 선택하여 정책 유형에 대한 서버-클라이언트 트래픽을 검사합니다.
- **Server(**서버**)**를 선택하여 정책 유형에 대한 클라이언트-서버 트래픽을 검사합니다.
- **Both(**모두**)**를 선택하여 정책 유형에 대한 서버-클라이언트 트래픽 및 클라이언트-서버 트래픽을 검사합니다.

레거시 **SMB** 검사 모드

검사할 SMB 버전을 지정합니다. 레거시 **SMB** 검사 모드가 활성화되면 DCE/RPC 전처리기는 SMB 버전 1 트래픽만 검사합니다. 이 옵션을 비활성화하면 DCE/RPC 전처리기는 SMB 버전 1, 2 및 3을 사용하는 트래픽을 검사합니다.

관련 항목

기본 content 또는 protected_content 키워드 인수, 2090 페이지
개요: byte_jump 및 byte_test 키워드

DCE/RPC 대상 기반 정책 옵션

각 대상 기반 정책에서 TCP, UDP, SMB 및 RPC over HTTP 전송 중 하나 이상을 활성화할 수 있습니다. 전송을 활성화할 때, 하나 이상의 탐지 포트, 즉, DCE/RPC 트래픽을 전달하는 것으로 알려진 포트를 지정해야 합니다.

Cisco는 기본 탐지 포트 사용을 권장합니다. 이는 잘 알려진 포트이거나 각 프로토콜에 일반적으로 사용하는 포트입니다. 기본이 아닌 포트에서 DCE/RPC 트래픽을 탐지한 경우에만 탐지 포트를 추가합니다.

Windows 대상 기반 정책에서는 네트워크 트래픽에 맞게 어떤 조합에서나 하나 이상의 전송에 대해 포트를 지정할 수 있지만, Samba 대상 기반 정책에서는 SMB 전송에만 포트를 지정할 수 있습니다.

참고 하나 이상의 전송이 활성화된 DCE/RPC 대상 기반 정책을 추가한 경우를 제외하고, 기본 대상 기반 정책에서는 하나 이상의 DCE/RPC 전송을 활성화해야 합니다. 예를 들어 모든 DCE/RPC 구현에 대해 호스트를 지정하고, 지정되지 않은 호스트에는 기본 대상 기반 정책을 구축하지 않을 수 있습니다. 이 경우 기본 대상 기반 정책에 대해 전송을 활성화하지 않을 수 있습니다.

또는 자동 탐지 포트, 즉 전처리기가 DCE/RPC 트래픽을 탐지하는 경우에만 포트가 DCE/RPC 트래픽을 전송하고 처리를 계속할지 결정하기 위해 전처리기가 처음 테스트하는 포트를 활성화하고 지정할 수도 있습니다.

자동 탐지 포트를 활성화할 때, 자동 탐지 포트가 전체 사용 후 삭제 포트 범위를 포함하기 위해 1024에서 65535까지의 포트 범위에 설정되어 있는지 확인합니다.

자동 탐지는 전송 탐지 포트에서 아직 식별되지 않은 포트에만 발생한다는 점에 유의하십시오.

RPC over HTTP Proxy Auto-Detect Ports(프록시 자동 탐지 포트) 옵션 또는 SMB Auto-Detect Ports(자동 탐지 포트) 옵션에 대한 자동 탐지 포트를 활성화하거나 지정할 가능성이 낮습니다. 이는 지정된 기본 탐지 포트를 제외하고는 이 둘을 위한 트래픽이 발생하거나 잠재력이 있을 가능성이 거의 없기 때문입니다.

각 대상 기반 정책을 통해 아래의 다양한 옵션을 지정할 수 있습니다. 어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

DCE/RPC 대상 기반 서버 정책을 구축할 호스트 IP 주소입니다. 또한 대상 기반 정책을 추가할 때는 대상 추가(Add Target) 팝업 윈도우의 **Server Address(**서버 주소**)** 필드에 이름이 지정됩니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 255개의 총 프로파일을 설정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

정책

모니터링된 네트워크 세그먼트에서 대상 호스트가 사용하는 Windows 또는 Samba DCE/RPC 구현

Auto-Detect Policy on SMB Session(SMB 세션에서 정책 자동 탐지**)** 전역 옵션을 활성화하여 SMB가 DCE/RPC 전송일 때 세션별로 이 옵션의 설정을 자동으로 대체할 수 있다는 점에 유의하십시오.

SMB 유효하지 않은 공유

하나 이상의 SMB 공유 리소스를 식별하는 전처리기는 사용자가 지정하는 공유 리소스에 연결하려는 시도가 있는 경우 이를 탐지합니다. 사용자는 쉼표로 구분된 목록에서 여러 공유를 지정할 수 있으며, 선택적으로 공유를 따옴표로 감쌀 수 있습니다. 이는 이전 소프트웨어 버전에서 필요했지만 더 이상 그럴 필요가 없습니다. 예를 들면 다음과 같습니다.

```
"C$", D$, "admin", private
```

전처리기는 **SMB Ports(SMB** 포트**)**를 활성화할 때 SMB 트래픽에서 유효하지 않은 공유를 탐지합니다.

대부분의 경우 Windows에서 명명되었고, 유효하지 않은 공유로 식별된 드라이브에 달러 표시를 추가해야 한다는 점에 유의하십시오. 예를 들어, C$ 또는 "C$"로 드라이브 C를 식별합니다.

또한 SMB 유효하지 않은 공유를 탐지하려면 **SMB Ports(SMB** 포트**)** 또는 **SMB Auto-Detect Ports(SMB** 자동 탐지 포트**)**를 활성화해야 합니다.

규칙 133:26을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

SMB 최대 **AndX** 체인

연속된 SMB AndX 명령에서 허용할 최대값입니다. 일반적으로, 연속된 여러 AndX 명령이 이상 작업을 나타내며 회피 시도를 나타낼 수 있습니다. 1을 지정하여 연속된 명령을 허용하지 않거나 0을 지정하여 연속된 명령의 수 탐지를 비활성화합니다.

동반되는 SMB 전처리기 규칙이 활성화되고 연속된 명령의 수가 구성한 값과 동일하거나 초과할 경우 전처리기는 먼저 연속된 명령의 수를 세고 이벤트를 생성한다는 점에 유의하십시오. 그런 다음 처리를 계속 진행합니다.

⚠

주의 SMB 프로토콜의 전문가만이 **SMB Maximum AndX Chains(SMB** 최대 **AndX** 체인**)** 옵션의 기본 설정을 변경해야 합니다.

규칙 133:20을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

RPC 프록시 트래픽 전용

RPC over HTTP Proxy Ports(RPC over HTTP 프록시 포트**)**를 활성화하면, 탐지된 클라이언트 측 RPC over HTTP가 프록시 트래픽 전용인지 또는 다른 웹 서버 트래픽을 포함하는지가 표시됩니다. 예를 들어, 포트 80은 프록시와 다른 웹 서버 트래픽을 모두 전달할 수 있습니다.

이 옵션을 비활성화하면, 프록시 및 다른 웹 서버 트래픽 모두 예상됩니다. 예를 들어, 서버가 전용 프록시 서버인 경우, 이 옵션을 활성화합니다. 활성화되었을 때, 전처리기는 트래픽이 DCE/RPC를 전달하고 있는지 확인하기 위해 트래픽을 테스트하고, 전달하고 있는 경우 처리를 계속 진행하고 그렇지 않은 경우 트래픽을 무시합니다. 이 옵션과 함께 **RPC over HTTP Proxy Ports(RPC over HTTP** 프록시 포트**)** 체크 박스도 활성화한 경우에만 기능이 추가됩니다.

RPC over HTTP 프록시 포트

관리되는 디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우 각 지정된 포트의 RPC over HTTP에서 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다.

활성화하면, 웹 서버에서 일반적으로 DCE/RPC와 기타 트래픽 모두에 기본 포트를 사용하기 때문에 트래픽이 필요한 가능성이 낮더라도, DCE/RPC 트래픽을 볼 수 있는 모든 포트를 추가할 수 있습니다. 이 탐지가 활성화되면 **RPC over HTTP Proxy Auto-Detect Ports(RPC over HTTP** 프록시 자동 탐지 포트**)**는 활성화되지 않지만, 탐지된 클라이언트 측 RPC over HTTP 트래픽이 프록시 트래픽뿐

이고 다른 웹 서버 트래픽은 포함되지 않는 경우 **RPC Proxy Traffic Only(RPC** 프록시 트래픽 전용**)**는 활성화됩니다.

참고 이 옵션은 선택하는 일이 거의 없을 것입니다.

RPC over HTTP 서버 포트

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 각 지정된 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다.

일반적으로 이 옵션을 활성화하는 경우 네트워크에서 프록시 웹 서버가 인식되지 않더라도 포트 범위를 1025~65535로 설정하여 **RPC over HTTP Server Auto-Detect Ports(RPC over HTTP** 서버 자동 탐지 포트**)**도 활성화해야 합니다. HTTP 서버 포트 기반의 RPC가 경우에 따라 재구성되는데, 이 경우 사용자는 이 옵션의 포트 목록에 재설정된 서버 포트를 추가해야 합니다.

TCP 포트

각 지정된 포트의 TCP에서 DCE/RPC 트래픽의 탐지를 활성화합니다.

적정 DCE/RPC 트래픽 및 익스플로잇은 다양한 포트를 사용하고, 포트 1024 이상의 다른 포트는 일반적입니다. 일반적으로 이 옵션을 활성화하면 해당 옵션에 대해 1025에서 최대 65535 포트 범위의 **TCP Auto-Detect Ports(TCP** 자동 탐지 포트**)**도 활성화해야 합니다.

UDP 포트

각 지정된 포트에서 UDP 내 DCE/RPC 트래픽의 탐지를 활성화합니다.

적정 DCE/RPC 트래픽 및 익스플로잇은 다양한 포트를 사용하고, 포트 1024 이상의 다른 포트는 일반적입니다. 일반적으로 이 옵션을 활성화하면 또한 해당 옵션에 대해 1025에서 최대 65535 포트 범위의 **UDP Auto-Detect Ports(UDP** 자동 탐지 포트**)**도 활성화해야 합니다.

SMB 포트

각 지정된 포트에서 SMB 내 DCE/RPC 트래픽의 탐지를 활성화합니다.

기본 탐지 포트를 사용하면 SMB 트래픽이 발생할 수 있습니다. 다른 포트를 사용할 경우 발생 가능성은 매우 낮습니다. 일반적으로, 기본 설정을 사용합니다.

Auto-Detect Policy on SMB Session(SMB 세션에서 정책 자동 탐지**)** 전역 옵션을 활성화하여 SMB가 DCE/RPC 전송일 때 세션별로 대상이 되는 정책에 대해 구성된 정책 유형을 자동으로 대체할 수 있다는 점에 유의하십시오.

RPC over HTTP 프록시 자동 탐지 포트

매니지드 디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우 지정된 포트에서 RPC over HTTP에서 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

활성화하면, 일반적으로 1025에서 65535까지 포트 범위를 지정하여 사용 후 삭제 포트의 전체 범위를 지원할 수 있습니다.

RPC over HTTP 서버 자동 탐지 포트

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 지정된 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

TCP 자동 탐지 포트

지정된 포트의 TCP에서 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

UDP 자동 탐지 포트

각 지정된 포트에서 UDP 내 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

SMB 자동 탐지 포트

SMB 내 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

참고 이 옵션은 선택하는 일이 거의 없을 것입니다.

SMB 파일 검사

파일 검색을 위한 SMB 트래픽의 검사를 활성화합니다. 다음 옵션을 이용할 수 있습니다.

- 파일 선택을 비활성화하려면 **Off(**끄기**)**를 선택합니다.
- SMB의 DCE/RPC 트래픽 검사 없이 파일 데이터를 검사하려면 **Only(**전용**)**를 선택합니다. 이 옵션을 선택하면 파일 및 DCE/RPC 트래픽 모두의 검사 성능을 높일 수 있습니다.
- SMB에서 파일 및 DCE/RPC 트래픽을 모두 검사하려면 **On(**켜기**)**을 선택합니다. 이 옵션을 선택하면 성능에 영향을 줄 수 있습니다.

다음에 대한 SMB 트래픽의 검사는 지원되지 않습니다.

- 단일 TCP 또는 SMB 세션에서 동시에 전송된 파일
- 여러 TCP 또는 SMB 세션을 통해 전송된 파일
- 메시지 서명이 협상될 때와 같이 비인접 데이터로 전송된 파일
- 데이터를 중첩하여 동일한 오프셋에 서로 다른 데이터로 전송된 파일
- 클라이언트가 파일 서버에 저장한 수정 사항에 대해 원격 클라이언트에 열린 파일

SMB 파일 검사 수준

SMB File Inspection(SMB 파일 검사**)**이 **Only(**전용**)** 또는 **On(**켜기**)**으로 설정된 경우, 파일이 SMB 트래픽에서 탐지될 때 바이트 수를 검사합니다. 다음 중 하나를 지정하십시오.

- 양수 값
- 전체 파일을 검사하려면 `0`
- 파일 검사를 비활성화하려면 `-1`

이 필드에는 액세스 컨트롤 정책의 Advanced(고급) 탭에 있는 File and Malware Settings(파일 및 악성 코드 설정) 섹션에 정의된 것과 동일하거나 작은 값을 입력합니다. 이 옵션에 파일 유형 탐지 시 검사할 바이트 수 제한에 정의된 것보다 큰 값을 설정한 경우, 시스템은 액세스 컨트롤 정책 설정의 기능을 최대로 사용합니다.

SMB File Inspection(SMB 파일 검사**)**을 **Off(**해제**)**로 설정한 경우, 이 필드는 비활성화됩니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

트래픽 관련 **DCE/RPC** 규칙

대부분의 DCE/RPC 전처리기 규칙은 SMB, 연결 지향 DCE/RPC 또는 연결 없는 DCE/RPC 트래픽에서 탐지된 이상 징후 및 회피 기술에 대해 트리거됩니다. 다음 표는 각 유형의 트래픽을 위해 활성화할 수 있는 규칙을 식별합니다.

표 ***216:*** 트래픽 관련 ***DCE/RPC*** 규칙

트래픽	전처리기 규칙 **GID:SID**
SMB	133:2~133:26 및 133:48~133:59
연결 지향 DCE/RPC	133:39를 통한 133:27
연결 없는 DCE/RPC를 탐지	133:43을 통한 133:40

DCE/RPC 전처리기 구성

전처리기 작동 방식을 제어하는 모든 전역 옵션을 수정함으로써, 그리고 사용자 네트워크의 DCE/RPC 서버를 그 위에서 운영되는 IP 주소 및 Windows 또는 Samba 버전 중 하나로 식별하는 하나 이상의 대상 기반 서버 정책을 지정함으로써 DCE/RPC 전처리기를 구성합니다. 또한 대상 기반 정책 설정에는 전송 프로토콜 활성화, DCE/RPC 트래픽을 해당 호스트로 전송하는 포트 지정 및 다른 서버 관련 옵션 설정이 포함되어 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정, 2203 페이지를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 왼쪽 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **DCE/RPC Configuration(DCE/RPC** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **DCE/RPC Configuration(DCE/RPC** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Global Settings(**전역 설정**)** 섹션의 옵션을 수정합니다(DCE/RPC 전역 옵션, 2231 페이지 참조).

단계 **7** 다음 옵션을 이용할 수 있습니다.

- 서버 프로파일 추가 - **Servers(**서버**)** 옆에 있는 추가( )을 클릭합니다. **Server Address(**서버 주소**)** 필드에 하나 이상의 IP 주소를 지정하고 **OK(**확인**)**를 클릭합니다.
- 서버 프로파일 삭제 - 정책 옆에 있는 삭제( )을 클릭합니다.
- 서버 프로파일 편집 - **Servers(**서버**)**에서 프로파일에 대해 설정된 주소를 클릭하거나 **default(**기본값**)**를 클릭합니다. **Configuration(**설정**)** 섹션에서 설정을 수정할 수 있습니다(DCE/RPC 대상 기반 정책 옵션, 2233 페이지 참조).

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 생성하려면 DCE/RPC 전처리기 규칙(GID 132 또는 133)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지, DCE/RPC 전역 옵션, 2231 페이지, DCE/RPC 대상 기반 정책 옵션, 2233 페이지, 트래픽 관련 DCE/RPC 규칙, 2238 페이지를 참고하십시오.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지
파일 및 악성코드 탐지 성능 및 저장 옵션, 1903 페이지
DCE/RPC 키워드, 2139 페이지
레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

DNS 전처리기

DNS 전처리기는 다음 특정 익스플로잇에 대해 DNS 이름 서버 응답을 검사합니다.

- RData 텍스트 필드에서 오버플로 시도
- 사용하지 않는 DNS 리소스 레코드 유형
- 실험적 DNS 리소스 레코드 유형

DNS 이름 서버 응답의 가장 일반적인 유형은 응답을 표시한 쿼리에서 도메인 이름에 해당하는 하나 이상의 IP 주소를 제공합니다. 예를 들면, 서버 응답의 다른 유형은 원래 쿼리된 서버에서 사용 가능한 정보를 제공하는 이름 서버의 이메일 메시지 또는 위치를 위한 대상을 제공합니다.

DNS 응답은 다음으로 구성됩니다.

- 메시지 헤더
- 하나 이상의 요청을 포함하는 Question(질문) 섹션
- Question(질문) 섹션의 요청에 응답하는 3가지 섹션
  - 답변
  - 권한
  - 추가 정보.

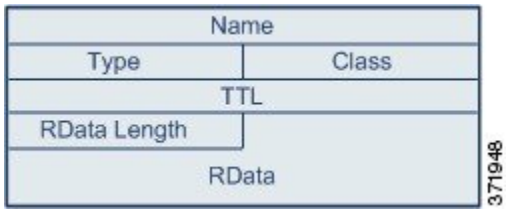
이 3가지 섹션에서 응답은 이름 서버에 유지되는 리소스 레코드(RR)의 정보를 반영합니다. 다음 표는 이러한 3가지 섹션에 대해 설명합니다.

표 ***217: DNS*** 이름 서버 ***RR*** 응답

섹션	포함 내용	예시
답변	선택 사항. 쿼리에 특정 응답을 제공하는 하나 이상의 리소스 레코드	도메인 이름에 해당하는 IP 주소
권한	선택 사항. 권위 있는 이름 서버를 가리키는 하나 이상의 리소스 레코드	응답에 대한 권위 있는 이름 서버의 이름

섹션	포함 내용	예시
추가 정보	선택 사항. Answer(응답) 섹션에 관련된 추가 정보를 제공한 하나 이상의 리소스 레코드	쿼리할 다른 서버의 IP 주소

많은 유형의 리소스 레코드가 있으며, 이는 모두 다음 구조를 준수합니다.



이론적으로, 모든 종류의 리소스 레코드는 이름 서버 응답 메시지의 Answer(답변), Authority(권한), 또는 Additional Information(추가 정보) 섹션에 사용될 수 있습니다. DNS 전처리기는 탐지하는 익스플로잇을 위해 3개의 응답 섹션 각각의 리소스 레코드를 검사합니다.

Type(유형) 및 RData 리소스 레코드 필드는 DNS 전처리기에 특히 중요합니다. Type(유형) 필드는 리소스 레코드 유형을 식별합니다. RData(리소스 데이터) 필드는 응답 콘텐츠를 제공합니다. RData 필드의 크기 및 내용은 리소스 레코드 유형에 따라 다릅니다.

DNS 메시지는 일반적으로 UDP 전송 프로토콜을 사용하지만 메시지 유형이 신뢰할 수 있는 전송을 요청하거나 메시지 크기가 UDP 기능을 초과할 경우 TCP도 사용합니다. DNS 전처리기는 UDP 및 TCP 트래픽 모두에서 DNS 서버 응답을 검사합니다.

세션이 삭제된 패킷 때문에 상태를 상실할 경우 DNS 전처리기는 중간에 선택된 TCP 세션을 검사하지 않으며, 검사를 중지합니다.

DNS 전처리기 옵션

포트

이 필드는 DNS 전처리기가 DNS 서버 응답에 대해 모니터링해야 하는 소스 포트 또는 포트를 지정합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

DNS 전처리기에 대해 구성할 일반적인 포트는 잘 알려진 포트 53인데, 이는 DNS 이름 서버가 UDP 및 TCP 모두에서 DNS 메시지에 사용하는 것입니다.

RData 텍스트 필드의 오버플로 시도 탐지

리소스 레코드 유형이 TXT(텍스트)이면 RData 필드는 변수 길이의 ASCII 텍스트 필드입니다.

선택 시 이 옵션은 MITRE's Current Vulnerabilities and Exposures(MITRE의 현재 취약성 및 노출) 데이터베이스의 CVE-2006-3441 항속에서 식별된 특정 취약성을 탐지합니다. 이는 Microsoft Windows 2000 서비스 팩 4, Windows XP 서비스 팩 1 및 서비스 팩 2, 그리고 Windows Server 2003 서비스 팩 1에서 잘 알려진 취약성입니다. 공격자는 이러한 취약성을 악용하고 호스트를 전송하거나 호스트가 RData

텍스트 필드의 길이에서 계산 착오를 일으키도록 하는 악의적으로 조작된 이름 서버 응답을 수신하도록 하여 버퍼 오버플로를 일으킴으로써 호스트를 완전히 제어할 수 있습니다.

네트워크가 이 취약성을 해결하기 위해 업그레이드된 적이 없는 운영체제를 실행하는 호스트를 포함하는 경우 사용자는 이 옵션을 활성화해야 합니다.

규칙 131:3을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

사용하지 않는 DNS RR 유형 탐지

RFC 1035는 여러 리소스 레코드 유형을 사용하지 않는 것으로 식별합니다. 이는 사용하지 않는 레코드 유형이기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 네트워크에 이들을 포함하도록 의도적으로 구성하지 않는 이상 일반 DNS 응답에서 이러한 레코드 유형이 발생하지 않습니다.

시스템을 구성하여 사용하지 않는 알려진 리소스 레코드 유형을 검색할 수 있습니다. 다음 표는 이러한 레코드 유형에 대해 나열하고 설명합니다.

표 ***218:*** 사용하지 않는 ***DNS*** 리소스 레코드 유형

RR 유형	코드	설명
3	MD	메일 대상
4	MF	메일 발송자

규칙 131:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

실험적 DNS RR 유형 탐지

RFC 1035는 여러 리소스 레코드 유형을 실험적인 것으로 식별합니다. 다음은 실험적 레코드 유형이기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 네트워크에 이들을 포함하도록 의도적으로 구성하지 않는 이상 일반 DNS 응답에서 이러한 레코드 유형이 발생하지 않습니다.

시스템을 구성하여 알려진 실험적 리소스 레코드 유형을 검색할 수 있습니다. 다음 표는 이러한 레코드 유형에 대해 나열하고 설명합니다.

표 ***219:*** 실험적 ***DNS*** 리소스 레코드 유형

RR 유형	코드	설명
7	MB	메일함 도메인 이름
8	MG	메일 그룹 멤버
9	MR	메일 이름 변경 도메인 이름
10	NUL	null 리소스 레코드

규칙 131:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

DNS 전처리기 구성

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **DCE Configuration(DCE** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **DCE Configuration(DCE** 구성**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** DNS 전처리기 옵션, 2241 페이지에서 설명하는 설정을 수정합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 생성하려면 DNS 전처리기 규칙(GID 131)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지 및 DNS 전처리기 옵션, 2241 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

침입 및 네트워크 분석 정책의 레이어, 1979 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

FTP/텔넷 디코더

FTP/텔넷 디코더는 FTP 및 텔넷 데이터 스트림을 분석하고, 규칙 엔진으로 처리하기 전에 FTP 및 텔넷 명령을 표준화합니다.

전역 FTP 및 텔넷 옵션

전역 옵션을 설정하여 FTP/텔넷 디코더가 패킷의 상태 저장 또는 상태 비저장 검사를 수행할지 여부, 디코더가 암호화된 FTP 또는 텔넷 세션을 탐지할지 여부, 그리고 암호화된 데이터가 발생한 후 디코더가 데이터 스트림 확인을 계속할지 여부를 결정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

상태 저장 검사

선택하면 FTP/텔넷 디코더가 상태를 저장하고 개별 패킷을 위한 세션 콘텍스트를 제공하며, 리어셈블한 세션만 검사할 수 있습니다. 이를 취소하면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

FTP 데이터 전송을 확인하려면, 이 옵션을 선택해야 합니다.

암호화된 트래픽 탐지

암호화된 텔넷 및 FTP 세션을 탐지합니다.

규칙 125:7 및 126:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

암호화된 데이터 검사 계속 진행

데이터 스트림이 암호화된 후에도 계속 검사하여 처리 가능한. 해독된 최종 데이터를 찾도록 전처리기에 지시합니다.

텔넷 옵션

FTP/텔넷 디코더에 의한 텔넷 명령의 표준화를 활성화 또는 비활성화할 수 있으며, 특정 이상 징후의 경우를 활성화 또는 비활성화할 수 있고 허용할 AYT(Are You There) 공격의 임계값 수를 설정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

텔넷 트래픽을 표준화할 포트를 나타냅니다. 텔넷은 일반적으로 TCP 포트 23에 연결됩니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다.

주의 암호화된 트래픽(SSL)은 디코딩될 수 없으므로, 포트 22(SSH)를 추가하면 예측되지 않은 결과를 얻을 수 있습니다.

표준화

지정된 포트로 향하는 텔넷 트래픽을 표준화합니다.

이상 징후 탐지

해당 SE(subnegotiation 종료) 없이 텔넷 SB(subnegotiation 시작)의 탐지를 활성화합니다.

텔넷은 SB(subnegotiation 시작)로 시작하고 SE(subnegotiation 종료)로 끝나는 subnegotiation을 지원합니다. 그러나, 텔넷 서버의 특정 구현은 해당 SE가 없는 SB를 무시합니다. 이는 우회하는 경우일 수 있는 이상 작업입니다. FTP가 제어 연결에서 텔넷 프로토콜을 사용하므로, 또한 이러한 작업에 취약합니다.

규칙 126:3을 활성화하여 이벤트를 생성하고 인라인 구축에서 이 이상 징후가 텔넷 트래픽에서 탐지될 때 문제가 되는 패킷을 삭제할 수 있으며, 규칙 125:9를 활성화하여 FTP 명령 채널에서 이 이상 징후가 탐지될 때 이벤트를 생성할 수 있습니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

AYT(Are You There) 공격 임계값 수

연속적인 AYT 명령의 수가 지정된 임계값을 초과하는 경우 이를 탐지합니다. Cisco는 AYT 임계값으로 기본값을 초과하지 않는 값을 설정할 것을 권장합니다.

규칙 126:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

서버 레벨 **FTP** 옵션

여러 FTP 서버에서 디코딩을 위한 옵션을 설정할 수 있습니다. 생성한 각 서버 프로파일은 서버 IP 주소 및 트래픽이 모니터링되어야 할 서버의 포트를 포함합니다. 특정 서버에 대해 어느 FTP 명령을 인증할지, 그리고 어느 FTP 명령을 무시할지 지정하고 명령에 대한 최대 매개변수 길이를 설정할 수 있습니다. 또한 디코더가 특정 명령을 위해 인증해야 할 특정 명령어 구문을 설정하고, 대안이 되는 최대 명령 매개변수 길이를 지정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

FTP 서버에서 하나 이상의 IP 주소를 지정하려면 이 옵션을 사용합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 하나 또는 둘 다로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 프로파일을 포함하여 최대 255개 프로파일을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 주소 블록을 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워 둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

포트

관리되는 디바이스가 트래픽을 모니터링해야 하는 FTP 서버에서 포트를 지정하려면 이 옵션을 사용합니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다. 포트 21은 잘 알려진 FTP 트래픽용 포트입니다.

File Get 명령

이 옵션을 사용하여 서버에서 클라이언트로 파일을 전송하는 데 사용되는 FTP 명령을 정의합니다. Support(지원팀)의 지시가 있는 경우가 아니면 이 값을 변경하지 마십시오.

주의 지원팀이 지시할 때만 **File Get Commands(File Get** 명령**)** 필드를 수정해야 합니다.

File Put 명령

이 옵션을 사용하여 클라이언트에서 서버로 파일을 전송하는 데 사용되는 FTP 명령을 정의합니다. Support(지원팀)의 지시가 있는 경우가 아니면 이 값을 변경하지 마십시오.

주의 지원팀이 지시할 때만 **File Put Commands(File Put** 명령**)** 필드를 수정해야 합니다.

추가 **FTP** 명령

이 문구를 사용하여 디코더가 탐지해야 하는 추가 명령을 지정합니다. 스페이스로 추가 명령을 구분합니다.

사용자가 추가할 수 있는 추가 명령에는 `XPWD`, `XCWD`, `XCUP`, `XMKD`, 그리고 `XRMD`가 포함되어 있습니다. 이 명령에 대한 자세한 내용은 네트워크 작업 그룹에 의한 디렉토리 지향 FTP 명령 사양인 RFC 775를 참고하십시오.

기본 최대 매개변수 길이

이 옵션을 사용하여 대체 매개변수 최대 길이가 설정되지 않은 명령에 대해 매개변수 최대 길이를 감지합니다. 대체 매개변수 최대 길이를 필요한 만큼 추가할 수 있습니다.

규칙 125:3을 활성화할 수 있습니다.이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

대체 매개변수 최대 길이

이 옵션을 사용하여 다른 매개변수 최대 길이를 탐지할 명령을 지정하고, 해당 명령에 대한 최대 매개변수 길이를 지정합니다. **Add(**추가**)**를 클릭하여 특정 명령을 위해 탐지할 다른 매개변수 최대 길이를 지정할 수 있는 회선을 추가합니다.

문자열 형식 공격에 대한 명령 확인

이 옵션을 사용하여 문자열 형식 공격에 대해 지정된 명령을 확인합니다.

규칙 125:5를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

명령의 유효성

이 옵션을 사용하여 특정 명령의 유효한 형식을 입력합니다. **Add(**추가**)**를 클릭하여 명령 유효성 검사 회선을 추가합니다.

규칙 125:2 및 125:4를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

FTP 전송 무시

이 옵션을 사용하여 데이터 전송 채널의 상태 확인 이외의 모든 검사를 비활성화하여 FTP 데이터 전송의 성능을 개선합니다.

참고 데이터 전송을 검사하려면 전역 FTP/Telnet **Stateful Inspection** 옵션을 선택해야 합니다.

FTP 명령 내 텔넷 이스케이프 코드 탐지

이 옵션을 사용하여 텔넷 명령이 FTP 명령 계통에서 사용되는 경우를 탐지합니다.

규칙 125:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

표준화 진행 중 삭제 명령 무시

Detect Telnet Escape Codes within FTP Commands(FTP 명령 내 텔넷 이스케이프 코드 탐지**)**를 선택한 경우 이 옵션을 사용하여 FTP 트래픽을 표준화할 때 텔넷 특성과 회선 삭제 명령을 무시합니다. 설정은 FTP 서버 처리가 텔넷 삭제 명령을 처리하는 방식에 일치해야 합니다. 이전 서버는 일반적으로 이를 처리하지만 새로운 FTP 서버는 일반적으로 텔넷 삭제 명령을 무시한다는 점에 유의하십시오.

문제 해결 옵션: **FTP** 명령 유효성 검사 구성 로그

Support(지원팀)는 문제 해결 통화 중에 사용자에게 시스템을 구성하여 서버에 나열된 각 FTP 명령에 대한 구성 정보를 인쇄하도록 요청할 수 있습니다.

⚠

주의 지원팀이 지시할 때만 **Log FTP Command Validation Configuration(FTP** 명령 유효성 검사 구성 로그**)**을 활성화하십시오.

FTP 명령 검증 성명

FTP 명령을 위한 유효성 입증 명령문을 설정할 때, 스페이스로 매개변수를 분리하여 대체 매개변수 그룹을 지정할 수 있습니다. 또한 유효성 입증 명령문에서 파이프 문자(|)로 이들을 분리하여 두 매개변수 간 이진 또는 관계를 생성할 수 있습니다. 매개변수를 대괄호([])로 묶는 것은 해당 매개변수가 선택 사항임을 나타냅니다. 매개변수를 중괄호({})로 묶는 것은 해당 매개변수가 요청된 것임을 나타냅니다.

FTP 커뮤니케이션의 일부로 수신된 매개변수의 문구를 인증하는 FTP 명령 매개변수 유효성 입증 명령문을 생성할 수 있습니다.

다음 표에 나열된 모든 매개변수는 FTP 명령 매개변수 유효성 입증 명령문에 사용할 수 있습니다.

표 ***220: FTP*** 명령 매개변수

사용 대상	발생하는 유효성 검사
`int`	표시된 매개변수는 정수여야 합니다.
`number`	표시된 매개변수는 1과 255 사이의 정수여야 합니다.
`char` _chars	표시된 매개변수는 _chars 인수에 지정된 특성 중 하나인 단일 특성이거나 그 구성원이어야 합니다. 예를 들어 `MODE`의 명령 유효성을 요휴성 입증 명령문 `char`로 정의하면 SBC는 `MODE` 명령을 위한 파라미터가 (Stream(스트림) 모드를 표시하는) `S`자와 (Block(차단) 모드를 표시하는) `B`자, (Compressed(압축된) 모드를 표시하는) `C`자로 이루어짐을 확인합니다.
`date` _datefmt	_datefmt가 `#`를 포함하는 경우, 표시된 파라미터는 숫자여야 합니다. _datefmt가 `C`를 포함하는 경우, 표시된 파라미터는 문자여야 합니다. _datefmt가 리터럴 문자열을 포함하는 경우, 표시된 매개변수는 리터럴 문자열에 일치해야 합니다.
문자열	표시된 매개변수는 문자열이어야 합니다.

사용 대상	발생하는 유효성 검사
`host_port`	표시된 매개변수는 RFC 959에 의해 정의된 대로 유효한 호스트 포트 지정자여야 하며, File Transfer Protocol 사양은 네트워크 작업 그룹에 의해 정의된 대로 유효한 호스트 포트 지정자여야 합니다.

필요한 경우 위 표의 문구를 조합하여 트래픽의 유효성을 입증해야 할 필요가 있는 각 FTP 명령을 정확하게 입증하는 매개변수 유효성 입증 명령문을 생성할 수 있습니다.

참고 TYPE 명령에서 복잡한 표현을 포함할 때, 스페이스로 이를 묶습니다. 또한, 표현 안의 각 피연산자를 스페이스로 묶습니다. 예를 들어, `char A | B` 를 입력합니다. `char A|B`는 올바르지 않습니다.

관련 항목

서버 레벨 FTP 옵션, 2245 페이지
Firepower System IP 주소 규칙, 19 페이지
FTP 명령 검증 성명, 2248 페이지

클라이언트 레벨 FTP 옵션

이러한 옵션을 사용하여 맞춤형 FTP 클라이언트 프로파일을 구성합니다. 옵션 설명에 전처리기 규칙이 포함되어 있지 않으면 이 옵션은 전처리기 규칙과 연결되어 있지 않은 것입니다.

네트워크

FTP 클라이언트의 하나 이상의 IP 주소를 지정하려면 이 옵션을 사용합니다.

단일 IP 주소나 주소 블록 또는 둘 중 하나 또는 모두로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. 최대 1024개의 문자를 지정할 수 있고, 기본 프로파일을 포함하여 최대 255개 프로파일을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 주소 블록을 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워 둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

최대 응답 길이

클라이언트가 수락하는 FTP 명령에 대해 허용되는 최대 응답 길이를 지정하려면 이 옵션을 사용합니다. 이는 기본 버퍼 오버플로를 탐지할 수 있습니다.

규칙 125:6을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

FTP 바운스 공격 탐지

FTP 바운스 공격을 탐지하려면 이 옵션을 사용합니다.

규칙 125:8을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

FTP 바운스 허용

FTP PORT 명령이 FTP 바운스 공격으로 처리되어서는 안 되는 호스트에서 추가 호스트 및 포트 목록을 구성하려면 이 옵션을 사용합니다.

FTP 명령 내 텔넷 이스케이프 코드 탐지

이 옵션을 사용하여 텔넷 명령이 FTP 명령 계통에서 사용되는 경우를 탐지합니다.

규칙 125:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

표준화 진행 중 삭제 명령 무시

Detect Telnet Escape Codes within FTP Commands를 선택한 경우 FTP 트래픽을 표준화할 때 텔넷 문자 및 줄 지우기 명령을 무시하려면 이 옵션을 사용합니다. 이 설정은 FTP 클라이언트가 텔넷 지우기 명령을 처리하는 방법과 일치해야 합니다. 이전 클라이언트는 일반적으로 이를 처리하지만 새로운 FTP 클라이언트는 일반적으로 텔넷 삭제 명령을 무시한다는 점에 유의하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

FTP/텔넷 디코더 설정

FTP 클라이언트에 대한 클라이언트 프로파일을 구성하여 클라이언트에서 FTP 트래픽을 모니터링할 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정, 2203 페이지를 참조하십시오.

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 2 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 3 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 4 **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **FTP and Telnet Configuration(FTP** 및 텔넷 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 5 **FTP and Telnet Configuration(FTP** 및 텔넷 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 6 **Global Settings(**전역 설정**)** 섹션의 옵션을 전역 FTP 및 텔넷 옵션, 2244 페이지에 설명된 대로 설정합니다.

단계 7 **Telnet Settings(**텔넷 설정**)** 섹션의 옵션을 텔넷 옵션, 2244 페이지에 설명된 대로 설정합니다.

단계 8 FTP 서버 프로파일 관리:

- 서버 프로파일 추가 - **FTP Server(FTP** 서버**)** 옆에 있는 추가( )을 클릭합니다. **Server Address(**서버 주소**)** 필드에 하나 이상의 클라이언트 IP 주소를 지정하고 **OK(**확인**)**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다.
- 서버 프로 파일 편집 - **FTP Server(FTP** 서버**)**의 맞춤형 프로파일에 대해 구성된 주소를 클릭하거나 **default(**기본값**)**를 클릭합니다. **Configuration(**설정**)** 섹션에서 설정을 수정할 수 있습니다(서버 레벨 FTP 옵션, 2245 페이지 참조).
- 서버 프로파일 삭제 - 프로파일 옆에 있는 삭제( )을 클릭합니다.

단계 9 FTP 클라이언트 프로파일 관리:

- 클라이언트 프로파일 추가 - **FTP Client(FTP** 클라이언트**)** 옆에 있는 추가( )을 클릭합니다. **Client Address** 필드에서 클라이언트에 대한 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수

있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다.

- 클라이언트 프로파일 편집 - **FTP Client(FTP** 클라이언트**)**에 추가한 프로파일에 대해 구성된 주소를 클릭하거나 **default(**기본값**)**를 클릭합니다. Configuration(설정) 페이지 영역에서 설정을 수정할 수 있습니다(클라이언트 레벨 FTP 옵션, 2249 페이지 참조).
- 클라이언트 프로파일 삭제 - 맞춤형 프로파일 옆에 있는 삭제( )을 클릭합니다.

단계 **10** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 생성하려면 FTP 및 텔넷 전처리기 규칙(GID 125 및 126)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지
레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

HTTP 검사 전처리기

HTTP Inspect(HTTP 검사) 전처리기는 다음 작업을 담당합니다.

- 사용자 네트워크 웹 서버로 전송된 HTTP 요청 및 사용자 네트워크 웹 서버에서 수신된 HTTP 응답 디코딩 및 표준화
- HTTP 관련 침입 규칙의 성능을 개선하기 위해 웹 서버로 전송된 메시지를 URI, 비 쿠키 헤더, 쿠키 헤더, 메서드 및 메시지 본문 구성 요소로 분리
- HTTP 관련 침입 규칙의 성능을 개선하기 위해 웹 서버에서 수신된 메시지를 상태 코드, 상태 메시지, 비 집합 쿠키 헤더, 쿠키 헤더 및 응답 본문 구성 요소로 분리
- 가능한 URI 인코딩 공격 탐지
- 추가 규칙을 처리하는 데 표준화된 데이터를 사용 가능하도록 하기

HTTP 트래픽은 여러 형식으로 인코딩될 수 있기 때문에 규칙의 적절한 검사를 어렵게 합니다. HTTP Inspect(HTTP 검사)는 14가지 유형의 인코딩을 디코딩하여 사용자의 HTTP 트래픽이 가능한 최상의 검사를 받을 수 있도록 합니다.

HTTP Inspect(HTTP 검사) 옵션을 전역으로, 단일 서버에서 또는 서버 목록에 대해 구성할 수 있습니다.

전처리기 엔진은 HTTP 표준화를 상태 비저장으로 수행합니다. 즉, HTTP 문자열을 패킷 단위로 표준화하며, TCP 스트림 전처리기에 의해 리어셈블된 HTTP 문자열만 처리할 수 있습니다.

전역 HTTP 정상화 옵션

HTTP Inspect(HTTP 검사) 전처리기에 제공되는 전역 HTTP 옵션은 전처리기가 작동하는 방식을 제어합니다. 이 옵션을 사용하여 웹 서버 포트로 지정되지 않은 포트가 HTTP 트래픽을 수신할 때 HTTP 표준화를 활성화하거나 비활성화합니다.

다음 사항을 참고하십시오.

- **Unlimited Decompression(**무제한 압축 해제**)**을 활성화하는 경우, 변경 사항을 커밋하면 **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)** 및 **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 옵션이 자동으로 65535로 설정됩니다.
- **Maximum Compressed Data Depth(**압축 데이터 최대 깊이**)** 또는 **Maximum Decompressed Data Depth(**압축 해제 데이터 최대 깊이**)**의 값이 다음에서 다른 경우 가장 높은 값을 사용합니다.
  - 기본 네트워크 분석 정책
  - 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

이상 HTTP 서버 탐지

웹 서버 포트로 지정되지 않은 포트로 전송되거나 해당 포트에서 수신되는 HTTP 트래픽을 탐지합니다.

참고 이 옵션을 설정하는 경우, HTTP 설정 페이지의 서버 프로파일에서 HTTP 트래픽을 수신하는 모든 포트를 나열해야 합니다. 이 옵션을 설정하지 않는 경우, 그리고 이 옵션 및 관련 전처리기 규칙을 활성화하는 경우, 서버를 오가는 일반 트래픽이 이벤트를 생성합니다. 기본 서버 프로파일은 보통 HTTP 트래픽에 사용되는 모든 포트를 포함하지만, 해당 프로파일을 수정한 경우, 이벤트가 생성되는 것을 방지하기 위해 다른 프로파일에 포트를 추가해야 할 수 있습니다.

규칙 120:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

HTTP 프록시 서버 탐지

Allow HTTP Proxy Use(HTTP 프록시 사용 허용**)** 옵션으로 정의되지 않은 프록시 서버를 사용하여 HTTP 트래픽을 탐지합니다.

규칙 119:17을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

압축 데이터 최대 수준

Inspect Compressed Data(압축 데이터 검사**)**(및 선택적으로, **Decompress SWF File(SWF** 파일 압축 해제**, LZMA)**, **Decompress SWF File(SWF** 파일 압축 해제**, Deflate)** 또는 **Decompress PDF File(PDF** 파일 압축 해제**, Deflate)**)가 활성화되어 있는 경우 압축 해제할 압축 데이터의 최대 크기를 설정합니다.

압축 해제된 데이터 최대 수준

Inspect Compressed Data(그리고 선택적으로 **Decompress SWF File(LZMA)**, **Decompress SWF File(Deflate)** 또는 **Decompress PDF File(Deflate)**) 옵션이 활성화된 경우 표준화된 압축 해제 데이터의 최대 크기를 설정합니다.

서버 레벨 **HTTP** 정상화 옵션

모니터링하는 각 서버에 대한 서버 수준 옵션을 모든 서버 또는 서버 목록에 대해 전역으로 설정할 수 있습니다. 또한, 미리 정의된 서버 프로파일을 사용하여 이 옵션을 설정하거나, 사용자 환경의 요구를 충족하도록 이들을 개별적으로 설정할 수 있습니다. 이 옵션 또는 이 옵션을 설정하는 기본 프로파일 중 하나를 사용하여 트래픽을 표준화할 HTTP 서버 포트와 표준화할 서버 응답 페이로드의 양, 그리고 표준화할 인코딩 유형을 지정합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

하나 이상 서버의 IP 주소를 지정하려면 이 옵션을 사용합니다. 단일 IP 주소나 주소 블록 또는 둘 중 하나 또는 모두로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.

최대 255개의 총 프로파일의 제한 외에도, 기본 프로파일을 포함하여 최대 496개의 문자 또는 약 26개의 항목을 하나의 HTTP 서버 목록에 포함할 수 있으며 모든 서버 프로파일에 대해 총 256개의 주소 항목을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

포트

HTTP 트래픽을 전처리기 엔진이 표준화하는 포트. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

오버사이즈 디렉토리 길이

지정한 값보다 긴 URL 디렉토리를 탐지합니다.

지정된 길이보다 긴 URL 요청을 전처리기가 감지하면 규칙 119:15를 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

클라이언트 흐름 수준

Ports(포트**)**에 정의된 클라이언트 측 HTTP 트래픽의 헤더 및 페이로드 데이터를 포함하여 원시 HTTP 패킷에서 규칙이 검사하는 바이트 수를 지정합니다. 규칙 내 HTTP 콘텐츠 규칙 옵션이 요청 메시지의 특정 부분을 검사할 때 클라이언트 흐름 수준은 적용되지 않습니다.

다음 중 하나를 지정합니다.

- 양수 값은 첫 번째 패킷에서 지정된 바이트 수를 검사합니다. 첫 번째 패킷이 지정된 것보다 작은 바이트를 포함하는 경우, 전체 패킷을 검사합니다. 지정된 값이 세그먼트 및 리어셈블된 패킷 모두에 적용된다는 점에 유의하십시오.

  또한 300 값은 여러 클라이언트 요청 헤더의 끝에 나타나는 큰 HTTP 쿠키의 검사를 일반적으로 수행하지 않는다는 점에 유의하십시오.

- 0은 한 세션의 여러 패킷을 포함하여 모든 클라이언트 측 트래픽을 검사하며, 필요 시 바이트 상한을 초과합니다. 이 값이 성능에 영향을 줄 수 있다는 점에 유의하십시오.

- -1은 클라이언트 측 트래픽을 모두 무시합니다.

서버 흐름 수준

Ports(포트**)**에 지정된 서버 측 HTTP 트래픽의 원시 HTTP 패킷에서 규칙이 검사하는 바이트 수를 지정합니다. **Inspect HTTP Responses**가 비활성화된 경우 원시 헤더와 페이로드가 검사에 포함되고, **Inspect HTTP Response**가 활성화된 경우 원시 응답 본문만 검사에 포함됩니다.

서버 흐름 수준은 **Ports(**포트**)**에 정의된 서버 측 HTTP 트래픽에서 규칙이 검사하는 세션의 원시 서버 응답 데이터의 바이트 수를 지정합니다. 이 옵션을 사용하여 HTTP 서버 응답 데이터의 조사 수준 및 성능의 균형을 맞출 수 있습니다. 규칙 내 HTTP 콘텐츠 규칙 옵션이 응답 메시지의 특정 부분을 검사할 때 서버 흐름 수준은 적용되지 않습니다.

클라이언트 흐름 수준과 달리, 서버 흐름 수준은 검사하는 규칙에 대해 HTTP 요청 패킷이 아닌 HTTP 응답별로 바이트 수를 지정합니다.

다음 값 중 하나를 지정할 수 있습니다.

- 양수 값:

  Inspect HTTP Responses가 활성화된 경우 원시 HTTP 응답 본문만 검사하고 원시 HTTP 헤더는 검사하지 않습니다. **Inspect Compressed Data**가 활성화된 경우 압축 해제 데이터도 검사합니다.

Inspect HTTP Responses가 비활성화된 경우 원시 패킷 헤더 및 페이로드를 검사합니다.

세션이 지정된 것보다 작은 응답 바이트를 포함하는 경우, 규칙은 주어진 세션의 모든 응답 패킷을 완전히 검사하며, 필요에 따라 여러 패킷에 걸쳐 검사합니다. 세션이 지정된 것보다 많은 응답 바이트를 포함하는 경우, 규칙은 해당 세션에 대해 지정된 수의 바이트만 검사하며, 필요에 따라 여러 패킷에 걸쳐 검사합니다.

흐름 수준 값이 작으면 **Ports(**포트**)**에 정의된 서버 측 트래픽을 대상으로 하는 규칙에서 오탐이 발생할 수 있습니다. 이러한 규칙의 대부분은 비 헤더 데이터의 처음 100바이트 정도에 있을 수 있는 HTTP 헤더 또는 콘텐츠를 대상으로 합니다. 헤더 길이는 일반적으로 300바이트보다 작지만, 헤더 크기는 다양할 수 있습니다.

또한 지정된 값이 세그먼트 및 리어셈블된 패킷 모두에 적용된다는 점에 유의하십시오.

- 0은 65535바이트가 넘는 세션의 응답 데이터를 포함하여 **Ports(**포트**)**에 정의된 모든 HTTP 서버 측 트래픽의 전체 패킷을 검사합니다.

  이 값이 성능에 영향을 줄 수 있다는 점에 유의하십시오.

- -1:

  Inspect HTTP Responses가 활성화된 경우 원시 HTTP 헤더만 검사하고 원시 HTTP 응답 본문은 검사하지 않습니다.

  Inspect HTTP Response(HTTP 응답 검사**)**가 비활성화된 경우 **Ports(**포트**)**에 정의된 모든 서버 측 트래픽을 무시합니다.

최대 헤더 길이

HTTP 요청에서(그리고 **Inspect HTTP Responses**가 활성화된 경우 HTTP 응답에서) 지정된 최대 바이트 수보다 긴 헤더 필드를 탐지합니다. 0 값은 이 옵션을 비활성화합니다. 활성화하려면 양수 값을 지정합니다.

규칙 119:19 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.를 활성화할 수 있습니다.

최대 헤더 수

HTTP 요청에서 헤더 수가 이 설정을 초과하는 경우 이를 탐지합니다. 0 값은 이 옵션을 비활성화합니다. 활성화하려면 양수 값을 지정합니다.

규칙 119:20 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.를 활성화할 수 있습니다.

최대 스페이스 수

접혀진 회선에서 공백의 수가 HTTP 요청에서 이 설정과 동일하거나 초과하는 경우 이를 탐지합니다. 0 값은 이 옵션을 비활성화합니다. 활성화하려면 양수 값을 지정합니다.

규칙 119:26 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.를 활성화할 수 있습니다.

HTTP 클라이언트 본문 추출 수준

HTTP 클라이언트 요청의 메시지 본문에서 추출할 바이트 수를 지정합니다. 침입 규칙을 사용하여 `content` 또는 `protected_content` 키워드 **HTTP Client Body(HTTP** 클라이언트 본문**)** 옵션을 선택하여 추출된 데이터를 검사할 수 있습니다.

클라이언트 본문을 무시하려면 -1을 지정합니다. 전체 클라이언트 본문을 추출하려면 0을 지정합니다. 추출할 특정 바이트를 확인하면 시스템 성능을 개선할 수 있다는 점에 유의하십시오. **HTTP Client Body(HTTP** 클라이언트 본문**)** 옵션이 침입 규칙에서 작동하려면 0보다 크거나 같은 값을 지정해야 합니다.

소규모 청크 크기

하나의 청크가 작은 것으로 고려되는 최대 바이트 수를 지정합니다. 양수 값을 지정합니다. 0 값은 이상 징후를 보이는 연속된 소규모 세그먼트의 탐지를 비활성화합니다. 자세한 내용은 **Consecutive Small Chunks(**연속된 소규모 청크**)** 옵션을 참고하십시오.

연속된 소규모 청크

얼마나 많은 연속된 작은 청크가 청크화된 이동 인코딩을 사용하는 클라이언트 또는 서버 트래픽에서 비정상적으로 큰 수를 나타내는지 지정합니다. **Small Chunk Size(**소규모 청크 크기**)** 옵션은 작은 청크의 최대 크기를 지정합니다.

예를 들어, **Small Chunk Size(**소규모 청크 크기**)**를 10으로 설정하고 **Consecutive Small Chunks(**연속된 소규모 청크**)**를 5로 설정하여 10바이트 이하의 연속된 5개의 청크를 탐지합니다.

전처리기 규칙 119:27을 활성화하여 클라이언트 트래픽의 과도한 소규모 청크에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 전처리기 규칙 120:7을 활성화하여 서버 트래픽의 과도한 소규모 청크에서 이벤트를 트리거할 수 있습니다. **Small Chunk Size(**소규모 청크 크기**)**가 활성화되고 이 옵션이 0 또는 1에 설정될 때, 이 규칙을 활성화하면 지정된 크기 또는 그보다 작은 모든 청크에서 이벤트가 트리거됩니다.

HTTP 메서드

시스템의 트래픽에 발생할 것으로 예상되는 GET 및 POST 외에 HTTP 요청 메서드를 지정합니다. 여러 개의 값을 구분하려면 쉼표를 사용하십시오.

침입 규칙은 HTTP 메서드에서 내용을 검색하기 위해 `content` 또는 `protected_content` 키워드와 **HTTP Method** 인수를 사용합니다. 규칙 119:31을 활성화하여 GET 및 POST 이외의 메서드 또는 이 옵션에 구성된 메서드가 트래픽에 발생할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

경고 없음

동반되는 전처리기 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

참고 이 옵션은 HTTP 표준 텍스트 규칙 및 공유 개체 규칙을 비활성화하지 않습니다.

HTTP 헤더 표준화

Inspect HTTP Responses(HTTP 응답 검사**)**가 활성화된 경우 요청 및 응답 헤더에서 비쿠키 데이터의 표준화를 활성화합니다. **Inspect HTTP Responses**가 활성화되지 않은 경우 요청 및 응답 헤더에서 쿠키를 비롯한 전체 HTTP 헤더의 표준화를 활성화합니다.

HTTP 쿠키 검사

HTTP 요청 헤더에서 쿠키 추출을 활성화합니다. 또한 **Inspect HTTP Responses(HTTP** 응답 검사**)**가 활성화된 경우 응답 헤더에서 set-cookie 데이터 추출을 활성화합니다. 쿠키 추출이 필요하지 않은 경우 이 옵션을 비활성화하면 성능을 높일 수 있습니다.

`Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스, 그리고 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않는다는 점에 유의하십시오.

HTTP 헤더 내 쿠키 표준화

HTTP 요청 헤더에서 쿠키의 표준화를 활성화합니다. **Inspect HTTP Responses(HTTP** 응답 검사**)**가 활성화된 경우 응답 헤더에서 set-cookie 데이터의 표준화도 활성화합니다. 이 옵션을 선택하기 전에 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)**를 선택해야 합니다.

HTTP 프록시 사용 허용

모니터링된 웹 서버가 HTTP 프록시로 사용되는 것을 허용합니다. 이 옵션은 HTTP 요청 검사에서만 사용됩니다.

URI만 검사

표준화된 HTTP 요청 패킷의 URI 부분만 검사합니다.

HTTP 응답 검사

HTTP 요청 메시지를 디코딩하고 표준화하는 것 외에도 HTTP 응답의 확장된 검사를 활성화하여 전처리기가 규칙 엔진에 의한 검사를 위해 응답 필드를 추출하도록 합니다. 이 옵션을 활성화하면 시스템이 응답 헤더, 본문, 상태 코드 등을 추출하며 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)**가 활성화된 경우 set-cookie 데이터도 추출합니다.

다음과 같이 규칙 120:2 및 120:3을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***221: HTTP*** 응답 규칙 검사

규칙	다음 상황에서 트리거됩니다.
120:2	잘못된 HTTP 응답 상태 코드가 발생합니다.
120:3	HTTP 응답에 콘텐츠 길이 또는 전송 인코딩이 포함되지 않습니다.

UTF 인코딩을 **UTF-8**로 표준화

Inspect HTTP Responses(HTTP 응답 검사**)**가 활성화된 경우 HTTP 응답에서 UTF-16LE, UTF-16BE, UTF-32LE 및 UTF32-BE 인코딩을 탐지하여 UTF-8로 표준화합니다.

UTF 표준화가 실패할 경우, 규칙 120:4를 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

압축 데이터 검사

Inspect HTTP Responses(HTTP 응답 검사**)**가 활성화된 경우 HTTP 응답 본문에 있는 gzip 및 deflate 호환 압축 데이터의 압축 해제 및 표준화된 압축 해제 데이터의 검사를 활성화합니다. 시스템은 청크 및 비 청크 HTTP 응답 데이터를 검사합니다. 시스템은 필요에 따라 여러 패킷에 걸쳐 패킷 별로 압축 해제된 데이터 패킷을 검사합니다. 즉 시스템이 검사를 위해 서로 다른 패킷의 압축 해제된 데이터를 결합하지 않습니다. **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)**, **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(**무제한 압축 해제**)**을 선택하지 않은 경우 **Server Flow Depth(**서버 흐름 수준**)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다.

다음과 같이 규칙 120:6 및 120:24를 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***222:*** 압축된 ***HTTP*** 응답 규칙 검사

규칙	다음 상황에서 트리거됩니다**.**
120:6	압축된 HTTP 응답의 압축 해제에 실패합니다.
120:24	압축된 HTTP 응답의 부분적 압축 해제에 실패합니다.

무제한 압축 해제

Inspect Compressed Data(그리고 선택적으로 **Decompress SWF File(LZMA)**, **Decompress SWF File(Deflate)** 또는 **Decompress PDF File(Deflate)**)가 활성화된 경우 여러 패킷에서 **Maximum Decompressed Data Depth**를 재정의합니다. 즉, 이 옵션은 여러 패킷에서 무제한 압축 해제를 활성화합니다. 이 옵션을 활성화해도 단일 패킷 내 **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)** 또는 **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)**에 영향을 주지 않는다는 점에 유의하십시오. 또한 이 옵션을 활성화하는 경우 변경을 커밋하면 **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)** 및 **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)**를 65535로 설정한다는 점에 유의하십시오.

JavaScript 표준화

Inspect HTTP Responses가 활성화된 경우 HTTP 응답 본문 내에서 Javascript의 탐지 및 표준화를 활성화합니다. 전처리기는 unescape 및 decodeURI 함수 및 String.fromCharCode 메서드와 같이 난독 처리된 JavaScript 데이터를 표준화합니다. 전처리기는 unescape, decodeURI 및 decodeURIComponent 함수에서 다음 인코딩을 표준화합니다.

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

전처리기는 연속적인 여백을 탐지하고 이를 단일 스페이스로 표준화합니다. 이 옵션을 활성화할 경우, 구성 필드를 사용하여 사용자가 난독 처리된 JavaScript 데이터에서 허용할 연속적인 여백의 최대 수를 지정할 수 있습니다. 1에서 65535까지의 값을 입력할 수 있습니다. 이 필드와 연결된 전처리기 규칙(120:10)이 활성화되는지 여부에 관계없이 0 값은 이벤트 생성을 비활성화합니다.

전처리기는 또한 JavaScript의 더하기(+) 연산자를 표준화하고 연산자를 사용하여 문자열을 연결합니다.

`file_data` 침입 규칙 키워드를 사용하여 침입 규칙이 표준화된 JavaScript 데이터를 가리키도록 할 수 있습니다.

다음과 같이 규칙 120:9, 120:10, 120:11을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***223: JavaScript*** 옵션 규칙 표준화

규칙	다음 상황에서 트리거됩니다.
120:9	전처리기 내 난독 처리 수준은 2와 같거나 큽니다.
120:10	JavaScript 난독 처리된 데이터에서 연속적인 여백의 수는 허용된 연속적인 여백의 최대 수에 구성된 값과 같거나 큽니다.
120:11	이스케이프 또는 인코딩된 데이터는 하나 이상의 인코딩 유형을 포함합니다.

SWF 파일 압축 해제**(LZMA)** 및 **SWF** 파일 압축 해제**(Deflate)**

HTTP Inspect Responses(HTTP 응답 검사**)**가 활성화된 경우 이러한 옵션은 HTTP 요청의 HTTP 응답 본문 내에 있는 파일의 압축된 부분을 압축 해제합니다.

참고 HTTP GET 응답에서 찾은 파일의 압축된 부분만 압축 해제할 수 있습니다.

- **Decompress SWF File(LZMA)(SWF** 파일 압축 해제**, LZMA)**은 Adobe ShockWave Flash(`.swf`) 파일의 LZMA 호환 가능 압축된 부분을 압축 해제합니다.
- **Decompress SWF File(SWF** 파일 압축 해제**, Deflate)**은 Adobe ShockWave Flash(`.swf`) 파일의 deflate 호환 가능 압축된 부분을 압축 해제합니다.

Maximum Compressed Data Depth(압축 데이터 최대 수준**)**, **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(**무제한 압축 해제**)**을 선택하지 않은 경우 **Server Flow Depth(**서버 흐름 수준**)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 침입 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다.

다음과 같이 규칙 120:12 및 120:13을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***224: SWF*** 파일 압축 해제 옵션 규칙

규칙	다음 상황에서 트리거됩니다.
120:12	deflate 파일 압축 풀기에 실패합니다.
120:13	LZMA 파일 압축 풀기에 실패합니다.

PDF 파일 압축 해제**(Deflate)**

HTTP Inspect Responses(HTTP 응답 검사**)**가 활성화된 경우, **Decompress PDF File(Deflate)(PDF** 파일 압축 해제**, Deflate)**은HTTP 요청의 HTTP 응답 본문 내에 있는 Portable Document Format(`.pdf`) 파일의 deflate 호환 가능 압축된 부분을 압축 해제합니다. 시스템은 `/FlateDecode` 스트림 필터를 사용하는 PDF 파일의 압축만 해제할 수 있습니다. 다른 스트림 필터(`/FlateDecode /FlateDecode` 포함)는 지원되지 않습니다.

참고 HTTP GET 응답에서 찾은 파일의 압축된 부분만 압축 해제할 수 있습니다.

Maximum Compressed Data Depth(압축 데이터 최대 수준**)**, **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(**무제한 압축 해제**)**을 선택하지 않은 경우 **Server Flow Depth(**서버 흐름 수준**)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 침입 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다.

다음과 같이 규칙 120:14, 120:15, 120:16, 120:17을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***225: PDF*** 파일 압축 해제***(Deflate)*** 옵션 규칙

규칙	다음 상황에서 트리거됩니다.
120:14	파일 압축 풀기에 실패합니다.
120:15	지원되지 않는 압축 유형 때문에 파일 압축 풀기에 실패합니다.
120:16	지원되지 않는 PDF 스트림 필터로 인해 파일 압축 풀기에 실패합니다.

규칙	다음 상황에서 트리거됩니다.
120:17	파일 구문 분석에 실패합니다.

원래 클라이언트 **IP** 주소 추출

X-Forwarded-For(XFF), True-Client-IP 또는 사용자가 정의한 HTTP 헤더에서 원래 클라이언트 IP 주소의 추출을 활성화합니다. 추출된 원래 클라이언트 IP 주소를 침입 이벤트 표 보기에서 표시할 수 있습니다.

규칙 119:23, 119:29, 119:30 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.을 활성화할 수 있습니다.

XFF 헤더 우선 순위

Extract Original Client IP Address(원래 클라이언트 **IP** 주소 추출**)**가 활성화된 경우 시스템이 원래 클라이언트 IP HTTP 헤더를 처리할 순서를 지정합니다. 모니터링되는 네트워크에서 XFF(X-Forwarded-For) 또는 True-Client-IP 이외의 원래 클라이언트 IP 헤더가 발생할 것으로 예상되는 경우, **Add(**추가**)**를 클릭하여 우선순위 목록에 다른 헤더 이름을 추가합니다. 그런 다음 각 헤더 유형 옆에 있는 위쪽 또는 아래쪽 화살표 아이콘을 사용하여 우선 순위를 조정합니다. 여러 XFF 헤더가 하나의 HTTP 요청에 표시되는 경우, 시스템은 가장 높은 우선 순위를 가진 헤더만 처리한다는 점에 유의하십시오.

URI 로그

HTTP 요청 패킷의 원시 URI 추출(있는 경우)을 활성화하고 세션에 대해 생성된 모든 침입 이벤트와 해당 URI를 연결합니다.

이 옵션을 활성화할 경우, 침입 이벤트 표 보기의 HTTP URI 열에서 추출한 URI의 첫 50자를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

호스트 이름 로그

HTTP 요청 호스트 헤더의 호스트 이름 추출(있는 경우)을 활성화하고 세션에 대해 생성된 모든 침입 이벤트와 해당 호스트 이름을 연결합니다. 여러 호스트 헤더가 있을 경우, 첫 번째 헤더에서 호스트 이름을 추출합니다.

이 옵션을 활성화할 경우, 침입 이벤트 표 보기의 HTTP Hostname(호스트 이름) 열에서 추출한 호스트 이름의 첫 50자를 표시할 수 있습니다. 패킷 보기에서 전체 호스트 이름을 최대 2048바이트까지 표시할 수 있습니다.

규칙 119:25를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

활성화된 119:24는 이 옵션의 설정에 상관없이 HTTP 요청에서 여러 호스트 헤더를 탐지하는 경우, 트리거됩니다.

프로파일

HTTP 트래픽에 표준화된 인코딩 유형을 지정합니다. 시스템은 대부분의 서버에 적절한 기본 프로파일, Apache 서버 및 IIS 서버의 기본 프로파일, 모니터링되는 트래픽의 요구 사항에 맞게 조정할 수 있는 맞춤형 기본 설정을 제공합니다.

- 모든 서버에 대해 적절한 표준 기본 프로파일을 사용하려면 **All(**모두**)**을 선택합니다.
- 시스템 제공 IIS 프로파일을 사용하려면 **IIS**를 선택합니다.
- 시스템 제공 Apache 프로파일을 사용하려면 **Apache**를 선택합니다.
- 자체 서버 프로파일을 생성하려면 **Custom(**맞춤형**)**을 선택합니다.

서버 레벨 **HTTP** 정상화 인코딩 옵션

HTTP 서버 수준 **Profile(**프로파일**)** 옵션을 `Custom(맞춤형)`으로 설정하면 HTTP 트래픽에 대해 표준화된 인코딩 유형을 지정하고, 다양한 인코딩 유형을 포함하는 트래픽에 대한 이벤트를 생성하도록 HTTP 전처리기 규칙을 활성화할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

ASCII 인코딩

인코딩된 ASCII 문자를 디코딩하고 규칙 엔진이 ASCII 인코딩된 URI에서 이벤트를 생성할지 여부를 지정합니다.

규칙 119:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

UTF-8 인코딩

URI에서 표준 UTF-8 유니코드 시퀀스를 디코딩합니다.

규칙 119:6을 활성화할 수 있습니다.이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

Microsoft %U 인코딩

4개 문자가 IIS 유니코드 코드 포인트와 관련이 있는 16진수로 인코딩된 값인 4개 문자가 뒤에 오는 %u를 사용하는 IIS %u 인코딩 체계를 디코딩합니다.

팁 적법한 클라이언트는 %u 인코딩을 거의 사용하지 않으며, 따라서 Cisco는 %u 인코딩으로 인코딩된 HTTP 트래픽을 디코딩할 것을 권장합니다.

규칙 119:3을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

베어 바이트 **UTF-8** 인코딩

UTF-8 값 디코딩 시 비ASCII 문자를 유효한 값으로 사용하는 베어 바이트 인코딩을 디코딩합니다.

팁 베어 바이트 인코딩을 사용하면 사용자는 IIS 서버를 에뮬레이트하고 비표준 인코딩을 정확하게 해석할 수 있습니다. 합법적인 클라이언트는 이런 방식으로 UTF-8을 인코딩하지 않으므로 Cisco는 이 옵션 활성화를 권장합니다.

규칙 119:4를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

Microsoft IIS 인코딩

유니코드 코드 포인트 매핑을 사용하여 디코딩합니다.

팁 이는 주로 공격 및 우회 시도에서 발견되므로 Cisco는 이 옵션 활성화를 권장합니다.

규칙 119:7을 활성화할 수 있습니다.이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

이중 인코딩

각각에서 디코딩을 수행하는 요청 URI를 통해 두 개 회선을 만들어 IIS 이중 인코딩된 트래픽을 디코딩합니다. 이는 주로 공격 시나리오에서 발견되므로 Cisco는 이 옵션 활성화를 권장합니다.

규칙 119:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

다중 슬래시 난독 처리

연속된 다중 슬래시를 단일 슬래시로 표준화합니다.

규칙 119:8을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

IIS 백슬래시 난독 처리

백슬래시를 사선으로 표준화합니다.

규칙 119:9를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

디렉토리 접근 공격

디렉토리 접근 공격 및 자기 참조 디렉토리를 표준화합니다. 이 트래픽 유형에 대한 이벤트를 생성하기 위해 해당 전처리기 규칙을 활성화하는 경우, 일부 웹사이트에서 디렉터리 접근 공격을 사용하는 파일을 참조하므로 잘못된 긍정이 생성될 수 있습니다.

규칙 119:10 및 119:11을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

탭 난독 처리

공백 구분 기호에 탭을 사용하는 비 RFC 표준을 표준화합니다. Apache 및 기타 비 IIS 웹 서버는 URL의 구분 기호로 탭 문자(0x09)를 사용합니다.

참고 이 옵션의 구성에 관계없이, 공백 문자(0x20)가 이 앞에 오는 경우 HTTP Inspect(HTTP 검사) 전처리기는 탭을 공백으로 처리합니다.

규칙 119:12를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

유효하지 않은 **RFC** 구분 기호

URI 데이터 내 행 바꿈(\n)을 표준화합니다.

규칙 119:13을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

Webroot 디렉토리 접근 공격

URL에서 초기 디렉토리를 가로질러 통과하는 디렉토리 접근 공격을 탐지합니다.

규칙 119:18을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

탭 **URI** 구분 기호

URI의 구분 기호로 탭 문자(0x09) 사용을 설정합니다. IIS의 Apache, 새 버전, 다른 웹 서버는 URL의 탭으로 구분 문자를 사용합니다.

참고 이 옵션의 구성에 관계없이, 공백 문자(0x20)가 이 앞에 오는 경우 HTTP Inspect(HTTP 검사) 전처리기는 탭을 공백으로 처리합니다.

비 **RFC** 문자

사용자가 추가한 비 RFC 문자 목록이 수신 및 발신 URI 데이터에 나타날 때 해당 필드에서 이를 탐지합니다. 이 필드를 수정할 경우, 바이트 문자를 나타내는 16진수 형식을 사용합니다. 이 옵션을 구성할 경우 값을 신중하게 설정합니다. 매우 일반적인 문자를 사용하면 이벤트가 과하게 생성될 수 있습니다.

규칙 119:14를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

최대 청크 인코딩 크기

URI 데이터에서 비정상적으로 큰 청크 크기를 탐지합니다.

규칙 119:16 및 119:22를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

파이프라인 디코딩 비활성화

파이프라인 요청에 대한 HTTP 디코딩을 비활성화합니다. 이 옵션을 비활성화하면, 파이프라인에 대기 중인 HTTP 요청이 디코딩되거나 분석되지 않고, 일반 패턴 일치만 사용하여 검사되기 때문에 성능이 향상됩니다.

엄격하지 않은 **URI** 구문 분석

엄격하지 않은 URI 구문 분석을 활성화합니다. "GET /index.html abc xo qr \n" 형식에서 비표준 URI를 수용하는 서버에서만 이 옵션을 사용합니다. 이 옵션을 사용하면, 두 번째 스페이스 뒤에 유효한 HTTP 식별자가 없는 경우에도 디코더는 URI가 첫 번째와 두 번째 스페이스 사이에 있다고 가정합니다.

확장된 **ASCII** 인코딩

HTTP 요청 URI 내 확장된 ASCII 문자의 구문 분석을 활성화합니다. 이 옵션은 사용자 지정 서버 프로파일에서만 사용 가능하며, Apache, IIS 또는 모든 서버에 제공된 기본 프로파일에서는 그렇지 않다는 점에 유의하십시오.

관련 항목

개요: HTTP content 및 protected_content 키워드 인수, 2094 페이지
Firepower System IP 주소 규칙, 19 페이지

HTTP 검사 전처리기 설정

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정, 2203 페이지를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **HTTP Configuration(HTTP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **HTTP Configuration(HTTP** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** Global Settings(전역 설정) 페이지 영역의 옵션을 수정합니다(전역 HTTP 정상화 옵션, 2253 페이지 참조).

단계 **7** 다음 3가지 옵션을 사용할 수 있습니다.

- 서버 프로파일 추가 - **Servers(**서버**)** 섹션 옆에 있는 추가( )을 클릭합니다. **Server Address(**서버 주소**)** 필드에 하나 이상의 클라이언트 IP 주소를 지정하고 **OK(**확인**)**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 목록에 최대 496개의 문자를 포함할 수 있고, 모든 서버 프로파일에 대해 총 256개의 주소 항목을 지정할 수 있으며, 기본 프로파일을 포함하여 총 255개의 프로파일을 생성할 수 있습니다.
- 서버 프로파일 편집 - **Servers(**서버**)**에 추가한 프로파일에 대해 설정된 주소를 클릭하거나 **default(**기본값**)**를 클릭합니다. **Configuration(**설정**)** 섹션에서 설정을 수정할 수 있습니다(서버 레벨 HTTP 정상화 옵션, 2254 페이지 참조). 또한 **Custom(**맞춤형**)**를 **Profile(**프로파일**)** 값으로 선택하면 서버 레벨 HTTP 정상화 인코딩 옵션, 2263 페이지에서 설명하는 인코딩 옵션을 수정할 수 있습니다.
- 서버 프로파일 삭제 - 맞춤형 프로파일 옆에 있는 삭제( )을 클릭합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 HTTP 전처리기 규칙(GID 119)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

추가 **HTTP** 검사 전처리기 규칙

다음 표의 **Preprocessor Rule GID:SID(**전처리기 규칙 **GID:SID)** 열에서 규칙을 활성화하여 특정 구성 옵션과 관련이 없는 HTTP Inspect(HTTP 검사) 전처리기 규칙에 대한 이벤트를 생성할 수 있습니다.

표 ***226:*** 추가 ***HTTP*** 검사 전처리기 규칙

전처리기 규칙 **GID:SID**	다음 상황에서 트리거 됩니다.
119:21	HTTP 요청 헤더에 둘 이상의 `content-length`(콘텐츠 길이) 필드가 있음.
119:24	HTTP 요청에 둘 이상의 Host(호스트) 헤더가 있음.
119:28	HTTP POST 메서드에는 `content-length` 헤더와 청크 분할된 `transfer-encoding`이 포함되어 있지 않습니다.
119:32	HTTP 버전 0.9가 트랙픽에서 발생함. TCP 스트림 구성 역시 활성화되어야 한다는 점에 유의하십시오.
119:33	HTTP URI가 이스케이프되지 않은 스페이스를 포함함.
119:34	TCP 연결이 24개 이상의 파이프라인 처리된 HTTP 요청을 포함함.
120:5	HTTP 응답 트래픽에서 UTF-7 인코딩이 발생함. UTF-7은 SMTP 트래픽에서와 같이 7비트 패리티가 필요한 경우에만 표시되어야 합니다.
120:8	`content-length` 또는 청크 크기가 유효하지 않습니다.
120:18	HTTP 서버 응답이 클라이언트가 요청하기 전에 발생함.
120:19	HTTP 응답이 여러 콘텐츠 길이를 포함함.
120:20	HTTP 응답이 여러 콘텐츠 인코딩을 포함함.
120:25	HTTP 응답이 잘못된 헤더 포딩을 포함함.
120:26	스팸 회선이 HTTP 응답 헤더 전에 발생함.
120:27	HTTP 응답이 헤더의 끝을 포함하지 않음.
120:28	잘못된 청크 크기가 발생하거나 청크 크기 뒤에 정크 문자가 있음.

Sun RPC 전처리기

RPC(원격 절차 호출) 표준화가 조각화된 RPC 레코드를 가져와 단일 레코드로 표준화하므로 규칙 엔진이 전체 레코드를 검사할 수 있습니다. 예를 들어, 공격자는 RPC `admind`가 실행되는 포트를 검색하려고 시도할 수 있습니다. 일부 UNIX 호스트는 RPC `admind`를 사용하여 원격 배포된 시스템 작업을 수행합니다. 호스트가 보안성이 낮은 인증을 수행할 경우, 악의적인 사용자가 원격 관리를 적용할 수 있습니다. Snort ID(SID) 575가 포함된 표준 텍스트 규칙(GID: 1)은 특정 위치의 콘텐츠를 검색해 이 공격을 탐지하여 부적절한 `portmap GETPORT` 요청을 식별합니다.

Sun RPC 전처리기 옵션

포트

트래픽을 표준화할 포트를 지정합니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다. 일반적인 RPC 포트는 111 및 32771입니다. 네트워크가 다른 포트에 RPC 트래픽을 전송할 경우 이들의 추가를 고려하십시오.

조각화된 **RPC** 레코드 탐지

조각화된 RPC 레코드를 탐지합니다.

규칙 106:1 및 106:5를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

1개의 패킷에서 여러 레코드 탐지

패킷(또는 리어셈블된 패킷)당 1개 이상의 RPC 요청을 탐지합니다.

규칙 106:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

단일 조각을 초과하는 조각화된 레코드 총합 탐지

현재 패킷 길이를 초과하는 리어셈블된 조각 레코드 길이를 탐지합니다.

규칙 106:3을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

1개의 패킷 크기를 초과하는 단일 조각 레코드 탐지

일부 레코드를 탐지합니다.

규칙 106:4를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

Sun RPC 전처리기 구성

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 2 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 3 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 4 **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **Sun RPC Configuration(Sun RPC** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 5 **Sun RPC Configuration(Sun RPC** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 6 Sun RPC 전처리기 옵션, 2269 페이지에서 설명하는 설정을 수정합니다.

단계 7 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 Sun RPC 전처리기 규칙(GID 106)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

SIP 전처리기

SIP(세션 시작 프로토콜)는 인터넷 텔레포니, 멀티미디어 컨퍼런싱, 인스턴트 메시징, 온라인 게임 및 파일 전송과 같은 클라이언트 애플리케이션의 한 명 이상의 사용자를 위한 하나 이상의 세션을 가진

통화 설정, 수정 및 세분화를 제공합니다. 각 SIP 요청의 *method(*메서드*)* 필드는 요청의 목적을 확인하고, Request-URI는 요청을 전송할 위치를 지정합니다. 각 SIP 응답의 상태 코드는 요청된 작업의 결과를 나타냅니다.

통화가 SIP를 사용하여 설치되면 RTP(실시간 전송 프로토콜)가 이후의 오디오 및 비디오 커뮤니케이션을 담당합니다. 세션의 이 부분은 경우에 따라 통화 채널, 데이터 채널 또는 오디오/비디오 데이터 채널로 지칭됩니다. RTP는 데이터 채널 파라미터 협상, 세션 공지 및 세션 초대를 위한 SIP 메시지 본문 내에서 SDP(세션 설명 프로토콜)를 사용합니다.

SIP 전처리기는 다음과 같은 작업을 담당합니다.

- SIP 2.0 트래픽 디코딩 및 분석
- SDP 데이터가 있는 경우 이를 포함하여 SIP 헤더 및 메시지 본문 추출, 추가 검사를 위해 규칙 엔진에 추출된 데이터 전달
- 다음 조건이 탐지되고 해당 전처리기 규칙이 활성화된 경우 이벤트를 생성:
  - 이상 징후 및 취약성 SIP 패킷 내의 알려진 취약성
  - 비순차 및 잘못된 통화 시퀀스
- 또는 통화 채널 무시

전처리기는 SIP 메시지 본문에 내장된 SDP 메시지에서 식별된 포트에 따라 RTP 채널을 식별하지만, 전처리기는 RTP 프로토콜 검사를 제공하지 않습니다.

SIP 전처리기를 사용하는 경우 다음 사항에 유의하십시오.

- UDP는 일반적으로 SIP에서 지원되는 미디어 세션을 전송합니다. UDP 스트림 전처리는 SIP 전처리기에 SIP 세션 추적을 제공합니다.
- SIP 규칙 키워드를 통해 SIP 패킷 헤더 또는 메시지 본문으로 이동하고 특정 SIP 메서드 또는 상태 코드의 패킷에 대한 탐지를 제한할 수 있습니다.

SIP 전처리기 옵션

다음 옵션의 경우, 1부터 65535바이트까지의 양수 값을 지정하거나 0을 지정해 연결된 규칙의 활성화 여부에 상관없이 옵션에서 이벤트 생성을 비활성화할 수 있습니다.

- 요청 **URI** 최대 길이
- 통화 **ID** 최대 길이
- 요청 이름 최대 길이
- 발신지 최대 길이
- 수신지 최대 길이
- 경유지 최대 길이
- 접촉 최대 길이

- 콘텐츠 최대 길이

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

SIP 트래픽을 위해 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

점검할 메서드

탐지할 SIP 메서드를 지정합니다. 다음 중 하나로 현재 정의된 SIP 메서드를 지정할 수 있습니다.

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

메서드는 대소문자를 구분하지 않습니다. 메서드 이름은 알파벳 문자, 숫자 및 밑줄 문자를 포함할 수 있습니다. 다른 특수 문자는 허용되지 않습니다. 메서드가 여러 개인 경우 쉼표로 구분하십시오.

향후 새 SIP 메서드가 정의될 수도 있기 때문에, 사용자의 구성은 현재 정의되지 않은 영문자열을 포함할 수 있습니다. 시스템은 최대 32개의 메서드까지 지원하는데, 최근 정의된 메서드 21개에 메서드 11개를 추가한 것입니다. 시스템은 사용자가 구성할 수 있는 정의되지 않은 모든 메서드를 무시합니다.

이 옵션에 지정한 메서드 외에도 총 32개의 메서드에는 침입 규칙에서 `sip_method` 키워드를 사용하여 지정된 메서드가 포함된다는 점에 유의하십시오.

세션 내 최대 대화 상자

스트림 세션 내에서 허용되는 최대 대화 상자 수를 지정합니다. 이 숫자보다 많은 대화 상자가 생성되는 경우 대화 상자 수가 지정된 최대 수를 초과하지 않을 때까지 가장 오래된 대화 상자부터 삭제됩니다. 1에서 4194303까지의 정수를 지정할 수 있습니다.

규칙 140:27을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정, 2024 페이지의 내용을 참조하십시오.

요청 **URI** 최대 길이

Request-URI 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:3이 활성화된 경우 더 긴 URI가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. 요청 URI 필드는 요청에 대한 대상 경로 또는 페이지를 나타냅니다.

통화 **ID** 최대 길이

요청 또는 응답 Call-ID 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:5가 활성화된 경우 더 긴 Call-ID가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. Call-ID 필드는 요청 및 응답에서 SIP 세션을 고유하게 식별합니다.

요청 이름 최대 길이

CSeq 트랜잭션 식별자에 지정된 메서드의 이름인 요청 이름에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:7이 활성화된 경우 더 긴 요청 이름이 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다.

발신지 최대 길이

요청 또는 응답 From 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:9가 활성화된 경우 더 긴 From 필드에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. From 필드는 메시지 초기자를 식별합니다.

수신지 최대 길이

요청 또는 응답 To 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:11이 활성화된 경우 더 긴 To 필드에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. To 필드는 메시지 수신자를 식별합니다.

경유지 최대 길이

요청 또는 응답 Via 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:13이 활성화된 경우 더 긴 Via 필드가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. Via 필드는 요청이 뒤따르는 경로를 제공하며, 응답에서는 수신 정보를 제공합니다.

접촉 최대 길이

요청 또는 응답 Contact 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:15가 활성화된 경우 더 긴 Contact 필드에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. Contact 필드는 이후의 메시지와 접촉할 위치를 지정하는 URI를 제공합니다.

콘텐츠 최대 길이

요청 또는 응답 메시지 본문의 콘텐츠에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:16이 활성화된 경우 더 긴 콘텐츠가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다.

오디오/비디오 데이터 채널 무시

데이터 채널 트래픽에 대한 검사를 활성화 및 비활성화합니다. 이 옵션을 활성화하면 전처리기는 비데이터 채널 SIP 트래픽에 대한 검사를 계속합니다.

관련 항목

SIP 키워드, 2142 페이지

SIP 전처리기 구성

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 2 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 3 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 4 **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SIP Configuration(SIP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 5 **SIP Configuration(SIP** 설정**)** 옆에 있는 편집 아이콘(수정( ))을 클릭합니다.

단계 6 SIP 전처리기 옵션, 2271 페이지에 설명된 대로 옵션을 수정합니다.

단계 7 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 SIP 전처리기 규칙(GID 140)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

추가 SIP 전처리기 규칙

다음 표의 SIP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 SIP 전처리기 규칙에서와 마찬가지로 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 이러한 규칙을 활성화해야 합니다.

표 ***227:*** 추가 ***SIP*** 전처리기 규칙

전처리기 규칙 **GID:SID**	다음 상황에서 트리거 됩니다.
140:1	전처리기가 시스템에서 허용되는 SIP 세션의 최대 수를 모니터링하고 있음.
140:2	요청된 Request_URI 필드가 SIP 요청에서 비어 있음.
140:4	Call-ID 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:6	SIP 요청 또는 응답 CSeq 필드의 시퀀스 번호 값이 231보다 작은 32비트 무부호 정수가 아님.
140:8	From 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:10	To 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:12	Via 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:14	요청된 Contact 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:17	UDP 트래픽의 단일 SIP 요청 또는 응답 패킷이 여러 메시지를 포함함. 이전 버전의 SIP는 여러 메시지를 지원했지만 SIP 2.0은 패킷당 1개의 메시지만 지원한다는 점에 유의하십시오.
140:18	UDP 트래픽의 SIP 요청 또는 응답에서 메시지 본문의 실제 길이가 SIP 요청 또는 응답 내 Content-Length 헤더 필드에 지정된 값과 다름.
140:19	전처리기가 SIP 응답의 CSeq 필드에서 메서드 이름을 인식하지 못함.
140:20	SIP 서버가 입증된 초대 메시지에 이의를 제기하지 않음. 이는 InviteReplay 청구 공격의 경우 발생한다는 점에 유의하십시오.
140:21	통화가 설정되기 전에 세션 정보가 변경됨. 이는 FakeBusy 청구 공격의 경우 발생한다는 점에 유의하십시오.
140:22	응답 상태 코드가 3자리 수가 아님.
140:23	Content-Type(콘텐츠 유형) 헤더 필드가 콘텐츠 형식을 지정하지 않고 메시지 텍스트가 데이터를 포함함.
140:24	SIP 버전이 1, 1.1, 또는 2.0가 아님.

전처리기 규칙 **GID:SID**	다음 상황에서 트리거 됩니다.
140:25	CSeq 헤더 및 메서드 필드에 지정된 메서드가 SIP 요청과 일치하지 않음.
140:26	전처리기가 SIP 요청 방법 필드에서 명명된 메서드를 인식하지 못함.

GTP 전처리기

GTP(GPRS[General Service Packet Radio] 터널링 프로토콜)는 GTP 코어 네트워크를 통한 통신을 제공합니다. GTP 전처리기는 GTP 트래픽 내 이상 징후를 탐지하고 검사를 위해 규칙 엔진에 명령 채널 신호 메시지를 전달합니다. `gtp_version`, `gtp_type` 및 `gtp_info` 규칙 키워드를 사용하여 익스플로잇 탐지를 위해 GTP 명령 채널 트래픽을 검사할 수 있습니다.

단일 구성 옵션을 사용하면 전처리기가 GTP 명령 채널 메시지를 검사하는 포트의 기본 설정을 변경할 수 있습니다.

GTP 전처리기 규칙

GTP 전처리기 규칙이 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하게 하려면 다음 표에서 해당 규칙을 활성화해야 합니다.

표 ***228: GTP*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
143:1	전처리기가 유효하지 않은 메시지 길이를 탐지하면 이벤트를 생성합니다.
143:2	전처리기가 유효하지 않은 정보 요소 길이를 탐지하면 이벤트를 생성합니다.
143:3	전처리기가 비순차적 정보 요소를 탐지하면 이벤트를 생성합니다.

GTP 전처리기 설정

이 절차를 수행하여 GTP 전처리기가 GTP 명령 메시지를 모니터링하는 포트를 수정할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 2 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 3 왼쪽 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 4 **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **GTP Command Channel Configuration(GTP** 명령 채널 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 5 **GTP Command Channel Configuration(GTP** 명령 채널 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 6 **Ports(**포트**)** 값을 입력합니다.

포트가 여러 개인 경우 쉼표로 구분하십시오.

단계 7 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 활성화하려면 GTP 전처리기 규칙(GID 143)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

IMAP 전처리기

Internet Message Application Protocol(인터넷 메시지 애플리케이션 프로토콜, IMAP)을 사용하여 원격 IMAP 서버의 이메일을 검색합니다. IMAP 전처리기는 서버-클라이언트 IMAP4 트래픽을 검사하고 관련 전처리기 규칙이 활성화되면 변칙 트래픽에 이벤트를 생성합니다. 전처리기는 또한 클라이언트-서버 IMAP4 트래픽의 이메일 첨부 파일을 추출하여 디코딩하고 규칙 엔진에 첨부 파일 데이터를 보낼 수 있습니다. 첨부 파일 데이터를 지정할 때 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다.

여러 첨부 파일이 있는 경우 추출 및 디코딩에 포함되며, 여러 패킷을 포괄하는 큰 첨부 파일도 포함됩니다.

IMAP 전처리기 옵션

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 다음 상황에서 **Base64 Decoding Depth(Base64** 디코딩 수준**)**, **7-Bit/8-Bit/Binary Decoding Depth(7**비트**/8**비트**/**이진 디코딩 수준**)**, **Quoted-Printable Decoding Depth(**따옴표로 묶인 인쇄 가능한 디코딩 수준**)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix** 디코딩 수준**)** 옵션의 값이 서로 다를 때 가장 높은 값이 사용된다는 점에 유의하십시오.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

IMAP 트래픽을 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Base64 디코딩 수준

Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

이 옵션이 활성화된 경우, 규칙 141:4를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

7비트**/8**비트**/**이진 디코딩 수준

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 데이터의 최대 바이트를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 양수 값을 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 141:6을 활성화하여 추출이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 손상된 데이터로 인해 추출이 실패할 수 있습니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

QP(Quoted-Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 QP 인코딩 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 141:5를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

Unix-to-Unix 디코딩 수준

Unix-to-Unix로 인코딩된(uuencoded) 각 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 비인코딩 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 141:7을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

관련 항목

file_data 키워드, 2180 페이지

IMAP 전처리기 구성

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **IMAP Configuration(IMAP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **IMAP Configuration(IMAP** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** IMAP 전처리기 옵션, 2278 페이지에서 설명하는 설정을 수정합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 활성화하려면 IMAP 전처리기 규칙(GID 141)을 활성화합니다(침입 규칙 상태 설정, 2024 페이지 참조).
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

침입 및 네트워크 분석 정책의 레이어, 1979 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

추가 **IMAP** 전처리기 규칙

다음 표의 IMAP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 IMAP 전처리기 규칙에서와 마찬가지로 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 이러한 규칙을 활성화해야 합니다.

표 ***229:*** 추가 ***IMAP*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
141:1	전처리기가 RFC 3501에 정의되지 않은 클라이언트 명령을 탐지하면 이벤트를 생성합니다.
141:2	전처리기가 RFC 3501에 정의되지 않은 서버 응답을 탐지하면 이벤트를 생성합니다.
141:3	전처리기가 시스템에서 허용되는 최대 메모리 양을 사용하는 경우 이벤트를 생성합니다. 여기서, 전처리기는 메모리를 사용할 수 있을 때까지 디코딩을 중지합니다.

POP 전처리기

Post Office Protocol(포스트 오피스 프로토콜, POP)을 사용하여 원격 POP 서버의 이메일을 검색합니다. POP 전처리기는 서버-클라이언트 POP3 트래픽을 검사하고 관련 전처리기 규칙이 활성화되면 변칙 트래픽에 이벤트를 생성합니다. 전처리기는 또한 클라이언트-서버 POP3 트래픽의 이메일 첨부 파일을 추출 및 디코딩하고 규칙 엔진에 첨부 파일 데이터를 보낼 수 있습니다. 첨부 파일 데이터를 지정할 때 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다.

여러 첨부 파일이 있는 경우 추출 및 디코딩에 포함되며, 여러 패킷을 포괄하는 큰 첨부 파일도 포함됩니다.

POP 전처리기 옵션

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 다음 상황에서 **Base64 Decoding Depth(Base64** 디코딩 수준**)**, **7-Bit/8-Bit/Binary Decoding Depth(7**비트**/8**비트**/**이진 디코딩 수준**)**, **Quoted-Printable Decoding Depth(**따옴표로 묶인 인쇄 가능한 디코딩 수준**)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix** 디코딩 수준**)** 옵션의 값이 서로 다를 때 가장 높은 값이 사용된다는 점에 유의하십시오.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

POP 트래픽을 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Base64 디코딩 수준

Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

이 옵션이 활성화된 경우, 규칙 142:4를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

7비트**/8**비트**/**이진 디코딩 수준

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 데이터의 최대 바이트를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 양수 값을 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 142:6을 활성화하여 추출이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 손상된 데이터로 인해 추출이 실패할 수 있습니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

QP(Quoted-Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 QP 인코딩 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 142:5를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

Unix-to-Unix 디코딩 수준

Unix-to-Unix로 인코딩된(uuencoded) 각 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 비인코딩 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 142:7을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지
file_data 키워드, 2180 페이지

POP 전처리기 구성

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **POP Configuration(POP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **POP Configuration(POP** 구성**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** POP 전처리기 옵션, 2281 페이지에서 설명하는 설정을 수정합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 활성화하려면 POP 전처리기 규칙(GID 142)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

추가 **POP** 전처리기 규칙

다음 표의 POP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 POP 전처리기 규칙에서와 마찬가지로 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 이러한 규칙을 활성화해야 합니다.

표 ***230:*** 추가 ***POP*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
142:1	전처리기가 RFC 1939에 정의되지 않은 클라이언트 명령을 탐지하면 이벤트를 생성합니다.
142:2	전처리기가 RFC 1939에 정의되지 않은 서버 응답을 탐지하면 이벤트를 생성합니다.
142:3	전처리기가 시스템에서 허용되는 최대 메모리 양을 사용하는 경우 이벤트를 생성합니다. 여기서, 전처리기는 메모리를 사용할 수 있을 때까지 디코딩을 중지합니다.

SMTP 전처리기

SMTP 전처리기는 규칙 엔진이 SMTP 명령을 표준화하도록 지시합니다. 전처리기는 또한 클라이언트-서버 트래픽의 이메일 첨부 파일을 추출하고 디코딩할 수 있습니다. 그리고, SMTP 트래픽에서 트리거된 침입 이벤트를 표시할 경우 이메일 파일 이름, 주소 및 헤더 데이터를 소프트웨어 버전에 따라 추출하여 컨텍스트를 제공할 수 있습니다.

SMTP 전처리기 옵션

표준화를 활성화하거나 비활성화하고, SMTP 디코더가 탐지하는 변칙 트래픽 유형을 제어하는 옵션을 구성할 수 있습니다.

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 다음 상황에서 **Base64 Decoding Depth(Base64** 디코딩 수준**)**, **7-Bit/8-Bit/Binary Decoding Depth(7**비트**/8**비트**/**이진 디코딩 수준**)**, **Quoted-Printable Decoding Depth(**따옴표로 묶인 인쇄 가능한 디코딩 수준**)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix** 디코딩 수준**)** 옵션의 값이 서로 다를 때 가장 높은 값이 사용된다는 점에 유의하십시오.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

SMTP 트래픽을 표준화할 포트를 지정합니다. 0 이상의 값을 지정할 수 있습니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

상태 저장 검사

이를 선택하면, SMTP 디코더가 상태를 저장하고 개별 패킷을 위한 세션 컨텍스트를 제공하며, 리어셈블한 세션만 검사할 수 있습니다. 이를 취소하면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

표준화

`All(모두)`로 설정된 경우, 모든 명령을 표준화합니다. 명령 다음에 나오는 하나 이상의 공백 문자를 확인합니다.

`None(없음)`으로 설정된 경우, 어떤 명령도 표준화하지 않습니다.

`Cmds`로 설정된 경우, **Custom Commands(**맞춤형 명령**)**에 나열된 명령을 표준화합니다.

사용자 지정 명령

Normalize(표준화**)**가 `Cmds`로 설정된 경우, 나열된 명령을 표준화합니다.

텍스트 상자에서 표준화되어야 하는 명령을 지정합니다. 명령 다음에 나오는 하나 이상의 공백 문자를 확인합니다.

스페이스(ASCII 0x20) 및 탭(ASCII 0x09) 문자는 표준화를 위한 공백 문자로 간주됩니다.

데이터 무시

메일 데이터를 처리하지 않습니다. MIME 메일 헤더 데이터만 처리합니다.

TLS 데이터 무시

Transport Layer Security(전송 레이어 보안) 프로토콜의 암호화된 데이터를 처리하지 않습니다.

경고 없음

동반되는 전처리기 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

알 수 없는 명령 탐지

SMTP 트래픽에서 알 수 없는 명령을 탐지합니다.

규칙 124:5를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

명령줄 최대 길이

SMTP 명령줄이 이 값보다 길 경우 이를 탐지합니다. 명령줄 길이를 탐지하지 않으려면 0을 지정합니다.

간단한 메일 전송 프로토콜의 네트워크 작업 그룹 사양인 RFC 2821은 명령줄 최대 길이로 512를 권장합니다.

규칙 124:1을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

헤더 행 최대 길이

SMTP 데이터 헤더 행이 이 값보다 길 경우 이를 탐지합니다. 데이터 헤더 행 길이를 탐지하지 않으려면 0을 지정합니다.

규칙 124:2 및 124:7을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

응답 회선 최대 길이

SMTP 응답 회선이 이 값보다 길 경우 이를 탐지합니다. 응답 회선 길이를 탐지하지 않으려면 0을 지정합니다.

RFC 2821는 응답 회선 최대 길이로 512를 권장합니다.

규칙 124:3을 활성화하여 이 옵션에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 해당 옵션이 활성화되면 **Alt Max Command Line Len(**대안적 명령줄 최대 길이**)**에 대해서도 가능합니다.

대안적 명령줄 최대 길이

지정된 모든 명령에 대한 SMTP 명령줄이 이 값보다 길 경우 이를 탐지합니다. 지정된 명령에 대한 명령줄 길이를 탐지하지 않으려면 0을 지정합니다. 여러 명령에 대해 다양한 기본 회선 길이가 설정됩니다.

이 설정은 지정된 명령에 대한 Max Command Line Len(명령줄 최대 길이) 설정을 무시합니다.

규칙 124:3을 활성화하여 이 옵션에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 해당 옵션이 활성화되면 **Max Response Line Len(**최대 응답 줄 길이**)**에 대해서도 가능합니다.

유효하지 않은 명령

이 명령어가 클라이언트 측에서 전송되는지 여부를 탐지합니다.

규칙 124:6을 활성화하여 이 옵션 및 **Invalid Commands(**유효하지 않은 명령**)**에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

유효한 명령

이 목록에 있는 명령을 허용합니다.

이 명령이 비어 있더라도 전처리기는 다음의 유효한 명령을 허용합니다. ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

참고 RCPT TO 및 MAIL FROM은 SMTP 명령입니다. 전처리기 구성은 RCPT와 MAIL의 명령 이름을 각각 사용합니다. 해당 코드 안에서, 전처리기는 RCPT와 MAIL을 정확한 명령 이름에 매핑합니다.

규칙 124:4를 활성화하여 이 옵션에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 해당 옵션이 구성되면 **Invalid Command(**유효하지 않은 명령**)**에 대해서도 가능합니다.

데이터 명령

SMTP DATA 명령이 RFC 5321당 데이터를 전송하는 것과 동일한 방식으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

이진 데이터 명령

BDAT 명령이 RFC 3030당 데이터를 전송하는 것과 유사한 방식으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

인증 명령

클라이언트와 서버 간의 인증 교환을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

xlink2state 탐지

X-Link2State Microsoft Exchange 버퍼 데이터 오버플로 공격의 일부인 패킷을 탐지합니다. 인라인 배포에서, 시스템은 해당 패킷을 삭제할 수 있습니다.

규칙 124:8을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

Base64 디코딩 수준

Ignore Data(데이터 무시**)**가 비활성화된 경우, Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수 값을 지정할 수도 있고 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(**데이터 무시**)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

이 옵션이 활성화된 경우, 규칙 124:10을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 잘못된 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

이 옵션은 **Enable MIME Decoding(MIME** 디코딩 활성화**)** 및 **Maximum MIME Decoding Depth(MIME** 디코딩 최대 수준**)**와 같이 더 이상 사용되지 않는 옵션을 대체한다는 점에 유의하십시오. 이 옵션은 이전 버전과의 호환성을 위해 기존 침입 정책에서 계속 지원됩니다.

7비트**/8**비트**/**이진 디코딩 수준

Ignore Data가 비활성화된 경우 디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 최대 데이터 바이트를 수를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 양수 값을 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다. **Ignore Data**가 선택된 경우 프리프로세서는 데이터를 추출하지 않습니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

Ignore Data(데이터 무시**)**가 비활성화된 경우, QP(Quoted−Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다.

1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 QP로 인코딩된 모든 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(**데이터 무시**)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

이 옵션이 활성화된 경우, 규칙 124:11을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 잘못된 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

Unix−to−Unix 디코딩 수준

Ignore Data(데이터 무시**)**가 비활성화된 경우, Unix−to−Unix로 인코딩된(uuencoded) 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 uuencoded 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(**데이터 무시**)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

이 옵션이 활성화된 경우, 규칙 124:13을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 잘못된 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

MIME 첨부 파일 이름 로그

MIME Content-Disposition 헤더에서 MIME 첨부 파일 이름의 추출을 활성화하고 파일 이름을 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 파일 이름이 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Attachment(이메일 첨부 파일) 열에서 이벤트와 관련된 파일 이름을 볼 수 있습니다.

수신지 주소 로그

SMTP RCPT TO 명령에서 수신자 전자 메일 주소의 추출을 활성화하고 수신자 주소를 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 수신자가 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Recipient(전자 메일 수신자) 열에서 이벤트와 관련된 수신자를 볼 수 있습니다.

발신지 주소 로그

SMTP MAIL FROM 명령에서 발신자 전자 메일 주소의 추출을 활성화하고 발신자 주소를 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 발신자 주소가 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Sender(이메일 발신자) 열에서 이벤트와 관련된 발신자를 볼 수 있습니다.

헤더 로그

전자 메일 헤더의 추출을 활성화합니다. 추출할 바이트 수는 **Header Log Depth(**헤더 로그 수준**)**에 지정된 값에 따라 결정됩니다.

이메일 헤더 데이터를 패턴으로 사용하는 침입 규칙을 작성하려면 `content` 또는 `protected_content` 키워드를 사용할 수 있습니다. 또한 침입 이벤트 패킷 보기에서 추출한 전자 메일 헤더를 볼 수 있습니다.

헤더 로그 수준

Log Headers(헤더 로그**)**가 활성화된 경우 추출할 전자 메일 헤더의 바이트 수를 지정합니다. 0~20480 바이트를 지정할 수 있습니다. 값을 0으로 지정하면 **Log Headers(**헤더 로그**)**가 비활성화됩니다.

관련 항목

기본 content 또는 protected_content 키워드 인수, 2090 페이지

SMTP 복호화 구성

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 2 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 3 탐색창에서 **Settings(**설정**)**를 클릭합니다.

단계 4 **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SMTP Configuration(SMTP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 5 **SMTP Configuration(SMTP** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 6 SMTP 전처리기 옵션, 2284 페이지에 설명된 대로 옵션을 수정합니다.

단계 7 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 SMTP 전처리기 규칙(GID 124)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

SSH 전처리기

SSH 전처리기는 다음을 탐지합니다.

- 시도-응답 버퍼 오버플로 익스플로잇
- CRC-32 익스플로잇

- SecureCRT SSH 클라이언트 버퍼 오버플로 익스플로잇
- 프로토콜 불일치
- 잘못된 SSH 메시지 방향
- 버전 1 또는 2 이외의 다른 버전 문자열

시도-응답 버퍼 오버플로 및 CRC-32 공격은 키 교환 이후에 발생하며, 따라서 암호화됩니다. 두 공격 모두 인증 시도 직후 서버에 20KB가 넘는 터무니없이 큰 페이로드를 보냅니다. CRC-32 공격은 SSH 버전 1에만 적용되고, 시도-응답 버퍼 오버플로 익스플로잇은 SSH 버전 2에만 적용됩니다. 버전 문자열은 세션 시작 시 읽혀집니다. 버전 문자열의 차이를 제외하면, 두 공격 모두 동일하게 취급됩니다.

SecureCRT SSH 익스플로잇 및 프로토콜 불일치 공격은 키 교환 전에, 보안 연결을 하려고 할 때 발생합니다. SecureCRT 익스플로잇은 버퍼 오버플로를 야기하는 클라이언트에 과도하게 긴 프로토콜 식별자 문자열을 보냅니다. 프로토콜 불일치는 비SSH 클라이언트 애플리케이션이 보안 SSH 서버에 연결을 시도하거나 서버와 클라이언트 버전 번호가 일치하지 않는 경우 발생합니다.

전처리기가 지정된 포트 또는 포트 목록의 트래픽을 검사하거나 자동으로 SSH 트래픽을 탐지하도록 설정할 수 있습니다. 전처리기는 지정된 수의 암호화된 패킷이 지정된 수의 바이트 내부를 통과할 때까지 또는 지정된 최대 수의 바이트가 지정된 수의 패킷 내부에서 초과될 때까지 계속해서 SSH 트래픽을 검사합니다. 최대 수의 바이트가 초과된 경우, CRC-32(SSH 버전 1) 또는 시도-응답 버퍼 오버플로(SSH 버전 2) 공격이 발생한 것으로 가정합니다. 전처리기는 설정하지 않아도 버전 1 또는 2 이외의 다른 모든 버전의 문자열 값을 탐지한다는 점에 유의하십시오.

또한 SSH 전처리기는 무차별 암호 대입 공격을 처리하지 않는다는 점도 주의해야 합니다.

SSH 전처리기 옵션

전처리기는 다음 사항 중 하나가 발생할 경우 세션에 대한 트래픽 검사를 중지합니다.

- 서버와 클라이언트 간 유효한 교환이 이 암호화된 패킷의 수만큼 발생하며 연결은 지속됩니다.
- **Number of Bytes Sent Without Server Response(**서버 응답 없이 전송된 바이트 수**)**에 도달한 후에 검사할 암호화된 패킷 수에 도달하며 공격이 있는 것으로 간주됩니다.

Number of Encrypted Packets to Inspect(검사할 암호화된 패킷 수**)**가 경과되는 동안 유효한 각 서버 응답은 **Number of Bytes Sent Without Server Response(**서버 응답 없이 전송된 바이트 수**)**를 재설정하며 패킷 카운트가 계속됩니다.

다음의 예시 SSH 전처리기 구성을 고려하십시오.

- **Server Ports(**서버 포트**)**: 22
- **Autodetect Ports(**자동 탐지된 포트**)**: 꺼짐
- **Maximum Length of Protocol Version String(**프로토콜 버전 문자열의 최대 길이**)**: 80
- **Number of Encrypted Packets to Inspect(**검사할 암호화된 패킷 수**)**: 25
- **Number of Bytes Sent Without Server Response(**서버 응답 없이 전송된 바이트 수**)**: 19,600

- 모든 탐지 옵션이 활성화됩니다.

예제에서, 전처리기는 포트 22에서만 트래픽을 검사합니다. 즉 연결 자동 탐지가 비활성화되므로 지정된 포트에서만 검사합니다.

또한, 다음 사항 중 하나가 발생할 경우 예제의 전처리기는 트래픽 검사를 중지합니다.

- 클라이언트는 누적해서 19,600 미만의 바이트를 포함하는 25개의 암호화된 패킷을 전송합니다. 공격이 전혀 없는 것으로 가정합니다.
- 클라이언트는 25개의 암호화된 패킷으로 19,600 이상의 바이트를 전송합니다. 이 경우, 예제의 세션이 SSH 버전 2 세션이므로 전처리기는 해당 공격이 시도-응답 버퍼 오버플로 익스플로잇이라고 간주합니다.

예제에서 전처리기는 트래픽을 처리하는 동안 발생하는 다음과 같은 모든 징후를 탐지합니다.

- 80바이트보다 큰 버전 문자열에서 트리거되었고 SecureCRT 익스플로잇을 나타내는 서버 오버플로
- 프로토콜 불일치
- 잘못된 방향으로 흐르는 패킷

마지막으로, 전처리기는 버전 1 또는 버전 2 외에도 자동으로 모든 버전 문자열을 탐지합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

서버 포트

SSH 전처리기가 트래픽을 검사할 포트를 지정합니다.

단일 포트 또는 쉼표로 구분된 포트 목록을 설정할 수 있습니다.

자동 탐지된 포트

전처리기는 자동으로 SSH 트래픽을 탐지할 수 있습니다.

이 옵션을 선택하면, 전처리기는 SSH 버전 번호에 대한 모든 트래픽을 검사합니다. 이는 클라이언트와 서버 패킷 모두가 버전 번호를 포함하지 않을 때 처리를 중지합니다. 이를 비활성화하면, 전처리기는 **Server Ports(**서버 포트**)** 옵션에서 확인된 트래픽만 검사합니다.

검사할 암호화된 패킷 수

세션당 검토할 스트림 리어셈블 암호화된 패킷 수를 지정합니다.

이 옵션을 0으로 설정하면 모든 트래픽이 통과할 수 있습니다.

검사할 암호화된 패킷 수를 줄이면 일부 공격이 탐지를 이스케이프할 수 있습니다. 검사할 암호화된 패킷 수를 늘리면 성능에 부정적인 영향을 줄 수 있습니다.

서버 응답 없이 전송된 바이트 수

시도-응답 버퍼 오버플로 공격 또는 CRC-32 공격이 있는 것으로 가정하기 전에 SSH 클라이언트가 응답을 받지 않고 서버에 보낼 수 있는 최대 바이트 수를 지정합니다.

전처리기가 시도-응답 버퍼 오버플로 또는 CRC-32 익스플로잇에서 오탐을 생성하는 경우 이 옵션의 값을 높이십시오.

프로토콜 버전 문자열의 최대 길이

문자열을 SecureCRT 익스플로잇으로 간주하기 전에 서버의 버전 문자열에 허용할 최대 바이트 수를 지정합니다.

시도-응답 버퍼 오버플로 공격 탐지

시도-응답 버퍼 오버플로 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:1을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. SFTP 세션이 때때로 규칙 128:1을 트리거할 수 있습니다.

SSH1 CRC-32 공격 탐지

CRC-32 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:2를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

서버 오버플로 탐지

SecureCRT SSH 클라이언트 버퍼 오버플로 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:3을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

프로토콜 불일치 탐지

프로토콜 불일치에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:4를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

오류 메시지 방향 탐지

트래픽이 잘못된 방향으로 흐르는 경우(즉, 가정한 서버가 클라이언트 트래픽을 생성하거나, 클라이언트가 서버 트래픽을 생성한 경우) 탐지를 활성화 또는 비활성화합니다.

규칙 128:5를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

지정된 페이로드에 대해 유효하지 않은 페이로드 크기 탐지

SSH 패킷에서 지정한 길이가 IP 헤더에 지정된 총 길이와 일관되지 않고 메시지 끝이 잘렸을 때, 즉, 전체 SSH 헤더에 충분한 데이터가 있지 않은 경우에 유효하지 않은 페이로드 크기를 가진 패킷 탐지를 활성화 또는 비활성화합니다.

규칙 128:6을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

유효하지 않은 버전 문자열 탐지

이를 활성화할 경우, 전처리기가 설정 없이도 버전 1 또는 2 이외의 다른 모든 버전의 문자열을 탐지한다는 점에 유의하십시오.

규칙 128:7을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

SSH 전처리기 구성

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SSH Configuration(SSH** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **SSH Configuration(SSH** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** SSH 전처리기 옵션, 2290 페이지에 설명된 대로 옵션을 수정합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 활성화하려면 SSH 전처리기 규칙(GID 128)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

SSL 전처리기

SSL 전처리기는 SSL 검사의 설정을 허용합니다. 이를 통해 암호화된 트래픽을 차단 또는 해독하거나 액세스 컨트롤로 트래픽을 검사할 수 있습니다. SSL 검사의 설정 여부와 상관없이 SSL 전처리기는 트래픽에서 탐지된 SSL 핸드셰이크 메시지를 분석하고, 세션이 암호화되는 시기를 결정합니다. 암호화된 트래픽을 식별하면 시스템은 암호화된 페이로드의 침입 및 파일 검사를 중지하는데, 이는 오탐을 줄이고 성능을 향상하는 데 도움이 됩니다.

SSL 전처리기는 또한 암호화된 트래픽에서 Heartbleed 버그를 악용하려는 시도를 탐지하고, 그러한 익스플로잇을 탐지하는 경우 이벤트를 생성합니다.

세션이 암호화되면 트래픽의 침입 및 악성코드 검사를 일시 중단할 수 있습니다. 또한 SSL 검사를 구성하는 경우 SSL 전처리기는 액세스 컨트롤로 차단, 해독 또는 검사할 수 있는 암호화된 트래픽을 식별합니다.

SSL 전처리기를 이용한 암호화된 트래픽 해독은 라이선스가 필요하지 않습니다. 악성코드 및 침입에 대한 암호화된 페이로드의 검사 정지, Heartbleed 버그 익스플로잇 탐지 등 다른 모든 SSL 전처리기 기능에는 Protection(보호) 라이선스가 필요합니다.

SSL 전처리 작동 방식

SSL 검사를 구성한 경우, SSL 전처리기는 암호화된 데이터의 침입 및 파일 검사를 중지하고 SSL 정책으로 암호화된 트래픽을 검사합니다. 이는 오탐을 줄이는 데 도움이 됩니다. SSL 전처리기는 SSL 핸드쉐이크를 검사할 때 상태 정보를 유지하며, 해당 세션에 대한 상태 및 SSL 버전을 모두 추적합니다. 세션 상태가 암호화되었음을 전처리기가 탐지하면 시스템은 해당 세션의 트래픽이 암호화되었음을 표시합니다. 암호화가 설정된 경우 암호화된 세션의 모든 패킷에 대한 처리를 중지하도록, 그리고 Heartbleed 버그를 악용하려는 시도를 탐지할 경우 이벤트를 생성하도록 시스템을 구성할 수 있습니다.

SSL 전처리기는 각 패킷에 대해 트래픽이 IP 헤더, TCP 헤더 및 TCP 페이로드를 포함하며 SSL 전처리를 위해 지정된 포트에서 발생한다는 것을 확인합니다. 다음 시나리오는 트래픽 검증을 위해 트래픽이 암호화되었는지 여부를 확인합니다.

- 시스템은 세션 내 모든 패킷을 관찰하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능은 활성화되지 않으며, 서버와 클라이언트 모두로부터 수신된 완료됨 메시지와 애플리케이션

레코드가 있지만 경고 레코드는 없는 각 측면으로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.

- 시스템은 트래픽 일부를 유실하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능은 활성화되지 않으며, 경고 레코드로 응답되지 않은 애플리케이션 레코드를 가진 각 측면으로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 세션 내 모든 패킷을 관찰하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능이 활성화되며, 클라이언트로부터 수신된 완료됨 메시지 및 애플리케이션 레코드가 있지만 경고 레코드는 없는 각 클라이언트로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 트래픽 일부를 유실하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능이 활성화되며, 경고 레코드로 응답되지 않은 애플리케이션 레코드를 가진 각 클라이언트로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.

암호화된 트래픽 처리를 중단하도록 선택할 경우, 시스템은 세션이 암호화된 것으로 표시한 후에는 세션의 이후 패킷을 무시합니다.

또한, SSL 핸드쉐이크 중, 전처리기는 하트비트 요청과 응답을 모니터링합니다. 전처리기는 다음을 탐지하는 경우 이벤트를 생성합니다.

- 페이로드 자체보다 큰 페이로드 길이 값을 포함하는 하트비트 요청
- Max Heartbeat Length(하트비트 최대 길이) 필드에 저장된 값보다 큰 하트비트 응답

참고 `ssl_state` 및 `ssl_version` 키워드를 규칙에 추가하여 SSL 상태 또는 버전 정보를 규칙과 함께 사용할 수 있습니다.

관련 항목

SSL 키워드, 2133 페이지
TLS/SSL 검사 요구 사항

SSL 전처리기 옵션

참고 시스템 제공 네트워크 분석 정책은 기본적으로 SSL 전처리기를 활성화합니다. Cisco는 암호화된 트래픽이 네트워크를 통과할 것으로 예상하는 경우 맞춤형 구축에서 SSL 전처리기를 비활성화하지 않을 것을 권장합니다.

SSL 검사를 구성하지 않으면 시스템은 암호화된 트래픽에서 해독 없이 악성코드와 침입을 검사하려고 시도합니다. SSL 전처리기를 활성화하면, 세션이 암호화되는 경우를 탐지합니다. SSL 전처리기를 활성화한 후, 규칙 엔진은 전처리기를 호출하여 SSL 상태 및 버전 정보를 얻을 수 있습니다. 침입 정책에서 `ssl_state` 및 `ssl_version` 키워드를 사용하여 규칙을 활성화하는 경우 SSL 프리프로세서도 활성화해야 합니다.

포트

SSL 전처리기가 암호화된 세션의 트래픽을 모니터링할 포트를 쉼표로 구분하여 지정합니다. 이 필드에 포함된 포트만 암호화된 트래픽을 검사합니다.

참고 SSL 전처리기가 SSL 모니터링을 위해 지정된 포트를 통해 비 SSL 트래픽을 탐지하는 경우, 해당 트래픽을 SSL 트래픽으로 디코딩하려고 시도한 다음 이를 손상된 것으로 표시합니다.

암호화된 트래픽 검사 중지

세션이 암호화된 것으로 표시되면 세션의 트래픽에 대한 검사를 활성화하거나 비활성화합니다.

암호화된 세션의 검사와 리어셈블리를 비활성화하려면 이 옵션을 활성화하십시오. SSL 전처리기가 이 세션에 대한 상태를 유지하므로 세션의 모든 트래픽의 검사를 비활성화할 수 있습니다. 이 옵션을 활성화하면 세션의 일부 패킷을 검증해 플로우가 심층 검사를 우회한 후 암호화되게 합니다. 모든 우회 세션은 **show snort statistics** 명령에 대한 응답에 표시되는, 빨리 감은 플로우 숫자를 높입니다. 또한 심층 검사를 우회하기 때문에 연결 이벤트에서의 이니시에이터와 반응기 바이트가 정확하지 않습니다. Snort가 검사한 패킷만 포함하며 심층 검사 우회 후의 패킷은 포함하지 않기 때문에, 실제 세션 값 미만이 됩니다. 이 동작은 연결 요약 이벤트와 위젯에 표시되는 모든 트래픽 값에 적용됩니다.

다음 두 조건 충족 시, 시스템은 암호화된 세션의 트래픽 검사를 중지합니다.

- SSL 전처리기가 활성화됨
- 이 옵션이 선택됨

이 옵션의 선택을 취소하면 **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 옵션을 수정할 수 없습니다.

서버 측 데이터가 신뢰됨

암호화된 트래픽 검사 중지가 활성화되면, 클라이언트측 트래픽에만 기반을 두는 암호화된 트래픽 식별이 활성화됩니다.

최대 하트비트 길이

바이트 수를 지정하면 Heartbleed 버그 악용 시도에 대한 SSL 핸드셰이크 내의 하트비트 요청 및 응답 검사를 활성화할 수 있습니다. `1~65535`까지의 정수를 지정할 수 있으며, `0`을 지정하여 옵션을 비활성화할 수도 있습니다.

전처리기가 실제 페이로드 길이보다 큰 페이로드 길이를 가진 하트비트 요청을 감지하고 규칙 137:3이 활성화되거나, 규칙 137:4가 활성화되었을 때 이 옵션에 설정된 값보다 하트비트 응답이 크다면 전처리기는 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다.

SSL 전처리기 구성

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 2 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 3 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 4 **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SSL Configuration(SSL** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 5 **SSL Configuration(SSL** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 6 SSL 전처리기 옵션, 2295 페이지에서 설명하는 설정을 수정합니다.

- **Ports(**포트**)** 필드에 값을 입력합니다. 쉼표로 여러 개의 값을 구분합니다.
- **Stop inspecting encrypted traffic(**암호화된 트래픽 검사 중지**)** 확인란을 선택하거나 선택 취소합니다.
- **Stop inspecting encrypted traffic(**암호화된 트래픽 검사 중지**)**를 선택했다면 **Server side data is trusted(**서버 측 데이터가 신뢰됨**)**을 선택하거나 선택 취소합니다.
- **Max Heartbeat Length(**최대 하트비트 길이**)** 필드에 값을 입력합니다.

  팁 0 값은 이 옵션을 비활성화합니다.

단계 7 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 활성화하려면 SSL 전처리기 규칙(GID 137)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지
TLS/SSL 검사 요구 사항

SSL 전처리기 규칙

이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 SSL 전처리기 규칙(GID 137)을 활성화합니다.

다음 표는 사용자가 활성화할 수 있는 SSL 전처리기 규칙에 대해 설명합니다.

표 ***231: SSL*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
137:1	ServerHello 메시지 후에 나타나는 ClientHello 메시지를 탐지합니다. 해당 메시지는 유효하지 않으며 이상 작업으로 간주됩니다.
137:2	SSL 전처리기 옵션인 **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능이 비활성화되면 ClientHelloo 없는 ServerHello 메시지를 탐지합니다. 해당 메시지는 유효하지 않으며 이상 작업으로 간주됩니다.
137:3	SSL 전처리기 옵션인 **Max Heartbeat Length(**최대 하트비트 길이**)**에 0이 아닌 값이 포함된 경우 페이로드 길이가 페이로드 자체보다 큰 하트비트 요청을 탐지합니다. 이는 Heartbleed 버그를 악용하려는 시도를 나타냅니다.
137:4	SSL 전처리기 옵션인 **Max Heartbeat Length(**하트비트 최대 길이**)**에 지정된 0이 아닌 값보다 큰 하트비트 응답을 탐지합니다. 이는 Heartbleed 버그를 악용하려는 시도를 나타냅니다.

90 장

SCADA 프리프로세서

다음 주제에서는 SCADA(감독 제어 및 데이터 획득) 프로토콜용 전처리기와 이를 구성하는 방법을 설명합니다.

- SCADA 전처리기 소개, 2299 페이지
- SCADA 전처리기 라이선스 요구 사항, 2299 페이지
- SCADA 전처리기 요구 사항 및 사전 요건, 2300 페이지
- Modbus 전처리기, 2300 페이지
- DNP3 전처리기, 2302 페이지
- CIP 전처리기, 2305 페이지
- S7Commplus 전처리기, 2309 페이지

SCADA 전처리기 소개

Supervisory Control(감시 제어) 및 Data Acquisition(데이터 획득. SCADA) 프로토콜은 제조, 생산, 정수처리, 배전, 공항 및 배송 시스템 등과 같은 산업, 인프라 및 설비의 데이터를 모니터링하고, 제어하며, 획득합니다. Firepower System은 전처리기에 Modbus, DNP3(Distributed Network Protocol), CIP(Common Industrial Protocol), S7Commplus SCADA 프로토콜을 제공하며, 이러한 프로토콜은 네트워크 분석 정책의 일부로 설정할 수 있습니다.

Modbus, DNP3, CIP 또는 S7Commplus 전처리기가 비활성화되고, 이러한 전처리기가 필요한 침입 규칙을 사용자가 활성화 및 구축하면 시스템은 해당 전처리기를 현재 설정을 바탕으로 자동으로 사용합니다. 단, 대응하는 네트워크 분석 정책에 대한 웹 인터페이스에서는 전처리기가 계속 비활성화됩니다.

SCADA 전처리기 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

SCADA 전처리기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

Modbus 전처리기

Modbus 프로토콜은 1979년 Modicon에 의해 처음 게시되어 널리 사용되는 SCADA 프로토콜입니다. Modbus 전처리기는 Modbus 트래픽 내 이상 징후를 탐지하고 규칙 엔진에 의한 처리를 위해 Modbus 프로토콜을 디코딩하는데, 특정 프로토콜 필드에 액세스하기 위해 Modbus 키워드를 사용합니다.

단일 구성 옵션을 사용하면 전처리기가 Modbus 트래픽을 검사할 포트에 대한 기본 설정을 변경할 수 있습니다.

관련 항목

SCADA 키워드, 2157 페이지

Modbus 전처리기 포트 옵션

포트

전처리기가 Modbus 트래픽을 검사하는 포트를 지정합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

Modbus 전처리기 구성

네트워크가 Modbus가 활성화된 디바이스를 포함하지 않는 경우, 트래픽에 적용한 네트워크 분석 정책에서 이 전처리기를 활성화해선 안 됩니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **SCADA Preprocessors(SCADA** 전처리기**)**의 **Modbus Configuration(Modbus** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **Modbus Configuration(Modbus** 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Ports(**포트**)** 필드에 값을 입력합니다.

쉼표로 여러 개의 값을 구분합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 Modbus 전처리기 규칙(GID 144)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지 및 Modbus 전처리기 규칙, 2302 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

Modbus 전처리기 규칙

이러한 규칙에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 다음 표에서 Modbus 전처리기 규칙을 활성화해야 합니다.

표 ***232: Modbus*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
144:1	Modbus 헤더 내 길이가 Modbus 기능 코드가 요청하는 길이에 일치하지 않을 경우 이벤트를 생성합니다. 각 Modbus 기능에는 요청과 응답에 대한 예상된 형식이 있습니다. 메시지 길이가 예상된 형식과 일치하지 않는 경우 이 이벤트가 생성됩니다.
144:2	Modbus 프로토콜 ID가 0이 아닐 때 이벤트를 생성합니다. 프로토콜 ID 필드는 Modbus로 다른 프로토콜을 다중화하는 데 사용됩니다. 전처리기가 다른 프로토콜을 처리하지 않으므로, 이 이벤트가 대신 생성됩니다.
144:3	전처리기가 예약된 Modbus 기능 코드를 탐지하면 이벤트를 생성합니다.

DNP3 전처리기

Distributed Network Protocol(DNP3)은 원래 전력발전소 간 일관된 커뮤니케이션을 제공하기 위해 개발된 SCADA 프로토콜입니다. DNP3은 또한 상수도산업, 산업 폐기물 처리업, 운송 산업 및 많은 기타 업계에서 널리 사용되고 있습니다.

DNP3 전처리기는 DNP3 트래픽 내 이상 징후를 탐지하고 규칙 엔진에 의한 처리를 위해 DNP3 프로토콜을 디코딩하는데, 특정 프로토콜 필드에 액세스하기 위해 DNP3 키워드를 사용합니다.

관련 항목

DNP3 키워드, 2158 페이지

DNP3 전처리기 옵션

포트

각 지정된 포트의 DNP3 트래픽 검사를 활성화합니다. 단일 포트 또는 쉼표로 구분된 포트 목록을 지정할 수 있습니다.

잘못된 **CRC** 로깅

DNP3 링크 레이어 프레임에 포함된 체크섬을 검증합니다. 유효하지 않은 체크섬을 가진 프레임은 무시됩니다.

규칙 145:1을 활성화하여 잘못된 체크섬이 탐지된 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

DNP3 전처리기 구성

네트워크가 DNP3가 활성화된 디바이스를 포함하지 않는 경우, 트래픽에 적용한 네트워크 분석 정책에서 이 전처리기를 활성화해선 안 됩니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **SCADA Preprocessors(SCADA** 전처리기**)**의 **DNP3 Configuration(DNP3** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **DNP3 Configuration(DNP3** 설정**)** 옆에 있는 수정( )을(를) 클릭합니다.

단계 **6** **Ports(**포트**)**에 대한 값을 입력합니다.

쉼표로 여러 개의 값을 구분합니다.

단계 **7** **Log bad CRCs(**배드 **CRC** 로그**)** 확인란을 선택하거나 선택 취소합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 DNP3 전처리기 규칙(GID 145)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지, DNP3 전처리기 옵션, 2302 페이지 및 DNP3 전처리기 규칙, 2304 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1987 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

DNP3 전처리기 규칙

이러한 규칙에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 다음 표에서 DNP3 전처리기 규칙을 활성화해야 합니다.

표 ***233: DNP3*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
145:1	**Log bad CRC(**잘못된 **CRC** 로깅**)**를 활성화한 경우 전처리기가 유효하지 않은 체크섬을 통해 연결 레이어 프레임을 탐지하면 이벤트를 생성합니다.
145:2	전처리기가 유효하지 않은 길이로 DNP3 연결 레이어 프레임을 탐지하면 이벤트를 생성하고 패킷을 차단합니다.
145:3	전처리기가 유효하지 않은 시퀀스 번호로 전송 레이어 세그먼트를 탐지하면 이벤트를 생성하고 리어셈블리 중에 패킷을 차단합니다.
145:4	완전한 조각이 리어셈블되기 전에 DNP3 리어셈블리 버퍼가 지워지면 이벤트를 생성합니다. 이는 다른 세그먼트가 대기된 후 FIR 플래그를 전송하는 세그먼트가 나타날 때 발생합니다.
145:5	전처리기가 예약된 주소를 사용하는 DNP3 연결 레이어 프레임을 탐지하면 이벤트를 생성합니다.
145:6	전처리기가 예약된 기능 코드를 사용하는 DNP3 요청 또는 응답을 탐지하면 이벤트를 생성합니다.

CIP 전처리기

CIP(Common Industrial Protocol)는 산업 자동화 애플리케이션을 지원하는, 다양한 분야에서 사용하는 애플리케이션 프로토콜입니다. ENIP(EtherNet/IP)는 이더넷 기반 네트워크에서 사용하는 CIP를 구현한 결과물입니다.

CIP 전처리기는 TCP 또는 UDP에서 실행하는 CIP와 ENIP를 탐지하고 침입 규칙 엔진에 전송합니다. 맞춤형 침입 규칙에서 CIP 및 ENIP 키워드를 이용하면 CIP와 ENIP 트래픽에서의 공격을 탐지할 수 있습니다. CIP 및 ENIP 키워드의 내용을 참조하십시오. 또한 액세스 컨트롤 규칙에서 CIP 및 ENIP 애플리케이션 조건을 지정하여 트래픽을 제어할 수도 있습니다. 애플리케이션 조건 및 필터 구성, 536 페이지의 내용을 참조하십시오.

CIP 전처리기 옵션

포트

CIP 및 ENIP 트래픽을 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

참고 기본 CIP 탐지 포트 44818과 TCP 스트림 **Perform Stream Reassembly on Both Ports(**두 포트 모두에서 스트림 리어셈블리 수행**)** 목록에 나열한 다른 모든 포트를 추가해야 합니다. TCP 스트림 전처리 옵션, 2337 페이지 및 사용자 지정 네트워크 분석 정책 만들기, 2220 페이지의 내용을 참조하십시오.

기본 연결되지 않음 시간 초과**(**초**)**

CIP 요청 메시지에 프로토콜별 시간 초과 값이 없으며 **TCP** 연결당 동시 연결되지 않은 요청의 최대 수에 도달하는 경우, 시스템은 이 옵션이 지정한 초 수를 메시지에 지정합니다. 타이머가 만료되면 향후 요청을 위한 공간 확보를 위해 메시지가 제거됩니다. 0부터 360까지의 정수를 지정할 수 있습니다. 0을 지정하면 프로토콜별 시간 초과 값이 없는 모든 트래픽이 먼저 만료됩니다.

TCP 연결당 최대 동시 연결되지 않은 요청 수

시스템 연결을 닫기 전에 응답하지 않을 수 있는 동시 요청 수입니다. 1에서 1만까지의 정수를 지정할 수 있습니다.

TCP 연결당 최대 **CIP** 연결 수

시스템이 허용하는 TCP 연결당 최대 동시 CIP 연결 수입니다. 1에서 1만 까지의 정수를 지정할 수 있습니다.

CIP 이벤트

기본적으로 애플리케이션 탐지기와 이벤트 뷰어는 세션당 같은 애플리케이션을 각각 한 번만 탐지하고 표시합니다. CIP 세션이 서로 다른 패킷에 있는 여러 애플리케이션을 포함할 수 있으며, 단일 CIP 패킷이 여러 애플리케이션을 포함할 수 있습니다. CIP 전처리기는 대응하는 침입 규칙에 따라 모든 CIP 및 ENIP 트래픽을 처리합니다.

다음 표에서는 이벤트 보기에 표시되는 CIP 값을 확인할 수 있습니다.

표 ***234: CIP*** 이벤트 필드 값

이벤트 필드	표시되는 값
애플리케이션 프로토콜	CIP 또는 ENIP
클라이언트	CIP 클라이언트 또는 ENIP 클라이언트
웹 애플리케이션	특정 애플리케이션이 다음과 같은 요소를 탐지합니다. • 트랙픽을 허용하거나 모니터링하는 액세스 컨트롤의 경우, 세션에서 탐지한 마지막 애플리케이션 프로토콜. 연결을 로깅ㄹ하도록 설정한 액세스 컨트롤 규칙은 지정된 CIP 애플리케이션에 대한 이벤트를 생성하지 않을 수 있으며, 연결을 로깅하도록 설정하지 않은 액세스 컨트롤 규칙은 CIP 애플리케이션에 대한 이벤트를 생성할 수 있습니다. • 트래픽을 차단하는 액세스 컨트롤 규칙의 경우, 차단을 트리거한 애플리케이션 프로토콜. 액세스 컨트롤 규칙이 CIP 애플리케이션 목록을 차단하는 경우, 이벤트 뷰어는 가장 먼저 탐지한 애플리케이션을 표시합니다.

CIP 전처리기 규칙

다음 표에 있는 CIP 전처리기 규칙이 이벤트를 생성하게 하려면, 해당 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 침입 규칙 상태 설정, 2024 페이지를 참고하십시오

표 ***235: CIP*** 전처리기 규칙

GID: SID	규칙 메시지
148:1	CIP_MALFORMED

GID: SID	규칙 메시지
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

CIP 전처리기 설정 지침

CIP 전처리기를 설정하는 경우 다음 사항에 유의하십시오.

- 기본 CIP 탐지 포트 44818과 TCP 스트림 **Perform Stream Reassembly on Both Ports(**두 포트 모두에서 스트림 리어셈블리 수행**)** 목록에 나열한 다른 모든 CIP 포트를 추가해야 합니다. CIP 전처리기 옵션, 2305 페이지, 사용자 지정 네트워크 분석 정책 만들기, 2220 페이지 및 TCP 스트림 전처리 옵션, 2337 페이지 섹션을 참고하십시오.
- 이벤트 뷰어는 CIP 애플리케이션에 특수한 처리를 제공합니다. CIP 이벤트, 2306 페이지의 내용을 참조하십시오.
- Cisco는 침입 방지 작업을 액세스 컨트롤 정책의 기본 작업으로 사용할 것을 권장합니다.
- CIP 전처리기는 침입 규칙과 액세스 컨트롤 규칙에서 지정한 CIP 애플리케이션이 트리거한 트래픽을 삭제하지 않는 등의 바람직하지 않은 행동을 유발할 수 있는, **Access Control: Trust All Traffic(**액세스 컨트롤**:** 모든 트래픽 신뢰**)**을 액세스 컨트롤 정책 기본 작업으로 지원하지 않습니다.
- CIP 전처리기는 차단되선 안 되는 CIP 애플리케이션 차단 등의 바람직하지 않은 행동을 유발할 수 있는, **Access Control: Block All Traffic(**액세스 컨트롤**:** 모든 트래픽 차단**)**을 액세스 컨트롤 정책 기본 작업으로 지원하지 않습니다.
- CIP 전처리기는 네트워크 검색 같은 CIP 애플리케이션에 대한 애플리케이션 가시성을 지원하지 않습니다.
- CIP 및 ENIP 애플리케이션을 탐지하고 액세스 컨트롤 규칙과 침입 규칙 등에서 이를 사용하려면, 해당하는 맞춤형 네트워크 분석 정책에서 CIP 전처리기를 수동으로 활성화해야 합니다. 사용자 지정 네트워크 분석 정책 만들기, 2220 페이지, 기본 네트워크 분석 정책 설정, 네트워크 분석 규칙 설정, 2206 페이지 섹션의 내용을 참조하십시오.
- CIP 전처리기 규칙과 CIP 침입 규칙을 트리거하는 트래픽을 삭제하려면, 해당하는 침입 정책에서 **Drop when Inline(**인라인시 삭제**)**가 활성화되어 있는지 확인합니다. 인라인 배포에서 삭제 작업 설정하기의 내용을 참조하십시오.
- 액세스 컨트롤 규칙을 이용해 CIP 또는 ENIP 애플리케이션 트래픽을 차단하려면, 해당하는 네트워크 분석 정책에서 인라인 표준화 전처리기와 전처리기의 **Inline Mode(**인라인 모드**)** 옵션이 활성화(기본 설정)되어 있는지 확인합니다. 사용자 지정 네트워크 분석 정책 만들기, 2220 페이지, 기본 네트워크 분석 정책 설정, 인라인 구축의 전처리기 트래픽 수정, 2224 페이지의 내용을 참조하십시오.

CIP 전처리기 설정

시작하기 전에

- 기본 CIP 탐지 포트 44818과 TCP 스트림 **Perform Stream Reassembly on Both Ports(**두 포트 모두에서 스트림 리어셈블리 수행**)** 목록에 CIP 포트로 나열한 다른 모든 포트를 추가해야 합니다. CIP 전처리기 옵션, 2305 페이지, 사용자 지정 네트워크 분석 정책 만들기, 2220 페이지 및 TCP 스트림 전처리 옵션, 2337 페이지 섹션을 참고하십시오.
- CIP 전처리기 설정 지침, 2307 페이지의 내용을 숙지하십시오.
- CIP 전처리기는 FTD 디바이스에서 지원되지 않습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **SCADA Preprocessors(SCADA** 전처리기**)**의 **CIP Configuration(CIP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** CIP 전처리기 옵션, 2305 페이지에서 설명한 모든 옵션을 수정할 수 있습니다.

단계 **6** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.를 원하는 경우, CIP 침입 규칙과 필요에 따라 CIP 전처리기 규칙(GID 148)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지, CIP 전처리기 규칙, 2306 페이지 및 CIP 이벤트, 2306 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

S7Commplus 전처리기

S7Commplus 전처리기는 S7Commplus 트래픽을 탐지합니다. 맞춤형 침입 규칙에서 S7Commplus 키워드를 이용해서 S7Commplus 트래픽에서의 침입을 탐지할 수 있습니다. S7Commplus 키워드, 2161 페이지의 내용을 참조하십시오.

S7Commplus 전처리기 구성

S7Commplus 전처리기는 모든 FTD 디바이스에서 지원됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **SCADA Preprocessors(SCADA** 전처리기**)**에서 **S7Commplus Configuration(S7Commplus** 설정**)**이 비활성화되었다면 **Enabled(**활성화됨**)**를 클릭합니다.

단계 **5** 필요에 따라 **S7Commplus Configuration(S7Commplus** 설정**)** 옆에 있는 수정( )을 클릭하고 **s7commplus_ports**를 수정하여 전처리기가 S7Commplus 트래픽을 검사하는 포트를 식별합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

단계 **6** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 침입 이벤트를 생성하려면 S7Commplus 전처리기 규칙(GID 149)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지을 참조해 주십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

91 장

전송 및 네트워크 계층 전처리기

다음 주제에서는 전송 및 네트워크 계층 전처리기와 이를 구성하는 방법을 설명합니다.

- 전송 및 네트워크 계층 전처리기 소개, 2311 페이지
- 전송 및 네트워크 레이어 전처리기에 대한 라이선스 요구 사항, 2312 페이지
- 전송 및 네트워크 계층 전처리기 요구 사항 및 사전 요건, 2312 페이지
- 고급 전송/네트워크 전처리기 설정, 2312 페이지
- 체크섬 확인, 2315 페이지
- 인라인 정상화 전처리기, 2317 페이지
- IP 조각 모음 전처리기, 2324 페이지
- 패킷 디코더, 2330 페이지
- TCP 스트림 전처리, 2334 페이지
- UDP 스트림 전처리, 2346 페이지

전송 및 네트워크 계층 전처리기 소개

전송 및 네트워크 레이어 전처리기는 IP 조각을 이용한 공격을 탐지하고 체크섬 유효성 검증을 수행하며, TCP와 UDP 세션 전처리를 수행합니다. 패킷이 전처리기로 전달되기 전에, 패킷 디코더는 전처리기 및 침입 규칙 엔진에서 쉽게 사용할 수 있는 형식으로 패킷 헤더와 페이로드를 변환하고 패킷 헤더에서 다양한 이상 작업을 탐지합니다. 패킷을 디코딩한 후 다른 전처리기에 전송하기 전에 인라인 표준화 전처리기는 인라인 배포를 위해 트래픽을 표준화합니다.

침입 규칙 또는 규칙 인수에 비활성화된 전처리기가 필요한 경우, 네트워크 분석 정책의 웹 인터페이스에서 전처리기가 비활성화 상태로 남아 있더라도 시스템은 자동으로 전처리기를 현재 구성으로 사용합니다.

전송 및 네트워크 레이어 전처리기에 대한 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

전송 및 네트워크 계층 전처리기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

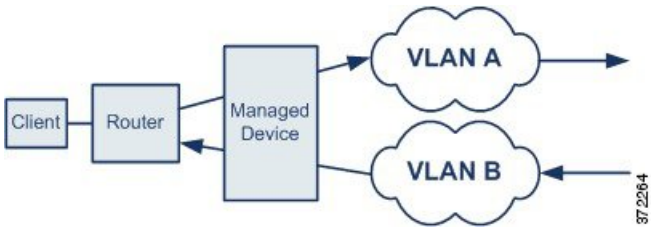
- 관리자
- 침입 관리자

고급 전송/네트워크 전처리기 설정

고급 전송 및 네트워크 전처리 설정은 액세스 제어 정책을 배포하는 모든 네트워크, 영역 및 VLAN에 글로벌로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다.

무시된 **VLAN** 헤더

동일한 연결에 대해 다른 방향으로 이동하는 트래픽의 서로 다른 VLAN 태그는 트래픽 리어셈블리 및 규칙 처리에 영향을 줄 수 있습니다. 예를 들어 다음 그림에서는 동일한 연결에 대한 트래픽을 VLAN A를 통해 전송하고 VLAN B를 통해 수신할 수 있습니다.



패킷이 구축에 맞게 올바르게 처리될 수 있도록 시스템이 VLAN 헤더를 무시하게 설정할 수 있습니다.

참고 이 옵션은 ASA FirePOWER에서는 지원되지 않습니다.

침입 삭제 규칙에서의 활성 응답

드롭 규칙은 규칙 상태가 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 침입 또는 전처리기 규칙입니다. 인라인 배포에서 시스템은 트리거 패킷을 삭제하고 패킷이 시작된 세션을 차단하여 TCP 또는 UDP 드롭 규칙에 응답합니다.

팁 UDP 데이터 스트림은 일반적으로 세션의 측면에서 평가되지 않으므로 스트림 전처리기는 캡슐화 IP 데이터그램 헤더의 소스 및 대상 IP 주소 필드와 UDP 헤더의 포트 필드를 사용하여 흐름 방향을 결정하고 UDP 세션을 식별합니다.

하나 이상의 *active responses(*활성 응답*)*를 시작하도록 시스템을 구성하면 위반 패킷이 TCP 또는 UDP 삭제 규칙을 트리거할 때 더욱 정확하고 구체적츠로 TCP 연결 또는 UDP 세션을 닫을 수 있습니다. 활성 응답은 라우티드 및 투명 구축을 포함한 인라인 구축에서 사용할 수 있습니다. 활성 응답은 패시브 구축에는 적합하지 않으며 지원되지 않습니다.

활성 응답을 구성하려면 다음을 수행합니다.

- TCP 또는 UDP(**resp** 키워드만 해당) 침입 규칙을 생성하거나 수정합니다. 침입 규칙 헤더 프로토콜, 2067 페이지의 내용을 참조하십시오.
- **react** 또는 **resp** 키워드를 침입 규칙에 추가합니다. x활성 응답 키워드, 2165 페이지를 참조하십시오.
- TCP 연결의 경우 원한다면 전송할 추가 활성 응답의 최대 수와, 활성 응답 간 대기 시간(초)을 지정할 수 있습니다. 자세한 내용은 고급 전송/네트워크 전처리기 옵션, 2314 페이지의 **Maximum Active Responses(**최대 활성 응답**)** 및 **Minimum Response Seconds(**최소 응답 시간 **(**초**))**를 참조하십시오.

활성 응답은 다음과 같은 일치하는 트래픽이 삭제 규칙을 트리거하면 세션을 닫습니다.

- **TCP** - 트리거 패킷을 삭제하고 클라이언트와 서버 트래픽 모두에 TCP Reset(RST) 패킷을 삽입합니다.

- **UDP** - ICMP 도달 불가 패킷을 세션의 각 끝 부분에 전송합니다.

고급 전송/네트워크 전처리기 옵션

연결을 추적할 때는 **VLAN** 헤더를 무시하십시오.

다음에서처럼 트래픽을 식별할 때 VLAN 헤더를 무시할지 포함할지를 지정합니다.

- 이 옵션을 선택하면 시스템은 VLAN 헤더를 무시합니다. 서로 다른 방향으로 이동하는 트래픽 내의 같은 연결에 대한 다른 VLAN 태그를 탐지하는, 구축된 디바이스에 이 설정을 사용하십시오.
- 이 옵션을 비활성화하면 시스템은 VLAN 헤더를 포함합니다. 서로 다른 방향으로 이동하는 트래픽 내의 같은 연결에 대한 다른 VLAN 태그를 탐지하지 않는, 구축된 디바이스에 이 설정을 사용하십시오.

참고 이 옵션은 ASA FirePOWER에서는 지원되지 않습니다.

최대 활성 응답

TCP 연결당 최대 활성 응답 수를 지정합니다. 추가 트래픽은 활성 응답이 시작된 연결에서 발생하고, 이전 활성 응답 이후 **Minimum Response Seconds(**최소 응답 시간**(**단위**:** 초**))**보다 트래픽이 더 많이 발생한 경우, 지정된 최대값에 도달하지 않는 한 시스템은 다른 활성 응답을 보냅니다. 0으로 설정하면 **resp** 또는 **react** 규칙이 트리거하는 추가 활성 응답이 비활성화됩니다. 침입 삭제 규칙에서의 활성 응답, 2313 페이지 및 활성 응답 키워드, 2165 페이지를 참조하십시오.

트리거된 **resp** 또는 **react** 규칙은 이 옵션의 구성과 상관없이 활성 응답을 시작합니다.

최소 응답 시간**(**단위**:** 초**)**

Maximum Active Responses(최대 활성 응답**)**에 도달할 때까지, 시스템이 능동 응답을 시작한 연결에 대한 추가 트래픽이 후속 능동 응답으로 이어지기 전의 대기 시간(단위: 초)을 지정합니다.

문제 해결 옵션**:** 세션 종료 로깅 임계값

주의 지원팀의 지시가 있을 때만 세션 종료 로깅 임계값을 수정하십시오.

Support(지원팀)는 문제 해결 통화 중에 시스템을 구성하여 개별 연결이 지정된 임계값을 초과하면 메시지를 로깅하도록 요청할 수 있습니다. 이 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

이 옵션은 세션이 종료되고 지정된 수가 초과된 경우 로깅된 메시지의 바이트 수를 지정합니다.

참고 1GB의 상한 값은 또한 스트림 처리에 할당된 관리되는 디바이스의 메모리 양에 의해 제한됩니다.

관련 항목

활성 응답 키워드, 2165 페이지

고급 전송/네트워크 전처리기 설정

이 작업을 수행하려면 관리자, 액세스 관리자 또는 Network Admin(네트워크 관리자)여야 합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(고급)**를 클릭합니다.

단계 **2** Transport/Network Layer Settings(전송/네트워크 계층 설정) 섹션 옆에 있는 수정( )을 클릭합니다.

단계 **3** 문제 해결 옵션 **Session Termination Logging Threshold(**세션 종료 로깅 임계값**)**를 제외하고, 고급 전송/네트워크 전처리기 옵션, 2314 페이지에서 설명하는 옵션을 수정합니다.

참고 **Ignore the VLAN header when tracking connectons(**연결 추적 시 **VLAN** 헤더 무시**)** 옵션은 ASA FirePOWER 모듈에서는 사용할 수 없습니다.

주의 지원팀의 지시가 있을 때만 **Session Termination Logging Threshold(**세션 종료 로깅 임계값**)**를 수정하십시오.

단계 **4** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 선택 사항으로, 액세스 제어 정책 수정, 1630 페이지에 설명된 대로 정책을 구성합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

체크섬 확인

시스템은 프로토콜 수준 체크섬을 모두 검증하여 전체 IP, TCP, UDP 및 ICMP 전송이 수신되고 기본 수준에서 패킷이 전송 중에 함부로 조작되거나 실수로 변경되지 않았는지 확인할 수 있습니다. 체크섬은 알고리즘을 사용하여 패킷 내 프로토콜의 무결성을 확인합니다. 종단 호스트가 패킷 내에 작성한 것과 동일한 값을 시스템이 산출할 경우 패킷은 변경되지 않은 것으로 간주됩니다.

체크섬 확인을 비활성화한 경우 네트워크는 삽입 공격의 영향을 받기 쉽습니다. 시스템은 체크섬 확인 이벤트를 생성하지 않는다는 점에 유의하십시오. 인라인 배포에서 시스템을 구성하여 유효하지 않은 체크섬을 가진 패킷을 삭제할 수 있습니다.

체크섬 확인 옵션

수동 또는 인라인 배포에서 다음 옵션을 **Enabled(**활성화**)** 또는 **Disabled(**비활성화**)**로, 또는 인라인 배포에서 **Drop(**삭제**)**으로 설정할 수 있습니다.

- **ICMP** 체크섬
- **IP** 체크섬
- **TCP** 체크섬
- **UDP** 체크섬

옵션을 **Drop(**삭제**)**으로 설정하고 위반 패킷을 삭제하려면 관련 네트워크 분석 정책에서 **Inline Mode(**인라인 모드**)**를 활성화하고 장치가 인라인으로 구축되었는지 확인해야 합니다.

또한 이러한 옵션을 수동 배포에서 **Drop(**삭제**)**으로 설정하는 것은, 또는 탭 모드의 인라인 배포에서 그렇게 설정하는 것은 이들을 **Enabled(**활성화**)**로 설정하는 것과 동일합니다.

모든 체크섬 확인 옵션의 기본값은 **Enabled**입니다. 하지만 FTD 라우팅 및 투명 인터페이스는 언제나 IP 체크섬 확인에 실패하는 패킷을 삭제합니다. FTD 라우팅 및 투명 인터페이스는 배드 체크섬이 있는 UDP 패킷을 수정한 후 패킷을 Snort 프로세스로 전달합니다.

관련 항목

인라인 구축의 전처리기 트래픽 수정, 2224 페이지

체크섬 확인

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **Checksum Verification(**체크섬 확인**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **Checksum Verification(**체크섬 확인**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** 체크섬 확인, 2315 페이지에 설명된 대로 옵션을 수정합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1985 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

인라인 정상화 전처리기

인라인 정상화 전처리기는 인라인 배포에서 공격자가 탐지를 우회하는 가능성을 최소화하기 위해 트래픽을 정상화합니다.

참고 시스템이 트래픽에 영향을 미치려면 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 관련 구성을 매니지드 디바이스에 구축해야 합니다.

IPv4, IPv6, ICMPv4, ICMPv6 및 TCP 트래픽의 모든 조합에 대해 표준화를 지정할 수 있습니다. 대부분의 표준화는 패킷 기준이며 인라인 표준화 전처리기에 의해 수행됩니다. 그러나 TCP 페이로드 표준화를 포함하여 대부분의 상태 관련 패킷 및 스트림 표준화는 TCP 스트림 전처리기가 처리합니다.

인라인 표준화는 패킷 디코더의 디코딩 직후 및 다른 전처리기의 처리 직전에 발생합니다. 표준화는 패킷 레이어의 내부에서 외부로 진행됩니다.

인라인 표준화 전처리기는 이벤트를 생성하지 않고 인라인 배포에서 다른 전처리기 및 규칙 엔진에 의한 사용을 위해 패킷을 준비합니다. 또한 전처리기를 통해 시스템이 처리하는 패킷이 네트워크 호스트에서 수신된 패킷과 동일한지 확인할 수 있습니다.

참고 인라인 구축에서는 인라인 모드를 활성화하고 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화된 인라인 표준화 전처리기를 구성하는 것이 좋습니다. 수동 구축에서는 적응형 프로파일을 사용하는 것이 좋습니다.

관련 항목

인라인 구축의 전처리기 트래픽 수정, 2224 페이지
적응형 프로파일 정보, 2371 페이지

인라인 표준화 옵션

최소 **TTL**

Reset TTL(TTL 재설정**)**이 이 옵션에 설정된 값보다 크거나 같을 때 다음을 지정합니다.

- **Normalize IPv4**가 활성화되었을 때 시스템이 IPv4 Time to Live (TTL) 필드에서 허용할 최소값. 값이 더 낮으면 TTL에 대한 패킷 값이 **Reset TTL**에 대해 설정된 값으로 표준화됩니다.
- **Normalize IPv6**이 활성화되었을 때 시스템이 IPv6 Hop Limit 필드에서 허용할 최소값. 값이 더 낮으면 Hop Limit에 대한 패킷 값이 **Reset TTL**에 대해 설정된 값으로 표준화됩니다.

필드가 비어 있는 경우 시스템은 값을 1로 가정합니다.

참고 FTD 라우팅 및 투명 인터페이스의 경우 **Minimum TTL(**최소 **TTL)** 및 **Reset TTL(TTL** 재설정**)** 옵션은 무시됩니다. 연결에 대한 최대 TTL은 초기 패킷의 TTL이 결정합니다. 후속 패킷에 대한 TTL은 줄일 수는 있지만 늘릴 수는 없습니다. 시스템은 TTL을 해당 연결에 대해 목격된 최저 TTL로 재설정합니다. 이렇게 하면 TTL 회피 공격을 방지할 수 있습니다.

패킷 디코딩 **Detect Protocol Header Anomalies(**포로토콜 헤더 이상 탐지**)** 옵션이 활성화되면, 이 옵션을 위해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.에 대한 디코더 규칙 카테고리의 다음 규칙을 활성화할 수 있습니다.

- 규칙 116:428을 활성화하여 시스템이 지정된 최소 값보다 작은 TTL 값이 포함된 IPv4 패킷을 탐지하는 경우 트리거할 수 있습니다.
- 규칙 116:270을 활성화하여 시스템이 지정된 최소 값보다 작은 홉 제한 값이 포함된 IPv6 패킷을 탐지하는 경우 트리거할 수 있습니다.

TTL 재설정

Minimum TTL(최소 **TTL)**보다 크거나 같은 값을 설정할 때, 다음을 표준화합니다.

- **Normalize IPv4**가 활성화된 경우 IPv4 TTL 필드
- **Normalize IPv6**이 활성화된 경우 IPv6 Hop Limit 필드

패킷 값이 **Minimum TTL**보다 작은 경우 시스템은 TTL 또는 Hop Limit 값을 이 옵션에 대해 설정된 값으로 변경하여 패킷을 표준화합니다. 이 필드에 아무 값도 입력하지 않거나 0 또는 **Minimum TTL(**최소 **TTL)**보다 작은 값으로 설정하면 이 옵션이 비활성화됩니다.

IPv4 표준화

IPv4 트래픽의 표준화를 활성화합니다. 시스템은 다음 조건 시 필요하다면 TTL 필드도 표준화합니다.

- 이 옵션을 활성화하고,

- **Reset TTL(TTL** 재설정**)**에 설정된 값이 TTL 표준화를 활성화합니다.

이 옵션을 활성화하면 추가 IPv4 옵션도 활성화할 수 있습니다.

이 옵션을 활성화하면, 시스템은 다음 기본 IPv4 표준화를 수행합니다.

- 과도한 페이로드를 가진 패킷을 IP 헤더에 지정된 데이터그램 길이로 줄입니다.
- 예전에는 Type of Service(서비스 유형, ToS)로 알려졌던 Differentiated Services(차별화된 서비스, DS) 필드의 내용을 지웁니다.
- 모든 옵션 옥텟을 1(무연산)로 설정합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. FTD 디바이스는 라우터 알림, 옵션 목록의 끝(EOOL), 특정 라우팅 또는 투명 인터페이스의 작업 없음(NOP)을 제외한 다른 IP 옵션을 포함하는 RSVP 패킷은 모두 삭제합니다.

조각화 금지 비트 표준화

IPv4 Flags(플래그) 헤더 필드의 단일 비트 Don't Fragment(조각화 금지) 하위 필드의 내용을 지웁니다. 이 옵션을 활성화하면 필요한 경우 다운스트림 라우터가 패킷을 삭제하는 대신 조각화할 수 있습니다. 또한 삭제할 조작된 패킷에 기반하여 회피를 방지할 수 있습니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

예약 비트 표준화

IPv4 Flags(플래그) 헤더 필드의 단일 비트 Reserved(예약) 하위 필드의 내용을 지웁니다. 일반적으로 이 옵션을 활성화합니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

TOS 비트 표준화

예전에는 Type of Service(서비스 유형, ToS)로 알려졌던 1바이트 Differentiated Services(차별화된 서비스, DS) 필드의 내용을 지웁니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

초과 페이로드 표준화

페이로드가 과도한 패킷을 IP 헤더 및 Layer(레이어) 2(예를 들어, Ethernet(이더넷)) 헤더에 지정된 데이터그램 길이로 줄이지만 최소 프레임 길이 이하로 줄이지는 않습니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. 초과 페이로드가 있는 패킷은 이러한 인터페이스에서는 항상 삭제됩니다.

IPv6 표준화

Hop-by-Hop Options(홉 바이 홉 옵션) 및 Destination Options(대상 옵션) 확장 헤더의 모든 Option Type(옵션 유형) 필드를 00(건너뛰기 및 처리 계속)으로 설정합니다. 이 옵션이 활성화되고 **Reset TTL(TTL** 재설정**)**에 설정된 값이 홉 제한 표준화를 활성화하는 경우 시스템에서도 필요에 따라 Hop Limit(홉 제한) 필드를 표준화합니다.

ICMPv4 표준화

ICMPv4 트래픽 내 Echo(Request)(에코(요청)) 및 Echo Reply(에코 응답) 메시지에서 8비트 Code(코드) 필드의 내용을 지웁니다.

ICMPv6 표준화

ICMPv6 트래픽 내 Echo(Request)(에코(요청)) 및 Echo Reply(에코 응답) 메시지에서 8비트 Code(코드) 필드의 내용을 지웁니다.

예약 비트 표준화**/**지우기

TCP 헤더에 있는 Reserved(예약) 비트를 지웁니다.

옵션 패딩 바이트 표준화**/**지우기

모든 TCP 옵션 패딩 바이트를 지웁니다.

URG=0인 경우 긴급 포인터 지우기

긴급(URG) 제어 비트가 설정되지 않은 경우 16비트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드의 내용을 지웁니다.

빈 페이로드의 긴급 포인터**/URG** 지우기

페이로드가 없는 경우 TCP 헤더 Urgent Pointer(긴급 포인터) 필드의 내용 및 URG 제어 비트를 비웁니다.

긴급 포인터가 설정되지 않은 경우 **URG** 지우기

긴급 포인터가 설정되지 않은 경우 TCP 헤더 URG 제어 비트를 지웁니다.

긴급 포인터 표준화

포인터가 페이로드 길이보다 긴 경우 2바이트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드를 페이로드 길이로 설정합니다.

TCP 페이로드 표준화

TCP Data(데이터) 필드의 표준화를 활성화하여 재전송된 데이터의 일관성을 유지합니다. 제대로 리어셈블될 수 없는 모든 세그먼트는 삭제됩니다.

SYN 데이터 제거

TCP 운영 체제 정책이 Mac OS가 아닌 경우 동기화(SYN) 패킷의 데이터를 제거합니다.

또한 이 옵션은 TCP 스트림 전처리기 **Policy(**정책**)** 옵션이 **Mac OS**로 설정돼 있지 않을 때 트리거할 수 있는 규칙 129:2를 비활성화합니다.

RST 데이터 제거

TCP 재설정(RST) 패킷에서 모든 데이터를 제거합니다.

Window로 데이터 절감

TCP Data(데이터) 필드를 Window 필드에 지정된 크기로 줄입니다.

MSS로 데이터 절감

페이로드가 Maximum Segment Size(최대 세그먼트 크기, MSS)보다 긴 경우 TCP Data(데이터) 필드를 MSS로 줄입니다.

해결할 수 없는 **TCP** 헤더 이상 징후 차단

이 옵션을 활성화하면 표준화된 경우 시스템은 유효하지 않고 수신 호스트가 차단할 가능성이 높은 변칙적 TCP 패킷을 차단합니다. 예를 들어, 시스템은 설정된 세션에 차후에 전송된 모든 SYN 패킷을 차단합니다.

시스템은 또한 규칙이 활성화되어 있는지 여부에 관계없이 다음 TCP 스트림 전처리기 규칙에 하나라도 일치하는 모든 패킷을 삭제합니다.

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14~129:19

Total Blocked Packets(전체 차단된 패킷) 성능 표는 인라인 배포와 수동 배포 및 탭 모드의 인라인 배포에서 차단된 패킷 수 및 인라인 배포에서 차단되었을 수도 있는 수를 추적합니다.

명시적 정체 알림

Explicit Congestion Notification(명시적 정체 알림, ECN) 플래그의 패킷별 또는 스트림별 표준화를 다음과 같이 활성화합니다.

- 협상에 관계없이 패킷별로 ECN 플래그를 지우려면 **Packet(**패킷**)**을 선택합니다
- ECN 사용이 협상되지 않은 경우 스트림별로 ECN 플래그를 지우려면 **Stream(**스트림**)**을 선택합니다

Stream(스트림**)**을 선택한 경우, 이 표준화를 실행하려면 TCP 스트림 전처리기 **Require TCP 3-Way Handshake(TCP 3**방향 핸드셰이크 요청**)** 옵션을 활성화해야 합니다.

기존 **TCP** 옵션 지우기

Allow These TCP Options(이러한 **TCP** 옵션 허용**)**을 활성화합니다.

이러한 **TCP** 옵션 허용

사용자가 트래픽에서 허용하는 특정 TCP 옵션의 표준화를 비활성화합니다.

시스템은 사용자가 명시적으로 허용하는 옵션을 표준화하지 않습니다. 이는 옵션을 No Operation(무연산, TCP 옵션 1)으로 설정함으로써 사용자가 명시적으로 허용하지 않는 옵션을 표준화합니다.

시스템은 **Allow These TCP Options(**이러한 **TCP** 옵션 허용**)** 설정 여부에 상관없이 다음 옵션을 항상 허용해야 합니다. 최상의 TCP 성능을 위해 자주 사용하는 옵션이기 때문입니다.

- 최대 세그먼트 크기(MSS)
- 창 크기 조정
- 타임 스탬프 TCP

시스템은 드물게 사용되는 다른 옵션은 자동으로 허용하지 않습니다.

다음의 예시에서처럼 옵션 키워드, 옵션 번호, 또는 둘 다로 이루어진 쉼표로 구분된 목록을 작성하여 특정 옵션을 허용할 수 있습니다.

```
sack, echo, 19
```

옵션 키워드를 지정하는 것은 키워드와 관련된 하나 이상의 TCP 옵션을 지정하는 것과 같습니다. 예를 들어, `sack`을 지정하는 것은 TCP 옵션 4(Selective Acknowledgment Permitted(허용된 선택적 수신 확인)) 및 5(Selective Acknowledgment(선택적 수신 확인))를 지정하는 것과 같습니다. 옵션 키워드는 대소문자를 구분하지 않습니다.

또한 모든 TCP 옵션을 허용하고 모든 TCP 옵션의 표준화를 효과적으로 비활성화하는 `any`를 지정할 수 있습니다.

다음 표는 허용할 TCP 옵션을 지정하는 방법에 대해 요약합니다. 필드를 비워 둘 경우, 시스템은 MSS, Window Scale(Window 크기), Time Stamp(타임 스탬프) 옵션만 허용합니다.

지정 대상	허용 대상
sack	TCP 옵션 4(Selective Acknowledgment Permitted(허용된 선택적 수신 확인)) 및 5(Selective Acknowledgment(선택적 수신 확인))
echo	TCP 옵션 6(Echo Request(에코 요청)) 및 7(Echo Reply(에코 응답))
partial_order	TCP 옵션 9(Partial Order Connection Permitted(허용된 부분 순서 연결)) 및 10(Partial Order Service Profile(부분 순서 서비스 프로파일))
conn_count	TCP Connection Count(연결 집계) 옵션 11(CC), 12(CC.New(새로운)), 그리고 13(CC.Echo(에코))

지정 대상	허용 대상
alt_checksum	TCP 옵션 14(Alternate Checksum Request(대체 체크섬 요청)) 및 15(Alternate Checksum(대체 체크섬))
md5	TCP 옵션 19(MD5 서명)
옵션 번호. 2~255.	키워드가 없는 옵션을 비롯한 특정 옵션
any	모든 TCP 옵션. 이 설정은 TCP 옵션 표준화를 효과적으로 비활성화합니다

이 옵션에 any를 지정하지 않은 경우, 표준화에는 다음이 포함됩니다.

- MSS, Window Scale(Window 크기), Time Stamp(타임 스탬프) 및 모든 명시적으로 허용된 옵션을 제외하고, 모든 옵션 바이트를 No Operation(무연산, TCP 옵션 1)으로 설정합니다.
- Time Stamp(타임 스탬프)가 존재하지만 유효하지 않은 경우, 또는 유효하지만 협상되지 않은 경우, Time Stamp(타임 스탬프) 옥텟을 No Operation(무연산)으로 설정합니다.
- Time Stamp(타임 스탬프)가 협상되었지만 존재하지 않는 경우 패킷을 차단합니다.
- Acknowledgment(수신 확인, ACK) 제어 비트가 설정되지 않은 경우 Time Stamp Echo Reply(타임 스탬프 에코 응답, TSecr) 옵션 필드를 비웁니다.
- SYN 제어 비트가 설정되지 않은 경우 MSS 및 Window Scale(Window 크기) 옵션을 No Operation(무연산, TCP 옵션 1)으로 설정합니다

관련 항목

침입 이벤트 성능 통계 그래프 유형, 2955 페이지

인라인 표준화 설정

시작하기 전에

- 위반 패킷을 표준화 또는 삭제하려면 인라인 구축의 전처리기 트래픽 수정, 2224 페이지에 설명된 대로 **Inline Mode(**인라인 모드**)**를 활성화합니다. 또한 매니지드 디바이스는 인라인으로 구축해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다(캐럿이 아니라 단어를 클릭).

단계 **4** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **Inline Normalization(**인라인 표준화**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **Inline Normalization(**인라인 표준화**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** 인라인 정상화 전처리기, 2317 페이지에 설명된 대로 옵션을 설정합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 인라인 표준화 Minimum TTL(최소 TTL) 옵션이 침입 이벤트를 생성하게 하려면, 패킷 디코더 규칙 116:429(IPv4)와 116:270 (IPv6) 중 하나 또는 둘 다를 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지 및 인라인 표준화 옵션, 2318 페이지를 참고하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1985 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

IP 조각 모음 전처리기

IP 데이터그램이 최대 전송 단위(MTU)보다 커서 2개 이상의 소규모 IP 데이터그램으로 쪼개진 경우 조각화됩니다. 단일 IP 데이터그램 조각에는 숨겨진 공격을 식별하기에 충분한 정보가 포함되어 있지 않을 수 있습니다. 공격자는 조각화된 패킷 내에 공격 데이터를 전송하여 탐지 우회를 시도할 수 있습니다. IP 조각 모음 전처리기는 규칙 엔진이 조각화된 IP 데이터그램에 대해 규칙을 실행하기 전에 이를 리어셈블하므로 규칙이 해당 패킷에서 공격을 더욱 적절히 식별할 수 있습니다. 조각화된 데이터그램이 리어셈블되지 않는 경우 데이터그램에 대해 규칙이 실행되지 않습니다.

IP 단편화 익스플로잇

IP 조각 모음을 활성화하면 티어드롭 공격과 같은 네트워크 호스트에 대한 공격 및 Jolt2 공격과 같은 시스템 자체에 대한 리소스 소모 공격을 탐지할 수 있습니다.

티어드롭 공격은 특정 운영 체제에서 버그를 공격하는데, 중첩되는 IP 조각을 리어셈블하려고 시도할 때 충돌을 야기합니다. IP 조각 모음 전처리기가 중첩되는 조각을 식별하도록 활성화 및 구성된 경

우 이를 수행합니다. IP 조각 모음 전처리기는 티어드롭과 같은 중첩되는 조각화 공격의 첫 번째 패킷을 탐지하지만 동일한 공격의 후속 패킷은 탐지하지 않습니다.

Jolt2 공격은 IP 조각 모음기를 혹사시키기 위한 시도로 동일한 조각화된 IP 패킷을 엄청난 수로 복제하여 전송해서 DoS(Denial-of-Service) 공격을 야기합니다. 메모리 사용량 한도는 IP 조각 모음 전처리기에서 이것 및 이와 유사한 공격을 차단하고, 철저한 검사를 기반으로 시스템 자체 보호를 유지합니다. 시스템은 공격에 의해 마비되지 않고 운영 상태를 유지하며 계속해서 네트워크 트래픽을 검사합니다.

다양한 운영 체제는 조각화된 패킷을 다양한 방법으로 리어셈블합니다. 호스트가 실행 중인 운영 체제를 결정할 수 있는 공격자는 또한 악성 패킷을 조각화하여 대상 호스트가 특정 방식으로 이를 리어셈블하도록 할 수 있습니다. 모니터링한 네트워크 상의 호스트가 어떤 운영 체제를 실행 중인지 시스템에서 알 수 없기 때문에 전처리기가 패킷을 부정확하게 검사하고 리어셈블할 수 있으므로 익스플로잇이 탐지되지 않고 통과될 수 있습니다. 이러한 유형의 공격을 줄이기 위해 조각 모음 전처리기를 네트워크의 각 호스트에 대한 패킷을 조각 모음하는 적절한 방법을 사용하도록 구성할 수 있습니다.

또한 수동 구축에서 적응형 프로파일을(를) 사용하여 패킷의 대상 호스트에 대한 호스트 운영체제 정보를 통해 IP 조각 모음 전처리기의 대상 기반 정책을 동적으로 선택할 수도 있습니다.

대상 기반 조각 모음 정책

호스트의 운영체제는 다음과 같은 3가지 기준을 바탕으로, 패킷을 리어셈블리할 때 우선해야 할 패킷 프래그먼트를 결정합니다.

- 운영체제가 프래그먼트를 수신한 순서
- 패킷의 오프셋(패킷 시작 부분에서 프래그먼트까지의 거리(단위: 바이트))
- 중첩 프래그먼트 대비 패키의 시작 위치와 마지막 위치

모든 운영 체제가 이러한 기준을 사용하지만, 조각화된 패킷을 리어셈블할 때 서로 다른 운영 체제는 서로 다른 조각을 지원합니다. 따라서, 네트워크에서 서로 다른 운영 체제를 사용 중인 두 호스트는 중첩되는 동일한 조각을 완전히 다른 방법으로 리어셈블할 수 있습니다.

사용 중인 호스트 중 하나의 운영 체제를 알고 있는 공격자는 중첩되는 패킷 조각에 숨겨진 악성 콘텐츠를 전송하여 탐지 우회를 시도하고 해당 호스트를 공격할 수 있습니다. 이 패킷은 리어셈블되고 검사될 때는 무해하게 보일 수 있지만 대상 호스트에 의해 리어셈블될 경우에는 악성 익스플로잇이 포함됩니다. 그러나, 모니터링된 네트워크 세그먼트에서 실행되는 운영 체제를 식별하기 위해 IP 조각 모음 전처리기를 구성한 경우, 이는 대상 호스트가 하는 것과 동일한 방법으로 조각을 리어셈블하여 공격을 식별할 수 있습니다.

IP 조각 모음 옵션

단순히 IP 조각 모음을 활성화하거나 비활성화하도록 선택할 수도 있습니다. 그러나 Cisco는 IP 조각 모음 전처리기의 활성화된 작업을 더욱 세밀한 수준으로 지정할 것을 권장합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

다음 전역 옵션을 설정할 수 있습니다.

Preallocated Fragments(미리 할당된 조각**)**

전처리기가 한 번에 처리할 수 있는 개별 조각의 최대 수입니다. 미리 할당할 조각 노드의 수를 지정하면 정적 메모리 할당이 활성화됩니다.

주의 개별 조각을 처리하면 메모리 중 약 1550바이트가 사용됩니다. 전처리기가 개별 조각을 처리하는 데 관리되는 디바이스에 미리 정해진 허용 가능한 메모리 제한보다 더 많은 메모리가 필요한 경우 해당 디바이스의 메모리 제한이 우선합니다.

각 IP 조각 모음 정책에 다음 옵션을 구성할 수 있습니다,

네트워크

조각 모음 정책을 적용할 호스트의 IP 주소입니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255개의 프로파일을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

정책

모니터링된 네트워크 세그먼트의 호스트 집합에 사용할 조각 모음 정책입니다.

대상 호스트의 운영체제에 따라 7가지 조각 모음 정책 중 하나를 선택하면 됩니다. 다음 표는 7개의 정책 및 각각을 사용하는 운영 체제를 나열합니다. First 및 Last 정책 이름은 해당 정책이 원래의 중첩 패킷을 지원하는지, 아니면 후속 중첩 패킷을 지원하는지 여부를 반영합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

표 ***236:*** 대상 기반 조각 모음 정책

정책	**Operating Systems**(운영 체제)
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect
First	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
(Windows용)	(Windows용)

시간 초과

조각화된 패킷을 리어셈블할 때 전처리기 엔진이 사용할 수 있는 최대 시간(단위: 초)을 지정합니다. 패킷이 지정된 기간 내에 리어셈블될 수 없는 경우, 전처리기 엔진은 패킷 리어셈블 시도를 중지하고 수신한 조각을 삭제합니다.

최소 **TTL**

패킷이 가질 수 있는 허용 가능한 최소 TTL 값을 지정합니다. 이 옵션은 TTL 기반 삽입 공격을 탐지합니다.

규칙 123:11을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

이상 징후 탐지

중첩되는 조각과 같은 조각화 문제를 식별합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

다음 규칙을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

- 123:1~123:4
- 123:5(BSD 정책)

- 123:6~123:8

중첩 제한

한 세션에서 중첩되는 세그먼트에 대해 구성된 수가 탐지된 경우 해당 세션에 대한 조각 모음이 중단됨을 명시합니다.

이 옵션을 구성하려면 **Detect Anomalies(**이상 징후 탐지**)**를 활성화해야 합니다. 빈 필드 값이 이 옵션을 비활성화합니다. 0 값은 무제한 중첩 세그먼트 수를 지정합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. 중첩되는 프래그먼트는 이러한 인터페이스에서는 항상 삭제됩니다.

규칙 123:12를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

최소 조각 크기

구성된 바이트 수보다 작은, 마지막이 아닌 조각이 탐지된 경우 패킷이 악성으로 간주됨을 명시합니다.

이 옵션을 구성하려면 **Detect Anomalies(**이상 징후 탐지**)**를 활성화해야 합니다. 빈 필드 값이 이 옵션을 비활성화합니다. 0 값은 무제한 바이트 수를 지정합니다.

규칙 123:13을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

IP 조각 모음 구성

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정, 2203 페이지를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **IP Defragmentation(IP** 조각 모음**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **IP Defragmentation(IP** 조각 모음**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** 원한다면 **Preallocated Fragments(**미리 할당된 프래그먼트**)** 필드에 값을 입력합니다.

단계 **7** 다음 옵션을 이용할 수 있습니다.

- 서버 프로파일 추가 - 패널 왼쪽의 **Servers(**서버**)** 옆에 있는 추가( )을 클릭하고, **Host Address(**호스트 주소**)** 필드에 값을 입력한 다음 **OK(**확인**)**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255가지 대상 기반 정책을 생성할 수 있습니다.
- 서버 프로파일 편집 - 패널 왼쪽의 **Servers(**서버**)**에서 설정한 주소를 클릭하거나 **default(**기본값**)**를 클릭합니다.
- 프로파일 삭제 - 정책 옆에 있는 삭제( )을 클릭합니다.

단계 **8** IP 조각 모음 옵션, 2325 페이지에 설명된 대로 옵션을 수정합니다.

단계 **9** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 IP 조각 모음 규칙(GID 123)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지 및 IP 조각 모음 옵션, 2325 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지
레이어 기본 사항, 1979 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

패킷 디코더

시스템은 전처리기에 캡처된 패킷을 보내기 전에 먼저 패킷 디코더에 패킷을 보냅니다. 패킷 디코더는 패킷 헤더와 페이로드를 전처리기 및 규칙 엔진이 쉽게 사용할 수 있는 형식으로 변환합니다. 각 스택 레이어는 데이터 링크 레이어에서 시작해서 네트워크 및 전송 레이어에 이르기까지 계속해서 차례로 디코딩됩니다.

패킷 디코더 옵션

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

GTP 데이터 채널 디코딩

캡슐화된 GTP(GPRS[General Packet Radio Service] 터널링 프로토콜) 데이터 채널을 디코딩합니다. 기본적으로, 디코더는 포트 3386의 버전 0 데이터 및 포트 2152의 버전 1 데이터를 디코딩합니다. `GTP_PORTS` 기본 변수를 사용하여 캡슐화된 GTP 트래픽을 식별하는 포트를 수정할 수 있습니다.

규칙 116:297 및 116:298을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

비표준 포트에서 **Teredo** 탐지

포트 3544 이외의 UDP 포트에서 확인된 IPv6 트래픽의 Teredo 터널링을 검사합니다.

IPv6 트래픽이 있으면 항상 시스템에서 검사합니다. 기본적으로, IPv6 검사에는 4in6, 6in4, 6to4 및 6in6 터널링 체계가 포함되며, UDP 헤더가 포트 3544를 지정하는 경우에는 Teredo 터널링도 포함됩니다.

IPv4 네트워크에서 IPv4 호스트는 Teredo 프로토콜을 사용하여 IPv4 NAT(Network Address Translation) 디바이스를 통해 IPv6 트래픽을 터널링할 수 있습니다. Teredo는 IPv4 NAT 디바이스의 배후에 있는 IPv6 연결을 허용하기 위해 IPv4 UDP 데이터그램 안에서 IPv6 패킷을 캡슐화합니다. 시스템은 일반적으로 UDP 포트 3544를 사용하여 Teredo 트래픽을 식별합니다. 그러나 공격자는 탐지를 피하기 위해 비표준 포트를사용할 수 있습니다. **Detect Teredo on Non-Standard Ports(**비표준 포트에서 **Teredo** 탐지**)**를 활성화하여 시스템이 Teredo 터널링의 모든 UDP 페이로드를 검사하도록 할 수 있습니다.

Teredo 디코딩은 첫 번째 UDP 헤더에서만, 그리고 IPv4가 외부 네트워크 레이어에 사용될 때만 수행됩니다. IPv6 데이터에서 캡슐화된 UDP 데이터로 인해 Teredo IPv6 레이어 다음에 두 번째 UDP 레이어가 나타나는 경우 규칙 엔진은 UDP 침입 규칙을 사용하여 내부 및 외부 UDP 레이어를 분석합니다.

정책-기타 규칙 카테고리의 침입 규칙 12065, 12066, 12067 및 12068은 Teredo 트래픽을 탐지하지만 디코딩하지는 않는다는 점에 유의하십시오. 필요에 따라 이러한 규칙을 사용하여 인라인 구축에서 Teredo 트래픽을 삭제할 수 있습니다. 하지만 **Detect Teredo on Non-Standard Ports(**비표준 포트에서 **Teredo** 탐지**)**를 활성화할 때는 이러한 규칙이 비활성화되어 있거나 트래픽을 삭제하지 않고 이벤트를 생성하도록 설정되어 있는지 확인해야 합니다.

과도한 길이 값 탐지

패킷 헤더가 실제 패킷 길이보다 큰 패킷 길이를 지정할 때를 탐지합니다.

이 옵션은 FTD 라우팅, 투명 및 인라인 인터페이스에 대해서는 무시됩니다. 헤더 길이가 너무 긴 패킷은 항상 삭제됩니다. 그러나 이 옵션은 FTD 인라인 탭과 수동 인터페이스에는 적용되지 않습니다.

규칙 116:6, 116:47, 116:97 및 116:275를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

유효하지 않은 **IP** 옵션 탐지

유효하지 않은 IP 옵션을 사용하는 익스플로잇을 식별하기 위해 유효하지 않은 IP 헤더 옵션을 탐지합니다. 예를 들어, 시스템을 마비시키는 방화벽에 대한 DoS(Denial-of-Service) 공격이 존재합니다. 방화벽은 유효하지 않은 Timestamp(타임 스탬프) 및 Security IP(보안 IP) 옵션의 분석을 시도하고 제로 길이를 점검하는 데 실패하는데, 이는 복구할 수 없는 무한 루프를 야기합니다. 규칙 엔진은 제로 길이 옵션을 식별하고, 방화벽에서 공격을 완화하는 데 사용할 수 있는 정보를 제공합니다.

FTD 디바이스는 라우터 알림, 옵션 목록의 끝(EOOL), 특정 라우팅 또는 투명 인터페이스의 작업 없음(NOP)을 제외한 다른 IP 옵션을 포함하는 RSVP 패킷은 모두 삭제합니다. 인라인, 인라인 탭 또는 수동 인터페이스의 경우 IP 옵션은 위에서 설명한 대로 처리됩니다.

규칙 116:4 및 116:5를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

실험적 **TCP** 옵션 탐지

실험적 TCP 옵션이 포함된 TCP 헤더를 탐지합니다. 다음 표는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
9	허용된 부분 순서 연결
10	부분 순서 서비스 프로파일
14	대체 체크섬 요청
15	대체 체크섬 데이터
18	트레일러 체크섬
20	우주 통신 프로토콜 표준(SCPS)
21	선택적 부정적 수신 확인(SCPS)
22	레코드 경계(SCPS)
23	손상(SPCS)
24	SNAP
26	TCP 압축 필터

이는 실험적 옵션이므로, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다.

참고 위 표에 나열된 실험적 옵션 외에도, 시스템은 26보다 큰 옵션 번호를 가진 모든 TCP 옵션을 실험적인 것으로 고려합니다.

규칙 116:58을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

사용하지 않는 **TCP** 옵션 탐지

사용하지 않는 TCP 옵션이 포함된 TCP 헤더를 탐지합니다. 이는 사용하지 않는 옵션이므로, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 다음 표는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
6	에코
7	에코 응답
16	Skeeter
17	Bubba
19	MD5 서명
25	Unassigned(지정되지 않음)

규칙 116:57을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

T/TCP 탐지

CC.ECHO 옵션이 포함된 TCP 헤더를 탐지합니다. CC.ECHO 옵션은 TCP for Transactions(트랜잭션용 TCP, T/TCP)가 사용되고 있음을 확인합니다. T/TCP 헤더 옵션은 널리 사용되지 않기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다.

규칙 116:56을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

기타 **TCP** 옵션 탐지

다른 TCP 디코딩 이벤트 옵션으로 탐지되지 않는 유효하지 않은 TCP 옵션을 통해 TCP 헤더를 탐지합니다. 예를 들어, 이 옵션은 정확하지 않은 길이 또는 옵션 데이터를 TCP 헤더 외부에 배치하는 길이를 가진 TCP 옵션을 탐지합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. 잘못된 TCP 옵션이 있는 패킷은 항상 삭제됩니다.

규칙 116:54, 116:55 및 116:59를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

프로토콜 헤더 이상 징후 탐지

더 많은 특정 IP 및 TCP 디코더 옵션으로 탐지되지 않는 다른 디코딩 오류를 탐지합니다. 예를 들어 디코더는 잘못된 형식의 데이터 연결 프로토콜 헤더를 탐지할 수 있습니다.

이 옵션은 FTD 라우팅, 투명 및 인라인 인터페이스에 대해서는 무시됩니다. 헤더 이상 징후가 있는 패킷은 항상 삭제됩니다. 그러나 이 옵션은 Threat Defense(위협 방어) 인라인 탭과 수동 인터페이스에는 적용되지 않습니다.

이 옵션을 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 다음 규칙 중 하나를 활성화해야 합니다.

GID: SID	다음 경우에 이벤트를 생성합니다.
116:467	패킷이 Cisco FabricPath 헤더로 캡슐화한 패킷의 최소 크기보다 작습니다.
116:468	헤더의 CMD(Cisco Meta Data) 필드에 유효한 CMD 헤더의 최소 크기보다 작은 헤더 길이가 포함되어 있습니다. CMD 필드는 Cisco Trustsec 프로토콜과 연결됩니다.
116:469	헤더의 CMD 필드에 잘못된 필드 길이가 포함되어 있습니다.
116:470	헤더의 CMD 필드에 잘못된 SGT(Security Group Tag, 보안 그룹 태그) 옵션 유형이 있습니다.
116:471	헤더의 CMD 필드에 예약한 값이 있는 SGT가 포함되어 있습니다.

또한 다른 패킷 디코더 옵션과 연결되지 않은 패킷 디코더 규칙은 무엇이든 활성화할 수 있습니다.

관련 항목

사전 정의된 기본 변수, 582 페이지

패킷 복호화 구성

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **Packet Decoding(**패킷 디코딩**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **Packet Decoding(**패킷 디코딩**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** 패킷 디코더 옵션, 2330 페이지에 설명된 대로 옵션을 활성화 또는 비활성화합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 패킷 디코더 규칙 (GID 116)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지 및 패킷 디코더 옵션, 2330 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 기본 사항, 1979 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

TCP 스트림 전처리

TCP 프로토콜은 연결이 존재할 수 있는 다양한 상태를 정의합니다. 각 TCP 연결은 소스 및 대상 IP 주소와 소스 및 대상 포트에 의해 식별됩니다. TCP는 동일한 연결 매개 변수 값을 가진 연결이 한 번에 하나만 존재하도록 허용합니다.

상태 관련 TCP 익스플로잇

침입 규칙에 `established` 인수로 `flow` 키워드를 추가한 경우, 침입 규칙 엔진은 상태 저장 모드에서 규칙 및 지시와 일치하는 패킷을 검사합니다. 상태 저장 모드는 클라이언트와 서버 사이의 적정 3방향 핸드셰이크로 설정된 TCP 세션의 일부인 트래픽만 평가합니다.

전처리기가 설정된 TCP 세션의 일부로 식별할 수 없는 모든 TCP 트래픽을 검색하도록 시스템을 구성할 수 있습니다. 그러나 이벤트가 시스템의 빠른 과부하를 야기하고 의미 있는 데이터를 제공하지 않으므로 일반적인 사용에는 권장되지 않습니다.

stick 및 snot과 같은 공격은 시스템의 광범위한 규칙 집합 및 자체 패킷 검사를 사용합니다. 이 도구는 Snort 기반 침입 규칙의 패턴에 따라 패킷을 생성하고, 네트워크를 통해 전송합니다. 사용자 규칙이 상태 저장 검사를 위한 규칙 구성을 위해 `flow` 또는 `flowbits` 키워드를 포함하지 않은 경우, 각 패킷은 규칙을 트리거하여 시스템을 마비시킵니다. 이러한 패킷은 설정된 TCP 세션의 일부가 아니며 의미 있는 정보를 제공하지 않으므로 상태 저장 검사를 통해 패킷을 무시할 수 있습니다. 상태 저장 검사를 수행하는 경우, 규칙 엔진은 설정된 TCP 세션의 일부인 해당 공격만 탐지하므로 분석가가 stick 또는 snot으로 인해 발생하는 이벤트 볼륨이 아닌 해당 공격에 집중할 수 있습니다.

대상 기반 **TCP** 정책

서로 다른 운영 체제는 TCP를 서로 다른 방식으로 구현합니다. 예를 들어, Windows 및 일부의 다른 운영 체제에서 세션을 재설정하려면 정확한 TCP 시퀀스 번호를 지닌 TCP 재설정 세그먼트가 필요한 반면, Linux 및 기타 운영 체제에서는 다양한 시퀀스 번호를 허용합니다. 이 예제에서, 스트림 전처리기는 대상 호스트가 시퀀스 번호에 근거한 재설정에 대응하는 방식을 정확하게 이해해야 합니다. 스트림 전처리기는 대상 호스트가 재설정을 유효한 것으로 간주하는 경우에 한해 세션 추적을 중지하므로, 전처리기가 스트림 검사를 중지한 후 공격이 패킷을 전송하여 탐지를 우회할 수 없습니다. TCP 구현의 다른 변경 사항에는 운영 체제가 TCP 타임 스탬프 옵션을 채택하는지 여부 등이 포함되 있으며, 이를 포함할 경우 타임 스탬프를 처리하는 방식 및 운영 체제가 SYN 패킷의 데이터를 수락하거나 무시하는지 여부를 포함합니다.

다양한 운영 체제는 또한 중첩되는 TCP 세그먼트를 다양한 방법으로 리어셈블합니다. 중첩되는 TCP 세그먼트는 접수되지 않은 일반 재전송을 반영할 수 있습니다. 세그먼트는 또한 호스트 중 하나의 운영 체제를 알고 있는 공격자가 중첩되는 세그먼트에 숨겨진 악성 콘텐츠를 전송하여 탐지를 우회하고 해당 호스트를 공격하는 시도를 나타낼 수 있습니다. 그러나, 스트림 전처리기를 구성하여 모니터링된 네트워크 세그먼트에서 실행되는 운영 체제를 인식할 수 있으며, 따라서 이는 대상 호스트가 하는 것과 동일한 방법으로 세그먼트를 리어셈블하여 공격을 식별하도록 허용합니다.

하나 이상의 TCP 정책을 만들어서 TCP 스트림 검사 및 리어셈블리를 모니터링된 네트워크 세그먼트에서 다른 운영 체제로 조정할 수 있습니다. 각 정책에 대해 13개 운영 체제 정책 중 하나를 확인합니다. 다른 운영 체제를 사용하는 호스트의 일부 또는 전체를 식별하기 위해 필요한 만큼 많은 TCP 정책을 사용하여 각 TCP 정책을 특정 IP 주소 또는 주소 블록에 바인딩합니다. 기본 TCP 정책은 다른 TCP 정책에서 식별하지 않는 모니터링된 네트워크의 모든 호스트에 적용되므로 기본 TCP 정책에 대한 IP 주소 또는 주소 블록을 지정할 필요가 없습니다.

또한 수동 구축에서 적응형 프로파일을(를) 사용하여 패킷의 대상 호스트에 대한 호스트 운영체제 정보를 통해 TCP 스트림 전처리기의 대상 기반 정책을 동적으로 선택할 수도 있습니다.

TCP 스트림 리어셈블리

스트림 전처리기는 TCP 세션의 서버-클라이언트 통신 스트림, 클라이언트-서버 통신 스트림, 또는 둘 다에 속하는 모든 패킷을 수집하고 리어셈블합니다. 이를 통해 규칙 엔진은 주어진 스트림에 속하는 개별 패킷만 검사하는 것이 아니라 단일, 리어셈블된 엔터티로서의 스트림을 검사할 수 있습니다.

규칙 엔진은 스트림 리어셈블리를 통해 개별 패킷 검사에서는 탐지하지 못할 수 있는 스트림 기반 공격을 식별할 수 있습니다. 규칙 엔진이 네트워크의 필요에 따라 리어셈블할 통신 스트림을 지정할 수 있습니다. 예를 들어, 사용자 웹 서버에서 트래픽을 모니터링하는 경우에는 본인의 웹 서버로부터 악성 트래픽을 수신할 가능성이 거의 없으므로 클라이언트 트래픽만 검사하기를 원할 수 있습니다.

각 TCP 정책에서 스트림 전처리기가 리어셈블할 트래픽을 식별하는, 쉼표로 구분된 포트 목록을 지정할 수 있습니다. 적응형 프로파일을(를) 활성화하는 경우, 포트에 대한 대안으로 또는 포트와 조합하여 리어셈블할 트래픽을 식별하는 서비스를 나열할 수 있습니다.

포트, 서비스, 또는 둘 다를 지정할 수 있습니다. 클라이언트 포트, 서버 포트 및 둘 다의 모든 조합에 대해 포트의 개별 목록을 지정할 수 있습니다. 또한 클라이언트 서비스, 서버 서비스 및 둘 다의 모든 조합에 대해 서비스의 개별 목록을 지정할 수 있습니다. 예를 들어 다음을 리어셈블하기를 원하는 것으로 가정합니다.

- 클라이언트로부터의 SMTP(포트 25) 트래픽
- FTP 서버 응답(포트 21)
- 두 방향 모두에서의 텔넷(포트 23) 트래픽

다음을 구성할 수 있습니다.

- 클라이언트 포트에 대해, `23, 25`를 지정합니다.
- 서버 포트에 대해, `21, 23`을 지정합니다.

또는, 그 대신, 다음을 설정할 수 있습니다.

- 클라이언트 포트에 대해, `25`를 지정합니다.
- 서버 포트에 대해, `21`을 지정합니다.
- 두 포트 모두에 대해, `23`을 지정합니다.

또한 포트 및 서비스를 결합하고 적응형 프로파일을(를) 활성화하는 경우 유효하게 될 다음 예를 고려하십시오.

- 클라이언트 포트에 대해, `23`을 지정합니다.
- 클라이언트 서비스에 대해, `smtp`를 지정합니다.
- 서버 포트에 대해, `21`을 지정합니다.
- 서버 서비스에 대해, `telnet`을 지정합니다.

포트를 무효화(예: `!80`)하면 TCP 스트림 전처리기가 해당 포트에 대한 트래픽 처리를 차단하여 성능을 높일 수 있습니다.

모든 포트에 대해 리어셈블리를 제공하려면 `all`을 인수로 지정할 수도 있지만, 그렇게 하면 이 전처리기에서 검사하는 트래픽의 양이 증가하여 불필요하게 성능이 저하될 수 있으므로 Cisco는 포트를 `all`로 설정하는 것을 권장하지 않습니다.

TCP 리어셈블리는 다른 전처리기에 추가한 포트를 자동으로 포함합니다. 그러나, 다른 전처리기 구성에 추가한 TCP 리어셈블리 목록에 포트를 명확하게 추가한 경우, 이러한 추가 포트는 정상적으로 처리됩니다. 여기에는 다음 전처리기를 위한 포트 목록이 포함됩니다.

- FTP/Telnet(서버 수준 FTP)
- DCE/RPC
- HTTP 검사
- SMTP
- 세션 시작 프로토콜
- POP
- IMAP
- SSL

추가 트래픽 유형(클라이언트, 서버, 둘 다)을 리어셈블하면 리소스 요구가 증대된다는 점에 유의하십시오.

TCP 스트림 전처리 옵션

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

다음 전역 TCP 옵션을 구성할 수 있습니다.

패킷 유형 성능 증대

활성화된 침입 규칙에 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 TCP 트래픽 무시를 활성화합니다. 단, 소스 및 목적지 포트가 모두 `any`로 설정된 TCP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 예외입니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다.

각 TCP 정책에 대해 다음 옵션을 구성할 수 있습니다.

네트워크

사용자가 TCP 스트림 리어셈블리 정책을 적용할 호스트 IP 주소를 지정합니다.

단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 비롯한 255개의 총 프로파일을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

정책

대상 호스트의 TCP 정책 운영 체제를 식별합니다. **Mac OS** 이외의 정책을 선택하는 경우, 시스템은 동기화(SYN) 패킷에서 데이터를 제거하고 규칙 129:2의 이벤트 생성을 비활성화합니다. 인라인 표준화 전처리기 **Remove Data on SYN(SYN**에서 데이터 제거**)** 옵션을 활성화하면 규칙 129:2도 비활성화됩니다.

다음 표는 각각을 사용하는 호스트 운영 체제 및 운영 체제 정책을 식별합니다.

표 ***237: TCP*** 운영 체제 정책

정책	**Operating Systems(**운영 체제**)**
First	알 수 없는 OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 커널 Linux 2.6 커널
이전 Linux	Linux 2.2 및 이전 커널
(Windows용)	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 이상
HPUX 10	HP-UX 10.2 이하

정책	**Operating Systems**(운영 체제)
Mac OS	Mac OS 10(Mac OS X)

팁 First 운영 체제 정책에서는 호스트 운영 체제를 알 수 없는 경우 일부 보호를 제공할 수 있습니다. 하지만, 이로 인해 공격이 누락될 수 있습니다. 알고 있는 경우 정확한 운영 체제를 지정하는 정책을 수정해야 합니다.

시간 초과

1에서 86400 사이의 시간(단위: 초)으로, 침입 규칙 엔진이 이 시간 동안 상태 표에서 비활성 스트림을 유지합니다. 스트림이 지정된 시간에 리어셈블되지 않는 경우, 침입 규칙 엔진은 이를 상태 표에서 삭제합니다.

참고 관리되는 디바이스가 네트워크 트래픽이 디바이스의 대역폭 제한에 도달할 가능성이 높은 세그먼트에 구축된 경우, 처리 오버헤드의 양을 낮추기 위해 이 값을 더 높게(예: 600초) 설정할 것을 고려해야 합니다.

FTD 디바이스는 이 옵션을 무시하며, 대신 고급 액세스 컨트롤 **Threat Defense Service Policy**(위협 방어 서비스 정책)의 설정을 사용합니다. 자세한 내용은 서비스 정책 규칙 구성, 1253 페이지를 참조하십시오.

최대 **TCP** 창

수신 호스트가 지정한 대로 허용된 1에서 1073725440바이트 사이의 최대 TCP 창 크기를 지정합니다. 값을 0으로 설정하면 TCP 창 크기 확인이 비활성화됩니다.

주의 상한은 RFC에서 허용하는 최대 창 크기이며 공격자의 탐지 회피를 방지하는 것이 목적이지만, 최대 창 크기를 너무 크게 설정하면 자체적으로 서비스 거부가 발생할 수 있습니다.

Stateful Inspection Anomalies(상태 저장 검사 이상 징후)가 활성화되면 이 옵션에 대해 규칙 129:6을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

중첩 제한

세션에서 중첩되는 세그먼트에 대해 0(무제한)과 255 사이의 구성된 번호가 탐지된 경우 해당 세션을 위한 세그먼트 리어셈블리가 중단되며, **Stateful Inspection Anomalies**(상태 저장 검사 이상 징후)가 활성화되고 동반되는 전처리기 규칙이 활성화된 경우 이벤트가 생성된다는 것을 지정합니다.

규칙 129:7을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

플러시 배율

인라인 구축에서, 비감소 크기의 세그먼트 1~2048 사이로 구성된 수에 이어 감소 크기의 세그먼트가 탐지된 경우 시스템은 탐지를 위해 누적된 세그먼트 데이터를 플러시합니다. 값을 0으로 설정하면 이러한 세그먼트 패턴의 탐지가 비활성화되며, 이는 요청 또는 응답의 종료를 나타낼 수 있습니다. 이 옵션을 적용하려면 Inline Normalization(인라인 표준화) **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화되어야 한다는 점에 유의하십시오.

상태 저장 검사 이상 징후

TCP 스택에서 비정상적 상태를 탐지합니다. TCP/IP 스택이 잘못 로깅된 경우 동반되는 전처리기 규칙이 활성화되면 이로 인해 많은 이벤트가 생성될 수 있습니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

다음 규칙을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

- 129:1~129:5
- 129:6(Mac OS만 해당)
- 129:8~129:11
- 129:13~129:19

다음에 유의하십시오.

- 규칙 129:6이 트리거되려면 **Maximum TCP Window(**최대 **TCP** 창**)**에 0보다 큰 값을 구성해야 합니다.
- 규칙 129:9 및 129:10이 트리거되려면 **TCP Session Hijacking(TCP** 세션 가로채기**)**도 활성화해야 합니다.

TCP 세션 가로채기

세션에서 수신된 후속 패킷에 대한 3방향 핸드셰이크 동안 TCP 연결의 양쪽에서 탐지된 하드웨어(MAC) 주소를 검증하여 TCP 세션 가로채기를 탐지합니다. 한쪽 또는 다른 쪽의 MAC 주소가 일치하지 않으면, **Stateful Inspection Anomalies**가 활성화되고 두 개의 해당 프리프로세서 규칙 중 하나가 활성화된 경우 시스템이 이벤트를 생성합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

규칙 129:9 및 129:10을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 이러한 규칙 중 하나가 이벤트를 생성하려면 **Stateful Inspaction Anomalies(**상태 저장 검사 이상 징후**)**도 활성화해야 합니다.

연속된 소규모 세그먼트

Stateful Inspection Anomalies가 활성화된 경우, 허용되는 연속 소형 TCP 세그먼트의 최대 수를 1~2048 범위로 지정합니다. 값을 0으로 설정하면 소규모 연속 세그먼트 확인이 비활성화됩니다.

이 옵션은 **Small Segment Size(**소규모 세그먼트 크기**)** 옵션과 함께 설정해야 합니다. 둘 다 비활성화하거나 둘 다 0이 아닌 값으로 설정합니다. 각 세그먼트의 길이가 1바이트라고 해도 개입 ACK 없이 최대 2000개의 연속 세그먼트를 수신하는 경우 일반적으로 예상하는 것보다 훨씬 많은 연속 세그먼트일 수 있음에 유의하십시오.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

규칙 129:12를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

소규모 세그먼트 크기

Stateful Inspection Anomalies가 활성화된 경우, 소형으로 간주되는 1~2048바이트의 TCP 세그먼트 크기를 지정합니다. 값을 0으로 설정하면 소규모 세그먼트의 크기가 비활성화됩니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

이 옵션은 **Consecutive Small Segment Size(**연속된 소규모 세그먼트 크기**)** 옵션과 함께 설정해야 합니다. 둘 다 비활성화하거나 둘 다 0이 아닌 값으로 설정합니다. 2048바이트 TCP 세그먼트는 일반적인 1500바이트 이더넷 프레임보다 크다는 점에 유의하십시오.

Ports Ignoring Small Segments(소규모 세그먼트를 무시하는 포트**)**

Stateful Inspection Anomalies(상태 저장 검사 이상 징후**)**, **Consecutive Small Segment Size(**연속된 소규모 세그먼트**)** 및 **Small Segment Size(**소규모 세그먼트 크기**)**가 활성화된 경우, 소규모 TCP 세그먼트 탐지를 무시하는 쉼표로 구분된 하나 이상의 포트 목록을 지정합니다. 이 옵션을 비워 두면 어떤 포트도 무시되지 않습니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

어느 포트든 목록에 추가할 수 있지만, 목록은 TCP 정책 내 **Perform Stream Reassembly on(**스트림 리어셈블리 수행**)** 포트 목록 중 하나에서 지정된 포트에만 영향을 미칩니다.

TCP 3방향 핸드셰이크 요청

TCP 3방향 핸드셰이크가 완료되는 경우에만 세션을 설정된 것으로 처리하도록 지정합니다. 성능을 향상시키고, SYN 플러드 공격으로부터 보호하며, 부분 비동기 환경에서 작업을 허용하려면 이 옵션을 비활성합니다. 설정된 TCP 세션의 일부가 아닌 정보를 전송하여 잘못된 긍정을 생성하려고 시도하는 공격을 차단하려면 이 옵션을 활성화합니다.

규칙 129:20을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

3방향 핸드셰이크 시간 제한

Require TCP 3-Way Handshake(TCP 3방향 핸드셰이크 요청**)**가 활성화된 경우 핸드셰이크 완료 기한이 되는 시간(단위: 초)을 0(무제한)에서 86400(24시간)까지의 범위에서 지정합니다. 이 옵션의 값을 수정하려면 **Require TCP 3-Way Handshake(TCP 3**방향 핸드셰이크 요청**)**를 활성화해야 합니다.

Firepower Software 디바이스 및 FTD 인라인, 인라인, 패시브 인터페이스의 경우, 기본값은 0입니다. FTD 라우팅 및 투명 인터페이스의 경우, 시간 초과는 항상 30 초이며, 여기서 구성된 값은 무시됩니다.

패킷 크기 성능 증대

전처리기가 리어셈블리 버퍼에서 대규모 패킷을 큐에 넣지 않도록 설정합니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다. 1~20바이트의 소규모 패킷을 사용하여 회피 시도를 차단하려면 이 옵션을 비활성화합니다. 모든 트래픽이 매우 큰 패킷으로 구성되어 있어서 그러한 공격이 없을 것임을 확신하는 경우 이 옵션을 활성화합니다.

레거시 리어셈블리

패킷을 리어셈블할 때 스트림 전처리기가 더 이상 사용되지 않는 Stream 4(스트림 4) 전처리기를 모방하도록 설정하여 스트림 전처리기가 리어셈블한 이벤트를 Stream 4(스트림 4) 전처리기가 리어셈블한 동일 데이터 스트림에 기반한 이벤트와 비교할 수 있습니다.

비동기 네트워크

모니터링된 네트워크가 비동기 네트워크, 즉, 시스템이 트래픽의 절반만 표시하는 네트워크인지 여부를 지정합니다. 이 옵션을 활성화할 경우, 시스템은 성능을 높이기 위해 TCP 스트림을 리어셈블하지 않습니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

클라이언트 포트에서 스트림 리어셈블리 수행

연결의 클라이언트 측 포트에 기반한 스트림 리어셈블리를 활성화합니다. 다시 말해, 일반적으로 $HOME_NET에 지정된 IP 주소에 의해 정의되는 웹 서버, 메일 서버, 또는 다른 IP 주소로 전송되는 스트림을 리어셈블합니다. 악성 트래픽이 클라이언트에서 시작될 것으로 예상되는 경우 이 옵션을 사용하십시오.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

클라이언트 서비스에서 스트림 리어셈블리 수행

연결의 클라이언트 측을 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 악성 트래픽이 클라이언트에서 시작될 것으로 예상되는 경우 이 옵션을 사용하십시오.

선택한 각 클라이언트 서비스에 대해 하나 이상의 클라이언트 탐지기가 활성화되어야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 연결된 클라이언트 애플리케이션에 활성화된 탐지기가 없는 경우, 시스템은 해당 애플리케이션의 모든 Cisco 제공 탐지기를 자동으로 활성화합니다. 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 해당 애플리케이션의 사용자 정의 탐지기를 활성화합니다.

이 기능을 사용하려면 보호 및 제어 라이선스가 필요합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

서버 포트에서 스트림 리어셈블리 수행

연결의 서버 측만을 위한 포트에 기반한 스트림 리어셈블리를 활성화합니다. 다시 말해, 일반적으로 $EXTERNAL_NET에 지정된 IP 주소에 의해 정의되는 웹 서버, 메일 서버, 또는 다른 IP 주소에서 시작되는 스트림을 리어셈블합니다. 서버 측 공격을 경계하고자 하는 경우 이 옵션을 사용합니다. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

참고 철저한 서비스 검사를 위해서는 Perform Stream Reassembly on Server Ports(서버 포트에서 스트림 리어셈블리 수행) 필드에 포트 번호를 추가하는 것 외에도 Perform Stream Reassembly on Server Services(서버 서비스에서 스트림 리어셈블리 수행) 필드에 서비스 이름을 추가합니다. 예를 들어 Perform Stream Reassembly on Server Ports(서버 포트에서 스트림 리어셈블리 수행) 필드에 포트 번호 80을 추가하는 것 외에도 Perform Stream Reassembly on Server Services(서버 서비스에서 스트림 리어셈블리 수행) 필드에 **'HTTP'** 서비스를 추가합니다.

서버 서비스에서 스트림 리어셈블리 수행

연결의 서버 측만을 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 서버 측 공격을 경계하고자 하는 경우 이 옵션을 사용합니다. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

하나 이상의 탐지기를 활성화해야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 서비스에 활성화된 탐지기가 없는 경우, 시스템은 연결된 애플리케이션 프로토콜의 모든 Cisco 제공 탐지기를 자동으로 활성화합니다. 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 애플리케이션 프로토콜의 사용자 정의 탐지기를 활성화합니다.

이 기능을 사용하려면 보호 및 제어 라이선스가 필요합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

두 포트 모두에서 스트림 리어셈블리 수행

연결의 클라이언트 및 서버 측 모두를 위한 포트에 기반한 스트림 리어셈블리를 활성화합니다. 동일한 포트의 악성 트래픽이 클라이언트와 서버 사이에서 어느 방향에서나 이동할 수 있을 것으로 예상되는 경우 이 옵션을 사용하십시오. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

두 서비스 모두에서 스트림 리어셈블리 수행

연결의 클라이언트 및 서버 측 모두를 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 동일한 서비스의 악성 트래픽이 클라이언트와 서버 사이에서 어느 방향에서나 이동할 수 있을 것으로 예상되는 경우 이 옵션을 사용하십시오. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

하나 이상의 탐지기를 활성화해야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 연결된 클라이언트 애플리케이션 또는 애플리케이션 프로토콜에 대해 활성화된 탐지기가 없을 경우 해당 애플리케이션 또는 애플리케이션 프로토콜에 대해 자동으로 모든 Cisco 제공 탐지기가 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션 또는 애플리케이션 프로토콜에 대해 활성화됩니다.

이 기능을 사용하려면 보호 및 제어 라이선스가 필요합니다.

이 옵션은 FTD 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

문제 해결 옵션: 최대 대기 바이트

Support(지원팀)는 문제 해결 통화 중 사용자에게 TCP 연결의 한 쪽에 대기될 수 있는 데이터의 양을 지정하도록 요청할 수 있습니다. 0 값은 무제한 바이트 수를 지정합니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

문제 해결 옵션: 최대 대기 세그먼트

Support(지원팀)는 문제 해결 통화 중 사용자에게 TCP 연결의 한 쪽에 대기될 수 있는 세그먼트의 최대 바이트 수를 지정하도록 요청할 수 있습니다. 0 값은 무제한 데이터 세그먼트 바이트 수를 지정합니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지
탐지기 활성화 및 비활성화, 2456 페이지
레이어 관리, 1985 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

TCP 스트림 전처리 구성

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정, 2203 페이지를 참조하십시오.

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 NAT 정책 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 왼쪽 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** Transport/Network Layer Preprocessors(전송/네트워크 계층 전처리기)의 **TCP Stream Configuration(TCP** 스트림 설정**)** 설정이 비활성화되어 있다면 **Enabled**를 클릭해 활성화합니다.

단계 **5** **TCP Stream Configuration(TCP** 스트림 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Global Settings(**전역 설정**)** 섹션의 **Packet Type Performance Boost(**패킷 유형 성능 증대**)** 확인란을 선택하거나 선택 취소합니다.

단계 **7** 다음 작업을 수행할 수 있습니다.

- 대상 기반 정책 추가 - Targets(대상) 섹션의 **Hosts(**호스트**)** 옆에 있는 추가( )를 클릭합니다. **Host Address(**호스트 주소**)** 필드에 하나 이상의 IP 주소를 지정합니다. 단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255가지 대상 기반 정책을 생성할 수 있습니다. 완료되면 **OK(**확인**)**를 클릭합니다.
- 기존 대상 기반 정책 편집 - **Hosts(**호스트**)**에서 편집할 정책의 주소를 클릭하거나, default(기본값)를 클릭해 기본 설정값을 편집합니다.
- TCP Stream Preprocessing(TCP 스트림 전처리) 옵션을 수정합니다(TCP 스트림 전처리 옵션, 2337 페이지 참조).

  주의 지원팀이 지시할 때만 **Maximum Queued Bytes(**최대 대기 바이트**)** 또는 **Maximum Queued Segments(**최대 대기 세그먼트**)**를 수정하십시오.

  팁 클라이언트, 서버 또는 두 서비스를 기반으로 스트림 리어셈블리 설정을 수정하려면 수정할 필드 내부를 클릭하거나 필드 옆에 있는 **Edit(**편집**)**를 클릭합니다. 화살표를 이용하여 팝업 창의 **Available(**사용 가능**)** 및 **Enabled(**활성화**)** 목록에서 서비스를 이동한 다음 **OK(**확인**)**를 클릭합니다.

- 기존 대상 기반 정책 삭제 - 제거할 정책 옆에 있는 삭제( )를 클릭합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 TCP Stream(TCP 스트림) 전처리기 규칙(GID 129)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지 및 TCP 스트림 전처리 옵션, 2337 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1985 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지
Firepower System IP 주소 규칙, 19 페이지

UDP 스트림 전처리

UDP 스트림 전처리는 규칙 엔진이 다음 인수 중 하나를 사용하여 `flow` 키워드를 포함하는 UDP 규칙에 대해 패킷을 처리할 때 발생합니다.

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP 데이터 스트림은 세션의 측면에서는 일반적으로 고려되지 않습니다. UDP는 커뮤니케이션 채널을 설정하고, 데이터를 교환하며, 채널을 종료하는 두 엔드포인트를 위한 수단을 제공하지 않는 비연결형 프로토콜입니다. 그러나, 스트림 전처리기는 흐름의 방향을 결정하고 세션을 확인하기 위해 캡슐화하는 IP 데이터그램 헤더의 소스 및 대상 IP 주소 필드, 그리고 UDP 헤더의 포트 필드를 사용합니다. 구성 가능한 타이머가 초과되는 경우, 또는 둘 중 한 쪽의 엔드포인트가 다른 엔드포인트에 도달할 수 없거나 요청된 서비스가 사용할 수 없다는 ICMP 메시지를 수신한 경우 세션이 종료됩니다.

시스템이 UDP 스트림 전처리와 관련된 이벤트를 생성하지 않는다는 점에 유의하십시오. 하지만, 관련된 패킷 디코더 규칙을 활성화하여 UDP 프로토콜 헤더 이상 징후를 탐지할 수 있습니다.

관련 항목

TCP 헤더 값 및 스트림 크기, 2129 페이지

UDP 스트림 전처리 옵션

시간 초과

전처리기가 상태 표에서 비활성 스트림을 유지하는 시간(단위: 초)을 지정합니다. 추가 데이터그램이 지정된 시간 안에 표시되지 않으면, 전처리기는 상태 표에서 스트림을 삭제합니다.

FTD 디바이스는 이 옵션을 무시하며, 대신 고급 액세스 컨트롤 **Threat Defense Service Policy(**위협 방어 서비스 정책**)**의 설정을 사용합니다. 자세한 내용은 서비스 정책 규칙 구성, 1253 페이지를 참조하십시오.

패킷 유형 성능 증대

활성화된 규칙에 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 TCP 트래픽을 무시하도록 전처리기를 설정합니다. 단, 소스 및 대상 포트가 모두 `any`로 설정된 UDP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 예외입니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다.

UDP 스트림 전처리 구성

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **UDP Stream Configuration(UDP** 스트림 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **UDP Stream Configuration(UDP** 스트림 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** UDP 스트림 전처리 옵션, 2346 페이지에 설명된 대로 옵션을 설정합니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 관련 패킷 디코더 규칙(GID 116)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, 2024 페이지 및 패킷 디코더, 2330 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

레이어 관리, 1985 페이지
충돌 및 변경: 네트워크 분석 및 침입 정책, 1976 페이지

92 장

특정 위협 탐지

다음 주제에서는 네트워크 분석 정책에서 전처리기를 사용해 특정 위협을 탐지하는 방법을 설명합니다.

- 특정 위협 탐지 소개, 2349 페이지
- 특정 위협 탐지 라이선스 요건, 2349 페이지
- 특정 위협 탐지 요구 사항 및 사전 요건, 2350 페이지
- Back Orifice 탐지, 2350 페이지
- 포트스캔 탐지, 2351 페이지
- 속도 기반 공격 방지, 2359 페이지

특정 위협 탐지 소개

네트워크 분석 정책에서 여러 전처리기를 사용하여 Back Orifice 공격, 여러 포트스캔 유형, 그리고 과도한 트래픽으로 네트워크를 무력화하려는 속도 기반 공격과 같은 사용자의 모니터링된 네트워크에 대한 특정 위협을 탐지할 수 있습니다. 침입 규칙 또는 규칙 인수에서 비활성화된 전처리기를 요구하면, 네트워크 분석 정책의 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 자동으로 전처리기를 현재 설정으로 사용합니다.

보안 없이 전송되는 민감한 수치 데이터를 탐지하려면 침입 정책에서 구성하는 민감한 데이터 탐지 기능을 사용할 수도 있습니다.

특정 위협 탐지 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

특정 위협 탐지 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

Back Orifice 탐지

Firepower System은 Back Orifice 프로그램의 존재를 탐지하는 전처리기를 제공합니다. 이 프로그램은 Windows 호스트에 대한 관리자 액세스 권한을 얻는 데 사용할 수 있습니다.

Back Orifice 탐지 전처리기

Back Orifice 전처리기는 Back Orifice 매직 쿠키인 "*!*QWTY?"(패킷의 처음 8바이트에 있으며 XOR로 암호화됨)에 대한 UDP 트래픽을 분석합니다.

Back Orifice 프리프로세서는 구성 페이지가 있지만, 구성 옵션은 없습니다. 활성화한 경우, 전처리기가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하게 하려면 전처리기 규칙을 활성화해야 합니다.

표 ***238: Back Orifice GID:SID***

전처리기 규칙 **GID:SID**	설명
105:1	Back Orifice 트래픽이 탐지됨
105:2	Back Orifice 클라이언트 트래픽이 탐지됨
105:3	Back Orifice 서버 트래픽이 탐지됨
105:4	Back Orifice Snort 버퍼 공격이 탐지됨

Back Orifice 탐지

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Back Orifice Detection(Back Orifice** 탐지**)**가 비활성화되었다면 **Enabled**를 클릭합니다.

참고 Back Orifice에는 사용자가 설정하는 옵션이 없습니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 Back Orifice Detection(Back Orifice 탐지) 규칙 105:1, 105:2, 105:3 또는 105:4를 활성화합니다. 자세한 내용은 침입 규칙 상태, 2023 페이지 및 Back Orifice 탐지 전처리기, 2350 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

포트스캔 탐지

포트스캔은 공격에 앞서 공격자가 종종 사용하는 네트워크 정찰의 형태입니다. 포트스캔에서 공격자는 특별히 고안된 패킷을 대상 호스트로 전송합니다. 호스트가 응답하는 패킷을 검사하여 공격자는 종종 호스트에서 어떤 포트가 열려 있는지, 그리고 직접적으로 또는 추론에 의해 이러한 포트에서 어떤 애플리케이션 프로토콜이 실행 중인지 확인할 수 있습니다.

포트스캔 자체는 공격의 증거가 되지 못합니다. 실제로, 공격자가 사용하는 포트스캔 기법 중 일부는 네트워크의 합법적인 사용자들도 사용할 수 있습니다. Cisco의 포트스캔 탐지기는 활동의 패턴을 탐지하여 어떤 포트스캔이 악의적일 수 있는지를 확인하도록 설계되었습니다.

포트스캔 유형, 프로토콜 및 필터링된 민감도 레벨

공격자들은 네트워크에 대한 프로브를 위해 여러 방법을 사용할 것입니다. 이들은 종종, 하나의 프로토콜 유형이 차단되면 다른 것을 사용할 수 있도록 대상 호스트에서 서로 다른 응답을 이끌어내기 위해 여러 프로토콜을 사용합니다.

표 ***239:*** 프로토콜 유형

프로토콜	설명
TCP	SYN 스캔, ACK 스캔, TCP connect() 스캔, 그리고 Xmas tree, FIN, NULL 등 특이한 플래그 조합의 스캔과 같은 TCP 프로브를 탐지합니다.
UDP	제로바이트 UDP 패킷과 같은 UDP 프로브를 탐지합니다.
ICMP	ICMP 에코 요청(ping)을 탐지합니다.
IP	IP 프로토콜 스캔을 탐지합니다. 이 스캔은 TCP 및 UDP 스캔과 다릅니다. 공격자가 열린 포트를 찾는 대신 대상 호스트에서 어떤 IP 프로토콜이 지원되는지를 알아보려고 하기 때문입니다.

포트스캔은 일반적으로 대상 호스트의 수, 스캔하는 호스트의 수, 스캔되는 포트의 수를 기반으로 네 가지 유형으로 구분됩니다.

표 ***240:*** 포트스캔 유형

유형	설명
포트스캔 탐지	공격자가 단일 대상 호스트에서 여러 포트를 스캔하기 위해 하나 또는 소수의 호스트를 사용하는 일대일 포트스캔입니다. 일대일 포트스캔의 특성: • 스캔하는 호스트 수가 적음 • 단일 호스트가 스캔됨 • 스캔되는 포트 수가 많음 이 옵션은 TCP, UDP 및 IP 포트스캔을 탐지합니다.

유형	설명
포트 스윕	공격자가 하나 또는 여러 호스트를 사용하여 여러 대상 호스트에서 단일 포트를 스캔하는 일대다 포트 스윕입니다. 포트 스윕에는 다음과 같은 특징이 있습니다. • 스캔하는 호스트 수가 적음 • 스캔되는 호스트 수가 많음 • 스캔되는 고유한 포트 수가 적음 이 옵션은 TCP, UDP, ICMP 및 IP 포트 스윕을 탐지합니다.
Decoy 포트스캔	공격자가 실제 스캐닝 IP 주소와 스푸핑된 소스 IP 주소를 혼합하는 일대일 포트스캔입니다. Decoy 포트스캔에는 다음과 같은 특징이 있습니다. • 많은 수의 스캐닝 호스트 • 한 번만 스캐닝된 적은 수의 포트 • 스캐닝된 단일 (또는 적은 수의) 호스트 Decoy 포트스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.
분산형 포트스캔	여러 호스트가 개방형 포트를 위해 단일 호스트를 쿼리하는 다대일 포트스캔입니다. 분산형 포트스캔에는 다음과 같은 특징이 있습니다. • 많은 수의 스캐닝 호스트 • 한 번만 스캐닝된 많은 수의 포트 • 스캐닝된 단일 (또는 적은 수의) 호스트 분산형 포트스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.

포트스캔 탐지기가 프로브에 대해 알게 되는 정보는 대개 검토된 호스트에서 음수 응답이 표시되는 것을 기반으로 합니다. 예를 들어, 웹 클라이언트가 웹 서버에 연결을 시도할 때, 클라이언트는 포트 80/tcp를 사용하며 서버는 해당 포트가 열려 있도록 하는 역할을 수행할 수 있습니다. 하지만 서버를 검토할 때, 공격자는 서버의 웹 서비스 제공 여부를 미리 확인할 수 없습니다. 포트스캔 탐지기에 음수 응답(즉 ICMP에 연결할 수 없는 패킷 또는 TCP RST 패킷)이 표시되면 해당 응답을 잠재적 포트스캔으로 기록합니다. 이러한 프로세스는 대상 호스트가 음수 응답을 필터링하는 방화벽 또는 라우터와 같은 디바이스의 다른 편에 있는 경우 더욱 복잡합니다. 이 경우 포트스캔은 사용자가 선택한 민감도 레벨을 기반으로 필터링된 포트스캔 이벤트를 생성할 수 있습니다.

표 ***241:*** 민감도 레벨

레벨	설명
낮음	대상 호스트에서 부정적인 응답만 탐지합니다. 이 민감도 레벨을 선택하면 오탐을 억제할 수 있지만, 일부 포트스캔 유형(느린 스캔, 필터링된 스캔)을 놓칠 수 있습니다. 이 레벨은 포트스캔 탐지에 가장 짧은 시간 창을 사용합니다.
중간	호스트에 대한 연결 수를 기반으로 포트스캔을 탐지합니다. 즉, 필터링된 포트스캔을 탐지할 수 있습니다. 그러나 네트워크 주소 변환기와 프록시 등 매우 활동적인 호스트는 오탐을 생성할 수 있습니다. 이 유형의 오탐을 완화하려면 이러한 활동적인 호스트의 IP 주소를 **Ignore Scanned(**스캔을 탐지하지 않음**)** 필드에 추가할 수 있습니다. 이 레벨은 포트스캔 탐지에 좀 더 긴 시간 창을 사용합니다.
높음	시간 창을 기반으로 포트스캔을 탐지합니다. 즉, 시간 기반 포트스캔을 탐지할 수 있습니다. 그러나 이 옵션을 사용할 경우 **Ignore Scanned(**스캔을 탐지하지 않음**)** 및 **Ignore Scanner(**스캐너를 탐지하지 않음**)** 필드에 IP 주소를 지정하여 시간에 따라 탐지기를 신중하게 조정해야 합니다. 이 레벨은 포트스캔 탐지에 훨씬 긴 시간 창을 사용합니다.

포트스캔 이벤트 생성

포트스캔 탐지가 활성화되면, 생성기 ID(GID) 122 및 SID 1에서 27 사이의 Snort ID(SID)(으)로 규칙을 활성화해야 다양한 포트스캔과 포트 스윕을 탐지할 수 있습니다.

참고 포트스캔 연결 탐지기에서 생성된 이벤트의 경우, 프로토콜 번호는 255로 설정됩니다. 포트스캔은 기본적으로 연결할 특정 프로토콜이 없기 때문에, IANA(Internet Assigned Numbers Authority, 인터넷 할당 번호 관리기관)에는 그에 할당된 프로토콜 번호가 없습니다. IANA는 255를 예약된 번호로 지정하여 해당 번호가 포트스캔 이벤트에서 사용되는 경우 해당 이벤트에 대해 연결된 프로토콜이 없음을 나타냅니다.

표 ***242:*** 포트스캔 탐지 ***SID(GID 122)***

포트스캔 유형	프로토콜	민감도 수준	전처리기 규칙 **SID**
포트스캔 탐지	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	1 5 17 21 이벤트를 생성하지 않습니다. 이벤트를 생성하지 않습니다. 9 13
포트 스윕	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	3, 27 7 19 23 25 26 11 15
Decoy 포트스캔	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	2 6 18 22 이벤트를 생성하지 않습니다. 이벤트를 생성하지 않습니다. 10 14

포트스캔 유형	프로토콜	민감도 수준	전처리기 규칙 **SID**
분산형 포트스캔	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	4 8 20 24 이벤트를 생성하지 않습니다. 이벤트를 생성하지 않습니다. 12 16

포트스캔 이벤트 패킷 보기

관련 전처리기 규칙을 활성화하면, 포트스캔 탐지기는 다른 모든 침입 이벤트를 수행할 때 표시될 수 있는 침입 이벤트를 생성합니다. 그러나, 패킷 보기에 표시되는 정보는 다른 유형의 침입 이벤트와는 다릅니다.

포트스캔 이벤트에 대한 패킷 보기로 드릴 다운하는 침입 이벤트 보기를 사용하는 것으로 시작합니다. 단일 포트스캔 이벤트가 여러 패킷에 기반하므로 포트스캔 패킷을 다운로드할 수 없습니다. 그러나, 포트스캔 패킷 보기는 모든 가용 패킷 정보를 제공합니다.

어떤 IP 주소에서도 주소를 클릭하여 콘텍스트 메뉴를 확인하고, **whois**를 선택하여 IP 주소 조회를 수행하거나 **View Host Profile(**호스트 프로파일 보기**)**을 선택하여 해당 호스트의 호스트 프로파일을 확인할 수 있습니다.

표 ***243:*** 포트스캔 패킷 보기

정보	설명
디바이스	이벤트를 탐지한 디바이스입니다.
시간	이벤트가 발생한 시간입니다.
메시지	전처리기에서 생성된 이벤트 메시지입니다.
Source IP(소스 IP)	스캐닝하는 호스트의 IP 주소입니다.
Destination IP(대상 IP)	스캐닝된 호스트의 IP 주소입니다.
우선 순위 집계	스캐닝된 호스트로부터의 음수 응답 수(예를 들어, TCP RSTs 및 ICMP에 도달할 수 없는)입니다. 음수 응답 수가 많을수록 우선 순위가 높습니다.
연결 집계	호스트에 연결된 활성 연결 수입니다. 이 값은 TCP 및 IP와 같은 연결 기반 스캔의 경우 더 정확합니다.

정보	설명
IP 집계	스캐닝된 호스트에 연결된 IP 주소가 변경된 횟수입니다. 예를 들어, 첫 번째 IP 주소가 10.1.1.1인 경우, 두 번째 IP는 10.1.1.2이며, 3번째 IP는 10.1.1.1이며, 다음으로 IP 수는 3입니다. 이 번호는 프록시 및 DNS 서버 등 활성 호스트의 경우 덜 정확합니다.
스캐너/스캐닝된 IP 범위	스캔 유형에 따른 스캐닝된 호스트 또는 스캐닝하는 호스트의 IP 주소 범위입니다. 포트 스윕의 경우, 이 필드는 스캐닝된 호스트의 IP 범위를 보여줍니다. 포트스캔의 경우, 이는 스캐닝하는 호스트의 IP 범위를 보여줍니다.
포트/프로토콜 집계	TCP와 UDP 포트스캔의 경우, 스캐닝되고 있는 포트가 변경된 횟수입니다. 예를 들어, 스캐닝된 첫 번째 포트가 80인 경우, 스캐닝된 두 번째 포트는 8080이고, 스캐닝된 세 번째 포트는 다시 80이며, 다음 포트 수는 3입니다. IP 프로토콜 포트스캔의 경우, 스캐닝된 호스트에 연결하기 위해 사용되고 있는 프로토콜의 변경 횟수입니다.
포트/프로토콜 범위	TCP와 UDP 포트스캔의 경우, 스캐닝된 포트 범위입니다. IP 프로토콜 포트스캔의 경우, 스캐닝된 호스트에 연결하려고 시도하는 데 사용되는 IP 프로토콜 수의 범위입니다.
개방 포트	스캐닝된 호스트에 개방된 TCP 포트입니다. 이 필드는 포트스캔이 하나 이상의 개방형 포트를 탐지하는 경우에만 나타납니다.

관련 항목

침입 이벤트 정보, 2909 페이지

포트스캔 탐지 구성

포트스캔 탐지 구성 옵션을 사용하면 포트스캔 탐지기가 스캔 활동을 보고하는 방식을 세부적으로 조정할 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 수정하려는 정책 옆에 있는 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 설정을 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Portscan Detection(**포트스캔 탐지**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **Portscan Detection(**포트스캔 탐지**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** **Protocol(**프로토콜**)** 필드에 활성화할 프로토콜을 지정합니다.

참고 TCP를 통해 스캔을 탐지할 수 있도록 TCP 스트림 프로세싱이 활성화되었는지, 그리고 UDP를 통해 스캔을 탐지할 수 있도록 UDP 스트림 프로세싱이 활성화되었는지 확인해야 합니다.

단계 **7** **Scan Type(**스캔 유형**)** 필드에 탐지할 포트스캔 유형을 지정합니다.

단계 **8** **Sensitivity Level(**민감도 수준**)** 목록에서 수준을 선택합니다(포트스캔 유형, 프로토콜 및 필터링된 민감도 레벨, 2352 페이지 참조).

단계 **9** 포트스캔 활동의 징후에 대한 특정 호스트를 모니터링하려면, **Watch IP(IP** 감시**)** 필드에 호스트 IP 주소를 입력합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 모든 네트워크 트래픽을 감시하려면 필드에 아무것도 입력하지 마십시오.

단계 **10** 호스트를 스캐너로 간주해 무시하려면, **Ignore Scanners(**스캐너 무시**)** 필드에 호스트 IP 주소를 입력합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다.

단계 **11** 호스트를 스캔 대상으로 간주해 무시하려면, **Ignore Scanned(**스캔한 대상 무시**)** 필드에 호스트 IP 주소를 입력합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다.

팁 **Ignore Scanners(**스캐너 무시**)**와 **Ignore Scanned(**스캔한 대상 무시**)** 필드를 이용해 네트워크에서 특별히 활성화한 호스트를 표시합니다. 시간이 지남에 따라 호스트 목록을 변경해야 합니다.

단계 **12** 중앙 스트림에서 선택된 세션의 모니터링을 중지하려면, **Detect Ack Scans(Ack** 스캔 탐지**)** 확인란을 선택 취소합니다.

참고 중앙 스트림 세션의 탐지는 ACK 스캔을 확인하는 데 도움이 되지만 특히 트래픽 과부하로 패킷을 삭제한 네트워크에 잘못된 이벤트를 발생시킬 수 있습니다.

단계 **13** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 포트스캔 탐지가 다양한 포트스캔과 포트 스윕을 탐지하게 하려면, 규칙 122:1~122:27을 활성화합니다. 자세한 내용은 침입 규칙 상태, 2023 페이지 및 포트스캔 이벤트 생성, 2354 페이지의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

속도 기반 공격 방지

속도 기반 공격은 공격을 저지르는 연결 또는 반복된 시도의 빈도에 따른 공격입니다. 속도 기반 탐지 기준을 사용하여 속도 기반 공격이 발생할 때 이를 탐지하고 공격이 발생하는 경우 이에 반응한 후 공격이 중단되면 일반 탐지 설정으로 돌아갈 수 있습니다.

네트워크의 호스트로 향하는 과도한 활동을 탐지하는 속도 기반 필터를 포함하도록 네트워크 분석 정책을 구성할 수 있습니다. 인라인 모드로 구축된 매니지드 디바이스에서 이 기능을 사용하여 지정된 시간 동안 속도 기반 공격을 차단한 후 이벤트만 생성되고 트래픽은 삭제하지 않는 상태로 되돌릴 수 있습니다.

SYN 공격 방지 옵션을 통해 SYN 플러드 공격에 대해 네트워크 호스트를 보호할 수 있습니다. 일정 기간 동안 발견된 패킷 수에 따라 개별 호스트 또는 전체 네트워크를 보호할 수 있습니다. 디바이스가 수동으로 구축된 경우, 이벤트를 생성할 수 있습니다. 디바이스가 인라인에 위치한 경우, 악성 패킷 또한 삭제할 수 있습니다. 시간 제한이 경과한 후 속도 상태가 중단될 경우, 이벤트 생성 및 패킷 삭제가 중지됩니다.

예를 들어 어느 한 IP 주소에서 최대 개수의 SYN 패킷을 허용하고, 해당 IP 주소에서 60초 동안 추가 연결을 차단하도록 설정을 구성할 수 있습니다.

또한 네트워크에서 호스트를 오가는 TCP/IP 연결을 제한하여 서비스 거부 공격(DoS) 또는 사용자의 과도한 활동을 방지할 수 있습니다. 시스템이 특정 IP 주소 또는 주소 범위를 오가는 성공적인 연결의 구성된 수를 탐지하는 경우, 추가 연결에서 이벤트를 생성합니다. 속도 기반 이벤트 생성은 속도 조

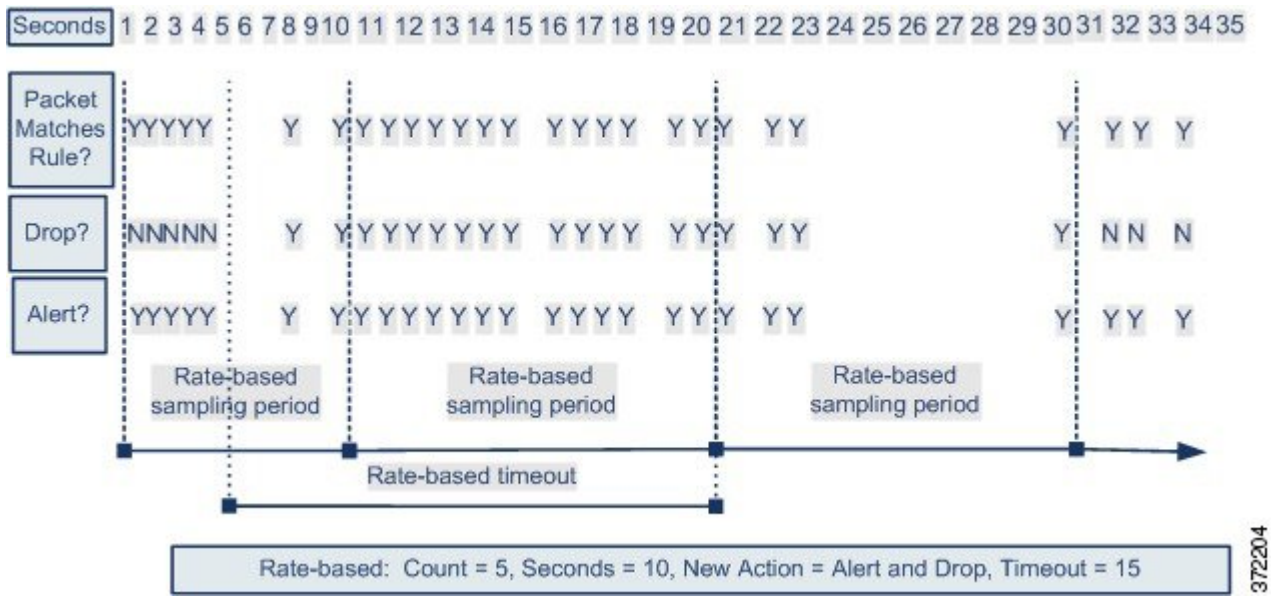
건의 발생 없이 시간 제한이 경과할 때까지 계속됩니다. 인라인 배포에서 속도 조건이 시간 초과될 때까지 패킷을 삭제하도록 선택할 수 있습니다.

예를 들어, 어느 것이든 하나의 IP 주소에서 최대 10개의 동시 연결이 성공할 수 있도록 설정을 구성할 수 있으며, 60초 동안 해당 IP 주소에서 추가 연결을 차단할 수 있습니다.

참고 내부 리소스에서의 디바이스 부하 균형 검사. 속도 기반 공격 방지를 설정할 때는 디바이스 단위가 아닌 리소스 단위로 트리거 속도를 설정해야 합니다. 속도 기반 공격 방지가 예상대로 작동하지 않는다면 트리거 속도를 줄여야 합니다. 올바른 속도를 결정하는 데 어려움이 있다면 지원팀에 문의하십시오.

다음 다이어그램은 공격자가 호스트에 액세스하기 위해 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지가 구성된 규칙을 트리거합니다. 속도 기반 설정은 10초 범위 안에 규칙 일치가 다섯 번 발생하면 규칙 속성을 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 새로운 규칙 속성은 15초 후 시간 초과됩니다.

시간이 초과되더라도 패킷은 이어지는 속도 기반 샘플링 기간 내에 여전히 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 이벤트 생성으로 돌아갑니다.



관련 항목

동적 침입 규칙 상태, 2032 페이지

속도 기반 공격 방지 예시

`detection_filter` 키워드 및 임계값 설정 그리고 삭제 기능은 트래픽 자체 또는 시스템에서 생성된 이벤트를 필터링할 다른 방법을 제공합니다. 속도 기반 공격 차단을 단독으로 사용하거나 임계값 설정, 삭제, 또는 `detection_filter` 키워드를 조합하여 사용할 수 있습니다.

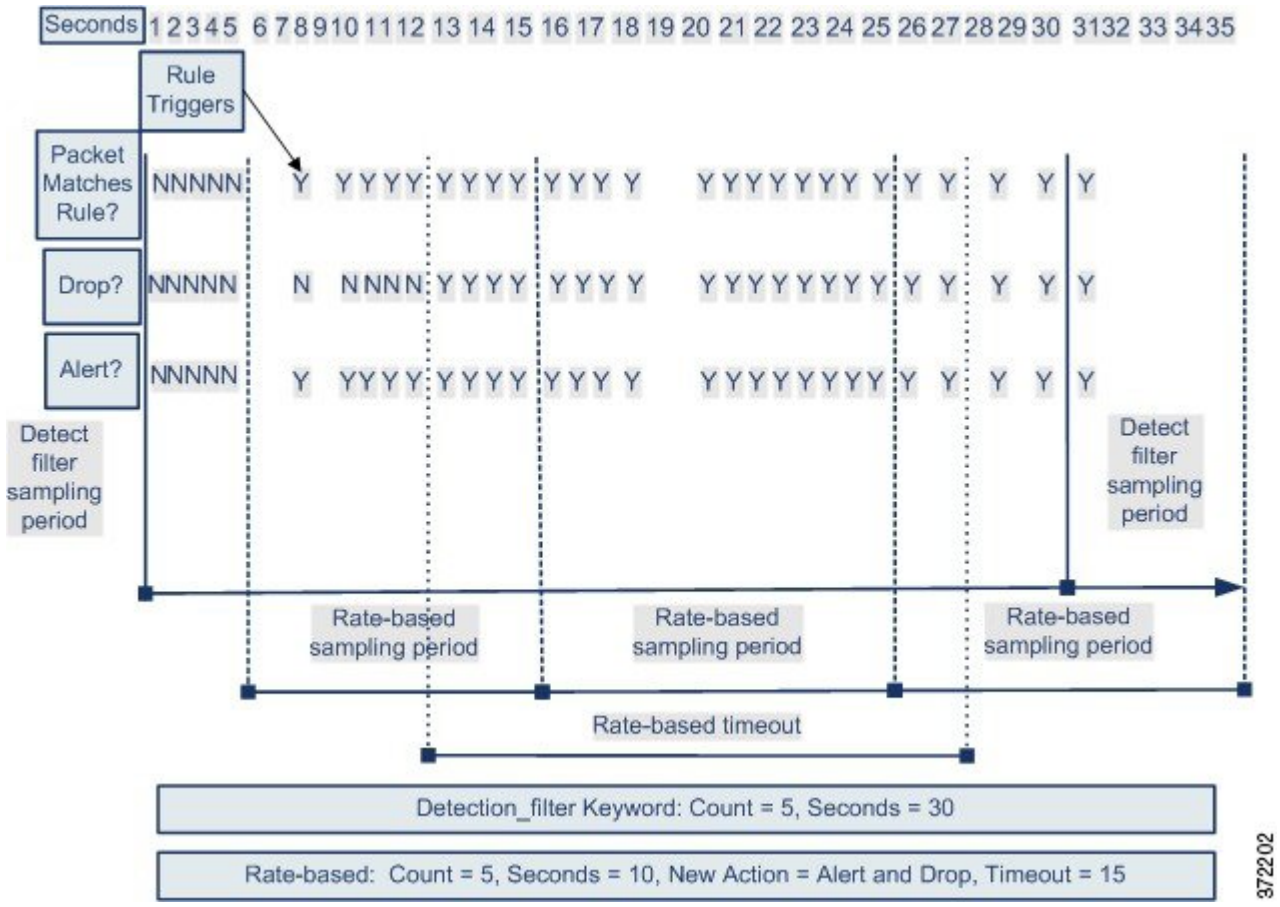
`detection_filter` 키워드, 임계값 설정 또는 억제, 속도 기반 기준 모두가 동일한 트래픽에 적용될 수도 있습니다. 규칙에 대한 삭제를 활성화하면, 속도 기반 변경이 발생한 경우에도 이벤트는 지정된 IP 주소에 대해 삭제됩니다.

detection_filter 키워드 예시

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 보여줍니다. 비밀번호를 찾는 반복된 시도는 또한 5로 설정된 계수와 함께 `detection_filter` 키워드를 포함하는 규칙을 트리거합니다. 이 규칙은 속도 기반 공격 방지가 설정되도록 합니다. 속도 기반 설정은 10초 범위 안에 규칙을 다섯 번 적중할 경우 규칙 속성을 20초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다.

다이어그램에 보여진 것과 같이, 속도가 `detection_filter` 키워드에 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 첫 5개의 패킷은 이벤트를 생성하지 않습니다. 규칙이 트리거되면 이벤트 알림이 시작되지만, 속도 기반 기준은 5개의 추가 패킷이 통과할 때까지 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하지 않습니다.

속도 기반 기준이 충족되면, 이벤트가 생성되고, 속도 기반 시간 제한이 만료되고 속도가 임계값 아래로 떨어질 때까지 패킷은 삭제됩니다. 20초가 지나면 속도 기반 작업이 시간 초과됩니다. 시간이 초과되더라도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 시간 제한이 발생할 때 샘플링된 속도는 이전 샘플링 기간의 임계값 속도보다 높으므로, 속도 기반 작업이 계속됩니다.



예제에는 이 내용이 없지만, Drop and Generate Events 규칙 상태를 `detection_filter` 키워드와 함께 사용하여 규칙에 대한 히트 수가 지정된 속도에 도달할 때 트래픽 삭제를 시작할 수 있습니다. 규칙에 대해 속도 기반 설정을 구성할 것인지 여부를 결정할 때는 규칙을 Drop and Generate Events(삭제 후 이벤트 생성)로 설정하고 `detection_filter` 키워드를 포함하는 경우 같은 결과가 생성되도록 할지, 아니면 침입 정책에서 속도 및 시간 초과 설정을 관리할지를 고려합니다.

관련 항목

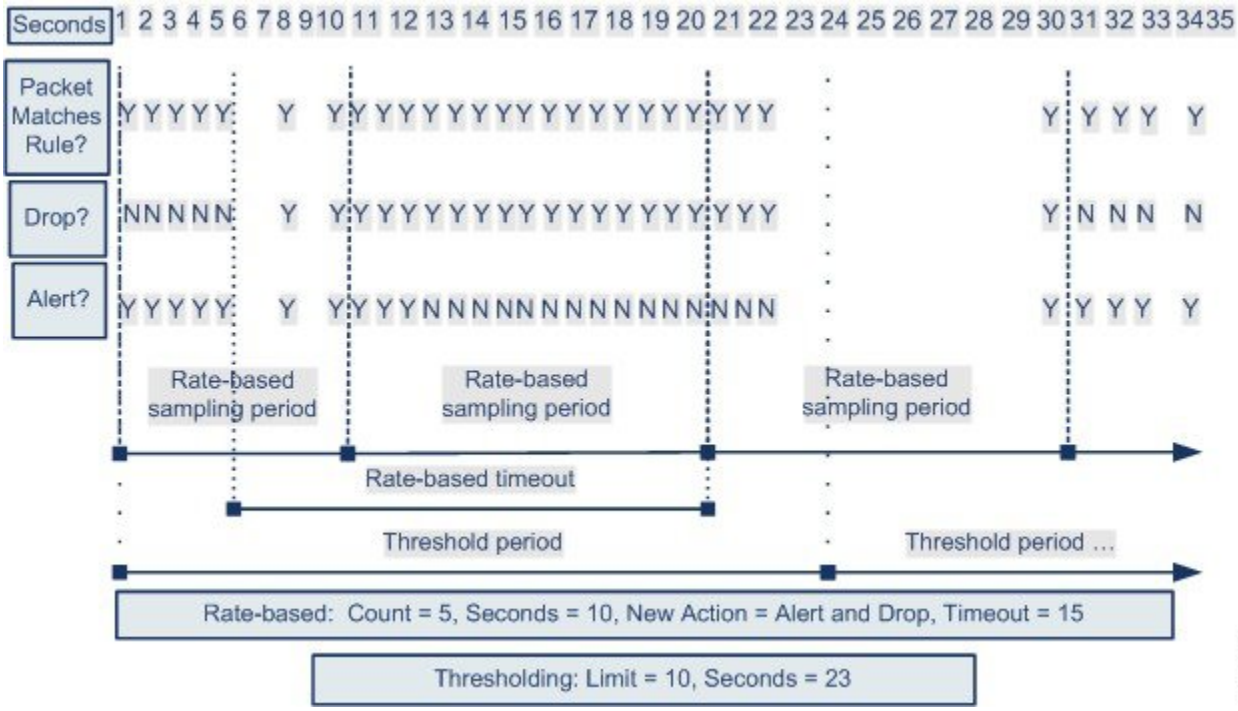
침입 규칙 상태, 2023 페이지

동적 규칙 상태 임계값 설정 및 삭제 예시

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지를 구성한 규칙을 트리거합니다. 속도 기반 설정은 10초 안에 규칙을 다섯 번 적중할 경우 규칙 속성을 15초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 또한, 제한 임계값은 규칙이 23초 안에 10개의 이벤트를 생성할 수 있도록 이벤트 수를 제한합니다.

다이어그램에 보여진 것과 같이, 규칙은 처음 5개의 일치 패킷의 이벤트를 생성합니다. 속도 기반 기준은 5개의 패킷 후 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하며, 다음 5개의 패킷 중에 규칙은 이벤트를 생성하고 시스템은 패킷을 삭제합니다. 10개의 패킷 후, 제한 임계값에 도달하므로, 나머지 패킷에 대해 시스템은 이벤트를 생성하지 않지만 패킷을 삭제합니다.

시간이 초과되더라도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 Generate Events(이벤트 생성)로 돌아갑니다.



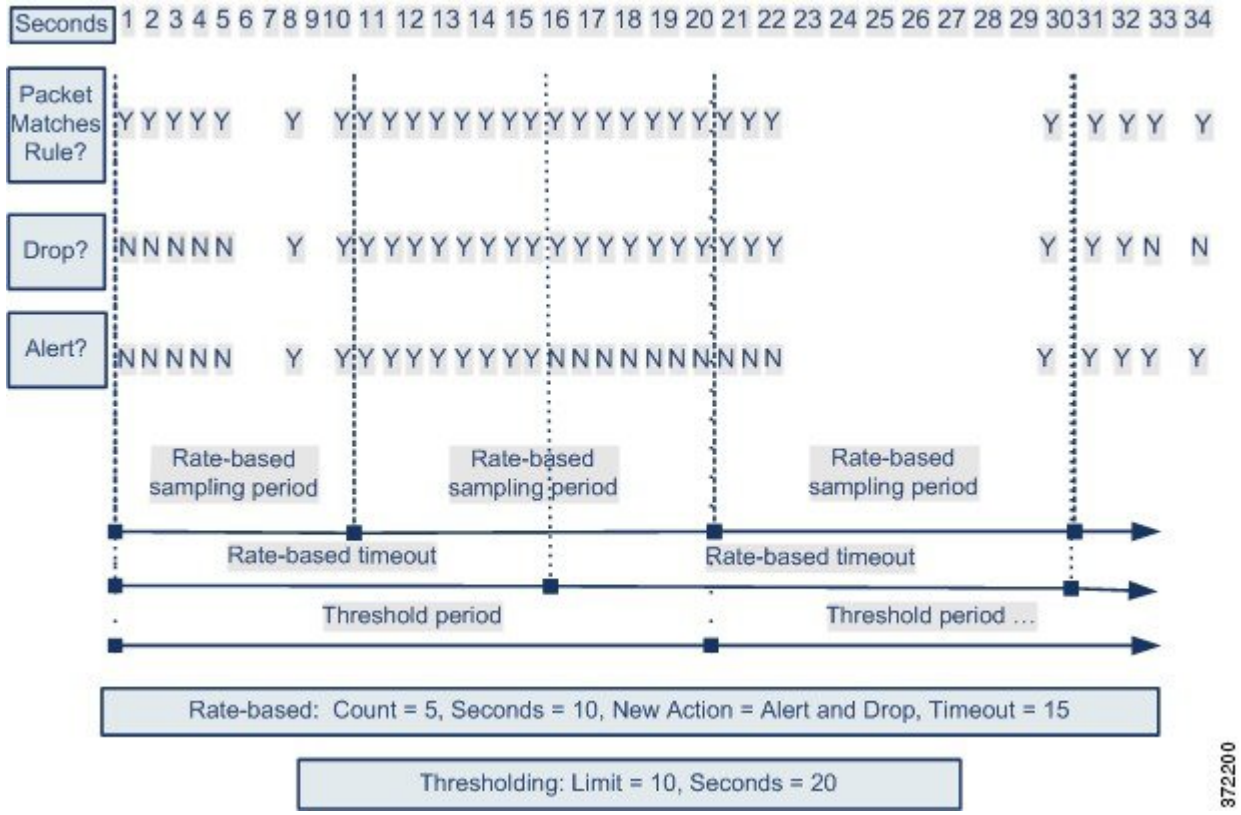
이 예에는 나와 있지 않지만, 임계값에 도달한 이후 속도 기반 기준 때문에 새 작업이 트리거되면 시스템은 작업 변화을 나타내는 단일 이벤트를 생성합니다. 따라서, 예를 들면, 제한 임계값인 10에 도달하고 시스템이 이벤트 생성을 중단하며 작업이 14번째 패킷에서 Drop and Generate Events(이벤트 삭제 및 생성)에서 Generate Events(이벤트 생성)로 변경되었을 때, 시스템은 작업 변화를 나타내는 11번째 이벤트를 생성합니다.

전정책적 속도 기반 탐지 및 임계값 설정 또는 삭제 예시

다음의 예시는 네트워크에서 호스트에 서비스 거부 공격(DoS) 공격을 시도한 공격자를 보여줍니다. 동일한 소스에서 호스트에 동시에 다수가 연결하면 정책 전반의 Control Simultaneous Connections(동시 연결 제어) 설정이 트리거됩니다. 설정은 10초 안에 한 개의 소스로부터 5개의 연결이 있을 때 이벤트를 생성하고 악성 트래픽을 삭제합니다. 또한, 전역 제한 임계값은 모든 규칙 또는 설정이 20초 안에 10개의 이벤트를 생성할 수 있도록 이벤트 수를 제한합니다.

다이어그램에 나와 있듯이, 정책 전반의 설정은 처음 10개의 일치 패킷에 대해 이벤트를 생성하고 트래픽을 삭제합니다. 10개의 패킷 후, 제한 임계값에 도달되므로, 나머지 패킷에 대한 어떤 이벤트도 생성되지 않지만 패킷이 삭제됩니다.

시간이 초과되더라도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 이벤트를 생성하고 트래픽을 삭제하는 속도 기반 작업은 계속됩니다. 속도 기반 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 중지됩니다.



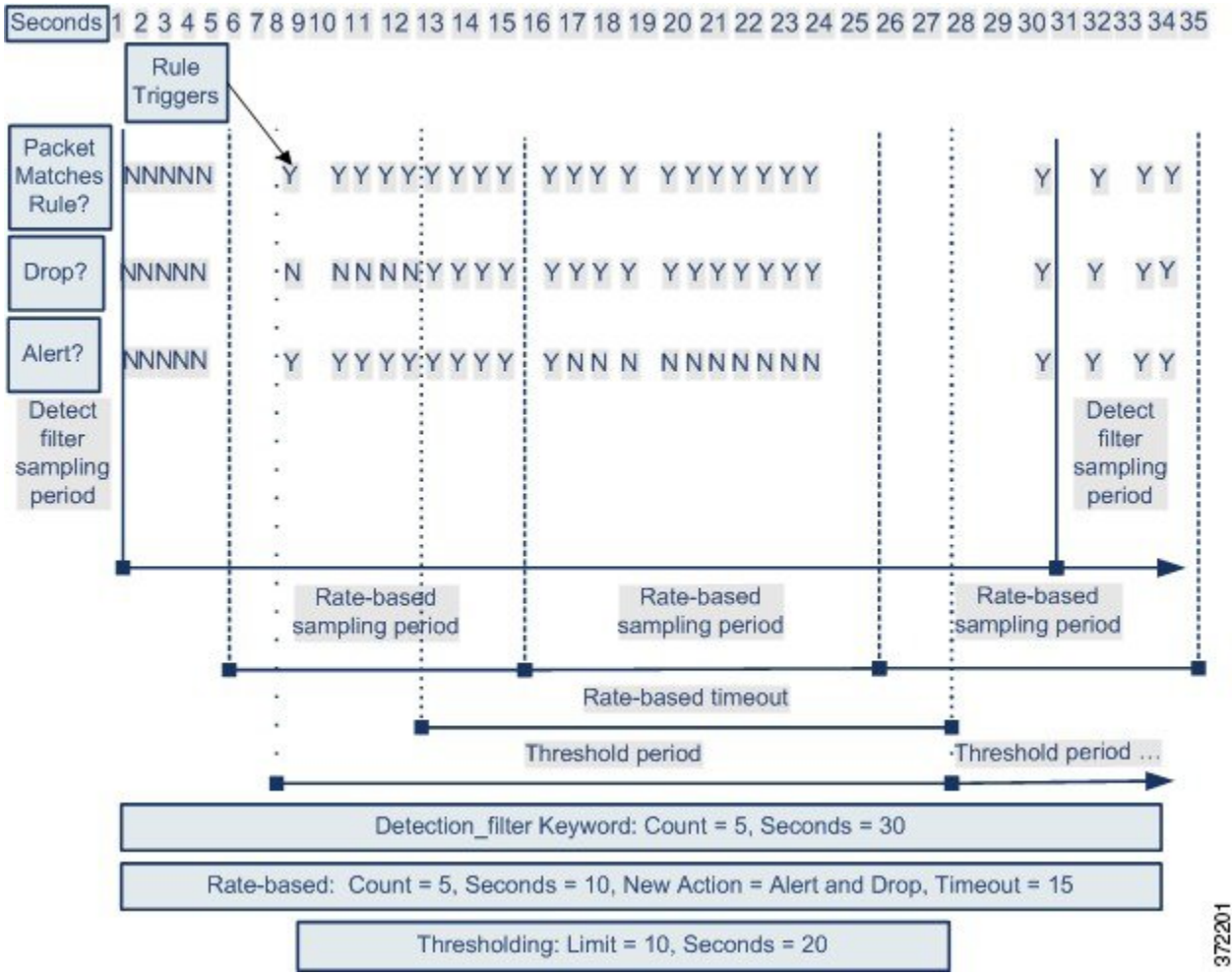
이 예에는 나와 있지 않지만, 임계값에 도달한 이후 속도 기반 기준 때문에 새 작업이 트리거되면 시스템은 작업 변화을 나타내는 단일 이벤트를 생성합니다. 따라서, 예를 들면, 제한 임계값인 10에 도달하고 시스템이 이벤트 생성을 중단하며 작업이 14번째 패킷에서 Drop and Generate Events(이벤트 삭제 및 생성)로 변경되었을 때, 시스템은 작업 변화를 나타내는 11번째 이벤트를 생성합니다.

여러 필터링 방법으로 속도 기반 탐지 예시

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 표시하고, `detection_filter` 키워드, 속도 기반 필터링, 임계값 설정이 상호 작용하는 경우에 대해 설명합니다. 비밀번호를 찾는 반복된 시도는 또한 5로 설정된 계수와 함께 `detection_filter` 키워드를 포함하는 규칙을 트리거합니다. 이 규칙에는 또한 15초 안에 다섯 번의 적중이 있을 경우 규칙 속성을 30초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경하는 속도 기반 공격 방지 설정이 있습니다. 또한, 제한 임계값은 규칙이 30초 안에 10개의 이벤트를 생성할 수 있도록 규칙을 제한합니다.

다이어그램에 표시된 대로 속도가 `detection_filter` 키워드에 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 첫 5개의 패킷은 이벤트 알림을 야기하지 않습니다. 규칙이 트리거되면 이벤트 알림이 시작되지만, 속도 기반 기준은 5개의 추가 패킷이 통과할 때까지 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하지 않습니다. 속도 기반 기준이 충족되면, 시스템은 패킷 11-15를 위한 이벤트를 생성하고 패킷을 삭제합니다. 15개의 패킷 후 제한 임계값에 도달하므로, 나머지 패킷에 대해 시스템은 이벤트를 생성하지 않지만 패킷을 중단합니다.

속도 기반 시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 이전 샘플링 기간의 임계값 속도보다 높으므로 새로운 작업이 계속됩니다.



속도 기반 공격 방지 옵션 및 설정

속도 기반 공격 방지는 잘못된 트래픽 패턴을 식별하고 정당한 요청에 대한 해당 트래픽의 영향을 최소화하려고 합니다. 속도 기반 공격은 일반적으로 다음 중 하나의 특성을 갖습니다.

- 네트워크의 호스트로 향하는 불완전한 연결을 포함하는, SYN 플러드 공격을 나타내는 모든 트래픽
- 네트워크의 호스트로 향하는 과도하고 완전한 연결을 포함하는, TCP/IP 연결 플러드 공격을 나타내는 모든 트래픽
- 특정 목적지 IP 주소 또는 주소로 이동하거나 특정 소스 IP 주소 또는 주소에서 오는 트래픽에서의 과도한 규칙 일치
- 모든 트래픽을 가로지르는 특정 규칙에 대한 과도한 일치 항목

네트워크 분석 정책에서 전체 정책에 대한 SYN flood 또는 TCP/IP 연결 flood 탐지를 구성할 수 있습니다. 침입 정책에서 개별적인 침입 또는 전처리기 규칙을 위한 속도 기반 필터를 설정할 수 있습니다. 수동으로 속도 기반 필터를 GID 135 규칙에 추가하거나 규칙 상태를 수정할 수는 없습니다. GID 135가 포함된 규칙은 해당 클라이언트를 소스 값으로 사용하고 해당 서버를 대상 값으로 사용합니다.

SYN Attack Prevention(SYN 공격 방지**)**이 활성화된 경우, 정의된 속도 조건이 초과되면 규칙 135:1이 트리거됩니다.

Control Simultaneous Connections(동시 연결 제어**)**가 활성화된 경우, 정의된 속도 조건이 초과되면 규칙 135:2가 트리거되고, 세션이 닫히거나 시간 초과되면 규칙 135:3이 트리거됩니다.

참고 내부 리소스에서의 디바이스 부하 균형 검사. 속도 기반 공격 방지를 설정할 때는 디바이스 단위가 아닌 리소스 단위로 트리거 속도를 설정해야 합니다. 속도 기반 공격 방지가 예상대로 작동하지 않는다면 트리거 속도를 줄여야 합니다. 올바른 속도를 결정하는 데 어려움이 있다면 지원팀에 문의하십시오.

각 속도 기반 필터에는 여러 구성 요소가 포함되어 있습니다.

- 정책 전반 또는 규칙 기반 소스나 대상 설정을 위한 네트워크 주소 지정
- 특정 시간(초) 이내 규칙 일치의 계수로 구성한 규칙 일치 비율
- 속도가 초과될 때 수행할 새 작업

  전체 정책에 대한 속도 기반 설정을 설정한 경우, 시스템이 속도 기반 공격을 탐지하면 이벤트를 생성하고, 인라인 배포에서 트래픽을 삭제할 수 있습니다. 개별 규칙에 대한 속도 기반 작업을 설정할 때 Generate Events(이벤트 생성), Drop and Generate Events(이벤트 삭제 및 생성), Disable(비활성화)라는 세 가지 작업을 사용할 수 있습니다.
- 시간 제한 값으로 설정한 작업 기간

시작한 경우, 속도가 해당 기간 동안 구성된 속도까지 떨어지더라도 시간 제한에 도달할 때까지 새로운 작업이 발생한다는 점에 유의하십시오. 시간 제한이 만료되면, 속도가 임계값 아래로 떨어진 경우, 규칙 작업은 규칙에 처음 설정된 작업으로 돌아갑니다. 정책 전반 설정의 경우, 작업은 트래픽과 일치하는 각 규칙의 작업으로 돌아갑니다. 일치하는 규칙이 없는 경우 작업이 중지됩니다.

인라인 배포에서 속도 기반 공격 차단을 구성하여 일시적으로 또는 영구적으로 공격을 차단할 수 있습니다. 속도 기반 구성없이, Generate Events(이벤트 생성)로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙에 대한 패킷을 삭제하지 않습니다. 하지만 속도 기반 기준이 구성되어 있는 규칙이 공격 트래픽과 일치하는 경우, 해당 규칙이 처음에는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있지 않더라도 속도 작업은 속도 작업이 활성화된 기간 동안 패킷이 삭제되도록 할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나 비활성화된 규칙에 일치하는 트래픽을 삭제할 수 없습니다. 하지만 정책 수준에서 속도 기반 필터를 설정하는 경우, 지정된 기간 이내에 SYN 패킷 또는 SYN/ACK 상호작용의 과도한 수를 포함하는 트래픽에 이벤트를 생성하거나 트래픽에 이벤트를 생성하고 삭제할 수 있습니다.

동일한 규칙에서 다중 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 나열된 첫 번째 필터의 우선 순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌할 때 시스템은 첫 번째 속도 기반 필터의 작업을 시행합니다. 마찬가지로, 필터가 충돌하는 경우 정책 전반의 속도 기반 필터는 개별 규칙에 설정된 속도 기반 필터를 재정의합니다.

관련 항목

규칙 페이지에서 동적 규칙 상태 설정, 2034 페이지

속도 기반 공격 방지, 탐지 필터링 및 임계값 설정 또는 삭제

`detection_filter` 키워드는 지정된 시간 내에 규칙 일치의 임계값 수가 나올 때까지 규칙이 트리거되지 않게 합니다. 규칙이 `detection_filter` 키워드를 포함할 경우, 시스템은 시간 제한별 규칙에서 패턴 일치한 수신 패킷 수를 추적할 수 있습니다. 시스템은 특정 소스 또는 대상 IP 주소에서 해당 규칙 적중 횟수를 카운트할 수 있습니다. 속도가 규칙의 속도를 초과한 후, 해당 규칙에 대한 이벤트 알림이 시작됩니다.

임계값 설정 및 삭제를 사용하여 소스 또는 대상에 대한 이벤트 알림 수를 제한함으로써 또는 해당 규칙에 대한 알림을 모두 삭제함으로써 과도한 이벤트를 줄일 수 있습니다. 또한 특정 임계값을 재정의하지 않는 각 규칙에 적용되는 전역 규칙 임계값을 설정할 수도 있습니다.

규칙에 억제를 적용할 경우, 정책 전반 또는 규칙 단위의 속도 기반 설정 때문에 속도 기반 작업 변화가 발생하더라도 시스템은 모든 사용 가능한 IP 주소에 대해 해당 규칙의 이벤트 알림을 억제합니다.

관련 항목

침입 이벤트 임계값, 2025 페이지
침입 정책 삭제 설정, 2029 페이지
전역 규칙 임계값 기본 사항, 2057 페이지

속도 기반 공격 방지 구성

정책 수준에서 속도 기반 공격 차단을 구성하여 SYN 플러드 공격을 차단할 수 있습니다. 또한 특정 소스로부터 또는 특정 대상을 향한 과도한 연결을 중지할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 설정을 클릭합니다.

단계 **4** **Specific Threat Detection(**특정 위협 탐지**)**의 **Rate-Based Attack Prevention(**속도 기반 공격 방지**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **5** **Rate-Based Attack Prevention(**속도 기반 공격 방지**)** 옆에 있는 수정( )을 클릭합니다.

단계 **6** 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트를 초과하도록 고안된 불완전 연결을 차단하려면 **SYN Attack Prevention(SYN** 공격 방지**)** 아래의 **Add(**추가**)**를 클릭합니다.
- 과도한 수의 연결을 방지하려면 **Control Simultaneous Connections** 아래에서 **Add**를 클릭합니다.

단계 **7** 트래픽을 추적할 방법을 지정합니다.

- 특정 소스 또는 소스 범위에서 출발하는 모든 트래픽을 추적하려면 **Track By(**추적 기준**)** 드롭다운 목록에서 **Source(**소스**)**를 선택하고 **Network(**네트워크**)** 필드에 단일 IP 주소 또는 주소 블록을 입력합니다.
- 특정 대상 또는 대상 범위로 향하는 모든 트래픽을 추적하려면 **Track By(**추적 기준**)** 드롭다운 목록에서 **Destination(**대상**)**을 선택하고 **Network(**네트워크**)** 필드에 IP 주소 또는 주소 블록을 입력합니다.

참고 시스템은 **Network(**네트워크**)** 필드에 포함된 각 IP 주소에 대한 개별 트래픽을 추적합니다. 구성한 속도 결과를 초과하는 단일 IP 주소로부터의 트래픽은 해당 IP 주소만을 위해 생성된 이벤트로 귀결됩니다. 한 예를 들어, 네트워크 구성에 `10.1.0.0/16`의 소스 CIDR 차단을 설정하고 10개의 동시 연결이 개방되어 있을 때 이벤트를 생성하도록 시스템을 구성할 수 있습니다. 10.1.4.21에서 8개의 연결이 열리고 10.1.5.10에서 6개의 연결이 열리는 경우, 어느 소스도 트리거하는 수의 연결을 갖고 있지 않으므로 시스템이 이벤트를 생성하지 않습니다. 그러나, 10.1.4.21에서 11개의 동시 연결이 열리는 경우, 시스템은 10.1.4.21로부터의 연결에 해당하는 이벤트만 생성합니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **8** 속도 추적 설정의 시작 속도를 지정합니다.

- SYN 공격 설정의 경우에는 **Rate(**속도**)** 필드에 초당 SYN 패킷 수를 지정합니다.
- 동시 연결 설정의 경우에는 **Count(**계수**)** 필드에 연결 수를 입력합니다.

내부 리소스에서의 디바이스 부하 균형 검사. 속도 기반 공격 방지를 설정할 때는 디바이스 단위가 아닌 리소스 단위로 트리거 속도를 설정해야 합니다. 속도 기반 공격 방지가 예상대로 작동하지 않는다면 트리거 속도를 줄여야 합니다. 올바른 속도를 결정하는 데 어려움이 있다면 지원팀에 문의하십시오.

단계 **9** 속도 기반 공격 방지 설정에 일치하는 패킷을 삭제하려면 **Drop(**삭제**)** 확인란을 선택합니다.

단계 **10** **Timeout(**시간 초과**)** 필드에 SYN 일치 패턴이 있거나 동시 연결이 존재하는 트래픽에 대한 이벤트 생성(적용 가능한 경우에는 이벤트 삭제)까지 대기하는 시간을 입력합니다.

주의 높은 시간 제한 값을 설정하면 인라인 배포에서 호스트로 향하는 연결을 완전히 차단할 수 있습니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

93 장

적응형 프로파일

다음 주제에서는 적응형 프로파일을 설정하는 방법을 설명합니다.

- 적응형 프로파일 정보, 2371 페이지
- 적응형 프로파일 라이선스요구 사항, 2372 페이지
- 적응형 프로파일 요구 사항 및 사전 요건, 2372 페이지
- 적응형 프로파일 및 Firepower 권장 규칙, 2372 페이지
- 적응형 프로파일 옵션, 2373 페이지
- 적응형 프로파일 구성, 2374 페이지

적응형 프로파일 정보

일반적으로, 시스템은 트래픽을 전처리하고 분석하기 위해 네트워크 분석 정책의 정적 설정을 사용합니다. 적응형 프로파일을 이용하면, 시스템은 네트워크 검색으로 탐지하거나 서드파티로부터 가져온 호스트 정보를 이용해 처리 동작을 조정할 수 있습니다.

적응형 프로파일대상 기반 프로파일에서처럼 네트워크 분석 정책에서 수동으로 설정할 수 있어, 대상 호스트의 운영체제와 같은 방식으로 IP 패킷을 조각 모음하고 스트림을 리어셈블하는 데 도움이 됩니다. 침입은 엔진을 통제한 다음 대상 호스트에서 사용하는 것과 동일한 형식으로 데이터를 분석합니다.

수동으로 설정한 대상 기반 프로파일은 사용자가 선택한 기본 운영체제 프로파일이나 특정 호스트에 구속한 프로파일을 적용합니다. 하지만 적응형 프로파일은(는) 대상 호스트의 호스트 프로파일 내 운영체제에 맞는 적절한 운영체제 프로파일로 전환합니다.

10.6.0.0/16 서브넷에 적응형 프로파일을(를) 구성하고 Linux에 기본 IP Defragmentation(조각 모음) 대상 기반 정책을 설정하는 방법을 고려해 보십시오. 설정을 구성하는 Firepower Management Center에는 10.6.0.0/16 서브넷을 포함하는 네트워크 맵이 있습니다.

- 시스템에서 10.6.0.0/16 서브넷에 없는 호스트 A의 트래픽을 탐지하면 디바이스는 Linux 대상 기반 정책을 사용하여 IP 조각을 리어셈블합니다.
- 10.6.0.0/16 서브넷에 있는 호스트 B의 트래픽을 탐지하면, 시스템은 네트워크 맵에서 호스트 B의 운영체제 데이터를 검색합니다. 시스템은 해당 운영체제를 기반으로 하는 프로파일을 이용해 호스트 B로 향하는 트래픽을 조각 모음합니다.

적응형 프로파일 라이선스요구 사항

FTD 라이센스

위협

기본 라이선스

보호

적응형 프로파일 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

적응형 프로파일 및 **Firepower** 권장 규칙

적응형 프로파일 기능은 액세스 제어 정책에 의해 호출되는 모든 침입 정책에 전역 적용되는 액세스 제어 정책의 고급 설정입니다. Firepower 권장 규칙 기능은 이 기능을 구성하는 개별 침입 정책에 적용됩니다.

Firepower 권장 규칙과 마찬가지로 적응형 프로파일은 규칙의 메타데이터를 호스트 정보와 비교하여 특정 호스트에 규칙을 적용해야 할지 여부를 결정합니다. 그러나 Firepower 권장 규칙은 해당 정보를 사용하여 규칙의 활성화 또는 비활성화를 위한 권장 사항을 제공하는 반면 적응형 프로파일은 해당 정보를 사용하여 특정 트래픽에 특정 규칙을 적용합니다.

Firepower 권장 규칙의 경우, 제안된 변경 사항을 규칙 상태에 구현하기 위해 상호 작용이 필요합니다. 반면 적응형 프로파일은 침입 정책을 수정하지 않습니다. 규칙의 적응형 처리는 패킷별로 이루어집니다.

또한 Firepower 권장 규칙으로 비활성화된 규칙이 활성화될 수 있습니다. 반면 적응형 프로파일은 침입 정책에서 이미 활성화된 규칙의 적용에만 영향을 미칩니다. 적응형 프로파일은 규칙 상태를 변경하지 않습니다.

적응형 프로파일과 Firepower 권장 규칙을 조합해 사용할 수 있습니다. 적응형 프로파일은 침입 정책을 구축할 때 규칙의 규칙 상태를 사용하여 해당 규칙을 적용 후보로 포함할지 여부를 결정하며, 권장 사항을 수락하거나 거부하는 사용자의 선택은 해당 규칙 상태에 반영됩니다. 두 가지 기능을 모두 사용하여 모니터링하는 각 네트워크에 가장 알맞은 규칙이 활성화 또는 비활성화되었는지 확인할 수 있으며, 그런 다음 활성화된 규칙을 특정 트래픽에 가장 효율적으로 적용할 수 있습니다.

관련 항목

Firepower 권장 규칙 정보, 2037 페이지

적응형 프로파일 옵션

적응형 프로파일 - 활성화됨

적응형 프로파일 활성화 또는 비활성화

적응형 프로파일 - 특성 업데이트 간격

사용자 사용자는 네트워크 맵 데이터가 Firepower Management Center에서 매니지드 디바이스로 동기화되는 간격(단위: 분)을 제어할 수 있습니다. 시스템은 데이터를 사용하여 트래픽을 처리할 때 어떤 프로파일을 사용할지 결정합니다. 이 옵션 값을 높이면 대규모 네트워크 성능을 개선할 수 있습니다.

적응형 프로파일 - 네트워크

원한다면 적응형 프로파일을(를) IP 주소, 주소 블록 및 네트워크 변수의 쉼표로 구분된 목록에 제한하여 성능을 개선할 수도 있습니다. 네트워크 변수를 사용한다면, 시스템은 액세스 컨트롤 정책에 대한 기본 침입 정책과 연결된 변수 모음의 변수 값을 사용합니다. 예를 들어 **192.168.1.101, 192.168.4.0/24, $HOME_NET**을 입력할 수도 있습니다. IPv4 및 IPv6가 지원됩니다.

기본값(**0.0.0.0/0**)은 적응형 프로파일 업데이트를 모든 네트워크에 적용합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 상위 정책에서 적응형 프로파일을(를) 활성화하고 실행했다면, Cisco는 기본 네트워크 제약 조건을 **0.0.0.0/0**으로 유지하거나 `any` 값이 있는 네트워크 변수를 사용하도록 권장합니다. 이 설정은 적응형 프로파일을(를) 모든 하위 도메인에서 모니터링되는 모든 호스트에 적용합니다.

관련 항목

트래픽이 식별되기 전에 통과하는 패킷 검사, 2202 페이지
Firepower System IP 주소 규칙, 19 페이지
변수 집합, 580 페이지

적응형 프로파일 구성

수동 구축의 경우 Cisco는 적응형 프로파일 구성을 권장합니다. 인라인 구축의 경우에는 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화된 인라인 표준화 전처리기를 설정해야 합니다.

주의 액세스 컨트롤 규칙이 AMP를 비롯한 애플리케이션 또는 파일 제어를 수행하거나, 침입 규칙이 서비스 메타데이터를 사용하게 하려면 적응형 프로파일을 반드시 활성화해야 합니다.

시작하기 전에

액세스 제어 정책에는 호스트/서비스 검색을 수행할 수 있는 네트워크 검색 정책이 있어야합니다. 또는 서드파티 소스에서 호스트 데이터를 가져와야 합니다.

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 **Advanced(**고급**)**을 클릭하고 Detection Enhancement Settings(탐지 개선 설정) 섹션 옆에 있는 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 적응형 프로파일 옵션, 2373 페이지에 설명된 대로 적응형 프로파일 옵션을 설정합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

인라인 정상화 전처리기, 2317 페이지
Snort® 재시작 시나리오, 505 페이지

XX 부

검색 및 ID

- 네트워크 검색 및 ID 소개, 2377 페이지
- 호스트 ID 소스, 2395 페이지
- 애플리케이션 탐지, 2439 페이지
- 영역 생성 및 관리, 2461 페이지
- ISE/ISE-PIC를 사용하여 사용자 제어, 2485 페이지
- 캡티브 포털을 사용하여 사용자 제어, 2505 페이지
- Remote Access VPN을 사용하여 사용자 제어, 2521 페이지
- TS 에이전트를 사용하여 사용자 제어, 2525 페이지
- ID 정책 생성 및 관리, 2529 페이지
- 네트워크 검색 정책, 2537 페이지

94 장

네트워크 검색 및 ID 소개

다음 주제에서는 네트워크 검색 및 ID 정책과 데이터를 간단히 소개합니다.

- 호스트, 애플리케이션 및 사용자 검색 및 ID 데이터에 사용, 2377 페이지
- 호스트 및 애플리케이션 탐지 기초, 2378 페이지
- 사용자 ID 정보, 2385 페이지
- Firepower System 호스트 및 사용자 제한, 2391 페이지

호스트, 애플리케이션 및 사용자 검색 및 ID 데이터에 사용

로그 검색 및 ID 데이터를 이용하면 다음과 같은 Firepower System의 다양한 기능을 활용할 수 있습니다.

- 네트워크 맵 보기 - 호스트와 네트워크 디바이스, 호스트 특성, 애플리케이션 프로토콜 또는 취약성을 그룹화하여 네트워크 자산 및 토폴로지를 자세히 볼 수 있습니다.
- 애플리케이션 및 사용자 제어 수행 - 애플리케이션, 영역, 사용자, 사용자 그룹, ISE 속성 조건을 이용해 액세스 컨트롤 규칙을 작성합니다.
- 호스트 프로파일 보기 - 탐지된 호스트에 사용할 수 있는 모든 정보를 완전하게 보여줍니다.
- 대시보드 보기 - (가장 중요한) 네트워크 자산과 사용자 활동을 한눈에 보는 기능을 제공합니다.
- 시스템이 로깅한 검색 이벤트 및 사용자 활동에 대한 자세한 정보를 확인합니다.
- 호스트 및 서버나 이들이 실행하는 클라이언트를 취약한 익스플로잇에 연결합니다.

  이렇게 하면 취약성을 확인 및 완화하고, 침입 이벤트가 네트워크에 주는 영향을 평가하고, 침입 규칙 상태를 조정해 네트워크 자산에 대한 보호를 극대화할 수 있습니다.
- 시스템이 특정 영향 플래그와 함께 침입 이벤트를 생성하거나 특정 검색 이벤트를 생성할 경우 이메일, SNMP 트랩 또는 시스템 로그를 통해 알림을 전송합니다.
- 허용되는 운영체제, 클라이언트, 애플리케이션 프로토콜 및 프로토콜의 화이트리스트로 조직의 규정준수를 모니터링합니다.
- 시스템이 검색 이벤트를 생성하거나 사용자 활동을 탐지할 때 상관관계 이벤트를 트리거 및 생성하는 규칙으로 상관관계 정책을 생성합니다.

- 적용 가능한 경우 NetFlow 로깅 및 사용 연결도 사용합니다.

호스트 및 애플리케이션 탐지 기초

호스트 및 애플리케이션 탐지를 수행 하려면 네트워크 검색 정책을 구성할 수 있습니다.

자세한 내용은 개요: 호스트 데이터 수집, 2395 페이지 및 개요: 애플리케이션 탐지, 2439 페이지의 내용을 참조하십시오.

운영 체제 및 호스트 데이터의 수동 탐지

수동 탐지는 네트워크 트래픽을(그리고 내보낸 전체 NetFlow 데이터를) 분석해 네트워크 맵을 작성하는, 시스템의 기본 방법입니다. 수동 탐지는 운영체제와 실행 중인 애플리케이션 같은, 네트워크 자산에 대한 상황에 맞는 정보를 제공합니다.

모니터링하는 호스트에서 오는 트래픽이 호스트의 운영체제에 대한 결정적 증거를 제공하지 않는다면, 네트워크 맵은 가장 가능성이 높은 운영체제를 표시합니다. 예를 들어 NAT 디바이스는 호스트가 NAT 디바이스 "뒤에" 있기 때문에, 여러 운영체제를 실행하는 것처럼 보일 수 있습니다. 판단의 정확도를 높이기 위해 시스템은 탐지한 운영체제 각각에 자신이 할당한 신뢰도 값과, 탐지한 운영체제 간의 보강 데이터 양을 사용합니다.

참고 시스템은 보고된 "알 수 없는" 애플리케이션과 운영체제는 판단할 때 고려하지 않습니다.

수동 탐지가 네트워크 자산을 올바르게 식별하지 못한다면, 매니지드 디바이스의 배치를 확인해 보십시오. 맞춤형 운영체제 지문과 맞춤형 애플리케이션 탐지기를 이용해 시스템의 수동 탐지 기능을 강화할 수도 있습니다. 또한 트래픽 분석에 기반을 두지 않지만 대신 스캔 결과 및 기타 정보 소스를 이용해 네트워크 맵을 바로 업데이트할 수 있는, 능동 탐지를 사용하는 방법도 있습니다.

운영 체제 및 호스트 데이터의 활성 탐지

능동 탐지는 활성 소스가 수집한 호스트 정보를 네트워크 맵에 추가합니다. 예를 들어 Nmap 스캐너를 사용하면 네트워크에서 대상으로 삼은 호스트를 능동적으로 스캔할 수 있습니다. Nmap은 호스트 상의 운영체제와 애플리케이션을 검색합니다.

또한 호스트 입력 기능을 사용하면 호스트 입력 데이터를 네트워크 맵에 능동적으로 추가할 수 있습니다. 호스트 입력 데이터에는 두 가지 카테고리가 있습니다.

- 사용자 입력 데이터 - Firepower System 사용자 인터페이스 통해 추가한 데이터입니다. 사용자 인터페이스를 통해 호스트의 운영체제나 애플리케이션 ID를 수정할 수 있습니다.
- 호스트 입력된 데이터를 가져오기-데이터 명령행 유틸리티를 사용 하 여 가져옵니다.

시스템은 각 활성 소스에 대해 하나의 ID를 유지합니다. 예를 들어 Nmap 스캔 인스턴스를 실행하면 이전 스캔 결과가 새 스캔 결과로 교체됩니다. 그러나 Nmap 스캔을 실행한 다음 그 결과를 명령줄을

통해 가져온 클라이언트의 데이터로 교체하면, 시스템은 Nmap 결과의 ID와 가져오기 클라이언트의 ID를 모두 유지합니다. 그런 다음 시스템은 네트워크 검색 정책에 설정된 우선순위를 사용하여 어떤 능동 ID를 현재 ID로 사용할 것인지 결정합니다.

사용자 입력은 서로 다른 사용자가 입력했다 하더라도 하나의 소스로 간주됩니다. 예를 들어 UserA가 호스트 프로파일을 통해 운영체제를 설정한 다음 UserB가 호스트 프로파일을 통해 정의를 변경하면, UserB가 설정한 정의가 유지되고 UserA가 설정한 정의는 폐기됩니다. 또한 사용자 입력은 다른 모든 활성 소스를 재정의하며, 존재하는 경우 현재 ID로 사용됩니다.

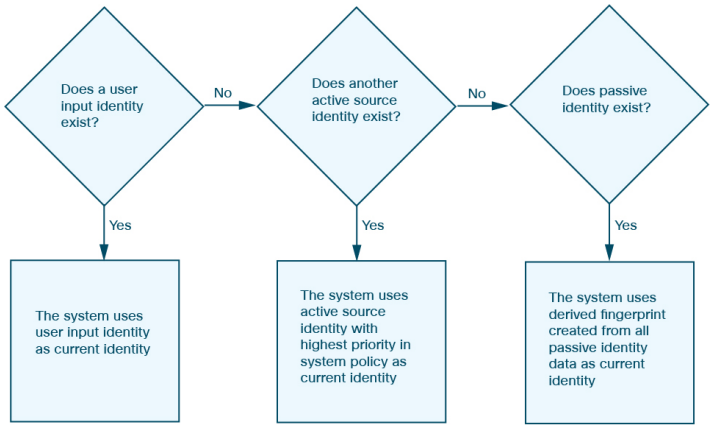
애플리케이션 및 운영 체제에 대한 현재 ID

호스트에 있는 애플리케이션 또는 운영체제의 현재 *ID*는 시스템이 가장 정확할 것이라고 판단하는 ID입니다.

시스템은 다음과 같은 용도로 운영체제 또는 애플리케이션에 대한 현재 ID를 사용합니다.

- 호스트에 취약성 할당
- 영향 평가
- 운영체제 식별, 호스트 프로파일 자격 및 규정준수 화이트 목록에 대해 작성한 상관관계 규칙 평가 시
- 워크플로의 Hosts(호스트) 및 Servers(서버) 테이블 보기에서 표시
- 호스트 프로파일에서 표시
- Discovery Statistics(검색 통계) 페이지리 운영체제 및 애플리케이션 통계 계산

시스템은 어떤 능동 ID를 애플리케이션 또는 운영체제에 대한 현재 ID로 사용할지를 결정할 때 소스 우선순위를 사용합니다.



예를 들어 사용자가 호스트에서 운영체제를 Windows 2003 Server로 설정하면 Windows 2003 Server가 현재 ID가 됩니다. 해당 호스트의 Windows 2003 Server 취약성에 대한 공격에는 더 높은 영향이 지정되고, 호스트 프로파일의 해당 호스트에 대해 나열된 취약성에는 Windows 2003 Server 취약성이 포함됩니다.

데이터베이스에 호스트의 특정 운영체제 또는 특정 애플리케이션에 대한 여러 소스의 정보가 포함될 수 있습니다.

시스템은 데이터에 대한 소스가 가장 높은 소스 우선순위를 가지고 있을 때 운영체제 또는 애플리케이션 ID를 현재 ID로 취급합니다. 가능한 소스의 우선순위 순서는 다음과 같습니다.

1. 사용자

2. 스캐너 및 애플리케이션(네트워크 검색 정책에 설정됨)

3. 매니지드 디바이스

4 . Netflow 레코드

우선순위가 더 높은 새 애플리케이션 ID는 현재 ID보다 상세정보이 부족하면 현재 애플리케이션 ID를 재정의하지 않습니다.

또한 ID 충돌이 발생하는 경우 충돌의 해결은 네트워크 검색 정책의 설정 또는 수동 해결에 의존하게 됩니다.

현재 사용자 ID

시스템은 다른 사용자가 같은 호스트에 여러 번 로그인하는 경우를 탐지하면 특정 시점에 지정된 호스트에 한 명의 사용자만 로그인하며 호스트의 현재 사용자가 마지막 권한 있는 사용자 로그인이라고 가정합니다. 권한 없는 사용자 로그인만 호스트에 로그인한 경우, 권한 없는 최근 로그인이 현재 사용자로 간주됩니다. 원격 세션을 통해 여러 사용자가 로그인한 경우 서버에서 보고한 마지막 사용자가 Firepower Management Center에 보고됩니다.

같은 사용자가 동일 호스트에 여러 번 로그인했음이 탐지되는 경우 시스템은 특정 호스트에 대한 사용자의 첫 번째 로그인만 기록하고 이후의 로그인은 무시합니다. 개별 사용자가 특정 호스트에 로그인하는 유일한 사람인 경우, 시스템에서는 원래 로그인만 기록합니다.

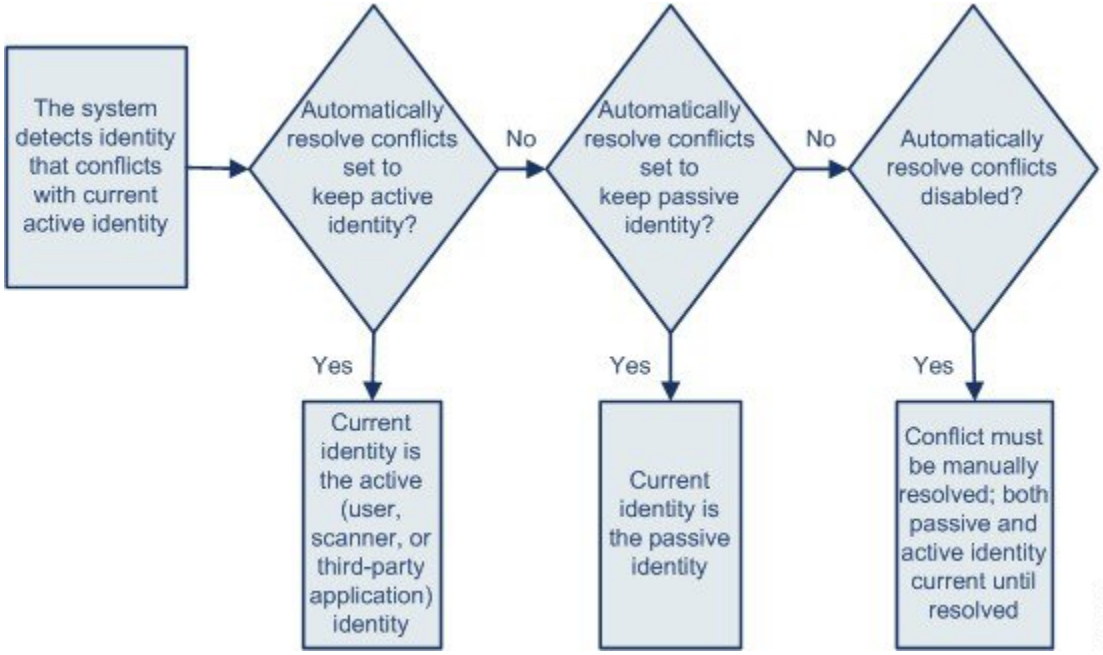
그러나 또 다른 사용자가 해당 호스트에 로그인하면 시스템에서는 새 로그인을 기록합니다. 그런 다음 원래 사용자가 다시 로그인하면 새 로그인이 기록됩니다.

애플리케이션 및 운영 체제 ID 충돌

시스템이 현재 능동 ID와 충돌하며 전에는 수동 ID로 보고되었던 새로운 수동 ID를 보고하면 *ID* 충돌이 발생합니다. 예를 들어 운영체제에 대한 이전 수동 ID가 Windows 2000으로 보고되면, Windows XP의 능동 ID가 현재 ID가 됩니다. 이후 시스템은 Ubuntu Linux 8.04.1의 새로운 수동 ID를 탐지합니다. 그러면 Windows XP와 Ubuntu Linux ID가 충돌하게 됩니다.

호스트의 운영체제 또는 호스트의 애플리케이션에서 ID 충돌이 발생하면, 시스템은 충돌이 해결될 때까지 충돌하는 두 ID를 모두 현재 ID로 나열하고 영향 평가에 두 ID를 모두 사용합니다.

관리자 권한이 있는 사용자는 항상 수동 ID를 사용하거나 항상 능동 ID를 사용하도록 선택하여 ID 충돌을 자동으로 해결할 수 있습니다. ID 충돌 자동 해결을 비활성화하지 않는 한 ID 충돌은 항상 자동으로 해결됩니다.



관리자 권한이 있는 사용자는 ID 충돌이 발생할 경우 이벤트를 생성하도록 시스템을 구성할 수도 있습니다. 그러면 해당 사용자는 Nmap 스캔을 상관관계 응답으로 사용하는 상관관계 규칙을 이용해 상관관계 정책을 설정할 수 있습니다. 이벤트가 발생하면 Nmap은 호스트를 스캔하여 업데이트된 호스트 운영체제 및 애플리케이션 데이터를 가져옵니다.

Firepower System의 Netflow 데이터

NetFlow는 라우터를 통과하여 이동하는 패킷에 대한 통계를 제공하는 Cisco IOS 애플리케이션입니다. 이는 Cisco 네트워킹 디바이스에서 제공되며 Juniper, FreeBSD, OpenBSD 디바이스에도 임베디드될 수 있습니다.

NetFlow가 네트워크 디바이스에서 활성화된 경우, 디바이스의 데이터베이스(NetFlow 캐시)는 라우터를 통과하는 플로우의 레코드를 저장합니다. Firepower System에서 연결이라고도 하는 플로우는 특정 포트, 프로토콜, 애플리케이션 프로토콜을 사용하여 소스 호스트와 대상 호스트 간의 세션을 나타내는 연속된 패킷입니다. 이 NetFlow 데이터를 내보내도록 네트워크 디바이스를 구성할 수 있습니다. 이 문서에서는 이러한 방식으로 구성된 네트워크 디바이스를 *NetFlow* 엑스포터라고 합니다.

Firepower System 매니지드 디바이스를 구성하여 NetFlow 엑스포터에서 레코드를 수집하고, 이러한 레코드의 데이터를 바탕으로 단방향 연결 종료 이벤트를 생성하고, 마지막으로 해당 이벤트를 Firepower Management Center에 전송하여 연결 이벤트 데이터베이스에 로깅할 수 있습니다. NetFlow 연결의 정보를 기반으로 호스트 및 애플리케이션 프로토콜 정보를 데이터베이스에 추가하도록 네트워크 검색 정책을 구성할 수도 있습니다.

매니지드 디바이스에 의해 직접 수집된 데이터를 보완하기 위해 이 검색 및 연결 데이터를 사용할 수 있습니다. 이는 매니지드 디바이스에서 모니터링할 수 없는 NetFlow 엑스포터 모니터링 네트워크를 보유하고 있는 경우 특히 유용합니다.

NetFlow 데이터를 사용하기 위한 요건

NetFlow 데이터 분석을 위해 Firepower System을 구성하기에 앞서 사용하려는 라우터 또는 기타 NetFlow 지원 디바이스에서 NetFlow 기능을 활성화하고 매니지드 디바이스의 센싱 인터페이스가 연결된 대상 네트워크로 NetFlow 데이터를 브로드캐스트하도록 디바이스를 구성해야 합니다.

Firepower System은 NetFlow 버전 5 및 NetFlow 버전 9 레코드를 모두 구문 분석할 수 있습니다. 데이터를 Firepower System으로 내보내려는 경우 NetFlow 엑스포터는 반드시 다음 버전 중 하나를 사용해야 합니다. 또한, 내보낸 NetFlow 템플릿과 레코드에 특정 필드가 있어야 합니다. NetFlow 엑스포터가 버전 9(맞춤 설정 가능)를 사용 중인 경우, 내보낸 템플릿과 레코드에 다음 필드가 포함되어 있는지 반드시 확인해야 합니다(순서는 상관없음).

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Firepower System은 매니지드 디바이스를 NetFlow 데이터 분석에 사용하므로, NetFlow 엑스포터를 모니터링할 수 있는 하나 이상의 매니지드 디바이스를 구축에 포함해야 합니다. 내보낸 NetFlow 데이터를 수집할 수 있는 네트워크에 이러한 매니지드 디바이스에 있는 하나 이상의 센싱 인터페이스를 연결해야 합니다. 매니지드 디바이스의 센싱 인터페이스에는 일반적으로 IP 주소가 없기 때문에 시스템은 NetFlow 레코드의 직접 수집을 지원하지 않습니다.

일부 네트워크 디바이스에서 사용 가능한 Sampled NetFlow 기능은 디바이스를 통과하는 패킷의 하위 집합에 대해서만 NetFlow 통계를 수집합니다. 이 기능을 활성화하면 네트워크 디바이스에서 CPU 사용률이 향상될 수 있지만, Firepower System의 분석을 위해 수집하는 NetFlow 데이터에 영향을 줄 수 있습니다.

NetFlow와 매니지드 디바이스 데이터의 차이점

Firepower는 NetFlow 데이터로 표시되는 트래픽을 직접 분석하지 않습니다. 대신, 내보낸 NetFlow 레코드를 연결 로그 및 호스트/애플리케이션 프로토콜 데이터로 변환합니다.

따라서 변환된 NetFlow 데이터와 매니지드 디바이스에서 직접 수집된 검색 및 연결 데이터 간에는 몇 가지 차이점이 있습니다. 다음 항목을 필요로 하는 분석을 수행할 경우 이러한 차이점에 유의해야 합니다.

- 탐지된 연결 수에 대한 통계
- 운영 체제 및 기타 호스트 관련 정보(취약성 포함)
- 클라이언트 정보, 웹 애플리케이션 정보, 공급업체 및 버전 서버 정보를 비롯한 애플리케이션 데이터
- 연결에서 어떤 호스트가 이니시에이터이고 어떤 호스트가 응답자인지 파악

네트워크 검색 정책과 액세스 제어 정책 비교

네트워크 검색 정책의 규칙을 사용하여 연결 로깅을 비롯한 NetFlow 데이터 수집을 구성합니다. 반면, Firepower System 매니지드 디바이스에서 탐지된 연결에 대한 연결 로깅은 액세스 제어 규칙별로 구성합니다.

연결 이벤트 유형

NetFlow 데이터 수집은 액세스 제어 규칙이 아닌 네트워크에 연결되므로 시스템이 로깅하는 NetFlow 연결을 세분화된 방식으로 제어할 수 없습니다.

NetFlow 데이터는 보안 인텔리전스 이벤트를 생성할 수 없습니다.

NetFlow 기반 연결 이벤트는 연결 이벤트 데이터베이스에만 저장할 수 있으며 시스템 로그 또는 SNMP 트랩 서버로 전송할 수 없습니다.

모니터링되는 세션별로 생성되는 연결 이벤트 수

매니지드 디바이스에서 직접 탐지된 연결의 경우 연결의 시작이나 끝 중 하나 또는 시작과 끝 둘 다에서 양방향 연결 이벤트를 로깅하도록 액세스 제어 규칙을 구성할 수 있습니다.

반면, 내보낸 NetFlow 레코드는 단방향 연결 데이터를 포함하므로 시스템은 처리하는 각 NetFlow 레코드에 대해 최소 두 개의 연결 이벤트를 생성합니다. 따라서 NetFlow 데이터 기반의 각 연결에 대해 요약의 연결 수가 2씩 증가하므로, 네트워크에서 실제로 발생하는 연결 수보다 많은 개수가 제공됩니다.

NetFlow 엑스포터는 연결이 계속 진행되는 중이라도 고정된 간격으로 레코드를 출력하므로, 세션이 오랫동안 실행되는 경우 여러 레코드를 내보낼 수 있으며 각 레코드가 연결 이벤트를 생성합니다. 예를 들어 NetFlow 엑스포터가 5분마다 내보내기를 실행하는데 특정 연결이 12분 동안 지속될 경우 해당 세션에 대해 연결 이벤트 6개가 생성됩니다.

- 첫 번째 5분 동안 이벤트 쌍 하나
- 두 번째 5분 동안 이벤트 쌍 하나
- 연결이 종료될 때 마지막 쌍

호스트 및 운영 체제 데이터

NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에는 운영 체제, NetBIOS 또는 호스트 유형(호스트 디바이스 또는 네트워크 디바이스) 정보가 없습니다. 그러나 호스트 입력 기능을 사용하여 호스트의 운영 체제를 수동으로 설정할 수 있습니다.

응용프로그램 데이터

매니지드 디바이스에서 직접 탐지하는 연결의 경우, 시스템은 연결의 패킷을 검토하여 애플리케이션 프로토콜, 클라이언트 및 웹 애플리케이션을 식별할 수 있습니다.

시스템은 NetFlow 레코드를 처리할 때 애플리케이션 프로토콜 ID를 추정하기 위해 `/etc/sf/services`의 포트 상관관계를 사용합니다. 그러나 그러한 애플리케이션 프로토콜에 대한 공급업체 또는 버전 정보가 없으며, 연결 로그에는 세션에서 사용된 클라이언트 또는 웹 애플리케이션에 대한 정보가 포함되지 않습니다. 그러나 호스트 입력 기능을 사용해 이러한 정보를 수동으로 제공할 수 있습니다.

단순한 포트 상관관계는, 비표준 포트에서 실행 중인 애플리케이션 프로토콜이 식별되지 않거나 잘못 식별될 수 있음을 의미합니다. 또한 상관관계가 존재하지 않는 경우 시스템은 연결 로그에서 애플리케이션 프로토콜을 `unknown`으로 표시합니다.

취약성 매핑

호스트 입력 기능을 사용하여 호스트의 운영 체제 ID 또는 애플리케이션 프로토콜 ID를 수동으로 설정하지 않으면 시스템이 NetFlow 엑스포터에서 모니터링하는 호스트에 취약성을 매핑할 수 없습니다. NetFlow 연결에는 클라이언트 정보가 없으므로 클라이언트 취약성을 NetFlow 데이터에서 생성된 호스트와 연결할 수 없습니다.

연결의 이니시에이터 및 **Responder** 정보

매니지드 디바이스에서 직접 탐지하는 연결의 경우, 시스템은 어떤 호스트가 이니시에이터(또는 소스)인지, 그리고 어떤 호스트가 responder(또는 대상)인지를 식별할 수 있습니다. 그러나 NetFlow 데이터에는 이니시에이터 또는 responder 정보가 포함되어 있지 않습니다.

Firepower System은 NetFlow 레코드를 처리할 때 특정 알고리즘을 사용하여 각 호스트에서 사용 중인 포트 및 해당 포트가 잘 알려진 포트인지 여부를 기반으로 이 정보를 확인합니다.

- 사용 중인 두 포트 모두 잘 알려진 포트이거나 둘 다 잘 알려진 포트가 아닌 경우 시스템은 낮은 번호의 포트를 사용하는 호스트를 responder로 간주합니다.
- 호스트 중 하나만 잘 알려진 포트인 경우 시스템은 이 호스트를 responder로 간주합니다.

따라서 잘 알려진 포트는 1~1023 범위의 포트이거나 매니지드 디바이스에서 `/etc/sf/services`에 애플리케이션 프로토콜 정보를 포함하는 포트입니다.

또한 매니지드 디바이스에서 직접 탐지된 연결의 경우 해당 연결 이벤트에 다음과 같이 두 개의 바이트 수가 기록됩니다.

- **Initiator Bytes(**이니시에이터 바이트**)** 필드에는 전송된 바이트가 기록됩니다.
- **Responder Bytes(Responder** 바이트**)** 필드에는 수신된 바이트가 기록됩니다.

단방향 NetFlow 레코드를 기반으로 하는 연결 이벤트는 한 개의 바이트 수만 포함합니다. 시스템은 포트 기반 알고리즘에 따라 이 개수를 **Initiator Bytes(**이니시에이터 바이트**)** 또는 **Responder Bytes(Responder** 바이트**)**에 할당합니다. 다른 필드는 0으로 설정됩니다. NetFlow 레코드의 연결 요약(집계된 연결 데이터)을 확인하는 경우에는 두 필드에 모두 정보가 입력되어 있을 수 있습니다.

NetFlow 전용 연결 이벤트 필드

일부 필드는 NetFlow 레코드에서 생성된 연결 이벤트에만 표시됩니다. 연결 이벤트 필드에서 제공되는 정보, 2896 페이지를 참조하십시오.

관련 항목

연결 이벤트 필드에서 제공되는 정보, 2896 페이지

사용자 ID 정보

사용자 ID 정보를 이용하면 정책 위반, 공격, 네트워크 취약성의 원인을 파악하고, 이를 추적해 관련 사용자를 확인할 수 있습니다. 예를 들어, 다음을 확인할 수 있습니다.

- 영향 레벨이 Vulnerable(취약 - 레벨 1: 빨간색)인 침입 이벤트가 대상으로 지정한 호스트의 소유자
- 내부 공격 또는 포트스캔을 시작한 사용자
- 지정한 호스트에 무단 액세스를 시도하는 사용자
- 대역폭을 너무 많이 사용하는 사용자
- 중요한 운영체제 업데이트를 적용하지 않은 사용자
- 회사 IT 정책을 위반하며 인스턴트 메시징 소프트웨어나 P2P 파일 공유 애플리케이션을 사용하는 사용자

이러한 정보를 충분히 파악하면 Firepower System의 다른 기능을 사용하여 위험을 완화하고, 액세스 제어를 수행하고, 다른 사용자의 작업 중단을 방지하는 조치를 취할 수 있습니다. 또한 이러한 기능을 통해 감사 제어 효과를 크게 높이고 규정 준수를 강화할 수 있습니다.

사용자 데이터를 수집하도록 사용자 ID 소스를 구성한 후에는 사용자 인식 및 사용자 제어를 수행할 수 있습니다.

비디오 ID 설정을 위한 YouTube 비디오

관련 항목

ID 용어, 2385 페이지
ID 구축, 2388 페이지

ID 용어

이 주제에서는 사용자 ID 및 사용자 제어와 관련해 자주 사용하는 용어를 설명합니다.

사용자 인식

ID 소스(또는 TS 에이전트 등)를 이용해 네트워크 상의 사용자를 식별합니다. 사용자 인식을 이용하면 신뢰할 수 있는(Active Directory 등) 소스와 신뢰할 수 없는(애플리케이션 기반) 소스의 사용자를 모두 식별할 수 있습니다. Active Directory를 ID 소스로 사용하려면 영역과 디렉터리를 설정해야 합니다. 자세한 내용은 사용자 ID 소스 정보를 참고하십시오.

사용자 제어

액세스 컨트롤 정책과 연결한 *ID* 정책을 설정합니다. (이후 ID 정책은 액세스 컨트롤 하위 정책으로 참조됩니다.) ID 정책은 ID 소스를 지정하면, 경우에 따라 해당 소스에 속하는 사용자와 그룹도 지정합니다.

ID 정책을 액세스 컨트롤 정책과 연결하면, 네트워크 트래픽에서의 사용자나 사용자 활동 모니터링, 신뢰, 차단 또는 허용 여부를 결정하게 됩니다. 자세한 내용은 액세스 제어 정책, 1625 페이지를 참고하십시오.

권한 있는 **ID** 소스

사용자 로그인(예: Active Directory)을 검증한 신뢰할 수 있는 서버입니다. 권한 있는 로그인에서 가져온 데이터를 사용하여 사용자 인식 및 사용자 제어를 수행할 수 있습니다. 권한 있는 사용자 로그인은 수동 및 활성 인증에서 가져옵니다.

- 패시브 인증은 외부 서버를 통해 사용자를 인증할 때 수행됩니다. ISE는 Firepower System에서 지원하는 패시브 인증 방법입니다.

  패시브 인증은 외부 소스를 통해 사용자를 인증할 때 수행됩니다. ISE/ISE-PIC 및 TS 에이전트는 Firepower System에서 지원하는 패시브 인증 방법입니다.

- 액티브 인증은 사전 구성된 매니지드 디바이스를 통해 사용자를 인증할 때 수행됩니다. 캡티브 포털(captive portal) 및 원격 액세스 VPN은 Firepower System에서 지원하는 액티브 인증 방법입니다.

권한 없는 **ID** 소스

사용자 로그인이 검증된 알 수 없거나 신뢰할 수 없는 서버입니다. 트래픽 기반 탐지는 Firepower System에서 지원하는 유일한 권한 없는 ID 소스입니다. 권한 없는 로그인에서 가져온 데이터를 사용하여 사용자 인식을 수행할 수 있습니다.

사용자 ID 모범 사례

ID 정책을 설정하기 전에 다음 정보를 검토하는 것이 좋습니다.

- 사용자 제한 확인
- 신뢰에 대해 AD 도메인당 하나의 영역 생성
- 상태 모니터
- 최신 버전의 ISE/ISE-PIC, 두 가지 교정 유형 사용
- 6.7에서 사용자 에이전트 지원 중단

- 종속 포털에는 라우팅 인터페이스, 여러 개별 작업이 필요함
- TS 에이전트 문제 해결 참조

Active Directory, LDAP 및 영역

Firepower System은 사용자 인식 및 제어를 위해 Active Directory 또는 LDAP를 지원합니다. Active Directory 또는 LDAP 리포지토리와 FMC 간의 연결을 영역이라고 합니다. LDAP 서버 또는 Active Directory 도메인당 하나의 영역을 생성해야 합니다. 지원되는 버전에 대한 자세한 내용은 영역에 지원되는 서버, 2463 페이지의 내용을 참조하십시오.

LDAP에서 지원하는 유일한 사용자 ID 소스는 종속 포털입니다. 다른 ID 소스(ISE/ISE-PIC 제외)를 사용하려면 Active Directory를 사용해야 합니다.

Active Directory에만 해당:

- 도메인 컨트롤러당 하나의 디렉터리를 생성합니다.

  자세한 내용은 영역 디렉터리 설정, 2475 페이지 섹션을 참조해 주십시오.

상태 모니터

FMC 상태 모니터는 다음을 비롯한 다양한 FMC 기능의 상태에 대한 유용한 정보를 제공합니다.

- 사용자/영역 불일치
- Snort 메모리 사용량
- ISE 연결 상태

상태 모듈에 대한 자세한 내용은 상태 모듈, 389 페이지의 내용을 참조하십시오.

상태 모듈을 모니터링하기위한 정책을 설정하려면 상태 정책 생성, 398 페이지의 내용을 참조하십시오.

디바이스별 사용자 제한

모든 물리적 또는 가상 FMC 디바이스에는 다운로드할 수 있는 사용자 수가 제한되어 있습니다. 사용자 제한에 도달하면 FMC의 메모리가 부족하여 결과적으로 신뢰할 수 없는 기능을 수행할 수 있습니다.

사용자 제한은 Firepower System 사용자 한도, 2392 페이지에서 설명합니다.

ISE/ISE-PIC ID 소스를 사용하는 경우 선택적으로 FMC가 모니터링하는 서브넷을 제한하여 ID 정책 생성, 2534 페이지에서 설명한 대로 ID 매핑 필터를 사용하여 메모리 사용량을 줄일 수 있습니다.

최신 버전의 ISE/ISE-PIC 사용

ISE/ISE-PIC ID 소스를 사용할 것으로 예상되는 경우 항상 최신 버전을 사용하여 최신 기능과 버그를 수정하는 것이 좋습니다.

pxGrid 2.0(버전 2.6 패치 6 이상 또는 2.7 패치 2 이상에서 사용됨)도 ISE/ISE-PIC에서 사용하는 교정을 EPS(Endpoint Protection Service)에서 ANC(Adaptive Network Control)로 변경합니다. ISE/ISE-PIC를 업그레이드하는 경우 EPS에서 ANC로 교정 정책을 마이그레이션해야 합니다.

ISE/ISE-PIC 사용에 대한 자세한 내용은 ISE/ISE-PIC 지침 및 제한 사항, 2488 페이지에서 확인할 수 있습니다.

ISE/ISE-PIC ID 소스를 설정하려면 사용자 제어에 대한 ISE/ISE-PIC 설정 방법, 2490 페이지의 내용을 참조하십시오.

캡티브 포털 정보

캡티브 포털은 LDAP 또는 Active Directory를 사용할 수 있는 유일한 사용자 ID 소스입니다. 또한 매니지드 디바이스는 라우팅된 인터페이스를 사용하도록 구성해야 합니다.

추가 지침은 캡티브 포털 가이드라인 및 제한 사항, 2506 페이지에서 볼 수 있습니다.

캡티브 포털을 설정하려면 여러 독립적인 작업을 수행해야 합니다. 자세한 내용은 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지를 참고하십시오.

TS Agent 정보

TS 에이전트 사용자 ID 소스는 Windows 터미널 서버에서 사용자 세션을 식별하는 데 필요합니다. TS 에이전트 소프트웨어는 *Cisco TS(Terminal Services)* 에이전트 가이드에 설명된 대로 터미널 서버 시스템에 설치해야 합니다. 또한 TS 에이전트 서버의 시간을 Firepower Management Center의 시간과 동기화해야 합니다.

TS 에이전트 데이터는 Users(사용자), User Activity(사용자 활동), Connection Event(연결 이벤트) 테이블에 표시되며 사용자 인식 및 사용자 제어에 사용할 수 있습니다.

자세한 내용은 TS 에이전트 가이드라인, 2525 페이지를 참고하십시오.

ID 정책을 액세스 제어 정책과 연결합니다.

영역, 디렉터리 및 사용자 ID 소스를 구성한 후에는 ID 정책에서 ID 규칙을 설정해야 합니다. 정책을 적용하려면 ID 정책을 액세스 제어 정책과 연결해야 합니다.

ID 정책 생성에 대한 자세한 내용은 ID 정책 생성, 2534 페이지의 내용을 참조하십시오.

ID 규칙 생성에 대한 자세한 내용은 ID 규칙 생성, 2531 페이지의 내용을 참조하십시오.

ID 정책을 액세스 제어 정책과 연결하려면 액세스 제어에 다른 정책 연결, 1641 페이지의 내용을 참조하십시오.

FMC의 사용자 에이전트 사용 중단 및 지원 종료

자세한 내용은 Cisco Firepower 사용자 에이전트 사용 중단 및 지원 종료를 참조하십시오.

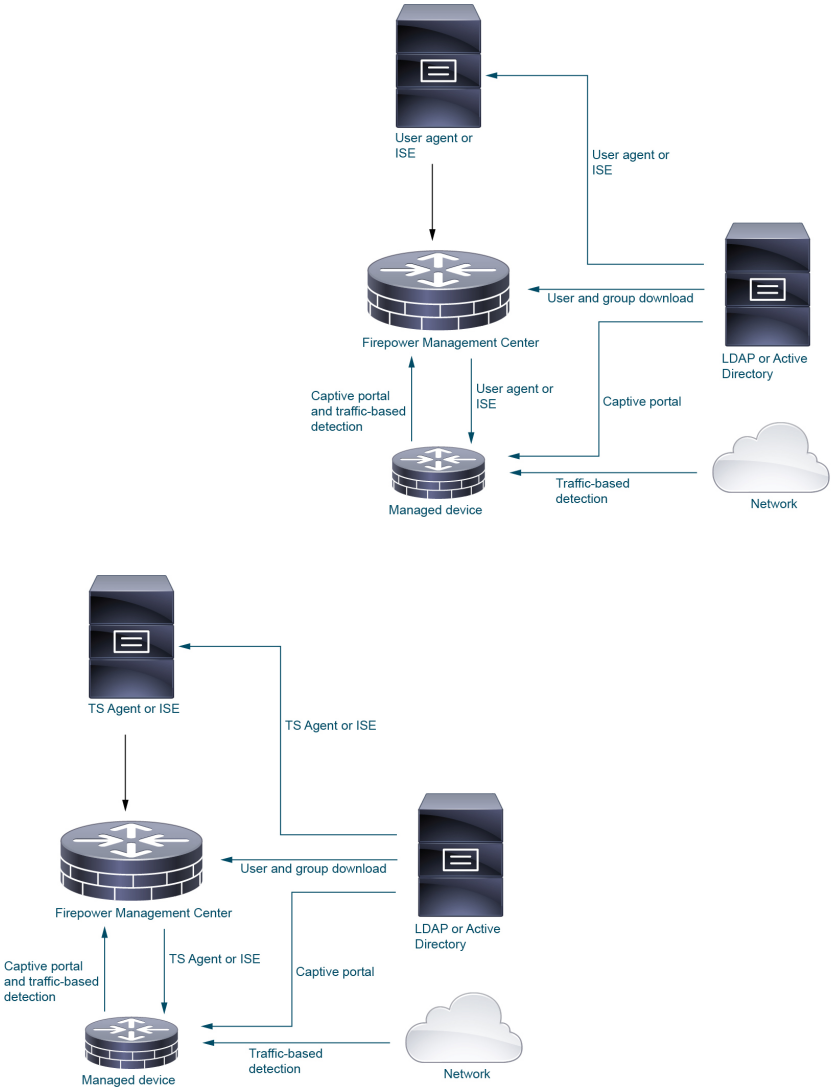
ID 구축

시스템이 사용자 로그인, ID 소스로부터 사용자 데이터를 탐지하면 해당 로그인의 사용자는 Firepower Management Center 사용자 데이터베이스의 사용자 목록과 비교하여 확인됩니다. 로그인 사용자가 기

존 사용자와 일치하면 로그인의 데이터가 사용자에게 할당됩니다. 로그인이 기존 사용자와 일치하지 않으면 SMTP 트래픽의 로그인이 아닌 경우 새 사용자가 생성됩니다. SMTP 트래픽의 일치하지 않는 로그인은 삭제됩니다.

사용자가 속하는 그룹은 가 사용자를 확인하고 Firepower Management Center할 때 사용자와 연결됩니다.

다음 다이어그램은 Firepower System이 사용자 데이터를 수집 및 저장하는 방법을 보여줍니다.



사용자 활동 데이터베이스

Firepower Management Center의 사용자 활동 데이터베이스에는 구성된 모든 ID 소스에서 탐지하거나 보고하는 네트워크의 사용자 활동 기록이 포함됩니다. 시스템에서는 다음과 같은 상황에서 이벤트를 기록합니다.

- 개별 로그인 또는 로그오프를 탐지한 경우
- 새 사용자를 탐지한 경우
- 시스템 관리자가 사용자를 수동으로 삭제하는 경우
- 데이터베이스에 없는 사용자를 탐지했으나 사용자 제한에 도달하여 사용자를 추가할 수 없는 경우

참고 TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE/ISE-PIC 등)로 모니터링할 경우, Firepower Management Center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 다른 수동 소스가 동일한 IP 주소로 활동을 보고할 경우, TS 에이전트 데이터만 Firepower Management Center에 로깅됩니다.

시스템이 탐지한 사용자 활동은 Firepower Management Center 웹 인터페이스로 확인할 수 있습니다. (**Analysis(**분석 > **Users(**사용자**)** > **User Activity(**사용자 활동).

사용자 데이터베이스

Firepower Management Center의 사용자 데이터베이스에는 구성된 모든 ID 소스에서 탐지하거나 보고한 기록이 포함됩니다. 사용자 제어에 대한 신뢰할 수 있는 소스에서 얻은 데이터를 사용할 수 있습니다.

지원되는 신뢰할 수 있거나 신뢰할 수 없는 ID 소스에 대한 자세한 내용은 사용자 ID 소스 정보 섹션을 참조하십시오.

Firepower System 사용자 한도, 2392 페이지에서도 설명하지만, Firepower Management Center이(가) 저장할 수 있는 총 사용자 수는 Firepower Management Center 모델에 따라 다릅니다. 사용자 한도에 도달하면, 시스템은 이전에 탐지하지 않은 사용자 데이터의 다음과 같은 ID 소스를 바탕으로 우선순위를 지정합니다.

- 새 사용자가 신뢰할 수 없는 ID 소스에서 왔다면, 시스템은 사용자를 데이터베이스에 추가하지 않습니다. 새 사용자를 추가하려면, 사용자를 수동으로 삭제하거나 데이터베이스 비우기를 이용해 삭제해야 합니다.
- 새 사용자가 신뢰할 수 있는 ID 소스에서 왔다면, 시스템은 가장 오랫동안 비활성 상태인 신뢰할 수 없는 사용자를 삭제하고 새 사용자를 데이터베이스에 추가합니다.

특정 사용자 이름을 제외하도록 ID 소스를 구성한 경우 해당 사용자 이름의 사용자 활동 데이터는 Firepower Management Center에 보고되지 않습니다. 이러한 제외된 사용자 이름은 데이터베이스에 남아 있지만 IP 주소와는 연결되지 않습니다. 시스템이 저장하는 데이터 유형에 대한 자세한 내용은 사용자 데이터, 3084 페이지 섹션을 참조하십시오.

Firepower Management Center 고가용성을 설정한 상태이고 기본 디바이스가 실패할 경우, 페일오버 다운타임 동안에는 캡티브 포털, ISE/ISE-PIC, TS 에이전트 또는 원격 액세스 VPN 디바이스에서 보고된 로그인을 식별할 수 없습니다. 사용자가 이전에 확인된 적이 있고 Firepower Management Center에 다운로드된 적이 있더라도 마찬가지입니다. 식별되지 않은 사용자는 Firepower Management Center

에서 알 수 없는 사용자로 로깅됩니다. 다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.

참고 TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE/ISE-PIC)로 모니터링할 경우, Firepower Management Center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 다른 수동 소스가 동일한 IP 주소로 활동을 보고할 경우, TS 에이전트 데이터만 Firepower Management Center에 로깅됩니다.

시스템이 새로운 사용자 세션을 탐지하면, 사용자 세션 데이터는 다음 중 하나가 발생할 때까지 사용자 데이터베이스 보관됩니다.

- Firepower Management Center의 사용자가 사용자 세션을 수동으로 삭제합니다.
- ID 소스가 해당 사용자 세션의 로그오프를 보고합니다.
- 영역의 **User Session Timeout: Authenticated Users(**사용자 세션 시간 초과**:** 인증된 사용자**)**, **User Session Timeout: Failed Authentication Users(**사용자 세션 시간 초과**:** 실패한 인증 사용자**)** 또는 **User Session Timeout: Guest Users(**사용자 세션 시간 초과**:** 게스트 사용자**)** 설정에서 지정된 대로 영역의 사용자 세션이 종료됩니다.

Firepower System 호스트 및 사용자 제한

Firepower Management Center 모델에 따라 구축을 통해 모니터링할 수 있는 개별 호스트 수와, 사용자 제어를 수행하기 위해 모니터링하고 사용할 수 있는 사용자 수가 결정됩니다.

관련 항목

FMC 데이터베이스에서 데이터 제거, 270 페이지

Firepower System 호스트 제한

시스템은 모니터링 중인 네트워크의 IP 주소와 관련된 활동을 감지하는 경우 (네트워크 검색 정책에 정의된 대로) 네트워크 맵에 호스트를 추가합니다. Firepower Management Center가 모니터링할 수 있는 호스트, 즉 네트워크 맵에 저장할 수 있는 호스트 수는 모델에 따라 다릅니다.

표 ***244: Firepower Management Center*** 모델별 호스트 제한

FMC 모델	호스트
MC1000	50,000
MC1600	50,000
MC2500	150,000
MC2600	150,000

FMC 모델	호스트
MC4500	600,000
MC4600	600,000
가상	50,000

네트워크 맵에 없는 호스트에 대한 상황 데이터를 볼 수 없습니다. 그러나 액세스 제어를 수행할 수 있습니다. 예를 들어, 호스트의 네트워크 규정준수 상황을 모니터하기 위한 규정준수 화이트리스트를 사용할 수 없는 경우에도 네트워크 맵에 없는 호스트를 오가는 트래픽에 대한 애플리케이션 제어를 수행할 수 있습니다.

참고 시스템은 MAC 전용 호스트를 IP 주소와 MAC 주소 모두로 식별하는 호스트와 별도로 계산합니다. 호스트와 연결된 모든 IP 주소는 하나의 호스트로 계산됩니다.

호스트 제한 도달 및 호스트 삭제

네트워크 검색 정책은 호스트 제한에 도달한 후 새 호스트가 탐지될 때 수행되는 작업을 제어합니다. 새 호스트를 삭제하거나 가장 오랫동안 비활성 상태였던 호스트를 교체할 수 있습니다. 또한 시스템 비활성화로 네트워크 맵에서 호스트를 제거하는 기간을 설정할 수 있습니다. 그러나 시스템이 삭제된 호스트와 관련된 활동을 탐지하는 경우 네트워크 맵에서 호스트, 전체 서브넷 또는 모든 호스트를 수동으로 제거할 수 있습니다.

다중 도메인 구축의 경우 각 리프 도메인에는 독립적인 네트워크 검색 정책이 있습니다. 따라서 각 리프 도메인은 시스템이 새 호스트를 검색하는 경우 고유한 동작을 제어합니다.

관련 항목

도메인 속성, 483 페이지
네트워크 검색 데이터 스토리지 설정, 2556 페이지

Firepower System 사용자 한도

Firepower Management Center 모델에 따라 모니터링할 수 있는 개별 사용자 수가 결정됩니다. 다음과 같은 경우 사용자가 Firepower Management Center 사용자 데이터베이스에 추가됩니다.

- 사용자가 영역에서 다운로드됩니다.
- 종속 포털 또는 RA-VPN 사용자가 로그인합니다.
- 모든 ID 소스에서 사용자가 탐지됩니다.

액세스 컨트롤 정책을 이용한 사용자 제어는 신뢰할 수 있는 사용자에만 적용됩니다.

다음에 유의하십시오.

- 다운로드된 사용자의 최대 수는 FMC 모델에 따라 다릅니다.

- 최대 동시 사용자 세션 수(즉, 로그인)는 FTD 모델에 따라 달라집니다. 단일 사용자는 서로 다른 고유한 IP 주소에서 여러 세션을 가질 수 있습니다.

참고 Firepower System은 모든 사용자 세션을 모든 FTD 디바이스에 다운로드합니다. 사용자 동시 사용자 세션 제한이 다른 디바이스가 있는 경우, 메모리가 구성된 제한에 도달하면 제한이 가장 작은 FTD에서 상태 경고를 보고합니다. (예를 들어, FMC가 FTD 4110 및 4120을 관리하는 경우 4110은 동시 사용자 세션 수가 최대값인 64,000에 도달하면 상태 경고를 보고합니다.)

표 ***245: Firepower Threat Defense*** 모델별 최대 동시 사용자 로그인 제한

FTD 모델	최대 동시 사용자 로그인 수
FTDv(지원되는 모든 하이퍼바이저)	64,000
ASA 5508-X, 5516-X	64,000
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 4110	64,000
Firepower 2140, 4112, 4115, 4120, 4125	150,000
Firepower 4140, 4145, 4150, 9300	300,000
ASA FirePOWER 서비스 모듈	2,000

표 ***246: Firepower Management Center*** 모델 [1] 최대 다운로드 사용자

FMC 모델	최대 다운로드 사용자
FMC1000	50,000
FMC1600	50,000
FMC2500	150,000
FMC2600	150,000
FMC4500	600,000
FMC4600	600,000
FMCv(지원되는 모든 하이퍼바이저)	50,000
FMC v300(지원되는 모든 하이퍼바이저)	150,000

[1] - FMC 모델은 단종 및 판매 중단될 수 있습니다. 자세한 내용은 단종 및 판매 종료 알림을 참조하십시오.

사용자 한도 도달 후 이전에 탐지하지 않은 새 사용자를 탐지하면, 시스템은 사용자 데이터의 ID 소스를 바탕으로 해당 데이터의 우선순위를 정합니다.

- 새 사용자를 신뢰할 수 없는 소스의 경우, 시스템은 권한 없는 사용자 데이터베이스에 추가 되지 않습니다. 새 사용자를 추가하려면, 사용자를 수동으로 삭제하거나 데이터베이스를 비워야 합니다.
- 새 사용자가 신뢰할 수 있는 ID 소스에서 왔다면, 시스템은 가장 오랫동안 비활성 상태인 신뢰할 수 없는 사용자를 삭제하고 신뢰할 수 있는 새 사용자를 데이터베이스에 추가합니다.

사용자 제어 문제 해결, 549 페이지에서 문제 해결 정보를 확인할 수 있습니다.

팁 트래픽 기반 탐지를 사용한다면, 프로토콜별로 사용자 기록을 제한해 불필요한 사용자 이름을 최소화하고 데이터베이스의 공간을 확보할 수 있습니다. 예를 들어 시스템이 AIM, POP3 및 IMAP 트래픽에서 발견한 사용자를 추가하지 못하게 할 수도 있습니다. 모니터링 대상이 아닌 계약자나 방문자가 보내는 트래픽임이 확실하기 때문입니다.

95 장

호스트 ID 소스

다음 주제는 호스트 ID 소스 관련 정보를 제공합니다.

- 개요: 호스트 데이터 수집, 2395 페이지
- 호스트 ID 소스 요구 사항 및 사전 요건, 2396 페이지
- 시스템에서 탐지할 수 있는 호스트 운영체제 결정, 2396 페이지
- 호스트 운영체제 식별, 2397 페이지
- 맞춤형 핑거프린팅, 2397 페이지
- 호스트 입력 데이터, 2406 페이지
- Nmap 스캐닝, 2414 페이지
- 호스트 ID 소스 기록, 2437 페이지

개요: 호스트 데이터 수집

Firepower System에서는 네트워크를 이동하는 트래픽을 수동으로 모니터링할 때 특정 패킷 헤더 값과 기타 네트워크 트래픽의 고유한 데이터를 설정된 정의(핑거프린트라고 함)와 비교하여 네트워크의 호스트에 대한 다음과 같은 정보를 확인합니다.

- 호스트의 수 및 유형(브리지, 라우터, 로드 밸런서 및 NAT 디바이스 같은 네트워크 디바이스 포함)
- 네트워크의 검색 지점에서 호스트로의 홉(hop) 수를 비롯한 기본 네트워크 토폴로지 데이터
- 호스트에서 실행 중인 운영체제
- 호스트의 애플리케이션 및 이러한 애플리케이션과 연결된 사용자

시스템이 호스트의 운영체제를 식별하지 못한다면, 맞춤형 클라이언트나 서버 핑거프린트를 만들 수 있습니다. 시스템은 이러한 핑거프린트를 사용하여 새 호스트를 식별합니다. 핑거프린트를 VDB(취약성 데이터베이스)의 시스템에 매핑하면 맞춤형 핑거프린트를 사용하여 호스트가 식별될 때마다 적절한 취약성 정보를 표시할 수 있습니다.

참고 모니터링하는 네트워크 트래픽에서 호스트 데이터를 수집하는 일 외에도, 시스템은 내보낸 NetFlow 기록에서 호스트 데이터를 수집할 수 있으며, 사용자는 Nmap 스캔과 호스트 입력 기능을 이용해 호스트 데이터를 능동적으로 추가할 수 있습니다.

호스트 ID 소스 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든, Leaf뿐인 사용자 지정 핑거 프린팅은 예외입니다.

사용자 역할

- 관리자
- 검색 관리자, 서드 파티 데이터 및 사용자 지정 매핑은 예외입니다.

시스템에서 탐지할 수 있는 호스트 운영체제 결정

핑거프린트할 수 있는 정확한 운영체제를 확인하려면, 맞춤형 OS 핑거프린트를 생성하는 중에 표시되는 사용 가능한 핑거프린트 목록을 확인하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** **Create Custom Fingerprint(**맞춤형 핑거프린트 만들기**)**를 클릭합니다.

단계 **4** **OS Vulnerability Mappings(**운영체제 취약성 매핑**)** 섹션의 드롭다운 목록에 표시되는 옵션 목록을 확인합니다. 이러한 옵션은 시스템이 핑거프린트할 수 있는 운영체제입니다.

다음에 수행할 작업

필요하다면 호스트 운영체제 식별, 2397 페이지 섹션을 참조하십시오.

호스트 운영체제 식별

시스템이 호스트의 운영체제를 올바르게 식별하지 못한다면(예를 들어 호스트 프로파일에서 "알 수 없음"으로 표시되거나 올바르게 식별되지 않는다면), 아래 방법을 시도해 보십시오.

프로시저

다음 방법 중 하나를 수행합니다.

- 네트워크 검색 ID 충돌 설정을 확인합니다.
- 호스트에 대한 맞춤형 핑거프린트를 만듭니다.
- 호스트에 대한 Nmap 스캔을 실행합니다.
- 호스트 입력 기능을 이용해 데이터를 네트워크로 가져옵니다.
- 수동으로 운영체제 정보를 입력합니다.

맞춤형 핑거프린팅

Firepower System에는 시스템이 탐지하는 각 호스트에서 운영체제를 식별하는 데 사용하는 운영체제 핑거프린트가 포함되어 있습니다. 그러나 운영체제와 일치하는 핑거프린트가 없기 때문에 시스템은 간혹 호스트 운영체제를 식별하지 못하거나 잘못 식별합니다. 이 문제를 바로잡으려면 알 수 없거나 잘못 식별된 운영체제에 고유한 운영체제 특성 패턴을 제공하는 맞춤형 핑거프린트를 생성하여, 식별 목적으로 운영체제의 이름을 제공해야 합니다.

시스템이 호스트의 운영체제를 확인할 수 없으면 호스트에 대한 취약성도 식별할 수 없습니다. 시스템은 각 호스트에 대한 취약성 목록을 운영체제 핑거프린트에서 가져오기 때문입니다. 예를 들어 Microsoft Windows를 실행하는 호스트를 탐지하는 경우 시스템은 탐지된 Windows 운영체제를 기반으로 해당 호스트에 대한 호스트 프로파일을 추가하는 저장된 Microsoft Windows 취약성 목록을 가지고 있습니다.

예를 들어 Microsoft Windows의 새 베타 버전을 실행하는 디바이스가 네트워크에 여러 개 있는 경우 시스템은 해당 운영체제를 식별하거나 호스트에 취약성을 매핑할 수 없습니다. 그러나 시스템에 Microsoft Windows에 대한 취약성 목록이 있음을 알고 있다면, 호스트 중 하나에 대한 맞춤형 핑거프린트를 생성해 동일한 운영체제를 실행하는 다른 호스트의 식별에 이를 활용할 수 있습니다. 핑거프린트에 Microsoft Windows에 대한 취약성 목록의 매핑을 포함하여, 해당 목록을 핑거프린트와 일치하는 각 호스트와 연결할 수 있습니다.

맞춤형 핑거프린트를 생성할 때, Firepower Management Center은(는) 동일한 운영체제를 실행하는 호스트의 해당 핑거프린트와 관련된 취약성 집합을 나열합니다. 생성한 맞춤형 핑거프린트에 취약성이 매핑되어 있지 않으면, 시스템은 핑거프린트를 사용하여 사용자가 핑거프린트에서 제공하는 맞춤형 운 체제 정보를 할당합니다. 이전에 탐지한 호스트에서 나오는 새 트래픽을 확인하면, 시스템은

새 핑거프린트 정보를 이용해 호스트를 업데이트합니다. 또한 시스템은 새 핑거프린트를 이용해 새로운 호스트와 호스트를 처음으로 탐지했을 때의 운영체제를 식별합니다.

맞춤형 핑거프린트를 만들기 전에, 호스트가 올바르게 식별되지 않는 이유를 파악하여 맞춤형 핑거프린트가 실용적인 해결책인지 결정해야 합니다.

시스템에서 두 가지 유형의 핑거프린트를 생성할 수 있습니다.

- 클라이언트 핑거프린트 - 호스트가 네트워크의 다른 호스트에서 실행 중인 TCP 애플리케이션에 연결될 때 전송하는 SYN 패킷을 기반으로 운영체제를 식별합니다.
- 서버 핑거프린트 - 실행 중인 TCP 애플리케이션에 대한 수신 연결에 응답하기 위해 호스트가 사용하는 SYN-ACK 패킷을 기반으로 운영체제를 식별합니다.

참고 클라이언트 및 서버 핑거프린트가 동일한 호스트와 일치한다면 클라이언트 핑거프린트를 사용합니다.

핑거프린트를 생성한 후에는 활성화해야 시스템이 해당 핑거프린트를 호스트와 연결할 수 있습니다.

관련 항목

클라이언트에 대한 맞춤형 핑거프린트 생성, 2401 페이지
서버에 대한 맞춤형 핑거프린트 생성, 2403 페이지

핑거프린트 관리

핑거프린트를 생성 및 활성화한 후에는 원하는 대로 내용을 수정하거나 취약성 매핑을 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다. 핑거프린트 생성을 위해 데이터를 기다리는 시스템은 핑거프린트가 생성될 때까지 10초마다 페이지를 자동으로 새로 고칩니다.

단계 **3** 맞춤형 핑거프린트를 관리합니다.

- 활성화/비활성화 - 핑거프린트 활성화 및 비활성화, 2399 페이지에 설명된 대로 핑거프린트를 활성화하거나 비활성화합니다.
- 생성 - 클라이언트에 대한 맞춤형 핑거프린트 생성, 2401 페이지 및 서버에 대한 맞춤형 핑거프린트 생성, 2403 페이지에 설명된 대로 핑거프린트를 생성합니다.
- 편집 - 활성 핑거프린트 편집, 2399 페이지 및 비활성 핑거프린트 편집, 2400 페이지에 설명된 대로 핑거프린트를 편집합니다.

- 삭제 - 삭제할 핑거프린트 옆에 있는 삭제( )을 클릭하고 **OK(**확인**)**를 눌러 확인합니다. 비활성화된 지문만 삭제할 수 있습니다.

핑거프린트 활성화 및 비활성화

맞춤형 핑거프린트는 반드시 활성화해야 시스템에서 이를 사용하여 호스트를 식별할 수 있습니다. 새 핑거프린트가 활성화되면 시스템은 이전에 검색된 호스트를 새 핑거프린트를 이용해 다시 식별하고 새 호스트를 검색합니다.

핑거프린트 사용을 중지하고 싶다면 먼저 비활성화해야 합니다. 핑거프린트를 비활성화하면 사용은 중지되지만 시스템에서 삭제되지는 않습니다. 핑거프린트를 비활성화하면 운영체제는 핑거프린트를 사용하는 호스트에 대해 unknown(알 수 없음)으로 표시됩니다. 호스트가 다시 탐지되고 다른 활성 핑거프린트와 일치한다면, 호스트는 해당 활성 핑거프린트로 식별됩니다.

핑거프린트를 삭제하면 시스템에서 완전히 제거됩니다. 비활성화한 핑거프린트는 삭제할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** 활성화하거나 비활성화할 핑거프린트 옆에 있는 슬라이더를 클릭합니다.

참고 생성한 핑거프린트가 유효한 경우에만 활성화 옵션을 사용할 수 있습니다. 슬라이더를 사용할 수 없다면 핑거프린트를 다시 생성해 보십시오.

활성 핑거프린트 편집

핑거프린트가 활성 상태이면 핑거프린트 이름, 설명, 맞춤형 운영체제 표시 등을 수정하고 추가 취약성을 매핑할 수 있습니다.

핑거프린트 이름, 설명, 맞춤형 운영체제 표시 등을 수정하고 추가 취약성을 매핑할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** 맞춤형 운영체제를 클릭합니다.

단계 **3** 편집할 핑거프린트 옆에 있는 수정( )을 클릭합니다.

단계 **4** 필요하다면 핑거프린트 이름, 설명 및 맞춤형 OS 표시를 수정합니다.

단계 **5** 취약성 매핑을 삭제하려면 페이지의 **Pre-Defined OS Product Maps(**사전 정의된 운영체제 제품 맵**)** 섹션에서 매핑 옆에 있는 **Delete(**삭제**)**를 클릭합니다.

단계 **6** 취약성 매핑에 대한 운영체제를 더 추가하려면 **Product(**제품**)**를 선택하고, 해당하는 경우 **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)**, **Extension(**확장**)**을 선택한 다음 **Add OS Definition(**운영체제 정의 추가**)**를 클릭합니다.

취약성 매핑이 **Pre-Defined OS Product Maps(**사전 정의된 운영체제 제품 맵**)** 목록에 추가됩니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

비활성 핑거프린트 편집

핑거프린트가 비활성 상태이면 핑거프린트의 모든 요소를 수정한 후 Firepower Management Center에 다시 제출할 수 있습니다. 여기에는 핑거프린트 유형, 목적지 IP 주소와 포트, 취약성 매핑 등 핑거프린트 생성 시 지정한 모든 속성이 포함됩니다. 비활성 핑거프린트를 편집하고 다시 제출하면 시스템에 다시 제출되며, 클라이언트 핑거프린트인 경우 활성화하기 전에 어플라이언스에 트래픽을 다시 전송해야 합니다. 비활성 핑거프린트에 대해서는 단일 취약성 매핑만 선택할 수 있습니다. 핑거프린트를 활성화한 후 추가 운영체제 및 버전을 취약성 목록에 매핑할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** 편집할 핑거프린트 옆에 있는 수정( )을 클릭합니다.

단계 **4** 필요한 대로 핑거프린트를 수정합니다.

- 클라이언트 핑거프린트를 수정하는 경우에는 클라이언트에 대한 맞춤형 핑거프린트 생성, 2401 페이지 섹션을 참조하십시오.
- 서버 핑거프린트를 수정하는 경우에는 서버에 대한 맞춤형 핑거프린트 생성, 2403 페이지 섹션을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 클라이언트 핑거프린트를 수정한 경우 호스트에서 (핑거프린트를 수집하는) 어플라이언스로 트래픽을 전송해야 합니다.

클라이언트에 대한 맞춤형 핑거프린트 생성

클라이언트 핑거프린트는 호스트가 네트워크의 다른 호스트에서 실행 중인 TCP 애플리케이션에 연결될 때 전송하는 SYN 패킷을 기반으로 운영체제를 식별합니다.

Firepower Management Center이(가) 모니터링되는 호스트와 직접 연결되지 않은 경우, FMC가 관리하며 클라이언트 핑거프린트 속성을 지정할 때 핑거프린트 처리할 호스트와 가장 가까운 디바이스를 지정할 수 있습니다.

핑거프린트 처리를 시작하기 전에 핑거프린트 처리할 호스트에 대한 다음 정보를 확인하십시오.

- 호스트 또는 Firepower Management Center을(를) 가져오기 위해 사용할 디바이스 간 네트워크 홉의 수 (Cisco는 Firepower Management Center 또는 디바이스를 호스트가 연결된 것과 동일한 서브넷에 연결할 것을 적극 권장합니다.)
- 호스트가 상주하는 네트워크에 연결된 네트워크 인터페이스(Firepower Management Center 또는 디바이스)
- 호스트의 실제 운영체제 벤더, 제품 및 버전
- 클라이언트 트래픽을 생성하기 위해 호스트에 액세스

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** **Create Custom Fingerprint(**맞춤형 핑거프린트 만들기**)**를 클릭합니다.

단계 **4** **Device(**디바이스**)** 드롭다운 목록에서 핑거프린트 수집에 사용할 Firepower Management Center 또는 디바이스를 선택합니다.

단계 **5** **Fingerprint Name(**핑거프린트 이름**)**을 입력합니다.

단계 **6** **Fingerprint Description(**핑거프린트 설명**)**을 입력합니다.

단계 **7** **Fingerprint Type(**핑거프린트 유형**)** 목록에서 **Client(**클라이언트**)**를 선택합니다.

단계 **8** **Target IP Address(**목적지 **IP** 주소**)** 필드에 핑거프린트 처리할 호스트의 IP 주소를 입력합니다.

핑거프린트는 (호스트의 다른 IP 주소가 아닌) 사용자가 지정하는 호스트 IP 주소를 통과하는 트래픽만을 기반으로 합니다.

단계 **9** 핑거프린트를 수집하기 위해 선택했던 디바이스와 호스트 간 네트워크 홉의 수를 **Target Distance(**대상 거리**)** 필드에 입력합니다.

주의 이 값은 호스트에 대한 물리적 네트워크 홉의 실제 숫자여야 하며, 시스템에 의해 탐지된 홉의 수와 같을 수도 있고 다를 수도 있습니다.

단계 **10** 호스트가 상주하는 네트워크 세그먼트에 연결된 네트워크 인터페이스를 **Interface(**인터페이스**)** 목록에서 선택합니다.

주의 여러 가지 이유로, Cisco는 매니지드 디바이스의 센싱 인터페이스를 핑거프린트에 사용하지 않을 것을 권장합니다. 첫째, 센싱 인터페이스가 span 포트에 있으면 핑거프린트가 작동하지 않습니다. 또한 디바이스에서 센싱 인터페이스를 사용하면 디바이스는 핑거프린트를 수집하는 데 걸리는 시간 동안 네트워크의 모니터링이 중단됩니다. 하지만 관리 인터페이스 또는 기타 사용 가능한 네트워크 인터페이스를 이용하면 핑거프린트 수집을 수행할 수 있습니다. 디바이스에서 어떤 인터페이스가 센싱 인터페이스인지 모르는 경우, 핑거프린트 처리에 사용 중인 특정 모델의 *Installation Guide(*설치 안내서*)*를 참조하십시오.

단계 **11** 핑거프린트 처리된 호스트에 대한 호스트 프로파일에 맞춤형 정보를 표시하려면(또는 핑거프린트 처리할 호스트가 **OS Vulnerability Mappings(**운영체제 취약성 매핑**)** 섹션에 상주하지 않는 경우), **Use Custom OS Display(**맞춤형 운영체제 표시 사용**)**를 선택하고 다음에 대해 호스트 프로파일에 표시할 값을 제공합니다.

- **Vendor String** 필드에 운영체제의 벤더 이름을 입력합니다. 예를 들어 Microsoft Windows의 벤더는 Microsoft입니다.
- **Product String** 필드에 운영체제의 제품 이름을 입력합니다. 예를 들어 Microsoft Windows 2000의 제품 이름은 Windows입니다.
- **Version String** 필드에 운영체제의 버전 번호를 입력합니다. 예를 들어 Microsoft Windows 2000의 버전 번호는 2000입니다.

단계 **12** OS Vulnerability Mappings섹션에서 취약성 매핑에 사용할 운영 체제, 제품 및 버전을 선택합니다.

핑거프린트를 사용하여 매칭 호스트에 대한 취약성을 식별하려는 경우 또는 맞춤형 운영체제 표시 정보를 할당하지 않은 경우 이 섹션에서 **Vendor(**벤더**)** 및 **Product(**제품**)** 값을 지정해야 합니다.

운영체제의 모든 버전에 대해 취약성을 매핑하려면 **Vendor(**벤더**)** 및 **Product(**제품**)** 값만 지정하십시오.

참고 선택한 운영체제에 **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록의 옵션이 모두 적용되지는 않을 수도 있습니다. 또한 핑거프린트 처리하려는 운영체제와 일치하는 정의가 목록에 나타나지 않으면 해당 값을 비워둘 수도 있습니다. 핑거프린트에서 OS 취약성 매핑을 생성하지 않으면 시스템은 핑거프린트에 의해 식별되는 호스트가 포함된 취약성 목록을 할당하는 데 핑거프린트를 사용할 수 없습니다.

예제**:**

예를 들어 맞춤형 핑거프린트를 통해 Redhat Linux 9의 취약성 목록을 매칭 호스트에 할당하려면 벤더로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 주 버전으로 **9**를 선택합니다.

예제**:**

Palm OS의 모든 버전을 추가하려면 **Vendor(**벤더**)** 목록에서 **PalmSource, Inc.**, **Product(**제품**)** 목록에서 **Palm OS**를 선택하고 다른 모든 목록은 기본 설정으로 두십시오.

단계 **13** **Create(**생성**)**를 클릭합니다.

상태에서 New(신규)가 잠시 표시된 후 Pending(대기 중)으로 변경되며, 핑거프린트가 트래픽을 확인할 때까지는 계속 대기 중으로 표시됩니다. 트래픽이 확인되면 상태는 Ready(준비)로 변경됩니다.

Custom Fingerprint(맞춤형 핑거프린트) 상태 페이지는 문제의 호스트에서 데이터를 수신할 때까지 10초마다 갱신합니다.

단계 **14** 목적지 IP 주소로 지정된 IP 주소를 사용하여, 핑거프린트 처리하려는 호스트에 액세스하고 어플라이언스에 대한 TCP 연결을 시작합니다.

정확한 핑거프린트를 생성하려면 핑거프린트를 수집하는 어플라이언스에 트래픽이 표시되어야 합니다. 스위치를 통해 연결된 경우 어플라이언스 외의 시스템에 대한 트래픽은 시스템에 표시되지 않을 수 있습니다.

예제:

예를 들어 핑거프린트 처리할 호스트에서 Firepower Management Center의 웹 인터페이스에 액세스하거나 호스트에서 FMC의 SSH에 액세스합니다. SSH를 사용한다면 아래 명령을 사용하십시오. 여기서 localIPv6address는 7단계에서 지정되었고 현재 호스트에 할당된 IPv6 주소이며, DCmanagementIPv6address는 FMC의 관리 IPv6 주소입니다. Custom Fingerprint(맞춤형 핑거프린트) 페이지가 다시 로드되어 "Ready(준비)" 상태가 됩니다.

```
ssh -b localIPv6address DCmanagementIPv6address
```

다음에 수행할 작업

- 핑거프린트 활성화 및 비활성화, 2399 페이지에 설명된 대로 핑거프린트를 활성화합니다.

서버에 대한 맞춤형 핑거프린트 생성

서버 핑거프린트는 실행 중인 TCP 애플리케이션에 대한 수신 연결에 응답하기 위해 호스트가 사용하는 SYN-ACK 패킷을 기반으로 운영체제를 식별합니다. 시작하기 전에 핑거프린트 처리할 호스트에 대한 다음 정보를 확인하십시오.

- 호스트와 핑거프린트를 가져오기 위해 사용할 어플라이언스 간 네트워크 홉의 수 Cisco는 어플라이언스의 미사용 인터페이스를 호스트가 연결된 것과 동일한 서브넷에 연결할 것을 적극 권장합니다.
- 호스트가 상주하는 네트워크에 연결된 (어플라이언스 상의) 네트워크 인터페이스
- 호스트의 실제 운영체제 공급업체, 제품 및 버전
- 현재 사용되고 있지 않으며 호스트가 있는 네트워크에서 인증된 IP 주소

팁 Firepower Management Center이(가) 모니터링되는 호스트와 직접 연결되지 않은 경우 서버 핑거프린트 속성을 지정할 때 핑거프린트 처리할 호스트와 가장 가까운 매니지드 디바이스를 지정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** **Create Custom Fingerprint(**맞춤형 핑거프린트 만들기**)**를 클릭합니다.

단계 **4** **Device(**디바이스**)** 목록에서 핑거프린트 수집에 사용할 Firepower Management Center 또는 매니지드 디바이스를 선택합니다.

단계 **5** **Fingerprint Name(**핑거프린트 이름**)**을 입력합니다.

단계 **6** **Fingerprint Description(**핑거프린트 설명**)**을 입력합니다.

단계 **7** **Fingerprint Type(**핑거프린트 유형**)** 목록에서 **Server(**서버**)**를 선택해 서버 핑거프린트 옵션을 표시합니다.

단계 **8** **Target IP Address(**목적지 **IP** 주소**)** 필드에 핑거프린트 처리할 호스트의 IP 주소를 입력합니다.

핑거프린트는 (호스트의 다른 IP 주소가 아닌) 사용자가 지정하는 호스트 IP 주소를 통과하는 트래픽만을 기반으로 합니다.

주의 Firepower System 버전 5.2 이상을 실행하는 어플라이언스에서만 IPv6 핑거프린트를 캡처할 수 있습니다.

단계 **9** 핑거프린트를 수집하기 위해 선택했던 디바이스와 호스트 간 네트워크 홉의 수를 **Target Distance(**대상 거리**)** 필드에 입력합니다.

주의 이 값은 호스트에 대한 물리적 네트워크 홉의 실제 숫자여야 하며, 시스템에 의해 탐지된 홉의 수와 같을 수도 있고 다를 수도 있습니다.

단계 **10** 호스트가 상주하는 네트워크 세그먼트에 연결된 네트워크 인터페이스를 **Interface(**인터페이스**)** 목록에서 선택합니다.

주의 여러 가지 이유로, Cisco는 매니지드 디바이스의 센싱 인터페이스를 핑거프린트에 사용하지 않을 것을 권장합니다. 첫째, 센싱 인터페이스가 span 포트에 있으면 핑거프린트가 작동하지 않습니다. 또한 디바이스에서 센싱 인터페이스를 사용하면 디바이스는 핑거프린트를 수집하는 데 걸리는 시간 동안 네트워크의 모니터링이 중단됩니다. 하지만 관리 인터페이스 또는 기타 사용 가능한 네트워크 인터페이스를 이용하면 핑거프린트 수집을 수행할 수 있습니다. 디바이스에서 어떤 인터페이스가 센싱 인터페이스인지 모르는 경우, 핑거프린트 처리에 사용 중인 특정 모델의 *Installation Guide(*설치 안내서*)*를 참조하십시오.

단계 **11** **Get Active Ports(**활성 포트 얻기**)**를 클릭합니다.

단계 **12** 핑거프린트를 수집하기 위해 선택한 디바이스가 연결을 시작하도록 할 포트를 **Server Port(**서버 포트**)** 필드에 입력하거나, **Get Active Ports(**활성 포트 얻기**)** 드롭다운 목록에서 포트를 선택합니다.

호스트에 대해 열려 있음을 확인한 서버 포트라면 무엇이든 사용할 수 있습니다(예: 호스트가 웹 서버를 실행 중인 경우 80).

단계 **13** 호스트와의 통신을 시도하기 위해 사용할 IP 주소를 **Source IP Address(**소스 **IP** 주소**)** 필드에 입력합니다.

네트워크에서 사용하도록 인증되었지만 현재 사용되고 있지 않은 소스 IP 주소(예: 현재 사용되고 있지 않은 DHCP 풀 주소)를 사용해야 합니다. 이렇게 하면 핑거프린트를 생성하는 동안 일시적으로 다른 호스트를 오프라인으로 탐색하지 않아도 됩니다.

핑거프린트를 생성하는 동안에는 네트워크 검색 정책에서 해당 IP 주소의 모니터링을 제외해야 합니다. 이렇게 하지 않으면 네트워크 맵 및 검색 이벤트 보기가 해당 IP 주소로 표시되는 호스트에 대한 부정확한 정보와 뒤섞이게 됩니다.

단계 **14** **Source Subnet Mask(**소스 서브넷 마스크**)** 필드에 사용 중인 IP 주소의 서브넷 마스크를 입력합니다.

단계 **15** **Source Gateway(**소스 게이트웨이**)** 필드가 나타나면 호스트에 대한 경로를 설정하기 위해 사용해야 할 기본 게이트웨이 IP 주소를 입력합니다.

단계 **16** 핑거프린트 처리된 호스트에 대한 호스트 프로파일에 맞춤형 정보를 표시하려면 또는 사용하려는 핑거프린트 이름이 OS Definition(운영체제 정의) 섹션에 없다면 Custom OS Display(맞춤형 운영체제 표시) 섹션에서 **Use Custom OS Display(**맞춤형 운영체제 표시 사용**)**를 선택합니다.

호스트 프로파일에 표시할 다음에 대한 값을 제공합니다.

- **Vendor String** 필드에 운영체제의 벤더 이름을 입력합니다. 예를 들어 Microsoft Windows의 벤더는 Microsoft입니다.
- **Product String** 필드에 운영체제의 제품 이름을 입력합니다. 예를 들어 Microsoft Windows 2000의 제품 이름은 Windows입니다.
- **Version String** 필드에 운영체제의 버전 번호를 입력합니다. 예를 들어 Microsoft Windows 2000의 버전 번호는 2000입니다.

단계 **17** OS Vulnerability Mappings섹션에서 취약성 매핑에 사용할 운영 체제, 제품 및 버전을 선택합니다.

핑거프린트를 사용하여 매칭 호스트에 대한 취약성을 식별하려는 경우 또는 맞춤형 운영체제 표시 정보를 할당하지 않은 경우 이 섹션에서 Vendor(벤더) 및 Product(제품) 이름을 지정해야 합니다.

운영체제의 모든 버전에 대해 취약성을 매핑하려면 벤더 및 제품 이름만 지정하십시오.

참고 선택한 운영체제에 **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록의 옵션이 모두 적용되지는 않을 수도 있습니다. 또한 핑거프린트 처리하려는 운영체제와 일치하는 정의가 목록에 나타나지 않으면 해당 값을 비워둘 수도 있습니다. 핑거프린트에서 OS 취약성 매핑을 생성하지 않으면 시스템은 핑거프린트에 의해 식별되는 호스트가 포함된 취약성 목록을 할당하는 데 핑거프린트를 사용할 수 없습니다.

예제**:**

예를 들어 맞춤형 핑거프린트를 통해 Redhat Linux 9의 취약성 목록을 매칭 호스트에 할당하려면 벤더로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

예제**:**

Palm OS의 모든 버전을 추가하려면 **Vendor(**벤더**)** 목록에서 **PalmSource, Inc.**, **Product(**제품**)** 목록에서 **Palm OS**를 선택하고 다른 모든 목록은 기본 설정으로 두십시오.

단계 **18** **Create(**생성**)**를 클릭합니다.
Custom Fingerprint(맞춤형 핑거프린트) 상태 페이지는 10초마다 갱신되며 "Ready(준비)" 상태로 다시 로드되어야 합니다.

참고 핑거프린트 처리 중에 대상 시스템이 응답을 중지하면 상태에 `ERROR: No Response` 메시지가 나타납니다. 이 메시지가 표시된다면 핑거프린트를 다시 제출하십시오. 3~5분 정도 기다렸다가(시간은 대상 시스템에 따라 달라질 수 있음) 수정( )을 클릭하여 Custom Fingerprint(맞춤형 핑거프린트) 페이지에 액세스한 다음 **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- 핑거프린트 활성화 및 비활성화, 2399 페이지에 설명된 대로 핑거프린트를 활성화합니다.

호스트 입력 데이터

서드파티의 네트워크 맵 데이터를 가져와 네트워크 맵을 보강할 수도 있습니다. 또한 운영체제나 애플리케이션 ID를 수정하여 또는 애플리케이션 프로토콜, 프로토콜, 호스트 속성, 웹 인터페이스를 사용하는 클라이언트 등을 삭제하여 호스트 입력 기능을 사용할 수 있습니다.

시스템에서는 운영체제 또는 애플리케이션의 현재 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

영향받는 호스트가 네트워크 맵에서 제거되면 서드파티 취약성을 제외한 모든 데이터가 폐기됩니다. 스크립트 설정 또는 파일 가져오기에 대한 자세한 내용은 *Firepower System Host Input API* 설명서 섹션을 참조하십시오.

가져온 데이터를 영향 상관관계에 포함하려면 데이터를 데이터베이스의 운영체제 및 애플리케이션 정의에 매핑해야 합니다.

서드파티 데이터 사용 요구 사항

서드파티 시스템의 검색 데이터를 자신의 네트워크로 가져올 수 있습니다. 하지만 Firepower 권장사항, 적응형 프로파일 또는 영향 평가처럼 침입 및 검색 데이터를 함께 사용하는 기능을 활성화하려면, 최대한 많은 요소를 대응하는 정의에 매핑해야 합니다. 서드파티 데이터 사용을 위한 다음 요구 사항을 고려해 보십시오.

- 네트워크 자산에 대한 특정 데이터가 포함된 서드파티 시스템이 있는 경우 호스트 입력 기능을 사용하여 해당 데이터를 가져올 수 있습니다. 그러나 서드파티에서 제품 이름을 다르게 지정할 수 있으므로 서드파티 벤더, 제품 및 버전을 해당 Cicso 제품 정의에 매핑해야 합니다. 제품을 매핑한 후에는 영향 상관관계를 허용하기 위해 Firepower Management Center 설정에서 영향 평가를 위한 취약성 매핑을 활성화해야 합니다. 버전 또는 벤더가 없는 애플리케이션 프로토콜의 경우 Firepower Management Center 설정에서 애플리케이션 프로토콜에 대한 취약성을 매핑해야 합니다.

- 서드파티에서 패치 정보를 가져오고 해당 패치에 의해 수정된 모든 취약성을 무효 상태로 표시하려면 서드파티 수정 이름을 데이터베이스의 수정 정의에 매핑해야 합니다. 그러면 수정에 의해 해결된 모든 취약성이 해당 수정을 추가한 호스트에서 제거됩니다.
- 서드파티에서 운영체제 및 애플리케이션 프로토콜 취약성을 가져와서 영향 상관관계에 사용하려면 서드파티 취약성 식별 문자열을 데이터베이스의 취약성에 매핑해야 합니다. 관련된 취약성이 있는 클라이언트가 많고 영향 평가에 클라이언트가 사용되지만, 서드파티 클라이언트 취약성을 가져와서 매핑할 수는 없습니다. 취약성을 매핑한 후에는 Firepower Management Center 설정에서 영향 평가를 위한 서드파티 취약성 매핑을 활성화해야 합니다. 벤더 또는 버전 정보가 없는 애플리케이션 프로토콜을 취약성에 매핑하려면 관리 사용자는 Firepower Management Center 설정에서 애플리케이션에 대한 취약성을 매핑해야 합니다.
- 애플리케이션 데이터를 가져와 영향 상관관계에 사용하려는 경우 각 애플리케이션 프로토콜에 대한 벤더 문자열을 해당 Cisco 애플리케이션 프로토콜 정의에 매핑해야 합니다.

관련 항목

서드파티 제품 매핑, 2407 페이지
서드파티 제품 수정 매핑, 2409 페이지
서드파티 취약성 매핑, 2410 페이지
서버의 취약성 매핑, 1389 페이지
맞춤형 제품 매핑 생성, 2411 페이지

서드파티 제품 매핑

사용자 입력 기능을 통해 서드파티의 데이터를 네트워크 맵에 추가할 때에는 서드파티에서 사용하는 공급업체, 제품 및 버전 이름을 Cisco 제품 정의에 매핑해야 합니다. 제품을 Cisco 정의에 매핑하면 이러한 정의에 따라 취약성이 할당됩니다.

마찬가지로 서드파티에서 패치 정보(예: 패치 관리 제품)를 가져오는 경우, 수정의 이름을 데이터베이스의 적절한 공급업체와 제품 그리고 해당 수정에 매핑해야 합니다.

서드파티 제품 매핑

서드파티의 데이터를 가져오는 경우 취약성을 할당하고 해당 데이터로 영향 상관관계를 수행하려면 Cisco 제품을 서드파티 이름에 매핑해야 합니다. 제품을 매핑하면 Cisco 취약성 정보가 서드파티 제품 이름과 연결되며, 이를 통해 시스템에서는 해당 데이터를 사용해 영향 상관관계를 수행할 수 있습니다.

호스트 입력 가져오기 기능을 사용하여 데이터를 가져올 경우 AddScanResult 기능을 사용하여 가져오는 동안 서드파티 제품을 운영체제 및 애플리케이션 취약성에 매핑해야 합니다.

예를 들어 Apache Tomcat을 애플리케이션으로 나열하는 서드파티의 데이터를 가져오며 해당 제품의 버전이 6임을 안다면, 다음 조건 하에 서드파티 맵을 추가할 수 있습니다.

- **Vendor Name(**벤더 이름**)**을 `Apache`로 설정합니다.
- **Product Name(**제품 이름**)**을 `Tomcat`으로 설정합니다.
- **Apache**를 **Vendor(**벤더**)** 드롭다운 목록에서 선택합니다.

- **Tomcat**을 **Product(**제품**)** 드롭다운 목록에서 선택합니다.
- **6**를 **Version(**버전**)** 드롭다운 목록에서 선택합니다.

이렇게 매핑하면 Apache Tomcat 6에 대한 취약성이 Apache Tomcat에 대한 애플리케이션 목록과 함께 호스트에 할당됩니다.

버전 또는 벤더가 없는 애플리케이션의 경우 Firepower Management Center 설정에서 애플리케이션 유형에 대한 취약성을 매핑해야 합니다. 관련된 취약성이 있는 클라이언트가 많고 영향 평가에 클라이언트를 사용했지만, 서드파티 클라이언트 취약성을 가져와서 매핑할 수는 없습니다.

팁 또 다른 Firepower Management Center에서 이미 서드파티 매핑을 생성한 경우 이를 내보낸 다음 이 FMC로 가져올 수 있습니다. 그런 다음 가져온 매핑을 필요에 맞게 수정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **User Third-Party Mappings(**사용자 서드파티 매핑**)**을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 새 맵 집합을 생성하려면 **Create Product Map Set(**제품 맵 집합 생성**)**를 클릭합니다.
- 편집 - 기존 맵 집합을 편집하려면 수정할 맵 집합 옆에 있는 수정( )을 클릭합니다. 보기 ( ) 이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** **Mapping Set Name(**집합 이름 매핑**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 서드파티 제품을 매핑하려면 **Add Product Map(**제품 맵 추가**)**을 클릭합니다.
- 편집 - 기존 서드파티 제품 맵을 편집하려면 수정할 맵 집합 옆에 있는 수정( )을 클릭합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **7** 서드파티 제품이 사용하는 **Vendor String**을 입력합니다.

단계 **8** 서드파티 제품이 사용하는 **Product String**을 입력합니다.

단계 **9** 서드파티 제품이 사용하는 **Version String**을 입력합니다.

단계 **10** Product Mappings(제품 매핑) 섹션에서 **Vendor(**벤더**)**, **Product(**제품**)**, **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)**, **Extension(**확장**)** 필드의 취약성 매핑에 사용할 운영체제, 제품, 버전을 선택합니다.

예제**:**

서드파티 문자열로 이름이 구성된 제품을 실행 중인 호스트에서 Redhat Linux 9의 취약성을 사용하도록 하려면 벤더로 **Redhat, Inc.,** 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

관련 항목

서버의 취약성 매핑, 1389 페이지

서드파티 제품 수정 매핑

수정 이름을 데이터베이스에 있는 특별한 수정 집합에 매핑하면, 서드파티 패치 관리 애플리케이션에서 데이터를 가져와 호스트 집합에 수정을 적용할 수 있습니다. 수정 이름을 호스트로 가져오면 시스템은 해당 수정으로 해결된 모든 취약성을 해당 호스트에 대해 무효 상태로 표시합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **User Third-Party Mappings(**사용자 서드파티 매핑**)**을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 새 맵 집합을 생성하려면 **Create Product Map Set(**제품 맵 집합 생성**)**를 클릭합니다.
- 편집 - 기존 맵 집합을 편집하려면 수정할 맵 집합 옆에 있는 수정( )을 클릭합니다. 보기 ( ) 이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** **Mapping Set Name(**집합 이름 매핑**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 서드파티 제품을 매핑하려면 **Add Fix Map(**수정 맵 추가**)**을 클릭합니다.
- 편집 - 기존 서드파티 제품 맵을 편집하려면 옆에 있는 수정( )을 클릭합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **7** 매핑할 수정의 이름을 **Third-Party Fix Name(**서드파티 수정 이름**)** 필드에 입력합니다.

단계 **8** **Product Mappings(**제품 매핑**)** 섹션에서, 수정 매핑에 사용할 운영체제, 제품 및 버전을 다음 표에서 선택합니다.

- **Vendor(**벤더**)**
- 제품
- 주 버전
- 부 버전
- 개정 버전
- 구축
- 패치
- 확장

예제:

매핑을 통해 Redhat Linux 9의 수정을 패치가 적용되는 호스트에 할당하려면 벤더로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**을 선택합니다.

단계 **9** **Save(**저장**)**를 클릭하여 수정 맵을 저장합니다.

서드파티 취약성 매핑

서드파티의 취약성 정보를 VDB에 추가하려면 가져온 각 취약성에 대한 서드파티 식별 문자열을 기존 SVID, Bugtraq 또는 SID에 매핑해야 합니다. 취약성에 대한 매핑을 생성하면 네트워크 맵에서 호스트로 가져온 모든 취약성에 대해 매핑이 제대로 작동하며, 그러한 취약성에 대해 영향 상관관계를 수행할 수 있게 됩니다.

상관관계가 발생하도록 하려면 서드파티 취약성에 대한 영향 상관관계를 활성화해야 합니다. 버전 또는 벤더가 없는 애플리케이션의 경우 Firepower Management Center 설정에서 애플리케이션 유형에 대한 취약성을 매핑해야 합니다.

관련된 취약성이 있는 클라이언트가 많고 영향 분석에 클라이언트가 사용되지만, 영향 평가에는 서드파티 클라이언트 취약성을 사용할 수 없습니다.

팁 또 다른 Firepower Management Center에서 이미 서드파티 매핑을 생성한 경우 이를 내보낸 다음 이 FMC로 가져올 수 있습니다. 그런 다음 가져온 매핑을 필요에 맞게 수정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **User Third-Party Mappings(**사용자 서드파티 매핑**)**을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 새로운 취약성 집합을 생성하려면 **Create Vulnerability Map Set(**취약성 맵 집합 생성**)**를 클릭합니다.
- 편집 - 기존 취약성 집합을 수정하려면 취약성 집합 옆에 있는 수정( )을 클릭합니다. 보기 ( ) 이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** **Add Vulnerability Map(**취약성 맵 추가**)**을 클릭합니다.

단계 **5** **Vulnerability ID(**취약성 **ID)** 필드에 취약성에 대한 서드파티 ID를 입력합니다.

단계 **6** **Vulnerability Description(**취약성 설명**)**을 입력합니다.

단계 **7** 선택 사항:

- **Snort Vulnerability ID Mappings(Snort** 취약성 **ID** 매핑**)** 필드에 Snort ID을(를) 입력합니다.
- **SVID Mappings(SVID** 매핑**)** 필드에 레거시 취약성 ID를 입력합니다.
- **Bugtraq Vulnerability ID Mappings(Bugtraq** 취약성 **ID** 매핑**)** 필드에 Bugtraq 식별 번호를 입력합니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

관련 항목

네트워크 검색 취약성 영향 평가 활성화, 2554 페이지
서버의 취약성 매핑, 1389 페이지

맞춤형 제품 매핑

제품 매핑을 사용해 서드파티에 의한 서버 입력이 적절한 Cisco 정의와 연결되었는지 확인할 수 있습니다. 제품 매핑을 정의 및 활성화하면, 매핑된 벤더 문자열이 있는 모니터링되는 호스트의 모든 서버 또는 클라이언트는 맞춤형 제품 매핑을 사용합니다. 따라서 서버의 벤더, 제품 및 버전을 명시적으로 설정하는 대신 특정 벤더 문자열로 네트워크 맵에 있는 모든 서버에 대해 취약성을 매핑할 수도 있습니다.

맞춤형 제품 매핑 생성

시스템이 서버를 VDB의 벤더나 제품에 매핑하지 못한다면, 수동으로 매핑을 생성할 수 있습니다. 맞춤형 제품 매핑을 활성화하면 시스템은 지정한 벤더 및 제품에 대한 취약성을, 해당 벤더 문자열이 발생하는 네트워크 맵의 모든 서버에 매핑합니다.

참고 맞춤형 제품 매핑은 애플리케이션 데이터의 소스(예: Nmap, 호스트 입력 기능 또는 Firepower System 자체)와 상관없이 애플리케이션 프로토콜의 모든 경우에 적용됩니다. 그러나 호스트 입력 기능을 사용하여 가져온 데이터에 대한 서드파티 취약성 매핑이 맞춤형 제품 매핑을 통해 설정한 매핑과 충돌하면, 서드파티 취약성 매핑은 맞춤형 제품 매핑을 재정의하며 입력이 발생할 경우 서드파티 취약성 매핑 설정을 사용합니다.

제품 매핑의 목록을 생성한 다음, 각 목록을 활성화 또는 비활성화하여 여러 매핑의 사용을 동시에 활성화 또는 비활성화할 수 있습니다. 매핑할 벤더를 지정하면 시스템은 해당 벤더의 제품만 포함하도록 제품 목록을 업데이트합니다.

맞춤형 제품 매핑을 생성한 후에는 맞춤형 제품 매핑 목록을 활성화해야 합니다. 맞춤형 제품 매핑의 목록을 활성화하면, 시스템은 지정된 벤더 문자열이 발생할 때 모든 서버를 업데이트합니다. 호스트 입력 기능을 통해 가져온 데이터의 경우, 이 서버에 대해 제품 매핑을 이미 명시적으로 설정하지 않았다면 취약성이 업데이트됩니다.

예를 들어 회사에서 Apache Tomcat 웹 서버에 대한 배너를 `Internal Web Server`를 읽도록 수정하면, 벤더 문자열 `Internal Web Server`를 벤더 **Apache** 및 제품 **Tomcat**에 매핑한 다음 해당 매핑이 포함된 목록을 활성화할 수 있습니다. `Internal Web Server`라는 레이블의 서버가 나타나는 모든 호스트는 데이터베이스에 Apache Tomcat에 대한 취약성을 포함합니다.

팁 이 기능을 사용하면 규칙에 대한 SID를 또 다른 취약성에 매핑하여 취약성을 로컬 침입 규칙에 매핑할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.
단계 2 **Custom Product Mappings(**맞춤형 제품 매핑**)**를 클릭합니다.
단계 3 **Create Custom Product Mapping List(**맞춤형 제품 매핑 목록**)**을 클릭합니다.
단계 4 **Custom Product Mapping List Name(**맞춤형 제품 매핑 목록 이름**)**을 입력합니다.
단계 5 **Add Vendor String(**벤더 문자열 추가**)**를 클릭합니다.
단계 6 선택한 벤더 및 제품 값에 매핑해야 할 애플리케이션을 식별하는 벤더 문자열을 **Vendor String** 필드에 입력합니다.
단계 7 매핑하고자 하는 벤더를 **Vendor(**벤더**)** 드롭다운 목록에서 선택합니다.
단계 8 매핑하고자 하는 제품을 **Product(**제품**)** 드롭다운 목록에서 선택합니다.
단계 9 **Add(**추가**)**를 클릭하여 매핑된 벤더 문자열을 목록에 추가합니다.
단계 10 선택적으로, 벤더 문자열 매핑을 목록에 더 추가하려면 필요에 따라 4~8단계를 반복합니다.
단계 11 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 제품 매핑 목록을 활성화합니다. 자세한 내용은 맞춤형 제품 매핑 활성화 및 비활성화, 2413 페이지를 참고하십시오.

맞춤형 제품 매핑 목록 편집

벤더 문자열을 추가 또는 제거하거나 목록 이름을 변경하여 기존의 맞춤형 제품 매핑 목록을 수정할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.
단계 2 **Custom Product Mappings(**맞춤형 제품 매핑**)**를 클릭합니다.
단계 3 편집할 제품 매핑 목록 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 맞춤형 제품 매핑 생성, 2411 페이지에 설명된 대로 목록을 변경합니다.
단계 5 완료하면 **Save(**저장**)**를 클릭합니다.

맞춤형 제품 매핑 활성화 및 비활성화

맞춤형 제품 매핑의 전체 목록 사용을 동시에 활성화 또는 비활성화할 수 있습니다. 맞춤형 제품 매핑 목록을 활성화하면, 매니지드 디바이스에 의해 탐지되었든 호스트 입력 기능을 통해 가져왔든, 해당 목록의 각 매핑이 지정된 벤더 문자열이 있는 모든 애플리케이션에 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **Custom Product Mappings(**맞춤형 제품 매핑**)**를 클릭합니다.

단계 **3** 맞춤형 제품 매핑 목록 옆에 있는 슬라이더를 클릭해 매핑을 활성화하거나 비활성화합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

호스트 입력 클라이언트 설정

호스트 입력 기능을 이용하면 다른 어플라이언스에서 실행 중인 클라이언트 프로그램에서 Firepower Management Center의 네트워크 맵을 업데이트할 수 있습니다. 예를 들어 네트워크 맵에서 호스트를 추가 또는 삭제하거나, 호스트 OS 및 서비스 정보를 업데이트하는 식입니다. 자세한 내용은 *Firepower System Host Input API* 설명서를 참고하십시오.

원격 클라이언트를 실행하기 전에 Host Input Client(호스트 입력 클라이언트) 페이지에서 클라이언트를 Firepower Management Center의 피어 데이터베이스에 추가해야 합니다. 또한 FMC에서 생성된 인증 인증서를 클라이언트에 복사해야 합니다. 이상의 완료하려면 클라이언트를 FMC에 연결할 수 있습니다.

다중 도메인 구축에서는 모든 도메인에서 클라이언트를 만들 수 있습니다. 인증 인증서가 있으면 클라이언트는 클라이언트 인증서의 도메인과 완결된 모든 리프 도메인에 대한 네트워크 앱 업데이트를 전송할 수 있습니다. 상위 도메인에 대한 인증서를 만든다면(또는 하위 도메인 추가 후 인증서 도메인이 상위 도메인이 된다면), 해당 인증서를 사용하는 모든 클라이언트는 *Firepower System Host Input API* 설명서에 설명된 대로 각 트랜잭션을 이용해 대상 리프 도메인을 지정해야 합니다.

Host Input Client(호스트 입력 클라이언트)는 현재 도메인과 연결된 클라이언트만 표시하므로, 인증서를 다운로드하거나 취소하려면 클라이언트가 생성된 도메인으로 전환해야 합니다.

이 연결은 TLS 1.2를 사용합니다.

프로시저

단계 **1** **System(**시스템**)** > **Integration(**통합**)**을(를) 선택합니다.

단계 **2** **Host Input Client(**호스트 입력 클라이언트**)**를 클릭합니다.

단계 **3** **Create Client(**클라이언트 생성**)**를 클릭합니다.

단계 **4** **Hostname(**호스트 이름**)** 필드에 호스트 입력 클라이언트를 실행하는 호스트의 IP 주소 또는 호스트 이름을 입력합니다.

참고 DNS 확인을 설정하지 않은 경우, IP 주소를 사용해야 합니다.

단계 **5** 인증서 파일을 암호화하려면, **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.
호스트 입력 서비스는 이제 Firepower Management Center의 포트 8307에 대한 호스트의 액세스를 허용하며, 클라이언트-서버 인증 중에 사용할 인증 인증서를 생성합니다.

단계 **7** 인증서 파일 옆에 있는 다운로드( )를 클릭합니다.

단계 **8** SSL/TLS 인증을 위해 클라이언트에서 사용하는 디렉터리에 인증서 파일을 저장합니다.

단계 **9** 클라이언트에 대한 액세스를 취소하려면 제거할 호스트 옆에 있는 삭제 삭제( )를 클릭합니다.

/firepower/fmc/fmc_config_guide/discovery-host-profiles/t_editing_server_identities.xml

Nmap 스캐닝

Firepower System 네트워크 트래픽의 패시브 분석을 통해 네트워크 맵을 기반 으로합니다. 이 수동 분석을 통해 얻은 정보가 유지할 수 있는 경우에 따라 시스템 조건에 따라 완료 합니다. 그러나 호스트 전체 정보를 확보 하는 데 적극적으로 검색할 수 있습니다. 예를 들어, 호스트가 열린 포트에서 실행 중인 서버를 가지고 있지만 시스템이 네트워크를 모니터링하는 동안 서버가 트래픽을 수신하거나 전송하지 않은 경우, 시스템은 해당 서버에 대한 정보를 네트워크 맵에 추가하지 않습니다. 그러나 활성 스캐너를 사용하여 해당 호스트를 직접 검색하면 프레즌스 서버를 탐지할 수 있습니다.

Firepower System Nmap™, 네트워크 탐사 및 보안 감사 오픈 소스 활성 스캐너는 통합됩니다.

Nmap을 사용하여 호스트를 검색할 때 시스템은 다음과 같이 합니다.

- 해당 호스트에 대 한 호스트 프로 파일의 서버 목록에 이전에 탐지 개방 포트 서버를 추가합니다. 호스트 프로파일에는 필터링되거나 닫힌 TCP 포트 또는 UDP 포트에서 검색된 서버가 검색 결과 섹션에 나열되어 있습니다. Nmap은 기본적으로 1660개 이상의 TCP 포트를 검색합니다.

  시스템이 Nmap 검사에서 식별 된 서버와 해당 서버 정의 하는 경우 시스템은 해당 Cisco 서버 정의를 서버에 대 한 Nmap 사용 하 여 이름을 매핑합니다.

- 검색 결과를 1500개 이상의 알려진 운영 체제 지문과 비교하여 운영 체제를 결정하고 각 운영 체제에 점수를 부여합니다. 호스트에 할당된 운영 체제는 점수가 가장 높은 운영 체제 지문입니다.

  시스템은 Nmap 운영 체제 이름을 Cisco 운영 체제 정의에 매핑합니다.

- 서버를 추가 및 운영 체제에 대 한 호스트에는 취약성을 할당합니다.

참고:

- Nmap이 호스트 프로파일에 결과를 추가하기 전에 호스트가 네트워크 맵에 존재해야 합니다.
- 호스트가 네트워크 맵에서 삭제되면 해당 호스트에 대한 Nmap 검색 결과가 모두 삭제됩니다.

팁 일부 검색 옵션(예: 포트 스캔)은 대역폭이 낮은 네트워크에 상당한 부하를 가할 수 있습니다. 네트워크 사용량이 적은 기간 동안 실행되도록 이와 같은 예약을 스캔합니다.

검색에 사용되는 기본 Nmap 기술에 대한 자세한 내용은 http://insecure.org/의 Nmap 설명서를 참조하십시오.

관련 항목

Nmap 스캔 자동화, 253 페이지

Nmap 교정 옵션

Nmap 교정을 생성하여 Nmap 스캔에 대한 설정을 정의합니다. Nmap 교정은 상관관계 정책에서 응답으로 사용하거나, 온디맨드 방식으로 실행하거나, 특정 시간에 실행되도록 예약할 수 있습니다.

Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트에서 운영체제 및 서버 데이터를 스캔하려는 경우 Nmap 제공 운영체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다.

다음 표에서는 Firepower System의 Nmap 교정에서 구성할 수 있는 옵션에 대해 설명합니다.

표 ***247: Nmap*** 교정 옵션

옵션	설명	해당 **Nmap** 옵션
이벤트에서 어떤 주소를 스캔하겠습니까?	상관관계 규칙에 대한 응답으로 Nmap 스캔을 사용할 때 이벤트의 어떤 주소를 스캔할 것인지, 소스 호스트 주소인지 대상 호스트 주소인지 아니면 둘 다인지를 제어하는 다음 옵션 중 하나를 선택합니다. • **Scan Source and Destination Addresses(**소스 및 대상 주소 스캔**)**는 이벤트에서 소스 IP 주소 및 대상 IP 주소로 표시되는 호스트를 스캔합니다. • **Scan Source Address Only(**소스 주소만 스캔**)**은 이벤트의 소스 IP 주소가 나타내는 호스트를 스캔합니다. • **Scan Destination Address Only(**대상 주소만 스캔**)**은 이벤트의 대상 IP 주소가 나타내는 호스트를 스캔합니다.	해당 없음

옵션	설명	해당 Nmap 옵션
스캔 유형	Nmap이 포트를 스캔하는 방법을 선택합니다. • **TCP Syn** 스캔은 완전한 TCP 핸드셰이크를 사용하지 않은 채 수천 개의 포트에 빠르게 연결합니다. 이 옵션을 사용하면 TCP 연결을 시작하기만 하고 완료하지 않음으로써, `admin` 계정이 원시 패킷 액세스 권한을 가지고 있거나 IPv6이 실행되지 않고 있는 호스트의 스텔스(stealth) 모드에서 빠르게 스캔할 수 있습니다. 호스트가 TCP Syn 스캔에서 전송된 Syn 패킷을 인식하면 Nmap은 연결을 재설정합니다. • **TCP Connect** 스캔은 `connect()` 시스템 호출을 사용하여 호스트의 운영체제를 통한 연결을 엽니다. Firepower Management Center 또는 매니지드 디바이스의 `admin` 사용자가 호스트에 대한 원시 패킷 권한을 가지고 있지 않거나 현재 IPv6 네트워크를 스캔 중인 경우 TCP Connect 스캔을 사용할 수 있습니다. 즉, TCP Syn 스캔을 사용할 수 없는 상황에서는 이 옵션을 사용해야 합니다. • **TCP ACK** 스캔은 ACK 패킷을 전송하여 포트의 필터링 여부를 확인합니다. • **TCP Window** 스캔은 TCP ACK 스캔과 동일한 방식으로 작동하지만, 포트가 열렸는지 또는 닫혔는지도 확인할 수 있습니다. • **TCP Maimon** 스캔은 FIN/ACK 프로브를 사용하여 BSD에서 파생된 시스템을 식별합니다.	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
UDP 포트 스캔	TCP 포트 외에 UDP 포트 스캔도 활성화합니다. UDP 포트 스캐닝은 시간이 많이 걸릴 수 있으므로 빠르게 스캔하려는 경우에는 이 옵션을 사용하지 마십시오.	`-sU`

옵션	설명	해당 **Nmap** 옵션
이벤트의 포트 사용	상관관계 정책에서 교정을 응답으로서 사용하려는 경우, 교정이 상관관계 응답을 트리거하는 이벤트에 지정된 포트만 스캔하도록 설정합니다. • **On(**켜기**)**을 선택하면 Nmap 교정 설정에서 지정한 포트가 아닌 상관관계 이벤트의 포트를 스캔합니다. 상관관계 이벤트의 포트를 스캔하면, 교정은 사용자가 Nmap 교정 설정에서 지정한 IP 주소의 포트를 스캔합니다. 또한 이러한 포트는 교정의 동적 스캔 대상에 추가됩니다. • **Off(**끄기**)**를 선택하면 Nmap 교정 설정에서 지정한 포트만 스캔합니다. 또한 Nmap이 운영체제 정보 및 서버 정보를 수집할지 여부도 제어할 수 있습니다. 새 서버와 관련된 포트를 스캔하려면 **Use Port From Event(**이벤트의 포트 사용**)** 옵션을 활성화하십시오.	해당 없음
보고 탐지 엔진 스캔	호스트를 보고한 탐지 엔진이 상주하는 어플라이언스에서 호스트를 스캔하도록 설정합니다. • 보고 탐지 엔진을 실행하는 어플라이언스에서 스캔하려면 **On(**켜기**)**을 선택합니다. • 교정에서 구성된 어플라이언스에서 스캔하려면 **Off(**끄기**)**를 선택합니다.	해당 없음

옵션	설명	해당 **Nmap** 옵션
빠른 포트 스캔	스캐닝을 수행하는 디바이스의 `/var/sf/nmap/share/nmap/nmap-services` 디렉터리에 있는 `nmap-services` 파일에 나열된 TCP 포트만 스캔하고 다른 포트 설정은 무시하도록 설정합니다. 이 옵션은 **Port Ranges and Scan Order(**포트 범위 및 스캔 순서**)** 옵션과 함께 사용할 수 없습니다. • 스캐닝을 수행하고 다른 포트 설정은 무시하는 디바이스의 `/var/sf/nmap/share/nmap/nmap-services` 디렉터리에 있는 `nmap-services` 파일에 나열된 포트만 스캔하려면, **On(**켜기**)**을 선택합니다. • 모든 TCP 포트를 스캔하려면 **Off(***끄기***)**를 선택합니다.	`-F`
포트 범위 및 스캔 순서	Nmap 포트 사양 구문을 사용하여 스캔할 특정 포트를 설정하고 스캔 순서를 지정합니다. 이 옵션은 **Fast Port Scan(**빠른 포트 스캔**)** 옵션과 함께 사용할 수 없습니다.	`-p`
벤더 및 버전 정보에 대한 열린 포트 탐색	서버 벤더 및 버전 정보의 탐지를 활성화합니다. 열린 포트에서 서버 벤더 및 버전 정보를 조사하면 Nmap은 서버 식별에 사용하는 서버 데이터를 얻게 됩니다. 그런 다음 해당 서버에 대한 Cisco 서버 데이터를 교체합니다. • 호스트의 열린 포트에서 서버 정보를 스캔하여 서버 벤더 및 버전을 식별하려면 **On(**켜기**)**을 선택합니다. • 호스트에 대한 Cisco 서버 정보를 계속해서 사용하려면 **Off(***끄기***)**를 선택합니다.	`-sV`

옵션	설명	해당 Nmap 옵션
서비스 버전 강도	서비스 버전에 대한 Nmap 프로브의 강도를 선택합니다. • 시간이 오래 걸리지만 정확도 높은 스캔을 위해 더 많은 프로브를 사용하려면 더 높은 숫자를 선택합니다. • 정확도는 떨어지지만 시간은 적게 걸리는 스캔을 위해 더 적은 프로브를 사용하려면 더 낮은 숫자를 선택합니다.	`--version-intensity` <intensity>
운영체제 탐지	호스트에 대한 운영체제 정보의 탐지를 활성화합니다. 호스트에 대한 운영체제의 탐지를 구성하면 Nmap은 호스트를 스캔하고 그 결과를 사용하여 각 운영체제에 대한 점수를 생성합니다. 이 점수는 운영체제가 호스트에서 실행되고 있을 가능성을 반영합니다. • 호스트에서 운영체제를 식별하기 위한 정보를 스캔하려면 **On(**켜기**)**을 선택합니다. • 호스트에 대한 Cisco 운영체제 정보를 계속해서 사용하려면 **Off(***끄기***)**를 선택합니다.	`-o`

옵션	설명	해당 **Nmap** 옵션
모든 호스트를 온라인으로 취급	호스트 검색 프로세스를 건너뛰고 대상 범위의 모든 호스트에서 포트 스캔을 실행하도록 설정합니다. 이 옵션을 활성화하면 Nmap은 **Host Discovery Method(**호스트 검색 방법**)** 및 **Host Discovery Port List(**호스트 검색 포트 목록**)**에 대한 설정을 무시합니다. • 호스트 검색 프로세스를 건너뛰고 대상 범위의 모든 호스트에서 포트 스캔을 실행하려면 **On(**켜기**)**을 선택합니다. • **Host Discovery Method(**호스트 검색 방법**)** 및 **Host Discovery Port List(**호스트 검색 포트 목록**)**에 대한 설정을 사용하여 호스트 검색을 수행하고 사용할 수 없는 호스트에 대한 포트 스캔은 건너뛰려면 **Off(***끄기***)**를 선택합니다.	`-PN`

옵션	설명	해당 Nmap 옵션
호스트 검색 방법	대상 범위의 모든 호스트에 대해 **Host Discovery Port List(**호스트 검색 포트 목록**)**에 나열된 포트에서(포트가 나열되지 않은 경우 해당 호스트 검색 방법에 대한 기본 포트에서) 호스트 검색을 수행하려면 선택합니다. 그러나 **Treat All Hosts As Online(**모든 호스트를 온라인으로 취급**)**도 활성화한 경우 **Host Discovery Method(**호스트 검색 방법**)** 옵션은 효과가 없으며 호스트 검색이 수행되지 않습니다. 호스트가 있으며 사용 가능한지를 알아보기 위해 Nmap으로 테스트할 때 사용할 방법을 선택합니다. • **TCP SYN** 옵션은 SYN 플래그가 설정된 빈 TCP 패킷을 전송하고 응답을 받으면 호스트가 사용 가능한 상태인 것으로 인식합니다. TCP SYN은 기본적으로 포트 80을 스캔합니다. 스테이트풀 방화벽 규칙이 있는 방화벽에서는 TCP SYN 스캔을 차단할 가능성이 적습니다. • **TCP ACK** 옵션은 ACK 플래그가 설정된 빈 TCP 패킷을 전송하고 응답을 받으면 호스트가 사용 가능한 상태인 것으로 인식합니다. TCP ACK도 기본적으로 포트 80을 스캔합니다. 스테이트리스 방화벽 규칙이 있는 방화벽에서는 TCP ACK 스캔을 차단할 가능성이 적습니다. • **UDP** 옵션은 UDP 패킷을 전송하고, 닫힌 포트에서 포트 도달 불가 응답이 돌아오면 호스트가 사용 가능한 상태인 것으로 간주합니다. UDP는 기본적으로 포트 40125를 스캔합니다.	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
호스트 검색 포트 목록	호스트 검색을 수행할 때 스캔할 포트의 맞춤형 목록을 쉼표로 구분하여 지정합니다.	호스트 검색 방법에 대한 포트 목록

옵션	설명	해당 Nmap 옵션
기본 NSE 스크립트	호스트 검색 및 서버/운영체제/취약성 탐지에 대한 Nmap 스크립트의 기본 세트 실행을 활성화합니다. 기본 스크립트 목록은 https://nmap.org/nsedoc/categories/default.html 을 참조하십시오. • 기본 Nmap 스크립트 세트를 실행하려면 **On(**켜기**)**을 선택합니다. • 기본 Nmap 스크립트 세트를 건너뛰려면 **Off(**끄기**)**를 선택합니다.	`-sC`
타이밍 템플릿	스캔 프로세스의 타이밍을 선택합니다. 높은 숫자를 선택할수록 스캔의 범위가 줄고 속도가 빨라집니다.	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap 스캔 지침

활성 스캐닝을 통해 귀중한 정보를 얻을 수 있지만 Nmap 등의 툴을 과용하면 네트워크 리소스에 과부하가 발생하거나 중요한 호스트가 충돌할 수도 있습니다. 활성 스캐너를 사용하는 동안에는 이러한 지침에 따라 반드시 필요한 호스트와 포트만 스캔할 수 있도록 스캐닝 전략을 세워야 합니다.

적절한 스캔 대상 선택

Nmap을 구성할 때 스캔할 호스트를 식별하는 스캔 대상을 생성할 수 있습니다. 스캔 대상에는 스캔할 단일 IP 주소, CIDR 블록 또는 IP 주소의 옥텟 범위, IP 주소 범위, IP 주소의 목록이나 범위는 물론 호스트의 포트도 포함됩니다.

다음과 같은 방법으로 대상을 지정할 수 있습니다.

- IPv6 호스트의 경우
  - 정확한 IP 주소(예: `192.168.1.101`)
- IPv4 호스트의 경우
  - 정확한 IP 주소(예: `192.168.1.101`) 또는 쉼표나 공백으로 구분한 IP 주소의 목록
  - CIDR 표기법을 사용한 IP 주소 블록(예를 들어 `192.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트를 스캔함)

- 옥텟 범위 주소 지정을 사용한 IP 주소 범위(예를 들어 `192.168.0-255.1-254`는 .0 또는 .255로 끝나는 주소를 제외한 192.168.x.x 범위의 모든 주소를 스캔함)
- 하이픈을 사용한 IP 주소 범위(예를 들어 `192.168.1.1 - 192.168.1.5`는 192.168.1.1과 192.168.1.5(포함) 사이의 6개 호스트를 스캔함)
- 쉼표나 공백으로 구분한 주소 목록 또는 범위(예를 들어 `192.168.1.0/24, 194.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트 및 194.168.1.1과 194.168.1.254(포함) 사이의 254개 호스트를 스캔함)

Nmap 스캔을 위한 이상적인 스캔 대상에는 시스템이 식별할 수 없는 운영체제의 호스트, 식별되지 않은 서버의 호스트 또는 네트워크에서 최근에 탐지되지 않은 호스트가 포함됩니다. 네트워크 맵에 이미 존재하지 않는 호스트에 대한 네트워크 맵에는 Nmap 결과를 추가할 수 없습니다.

⚠

주의

- Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오.
- 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.
- 사용자는 대상을 스캔할 권한이 있어야 합니다. 자신 또는 자신의 회사에 속하지 않은 호스트를 스캔하기 위해 Nmap을 사용하는 것은 불법일 수 있습니다.

스캔할 적절한 포트 선택

설정하는 각 스캔 대상에 대해 스캔할 포트를 선택할 수 있습니다. 각 대상에서 스캔해야 할 정확한 포트 집합을 식별하려면 개별 포트 번호, 포트 범위 또는 포트 번호와 포트 범위의 시리즈를 지정할 수 있습니다.

기본적으로 Nmap은 1~1024의 TCP 포트를 스캔합니다. 상관관계 정책에서 교정을 응답으로서 사용하려는 경우, 교정이 상관관계 응답을 트리거하는 이벤트에 지정된 포트만 스캔하게 할 수 있습니다. 온디맨드 방식으로 또는 예약된 작업으로 교정을 실행하는 경우 또는 이벤트에서 포트를 사용하지 않는 경우 다른 포트 옵션을 사용하여 어떤 포트를 스캔할지 결정할 수 있습니다. `nmap-services` 파일에 나열된 TCP 포트만 스캔하고 다른 포트 설정은 무시하도록 선택할 수 있습니다. TCP 포트 외에 UDP 포트도 스캔할 수 있습니다. UDP 포트 스캐닝은 시간이 많이 걸릴 수 있으므로 빠르게 스캔하려는 경우에는 이 옵션을 사용하지 마십시오. 스캔할 특정 포트 또는 포트 범위를 선택하려면 포트를 식별하기 위한 Nmap 포트 사양 구문을 사용하십시오.

호스트 검색 옵션 설정

호스트에 대한 포트 스캔을 시작하기 전에 호스트 검색 수행 여부를 결정할 수 있습니다. 또는 스캔하려는 모든 호스트가 온라인 상태라고 가정할 수 있습니다. 모든 호스트를 온라인 상태로 취급하지 않으려는 경우 원하는 호스트 검색 방법을 선택할 수 있으며, 필요에 따라 호스트 검색 중 스캔할 포트 목록을 맞춤형할 수 있습니다. 호스트 검색은 나열된 포트에서 운영체제 또는 서버 정보를 조사하지 않습니다. 특정 포트에 대한 응답을 사용하여 호스트가 활성 상태이며 사용 가능한지만 확인합니다. 호스트 검색을 수행했는데 호스트가 사용 가능하지 않으면 Nmap은 해당 호스트에서 포트를 스캔하지 않습니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지
Nmap 스캔 자동화, 253 페이지

예: Nmap을 사용하여 알 수 없는 운영 체제 확인

이 예에서는 알 수 없는 운영체제를 확인하도록 설계된 Nmap 설정을 안내합니다. Nmap 설정 전체 과정은 Nmap 스캔 관리, 2426 페이지 섹션을 참조하십시오.

시스템이 네트워크에 있는 호스트의 운영체제를 확인할 수 없다면, Nmap을 사용하여 호스트를 능동적으로 스캔할 수 있습니다. Nmap은 스캔에서 얻은 정보를 사용하여 가능한 운영체제를 평가합니다. 그런 다음 호스트 운영체제 식별의 점수가 가장 높은 운영체제를 사용합니다.

Nmap을 사용하여 새 호스트에서 운영체제와 서버 정보를 확인하면 시스템은 스캔된 호스트에서 해당 정보를 모니터링하지 않습니다. Nmap을 사용하여 호스트를 검색하고 시스템에서 알 수 없는 운영체제가 포함된 것으로 표시한 호스트의 서버 운영체제를 검색하는 경우 유사한 호스트 그룹을 식별할 수 있습니다. 그런 다음 이들 중 하나를 기반으로 맞춤형 핑거프린트를 생성하여, Nmap 스캔을 기반으로 호스트에서 실행 중임을 알고 있는 운영체제의 핑거프린트와 연결할 수 있습니다. 가능하면 Nmap과 같은 서드파티 소스를 통해 고정 데이터를 입력하기보다 맞춤형 핑거프린트를 사용하십시오. 맞춤형 핑거프린트를 사용하면 시스템은 계속해서 호스트 운영체제를 모니터링하고 필요 시 업데이트할 수 있기 때문입니다.

이 예에서는 다음 작업을 수행하게 됩니다.

1. Nmap 스캔 인스턴스 추가, 2427 페이지에 설명된 대로 스캔 인스턴스를 설정합니다.
2. 다음 설정을 사용하여 Nmap 교정을 생성합니다.
   - **Use Port From Event(**이벤트의 포트 사용**)**를 활성화해 새 서버와 관련된 포트를 스캔합니다.
   - **Detect Operating System(**운영체제 탐지**)**를 활성화해 호스트에 대한 운영체제 정보를 탐지합니다.
   - **Probe open ports for vendor and version information(**벤더 및 버전 정보에 대한 열린 포트 탐색**)**을 활성화해 서버 벤더 및 버전 정보를 탐지합니다.
   - 호스트가 존재하는 것을 아는 경우 **Treat All Hosts as Online(**모든 호스트를 온라인으로 취급**)**을 활성화합니다.
3. 시스템이 알려지지 않은 운영체제의 호스트를 탐지할 때 트리거되는 상관관계 규칙을 생성합니다. 이 규칙은 검색 이벤트가 발생할 때,호스트의 **OS** 정보가 변경될 때, 그리고 **OS** 이름을 알 수 없음 조건을 충족할 때 트리거됩니다.
4. 상관관계 규칙이 포함된 상관관계 정책을 생성합니다.
5. 상관관계 정책에서, 2단계에서 생성한 Nmap 교정을 3단계에서 생성한 규칙에 추가합니다.
6. 상관관계 정책을 활성화합니다.
7. 네트워크 검색이 다시 시작되고 네트워크 맵이 재작성되도록 네트워크 맵의 호스트를 삭제합니다.

8. 하루나 이틀 후, 상관관계 정책에 의해 생성된 이벤트를 검색합니다. 호스트에서 탐지된 운영체제에 대한 Nmap 결과를 분석하여 네트워크에 시스템이 인식하지 못한 특별한 호스트 설정에 있는지 알아봅니다.
9. Nmap 결과가 동일한 알 수 없는 운영체제의 호스트를 찾으면 그러한 호스트 중 하나에 대해 맞춤형 핑거프린트를 생성하고 향후 유사한 호스트를 식별하는 데 사용합니다.

관련 항목

Nmap 교정 생성, 2430 페이지
상관관계 규칙 설정, 2587 페이지
Nmap 스캔 결과, 2434 페이지
클라이언트에 대한 맞춤형 핑거프린트 생성, 2401 페이지
상관관계 정책 설정, 2585 페이지

예: Nmap을 사용하여 새 호스트에 응답

이 예에서는 새 호스트에 응답하도록 설계된 Nmap 설정을 안내합니다. Nmap 설정 전체 과정은 Nmap 스캔 관리, 2426 페이지의 내용을 참조하십시오.

침입 가능성이 있는 서브넷에서 시스템이 새 호스트를 탐지하면, 이에 대한 정확한 취약성 정보가 있는지 확인하기 위해 해당 호스트를 스캔할 수 있습니다.

그렇게 하려면 이 서브넷에 새 호스트가 나타날 때 이를 탐지하고 호스트에서 Nmap 스캔을 수행하는 교정을 실행하는 상관관계 정책을 생성 및 활성화하면 됩니다.

이렇게 하려면 다음 작업을 수행해야 합니다.

1. Nmap 스캔 인스턴스 추가, 2427 페이지에 설명된 대로 스캔 인스턴스를 설정합니다.
2. 다음 설정을 사용하여 Nmap 교정을 생성합니다.
   - **Use Port From Event(**이벤트의 포트 사용**)**를 활성화해 새 서버와 관련된 포트를 스캔합니다.
   - **Detect Operating System(**운영체제 탐지**)**를 활성화해 호스트에 대한 운영체제 정보를 탐지합니다.
   - **Probe open ports for vendor and version information(**벤더 및 버전 정보에 대한 열린 포트 탐색**)**을 활성화해 서버 벤더 및 버전 정보를 탐지합니다.
   - 호스트가 존재하는 것을 아는 경우 **Treat All Hosts as Online(**모든 호스트를 온라인으로 취급**)**을 활성화합니다.
3. 시스템이 특정 서브넷에서 새 호스트를 탐지할 때 트리거되는 상관관계 규칙을 생성합니다. 규칙은 검색 이벤트가 발생할 때 및 새 호스트가 탐지될 때 트리거되어야 합니다.
4. 상관관계 규칙이 포함된 상관관계 정책을 생성합니다.
5. 상관관계 정책에서, 2단계에서 생성한 Nmap 교정을 3단계에서 생성한 규칙에 추가합니다.
6. 상관관계 정책을 활성화합니다.

7. 새 호스트에 대한 알림이 제공되면 해당 호스트 프로파일에서 Nmap 스캔의 결과를 확인하고 호스트에 적용되는 취약성을 해결합니다.

정책을 활성화하면, 교정 상태 보기(**Analysis(분석)** > **Correlation(상관관계)** > **Status(상태)**)를 주기적으로 확인해 교정 시작 시기를 확인할 수 있습니다. 교정의 동적 스캔 대상은 서버 탐지의 결과로서 스캔한 호스트의 IP 주소를 포함해야 합니다. Nmap에서 탐지한 운영체제와 서버를 기반으로, 그러한 호스트의 호스트 프로파일을 검토하여 호스트에 대해 해결해야 할 취약성이 있는지 알아보십시오.

⚠

주의 대규모 동적 네트워크가 있는 경우 새 호스트 탐지가 너무 빈번하여 스캔 사용에 응답하지 못할 수 있습니다. 리소스 과부하를 피하려면 자주 발생하는 이벤트에 대한 응답으로 Nmap 스캔을 사용하지 마십시오. 또한 Nmap을 사용하여 새 호스트에서 운영체제와 서버 정보를 확인하면 Cisco는 스캔된 호스트에서 해당 정보를 모니터링하지 않습니다.

관련 항목

Nmap 교정 생성, 2430 페이지
상관관계 규칙 설정, 2587 페이지
상관관계 정책 설정, 2585 페이지

Nmap 스캔 관리

Nmap 스캔을 사용하려면 최소한 Nmap 스캔 인터페이스와 Nmap 교정은 설정해야 합니다. Nmap 스캔 대상 설정은 선택사항입니다.

프로시저

단계 **1** Nmap 스캔 설정:

- Nmap 스캔 인스턴스 추가, 2427 페이지에 설명된 대로 Nmap 스캔 인스턴스를 추가합니다.
- Nmap 교정 생성, 2430 페이지에 설명된 대로 Nmap 교정을 생성합니다.
- 선택적으로, Nmap 스캔 대상 추가, 2429 페이지에 설명된 대로 Nmap 스캔 대상을 추가합니다.

단계 **2** Nmap 스캔 실행:

- 온디맨드 Nmap 스캔 실행, 2433 페이지에 설명된 대로 온디맨드 Nmap 스캔을 실행합니다.
- Nmap 스캔 자동화, 253 페이지에 설명된 대로 자동 Nmap 스캔을 설정합니다.
- Nmap 스캔 예약, 253 페이지에 설명된 대로 자동 Nmap 스캔을 예약합니다.

다음에 수행할 작업

- 관련 작업을 확인해 진행 중인 Nmap 스캔을 모니터링합니다(작업 메시지 보기, 445 페이지 참조).
- 선택적으로, 스캔을 개선합니다.

- Nmap 스캔 인스턴스 편집, 2428 페이지에 설명된 대로 Nmap 스캔 인스턴스를 편집합니다.
- Nmap 스캔 대상 편집, 2430 페이지에 설명된 대로 Nmap 스캔 대상을 편집합니다.
- Nmap 교정 편집, 2433 페이지에 설명된 대로 Nmap 교정을 편집합니다.

Nmap 스캔 인스턴스 추가

네트워크에서 취약성을 스캔하기 위해 사용할 각 Nmap 모듈에 대해 별도의 스캔 인스턴스를 설정할 수 있습니다. Firepower Management Center의 로컬 Nmap 모듈 및 원격으로 스캔을 실행하기 위해 사용할 디바이스에 대해 스캔 인스턴스를 설정할 수 있습니다. 원격 디바이스에서 스캔을 실행하는 경우에도, 각 스캔의 결과는 스캔을 구성하는 Firepower Management Center에 항상 저장됩니다. 미션 크리티컬 호스트에 대한 악의적인 스캔 또는 실수로 이루어지는 스캔을 방지하려면, 인스턴스로 스캔해서는 안 되는 호스트를 나타내기 위해 인스턴스에 대한 블랙리스트를 생성할 수 있습니다.

기존 스캔 인스턴스와 동일한 이름의 스캔 인스턴스를 추가할 수는 없습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 인스턴스를 표시하며 이러한 인스턴스는 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 인스턴스도 표시되지만, 이러한 인스턴스는 편집할 수 없습니다. 하위 도메인에서 생성된 스캔 인스턴스를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 Nmap 스캔 인스턴스 목록에 액세스합니다.

- **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.
- **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 교정 추가:

- 첫 번째 방법으로 목록에 액세스했다면, Add a New Instance(새 인스턴스 추가) 섹션을 찾은 다음 드롭다운 목록에서 Nmap Remediation 모듈을 선택하고 **Add(**추가**)**를 클릭합니다.
- 두 번째 방법으로 목록에 액세스했다면 **Add Nmap Instance(Nmap** 인스턴수 추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**을 클릭합니다.

단계 **4** **Description(**설명**)**을 입력합니다.

단계 **5** 선택적으로, 다음 명령문을 사용하여 이 검색 인스턴스로 스캔해서는 안 되는 호스트 또는 네트워크를 **Blacklisted Scan hosts(**블랙리스트에 추가한 스캔 호스트**)** 필드에 지정합니다.

- IPv6 호스트의 경우 정확한 IP 주소(예: `2001:DB8::fedd:eeff`)
- IPv4 호스트의 경우 정확한 IP 주소(예: `192.168.1.101`) 또는 CIDR 표기법을 사용하는 IP 주소 블록(예: `192.168.1.0/24`는 `192.168.1.1`과 `192.168.1.254` 사이(포함)의 254개 호스트를 스캔함)
- 주소 값을 부정하기 위해 느낌표(!)를 사용할 수는 없습니다.

참고 스캔 대상을 블랙리스트에 추가된 네트워크에 있는 호스트로 구체적으로 지정하는 경우 해당 스캔은 실행되지 않습니다.

단계 **6** 선택적으로, Firepower Management Center 대신 원격 디바이스에서 스캔을 실행하려면 FMC 웹 인터페이스에서 디바이스의 Information(정보) 페이지 **Remote Device Name(**원격 디바이스 이름**)** 필드에 나타나는 디바이스의 IP 주소 또는 이름을 지정합니다.

단계 **7** **Create(**생성**)**를 클릭합니다.
시스템이 인스턴스 생성을 완료하면, 편집 모드에 인스턴스가 표시됩니다.

단계 **8** 선택적으로, Nmap 교정을 인스턴스에 추가합니다. 이렇게 하려면 인스턴스의 Configured Remediations(설정된 교정) 섹션을 찾은 다음 **Add(**추가**)**를 클릭하고Nmap 교정 생성, 2430 페이지에 설명된 대로 교정을 생성해야 합니다.

단계 **9** **Cancel(**취소**)**을 클릭하여 인스턴스 목록으로 돌아갑니다.

참고 **Scanners(**스캐너**)** 옵션을 통해 Nmap 스캔 인터페이스 목록에 액세스했다면, 추가한 인스턴스에 교정을 추가해야 해당 인스터스가 시스템에서 표시됩니다. 교정을 추가하지 않은 인스턴스를 확인하려면 **Instances(**인스턴스**)** 메뉴 옵션을 이용해 목록에 액세스하십시오.

Nmap 스캔 인스턴스 편집

스캔 인스턴스를 편집할 때 인스턴스와 관련된 교정을 확인, 추가, 삭제할 수 있습니다. 인스턴스에 프로파일된 Nmap 모듈을 더 이상 사용하지 않으려는 경우 Nmap 스캔 인스턴스를 삭제할 수 있습니다. 스캔 인스턴스를 삭제할 때 해당 인스턴스를 사용하는 교정도 삭제할 수 있습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 인스턴스를 표시하며 이러한 인스턴스는 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 인스턴스도 표시되지만, 이러한 인스턴스는 편집할 수 없습니다. 하위 도메인에서 생성된 스캔 인스턴스를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 Nmap 스캔 인스턴스 목록에 액세스합니다.

- **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.
- **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 편집할 인스턴스 옆에 있는 보기 ( )을 클릭합니다.

단계 **3** Nmap 스캔 인스턴스 추가, 2427 페이지에 설명된 대로 스캔 인스턴스 설정을 변경합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 선택적으로, 스캔 인스턴스에 새 교정을 추가할 수 있습니다(다음 참조). Nmap 교정 생성, 2430 페이지
- 선택적으로, 인스턴스에 연결된 교정을 편집할 수 있습니다(Nmap 교정 편집, 2433 페이지 참조).
- 선택적으로, 인스턴스에 연결된 교정을 삭제할 수 있습니다(온디맨드 Nmap 스캔 실행, 2433 페이지 참조).
- 선택적으로, 스캔 인스턴스 옆에 있는 삭제( )을 클릭하여 인스턴스를 삭제할 수 있습니다.

Nmap 스캔 대상 추가

Nmap 모듈을 구성할 때 온디맨드 또는 예약된 스캔을 수행할 호스트와 포트를 식별하는 스캔 대상을 생성 및 저장할 수 있습니다. 그러면 매번 새로운 스캔 대상을 작성할 필요가 없습니다. 스캔 대상에는 스캔할 단일 IP 주소 또는 IP 주소 블록은 물론 호스트의 포트도 포함됩니다. Nmap 대상에 대해 Nmap 옥텟 범위 주소 지정 또는 IP 주소 범위를 사용할 수도 있습니다. Nmap 옥텟 범위 주소 지정에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

참고:

- 다수의 호스트가 포함된 스캔 대상을 스캔하는 데에는 많은 시간이 소요될 수 있습니다. 해결책은 한 번에 더 적은 수의 호스트를 스캔하는 것입니다.
- Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오. 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.
- 다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 대상을 표시하며 이러한 규칙은 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 대상도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인의 스캔 대상을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 1 **Policies(정책)** > **Actions(작업)** > **Scanners(스캐너)**을(를) 선택합니다.

단계 2 툴바에서 **Targets(대상)**를 클릭합니다.

단계 3 **Create Scan Target(스캔 대상 생성)**을 클릭합니다.

단계 4 이 스캔 대상에 사용할 이름을 **Name(이름)** 필드에 입력합니다.

단계 5 **IP Range(IP 범위)** 문자함에는 Nmap 스캔 지침, 2422 페이지에서 설명하는 구문을 사용하여 스캔할 호스트를 지정합니다.

참고 스캔 대상에서 IP 주소나 범위의 목록에 쉼표를 사용하는 경우, 대상을 저장할 때 쉼표는 공백으로 변환됩니다.

단계 6 스캔할 포트를 **Ports(포트)** 필드에 지정합니다.

1~65535의 값을 사용하여 다음 중 하나를 입력할 수 있습니다.

- 포트 번호
- 쉼표로 구분된 포트 목록
- 대시로 구분된 포트 번호의 범위
- 대시로 구분된, 쉼표로 구분된 포트 번호의 범위

단계 **7** **Save(**저장**)**를 클릭합니다.

관련 항목

Nmap 스캔 자동화, 253 페이지

Nmap 스캔 대상 편집

팁 특정 IP 주소를 스캔하기 위해 교정을 사용하고자 하지만 호스트가 교정을 실행한 상관관계 정책 위반과 관련되어 있기 때문에 IP 주소가 대상에 추가된 경우, 교정의 동적 스캔 대상을 편집할 수 있습니다.

나열된 호스트를 더 이상 스캔하지 않으려면 스캔 대상을 삭제하십시오.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 대상을 표시하며 이러한 규칙은 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 대상도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인의 스캔 대상을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 툴바에서 **Targets(**대상**)**를 클릭합니다.

단계 **3** 편집하려는 스캔 대상 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 필요한 대로 수정합니다. 자세한 내용은 Nmap 스캔 대상 추가, 2429 페이지를 참고하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 선택적으로 스캔 대상 옆에 있는 삭제( )을 클릭하여 대상을 삭제할 수 있습니다.

Nmap 교정 생성

Nmap 교정은 기존 Nmap 스캔 인스턴스에 추가하는 방법으로만 생성할 수 있습니다. 교정은 스캔에 대한 설정을 정의합니다. Nmap 교정은 상관관계 정책에서 응답으로 사용하거나, 온디맨드 방식으로 실행하거나, 특정 시간에 예약한 작업으로 실행할 수 있습니다.

Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오. 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.

Nmap 기능에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 Nmap 교정을 표시하며, 이러한 교정은 편집할 수 있습니다. 상위 도메인에서 생성된 Nmap 교정도 표시되지만, 이러한 교정은 수정할 수 없습니다. 하위 도메인의 Nmap 교정을 보고 편집하려면 해당 도메인으로 전환하십시오.

시작하기 전에

- Nmap 스캔 인스턴스 추가, 2427 페이지의 설명에 따라 Nmap 스캔 인스턴스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가할 인스턴스 옆에 있는 보기 ( )을 클릭합니다.

단계 **3** Configured Remediations(설정된 교정) 섹션에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **Remediation Name(**교정 이름**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** 침입 이벤트, 연결 이벤트 또는 사용자 이벤트를 트리거하는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우 **Scan Which Address(es) From Event(**이벤트에서 어떤 주소를 스캔하시겠습니까**)?** 옵션을 설정합니다.

팁 검색 이벤트 또는 호스트 입력 이벤트에서 트리거되는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우, 기본적으로 교정은 이벤트와 관련된 호스트의 IP 주소를 스캔합니다. 이 옵션은 설정할 필요가 없습니다.

참고 트래픽 프로파일 변경을 트리거하는 상관관계 규칙에는 Nmap 교정을 응답으로서 할당하지 마십시오.

단계 **7** **Scan Type(**스캔 유형**)** 옵션을 설정합니다.

단계 **8** 선택적으로, TCP 포트 외에 UDP 포트도 스캔하려면 **Scan for UDP ports(UDP** 포트 스캔**)** 옵션에 대해 **On(**켜기**)**을 선택합니다.

팁 UDP 포트스캔은 TCP 포트스캔보다 시간이 더 걸립니다. 스캔 속도를 높이려면 이 옵션을 비활성화하십시오.

단계 **9** 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하려는 경우 **Use Port From Event(**이벤트의 포트 사용**)** 옵션을 설정합니다.

단계 **10** 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하고 이벤트를 탐지한 탐지 엔진을 실행하는 어플라이언스를 사용하여 스캔을 실행하려는 경우 **Scan from reporting detection engine(**보고 탐지 엔진에서 스캔**)** 옵션을 설정합니다.

단계 **11** **Fast Port Scan(**빠른 포트 스캔**)** 옵션을 설정합니다.

단계 **12** Nmap 포트 사양 구문을 사용하여 기본적으로 스캔할 포트를 원하는 스캔 순서대로 **Port Ranges and Scan Order(**포트 범위 및 스캔 순서**)** 필드에 입력합니다.

다음 형식을 사용합니다.

- 1~65535의 값을 지정합니다.
- 쉼표나 공백을 사용하여 포트를 구분합니다.
- 포트 범위를 표시하려면 하이픈을 사용합니다.
- TCP 및 UDP 포트를 모두 스캔하는 경우, 스캔할 TCP 포트의 목록 앞에는 T를 추가하고 UDP 포트의 목록 앞에는 U를 추가합니다.

참고 8단계에 설명된 대로, 상관관계 정책 위반에 대한 응답으로 교정이 실행되는 경우 **Use Port From Event(**이벤트의 포트 사용**)** 옵션은 이 설정을 재정의합니다.

예제**:**

UDP 트래픽에 대해 포트 53 및 111을 스캔하고 TCP 트래픽에 대해 포트 21~25를 스캔하려면 `U:53,111,T:21-25`를 입력합니다.

단계 **13** 열린 포트에서 서버 벤더 및 버전 정보를 탐색하려면 **Probe open ports for vendor and version information(**벤더 및 버전 정보에 대한 열린 포트 탐색**)**을 설정합니다.

단계 **14** 열린 포트를 탐색하려는 경우 **Service Version Intensity(**서비스 버전 강도**)** 드롭다운 목록에서 숫자를 선택하여 사용되는 프로브의 수를 설정합니다.

단계 **15** 운영체제 정보를 스캔하려면 **Detect Operating System(**운영체제 탐지**)**설정을 구성합니다.

단계 **16** 호스트 검색 발생 여부 및 포트 스캔을 사용 가능한 호스트에 대해서만 실행할지 여부를 결정하려면 **Treat All Hosts As Online(**모든 호스트를 온라인으로 취급**)**을 구성합니다.

단계 **17** Nmap이 호스트 가용성을 테스트할 때 사용할 방법을 설정하려면, **Host Discovery Method(**호스트 검색 방법**)** 드롭다운 목록에서 방법을 선택합니다.

단계 **18** 호스트 검색 중 맞춤형 포트 목록을 스캔하려면 선택한 호스트 검색 방법에 적절한 포트 목록을 쉼표로 구분하여 **Host Discovery Port List(**호스트 검색 포트 목록**)** 필드에 입력합니다.

단계 **19** 호스트 검색 및 서버, 운영체제, 취약성 검색에 대해 기본 Nmap 스크립트 세트를 사용할지 여부를 제어하려면 **Default NSE Scripts(**기본 **NSE** 스크립트**)** 옵션을 구성합니다.

팁 기본 스크립트 목록은 http://nmap.org/nsedoc/categories/default.html을 참조하십시오.

단계 **20** 스캔 프로세스의 시간을 설정하려면 **Timing Template(**타이밍 템플릿**)** 드롭다운 목록에서 타이밍 템플릿 숫자를 선택합니다.

빠르지만 범위가 좁은 스캔을 원한다면 높은 숫자를, 느리지만 범위가 넓은 스캔을 원한다면 낮은 숫자를 선택합니다.

단계 **21** **Create(**생성**)**를 클릭합니다.
시스템이 교정 생성을 완료하면, 편집 모드에 교정이 표시됩니다.

단계 **22** **Done(**완료**)**을 클릭하여 관련된 인스턴스로 돌아갑니다.

단계 **23** **Cancel(**취소**)**을 클릭하여 인스턴스 목록으로 돌아갑니다.

관련 항목

Nmap 스캔 자동화, 253 페이지
Nmap 교정 옵션, 2415 페이지

Nmap 교정 편집

Nmap 교정에 대한 수정은 진행 중인 스캔에 영향을 미치지 않습니다. 새 설정은 다음 스캔이 시작될 때 적용됩니다. 더 이상 필요하지 않은 Nmap 교정은 삭제할 수 있습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 Nmap 교정을 표시하며, 이러한 교정은 편집할 수 있습니다. 상위 도메인에서 생성된 Nmap 교정도 표시되지만, 이러한 교정은 수정할 수 없습니다. 하위 도메인의 Nmap 교정을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 Nmap 스캔 인스턴스 목록에 액세스합니다.

- **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.
- **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 편집하려는 교정에 액세스합니다.

- 첫 번째 방법으로 목록에 액세스했다면, 관련 인스턴스 옆에 있는 아이콘(보기 ( ))을 클릭한 다음 Configured Remediations(설정한 교정) 섹션에서 편집할 교정 옆에 있는 해당 아이콘을 다시 클릭합니다.
- 두 번째 방법으로 목록에 액세스했다면, 편집할 교정 옆에 있는 아이콘(보기 ( ))을 클릭합니다.

단계 **3** Nmap 교정 생성, 2430 페이지에 설명된 대로 필요한 대로 수정합니다.

단계 **4** 변경사항을 저장하려면 **Save(**저장**)**를 클릭하고, 저장하지 않고 나가려면 **Done(**완료**)**을 클릭합니다.

단계 **5** 아니면 그 옆에 있는 아이콘(삭제( ))을 클릭하여 교정을 삭제할 수 있습니다.

온디맨드 Nmap 스캔 실행

필요할 때마다 온디맨드 Nmap 스캔을 실행할 수 있습니다. 스캔할 IP 주소와 포트를 입력하거나 기존 스캔 대상을 선택하여 온디맨드 스캔을 위한 대상을 지정할 수 있습니다.

Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오. 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.

시작하기 전에

- 선택적으로, Nmap 스캔 대상을 추가합니다(Nmap 스캔 대상 추가, 2429 페이지 참조).

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 2 스캔 수행에 사용할 Nmap 교정 옆에 있는 스캔( )을 클릭합니다.

단계 3 선택적으로, 저장된 스캔 대상을 사용하여 스캔하려면 **Saved Targets(**저장한 대상**)** 드롭다운 목록에서 대상을 선택하고 **Load(**로드**)**를 클릭합니다.

참고 스캔 대상을 추가하려면 대화 상자 상단의 수정( )을 클릭합니다.

단계 4 **IP Range(s)(IP** 범위**)** 필드에서 스캔할 호스트의 IP 주소를 지정하거나 로드된 목록을 수정합니다.

참고:

- IPv4 주소의 호스트에 대해서는 여러 IP 주소를 쉼표로 구분하여 지정하거나 CIDR 표기법을 사용할 수 있습니다. 또한 앞에 느낌표(!)를 사용하여 IP 주소를 부정할 수 있습니다.
- IPv6 주소의 호스트에 대해서는 정확한 IP 주소를 사용해야 합니다. 범위는 지원되지 않습니다.

단계 5 **Ports(**포트**)** 필드에서 스캔할 포트를 지정하거나 로드된 목록을 수정합니다.

포트 번호, 쉼표로 구분된 포트 목록 또는 대시로 구분된 포트 번호 범위를 입력할 수 있습니다.

단계 6 다중 도메인 구축의 경우에는 **Domain(**도메인**)** 필드를 사용하여 스캔을 수행할 리프 도메인을 지정합니다.

단계 7 **Scan Now(**지금 스캔**)**를 클릭합니다.

다음에 수행할 작업

- 필요한 경우 작업 상태를 모니터링합니다. 작업 메시지 보기, 445 페이지를 참조하십시오.

관련 항목

Nmap 스캔 자동화, 253 페이지
Firepower System IP 주소 규칙, 19 페이지
검색 내 포트, 2829 페이지

Nmap 스캔 결과

진행 중인 Nmap 스캔을 모니터링하고, Firepower System을 통해 이전에 수행한 스캔의 결과나 Firepower System 외부에서 수행한 결과를 가져오고, 스캔 결과를 확인 및 분석할 수 있습니다.

로컬 Nmap 모듈을 사용하여 생성한 스캔 결과를 팝업 윈도우에서 렌더링된 페이지로서 볼 수 있습니다. Nmap 결과 파일을 원시 XML 형식으로 다운로드할 수도 있습니다.

또한 호스트 프로파일 및 네트워크 맵에서 Nmap으로 탐지한 운영체제 및 서버 정보를 볼 수 있습니다. 호스트의 스캔이 필터링된 포트 또는 닫힌 포트에서 서버에 대한 서버 정보를 생성하는 경우, 또

는 스캔에서 운영체제 정보나 서버 섹션에 포함할 수 없는 정보를 수집하는 경우 호스트 프로파일의 Nmap Scan Results(Nmap 스캔 결과) 섹션에 그러한 결과가 포함됩니다.

Nmap 스캔 결과 보기

Nmap 스캔이 완료되면 스캔 결과 테이블을 볼 수 있습니다.

찾고 있는 정보에 따라 결과 보기를 조작할 수 있습니다. 스캔 결과에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 스캔 결과 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

Nmap 버전 1.01 DTD(http://insecure.org에서 다운로드 가능)를 사용하여 Nmap 결과를 다운로드하고 볼 수 있습니다.

스캔 결과를 지울 수도 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 툴바에서 **Scan Results(**스캔 결과**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 이벤트 시간 제약 조건, 2811 페이지에 설명된 대로 시간 범위를 조정합니다.
- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflows)**를 클릭합니다.
- 스캔 결과를 팝업 창에서 렌더링된 페이지로서 보려면 스캔 작업 옆에 있는 **View(**보기**)**를 클릭합니다.
- 텍스트 편집기에서 원시 XML 코드를 볼 수 있도록 스캔 결과 파일의 복사본을 저장하려면 스캔 작업 옆에 있는 **Download(**다운로드**)**를 클릭합니다.
- 검사 결과를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
- 표시되는 열을 제한하려면 숨기려는 열 머리글의 닫기(✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, **Disabled Columns(**비활성화된 열**)** 아래에서 열 이름을 클릭합니다.

- 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용, 2801 페이지 섹션을 참조하십시오.
- 스캔 인스턴스와 교정을 설정하려면 툴바에서 **Scanners(**스캐너**)**를 클릭하고 Nmap 스캔 관리, 2426 페이지 섹션을 참조하십시오.

- 워크플로 페이지 내부와 페이지 사이를 이동하는 방법은 워크플로 페이지 탐색 툴, 2798 페이지 섹션을 참조하십시오.
- 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)** 드롭다운 목록에서 확인할 이벤트 보기의 이름을 선택합니다.
- 스캔 결과를 검색하려면 해당 필드에 검색 기준을 입력합니다.

관련 항목

Nmap 스캔 결과 필드, 2436 페이지

Nmap 스캔 결과 필드

Nmap 스캔을 실행할 때 Firepower Management Center은(는) 데이터베이스에서 스캔 결과를 수집합니다. 다음 표는 스캔 결과 테이블에서 확인하고 검색할 수 있는 필드를 설명합니다.

표 ***248:*** 검색 결과 필드

필드	설명
시작 시간	결과를 생성한 스캔이 시작된 날짜와 시간
종료 시간	결과를 생성한 스캔이 종료된 날짜와 시간
대상	결과를 생성한 스캔에 대한 스캔 대상의 IP 주소(DNS 확인이 활성화된 경우에는 호스트 이름)
스캔 유형	결과를 생성한 스캔의 유형을 나타내기 위한 서드파티 스캐너의 이름 또는 `Nmap`
스캔 모드	결과를 생성한 스캔의 모드 • `On Demand` - 온디맨드 방식으로 실행된 스캔의 결과 • `Imported` - 다른 시스템에서 실행하고 Firepower Management Center(으)로 가져온 스캔의 결과. • `Scheduled` - 예약 작업으로서 실행한 스캔의 결과
결과	스캔의 결과입니다.
도메인	스캔 대상의 도메인입니다. 이 필드는 다중 도메인 구축에서만 표시됩니다.

관련 항목

이벤트 검색, 2825 페이지

Nmap 스캔 결과 가져오기

Firepower System 외부에서 수행된 Nmap 스캔에 의해 생성된 XML 결과 파일을 가져올 수 있습니다. Firepower System.에서 전에 다운로드한 XML 결과 파일을 가져올 수도 있습니다. Nmap 스캔 결과를 가져오려면 결과 파일은 XML 형식이어야 하며 Nmap 버전 1.01 DTD를 준수해야 합니다. Nmap 결과 생성 및 Nmap DTD에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

호스트가 네트워크 맵에 있어야만 Nmap이 결과를 호스트 프로파일에 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 툴바에서 **Import Results(**결과 가져오기**)**를 클릭합니다.

단계 **3** 다중 도메인 구축의 경우에는 **Domain(**도메인**)** 드롭다운 목록에서 리프 도메인을 선택해 가져온 결과를 저장할 곳을 지정합니다.

단계 **4** 결과 파일을 찾아보려면 **Browse(**찾기**)**를 클릭합니다.

단계 **5** Import Results(가져오기 결과) 페이지로 돌아온 후 **Import(**가져오기**)**를 클릭하여 결과를 가져옵니다.

호스트 ID 소스 기록

기능	버전	세부 사항
호스트 입력 데이터 기능에 대한 보안 개선	6.5	이제 FMC와 호스트 입력 클라이언트 간의 통신에 TLS 1.2를 사용합니다. 이 정보를 이용해 항목 호스트 입력 클라이언트 설정, 2413 페이지을(를) 업데이트했습니다.

96 장

애플리케이션 탐지

다음 주제에서는 Firepower System 애플리케이션 탐지를 설명합니다.

- 개요: 애플리케이션 탐지, 2439 페이지
- 애플리케이션 탐지 요구 사항 및 사전 요건, 2445 페이지
- 맞춤형 애플리케이션 탐지기, 2445 페이지
- 탐지기 상세정보 보기 또는 다운로드, 2454 페이지
- 탐지기 목록 정렬, 2454 페이지
- 탐지기 목록 필터링, 2455 페이지
- 다른 탐지기 페이지로 이동, 2456 페이지
- 탐지기 활성화 및 비활성화, 2456 페이지
- 맞춤형 애플리케이션 탐지기 편집, 2457 페이지
- 탐지기 삭제, 2458 페이지

개요: 애플리케이션 탐지

Firepower System은 IP 트래픽을 분석할 때 네트워크에서 일반적으로 사용되는 애플리케이션 식별을 시도합니다. 애플리케이션 인식은 애플리케이션 제어에 중요한 요소입니다.

시스템에서는 세 가지 유형의 애플리케이션을 탐지합니다.

- HTTP 및 SSH 등의 애플리케이션 프로토콜은 호스트 간 통신을 나타냅니다.
- 웹 브라우저 및 이메일 클라이언트 등의 클라이언트는 호스트웨어에서 실행되는 소프트웨어를 나타냅니다.
- MPEC 비디오 및 Facebook 등의 웹 애플리케이션은 HTTP 트래픽에 대한 요청 RUL 또는 콘텐츠를 나타냅니다.

시스템은 탐지기에서 지정된 특성에 따라 네트워크 트래픽에서 애플리케이션을 식별합니다. 예를 들어 시스템은 패킷 헤더 내 ASCII 패턴에 의해 애플리케이션을 식별할 수 있습니다. 또한 SSL(Secure Socket Layers) 프로토콜 탐지기는 보안 세션의 정보를 사용하여 세션에서 애플리케이션을 식별합니다.

Firepower System에는 두 가지 소스의 애플리케이션 탐지기가 있습니다.

- 시스템 제공 탐지기는 웹 애플리케이션, 클라이언트, 애플리케이션 프로토콜을 탐지합니다.

  애플리케이션(및 운영 체제)의 시스템 제공 탐지기 사용 여부는 Firepower System 및 설치한 VDB 버전에 따라 다릅니다. 신규 및 업데이트된 탐지기 정보는 릴리스 정보 및 참고 자료에서 확인할 수 있습니다. 전문 서비스에서 작성한 개별 탐지기를 가져올 수도 있습니다.

- 사용자 정의 애플리케이션 프로토콜 탐지기는 사용자가 생성한 것으로 웹 애플리케이션, 클라이언트, 애플리케이션 프로토콜을 탐지합니다.

내장된 애플리케이션 프로토콜 탐지기를 통해 애플리케이션 프로토콜을 탐지할 수 있으며 클라이언트의 탐지를 기반으로 애플리케이션 프로토콜의 존재를 암시합니다.

시스템은 네트워크 검색 정책에서 정의된 대로 모니터링되는 네트워크의 호스트에서 실행되는 애플리케이션 프로토콜만 식별합니다. 예를 들어 모니터링하지 않는 원격 사이트의 FTP 서버에 내부 호스트가 액세스하는 경우 시스템은 애플리케이션 프로토콜을 FTP로 식별하지 않습니다. 반면 원격 또는 내부 호스트가 모니터링 중인 FTP 서버에 액세스하면 시스템은 애플리케이션 프로토콜을 분명하게 식별할 수 있습니다.

시스템이 모니터링되는 호스트에서 모니터링되지 않는 서버에 연결하기 위해 사용되는 클라이언트를 식별할 수 있는 경우, 시스템은 클라이언트의 해당 애플리케이션 프로토콜을 식별하지만 해당 프로토콜을 네트워크 맵에 추가하지 않습니다. 애플리케이션 탐지가 발생하려면 클라이언트 세션에는 서버의 응답이 포함되어야 합니다.

시스템이 탐지하는 각 애플리케이션의 특성 정의는 애플리케이션 특성, 538 페이지의 내용을 참조하십시오. 시스템은 해당 특성을 사용해 애플리케이션 필터라는 애플리케이션 그룹을 생성합니다. 애플리케이션 필터는 액세스 제어를 수행하고 보고서와 대시보드 위젯에서 사용되는 데이터 및 검색 결과를 제한합니다.

또한 내보낸 NetFlow 기록, Nmap 활성 스캐닝, 호스트 인풋 기능에 사용되는 애플리케이션 탐지기 데이터를 보완할 수 있습니다.

관련 항목

애플리케이션 제어 구성 모범 사례, 541 페이지
애플리케이션 탐지기 기초, 2440 페이지

애플리케이션 탐지기 기초

Firepower System은 *application detectors(*애플리케이션 탐지기*)*를 사용하여 네트워크 상의 자주 사용하는 애플리케이션을 식별합니다. Detectors(탐지기) 페이지(**Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**)를 이용해 탐지기 목록을 확인하고 탐지 기능을 맞춤형할 수 있습니다.

탐지기를 수정하거나 탐지기 유형에 따라 탐지기 상태(활성화 또는 비활성화)를 바꿀 수 있습니다. 시스템은 애플리케이션 트래픽을 분석하는 데 활성 탐지기만 사용합니다.

참고 Cisco에서 제공하는 탐지기는 Firepower System 및 VDB 업데이트에 따라 변경될 수 있습니다. 업데이트된 탐지기 관련 정보는 릴리즈 노트와 참고 자료에서 확인할 수 있습니다.

Cisco가 제공하는 내부 탐지기

내부 탐지기는 클라이언트, 웹 애플리케이션 및 애플리케이션 프로토콜 트래픽에 대한 특수 카테고리의 탐지기입니다. 내부 탐지기는 시스템 업데이트와 함께 제공되며 항상 작동합니다.

애플리케이션이 클라이언트 관련 활동을 탐지할 목적으로 설계한 내부 탐지기와 일치하며 특정한 클라이언트 탐지기가 존재하지 않는다면, 일반 클라이언트가 보고될 수 있습니다.

Cisco가 제공하는 클라이언트 탐지기

클라이언트 탐지기는 클라이언트 트래픽을 탐지하고 VDB 또는 시스템 업데이트를 통해 전달되며, Cisco Professional Services의 가져오기를 위해 제공됩니다. 클라이언트 탐지기를 활성화 또는 비활성화할 수 있습니다. 가져온 클라이언트 탐지기만 내보낼 수 있습니다.

Cisco가 제공하는 웹 애플리케이션 탐지기

웹 애플리케이션 탐지기는 HTTP 트래픽 페이로드의 웹 애플리케이션을 탐지하며 VDB 또는 시스템 업데이트를 통해 전달됩니다. 웹 애플리케이션 탐지기는 항상 작동합니다.

Cisco가 제공하는 애플리케이션 프로토콜**(**포트**)** 탐지기

포트 기반 애플리케이션 프로토콜 탐지기는 잘 알려진 포트를 사용하여 네트워크 트래픽을 식별합니다. 이러한 탐지기는 VDB 또는 시스템 업데이트를 통해 전달되며, Cisco Professional Services의 가져오기를 위해 제공됩니다. 애플리케이션 프로토콜 탐지기를 활성화 또는 비활성화할 수 있으며, 탐지기 정의를 확인해 맞춤형 탐지기의 기본 토대로 사용할 수 있습니다.

Cisco가 제공하는 애플리케이션 프로토콜**(Firepower)** 탐지기

Firepower 기반 애플리케이션 프로토콜 탐지기는 Firepower 애플리케이션 핑거프린트를 사용해 네트워크 트래픽을 분석하며 VDB 또는 시스템 업데이트를 통해 전달됩니다. 애플리케이션 프로토콜 탐지기를 활성화 또는 비활성화할 수 있습니다.

맞춤형 애플리케이션 탐지기

맞춤형 애플리케이션 탐지기는 패턴 기반 탐지기입니다. 클라이언트, 웹 애플리케이션 또는 애플리케이션 프로토콜 트래픽의 패킷에 있는 패턴을 탐지합니다. 사용자는 가져온 탐지기와 맞춤형 탐지기에 대한 완전한 제어 권한을 갖습니다.

웹 인터페이스에서 애플리케이션 프로토콜 식별

아래 테이블은 탐지한 애플리케이션 프로토콜을 Firepower System이 식별하는 방법을 설명합니다.

표 ***249:*** 애플리케이션 프로토콜의 ***Firepower System*** 식별

식별	설명
애플리케이션 프로토콜 이름	애플리케이션 프로토콜이 다음 조건을 충족하면 Firepower Management Center은(는) 이름이 있는 애플리케이션 프로토콜을 식별합니다. • 애플리케이션 프로토콜이 시스템에 의해 긍정적으로 식별된 경우 • 애플리케이션 프로토콜이 NetFlow 데이터를 통해 식별되었으며 `/etc/sf/services`에 포트 애플리케이션 프로토콜 상관관계가 있는 경우 • 애플리케이션 프로토콜이 호스트 입력 기능을 통해 수동으로 식별된 경우 • 애플리케이션 프로토콜이 Nmap 또는 다른 활성 소스에 의해 식별된 경우
`pending`	시스템이 애플리케이션을 긍정적으로도 부정적으로도 식별할 수 없는 경우 Firepower Management Center은(는) 애플리케이션 프로토콜을 `pending`으로 식별합니다. 대부분의 경우 시스템은 보류 중인 애플리케이션을 식별하려면 더 많은 데이터를 수집 및 분석해야 합니다. Application Details 및 Servers 테이블과 호스트 프로파일에서 `pending` 상태는 (탐지된 클라이언트 또는 웹 애플리케이션 트래픽에서 추론하는 대신) 특정 애플리케이션 프로토콜 트래픽이 탐지된 애플리케이션 프로토콜에 대해서만 나타납니다.
`unknown`	Firepower Management Center은(는) 다음과 같은 경우 애플리케이션 프로토콜을 `unknown(알 수 없음)`으로 식별합니다. • 애플리케이션이 시스템의 어떤 탐지기와도 일치하지 않는 경우 • 애플리케이션 프로토콜이 NetFlow 데이터를 통해 식별되었지만 `/etc/sf/services`에 포트 애플리케이션 프로토콜 상관관계가 없는 경우
공백	사용 가능한 모든 탐지된 데이터가 검토되었지만 애플리케이션 프로토콜이 식별되지 않았습니다. Application Details 및 Servers 테이블과 호스트 프로파일에서, 탐지된 애플리케이션 프로토콜이 없는 비 HTTP 일반 클라이언트 트래픽에 대해 애플리케이션 프로토콜은 비어 있게 됩니다.

클라이언트 탐지의 암시적 애플리케이션 프로토콜 탐지

모니터링되지 않는 서버에 액세스하는 모니터링되는 호스트가 사용하는 클라이언트를 시스템이 식별할 수 있는 경우, Firepower Management Center은(는) 클라이언트와 상응하는 애플리케이션 프로토콜이 연결에 사용되고 있다고 추론합니다. 시스템은 모니터링되는 네트워크에서만 애플리케이션을 추적하므로, 일반적으로 연결 로그에는 모니터링되는 호스트가 모니터링되지 않는 서버에 액세스하는 연결에 대한 애플리케이션 프로토콜 정보가 포함되지 않습니다.

이 프로세스, 즉 암시작 애플리케이션 프로토콜 탐지는 다음과 같은 결과를 유발합니다.

- 시스템은 이러한 서버에 대해 New TCP Port 또는 New UDP Port 이벤트를 생성하지 않으므로 Servers 테이블에 서버가 나타나지 않습니다. 또한 이러한 애플리케이션 프로토콜의 탐지를 기준으로 사용하여 검색 이벤트 알림 또는 상관관계 규칙을 트리거할 수 없습니다.
- 애플리케이션 프로토콜은 호스트와 연결되지 않으므로 호스트 프로파일의 상세정보를 볼 수 없거나, 서버 ID를 설정할 수 없거나, 트래픽 프로파일 또는 상관관계 규칙에 대한 호스트 프로파일 자격에서 해당 정보를 사용할 수 없습니다. 또한 시스템은 이러한 유형의 탐지를 기반으로 취약성을 호스트와 연결하지 않습니다.

하지만 연결에 존재하는 애플리케이션 프로토콜 정보에 대한 상관관계 이벤트를 트리거할 수는 있습니다. 또한 연결 로그에서 애플리케이션 프로토콜 정보를 사용하여 연결 추적기 및 트래픽 프로파일을 생성할 수 있습니다.

호스트 제한 및 검색 이벤트 로깅

클라이언트, 서버 또는 웹 애플리케이션을 탐지하면, 시스템은 연결된 호스트가 이미 최대 클라이언트, 서버 또는 웹 애플리케이션 수에 도달하지 않은 경우 검색 이벤트를 생성합니다.

호스트 프로파일은 호스트당 클라이언트 최대 16개, 서버 100개, 웹 애플리케이션 100개를 표시합니다.

클라이언트, 서버 또는 웹 애플리케이션의 탐지에 의존하는 작업은 이 제한의 영향을 받지 않습니다. 예를 들어 서버를 트리거하도록 구성된 액세스 컨트롤 규칙은 여전히 연결 이벤트를 기록합니다.

애플리케이션 탐지 특별 고려 사항

SFTP

SFTP 트래픽을 탐지하려면 동일한 규칙에서도 SSH를 탐지해야 합니다.

Squid

다음과 같은 경우 시스템은 Squid 서버 트래픽을 분명하게 식별합니다.

- 시스템은 모니터링되는 네트워크 호스트에서 프록시 인증이 활성화된 Squid 서버로의 연결을 탐지하거나
- 모니터링되는 네트워크의 Squid 프록시 서버에서 대상 시스템(클라이언트가 정보 또는 다른 리소스를 요청하는 대상 서버)으로의 연결을 탐지한 경우

그러나 다음과 같은 경우 시스템은 Squid 서비스 트래픽을 식별할 수 없습니다.

- 모니터링되는 네트워크의 호스트가 프록시 인증이 비활성화된 Squid 서버에 연결하거나,
- Squid 프록시 서버가 HTTP 응답에서 헤더 필드를 제거하도록 구성된 경우

SSL 애플리케이션 탐지

시스템은 세션 내 애플리케이션 프로토콜, 클라이언트 애플리케이션, 또는 웹 애플리케이션을 식별하기 위해 SSL(Secure Socket Layers) 세션의 세션 정보를 사용할 수 있는 애플리케이션 탐지기를 제공합니다.

시스템이 암호화된 연결을 탐지하면 가능한 경우 해당 연결을 SMTPS 등의 일반 HTTPS 연결 또는 보다 특정한 보안 프로토콜로 표시합니다. 시스템이 SSL 세션을 탐지하면 `SSL 클라이언트`를 세션에 대한 연결 이벤트의 클라이언트 필드에 추가합니다 세션에 대한 웹 애플리케이션이 확인될 경우, 시스템에서는 트래픽에 대한 검색 이벤트를 생성합니다.

SSL 애플리케이션 트래픽의 경우 관리되는 디바이스는 서버 인증서에서 일반 이름을 탐지하고 이를 SSL 호스트 패턴의 클라이언트 또는 웹 애플리케이션과 일치시킬 수 있습니다. 시스템이 특정 클라이언트를 식별하는 경우 `SSL 클라이언트`가 해당 클라이언트의 이름으로 변경됩니다.

SSL 애플리케이션 트래픽이 암호화되므로 시스템은 암호화된 스트림에 있는 애플리케이션 데이터가 아닌 인증서의 정보만 사용하여 식별 작업을 수행합니다. 이러한 이유로 인해 SSL 호스트 패턴에서 애플리케이션을 만든 회사만 식별할 수 있는 경우가 간혹 있으므로, 같은 회사에서 제작한 SSL 애플리케이션의 경우 동일한 식별 과정을 거쳤을 수 있습니다.

HTTPS 세션이 HTTP 세션 내에서 실행되는 등의 일부 경우에는 관리되는 디바이스가 클라이언트 측 패킷의 클라이언트 인증서에서 서버 이름을 탐지합니다.

SSL 애플리케이션 식별을 활성화하려면 응답자 트래픽을 모니터링하는 액세스 제어 규칙을 생성해야 합니다. 그러한 규칙에는 SSL 애플리케이션에 대한 애플리케이션 조건 또는 SSL 인증서의 URL을 사용하는 URL 조건이 있어야 합니다. 네트워크 검색 시 응답자 IP 주소는 네트워크 검색 정책에서 모니터링할 네트워크에 반드시 있지 않아도 됩니다. 액세스 제어 정책 설정은 트래픽의 식별 여부를 결정합니다. SSL 애플리케이션에 대해 탐지기를 식별하려면, 애플리케이션 탐지기 목록 또는 액세스 제어 규칙에서 애플리케이션 조건을 추가할 때 `SSL protocol` 태그별로 필터링할 수 있습니다.

참조된 웹 애플리케이션

웹 서버는 종종 광고 서버인 다른 웹 사이트에 대한 트래픽을 가끔 참조합니다. 네트워크에서 발생하는 참조된 트래픽의 문맥을 더 잘 이해할 수 있도록, 시스템은 참조된 세션에 대한 이벤트의 **Web Application(**웹 애플리케이션**)** 필드에 트래픽을 참조한 웹 애플리케이션을 나열합니다. VDB에는 알려진 참조 사이트의 목록이 포함되어 있습니다. 시스템이 이 사이트 중 하나의 트래픽을 탐지하면 해당 트래픽에 대한 이벤트와 함께 참조 사이트가 저장됩니다. 예를 들어 Facebook을 통해 액세스하는 광고가 실제로 Advertising.com에 호스팅되면 탐지된 Advertising.com 트래픽은 Facebook 웹 애플리케이션에 연결됩니다. 시스템은 또한 웹사이트가 다른 사이트에 단순 링크를 제공하는 등의 경우 참조하는 URL을 탐지할 수 있습니다. 이 경우 참조하는 URL이 참조된 이벤트 필드에 나타납니다.

참조하는 애플리케이션이 존재하는 경우 이벤트에는 트래픽에 대한 웹 애플리케이션으로 나열되는 반면 URL은 참조 사이트를 나타냅니다. 위의 예에서 해당 트래픽에 대한 연결 이벤트의 웹 애플리케이션은 Facebook일 수 있지만 URL은 Advertising.com입니다. 참조하는 웹 애플리케이션이 탐지되지

않거나 호스트가 스스로를 참조하거나 참조 연결이 있는 경우 참조하는 웹 애플리케이션이 웹 애플리케이션에 표시될 수 있습니다. 대시보드에서 웹 애플리케이션의 연결 및 바이트 카운트에는 웹 애플리케이션이 스스로 참조한 트래픽과 연결된 세션이 포함됩니다.

참조된 트래픽에 대해 특별히 작동하는 규칙을 생성하는 경우 참조하는 애플리케이션보다 참조된 애플리케이션에 대한 조건을 추가해야 합니다. 예를 들어 Facebook에서 참조되는 Advertising.com 트래픽을 차단하려면 Advertising.com 애플리케이션에 대한 액세스 제어 규칙에 애플리케이션 조건을 추가합니다.

애플리케이션 탐지 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 검색 관리자

맞춤형 애플리케이션 탐지기

네트워크에서 맞춤형 애플리케이션을 이용한다면, 애플리케이션을 식별하는 데 필요한 정보를 시스템에 제공하는 맞춤형 웹 애플리케이션, 클라이언트 또는 애플리케이션 프로토콜 탐지기를 만들 수 있습니다. 애플리케이션 탐지기 유형은 **Protocol(**프로토콜**)**, **Type(**유형**)**, **Direction(**방향**)** 필드에서 선택한 내용에 따라 결정됩니다.

서버 트래픽에서 애플리케이션 프로토콜의 탐지 및 식별을 시작하려면, 클라이언트 세션에 시스템에 대한 서버의 Responder 패킷이 포함되어야 합니다. UDP 트래픽의 경우 시스템은 Responder 패킷의 소스를 서버로 지정합니다.

또 다른 Firepower Management Center에서 이미 탐지기를 생성한 경우 이를 내보낸 다음 이 Firepower Management Center(으)로 가져올 수 있습니다. 그런 다음 가져온 탐지기를 필요에 맞게 편집할 수 있습니다. 맞춤형 탐지기는 물론 Cisco Professional Services에서 제공한 탐지기도 내보내고 가져올 수 있습니다. 하지만 다른 유형의 Cisco 제공 탐지기는 내보내거나 가져올 수 없습니다.

맞춤형 애플리케이션 탐지기 및 사용자 정의 애플리케이션 필드

다음 필드를 이용해 사용자 정의 애플리케이션 탐지기 및 맞춤형 애플리케이션을 설정할 수 있습니다.

맞춤형 애플리케이션 탐지기 필드: 일반

다음 필드를 사용하여 기본 및 고급 맞춤형 애플리케이션 탐지기를 설정합니다.

애플리케이션 프로토콜

탐지할 애플리케이션 프로토콜입니다. 시스템이 제공한 애플리케이션일 수도 있고 사용자 정의 애플리케이션일 수도 있습니다.

애플리케이션이 액티브 인증에서 면제될 수 있게 하려면(ID 규칙에서 설정되게 하려면), **User-Agent Exclusion(**사용자-에이전트 제외**)** 태그가 있는 애플리케이션 프로토콜을 선택하거나 생성해야 합니다.

설명

애플리케이션 탐지기에 대한 설명입니다.

이름

애플리케이션 탐지기의 이름입니다.

탐지기 유형

탐지기의 유형(기본 또는 고급)입니다. 기본 애플리케이션 탐지기는 웹 인터페이스에서 일련의 필드로 생성됩니다. 고급 애플리케이션 탐지기는 외부에서 생성되며 맞춤형 .lua 파일로 업로드됩니다.

맞춤형 애플리케이션 탐지기 필드: 탐지 패턴

다음 필드를 사용하여 기본 맞춤형 애플리케이션 탐지기의 탐지 패턴을 설정합니다.

Direction(방향**)**

탐지기가 검사해야 하는 트래픽의 소스(**Client(**클라이언트**)** 또는 **Server(**서버**)** 입니다.

Offset(오프셋**)**

패킷 페이로드 시작 지점을 기준으로 한 패킷 위치(단위: 바이트)로, 시스템이 패킷 검색을 시작해야 하는 위치를 말합니다.

패킷 페이로드는 바이트 0에서 시작되므로, 패킷 페이로드의 시작 부분부터 진행할 바이트의 수에서 1을 뺀 값으로 오프셋을 계산합니다. 예를 들어 패킷의 5번째 비트에서 패턴을 검색하려면 **Offset** 필드에 4를 입력합니다.

패턴

선택한 **Type(**유형**)**과 연결된 패턴 문자열입니다.

포트

탐지기가 검사해야 하는 트래픽의 포트입니다.

프로토콜

탐지할 프로토콜입니다. 프로토콜 선택에 따라 **Type(**유형**)**과 **URL** 필드 중 무엇을 표시할지가 결정됩니다.

프로토콜(그리고 경우에 따라 **Type(**유형**)** 및 **Direction(**방향**)** 필드의 후속 선택 사항)에 따라 사용자가 생성하는 애플리케이션 탐지기 유형이 결정됩니다(웹 애플리케이션, 클라이언트 또는 애플리케이션 프로토콜).

탐지기 유형	프로토콜	유형 또는 방향
웹 애플리케이션	HTTP	**Type(**유형**)**은 **Content Type(**콘텐츠 유형**)** 또는 **URL**임
	RTMP	Any(모든)
	SSL	Any(모든)
Client(클라이언트)	HTTP	**Type(**유형**)**은 **User Agent(**사용자 에이전트**)** 임
	SIP	Any(모든)
	TCP 또는 UDP	**Direction(**방향**)**은 **Client(**클라이언트**)** 임
애플리케이션 프로토콜	TCP 또는 UDP	**Direction(**방향**)**은 **Server(**서버**)** 임

유형

입력한 패턴 문자열의 유형입니다. 표시되는 옵션은 선택한 **Protocol(**프로토콜**)**에 따라 달라집니다. **RTMP**를 프로토콜로 선택한 경우, **URL** 필드가 **Type(**유형**)** 필드 대신 표시됩니다.

참고 **User Agent(**사용자 에이전트**)**를 **Type(**유형**)**으로 선택한 경우, 시스템은 자동으로 애플리케이션 **Tag(**태그**)**를 **User-Agent Exclusion(**사용자-에이전트 제외**)**으로 설정합니다.

유형 선택	문자열 특징
ASCII	문자열은 ASCII 인코딩됩니다.
공용 이름	문자열은 서버 응답 메시지 내 commonName 필드의 값입니다.
콘텐츠 유형	문자열은 서버 응답 헤더 내 콘텐츠 유형 필드의 값입니다.
16진수	문자열은 16 진수 표기법으로 표시됩니다.
조직 단위	문자열은 서버 응답 메시지 내 organizationName 필드의 값입니다.
SIP 서버	문자열은 메시지 헤더 내 From 필드의 값입니다.
SSL 호스트	문자열은 ClientHello 메시지 내 server_name 필드의 값입니다.

유형 선택	문자열 특징
URL	문자열은 URL입니다. 참고 탐지기는 사용자가 입력한 문자열이 URL 전체 섹션이라고 가정합니다. 예를 들어 **cisco.com**을 입력하면 **www.cisco.com/support** 및 **www.cisco.com**과는 일치하지만 **www.wearecisco.com**과는 일치하지 않습니다.
사용자 에이전트	문자열은 GET 요청 헤더 내 사용자-에이전트 필드의 값입니다. SIP 프로토콜에도 사용 가능하며 문자열은 SIP 메시지 헤더 내 사용자-에이전트 필드의 값임을 나타냅니다.

URL

RTMP 패킷의 C2 메시지 내 swfURL 필드의 전체 URL 또는 URL 섹션입니다. 이 필드는 **RTMP**를 **Protocol(**프로토콜**)**로 선택했을 때 **Type(**유형**)** 필드 대신 표시됩니다.

참고 탐지기는 사용자가 입력한 문자열이 URL 전체 섹션이라고 가정합니다. 예를 들어 **cisco.com**을 입력하면 **www.cisco.com/support** 및 **www.cisco.com**과는 일치하지만 **www.wearecisco.com**과는 일치하지 않습니다.

사용자 정의 애플리케이션 필드

다음 필드를 사용하여 기본 및 고급 맞춤형 애플리케이션 탐지기에서 사용자 정의 애플리케이션을 설정합니다.

사업 타당성

조직의 비즈니스 운영(레크리에이션과 반대) 상황 내에서 애플리케이션이 사용될 가능성(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 또는 **Very Low(**매우 낮음**)**)입니다. 애플리케이션에 가장 알맞은 옵션을 선택합니다.

범주

가장 중요한 기능을 설명하는 일반 애플리케이션 분류

설명

애플리케이션에 대한 설명입니다.

이름

애플리케이션의 이름입니다.

위험

애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 또는 **Very Low(**매우 낮음**)**)입니다. 애플리케이션에 가장 알맞은 옵션을 선택합니다.

태그

애플리케이션에 관한 추가 정보를 제공하는, 하나 이상의 미리 정의된 태그입니다. 애플리케이션이 액티브 인증에서 면제될 수 있게 하려면(ID 규칙에서 설정되게 하려면), **User-Agent Exclusion(**사용자-에이전트 제외**)** 태그를 애플리케이션에 추가해야 합니다.

맞춤형 애플리케이션 탐지기 설정

기본 또는 고급 맞춤형 애플리케이션 탐지기를 설정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **Create a Custom Detector(**맞춤형 탐지기 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Application Protocol(**애플리케이션 프로토콜**)**을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 기존 애플리케이션 프로토콜에 대한 탐지기를 생성하는 경우(예: 비표준 포트에서 특정 애플리케이션 프로토콜을 탐지하려는 경우), 드롭다운 목록에서 애플리케이션 프로토콜을 선택합니다.
- 사용자 정의 애플리케이션에 대한 탐지기를 생성하는 경우에는 사용자 정의 애플리케이션 생성, 2450 페이지에서 설명하는 절차를 따르십시오.

단계 **5** **Detector Type(**탐지기 유형**)**을 선택합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Detection Patterns(**탐지 패턴**)** 또는 **Detection Criteria(**탐지 기준**)**를 설정합니다.

- 기본 탐지기를 설정하는 경우에는, 기본 탐지기에서 탐지 패턴 지정, 2451 페이지에 설명된 대로 미리 설정한 **Detection Patterns(**탐지 패턴**)**를 지정합니다.
- 고급 탐지기를 설정하는 경우에는, 고급 탐지기에서 탐지 기준 지정, 2452 페이지에 설명된 대로 맞춤형 **Detection Criteria(**탐지 기준**)**를 지정합니다.

  주의 고급 맞춤형 탐지기는 복잡하며 유효한 .lua 파일을 구성하는 방법을 알아야 합니다. 잘못 설정된 탐지기는 성능이나 탐지 기능에 악영향을 줄 수 있습니다.

단계 **8** 원한다면 **Packet Captures(**패킷 캡처**)**를 이용해 맞춤형 애플리케이션 프로토콜 탐지기 테스트, 2453 페이지에 설명된 대로 새 탐지기를 테스트합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

참고 애플리케이션을 액세스 컨트롤 규칙에 포함하면 탐지기가 자동으로 활성화되며, 사용 중인 동안에는 비활성화할 수 없습니다.

다음에 수행할 작업

- 탐지기 활성화 및 비활성화, 2456 페이지에 설명된 대로 탐지기를 활성화합니다.

관련 항목

맞춤형 애플리케이션 탐지기 및 사용자 정의 애플리케이션 필드, 2445 페이지

사용자 정의 애플리케이션 생성

여기서 생성하는 애플리케이션, 카테고리 및 태그는 액세스 컨트롤 규칙과 애플리케이션 필터 개체 관리자에서도 사용할 수 있습니다.

주의 사용자 정의 애플리케이션을 생성하면 구축 단계를 거치지 않고 Snort 프로세스가 바로 재시작합니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 시작합니다.

프로시저

단계 **1** Create Detector(탐지기 생성) 페이지에서 **Add(**추가**)**를 클릭합니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** **Description(**설명**)**을 입력합니다.

단계 **4** **Business Relevance(**사업 타당성**)**를 선택합니다.

단계 **5** **Risk(**위험**)**를 선택합니다.

단계 **6** 카테고리를 추가하려면 Categories 옆에 있는 **Add(**추가**)**를 클릭하고 새 카테고리 이름을 입력하거나, **Categories(**카테고리**)** 드롭다운 목록에서 기존 카테고리를 선택합니다.

단계 **7** 선택 사항으로, 태그를 추가하려면 Tags(태그) 옆에 있는 **Add(**추가**)**를 클릭하고 새 태그 이름을 입력하거나 **Tags(**태그**)** 드롭다운 목록에서 기존 태그를 선택합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

관련 항목

맞춤형 애플리케이션 탐지기 및 사용자 정의 애플리케이션 필드, 2445 페이지

기본 탐지기에서 탐지 패턴 지정

특정 패턴 문자열의 애플리케이션 프로토콜 패킷 헤더를 검색하도록 맞춤형 애플리케이션 프로토콜 탐지기를 설정할 수 있습니다. 여러 패턴을 검색하도록 탐지기를 구성할 수도 있습니다. 이 경우 애플리케이션 프로토콜을 긍정적으로 식별하려면 애플리케이션 프로토콜 트래픽은 탐지기에 대한 모든 패턴을 매칭해야 합니다.

애플리케이션 프로토콜 탐지기는 ASCII 또는 16진수 패턴을 검색할 수 있습니다(임의의 오프셋 사용).

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 시작합니다.

프로시저

단계 **1** Detection Patterns(탐지 패턴) 섹션의 Create Detector(탐지기 생성) 페이지에서 **Add(추가)**를 클릭합니다.

단계 **2** 탐지기가 검사해야 하는 트래픽의 **Protocol(프로토콜)**을 선택합니다.

단계 **3** 탐지할 패턴 **Type(유형)**을 지정합니다.

단계 **4** 지정한 **Type(유형)**과 일치하는 **Pattern String(패턴 문자열)**을 입력합니다.

단계 **5** 원한다면 **Offset(오프셋)**을 입력합니다(단위: 바이트).

단계 **6** 사용하는 포트를 기준으로 애플리케이션 프로토콜 트래픽을 식별하려면 **Port(s)(포트)** 필드에 1~65535 범위의 포트를 입력합니다. 여러 포트를 사용하려면 쉼표로 구분합니다.

단계 **7** 원한다면 **Direction(방향)**을 선택합니다. **`Client`(클라이언트)** 또는 **`Server`(서버)**를 선택할 수 있습니다.

단계 **8** **OK(확인)**를 클릭합니다.

팁 패턴을 삭제하려면 삭제할 패턴 옆에 있는 삭제( )을 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

관련 항목

고급 탐지기에서 탐지 기준 지정, 2452 페이지

고급 탐지기에서 탐지 기준 지정

주의 고급 맞춤형 탐지기는 복잡하며 유효한 .lua 파일을 구성하는 방법을 알아야 합니다. 잘못 설정된 탐지기는 성능이나 탐지 기능에 악영향을 줄 수 있습니다.

주의 신뢰할 수 없는 소스의 .lua 파일을 업로드하지 마십시오.

맞춤형.lua 파일은 맞춤형 애플리케이션 탐지기 설정을 포함합니다. 맞춤형 .lua 파일을 생성하려면 lua 프로그래밍 언어를 잘 알고 Cisco의 C-lua API에 익숙해야 합니다. Cisco는 다음을 이용해 .lua 파일을 준비할 것을 적극 권장합니다.

- lua 프로그래밍 언어에 대한 서드파티 지침 및 참조 자료
- 오픈 소스 탐지기 개발자 안내서: https://www.snort.org/downloads
- OpenAppID Snort 커뮤니티 리소스: http://blog.snort.org/search/label/openappid

참고 시스템은 시스템 호출이나 파일 I/O를 참조하는 .lua 파일은 지원하지 않습니다.

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지의 설명에 따라 사용자 정의 애플리케이션 프로토콜 탐지기 설정을 시작합니다.
- 비교 가능한 탐지기에 대한 .lua 파일을 다운로드하고 조사해 유효한 .lua 파일 생성을 준비합니다. 탐지기 파일 다운로드에 관한 자세한 내용은 탐지기 상세정보 보기 또는 다운로드, 2454 페이지 섹션을 참조하십시오.
- 맞춤형 애플리케이션 탐지기 설정을 포함하는 유효한 .lua 파일을 생성합니다.

프로시저

단계 1 Detection Criteria(탐지 기준) 섹션에 있는 고급 맞춤형 애플리케이션 탐지기의 Create Detector(탐지기 생성) 페이지에서 **Add(추가)**를 클릭합니다.

단계 2 **Browse...(찾기...)**를 클릭해 `.lua` 파일로 이동하고 파일을 다운로드합니다.

단계 3 **OK(확인)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

관련 항목

기본 탐지기에서 탐지 패턴 지정, 2451 페이지

맞춤형 애플리케이션 프로토콜 탐지기 테스트

탐지하려는 애플리케이션 프로토콜에서 온 트래픽의 패킷을 포함하는 패킷 캡처(pcap) 파일이 있는 경우 pcap 파일을 기준으로 맞춤형 애플리케이션 프로토콜 탐지기를 테스트할 수 있습니다. Cisco는 불필요한 트래픽이 없는 단순하고 깔끔한 pcap 파일 사용을 권장합니다.

Pcap 파일은 256KB 이하여야 합니다. 그보다 큰 pcap 파일을 기준으로 탐지기를 테스트하면, Firepower Management Center은(는) 파일을 자동으로 자른 다음 불완전한 파일을 테스트합니다. 파일을 이용해 탐지기를 테스트하려면 먼저 pcap에 있는 해결되지 않은 체크섬을 수정해야 합니다.

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기를 설정합니다.

프로시저

단계 1 Packet Captures(패킷 캡처) 섹션의 Create Detector(탐지기 생성) 페이지에서 **Add(추가)**를 클릭합니다.

단계 2 팝업 윈도우에서 pcap 파일을 찾아 **OK(확인)**를 클릭합니다.

단계 3 pcap 파일의 내용을 기준으로 탐지기를 테스트하려면 pcap 파일 옆에 있는 Evaluate(평가)를 클릭합니다. 테스트의 성공 여부를 나타내는 메시지가 표시됩니다.

단계 4 선택적으로, 추가 pcap 파일을 기준으로 탐지기를 테스트하려면 1~3단계를 반복합니다.

팁 pcap 파일을 삭제하려면 삭제할 파일 옆에 있는 삭제( )를 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

탐지기 상세정보 보기 또는 다운로드

탐지기 목록을 사용하여 애플리케이션 탐지기 상세정보(모든 탐지기에 해당)를 확인하고 탐지기 상세정보를 다운로드할 수 있습니다(맞춤형 애플리케이션 탐지기에만 해당).

프로시저

단계 **1** 애플리케이션 탐지기 상세정보를 확인하려면 다음 하나를 수행하십시오.

- https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html에서 관련 VDB 버전에 대한 *Cisco Firepower* 애플리케이션 탐지기 참조를 확인하십시오.
- a. **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

  b. 목록을 필터링해 특정 탐지기를 찾습니다.

  c. 클릭합니다. 정보()

단계 **2** 맞춤형 애플리케이션 탐지기에 대한 탐지기 세부 사항을 다운로드하려면 다운로드()를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 설정이 상위 도메인에 속하거나 필요한 권한이 없는 것입니다.

탐지기 목록 정렬

기본적으로 Detectors(탐지기) 페이지에는 탐지기가 이름별 알파벳순으로 나열됩니다. 열 제목 옆에 있는 위쪽 또는 아래쪽 화살표는 페이지가 해당 방향에서 해당 열을 기준으로 정렬된다는 것을 나타냅니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** 적절한 컬럼 헤드를 클릭합니다.

탐지기 목록 필터링

프로시저

단계 1 **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 2 탐지기 목록에 대한 필터 그룹, 2455 페이지에서 설명하는 필터 그룹 중 하나를 확장하고 필터 옆에 있는 확인란을 선택합니다. 그룹의 모든 필터를 선택하려면 그룹 이름을 마우스 오른쪽 버튼으로 클릭하고 **Check All(**모두 선택**)**을 선택합니다.

단계 3 필터를 제거하려면 **Filters(**필터**)** 필드의 필터 이름에서 제거( )를 클릭하거나 필터 목록에서 필터를 비활성화합니다. 그룹의 모든 필터를 제거하려면 그룹 이름을 마우스 오른쪽 버튼으로 클릭하고 **Uncheck All(**모두 선택 해제**)**을 선택합니다.

단계 4 필터를 모두 제거하려면, 탐지기에 적용된 목록 옆에 있는 **Clear all(**모두 선택 취소**)**을 클릭합니다.

탐지기 목록에 대한 필터 그룹

탐지기 목록을 필터링할 때는 여러 필터 그룹을 독립적으로나 조합해서 사용할 수 있습니다.

이름

입력한 문자열이 들어 있는 이름이나 설명의 탐지기를 찾습니다. 문자열은 영숫자나 특수 문자를 포함할 수 있습니다.

사용자 지정 필터

개체 관리 페이지에서 생성된 맞춤형 애플리케이션 필터와 일치하는 탐지기를 찾습니다.

작성자

탐지기를 생성한 사용자에 따라 탐지기를 찾습니다. 탐지기를 다음 기준으로 필터링할 수 있습니다.

- 맞춤형 탐지기를 생성하거나 가져온 개별 사용자
- Cisco - Cisco가 제공한 모든 탐지기를 나타냅니다. 단, 개별적으로 가져온 애드온 탐지기는 예외입니다(탐지기를 가져온 사용자는 탐지기의 작성자가 됩니다).
- **Any User** 0 Cisco에서 제공하지 않은 모든 탐지기를 나타냅니다.

주/도

상태(**Active** 또는 **Inactive**)에 따라 탐지기를 찾습니다.

유형

애플리케이션 탐지기 기초, 2440 페이지에서 설명하는 것처럼 탐지기 유형에 따라 탐지기를 찾습니다.

프로토콜

탐지기가 검사하는 트래픽 프로토콜에 따라 탐지기를 찾습니다.

카테고리

탐지하는 애플리케이션에 할당된 카테고리에 따라 탐지기를 찾습니다.

태그

탐지하는 애플리케이션에 할당된 태그에 따라 탐지기를 찾습니다.

위험

탐지하는 애플리케이션에 할당된 위험(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 및 **Very Low(**매우 낮음**)**에 따라 탐지기를 찾습니다.

사업 타당성

탐지하는 애플리케이션에 할당된 비즈니스 연관성(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 및 **Very Low(**매우 낮음**)**에 따라 탐지기를 찾습니다.

다른 탐지기 페이지로 이동

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** 다음 페이지를 보려면 오른쪽 화살표(>)을 클릭합니다.

단계 **3** 이전 페이지를 보려면 왼쪽 화살표(<)을 클릭합니다.

단계 **4** 다른 페이지를 보려면 페이지 번호를 입력하고 Enter를 누릅니다.

단계 **5** 마지막 페이지로 이동하려면 오른쪽 끝 화살표(>|)을 클릭합니다.

단계 **6** 첫 페이지로 이동하려면 왼쪽 끝 화살표(|<)을 클릭합니다.

탐지기 활성화 및 비활성화

네트워크 트래픽 분석에 사용할 수 있으려면 탐지기를 먼저 활성화해야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다.

시스템의 탐지 기능을 보완하기 위해 포트마다 여러 애플리케이션 탐지기를 활성화할 수 있습니다.

정책의 액세스 제어 규칙에 애플리케이션이 포함되어 있고 정책이 구축될 때 해당 애플리케이션에 대한 활성 탐지기가 없으면 하나 이상의 탐지기가 자동으로 활성화됩니다. 마찬가지로, 구축된 정책에서 애플리케이션이 사용 중일 때 탐지기를 비활성화하여 해당 애플리케이션에 대한 활성 탐지기가 없어지면 탐지기를 비활성화할 수 없습니다.

팁 성능을 높이려면 사용하지 않을 애플리케이션 프로토콜, 클라이언트 또는 웹 애플리케이션 탐지기를 비활성화하십시오.

주의 맞춤형 애플리케이션 탐지기를 활성화하거나 비활성화하면 구축 프로세스를 거치지 않고 Snort 프로세스가 바로 재시작됩니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** 활성화하거나 비활성화할 탐지기 옆에 있는 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

참고 일부 애플리케이션 탐지기는 다른 탐지기에 필요합니다. 이러한 탐지기 중 하나를 비활성화하면 여기에 의존하는 탐지기도 비활성화됨을 알리는 경고가 나타납니다.

맞춤형 애플리케이션 탐지기 편집

다음 절차를 이용해 맞춤형 애플리케이션 탐지기를 수정하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** 수정할 탐지기 옆에 있는 수정( )을 클릭합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 맞춤형 애플리케이션 탐지기 설정, 2449 페이지에 설명된 대로 탐지기를 변경합니다.

단계 **4** 탐지기의 상태에 따라 다음 저장 옵션을 사용할 수 있습니다.

- 비활성 탐지기를 저장하려면 **Save(**저장**)**를 클릭합니다.
- 비활성 탐지기를 새로운 비활성 탐지기로 저장하려면 **Save as New(**새 탐지기로 저장**)**를 클릭합니다.
- 활성 탐지기를 저장하고 바로 사용하려면 **Save and Reactivate(**저장 및 재활성화**)**를 클릭합니다.

  주의 사용자 정의 애플리케이션 탐지기를 저장하고 재활성화하면 구축 프로세스를 거치지 않고 Snort 프로세스가 바로 재시작됩니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

- 활성 탐지기를 새로운 비활성 탐지기로 저장하려면 **Save as New(**새 탐지기로 저장**)**를 클릭합니다.

탐지기 삭제

맞춤형 탐지기는 물론 Cisco Professional Services에서 제공한 추가 탐지기도 개별적으로 삭제할 수 있습니다. 다른 Cisco 제공 탐지기는 삭제할 수 없지만, 이중 다수는 비활성화할 수 있습니다.

참고 구축된 정책에서 탐지기를 사용하는 경우에는, 해당 탐지기를 삭제할 수 없습니다.

주의 활성화된 사용자 정의 애플리케이션 탐지기를 삭제하면 구축 프로세스를 거치지 않고 Snort 프로세스가 바로 재시작됩니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** 삭제할 탐지기 옆에 있는 삭제( )를 클릭합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 3 **OK(**확인**)**를 클릭합니다.

97 장

영역 생성 및 관리

다음 주제에서는 사용자 인식 및 제어를 위한 사용자 저장소인, 영역을 생성하고 관리하는 방법을 설명합니다.

- 영역 및 영역 시퀀스 정보, 2461 페이지
- 영역 라이선스 요건, 2465 페이지
- 영역 요구 사항 및 사전 요건, 2466 페이지
- 영역 생성, 2466 페이지
- 영역 시퀀스 생성, 2477 페이지
- 영역 관리, 2479 페이지
- 영역 비교, 2479 페이지
- 영역 및 사용자 다운로드 문제 해결, 2480 페이지
- 영역 히스토리, 2484 페이지

영역 및 영역 시퀀스 정보

영역은 Firepower Management Center와 사용자가 모니터링하는 서버의 사용자 계정 간 연결을 의미합니다. 또한 서버의 연결 설정 및 인증 필터 설정을 지정합니다. 영역에는 다음과 같은 기능이 있습니다.

- 활동을 모니터링할 사용자 및 사용자 그룹을 지정할 수 있습니다.
- 신뢰할 수 있는 사용자는 물론 일부 신뢰할 수 없는 사용자, 즉 트래픽 기반 탐지로 탐지한 POP3 및 IMAP 사용자와 트래픽 기반 탐지로 탐지한 사용자, , 또는 ISE/ISE-PIC의 사용자 메타데이터에 대한 사용자 저장소를 쿼리합니다.

영역 시퀀스는 ID 정책에 사용할 두 개 이상의 영역으로 구성된 순서가 지정된 목록입니다. 영역 시퀀스를 ID 규칙과 연결할 경우 Firepower System은 영역 시퀀스에 지정된 순서대로 Active Directory 도메인을 검색합니다.

한 영역 내에 여러 도메인 컨트롤러를 디렉터리로 추가할 수 있지만, 이러한 컨트롤러는 같은 기본 영역 정보를 공유해야 합니다. 영역 내의 디렉터리는 모두 LDAP 서버이거나 모두 AD(Active Directory) 서버여야 합니다. 영역을 활성화하고 나면 다음번에 Firepower Management Center이 서버를 쿼리할 때 저장한 변경 사항이 적용됩니다.

사용자 인식을 수행하려면 영역에 지원되는 서버에 대해 영역을 구성해야 합니다. 시스템은 이러한 연결을 이용해 POP3 및 IMAP 사용자에 연결된 데이터의 서버를 쿼리하고, 트래픽 기반 탐지를 통해 검색한 LDAP 사용자 관련 데이터를 수집합니다.

시스템은 POP3 및 IMAP 로그인에서 이메일 주소를 사용하여 Active Directory, OpenLDAP의 LDAP 사용자에 대해 상관관계를 지정합니다. 예를 들어 매니지드 디바이스가 LDAP 사용자와 동일한 이메일 주소의 사용자에 대해 POP3 로그인을 탐지하면, 시스템은 LDAP 사용자의 메타데이터를 해당 사용자와 연결합니다.

사용자 제어를 수행하려는 경우 다음을 구성할 수 있습니다.

- ISE/ISE-PIC용 AD 서버의 영역 또는 영역 시퀀스
- AD 서버 또는 캡티브 포털용 LDAP 서버의 영역 또는 영역 시퀀스

사용자 다운로드 정보

Firepower Management Center과 LDAP 또는 AD 서버 간 연결을 구성하는 영역 또는 영역 시퀀스를 설정해 탐지한 특정 사용자에 대한 사용자 및 사용자 그룹 메타데이터를 검색할 수 있습니다.

- 사용자 에이전트 또는 ISE/ISE-PIC에서 보고하거나 종속 포털을 통해 인증하는 LDAP 및 AD 사용자. 이 메타데이터는 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 트래픽 기반 탐지에서 탐지된 POP3 및 IMAP 사용자 로그인(해당 사용자의 이메일 주소가 LDAP 또는 AD 사용자와 동일한 경우). 이 메타데이터는 사용자 인식에 사용할 수 있습니다.

영역에서 LDAP 서버나 Active Directory 도메인 컨트롤러 연결을 디렉터리로 설정할 수 있습니다. 사용자 인식 및 사용자 제어용으로 영역의 사용자 및 사용자 그룹 데이터를 다운로드하려면 **Download users and user groups for access control(**액세스 컨트롤을 위해 사용자 및 사용자 그룹 다운로드**)**을 선택해야 합니다.

Firepower Management Center에서는 각 사용자에 대한 다음과 같은 정보 및 메타데이터를 얻습니다.

- LDAP 사용자 이름
- 이름 및 성
- 이메일 주소
- 부서
- 전화 번호

사용자 활동 데이터 정보

사용자 활동 데이터는 사용자 활동 데이터베이스에 저장되며 사용자 ID 데이터는 사용자 데이터베이스에 저장됩니다. 액세스 컨트롤에서 저장하고 사용할 수 있는 최대 사용자 수는 Firepower Management Center 모델에 따라 달라집니다. 포함할 사용자 및 그룹을 선택할 때는 총 사용자 수가 모델 제한보다 작은지 확인하십시오. 액세스 컨트롤 파라미터가 너무 광범위하면, Firepower Management Center에서는 최대한 많은 사용자의 정보를 가져오며 검색에 실패한 사용자 수를 메시지 센터의 Tasks(작업) 탭 페이지에 보고합니다.

선택적으로 매니지드 디바이스가 사용자 인식 데이터를 감시하는 서브넷을 제한하기 위해 *Cisco Firepower Threat Defense* 명령 참조에 설명된 대로 **configure identity-subnet-filter** 명령을 사용할 수 있습니다.

참고 사용자 저장소에서 시스템이 탐지한 사용자를 제거할 경우, Firepower Management Center은(는) 절대로 사용자 데이터베이스에서 해당 사용자를 제거하지 않습니다. 반드시 수동으로 삭제해야 합니다. 그러나 Firepower Management Center이(가) 신뢰할 수 있는 사용자 목록을 다음에 업데이트할 때 LDAP 변경 사항이 액세스 컨트롤 규칙에 반영됩니다.

비디오 영역 만들기에 대한 YouTube 비디오.

영역 및 신뢰할 수 있는 도메인

Firepower Management Center에서 영역을 구성하는 경우, 영역은 Active Directory 또는 LDAP 도메인에 연결됩니다.

서로를 신뢰하는 Microsoft Active Directory (AD) 도메인은 일반적으로 *forest(*포레스트*)*라고 합니다. 이 신뢰 관계는 도메인이 다양한 방법으로 서로의 리소스에 액세스하게 할 수 있습니다. 예를 들어 도메인 A에 정의된 사용자 계정은 도메인 B에 정의된 그룹의 멤버로 표시할 수 있습니다.

Firepower System 및 신뢰할 수 있는 도메인

Firepower System은 신뢰할 수 있는 AD 도메인을 지원하지 않습니다. 즉 Firepower System은 설정한 어떤 도메인이 서로 신뢰하는지 추적하지 않으며, 어떤 도메인이 상위 또는 하위 도메인이지 알지 못합니다. 또한 Firepower System은 교차 도메인 신뢰를 이용하는 환경에 대한 지원을 보장하도록 테스트되지 않았으며, 신뢰 관계가 Firepower System 외부에서 실행되었다 하더라도 마찬가지입니다.

영역에 지원되는 서버

다음과 같은 서버 유형에 연결하도록 영역을 구성할 수 있습니다. 단, Firepower Management Center에서 TCP/IP를 통해 이러한 서버에 액세스할 수 있어야 합니다.

서버 유형	사용자 에이전트 데이터 검색용으로 지원되는지 여부	**ISE** 데이터 검색용으로 지원되는지 여부	캡티브 포털 데이터 검색용으로지원되는지 여부	**RA VPN** 데이터 검색용으로 지원되는지 여부
Windows Server 2008및 Windows Server 2012의 Microsoft Active Directory	예	예	예	예
Linux의 OpenLDAP	아니요	아니요	예	예

서버 유형	ISE/ISE-PIC 데이터 검색용으로 지원되는지 여부	TS 에이전트 데이터 검색용으로 지원되는지 여부	캡티브 포털 데이터 검색용으로 지원되는지 여부
Windows Server 2012, 2016 및 2019의 Microsoft Active Directory	예	예	예
Linux의 OpenLDAP	아니요	아니요	예

참고 TS 에이전트가 다른 패시브 인증 ID 소스(ISE/ISE-PIC)와 공유하는 Microsoft Active Directory Windows Server에 설치된 경우, Firepower Management Center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 수동 ID 소스가 동일한 IP 주소별로 활동을 보고할 경우, TS 에이전트 데이터만 Firepower Management Center에 로깅됩니다.

서버 그룹 컨피그레이션과 관련하여 다음 사항에 유의하십시오.

- 사용자 그룹 또는 그룹 내의 사용자에 대해 사용자 제어를 수행하려면 LDAP 또는 Active Directory 서버에서 사용자 그룹을 구성해야 합니다.
- 그룹 이름은 LDAP가 내부에서 사용하기 때문에 `s-`로 시작해선 안 됩니다.

  그룹 이름과 조직 단위 이름에는 별표(*), 등호(=), 백슬래시(\) 같은 특수문자가 있으면 안 됩니다. 특수문자가 있으면 해당 그룹이나 조직 단위의 사용자는 다운로드되지 않으며 ID 정책에 사용할 수 없습니다.
- 서버의 하위 그룹 멤버인 사용자를 추가하거나 제외하는 Active Directory 영역을 설정하는 경우, Microsoft는 Windows Server 2012에서 Active Directory의 그룹당 사용자 수가 5,000명 이하일 것을 권장합니다. 자세한 내용은 MSDN의 Active Directory 최대 제한 - 확장성을 참조하십시오.

  필요한 경우 Active Directory 서버 구성을 수정하여 이러한 기본값 제한을 늘리고 더 많은 사용자를 수용할 수 있습니다.

지원되는 서버 개체 클래스 및 속성 이름

영역의 서버가 반드시 다음 표에 나와 있는 속성 이름을 사용해야 Firepower Management Center에서 해당 서버의 사용자 메타데이터를 검색합니다. 서버에서 속성 이름이 잘못된 경우 Firepower Management Center에서는 해당 속성의 정보를 데이터베이스에 입력할 수 없습니다.

표 *250: Firepower Management Center* 필드에 대한 속성 이름 지도

메타데이터	**FMC** 특성	**LDAP ObjectClass**	**Active Directory** 속성	**OpenLDAP** 속성
LDAP 사용자 이름	사용자 이름	• user • inetOrgPerson	samaccountname	cn uid
이름	First Name(이름)		givenname	givenname
last name(성)	Last Name(성)		sn	sn
email address(이메일 주소)	Email(이메일)		mail userprincipalname(메일에 값이 없는 경우)	mail
department	부서		department distinguishedname(부서에 값이 없는 경우)	ou
전화번호	전화번호		telephonenumber	telephonenumber

참고 그룹에 대한 LDAP ObjectClass는 `group`, `groupOfNames`, (`group-of-names` for Active Directory) 또는 `groupOfUniqueNames`입니다.

ObjectClasses 및 속성에 대한 자세한 내용은 다음 참조 자료를 참조하십시오.

- Microsoft Active Directory:
  - ObjectClasses: MSDN의 모든 클래스
  - Attributes: MSDN의 모든 속성
- OpenLDAP: RFC 4512

영역 라이선스 요건

FTD 라이센스

Any(모든 상태)

기본 라이선스

제어

영역 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

영역 생성

다음 절차를 수행하면 영역(FMC와 Active Directory 포리스트 간 연결) 및 디렉터리(FMC와 LDAP 서버 또는 Active Directory 도메인 컨트롤러 간 연결)를 만들 수 있습니다.

(권장) FMC에서 Active Directory 서버로 안전하게 연결하려면 먼저 다음 작업을 수행합니다.

- Active Directory 서버의 루트 인증서 내보내기, 2473 페이지
- Active Directory 서버 이름 찾기, 2472 페이지

Microsoft는 Active Directory 서버가 2020년에 LDAP 바인딩 및 LDAP 서명을 시행할 것이라고 발표했습니다. Microsoft는 이러한 설정을 기본 설정으로 사용할 때 Microsoft Windows에 권한 상승 취약점이 존재하여 MITM(man-in-the-middle) 공격자가 Windows LDAP 서버에 인증 요청을 성공적으로 전달할 수 있기 때문에 이러한 요구 사항을 적용하고 있습니다. 자세한 내용은 Microwoft 지원 사이트에서 2020 LDAP 채널 바인딩 및 Windows용 LDAP 서명 요구 사항을 참조하십시오.

영역 디렉터리 설정 필드에 대한 자세한 내용은 영역 필드, 2467 페이지 및 영역 디렉토리 및 다운로드 동기화, 2470 페이지의 내용을 참조하십시오.

참고 모든 Microsoft Active Directory(AD) 영역에 대한 고유 **AD Primary Domain(AD** 기본 도메인)을 지정해야 합니다. 다른 AD 영역에 동일한 **AD Primary Domain(AD** 기본 도메인)을 지정할 수는 있지만, 시스템이 제대로 작동하지 않습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다.

프로시저

단계 1 Firepower Management Center에 로그인합니다.

단계 2 **System(**시스템**)** > **Integration(**통합**)** 버튼을 클릭합니다.

단계 3 **Realms(**영역**)**를 클릭합니다.

단계 4 새 영역을 생성하려면 **Add Realm(**영역 추가**)**을 클릭합니다.

단계 5 다른 작업(영역 활성화, 비활성화, 삭제 등)을 수행하는 방법은 영역 관리, 2479 페이지 섹션을 참조하십시오.

단계 6 영역 필드, 2467 페이지에 설명된 대로 영역 정보를 입력합니다.

단계 7 (선택 사항). **Test(**테스트**)**를 클릭해 영역에 대한 연결을 테스트합니다.

참고 Microsoft Active Directory 영역 테스트가 성공하려면, **AD Join Username(AD** 죠인 사용자 이름**)**과 **AD Join Password(AD** 죠인 비밀번호**)** 필드 모두에 값을 입력해야 하며 사용자는 컴퓨터를 도메인에 추가할 수 있는 권한이 있어야 합니다. 자세한 내용은 영역 필드, 2467 페이지를 참고하십시오.

단계 8 **OK(**확인**)**를 클릭합니다.

단계 9 에 설명된 대로영역 디렉터리 설정, 2475 페이지 디렉터리를 한 개 이상 설정합니다.

단계 10 사용자 및 그룹 다운로드, 2476 페이지에서 논의한 대로 사용자 및 사용자 그룹 다운로드(액세스 컨트롤에 필요)를 설정합니다.

단계 11 **Realm Configuration(**영역 설정**)**을 클릭합니다.

단계 12 **ISE/ISE-PIC Users(ISE/ISE-PIC** 사용자**)**, **TS Agent Users(TS** 에이전트 사용자**)**, **Captive Portal Users(**종속 포털 사용자**)**, **Failed Captive Portal Users(**실패한 종속 포털 사용자**)**, 및 **Guest Captive Portal Users(**게스트 종속 포털 사용자**)**에 대한 사용자 세션 시간 초과 값을 분 단위로 입력합니다.

단계 13 영역 설정을 완료했으면 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 영역 디렉터리 설정, 2475 페이지
- 영역을 편집, 삭제, 활성화 또는 비활성화합니다(영역 관리, 2479 페이지 참조).
- 영역 비교, 2479 페이지에 전달하는 고성능 고속 어플라이언스입니다.
- 필요한 경우 작업 상태를 모니터링합니다. 작업 메시지 보기, 445 페이지를 참조하십시오.

영역 필드

다음 필드는 영역을 구성하는 데 사용됩니다.

영역 컨피그레이션 필드

이러한 설정은 영역의 모든 Active Directory 서버 또는 (디렉터리라고도 하는) 도메인 컨트롤러에 적용됩니다.

이름

영역의 고유한 이름입니다.

- ID 정책에 영역을 사용하려는 경우, 시스템은 영숫자 및 특수 문자를 지원합니다.
- RA VPN 설정에서 영역을 사용하려는 경우, 시스템에서는 영숫자와 하이픈(-), 밑줄(_), 더하기(+) 문자를 지원합니다.

설명

(선택 사항). 영역에 대한 설명을 입력합니다.

유형

영역의 유형으로, Microsoft Active Directory의 경우에는 **AD**이며 다른 지원되는 저장소의 경우에는 **LDAP**입니다. 지원되는 LDAP 저장소 목록은 영역에 지원되는 서버, 2463 페이지 섹션을 참조하십시오. LDAP 리포지토리를 사용하여 종속 포털 사용자를 인증할 수 있습니다. 다른 모든 경우에는 Active Directory가 필요합니다.

참고 캡티브 포털만 LDAP 영역을 지원합니다.

AD Primary Domain(AD 기본 도메인)

Microsoft Active Directory 영역에만 해당됩니다. 사용자가 인증해야 하는 Active Directory 서버의 도메인입니다.

참고 모든 Microsoft Active Directory(AD) 영역에 대한 고유 **AD Primary Domain(AD 기본 도메인)**을 지정해야 합니다. 다른 AD 영역에 동일한 **AD Primary Domain(AD 기본 도메인)**을 지정할 수는 있지만, 시스템이 제대로 작동하지 않습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다.

Directory Username and Directory Password(디렉토리 사용자 이름 및 디렉토리 비밀번호)

검색하려는 사용자 정보에 대한 적절한 액세스 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다.

다음에 유의하십시오.

- Microsoft Active Directory의 경우 사용자는 상승된 권한이 없어도 됩니다. 도메인에 어떤 사용자라도 지정할 수 있습니다.
- OpenLDAP의 경우 사용자의 액세스 권한은 OpenLDAP 사양 섹션 8에서 설명하는 `<level>` 파라미터에 의해 결정됩니다. 사용자의 `<level>`은 `auth` 이상이어야 합니다.

- 사용자 이름은 완전 해야 합니다 (예: **administrator@mydomain.com**, 관리자 아님).

Base DN(기본 **DN)**

Firepower Management Center이 사용자 데이터 검색을 시작해야 하는 서버의 디렉토리 트리입니다.

일반적으로, 기본 DN(distinguished name)은 회사 도메인 이름 및 운영 단위를 나타내는 기본 구조를 가지고 있습니다. 예를 들어, 예시 회사의 보안조직은 **ou=security,dc=example,dc=com**의 기본 DN을 가질 수 있습니다.

Group DN(그룹 **DN)**

Firepower Management Center이 그룹 속성으로 사용자를 검색해야 하는 서버의 디렉토리 트리입니다. 지원되는 그룹 속성 목록은 지원되는 서버 개체 클래스 및 속성 이름, 2464 페이지에서 확인할 수 있습니다.

참고 그룹 이름과 조직 단위 이름에는 별표(*), 등호(=), 백슬래시(\) 같은 특수문자가 있으면 안 됩니다. 해당 그룹의 사용자는 다운로드되지 않으며 ID 정책에 사용할 수 없기 때문입니다.

Group Attribute(그룹 속성**)**

(선택 사항). 서버, 구성원 또는 고유 구성원의 그룹 속성입니다.

아래 필드는 기존 영역을 편집할 때만 사용할 수 있습니다.

사용자 세션 시간 초과

사용자 세션이 시간 초과될 때까지의 시간을 분 단위로 입력합니다. 기본값은 사용자 로그인 이벤트 후 1,440(24시간)입니다. 시간이 초과되면 사용자의 세션은 종료됩니다. 사용자가 다시 로그인하지 않고 계속 액세스하면, 해당 사용자는 Firepower Management Center가 Unknown(알 수 없음)으로 간주합니다(**Failed Captive Portal Users(**실패한 캡티브 포털 사용자**)** 제외).

다음에 대한 시간 초과 값을 설정할 수 있습니다.

- 사용자 에이전트 및 **ISE/ISE-PIC** 사용자: 사용자 에이전트 또는 ISE/ISE-PIC가 추적하는 사용자의 시간 초과 값으로, 패시브 인증의 유형입니다.

  지정하는 시간 초과 값은 pxGrid SXP 세션 주제 구독(예: 대상 SGT 매핑)에 적용되지 않습니다. 대신 ISE에서 지정된 매핑에 대한 삭제 또는 업데이트 메시지가 없는 한 세션 주제 매핑이 유지됩니다.

  ISE/ISE-PIC에 대한 자세한 내용은 ISE/ISE-PIC ID 소스, 2485 페이지의 내용을 참조하십시오.

- 캡티브 포털 사용자: 캡티브 포털을 이용해 무사히 로그인한 사용자의 시간 초과 값으로, 액티브 인증의 유형입니다. 자세한 내용은 캡티브 포털 ID 소스, 2505 페이지를 참고하십시오.

- 실패한 캡티브 포털 사용자: 캡티브 포털을 사용하여 무사히 로그인하지 못한 사용자의 시간 초과 값입니다. Firepower Management Center가 사용자를 Failed Auth User(실패한 인증 사용자)로 간주하기 전의 최대 로그인 시도 횟수를 설정할 수 있습니다. Failed Auth User(실패

한 인증 사용자)는 액세스 컨트롤 정책을 이용해 네트워크에 대한 액세스를 받을 수 있으며, 이 경우 이 시간 초과 값이 해당 사용자에게 적용됩니다.

캡티브 포털 로그인에 대한 자세한 내용은 캡티브 포털(captive portal) 필드, 2516 페이지 섹션을 참조하십시오.

- 게스트 캡티브 포털 사용자: 게스트 사용자로 캡티브 포털에 로그인한 사용자의 시간 초과 값입니다. 자세한 내용은 캡티브 포털 ID 소스, 2505 페이지를 참고하십시오.

영역 디렉토리 및 다운로드 동기화

영역 디렉토리 필드

이러한 설정은 영역의 개별 서버(Active Directory 도메인 컨트롤러 등)에 적용됩니다.

Hostname / IP Address(호스트 이름/IP 주소)

Active Directory 도메인 컨트롤러 시스템의 정규화된 호스트 이름입니다. 정규화된 이름을 찾으려면 Active Directory 서버 이름 찾기, 2472 페이지의 내용을 참조하십시오.

포트

Firepower Management Center와 컨트롤러를 연결하는 데 사용할 포트입니다.

암호화

(적극 권장함.) Firepower Management Center와 서버를 연결하는 데 사용할 암호화 방법입니다.

- **STARTTLS** — 암호화된 LDAP 연결
- **LDAPS** — 암호화된 LDAP 연결
- **None(없음)** — 암호화되지 않은 LDAP 연결(안전하지 않은 트래픽)

Active Directory 서버와 안전하게 통신하려면 Active Directory에 안전하게 연결, 2472 페이지의 내용을 참조하십시오.

SSL 인증서

서버에 인증하는 데 사용할 SSL 인증서입니다. SSL 인증서를 사용하려면 **STARTTLS** 또는 **LDAPS**를 **Encryption(암호화)** 유형으로 구성해야 합니다.

인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 **Hostname / IP Address(호스트 이름/IP 주소)**와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서에서 **computer1.example.com**을 사용하면, 연결이 실패합니다.

사용자 **Download(다운로드)** 필드

AD Primary Domain(AD 기본 도메인)

Microsoft Active Directory 영역에만 해당됩니다. 사용자가 인증해야 하는 Active Directory 서버의 도메인입니다.

참고 모든 Microsoft Active Directory(AD) 영역에 대한 고유 **AD Primary Domain(AD** 기본 도메인**)**을 지정해야 합니다. 다른 AD 영역에 동일한 **AD Primary Domain(AD** 기본 도메인**)**을 지정할 수는 있지만, 시스템이 제대로 작동하지 않습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다.

Download users and groups(사용자 및 그룹 다운로드**)(**사용자 액세스 제어의 필수 사항**)**

사용자 인식 및 사용자 제어를 위해 사용자와 그룹을 다운로드할 수 있습니다.

Begin automatic download at, Repeat every(자동 다운로드 시작 기준**,** 반복 빈도**)**

자동 다운로드의 빈도를 지정합니다.

지금 다운로드

그룹 및 사용자를 AD와 동기화하려면 클릭합니다.

Available Groups(사용 가능한 그룹**), Add to Include(**포함에 추가**), Add to Exclude(**제외에 추가**)**

정책에서 사용할 수 있는 그룹을 제한합니다.

- 그룹을 **Add to Include(**포함에 추가**)** 또는 **Add to Exclude(**제외에 추가**)** 필드로 이동하지 않는 한 **Available Groups(**사용 가능한 그룹**)** 필드에 표시되는 그룹은 정책에 사용할 수 있습니다.
- 그룹을 **Add to Include(**포함에 추가**)** 필드로 이동하면 이러한 그룹만 다운로드되고 사용자 데이터를 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 그룹을 **Add to Exclude(**제외에 추가**)** 필드로 이동하면 이러한 그룹을 제외한 모든 그룹이 다운로드되고 사용자 데이터를 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 포함되지 않은 그룹에 있는 사용자를 포함하려면, 아래 **Groups to Include(**포함할 그룹**)** 필드에 사용자 이름을 입력하고 **Add(**추가**)**를 클릭합니다.
- 제외되지 않은 그룹에 있는 사용자를 제외하려면, 아래 **Groups to Exclude(**제외할 그룹**)** 필드에 사용자 이름을 입력하고 **Add(**추가**)**를 클릭합니다.

참고 Firepower Management Center에 다운로드한 사용자는 **R = I - (E+e) + i** 수식으로 계산하며, 수식의 항목은 다음과 같습니다.

- R은 다운로드한 사용자의 목록입니다.
- I는 포함된 그룹입니다.
- E는 제외된 그룹입니다.
- e는 제외된 사용자입니다.
- i는 포함된 사용자입니다.

다음 위치에서 자동 다운로드 시작
AD에서 사용자 및 그룹을 다운로드할 시간 및 시간 간격을 입력합니다.

Active Directory에 안전하게 연결

Active Directory 서버와 FMC(권장 사항)간에 보안 연결을 만들려면 다음 작업을 모두 수행해야 합니다.

- Active Directory 서버의 루트 인증서를 내보냅니다.
- 신뢰할 수 있는 인증서 저장소로 루트 인증서를 가져옵니다.
- Active Directory 서버의 정규화된 이름을 찾습니다.
- 영역 디렉터리를 생성합니다.

자세한 내용은 다음 작업 중 하나를 참조하십시오.

관련 항목

Active Directory 서버의 루트 인증서 내보내기, 2473 페이지
Active Directory 서버 이름 찾기, 2472 페이지
영역 디렉터리 설정, 2475 페이지

Active Directory 서버 이름 찾기

FMC에서 영역 디렉터리를 설정하려면 정규화된 서버 이름을 알아야 합니다. 이 이름은 다음 절차에서 설명하는 대로 찾을 수 있습니다.

시작하기 전에

컴퓨터 이름을 보려면 충분한 권한이 있는 사용자로 Active Directory 서버에 로그인해야 합니다.

프로시저

단계 **1** Active Directory 서버에 로그인합니다.
단계 **2** **Start(**시작**)**를 클릭합니다.
단계 **3** **This PC(**이 **PC)**를 마우스 오른쪽 버튼으로 클릭합니다.
단계 **4** **Properties(**속성**)**를 클릭합니다.
단계 **5** **Advanced System Settings**(고급 시스템 설정)를 클릭합니다.
단계 **6** **Computer Name(**컴퓨터 이름**)** 탭을 클릭합니다.
단계 **7** 전체 컴퓨터 이름의 값을 기록해 둡니다.
FMC에서 영역 디렉터리를 설정할 때 이 이름을 정확하게 입력해야 합니다.

다음에 수행할 작업

영역 디렉터리를 생성합니다.

관련 항목

Active Directory 서버의 루트 인증서 내보내기, 2473 페이지

Active Directory 서버의 루트 인증서 내보내기

다음 작업에서는 Active Directory 서버의 루트 인증서를 내보내는 방법을 설명합니다. 이 인증서는 사용자 ID 정보를 얻기 위해 FMC에 안전하게 연결하는 데 필요합니다.

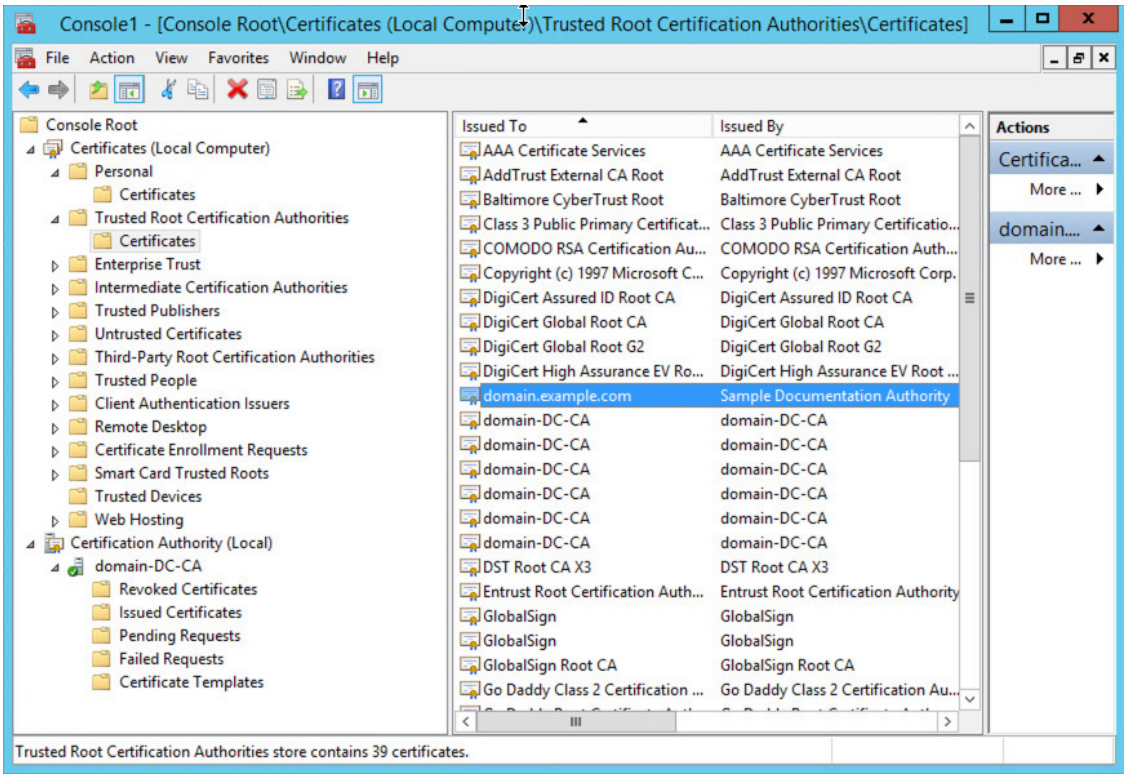
시작하기 전에

Active Directory 서버 루트 인증서의 이름을 알아야 합니다. 루트 인증서의 이름이 도메인과 같거나 인증서의 이름이 다를 수 있습니다. 다음 절차에서는 이름을 찾을 수 있는 한 가지 방법을 보여줍니다. 다른 방법이 있을 수도 있습니다

프로시저

단계 **1** 다음은 Active Directory 서버 루트 인증서의 이름을 찾는 한 가지 방법입니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.

a) Microsoft Management Console을 실행할 권한이 있는 사용자로 Active Directory 서버에 로그인합니다.
b) **Start(**시작**)**를 클릭하고 **mmc**를 입력합니다.
c) **File(**파일**)** > **Add/Remove Snap-in(**스냅인 추가/제거**)**을 클릭합니다.
d) 왼쪽 창의 Available Snap-ins(사용 가능한 스냅인) 목록에서 **Certificates(local)(**인증서**(**로컬**))**을 클릭합니다.
e) **Add(**추가**)**를 클릭합니다.
f) Certificates snap-in(인증서 스냅인) 대화 상자에서 **Computer Account(**컴퓨터 계정**)**를 클릭하고 **Next(**다음**)**를 클릭합니다.
g) Select Computer(컴퓨터 선택) 대화 상자에서 **Local Computer(**로컬 컴퓨터**)**를 클릭하고 **Finish(**마침**)**를 클릭합니다.
h) *Windows Server 2012*만 해당. 인증 기관 스냅인을 추가하려면 위의 단계를 반복합니다.
i) **Console Root(**콘솔 루트**)** > **Trusted Certification Authorities(**신뢰할 수 있는 인증 기관**)** > **Certificates(**인증서**)**를 클릭합니다.
서버의 신뢰할 수 있는 인증서가 오른쪽 창에 표시됩니다. 다음 그림은 Windows Server 2012의 예시일뿐입니다. 사용자마다 다르게 보일 수 있습니다.



단계 **2** **certutil** 명령을 사용하여 인증서를 내보냅니다.

이것이 인증서를 내보내는 유일한 방법입니다. 이 방법은 특히 웹 브라우저를 실행하고 Active Directory 서버에서 FMC에 연결할 수 있는 경우 인증서를 내보내는 편리한 방법입니다.

a) **Start(**시작**)**를 클릭하고 **cmd**를 입력합니다.

b) **certutil -ca.cert** *certificate-name* 명령을 입력합니다.
서버의 인증서가 화면에 표시됩니다.

c) 전체 인증서를 클립 보드에 복사합니다. **-----BEGIN CERTIFICATE-----**(으)로 시작하여 **-----END CERTIFICATE-----**(으)로 끝납니다(해당 문자열 포함).

다음에 수행할 작업

신뢰할 수 있는 CA 개체 추가, 625 페이지에서 설명한 대로 Active Directory 서버의 인증서를 신뢰할 수 있는 CA 인증서로 FMC에 가져옵니다.

관련 항목

Active Directory 서버 이름 찾기, 2472 페이지

영역 디렉터리 설정

이 절차를 이용하면 영역 디렉터리를 생성할 수 있으며, 이 디렉터리는 LDAP 서버 또는 Microsoft Active Directory 도메인 컨트롤러에 해당합니다. Active Directory 서버는 여러 도메인 컨트롤러를 보유할 수 있으며, 각 컨트롤러는 서로 다른 사용자 및 그룹을 인증할 수 있습니다.

Microsoft는 Active Directory 서버가 2020년에 LDAP 바인딩 및 LDAP 서명을 시행할 것이라고 발표했습니다. Microsoft는 이러한 설정을 기본 설정으로 사용할 때 Microsoft Windows에 권한 상승 취약점이 존재하여 MITM(man-in-the-middle) 공격자가 Windows LDAP 서버에 인증 요청을 성공적으로 전달할 수 있기 때문에 이러한 요구 사항을 적용하고 있습니다. 자세한 내용은 Microwoft 지원 사이트에서 2020 LDAP 채널 바인딩 및 Windows용 LDAP 서명 요구 사항을 참조하십시오.

아직 수행하지 않은 경우 TLS/SSL 암호화를 사용하여 Active Directory 서버에서 인증을 시작하는 것이 좋습니다.

영역 디렉터리 설정 필드에 대한 자세한 내용은 영역 필드, 2467 페이지을(를) 참고하십시오.

시작하기 전에

(권장) FMC에서 Active Directory 서버로 안전하게 연결하려면 먼저 다음 작업을 수행합니다.

- Active Directory 서버의 루트 인증서 내보내기, 2473 페이지
- Active Directory 서버 이름 찾기, 2472 페이지

프로시저

단계 **1** 아직 수행하지 않았다면 Firepower Management Center에 로그인하고 **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**를 클릭합니다.

단계 **2** Realms(영역) 페이지에서 디렉터리를 설정할 영역의 이름을 클릭합니다.

단계 **3** Directory(디렉터리) 페이지에서 **Add Directory(**디렉터리 추가**)**를 클릭합니다.

단계 **4** LDAP 서버 또는 Active Directory 도메인 컨트롤러의 **Hostname / IP Address(**호스트 이름**/IP** 주소**)**와 **Port(**포트**)**를 입력합니다.
시스템은 LDAP 쿼리를 사용자가 지정한 호스트 이름이나 IP 주소로 보냅니다. 호스트 이름이 LDAP 서버 또는 Active Directory 도메인 컨트롤러의 IP 주소로 확인된다면, **Test(**테스트**)**는 성공하게 됩니다.

단계 **5** **Encryption Mode(**암호화 모드**)**를 선택합니다.

단계 **6** 목록에서 **SSL Certificate(SSL** 인증서**)**를 선택하거나 추가(+)를 클릭하여 인증서를 추가합니다.

단계 **7** 연결을 테스트하려면 **Test(**테스트**)**를 클릭합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다. Realms(영역) 페이지로 돌아옵니다.

단계 **10** 영역을 아직 활성화하지 않았다면 Realms(영역) 페이지에서 **State(**상태**)**를 활성화쪽으로 밉니다.

다음에 수행할 작업

- 사용자 및 그룹 다운로드, 2476 페이지에 전달하는 고성능 고속 어플라이언스입니다.

관련 항목

Active Directory 서버의 루트 인증서 내보내기, 2473 페이지
Active Directory 서버 이름 찾기, 2472 페이지
영역 시퀀스 생성, 2477 페이지

사용자 및 그룹 다운로드

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	제어	Any(모든)	Any(모든)	관리자, 액세스 관리자, 네트워크 관리자

이 섹션은 Active Directory 서버의 사용자와 그룹을 Firepower Management Center로 다운로드하는 방법을 설명합니다. 포함할 그룹을 지정하지 않으면 시스템은 제공된 매개변수와 일치하는 모든 그룹에 대한 사용자 데이터를 검색합니다. 성능상의 이유로 Cisco에서는 액세스 제어에서 사용하려는 사용자를 나타내는 그룹만 명시적으로 포함할 것을 권장합니다.

Firepower Management Center이(가) 서버에서 검색할 수 있는 최대 사용자 수는 Firepower Management Center 모델에 따라 다릅니다. 영역의 다운로드 매개변수 범위가 너무 넓으면 Firepower Management Center에서는 최대한 많은 사용자의 정보를 가져오며, 가져오는 데 실패한 사용자 수를 Message Center(메시지 센터)의 Task(작업)에 보고합니다.

영역 컨피그레이션 필드에 대한 자세한 내용은 영역 필드, 2467 페이지를 참고하십시오.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**를 클릭합니다.

단계 **3** 사용자 및 그룹을 수동으로 다운로드하려면 영역 옆에 있는 다운로드( )를 클릭하여 사용자와 사용자 그룹을 다운로드합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다. 이 절차의 나머지 부분은 건너뛰어도 됩니다.

단계 **4** 자동 사용자 및 그룹 다운로드에 대한 영역을 설정하려면 자동 사용자 및 그룹 다운로드에 설정할 영역 옆에 있는 편집( )을 클릭합니다.

단계 **5** User Access Control(사용자 액세스 제어) 페이지에서 **Download users and groups (required for user access control)(**사용자 및 그룹 다운로드**)(**사용자 액세스 제어의 필수 사항**)**를 확인합니다.

단계 **6** 목록에서 **Begin automatic download at(**자동 다운로드 시작 기준**)**의 시간을 선택합니다.

단계 **7** **Repeat Every(**반복 빈도**)** 목록에서 다운로드 간격을 선택합니다.

단계 **8** 다운로드에서 사용자 그룹을 포함하거나 제외하려면 **Available Groups(**사용 가능한 그룹**)** 열에서 사용자 그룹을 선택하고 **Add to Include(**포함에 추가**)** 또는 **Add to Exclude(**제외에 추가**)**를 클릭합니다.

사용자가 여러 명인 경우 쉼표로 구분하십시오. 또한 이 필드에서 와일드카드 문자로 별표(*)를 사용할 수 있습니다.

참고 해당 그룹의 사용자에 대해 사용자 제어를 수행하려면 **Add to Include(**포함에 추가**)**를 선택해야 합니다.

다음 지침을 사용하십시오.

- **Available Groups(**사용 가능한 그룹**)** 상자에 그룹을 그대로 두면 해당 그룹이 다운로드되지 않습니다.
- 그룹을 **Add to Include(**포함에 추가**)** 상자로 이동하면 그룹이 다운로드되고 사용자 데이터를 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 그룹을 **Add to Exclude(**제외에 추가**)** 상자로 이동하면 그룹이 다운로드되고 사용자 데이터를 사용자 인식에 사용할 수 있으나, 사용자 제어에는 사용할 수 없습니다.
- 포함되지 않은 그룹에 있는 사용자를 포함하려면, 아래 **Groups to Include(**포함할 그룹**)** 필드에 사용자 이름을 입력하고 **Add(**추가**)**를 클릭합니다.
- 제외되지 않은 그룹에 있는 사용자를 제외하려면, 아래 **Groups to Exclude(**제외할 그룹**)** 필드에 사용자 이름을 입력하고 **Add(**추가**)**를 클릭합니다.

영역 시퀀스 생성

다음 절차를 수행하면 Firepower System에서 ID 정책을 적용할 때 검색하는 영역의 순서가 지정된 목록인 영역 시퀀스를 생성할 수 있습니다. 영역을 추가하는 것과 정확히 동일한 방식으로 ID 규칙에 영역 시퀀스를 추가합니다. 차이점은 Firepower System이 ID 정책을 적용할 때 영역 시퀀스에 지정된 순서대로 모든 영역을 검색한다는 점입니다.

시작하기 전에

각각 Active Directory 서버와의 연결에 해당하는 영역을 2개 이상 생성하고 활성화해야 합니다. LDAP 영역에 대한 영역 시퀀스를 생성할 수 없습니다.

- 영역 디렉터리 설정, 2475 페이지에 설명된 대로 디렉터리를 생성합니다.
- 사용자 및 그룹 다운로드, 2476 페이지에 설명된 대로 사용자 및 그룹을 다운로드하고 영역을 활성화합니다.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **System(**시스템**)** > **Integration(**통합**)** > **Realms Sequences(**영역 시퀀스**)**를 클릭합니다.

단계 3 **Add Sequence(**시퀀스 추가**)**를 클릭합니다.

단계 4 **Name(**이름**)** 필드에 영역 시퀀스를 식별하는 이름을 입력합니다.

단계 5 (선택 사항). **Description(**설명**)** 필드에 영역 시퀀스에 대한 설명을 입력합니다.

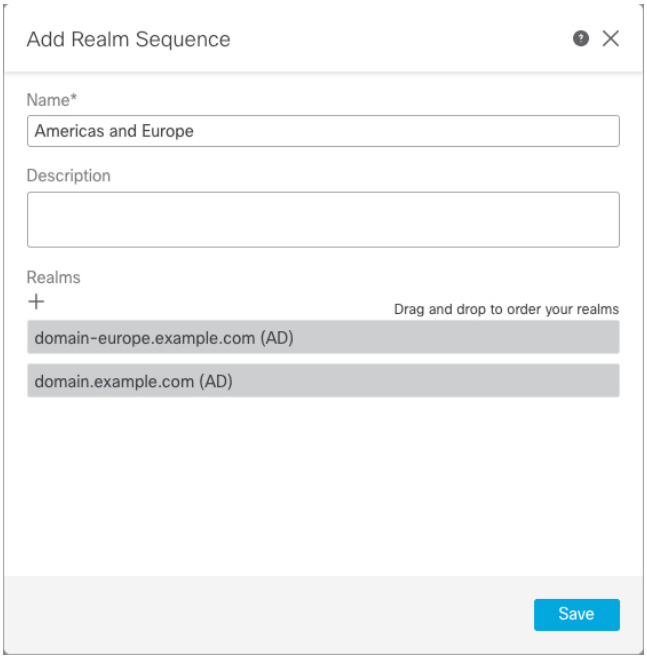
단계 6 Realms(영역) 아래에서 추가(+)를 클릭합니다.

단계 7 시퀀스에 추가할 각 영역의 이름을 클릭합니다.

검색 범위를 좁히려면 **Filter(**필터**)** 필드에 영역 이름의 전체 또는 일부를 입력합니다.

단계 8 **OK(**확인**)**를 클릭합니다.

단계 9 Add Realm Sequence(영역 시퀀스 추가) 대화 상자에서 Firepower System이 검색할 순서대로 영역을 끌어다 놓습니다.
다음 그림에는 두 개의 영역으로 구성된 영역 시퀀스의 예가 나와 있습니다. **domain.example.com** 영역보다 먼저 **domain-europe.example.com** 영역을 검색합니다.



단계 10 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

ID 정책 생성, 2534 페이지의 내용을 참조하십시오.

관련 항목

영역 디렉터리 설정, 2475 페이지

영역 관리

이 섹션에서는 Realms(영역) 페이지에서 컨트롤을 사용해 영역에 대한 유지 관리 작업을 수행하는 방법을 설명합니다. 다음에 유의하십시오.

- 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)** 버튼을 클릭합니다.

단계 **3** **Realms(**영역**)**를 클릭합니다.

단계 **4** 영역을 삭제하려면 삭제( )을 클릭합니다.

단계 **5** 영역을 편집하려면 영역 옆의 수정( )을 클릭하고 영역 생성, 2466 페이지에 설명된 대로 영역을 변경합니다.

단계 **6** 영역을 활성화하려면 **State(**상태**)**를 오른쪽으로 밉니다. 영역을 비활성화하려면 왼쪽으로 밉니다.

단계 **7** 사용자 및 사용자 그룹을 다운로드하려면 다운로드( )을 클릭합니다.

단계 **8** 영역을 복사하려면 복사 ( )을 클릭합니다.

단계 **9** 영역을 비교하려면 영역 비교, 2479 페이지을(를) 참고하십시오.

영역 비교

이 작업을 수행하려면 관리자, 액세스 관리자, Network Admin(네트워크 관리자) 또는 보안 승인자이어야 합니다.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)** 버튼을 클릭합니다.

단계 **3** **Realms(**영역**)**를 클릭합니다.

단계 **4** **System(**시스템**)** > **Integration(**통합**)** 버튼을 클릭합니다.

단계 **5** **Realms(**영역**)**를 클릭합니다.

단계 **6** **Compare Realms(**영역 비교**)**를 클릭합니다.
단계 **7** **Compare Against(**비교 대상**)** 목록에서 **Compare Realm(**영역 비교**)**을 선택합니다.
단계 **8** **Realm A(**영역 **A)** 및 **Realm B(**영역 **B)** 목록에서 비교할 영역을 선택합니다.
단계 **9** **OK(**확인**)**를 클릭합니다.
단계 **10** 변경 사항을 개별적으로 탐색하려면 제목 표시줄 위의 **Previous(**이전**)** 또는 **Next(**다음**)**를 클릭합니다.
단계 **11** (선택 사항). **Comparison Report(**비교 보고서**)**를 클릭하여 영역 비교 보고서를 생성합니다.
단계 **12** (선택 사항). **New Comparison(**새 비교**)**을 클릭하여 새 영역 비교 보기를 생성합니다.

영역 및 사용자 다운로드 문제 해결

서버 연결 동작이 정상적이지 않을 경우 영역 컨피그레이션, 디바이스 설정 또는 서버 설정을 조정하는 방법을 고려하십시오. 기타 관련 문제 해결 정보를 보려면 다음을 참조하십시오.

- ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결, 2500 페이지
- 캡티브 포털(captive portal) ID 소스 문제 해결, 2518 페이지
- 원격 액세스 VPN ID 소스 문제 해결, 2523 페이지
- 사용자 제어 문제 해결, 549 페이지

증상: 영역 및 그룹이 보고되었지만 다운로드되지는 않음

Firepower Management Center의 상태 모니터는 사용자 또는 영역의 불일치를 알려주며, 이러한 불일치는 다음과 같이 정의됩니다.

- 사용자 불일치: 사용자가 다운로드되지 않고 Firepower Management Center에 보고됩니다.

  사용자 불일치가 발생하는 일반적인 이유는 사용자가 Firepower Management Center 다운로드에서 제외된 그룹에 속하기 때문입니다. 영역 필드, 2467 페이지에서 논의된 정보를 검토합니다.

- 영역 불일치: 사용자가 Firepower Management Center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다.

예를 들어 Firepower Management Center의 **domain.example.com**(이)라는 도메인에 대응하는 영역을 정의했지만 로그인이 **another-domain.example.com**(이)라는 도메인에서 보고되었다면, 이것은 영역 불일치가 됩니다. 이 도메인의 사용자는 Firepower Management Center가 Unknown(알 수 없음)으로 식별합니다.

불일치 임계값이 백분율로 설정되며, 해당 값보다 높으면 상태 경고가 트리거됩니다. 예:

- 기본 불일치 임계값 50%를 사용하고 여덟 개 수신 세션에서 두 개 영역이 불일치하는 경우, 불일치 비율은 25%이고 어떠한 경고도 트리거되지 않습니다.
- 불일치 임계값을 30%로 설정하고 다섯 개 수신 세션에서 세 개 영역이 불일치하는 경우, 불일치 비율은 60%이며 경고가 트리거됩니다.

ID 규칙과 일치하지 않는 Unknown users(알 수 없는 사용자)에게 적용되는 정책은 없습니다. (Unknown users(알 수 없는 사용자)에 ID 규칙을 설정할 수 있지만, 사용자와 영역을 정확하게 식별하여 규칙 수를 최소한으로 유지하는 것이 좋습니다.)

자세한 내용은 영역 또는 사용자 불일치 탐지, 2483 페이지를 참고하십시오.

증상: 액세스 제어 정책이 그룹 구성원 자격과 일치하지 않음

이 솔루션은 다른 AD 도메인과 트러스트 관계에 있는 AD 도메인에 적용됩니다. 아래 설명 내용에서 외부 도메인이란 사용자가 로그인하는 것과 다른 도메인을 의미합니다.

사용자가 신뢰할 수 있는 외부 도메인의 정의된 그룹에 속하는 경우, Firepower는 외부 도메인의 구성원 자격을 추적하지 않습니다. 예를 들어 다음과 같은 시나리오를 가정해 보십시오.

- 도메인 컨트롤러 1 및 2는 서로 신뢰합니다.
- 도메인 컨트롤러 2에 그룹 A가 정의되어 있습니다.
- 컨트롤러 1의 사용자 `mparvinder`는 그룹 A의 구성원입니다.

사용자 `mparvinder`가 그룹 A에 있지만, 구성원 자격 그룹 A를 지정하는 Firepower 액세스 제어 정책 규칙이 일치하지 않습니다.

솔루션: 도메인 컨트롤러 1에 유사한 그룹을 생성합니다. 여기에는 그룹 A에 속한 모든 도메인 1 어카운트가 포함됩니다. 그룹 A 또는 그룹 B의 모든 구성원과 일치하도록 액세스 컨트롤 정책을 변경합니다.

증상: 액세스 제어 정책이 하위 도메인 구성원 자격과 일치하지 않음

사용자가 상위 도메인의 하위 도메인에 속한 경우, Firepower는 도메인 간의 상위/하위 관계를 추적하지 않습니다. 예를 들어 다음과 같은 시나리오를 가정해 보십시오.

- 도메인 `child.parent.com`은 `parent.com`의 하위 도메인입니다.
- 사용자 `mparvinder`는 `child.parent.com`에 정의되어 있습니다.

사용자 `mparvinder`가 하위 도메인에 있더라도, `parent.com`과 일치하는 Firepower 액세스 컨트롤 정책은 `child.parent.com` 도메인의 `mparvinder`와 일치하지 않습니다.

솔루션: `parent.com` 또는 `child.parent.com`의 구성원 자격과 일치하도록 액세스 제어 정책 규칙을 변경합니다.

증상: 영역 또는 영역 디렉토리 테스트 실패

디렉터리 페이지 (테스트) 버튼 호스트 이름 또는 IP 주소를 입력 한 LDAP 쿼리를 보냅니다. 작업이 실패한다면 다음 사항을 확인해 주십시오.

- 입력한 **Hostname(**호스트 이름**)**은 LDAP 서버 또는 Active Directory 도메인 컨트롤러의 IP 주소로 확인됩니다.
- 입력한 **IP Address(IP** 주소**)**가 유효합니다.

영역 설정 페이지에서 **Test(**테스트**)** 버튼을 누르면 다음 사항을 확인합니다.

- DNS는 **AD Primary Domain(AD** 기본 도메인**)**을 LDAP 서버 또는 Active Directory 도메인 컨트롤러의 IP 주소로 확인합니다.
- **AD Join Username(AD** 조인 사용자 이름**)**과 **AD Join Password(AD** 조인 비밀번호**)**가 올바릅니다.

  AD Join Username(AD 조인 사용자 이름**)**은 온전한 이름이어야 합니다(예: **`administrator`**가 아닌 **`administrator@mydomain.com`**).
- 사용자는 도메인에서 컴퓨터를 생성하고 Firepower Management Center를 도메인에 도메인 컴퓨터로 조인할 권한을 가집니다.

증상**:** 예기치 않은 시간에 사용자 시간 초과가 발생함

예기치 않은 간격으로 사용자 시간 초과가 발생할 경우 ISE/ISE-PIC, 또는 TS 에이전트 서버의 시간이 Firepower Management Center의 시간과 동기화되었는지 확인하십시오. 어플라이언스가 동기화되지 않은 경우, 시스템이 예기치 않은 간격으로 사용자 시간 초과를 수행할 수 있습니다.

증상**:** 영역 설정에 지정된 대로 사용자가 포함되지 않거나 제외됨

서버에 있는 하위 그룹의 구성원인 사용자를 포함하거나 제외하는 Active Directory 영역을 구성할 경우, Microsoft Windows 서버는 보고하는 사용자 수를 제한합니다.

- Microsoft Windows Server 2012의 그룹당 사용자 수 5,000명

필요한 경우, 서버 컨피그레이션을 수정하여 이러한 기본값 제한을 늘리고 더 많은 사용자를 수용할 수 있습니다.

증상**:** 사용자가 다운로드되지 않음

가능한 원인은 다음과 같습니다.

- 영역 **Type(**유형**)**을 잘못 설정한 경우, 사용자와 그룹을 다운로드할 수 없습니다. Firepower System이 기대하는 속성과 저장소가 제공하는 속성이 일치하지 않기 때문입니다. 예를 들어 Microsoft Active Directory 영역의 **Type(**유형**)**을 **LDAP**로 설정하면, Firepower System은 Active Directory에서 `none(없음)`으로 설정되는 `uid` 속성을 기대합니다. (Active Directory 저장소는 사용자 ID에 `sAMAccountName`을 사용합니다.)

  솔루션: 영역 **Type(**유형**)** 필드를 적절하게 설정합니다. Microsoft Active Directory의 경우에는 **AD**이며, 다른 지원되는 LDAP 저장소의 경우에는 **LDAP**입니다.
- 그룹 또는 조직 단위 이름에 특수 문자가 있는 Active Directory 그룹의 사용자는 ID 정책 규칙에 사용하지 못할 수도 있습니다. 예를 들어 그룹 또는 조직 단위 이름에 별표(*), 등호(=), 백슬래시(\) 같은 특수문자가 있다면, 해당 그룹의 사용자는 다운로드되지 않으며 ID 정책에 사용할 수 없습니다.

  솔루션: 그룹 또는 조직 단위 이름에서 특수 문자를 제거합니다.

증상: 이전에 확인되지 않은 **ISE** 사용자에 대한 사용자 데이터가 웹 인터페이스에 표시되지 않음

데이터베이스에 데이터가 아직 없는 ISE 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. Active Directory 서버에서 이러한 정보를 정상적으로 검색하기까지 추가 시간이 필요한 경우도 있습니다. 데이터 검색에 성공할 때까지 ISE 또는 사용자 에이전트 사용자에 의해 확인된 활동이 웹 인터페이스에 표시되지 않습니다.

데이터베이스에 데이터가 아직 없는 ISE/ISE-PIC 또는 TS 에이전트 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. Microsoft Windows 서버에서 이러한 정보를 정상적으로 검색하기까지 추가 시간이 필요한 경우도 있습니다. 데이터 검색에 성공할 때까지 ISE/ISE-PIC 또는 TS 에이전트 사용자에 의해 확인된 활동이 웹 인터페이스에 표시되지 않습니다.

그리고 이로 인해 시스템이 액세스 제어 규칙을 사용하는 사용자의 트래픽을 처리하지 못할 수도 있습니다.

증상: 이벤트에 예기치 않은 사용자 데이터가 있음

사용자 또는 사용자 활동 이벤트에 예기치 않은 IP 주소가 있을 경우 영역을 확인하십시오. 시스템에서는 동일한 **AD Primary Domain(AD** 기본 도메인**)** 값으로 여러 영역을 구성하는 것을 지원하지 않습니다.

영역 또는 사용자 불일치 탐지

이 섹션은 다음과 같이 정의되는 영역 또는 사용자 불일치를 탐지하는 방법을 설명합니다.

- 사용자 불일치: 사용자가 다운로드되지 않고 Firepower Management Center에 보고됩니다.

  사용자 불일치가 발생하는 일반적인 이유는 사용자가 Firepower Management Center 다운로드에서 제외된 그룹에 속하기 때문입니다. 영역 필드, 2467 페이지에서 논의된 정보를 검토합니다.

- 영역 불일치: 사용자가 Firepower Management Center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다.

자세한 정보는 영역 및 사용자 다운로드 문제 해결, 2480 페이지 섹션을 참조하십시오.

ID 규칙과 일치하지 않는 Unknown users(알 수 없는 사용자)에게 적용되는 정책은 없습니다. (Unknown users(알 수 없는 사용자)에 ID 규칙을 설정할 수 있지만, 사용자와 영역을 정확하게 식별하여 규칙 수를 최소한으로 유지하는 것이 좋습니다.)

프로시저

단계 **1** 영역 또는 사용자 불일치 탐지 활성화:

a) 아직 하지 않았다면 Firepower Management Center에 로그인합니다.
b) **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)**를 클릭합니다.
c) 새 상태 정책을 만들거나 기존 정책을 편집합니다.
d) Editing Policy(정책 편집) 페이지에서 **Policy Runtime Interval(**정책 런타임 간격**)**을 설정합니다. 이것은 모든 상태 모니터링 작업을 실행하는 빈도가 됩니다.
e) 왼쪽 창에서 **Realm(**영역**)**을 클릭합니다.

f) 다음 정보를 입력합니다.

- **Enabled(**활성화됨**)**: **On(**켜기**)** 클릭
- **Warning Users match threshold(**사용자 경고 일치 임계값**) %**: 상태 모니터에서 경고가 표시되게 하는 영역 불일치 또는 사용자 불일치의 비율입니다. 자세한 내용은 영역 및 사용자 다운로드 문제 해결, 2480 페이지를 참고하십시오.

g) 페이지 하단의 **Save Policy & Exit(**정책 저장 및 종료**)**를 클릭합니다.

h) 상태 정책 적용, 399 페이지에 설명된 대로 상태 정책을 매니지드 디바이스에 적용합니다.

단계 **2** 다음 방법 중 하나를 이용해 사용자 및 영역 불일치를 확인합니다.

- 경고 임계값을 초과한 경우, Firepower Management Center 상단 탐색 창에서 **Warning(**경고**)** > **Health(**상태**)**를 클릭합니다. Health Monitor(상태 모니터)가 열립니다.
- **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 클릭합니다.

단계 **3** Display(표시) 열의 Health Monitor(상태 모니터링) 페이지에서 **Realm: Domain(**영역**:** 도메인**)** 또는 **Realm: User(**영역**:** 사용자**)**를 확장해 불일치 관련 정보를 확인합니다.

관련 항목

상태 정책, 398 페이지
상태 모니터링 구성, 397 페이지
상태 모니터 상태 카테고리, 420 페이지

영역 히스토리

기능	버전	세부 사항
영역 시퀀스	6.7.0	영역 시퀀스는 ID 규칙을 적용할 둘 이상의 영역으로 구성된 순서가 지정된 목록입니다. 영역 시퀀스를 ID 정책과 연결할 경우 Firepower System은 영역 시퀀스에 지정된 순서대로 Active Directory 도메인을 검색합니다.
사용자 제어를 위한 영역입니다.	—	버전 6.0 이전에 도입된 기능. 영역은 FMC와 Active Directory 또는 LDAP 사용자 저장소 간의 연결입니다.

98 장

ISE/ISE-PIC를 사용하여 사용자 제어

다음 주제는 ISE/ISE-PIC를 이용해 사용자 인식 및 사용자 제어를 수행하는 방법을 설명합니다.

- ISE/ISE-PIC ID 소스, 2485 페이지
- ISE/ISE-PIC의 라이선스 요구 사항, 2487 페이지
- ISE/ISE-PIC 요구 사항 및 사전 요건, 2487 페이지
- ISE/ISE-PIC 지침 및 제한 사항, 2488 페이지
- 사용자 제어에 대한 ISE/ISE-PIC 설정 방법, 2490 페이지
- ISE/ISE-PIC 구성, 2492 페이지
- 사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지
- ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결, 2500 페이지
- ISE/ISE-PIC 기록, 2502 페이지

ISE/ISE-PIC ID 소스

패시브 인증에 ISE/ISE-PIC를 사용하기 위해 Cisco Identity Services Engine(ISE) 또는 ISE Passive Identity Connector(ISE-PIC) 구축을 Firepower System에 통합할 수 있습니다.

ISE/ISE-PIC은 신뢰할 수 있는 ID 소스로서 액티브 디렉터리(AD), LDAP, RADIUS, RSA로 인증하는 사용자에 대한 사용자 인식 데이터를 제공합니다. 또한 액티브 디렉터리 사용자에 대한 사용자 제어를 수행할 수 있습니다. ISE/ISE-PIC에서는 실패한 로그인 시도 또는 ISE 게스트 서비스 사용자의 활동을 보고하지 않습니다.

참고 Firepower 시스템은 IEEE 802.1x 머신 인증을 구문 분석하지 않지만, 802.1x 사용자 인증은 구문 분석합니다. ISE에서 802.1x를 사용한다면 사용자 인증을 포함해야 합니다. 802.1x 머신 인증은 정책에서 사용할 수 있는 사용자 ID를 FMC에 제공하지 않습니다.

Cisco ISE/ISE-PIC에 대한 자세한 정보는 *Cisco Identity Services Engine* 관리자 설명서와 *Identity Services Engine Passive Identity Connector(ISE-PIC)* 설치 및 관리자 가이드을 참조하십시오.

참고 최신 기능 집합과 가장 많은 수의 문제를 해결하려면 최신 버전의 ISE/ISE-PIC를 사용하는 것이 좋습니다.

대상 SGT(Security Group Tag) 매칭

ISE를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 SGT(Security Group Tag)를 정의하고 사용하는 경우, SGT를 소스 및 대상 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 이렇게 하면 보안 그룹 멤버십에 따른 액세스를 IP 주소가 아니라 네트워크 개체를 기준으로 차단 또는 허용할 수 있습니다.

SGT 태그 매칭은 다음과 같은 이점을 제공합니다.

- FMC는 ISE에서 SXP(Security Group Tag eXchange Protocol) 매핑을 구독할 수 있습니다.

  ISE는 SXP를 사용하여 IP-to-SGT 매핑 데이터베이스를 매니지드 디바이스에 전파합니다. ISE 서버를 사용하도록 FMC를 구성한다면, ISE에서 SXP 항목을 수신 대기하려면 옵션을 활성화합니다. 이로 인해 FMC는 ISE에서 직접 보안 그룹 태그 및 매핑에 대해 학습합니다. 그런 다음 FMC는 매니지드 디바이스에 SGT 및 매핑을 게시합니다.

  SXP 주제는 ISE 및 기타 SXP 준수 디바이스(예: 스위치) 간의 SXP 프로토콜을 통해 학습한 정적 및 동적 매핑에 따라 보안 그룹 태그를 수신합니다.

  ISE에서 보안 그룹 태그를 생성하고 각 태그에 호스트 또는 네트워크 IP 주소를 할당할 수 있습니다. 또한 사용자 어카운트에 SGT를 할당할 수 있으며, SGT는 사용자의 트래픽에 할당됩니다. 네트워크의 스위치와 라우터가 이 작업을 수행하도록 구성된 경우, 이러한 태그는 ISE, Cisco TrustSec 클라우드로 제어되는 네트워크에 진입할 때 패킷에 할당됩니다.

  ISE-PIC는 SXP를 지원하지 않습니다.

- FMC 및 매니지드 FTD 디바이스는 추가 정책을 구축 없이 SGT 매핑을 학습할 수 있습니다. (즉 액세스 제어 정책을 구축하지 않고도 SGT 매핑에 대한 연결 이벤트를 볼 수 있습니다.)

- 네트워크를 분할해 중요한 비즈니스 자산을 보호하는 Cisco TrustSec를 지원합니다.

- SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가할 때, 매니지드 디바이스는 다음 우선순위를 사용합니다.

  1. 패킷에 정의된 소스 SGT 태그(있는 경우).

     SGT 태그를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.

     SGT 태그를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.

  2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. SGT는 소스 또는 대상과 일치할 수 있습니다.

3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있다면, 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.

예:

- ISE에서 Guest Users(게스트 사용자)라는 이름의 SGT 태그를 생성하고 192.0.2.0/24 네트워크에 연결합니다.

  예를 들어 액세스 제어 규칙에서 Guest Users(게스트 사용자)를 소스 SGT 조건으로 사용하고, 네트워크에 액세스하는 사람이 특정 URL, 웹 사이트 범주 또는 네트워크만 액세스하도록 제한할 수 있습니다.

- ISE에서 Restricted Networks(제한된 네트워크)라는 이름의 SGT 태그를 생성하고 198.51.100.0/8 네트워크에 연결합니다.

  예를 들어 Restricted Networks(제한된 네트워크)를 대상 SGT 규칙 조건으로 사용하고, Guest Users(게스트 사용자)와 네트워크 액세스 자격이 없는 사용자가 있는 네트워크에서의 액세스를 차단할 수 있습니다.

관련 항목

ISE/ISE-PIC 지침 및 제한 사항, 2488 페이지

ISE/ISE-PIC의 라이선스 요구 사항

FTD 라이센스

Any(모든 상태)

기본 라이선스

제어

ISE/ISE-PIC 요구 사항 및 사전 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

- 관리자

- 액세스 관리자
- Network Admin(네트워크 관리자)

ISE/ISE-PIC 지침 및 제한 사항

Firepower System으로 ISE/ISE-PIC를 구성하는 경우에는 이 섹션에서 설명하는 지침을 사용하십시오.

ISE/ISE-PIC 버전 및 설정 호환성

ISE/ISE-PIC 버전과 설정은 다음과 같이 Firepower와의 통합 및 상호작용에 영향을 줍니다.

- 최신 기능 집합을 사용하려면 최신 버전의 ISE/ISE-PIC를 사용하는 것이 좋습니다.
- ISE/ISE-PIC 서버와 Firepower Management Center의 시간을 동기화합니다. 그렇지 않으면 시스템이 예기치 않은 간격으로 사용자 시간 제한을 수행할 수 있습니다.
- ISE 또는 ISE-PIC 데이터를 사용하여 사용자 제어를 구현하려면, 영역 생성, 2466 페이지에서 설명하는 것처럼 pxGrid 페르소나를 가정하는 ISE 서버의 영역을 설정하고 활성화합니다.
- ISE 서버에 연결되는 각 Firepower Management Center 호스트 이름은 고유해야 합니다. 그렇지 않으면 단일 Firepower Management Center에 대한 연결이 중단됩니다.
- 많은 사용자 그룹을 모니터링하도록 ISE/ISE-PIC를 설정하는 경우 시스템은 매니지드 디바이스 메모리 제한으로 인해 그룹을 기준으로 사용자 매핑을 삭제할 수 있습니다. 그 결과, 영역이 있는 규칙 또는 사용자 조건이 정상적으로 수행되지 않을 수 있습니다.

  FTD v6.7 이상을 실행하는 디바이스의 경우, 선택적으로 **configure identity-subnet-filter** 명령을 사용하여 매니지드 디바이스가 모니터링하는 서브넷을 제한할 수 있습니다. 자세한 내용은 *Firepower Threat Defense* 명령 참조에 나와 있습니다.

이 시스템 버전과 호환되는 특정 ISE/ISE-PIC 버전에 대한 자세한 내용은 *Cisco Firepower* 호환성 가이드를 참고하십시오.

ISE에서 클라이언트 승인

ISE 서버와 Firepower Management Center 디바이스 간의 연결에 성공하려면 ISE에서 클라이언트를 수동으로 승인해야 합니다. (일반적으로 클라이언트 두 개가 존재합니다. 하나는 연결 테스트용이며, 다른 하나는 ISE 에이전트용입니다.)

또한 *Cisco Identity Services Engine* 관리자 가이드의 사용자 및 외부 ID 소스 관리 장에서 설명하는 것처럼 ISE에서 **Automatically approve new accounts(**새 어카운트 자동 승인**)**를 활성화할 수도 있습니다.

SGT(Security Group Tag)

보안 그룹 태그(SGT)는 신뢰할 수 있는 네트워크 내의 트래픽 소스 권한을 지정합니다. Cisco ISE 및 Cisco TrustSec에서는 SGA(Security Group Access)라는 기능을 사용하여 네트워크로 들어오는 패킷에 SGT 속성을 적용합니다. 이러한 SGT는 ISE 또는 TrustSec 내에서 사용자가 할당한 보안 그룹에 해당합니다. ISE를 ID 소스로 구성하는 경우 Firepower System은 이러한 SGT를 사용하여 트래픽을 필터링할 수 있습니다.

보안 그룹 태그는 액세스 제어 규칙에서 소스 및 대상 일치 기준으로 사용할 수 있습니다.

소스 SGT 태그 외에 대상 SGT 태그도 매칭할 때는, 다음 사항이 적용됩니다.

필수 ISE 버전: 2.6 패치 6 이상, 2.7 패치 2 이상

라우터 지원: 이더넷을 통한 SGT 인라인 태깅을 지원하는 모든 Cisco 라우터 자세한 내용은 Cisco Group Based Policy Platform and Capability Matrix Release(Cisco Group 기반 정책 플랫폼 및 기능 매트릭스 릴리스) 등의 참조 자료에서 확인하십시오.

제한 사항:

- QoS(Quality Service) 정책은 소스 SGT 매칭만 사용합니다. 대상 SGT 매칭은 사용하지 않습니다.
- RA-VPN은 RADIUS에서 바로 SGT 매핑을 수신하지 않습니다.

FMC가 FirePOWER Services 디바이스를 이용해 ASA를 관리한다면, SXP 구독은 캡티브 포털 ID 규칙을 디바이스에 구축했을 때만 작동합니다.

ISE 및 고가용성

기본 Firepower Management Center가 실패하는 경우에는 다음이 발생합니다.

- 대기 상태가 기본으로 승격하지 않은 한, 보조 Firepower Management Center의 사용자 데이터베이스는 읽기 전용입니다.

  저장소(예: Active Directory)에 추가된 사용자는 Firepower Management Center에 다운로드되지 않으며 이러한 사용자는 Unknown(알 수 없음)으로 식별됩니다.

  새 SGT는 사용되지 않습니다.

- 대기 상태가 기본으로 승격되면, 모든 작업자는 다시 정상 상태가 됩니다. 즉 사용자가 다운로드되고, 새 SGT를 사용하며, 사용자는 가능한 경우 식별됩니다.

ISE 기본 서버가 실패한다면, 사용자는 보조를 기본으로 직접 승격해야 합니다. 자동 페일오버는 실행되지 않습니다.

엔드포인트 위치**(**또는 위치 **IP)**

엔드포인트 위치 속성은 ISE에서 식별된 사용자를 인증하기 위해 ISE를 사용한 네트워크 디바이스의 IP 주소입니다.

ISE 속성

ISE 연결을 구성하면 Firepower Management Center 데이터베이스에 ISE 속성 데이터가 입력됩니다. 사용자 인식 및 사용자 제어에 다음과 같은 ISE 속성을 사용할 수 있습니다. ISE-PIC에서는 이러한 작업이 지원되지 않습니다.

엔드포인트 프로파일**(**또는 디바이스 유형**)**

엔드포인트 프로파일 속성은 ISE에서 식별된 사용자의 엔드포인트 디바이스 유형입니다.

사용자 제어에 대한 ISE/ISE-PIC 설정 방법

다음 구성 중 하나에서 ISE/ISE-PIC를 사용할 수 있습니다.

- 영역, ID 정책 및 관련 액세스 제어 정책을 이용합니다.

  영역을 사용하여 정책 내 네트워크 리소스에 대한 사용자 액세스를 제어합니다. 정책에서 ISE/ISE-PIC SGT(Security Group Tags) 메타데이터를 계속 사용할 수 있습니다.

- 액세스 제어 정책만 사용할 수 있습니다. 영역 또는 ID 정책은 필요 없습니다.

  SGT 메타데이터만 사용하여 네트워크 액세스를 제어하려면 이 방법을 사용해야 합니다.

관련 항목

영역을 사용하지 않고 ISE를 구성하는 방법, 2490 페이지
영역을 사용해 사용자 제어에 대한 ISE/ISE-PIC를 설정하는 방법, 2491 페이지

영역을 사용하지 않고 ISE를 구성하는 방법

이 항목에서는 SGT 태그를 이용해 네트워크 액세스를 허용 또는 차단하도록 ISE를 구성하려면 수행해야 하는 작업을 개략적으로 설명합니다.

프로시저

	명령 또는 동작	목적
단계 1	SGT 매칭: ISE에서 SXP를 활성화합니다.	그러면 SGT 메타데이터 변경 시 FMC가 ISE에서 업데이트를 받게 됩니다.
단계 2	ISE/ISE-PIC에서 시스템 인증서를 내보냅니다.	ISE/ISE-PIC pxGrid, 모니터링(MNT) 서버 및 FMC를 안전하게 연결하려면 인증서가 있어야 합니다. FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 2495 페이지의 내용을 참조하십시오.
단계 3	ISE/ISE-PIC ID 소스를 생성합니다.	ISE/ISE-PIC ID 소스를 사용하면 ISE/ISE-PIC가 제공하는 SGT(Security Group Tags)를 사용하여 사용자 활동을 제어할 수 있습니다. 사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지의 내용을 참조하십시오.
단계 4	액세스 제어 규칙을 생성합니다.	액세스 제어 규칙은 트래픽이 규칙 기준과 일치할 때 수행할 작업(예: 허용 또는 차단)을 지정합니다. 액세스 제어 규칙에서는 소스 및 대상 SGT 메타데이터를 매칭 기준으로 사용할 수 있습니다. 액세스 제어 규칙 소개, 1645 페이지의 내용을 참조하십시오.

	명령 또는 동작	목적
단계 5	액세스 제어 정책을 매니지드 디바이스에 구축합니다.	효과를 발휘하려면 정책은 매니지드 디바이스에 구축해야 합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

다음에 수행할 작업

FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 2495 페이지

영역을 사용해 사용자 제어에 대한 ISE/ISE-PIC를 설정하는 방법

시작하기 전에

이 항목에서는 사용자 제어를 위해 ISE/ISE-PIC를 구성하고 사용자나 그룹의 네트워크 액세스를 허용 또는 차단하려면 수행해야 하는 작업을 개략적으로 설명합니다. 사용자와 그룹은 영역에 지원되는 서버, 2463 페이지에 나열된 모든 서버에 저장할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	대상 SGT에만 해당: ISE에서 SXP를 활성화합니다.	그러면 SGT 메타데이터 변경 시 FMC가 ISE에서 업데이트를 받게 됩니다.
단계 2	ISE/ISE-PIC에서 시스템 인증서를 내보냅니다.	ISE/ISE-PIC pxGrid, 모니터링(MNT) 서버 및 FMC를 안전하게 연결하려면 인증서가 있어야 합니다. FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 2495 페이지의 내용을 참조하십시오.
단계 3	영역을 생성합니다.	영역 생성의 유일한 목적은 선택한 사용자 및 그룹을 기준으로 네트워크 액세스를 제어하는 것입니다. 영역 생성, 2466 페이지의 내용을 참조하십시오.
단계 4	사용자 및 그룹을 다운로드하고 영역에서 활성화합니다.	사용자 및 그룹을 다운로드하면 액세스 제어 규칙에서 사용할 수 있습니다. 을 참조하십시오. 사용자 및 그룹 다운로드, 2476 페이지을 참조하십시오.
단계 5	ISE/ISE-PIC ID 소스를 생성합니다.	ISE/ISE-PIC ID 소스를 사용하면 ISE/ISE-PIC가 제공하는 SGT(Security Group Tags)를 사용하여 사용자 활동을 제어할 수 있습니다.

	명령 또는 동작	목적
		사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지의 내용을 참조하십시오.
단계 **6**	ID 정책을 생성합니다.	ID 정책은 하나 이상의 ID 규칙에 대한 컨테이너입니다. ID 정책 생성, 2534 페이지의 내용을 참조하십시오.
단계 **7**	ID 규칙을 생성합니다.	ID 규칙은 영역을 이용해 사용자 및 그룹의 네트워크 액세스를 제어하는 방법을 지정합니다. ID 규칙 생성, 2531 페이지의 내용을 참조하십시오.
단계 **8**	ID 정책을 액세스 제어 정책과 연결합니다.	이렇게 하면 액세스 제어 정책은 영역에 있는 사용자 및 그룹을 사용할 수 있습니다.
단계 **9**	액세스 제어 규칙을 생성합니다.	액세스 제어 규칙은 트래픽이 규칙 기준과 일치할 때 수행할 작업(예: 허용 또는 차단)을 지정합니다. 액세스 제어 규칙에서는 소스 및 대상 SGT 메타데이터를 매칭 기준으로 사용할 수 있습니다. 액세스 제어 규칙 소개, 1645 페이지의 내용을 참조하십시오.
단계 **10**	액세스 제어 정책을 매니지드 디바이스에 구축합니다.	효과를 발휘하려면 정책은 매니지드 디바이스에 구축해야 합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

다음에 수행할 작업

FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 2495 페이지

ISE/ISE-PIC 구성

다음 항목에서는 FMC에서 ID 정책과 함께 사용하도록 ISE/ISE-PIC 서버를 구성하는 방법을 설명합니다.

ISE/ISE-PIC 서버에서 인증서를 내보내 FMC를 이용해 인증하고 SXP 주제를 게시해야 합니다. 이렇게 해야 ISE 서버에서 업데이트된 SGT(Security Group Tags)를 사용하여 FMC를 업데이트할 수 있습니다.

관련 항목

FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 2495 페이지
ISE에서 보안 그룹 및 SXP 게시 구성, 2493 페이지

ISE에서 보안 그룹 및 SXP 게시 구성

TrustSec 정책 및 SGT(Security Group Tag)를 생성하려면 Cisco ISE(Identity Services Engine)에서 수행해야 할 구성이 많이 있습니다. TrustSec을 구현하는 방법에 대한 더 자세한 내용은 ISE 설명서를 참조하십시오.

다음 절차에서는 ISE에서 FTD 디바이스에 대해 구성해야 하는 핵심 설정의 중요 사항을 골라서 설명하므로 이를 따라 정적 SGT-IP 주소 매핑을 다운로드하고 적용할 수 있습니다. 그러면 이 매핑을 액세스 제어 규칙에서 소스 및 대상 SGT 일치에 사용할 수 있습니다. 자세한 내용은 ISE 설명서를 참조하십시오.

이 절차의 스크린 샷은 ISE 2.4를 기준으로 합니다. 이러한 기능에 대한 정확한 경로는 이후 릴리스에서 변경될 수 있지만 개념 및 요구 사항은 동일합니다. ISE 2.4 이상 및 2.6 이상 버전이 권장되더라도 구성은 ISE 2.2 패치 1부터 작동해야 합니다.

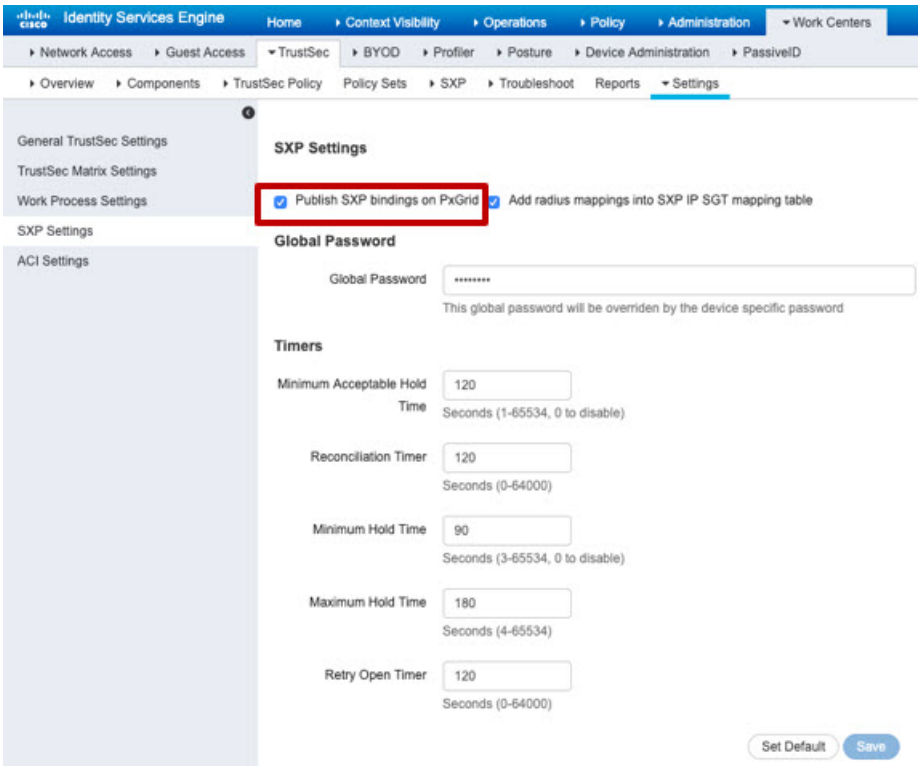
시작하기 전에

SGT-IP 주소 정적 매핑을 게시하고, 사용자 세션-SGT 매핑을 가져와 FTD 디바이스가 이를 수신할 수 있도록 하려면 ISE Plus 라이선스가 있어야 합니다.

프로시저

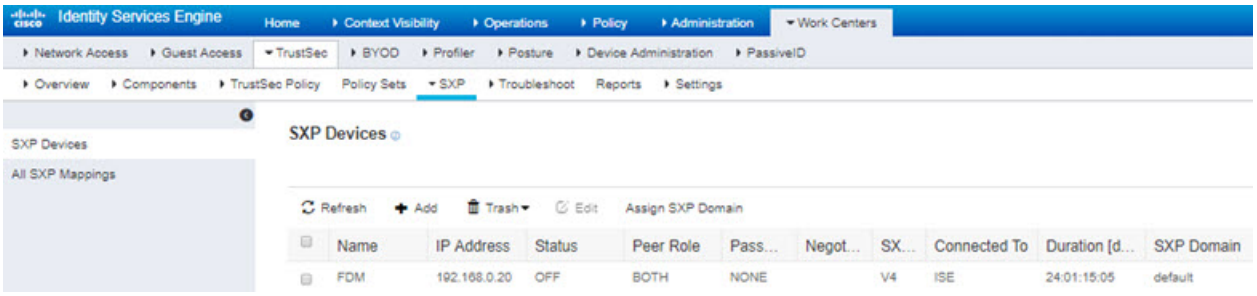
단계 **1** **Work Center(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **SXP Settings(SXP** 설정**)**를 선택하고 **Publish SXP Bindings on PxGrid(PxGrid**에서 **SXP** 바인딩 게시**)** 옵션을 선택합니다.

이 옵션을 선택하면 ISE에서 SXP를 사용하여 SGT 매핑을 전송합니다. FTD 디바이스에서 SXP 항목에 대한 목록의 내용을 "수신 대기"하도록 설정하려면 이 옵션을 선택해야 합니다. 정적 SGT-IP 주소 매핑에 대한 정보를 가져오려면 FTD 디바이스에 대해 이 옵션을 선택해야 합니다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 옵션이 필수 사항이 아닙니다.

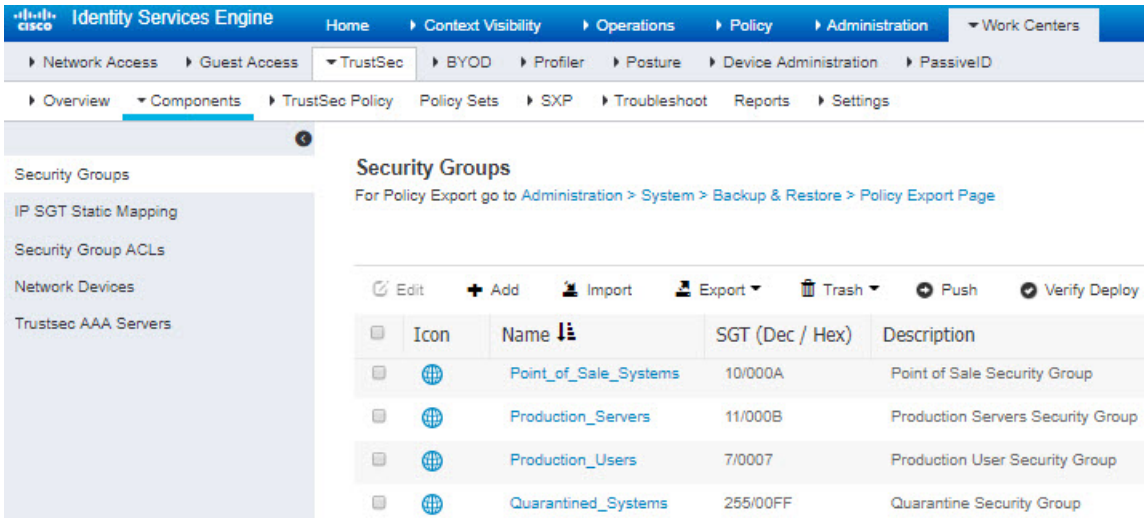


단계 **2** **Work Centers(**작업 센터**)** > **TrustSec** > **SXP** > **SXP Devices(SXP** 디바이스**)**를 선택하고 디바이스를 추가합니다.

이 디바이스가 실제 디바이스일 필요는 없으며, FTD 디바이스의 관리 IP 주소를 사용할 수도 있습니다. 이 표에는 ISE에서 정적 SGT-IP 주소 매핑을 게시하도록 유도하는 디바이스가 하나 이상 필요합니다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.

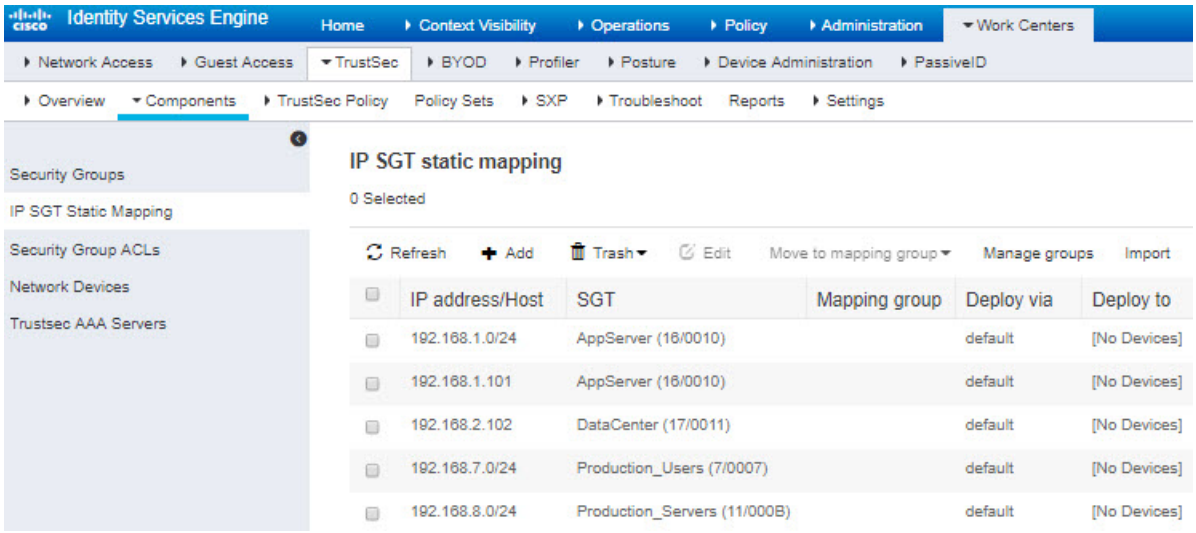


단계 **3** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **Security Groups(**보안 그룹**)**를 선택하고 SGT(Security Group Tag)가 정의되어 있는지 확인합니다. 필요에 따라 새로 생성합니다.



단계 **4** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **IPSGT Static Mapping(IPSGT** 정적 매핑**)**을 선택하고 호스트 및 네트워크 IP 주소를 SGT(Security Group Tag)에 매핑합니다.

단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.



FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기

아래 섹션에서는 다음을 수행하는 방법을 설명합니다.

- ISE/ISE-PIC 서버에서 시스템 인증서를 내보냅니다.

  이러한 인증서는 ISE/ISE-PIC 서버에 안전하게 연결하는 데 필요합니다. ISE 시스템 설정 방법에 따라 1개 또는 최대 3개의 인증서를 내보내야 합니다.

- pxGrid 서버용 인증서 1개
- 모니터링(MNT) 서버용 인증서 1개
- FMC용 인증서 1개(개인 키 포함)

- 이러한 인증서를 FMC로 가져옵니다.

관련 항목

시스템 인증서 내보내기, 2496 페이지
ISE/ISE-PIC 인증서 가져오기, 2497 페이지

시스템 인증서 내보내기

시스템 인증서 또는 인증서와 그 연결된 개인 키를 내보낼 수 있습니다. 인증서 및 해당 개인 키를 백업용으로 내보내는 경우 나중에 필요하면 인증서와 키를 다시 가져올 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

프로시저

단계 **1** 선택 . **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** 인증서만 내보낼지 아니면 인증서 및 연결된 개인 키를 내보낼지를 선택합니다.

팁 인증서와 연결된 개인 키의 값이 노출될 수 있으므로 개인 키는 내보내지 않는 것이 좋습니다. 노드 간 통신용으로 와일드카드 시스템 인증서를 다른 Cisco ISE 노드로 가져오기 위해 내보내는 등의 경우와 같이 개인 키를 내보내야 하는 경우에는 개인 키용 암호화 비밀번호를 지정합니다. 개인 키의 암호를 해독하려면 이 인증서를 다른 Cisco ISE 노드로 가져오는 동안 이 비밀번호를 지정해야 합니다.

단계 **4** 개인 키를 내보내도록 선택한 경우 비밀번호를 입력합니다. 비밀번호는 8자 이상이어야 합니다.

단계 **5** **Export(**내보내기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 파일 시스템에 인증서를 저장합니다.

인증서만 내보내는 경우에는 PEM 형식으로 인증서가 저장됩니다. 인증서와 개인 키를 모두 내보내는 경우에는 PEM 형식 인증서와 암호화된 개인 키 파일을 포함하는 .zip 파일로 인증서가 내보내집니다.

ISE/ISE-PIC 인증서 가져오기

이 절차는 선택사항입니다. 사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지의 설명에 따라 ISE/ISE-PIC ID 소스를 생성할 때 ISE 서버 인증서를 가져올 수도 있습니다.

시작하기 전에

시스템 인증서 내보내기, 2496 페이지의 설명에 따라 ISE/ISE-PIC 서버에서 인증서를 내보냅니다. FMC에 로그인하는 장치에 인증서와 키가 있어야 합니다.

다음 두 가지 유형의 인증서 개체를 가져옵니다.

- ISE/ISE-PIC를 사용하여 인증하는 데 필요한 FMC용 내부 인증서 및 개인 키
- pxGrid 및 ISE 모니터링(MNT) 서버를 위한 신뢰할 수 있는 인증 기관(CA) 1곳 이상

  ISE/ISE-PIC 시스템 설정 방법에 따라 별개의 인증서 2개가 필요할 수도 있고 1개만 필요할 수도 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 FMC에 로그인합니다.
단계 **2** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 클릭합니다.
단계 **3** **PKI**를 확장합니다.
단계 **4** **Internal Certs(**내부 인증서**)**를 클릭합니다.
단계 **5** **Add Internal Cert**를 클릭합니다.
단계 **6** 화면에 표시되는 메시지에 따라 인증서와 개인 키를 가져옵니다.
단계 **7** **Trusted CAs(**신뢰할 수 있는 **CA)**를 클릭합니다.
단계 **8** **Add Trusted CA(**신뢰하는 **CA** 추가**)**를 클릭합니다.
단계 **9** 화면에 표시되는 메시지에 따라 pxGrid 서버 인증서를 가져옵니다.
단계 **10** 필요하다면 앞의 단계를 반복하여 MNT 서버의 신뢰할 수 있는 CA를 가져옵니다.

다음에 수행할 작업

사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지

사용자 제어를 위한 ISE/ISE-PIC 설정

다음 절차에서는 ISE/ISE-PIC ID 소스를 구성하는 방법을 설명합니다. 이 작업을 수행하려면 전역 도메인에 있어야 합니다.

시작하기 전에

- Microsoft Active Directory 서버 또는 지원되는 LDAP 서버에서 사용자 세션을 가져오려면, 영역 생성, 2466 페이지의 설명에 따라 pxGrid 가상 사용자를 가정하여 ISE 서버에 대한 영역을 구성하고 활성화합니다.
- ISE 또는 ISE-PIC 연결을 구성합니다. 자세한 내용은 ISE/ISE-PIC ID 소스, 2485 페이지 및 ISE/ISE-PIC 설정 필드, 2499 페이지를 참조하십시오.
- SXP를 통해 게시된 SGT-IP 주소 매핑을 비롯한 ISE에 정의된 모든 매핑을 가져오려면 다음 절차를 따르십시오. 다음 옵션을 사용할 수도 있습니다.
  - 패킷에 있는 SGT 정보만 사용하고 ISE에서 다운로드한 매핑은 사용하지 않으려면, 액세스 제어 규칙 생성 및 수정, 1651 페이지에서 설명하는 단계는 건너뛰십시오. 이 경우에는 SGT 태그를 소스 조건으로만 사용할 수 있으며 이러한 태그는 대상 기준과 일치하지 않습니다.
  - 패킷과 사용자 대 IP 주소/SGT 매핑만 사용하려면, ISE ID 소스의 SXP 주제는 구독해선 안 되며, SXP 매핑을 게시하도록 ISE를 구성해선 안 됩니다. 소스 및 대상 일치 조건 둘 다에 이 정보를 사용할 수 있습니다.
- ISE/ISE-PIC 서버에서 인증서를 내보내고, 원한다면 FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 2495 페이지의 설명에 따라 FMC에 인증서를 가져옵니다.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **System(**시스템**)** > **Integration(**통합**)** 버튼을 클릭합니다.

단계 **3** **Identity Sources(ID** 소스**)**를 클릭합니다.

단계 **4** ISE 연결을 활성화하려면 **Service Type(**서비스 유형**)**으로 **Identity Services Engine(ID** 서비스 엔진**)**을 클릭합니다.

참고 연결을 비활성화하려면 **None(**없음**)**을 클릭합니다.

단계 **5** **Primary Host Name/IP Address(**기본 호스트 이름**/IP** 주소**)**를 입력하고 필요에 따라 **Secondary Host Name/IP Address(**보조 호스트 이름**/IP** 주소**)**를 입력합니다.

단계 **6** **PxGrid Server CA** 및 **MNT** 서버 **CA** 목록에서 적절한 인증서 인증 기관과 **FMC** 서버 인증서 목록에서 적절한 인증서를 클릭합니다. 추가(+)을 클릭하여 인증서를 추가할 수도 있습니다.

참고 **FMC Server Certificate(FMC** 서버 인증서**)**에는 **clientAuth** 확장된 키 사용 값을 포함해야 하거나, 확장된 키 사용 값을 포함하지 않아야 합니다.

단계 **7** (선택 사항). CIDR 블록 표기법을 사용하려면 **ISE Network Filter(ISE** 네트워크 필터**)**를 입력합니다.

단계 **8** Subscribe To(구독 대상) 섹션에서 다음을 확인합니다.

- ISE 서버에서 ISE 사용자 세션 정보를 가져오는 **Session Directory Topic(**세션 디렉터리 주제

- ISE 서버에서 제공하는 SGT-to-IP 매핑에 대한 업데이트를 수신하는 **SXP** 주제 이 옵션은 액세스 제어 규칙에서 목적지 SGT 태깅을 사용할 때 필요합니다.

단계 **9** 연결을 테스트하려면 **Test(**테스트**)**를 클릭합니다.

다음에 수행할 작업

- ID 정책 생성, 2534 페이지에 설명된 대로 ID 정책을 사용하여 제어할 사용자 및 기타 옵션을 지정합니다.
- 액세스 제어에 다른 정책 연결, 1641 페이지에 설명된 대로 ID 규칙을 트래픽을 필터링하고 필요에 따라 검사하는 액세스 제어 규칙과 연결합니다.
- 컨피그레이션 변경 사항 구축, 498 페이지에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- 워크플로 사용, 2793 페이지에 설명된 대로 사용자 활동을 모니터링합니다.

관련 항목

ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결, 2500 페이지
신뢰할 수 있는 인증 기관 개체, 624 페이지
내부 인증서 개체, 627 페이지

ISE/ISE-PIC 설정 필드

다음 필드를 사용하여 ISE/ISE-PIC에 대한 연결을 구성합니다.

Primary and Secondary Host Name/IP Address(기본 및 보조 호스트 이름**/IP** 주소**)**

기본과 보조 pxGrid ISE 서버(선택 사항)의 호스트 이름 또는 IP 주소입니다.

사용자가 지정한 호스트 이름이 사용한 포트는 ISE와 Firepower Management Center 모두가 연결할 수 있어야 합니다.

pxGrid 서버 **CA**

PxGrid 프레임워크용 인증 증명입니다. 구축에 기본 및 보조 pxGrid 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.

MNT 서버 **CA**

벌크 다운로드 수행 시의 ISE 인증서용 인증 증명입니다. 구축에 기본 및 보조 MNT 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.

FMC 서버 인증서

ISE/ISE-PIC에 연결하거나 벌크 다운로드를 수행하려면 Firepower Management Center에서 ISE/ISE-PIC에 제공해야 하는 인증서와 키입니다.

참고 **FMC Server Certificate(FMC** 서버 인증서**)**에는 clientAuth 확장된 키 사용 값을 포함해야 하거나, 확장된 키 사용 값을 포함하지 않아야 합니다.

ISE 네트워크 필터

ISE가 Firepower Management Center에 보고하는 데이터를 제한하기 위해 설정할 수 있는 선택적 필터입니다. 네트워크 필터를 제공하는 경우 ISE는 필터 내의 네트워크에서 데이터를 보고합니다. 다음과 같은 방법으로 필터를 지정할 수 있습니다.

- **any (**모두**)** 를 지정하려면 필드를 비워 둡니다.
- CIDR 표기법을 사용하여 단일 IPv4 주소 블록을 입력합니다.
- CIDR 표기법을 사용하여 IPv4 주소 블록 목록을 쉼표로 구분해 입력합니다.

참고 이 Firepower System 버전에서는 ISE 버전에 관계없이 IPv6 주소를 사용한 필터링을 지원하지 않습니다.

구독**:**

Session Directory Topic(세션 디렉토리 주제**)**:이 확인란을 선택하면 ISE 서버에서 사용자 세션 정보를 구독할 수 있습니다. SGT 및 엔드포인트 메타데이터를 포함합니다.
SXP Topic(SXP 주제**)**: 이 확인란을 선택하면 ISE 서버에서 SXP 매핑을 구독합니다.

관련 항목

신뢰할 수 있는 인증 기관 개체, 624 페이지
내부 인증서 개체, 627 페이지

ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결

Cisco TrustSec 문제 해결

디바이스 인터페이스는 ISE/ISE-PIC 또는 네트워크의 Cisco 디바이스(Cisco TrustSec이라고 함)에서 SGT(Security Group Tag)를 전파하도록 설정할 수 있습니다. Device Management(디바이스 관리) 페이지(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**)에서 디바이스를 재부팅하고 나면 인터페이스에 대한 **Propagate Security Group Tag(**보안 그룹 태그 전파**)** 확인란이 선택됩니다. 인터페이스에서 TrustSec 데이터를 전파하지 않도록 하려면 확인란의 선택을 취소합니다.

ISE/ISE-PIC 문제 해결

기타 관련 문제 해결 정보를 보려면 영역 및 사용자 다운로드 문제 해결, 2480 페이지 및 사용자 제어 문제 해결, 549 페이지을 참조하십시오.

ISE 또는 ISE-PIC 연결에 문제가 발생한 경우 다음을 확인하십시오.

- ISE를 Firepower System과 성공적으로 통합하려면 우선 ISE에서 pxGrid Identity Mapping(pxGrid ID 매핑) 기능을 활성화해야 합니다.
- 기본 서버가 실패하는 경우, 사용자는 보조를 기본으로 직접 승격해야 합니다. 자동 페일오버는 실행되지 않습니다.
- ISE 서버와 Firepower Management Center 디바이스 간의 연결에 성공하려면 ISE에서 클라이언트를 수동으로 승인해야 합니다. (일반적으로 클라이언트 두 개가 존재합니다. 하나는 연결 테스트용이며, 다른 하나는 ISE 에이전트용입니다.)

  또한 *Cisco Identity Services Engine* 관리자 가이드의 사용자 및 외부 ID 소스 관리 장에서 설명하는 것처럼 ISE에서 **Automatically approve new accounts(**새 어카운트 자동 승인**)**를 활성화할 수도 있습니다.
- **FMC Server Certificate(FMC** 서버 인증서**)**에는 **clientAuth** 확장된 키 사용 값을 포함해야 하거나, 확장된 키 사용 값을 포함하지 않아야 합니다.
- ISE 서버의 시간은 Firepower Management Center의 시간과 동기화되어야 합니다. 어플라이언스가 동기화되지 않은 경우, 시스템이 예기치 않은 간격으로 사용자 시간 초과를 수행할 수 있습니다.
- 구축에 기본 및 보조 pxGrid 노드가 포함되는 경우,
  - 두 노드의 인증서에 같은 인증 기관이 서명해야 합니다.
  - 호스트 이름이 사용한 포트는 ISE 서버와 Firepower Management Center 모두가 연결할 수 있어야 합니다.
- 구축에 기본 및 보조 MNT 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.

ISE에서 사용자-IP 및 SGT(Security Group Tag)-IP 매핑을 수신하는 서브넷을 제외하려면 **configure identity-subnet-filter** {**add** | **remove**} 명령을 사용합니다. 일반적으로 Snort ID 상태 모니터 메모리 오류를 방지하기 위해 메모리 부족 관리 디바이스에 대해 이 작업을 수행해야 합니다.

ISE 또는 ISE-PIC에서 보고된 사용자 데이터에 문제가 발생한 경우 다음을 참고하십시오.

- 데이터베이스에 데이터가 아직 없는 ISE 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. 시스템이 사용자 다운로드에서 사용자에 대한 정보를 성공적으로 검색할 때까지 ISE 사용자가 보여준 활동이 액세스 제어 규칙으로 처리되지 않으며, 웹 인터페이스에 표시되지도 않습니다.
- LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.
- Firepower Management Center는 ISE 게스트 서비스 사용자의 데이터를 수신하지 않습니다.
- ISE 버전 및 컨피그레이션은 Firepower System에서 ISE를 사용할 수 있는 방법에 영향을 미칩니다. 자세한 정보는 ISE/ISE-PIC ID 소스, 2485 페이지의 내용을 참고하십시오.
-
- ISE-PIC는 ISE 속성 데이터를 제공하지 않습니다.

- ISE-PIC는 ANC 교정을 수행할 수 없습니다.
- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 RFC 959를 참조하십시오.

지원되는 기능에 문제가 발생할 경우 ISE/ISE-PIC ID 소스, 2485 페이지에서 버전 호환성에 대한 자세한 내용을 참조하십시오.

ISE/ISE-PIC 기록

기능	버전	세부 사항
pxGrid 2.0은 지원되는 ISE/ISE-PIC 버전의 기본값입니다.	6.7.0	다음에 유의하십시오. • 지원되는 ISE/ISE-PIC 버전: 2.6 패치 6 이상, 2.7 패치 2 이상 • 적응형 네트워크 제어(ANC) 정책은 EPS(Endpoint Protection Service) 교정을 대체합니다. FMC에 EPS 정책이 구성된 경우 ANC를 사용하려면 마이그레이션해야 합니다.
선택적으로 ISE에서 사용자-IP 및 SGT(Security Group Tag)-IP 매핑을 수신하는 서브넷을 제외합니다. 일반적으로 Snort ID 상태 모니터 메모리 오류를 방지하기 위해 메모리 부족 관리 디바이스에 대해 이 작업을 수행해야 합니다.	6.7.0	새 명령: **configure identity-subnet-filter** {**add** | **remove**}

기능	버전	세부 사항
대상 SGT 매칭(Security Group Tag)	6.5.0	기능이 도입되었습니다. 액세스 제어 규칙의 소스 및 대상 매칭 기준 모두에 대해 ISE SGT 태그를 사용할 수 있습니다. SGT 태그는 ISE에서 얻은 태그-호스트/네트워크 매핑입니다. 신규/수정된 화면: • 대상 SGT 매칭을 구성하는 방법: **System(**시스템**)** > **Integration(**통합**)** > **Identity Sources(ID** 소스**)** > **ISE/ISE-PIC** • **Session Directory Topic(**세션 디렉토리 주제**)**:ISE 서버 세션 정보를 구독합니다. • **SXP Topic(SXP** 주제**)**: ISE 서버에서 SGT 태그 업데이트를 구독합니다. • **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**의 신규 및 이름 변경된 열 • 이름 변경: 보안 그룹 태그가 소스 SGT로 변경되었습니다. • 신규: 대상 SGT
ISE-PIC와의 통합	6.2.1	이제 ISE-PIC의 데이터를 사용할 수 있습니다.
ISE와 통합되었습니다.	6.0	기능이 도입되었습니다. Cisco의 PxGrid(Platform Exchange Grid)를 구독하면, Firepower Management Center는 추가적인 사용자 데이터, 디바이스 유형 데이터, 디바이스 위치 데이터 및 SGT(Security Group Tag, 네트워크 액세스 제어 기능을 제공하기 위해 ISE에서 사용하는 방법)를 다운로드할 수 있습니다.

99 장

캡티브 포털을 사용하여 사용자 제어

- 캡티브 포털 ID 소스, 2505 페이지
- 캡티브 포털 라이선스 요구 사항, 2506 페이지
- 캡티브 포털 요구 사항 및 사전 요건, 2506 페이지
- 캡티브 포털 가이드라인 및 제한 사항, 2506 페이지
- 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지
- 캡티브 포털(captive portal) ID 소스 문제 해결, 2518 페이지
- 캡티브 포털 기록, 2519 페이지

캡티브 포털 ID 소스

캡티브 포털(captive portal)은 Firepower System에서 지원하는 권한 있는 ID 소스 중 하나입니다. 이는 관리되는 디바이스를 사용해 네트워크에서 사용자가 인증하는 액티브 인증 방법입니다.

인터넷 또는 제한적 리소스에 액세스하기 위한 인증을 요구하기 위해 캡티브 포털을 사용합니다. 선택적으로 리소스에 게스트 액세스를 설정할 수 있습니다. 시스템이 캡티브 포털 사용자를 인증하면 액세스 제어 규칙에 따라 사용자 트래픽을 처리합니다. 캡티브 포털은 HTTP와 HTTPS 트래픽에 한해 인증을 수행합니다.

참고 캡티브 포털이 인증을 수행할 수 있기 전에 HTTPS 트래픽의 암호를 해독해야 합니다.

캡티브 포털(captive portal)은 실패한 인증 시도도 기록합니다. 실패한 시도는 데이터베이스의 사용자 목록에 새 사용자를 추가하지 않습니다. 캡티브 포털(captive portal)에서 보고하는 실패한 인증 활동의 사용자 활동 유형은 **Failed Auth User(**실패한 인증 사용자**)**입니다.

캡티브 포털(captive portal)에서 수집한 인증 데이터는 사용자 인식 및 사용자 제어에 사용할 수 있습니다.

관련 항목

사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지

캡티브 포털 라이선스 요구 사항

FTD 라이센스

Any(모든 상태)

기본 라이선스

제어

캡티브 포털 요구 사항 및 사전 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

캡티브 포털 가이드라인 및 제한 사항

ID 정책에서 캡티브 포털(captive portal)을 구성 및 구축할 경우, 지정된 영역의 사용자는 다음 디바이스를 통해 네트워크에 대한 액세스를 인증합니다.

- 7000 및 8000 Series 디바이스의 가상 라우터
- 버전 9.5(2) 이상을 실행하는 라우팅 모드의 ASA FirePOWER 디바이스
- 라우팅 모드의 Firepower Threat Defense 디바이스

참고 원격 액세스 VPN 사용자가 보안 게이트웨이로 작동하는 매니지드 디바이스를 통해 이미 활성으로 인증된 경우에는 ID 정책에 구성되어 있더라도 캡티브 포털(captive portal) 액티브 인증이 이루어지지 않습니다.

라우팅 인터페이스 필요

캡티브 포털(captive portal) 액티브 인증은 라우팅 인터페이스가 구성된 디바이스에서만 수행할 수 있습니다.

액세스 제어 정책에서 참조한 ID 정책에 하나 이상의 캡티브 포털(captive portal) ID 규칙이 포함되어 있고 다음을 관리하는 Firepower Management Center에서 정책을 구축할 경우:

- 라우팅 인터페이스가 구성된 하나 이상의 디바이스 - 정책 구축에 성공하고 라우팅 인터페이스가 액티브 인증을 수행합니다.

  시스템은 ASA with FirePOWER 디바이스에서 인터페이스의 유형을 검증하지 않습니다. ASA with FirePOWER 디바이스에서 인라인(탭 모드) 인터페이스에 캡티브 포털 정책을 적용하면 정책 구축은 성공하지만 해당 규칙과 일치하는 트래픽의 사용자는 Unknown(알 수 없음)으로 식별됩니다.

- 하나 이상의 NGIPSv 디바이스 - 정책 구축에 실패합니다.

캡티브 포털 및 정책

ID 정책에서 캡티브 포털(captive portal)을 구성하고 ID 규칙에서 액티브 인증을 호출합니다. ID 정책은 액세스 컨트롤 정책과 연결됩니다.

액세스 컨트롤 정책의 **Active Authentication(**액티브 인증**)** 탭 페이지에서 캡티브 포털 ID 정책 일부를 설정하고 액세스 컨트롤 정책과 연결된 ID 규칙에서 나머지를 설정할 수 있습니다.

주의 SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거함 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

캡티브 포털 요건 및 제한 사항

다음 요건 및 제한 사항을 참고하십시오.

- 시스템은 초당 최대 20개의 캡티브 포털(captive portal) 로그인을 지원합니다.
- 실패한 로그인 시도가 최대 로그인 시도 횟수에 적용될 때, 실패한 로그인 시도 사이에는 최대 5분의 제한이 적용됩니다. 5분 제한은 사용자가 설정할 수 없습니다.

  (최대 로그인 시도는 연결 이벤트: **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**에 표시됩니다.)

  실패한 로그인 사이의 경과 시간을 5분을 초과하는 경우 사용자는 인증을 위해 캡티브 포털로 재전송되며, 실패한 로그인 사용자나 게스트 사용자로 지정하지 않고, Firepower Management Center에 보고되지 않습니다.

- 캡티브 포털은 TLS v1.0 연결을 협상하지 않습니다.

TLS v1.1 및 v1.2 연결만 지원됩니다.

- 사용자 로그아웃을 확인하는 유일한 방법은 브라우저를 닫고 다시 여는 것입니다. 그러지 않으면, 경우에 따라 사용자가 캡티브 포털에서 로그아웃한 다음 같은 브라우저를 이용해 다시 인증하지 않고도 네트워크에 액세스할 수 있습니다.
- 영역이 상위 도메인에 대해 생성되었고 매니지드 디바이스가 해당 상위 도메인의 하위 도메인에 대한 로그인을 탐지했다면, 사용자의 이후 로그아웃은 매니지드 디바이스가 탐지하지 않습니다.
- 캡티브 포털(captive portal)에 ASA FirePOWER 디바이스를 사용하려는 경우(ASA 버전 9.5(2) 이상을 실행하는 라우팅 모드에서), **captive-portal** ASA CLI 명령을 사용하여 액티브 인증을 위한 캡티브 포털(captive portal)을 활성화하고 *ASA Firewall* 설정 가이드(버전 9.5(2) 이상): https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html에 설명된 대로 포트를 정의합니다.
- 캡티브 포털에 사용할 디바이스의 IP 주소 및 포트를 대상으로 하는 트래픽을 허용해야 합니다.
- HTTPS 트래픽에 대한 캡티브 포털(captive portal) 액티브 인증을 수행하려면, SSL 정책을 사용하여 인증하려는 사용자의 트래픽을 암호 해독해야 합니다. 매니지드 디바이스에서 캡티브 포털(captive portal) 사용자의 웹 브라우저와 캡티브 포털(captive portal) 데몬 간의 연결에서 트래픽을 암호 해독할 수 없습니다. 이 연결은 캡티브 포털(captive portal) 사용자를 인증하는 데 사용됩니다.
- 매니지드 디바이스를 통해 허용되는 비 HTTP 또는 HTTPS 트래픽의 양을 제한하려면 ID 정책의 **Ports(포트)** 탭 페이지에 일반적인 HTTP 및 HTTPS 포트를 입력해야 합니다.

  매니지드 디바이스는 수신하는 요청이 HTTP 또는 HTTPS 프로토콜을 사용하지 않는다고 판단하면 이전에 확인하지 않은 사용자를 **Pending(보류 중)**에서 **Unknown(알 수 없음)**으로 변경합니다. 매니지드 디바이스가 사용자를 **Pending(보류 중)**에서 다른 상태로 변경하면, 액세스 컨트롤과 서비스 품질 및 SSL 정책이 해당 트래픽에 적용될 수 있습니다. 다른 정책이 비 HTTP 또는 HTTPS 트래픽을 허용하지 않는다면, 캡티브 포털 ID 정책에 대한 포트 설정으로 원치 않는 트래픽이 매니지드 디바이스를 통해 허용되는 일을 방지할 수 있습니다.

사용자 제어에 대한 캡티브 포털 설정 방법

캡티브 포털로 사용자 활동을 제어하는 방법 개요:

시작하기 전에

캡티브 포털을 액티브 인증에 활용하려면, 액세스 컨트롤 정책과 ID 정책, SSL 정책을 설정하고 ID와 SSL 정책을 액세스 컨트롤 정책에 연결해야 합니다. 마지막으로, 사용자는 정책을 매니지드 디바이스에 구축해야 합니다. 이 주제는 이러한 작업에 대한 개략적인 정보를 제공합니다.

전체 절차 예시는 캡티브 포털 설정 1부: ID 정책 생성, 2510 페이지에서부터 시작합니다.

먼저 다음 작업을 수행하십시오.

- 라우팅 인터페이스가 구성된 하나 이상의 디바이스를 Firepower Management Center에서 관리하는지 확인합니다.

  특히 Firepower Management Center가 FirePOWER 디바이스를 이용해 ASA를 관리한다면, 캡티브 포털 가이드라인 및 제한 사항, 2506 페이지을(를) 반드시 참조하십시오.

- 암호화된 인증을 캡티브 포털과 함께 사용하려면 PKI 개체를 만들거나, 액세스하는 Firepower Management Center의 장치에서 인증서 데이터와 키를 사용할 수 있게 해야 합니다. PKI 개체를 생성하는 방법은 PKI 개체, 618 페이지 섹션을 참조하십시오.

프로시저

단계 **1** 다음 주제에서 설명하는 방법에 따라 영역을 생성하고 활성화합니다.

- 영역 디렉터리 설정, 2475 페이지
- 사용자 및 그룹 다운로드, 2476 페이지

단계 **2** 캡티브 포털에 대한 액티브 인증 ID 정책을 생성합니다.

ID 정책을 이용하면 영역에 있는 선택된 사용자는 캡티브 포털로 인증 후 리소스에 액세스할 수 있습니다.

자세한 내용은 캡티브 포털 설정 1부: ID 정책 생성, 2510 페이지를 참고하십시오.

단계 **3** 캡티브 포털 포트(기본적으로 TCP 885)의 트래픽을 허용하는, 캡티브 포털에 대한 액세스 컨트롤 규칙을 설정합니다.

캡티브 포털이 사용할 수 있는 모든 TCP 포트를 선택할 수 있습니다. 어떤 포트를 선택하든, 해당 포트에서의 트래픽을 허용하는 규칙을 생성해야 합니다.

자세한 내용은 캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 2512 페이지를 참고하십시오.

단계 **4** 다른 액세스 컨트롤 규칙을 추가해 선택한 영역의 사용자가 캡티브 포털을 이용해 리소스에 액세스하게 합니다.

이렇게 하면 사용자는 캡티브 포털을 이용해 인증할 수 있습니다.

자세한 내용은 캡티브 포털 설정 3부: 사용자 액세스 컨트롤 규칙 생성, 2513 페이지를 참고하십시오.

단계 **5** SSL 암호 해독 설정 - 캡티브 포털 사용자가 HTTPS 프로토콜을 이용해 웹 페이지에 액세스할 수 있도록 **Unknown(**알 수 없는**)** 사용자에 대한 정책을 재서명합니다.

캡티브 포털은 먼저 HTTPS 트래픽이 해독된 후 캡티브 포털로 전송된 경우에만 사용자를 인증할 수 있습니다. 캡티브 포털은 시스템이 **Unknown(**알 수 없는**)** 사용자로 인식합니다.

자세한 내용은 캡티브 포털 설정 4부: SSL 암호 해독 생성-정책 재서명, 2514 페이지를 참고하십시오.

단계 **6** ID 및 SSL p정책을 2단계의 액세스 컨트롤 정책에 연결합니다.

이 마지막 단계는 시스템이 캡티브 포털을 이용해 인증하게 합니다.

자세한 내용은 캡티브 포털 설정 5부: ID 및 SSL 정책과 액세스 컨트롤 정책 연결, 2515 페이지를 참고하십시오.

다음에 수행할 작업

캡티브 포털 설정 1부: ID 정책 생성, 2510 페이지의 내용을 참조하십시오.

관련 항목

캡티브 포털에서 애플리케이션 제외, 2517 페이지
PKI 개체, 618 페이지
캡티브 포털(captive portal) ID 소스 문제 해결, 2518 페이지
Snort® 재시작 시나리오, 505 페이지

캡티브 포털 설정 1부: ID 정책 생성

시작하기 전에

이 5단계 절차는 캡티브 포털과 SSL 암호화 모두에 대해 기본 TCP 포트 885와 Firepower Management Center 서버 인증서를 사용해 캡티브 포털을 설정하는 방법을 보여줍니다. 이 예시의 각 단계는 액티브 인증 수행을 위해 캡티브 포털을 활성화하는 데 필요한 작업을 하나씩 설명합니다.

이 절차의 모든 단계를 수행하면, 도메인에 있는 사용자를 위해 작동하도록 캡티브 포털을 설정할 수 있습니다. 원한다면 절차의 각 단계에서 설명하는 추가 작업을 수행할 수도 있습니다.

전체 절차의 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지에서 확인할 수 있습니다.

프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **Policies(**정책**)** > **Access Control(**액세스 컨트롤**)** > **Identity(ID)**를 클릭하고 ID 정책을 만들거나 편집합니다.

단계 3 (선택 사항). **Add Category(**카테고리 추가**)**를 클릭해 캡티브 포털 ID 규칙의 카테고리를 추가하고 카테고리의 **Name(**이름**)**을 입력합니다.

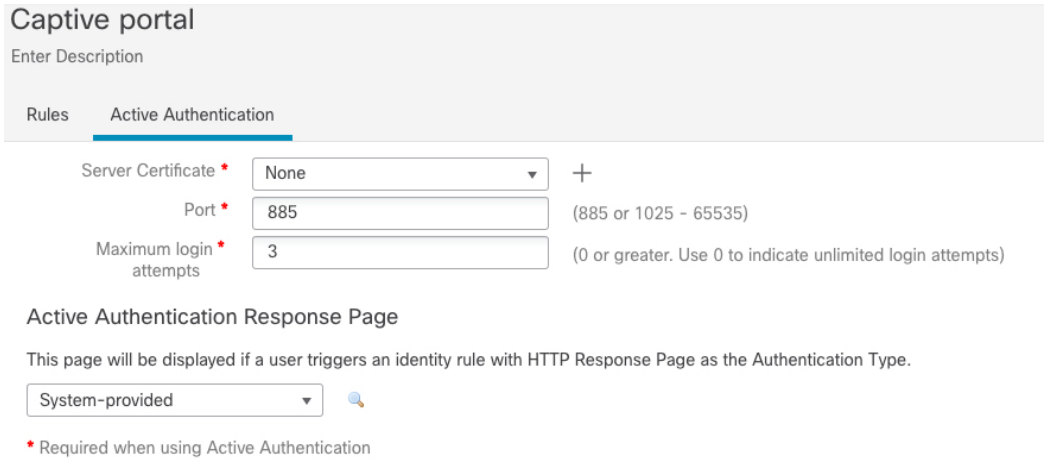
단계 4 **Active Authentication(**활성 인증**)**을 클릭합니다.

단계 5 목록에서 적절한 **Server Certificate(**서버 인증서**)**를 선택하거나 추가(+)를 클릭하여 인증서를 추가합니다.

참고 캡티브 포털은 DSA(Digital Signature Algorithm) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서 사용을 지원하지 않습니다.

단계 6 **885**을(를) **Port(**포트**)** 필드에 입력하고 **Maximum login attempts(**최도 로그인 시도 횟수**)**를 지정합니다.

단계 7 (선택 사항). 캡티브 포털(captive portal) 필드, 2516 페이지에 설명된 대로 **Active Authentication Response Page(**액티브 인증 응답 페이지**)**를 선택합니다.
다음 그림은 예를 보여줍니다.



단계 8 **Save(**저장**)**를 클릭합니다.

단계 9 **Rules(**규칙**)**를 클릭합니다.

단계 10 **Add Rule(**규칙 추가**)**를 클릭하여 새 캡티브 포털 ID 정책 규칙을 추가하거나 수정( )을 클릭하여 기존 규칙을 편집합니다.

단계 11 규칙의 **Name(**이름**)**을 입력합니다.

단계 12 **Action(**작업**)** 목록에서 **Active Authentication(**액티브 인증**)**을 선택합니다.

시스템은 HTTP 및 HTTPS 트래픽에서만 캡티브 포털 액티브 인증을 시행할 수 있습니다. ID 규칙 **Action(**작업**)**이 **Active Authentication(**액티브 인증**)**(사용자가 캡티브 포털을 이용 중임)이거나, 사용자가 패시브 인증을 이용하며 **Realms & Settings(**영역 및 설정**)** 페이지에서 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없다면 액티브 인증 사용**)**에 대한 옵션을 선택했다면 TCP 포트 제약 조건만 사용합니다.

단계 13 **Realm & Settings(**영역 및 설정**)**를 클릭합니다.

단계 14 **Realms(**영역**)** 목록에서 사용자 인증에 사용할 영역을 선택합니다.

단계 15 (선택 사항). **Identify as Guest if authentication cannot identify user(**인증이 사용자를 식별할 수 없는 경우 게스트로 식별**)**를 선택합니다. 자세한 내용은 캡티브 포털(captive portal) 필드, 2516 페이지를 참고하십시오.

단계 16 목록에서 **Authentication Protocol(**인증 프로토콜**)**을 선택합니다.

단계 17 (선택 사항). 특정 애플리케이션 트래픽을 캡티브 포털에서 제외하는 방법은 캡티브 포털에서 애플리케이션 제외, 2517 페이지 섹션을 참조하십시오.

단계 18 규칙 조건 유형, 525 페이지에 설명된 대로 조건을 규칙(포트, 네트워크 등)에 추가합니다.

단계 19 **Add(**추가**)**를 클릭합니다.

단계 20 페이지 상단에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 2512 페이지를 계속 진행합니다.

캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성

절차의 이 부분은 캡티브 포털이 캡티브 포털의 기본 포트인 TCP 포트 885를 이용해 클라이언트로 통신하게 하는, 액세스 컨트롤 규칙 생성 방법을 보여줍니다. 원한다면 다른 포트를 선택할 수도 있지만, 반드시 캡티브 포털 설정 1부: ID 정책 생성, 2510 페이지에서 선택한 포트여야 합니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지에서 확인할 수 있습니다.

프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 아직 하지 않았다면, PKI 개체, 618 페이지에 설명된 대로 종속 포털에 대한 인증서를 만듭니다.

단계 3 **Policies**(정책) > **Access Control**(액세스 제어) > **Access Control**(액세스 제어)을 클릭하고 액세스 컨트롤 정책을 편집합니다.

단계 4 **Add Rule**(규칙 추가)을 클릭합니다.

단계 5 규칙의 **Name**(이름)을 입력합니다.

단계 6 **Action**(작업) 목록에서 **Allow**(허용)를 선택합니다.

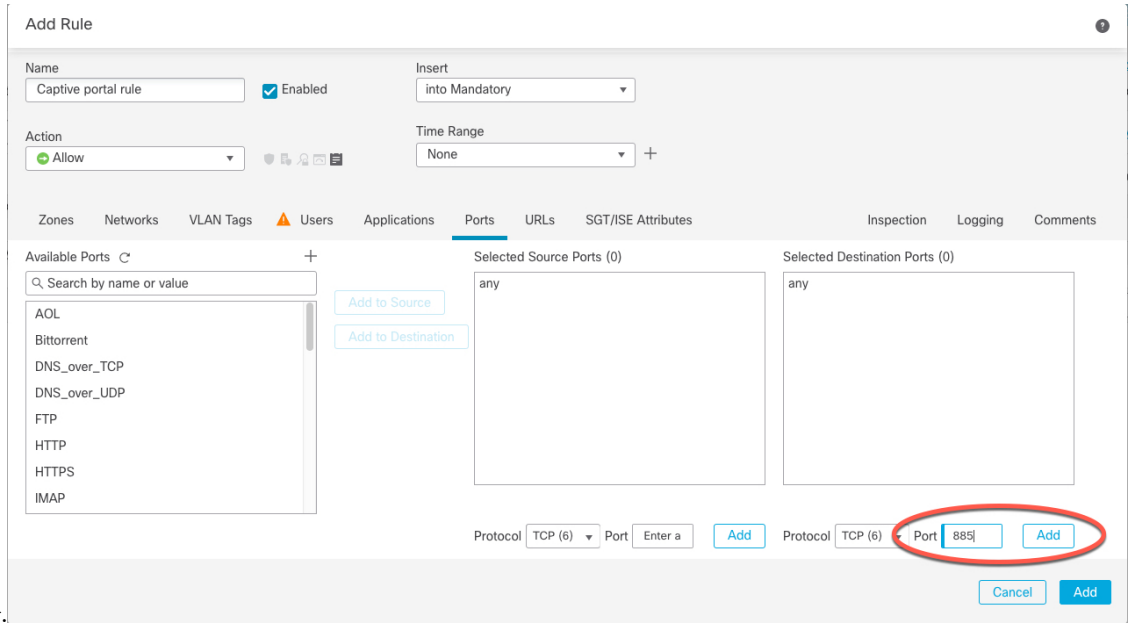
단계 7 **Ports**(포트)를 클릭합니다.

단계 8 **Selected Destination Ports**(선택한 대상 포트)의 **Protocol**(프로토콜) 목록에서 **TCP**를 선택합니다.

단계 9 **Port**(포트) 필드에 **885**을(를) 입력합니다.

단계 10 **Port**(포트) 필드에 **Add**(추가)를 클릭합니다.

다음 그림은 관련 예시를 보여줍니



다.

단계 **11** 페이지 하단의 **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 설정 3부: 사용자 액세스 컨트롤 규칙 생성, 2513 페이지를 계속 진행합니다.

캡티브 포털 설정 3부: 사용자 액세스 컨트롤 규칙 생성

절차의 이 부분은 영역 내 사용자가 캡티브 포털을 이용해 인증할 수 있게 하는 액세스 컨트롤 규칙을 추가하는 방법을 설명합니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지에서 확인할 수 있습니다.

프로시저

단계 **1** 규칙 편집기에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **2** 규칙의 **Name(**이름**)**을 입력합니다.

단계 **3** **Action(**작업**)** 목록에서 **Allow(**허용**)**를 선택합니다.

단계 **4** **Users(**사용자**)**를 클릭합니다.

단계 **5** **Available Realms(**사용 가능한 영역**)** 목록에서 허용할 영역을 클릭합니다.

단계 **6** 영역이 표시되지 않는다면 새로 로침( )을 클릭합니다.

단계 7 **Available Users(**사용 가능한 사용자**)** 목록에서 규칙에 추가할 사용자를 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.

단계 8 (선택 사항). 규칙 조건 유형, 525 페이지에 설명된 대로 액세스 컨트롤 정책에 조건을 추가합니다.

단계 9 **Add(**추가**)**를 클릭합니다.

단계 10 액세스 컨트롤 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

단계 11 정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다. 규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

다음에 수행할 작업

캡티브 포털 설정 4부: SSL 암호 해독 생성-정책 재서명, 2514 페이지를 계속 진행합니다.

캡티브 포털 설정 4부: SSL 암호 해독 생성-정책 재서명

절차의 이 부분은 트래픽이 캡티브 포털에 도달하기 전에 트래픽을 해독하고 재서명하는 SSL 액세스 정책을 생성하는 방법을 설명합니다. 캡티브 포털은 해독한 트래픽만 인증할 수 있습니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지에서 확인할 수 있습니다.

프로시저

단계 1 아직 하지 않았다면, PKI 개체, 618 페이지에 설명된 대로 SSL 트래픽을 해독하는 인증서 개체를 만듭니다.

단계 2 **Policies(**정책**)** > **Access Control(**액세스 컨트롤**)** > **SSL**을 클릭합니다.

단계 3 **New Policy(**새로운 정책**)**를 클릭합니다.

단계 4 **Name(**이름**)**을 입력하고 정책에 대한 **Default Action(**기본 작업**)**을 선택합니다. 기본 작업은 SSL 정책 기본 작업, 1794 페이지에서 설명합니다.

단계 5 **Save(**저장**)**를 클릭합니다.

단계 6 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 7 규칙의 **Name(**이름**)**을 입력합니다.

단계 8 **Action(**작업**)** 목록에서 **Decrypt - Resign(**암호 해독 - 재서명**)**을 선택합니다.

단계 9 **with** 목록에서 PKI 개체를 선택합니다.

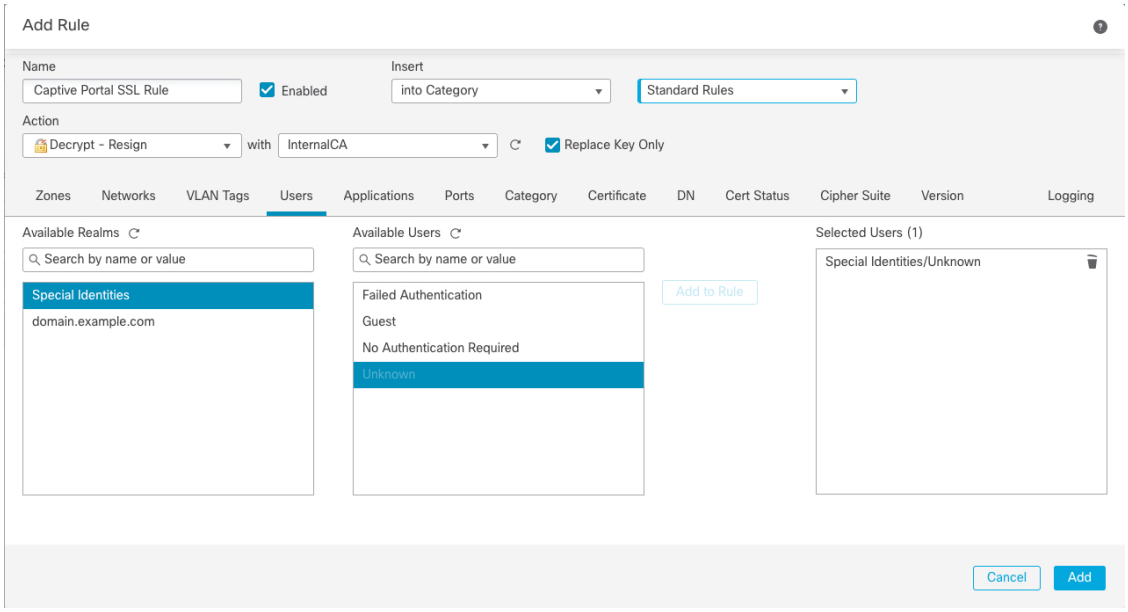
단계 10 **Users(**사용자**)**를 클릭합니다.

단계 11 **Available Realms(**사용 가능한 영역**)** 목록 위에 있는 새로 로침( )을(를) 클릭합니다.

단계 12 **Available Realms(**사용 가능한 영역**)** 목록에서 **Special Identities(** 특수 **ID)**를 클릭합니다.

단계 13 **Available Users(**사용 가능한 사용자**)** 목록에서 **Unknown(**알 수 없음**)**을 클릭합니다.

단계 14 **Add to Rule(**규칙에 추가**)**을 클릭합니다.
다음 그림은 예를 보여줍니다.



단계 15 (선택 사항). TLS/SSL 규칙 조건, 1816 페이지에 설명된 대로 다른 옵션을 설정합니다.

단계 16 **Add(**추가**)**를 클릭합니다.

단계 17 페이지 상단에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 설정 5부: ID 및 SSL 정책과 액세스 컨트롤 정책 연결, 2515 페이지를 계속 진행합니다.

캡티브 포털 설정 5부: ID 및 SSL 정책과 액세스 컨트롤 정책 연결

절차의 이 부분은 ID 정책과 SSL **Decrypt - Resign(**암호 해독 - 재서명**)** 규칙을 앞에서 생성한 액세스 컨트롤 정책과 연결하는 방법을 설명합니다. 이렇게 하면 사용자는 캡티브 포털을 이용해 인증할 수 있습니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지에서 확인할 수 있습니다.

프로시저

단계 1 **Policies(정책)** > **Access Control(액세스 컨트롤)** > **Access Control(액세스 컨트롤)**을 클릭하고 캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 2512 페이지에서 설명한 방법에 따라 생성한 액세스 컨트롤 정책을 편집합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 2 새로운 액세스 컨트롤 정책을 만들거나 기존 정책을 편집합니다.

단계 3 페이지 상단에서 **Identity Policy(ID 정책)** 옆에 있는 링크를 클릭합니다.

단계 4 목록에서 ID 정책의 이름을 선택하고, 페이지 상단의 **Save(저장)**를 클릭합니다.

단계 5 앞의 단계를 반복해 캡티브 포털 SSL 정책을 액세스 컨트롤 정책과 연결합니다.

단계 6 아직 하지 않았다면, 액세스 제어 정책에 대한 대상 디바이스 설정, 1635 페이지에 설명된 대로 매니지드 디바이스에 정책을 대상으로 지정합니다.

다음에 수행할 작업

- 컨피그레이션 변경 사항 구축, 498 페이지에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- 워크플로 사용, 2793 페이지에 설명된 대로 사용자 활동을 모니터링합니다.

캡티브 포털(captive portal) 필드

다음 필드를 사용하여 ID 정책의 **Active Authentication(액티브 인증)** 탭에서 캡티브 포털(captive portal)을 설정합니다. Identity Rule Fields(ID 규칙 필드), 2532 페이지도 참조하십시오.

서버 인증서

캡티브 포털(captive portal) 데몬에서 표시되는 서버 인증서.

참고 캡티브 포털은 DSA(Digital Signature Algorithm) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서 사용을 지원하지 않습니다.

Port(포트)

캡티브 포털(captive portal) 연결에 사용할 포트 번호입니다. ASA FirePOWER 디바이스를 캡티브 포털(captive portal)에 사용하려는 경우, 이 필드의 포트 번호는 **captive-portal** CLI 명령을 사용하여 ASA FirePOWER 디바이스에서 설정한 포트 번호와 일치해야 합니다.

Maximum login attempts(최대 로그인 시도 횟수)

시스템이 사용자의 로그인 요청을 거부하기 전까지 허용되는 최대 실패 로그인 시도 횟수.

Active Authentication Response Page(액티브 인증 응답 페이지)

다음 옵션을 선택합니다.

- 일반적인 응답을 사용하려면, **System-provided(**시스템 제공**)**를 클릭합니다. 이 페이지에 대한 HTML 코드를 보려면 보기 ( )를 클릭합니다.
- 맞춤형 응답을 생성하려면, **Custom(**맞춤형**)**을 선택합니다. 대체하거나 수정할 수 있는 시스템 제공 코드가 표시되는 창이 나타납니다. 완료했으면 변경사항을 저장합니다. 수정( )을 클릭하여 사용자 지정 페이지를 편집할 수 있습니다.

관련 항목

내부 인증서 개체, 627 페이지

캡티브 포털에서 애플리케이션 제외

애플리케이션(HTTP 사용자-에이전트 설정에서 식별됨)을 선택하고 캡티브 포털(captive portal) 액티브 인증에서 이를 제외할 수 있습니다. 이렇게 하면 선택한 애플리케이션의 트래픽이 인증 없이 ID 정책을 통과할 수 있습니다.

참고 **User-Agent Exclusion(**사용자-에이전트 제외**) Tag(**태그**)**가 있는 애플리케이션만 이 목록에 표시됩니다.

프로시저

단계 **1** ID 규칙 편집기 페이지의 **Realm & Settings(**영역 및 설정**)**에서 **Application Filters(**애플리케이션 필터**)** 목록에 있는 Cisco 제공 필터를 사용하여 필터에 추가할 애플리케이션 목록의 범위를 좁힙니다.

- 목록을 확장 및 축소하려면 각 필터 유형 옆에 있는 화살표를 클릭합니다.
- 필터 유형을 마우스 오른쪽 버튼으로 클릭하고 **Check All(**모두 선택**)** 또는 **Uncheck All(**모두 선택해제**)**을 클릭합니다. 목록은 각 유형의 필터를 얼마나 많이 선택했는지를 나타낸다는 점에 유의하십시오.
- 나타나는 필터를 축소하려면, **Search by name(**이름으로 검색**)** 필드에 검색 문자열을 입력합니다. 이는 카테고리 및 태그에 특히 유용합니다. 검색을 지우려면 지우기( ) 아이콘을 클릭합니다.
- 필터 목록을 새로 고침하고 선택한 모든 필터를 지우려면 다시 로드( )을 클릭합니다.
- 모든 필터 및 검색 필드를 지우려면, **Clear All Filters(**모든 필터 지우기**)**를 클릭합니다.

참고 목록은 한 번에 100개의 애플리케이션을 표시합니다.

단계 **2** **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 필터에 추가하려는 애플리케이션을 선택합니다.

- 나타나는 개별 애플리케이션의 범위를 좁히려면 **Search by name(**이름으로 검색**)** 필드에 검색 문자열을 입력합니다. 검색을 지우려면 지우기( ) 아이콘을 클릭합니다.
- 개별 가용 애플리케이션 목록을 조회하려면 목록 하단의 페이징을 사용합니다.
- 애플리케이션을 새로 고침하고 선택한 모든 애플리케이션을 지우려면 다시 로드( )을 클릭합니다.

단계 **3** 선택한 애플리케이션을 추가하여 외부 인증에서 제외합니다. 클릭하여 드래그하거나 **Add to Rule(**규칙에 추가**)**을 클릭할 수 있습니다. 결과는 선택한 애플리케이션 필터의 조합이 됩니다.

다음에 수행할 작업

- ID 규칙 생성, 2531 페이지에 설명된 대로 ID 규칙을 계속 구성합니다.

캡티브 포털(captive portal) ID 소스 문제 해결

기타 관련 문제 해결 정보를 보려면 영역 및 사용자 다운로드 문제 해결, 2480 페이지 및 사용자 제어 문제 해결, 549 페이지을 참조하십시오.

캡티브 포털(captive portal)에 문제가 발생한 경우 다음을 확인하십시오.

- 캡티브 포털(captive portal) 서버의 시간은 Firepower Management Center의 시간과 동기화되어야 합니다.
-
- Firepower Management Center와 매니지드 디바이스 간의 연결에 실패했을 때, 사용자가 이전에 확인된 적이 있고 Firepower Management Center에 다운로드된 경우가 아니라면 다운타임 동안에는 디바이스에서 보고된 어떤 캡티브 포털(captive portal) 로그인도 식별할 수 없습니다. 식별되지 않은 사용자는 Firepower Management Center에서 알 수 없는 사용자로 로깅됩니다. 다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.
- 캡티브 포털(captive portal)에 사용할 디바이스에 인라인 및 라우팅 인터페이스가 모두 포함된 경우, 캡티브 포털(captive portal) ID 규칙에 영역 조건을 구성하여 캡티브 포털(captive portal) 디바이스에서 라우팅 인터페이스만 대상이 되도록 해야 합니다.
- 시스템은 ASA with FirePOWER 디바이스에서 인터페이스의 유형을 검증하지 않습니다. ASA with FirePOWER 디바이스에서 인라인(탭 모드) 인터페이스에 캡티브 포털 정책을 적용하면 정책 구축은 성공하지만 해당 규칙과 일치하는 트래픽의 사용자는 Unknown(알 수 없음)으로 식별됩니다.
- Kerberos 인증에 성공하려면 매니지드 디바이스의 호스트 이름이 15자 미만이어야 합니다.
- 사용자 로그아웃을 확인하는 유일한 방법은 브라우저를 닫고 다시 여는 것입니다. 그러지 않으면, 경우에 따라 사용자가 캡티브 포털에서 로그아웃한 다음 같은 브라우저를 이용해 다시 인증하지 않고도 네트워크에 액세스할 수 있습니다.

- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 RFC 959를 참조하십시오.

캡티브 포털 기록

기능	버전	세부 사항
캡티브 포털입니다.	6.0	기능이 도입되었습니다. 캡티브 포털을 이용하면 브라우저 창의 메시지를 통해 사용자가 자격 증명을 입력하게 할 수 있습니다. 이러한 매핑을 통해 사용자 또는 사용자 그룹을 기반으로 정책을 설정할 수 있습니다.

100 장

Remote Access VPN을 사용하여 사용자 제어

다음 주제는 Remote Access VPN을 이용해 사용자 인식 및 사용자 제어를 수행하는 방법을 설명합니다.

- Remote Access VPN ID 소스, 2521 페이지
- 사용자 제어에 대한 RA VPN 설정, 2522 페이지
- 원격 액세스 VPN ID 소스 문제 해결, 2523 페이지
- RA VPN 기록, 2523 페이지

Remote Access VPN ID 소스

Firepower Threat Defense 는 원격 액세스 SSL 및 IPsec IKEv2 VPN을 지원하는 보안 게이트웨이 기능을 제공합니다. 전체 터널 클라이언트인 AnyConnect Secure Mobility Client는 원격 사용자를 위해 보안 게이트웨이에 보안 SSL 및 IPsec-IKEv2 연결을 제공합니다. AnyConnect는 Firepower Threat Defense 디바이스에 원격 VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

새 Remote Access VPN 정책 생성, 1166 페이지에 설명된 대로 안전한 VPN 게이트웨어를 설정할 때, 사용자가 Active Directory 저장소에 있다면 이러한 사용자에 대한 ID 정책을 설정하고 ID 정책을 액세스 컨트롤 정책과 연결할 수 있습니다.

원격 사용자가 제공한 로그인 정보는 LDAP 또는 AD 영역 또는 RADIUS 서버 그룹에서 검증합니다. 이러한 엔터티는 Firepower Threat Defense 보안 게이트웨이와 통합됩니다.

참고 사용자가 Active Directory를 인증 소스로 사용하여 RA VPN으로 인증하는 경우 사용자 이름을 사용하여 로그인해야 합니다. `domain\username` 또는 `username@domain` 형식은 실패하게 됩니다. (Active Directory는 이 사용자 이름을 로그온 이름 또는 경우에 따라 `sAMAccountName`으로 참조합니다.) 자세한 내용은 MSDN의 User Naming Attributes를 참조하십시오.

RADIUS를 사용하여 인증하는 경우 사용자는 위의 형식 중 하나로 로그인할 수 있습니다.

VPN 연결을 통해 인증되면 원격 사용자는 *VPN ID*를 사용합니다. Firepower Threat Defense 보안 게이트웨이의 *ID* 정책에서 이 VPN ID를 사용하여 해당 원격 사용자에게 속하는 네트워크 트래픽을 인식하고 필터링합니다.

ID 정책은 네트워크 리소스에 대한 액세스 권한을 가진 사용자를 확인하는 액세스 제어 정책과 연결됩니다. 이러한 방식으로 원격 사용자는 네트워크 리소스에 대한 액세스가 차단되거나 허용됩니다.

관련 항목

Firepower Threat Defense VPN 개요, 1121 페이지
Firepower Threat Defense 원격 액세스 VPN 개요, 1155 페이지
VPN 기본 사항, 1122 페이지
Remote Access VPN 기능, 1156 페이지
Remote Access VPN에 대한 지침 및 제한 사항, 1162 페이지
새 Remote Access VPN 정책 생성, 1166 페이지

사용자 제어에 대한 RA VPN 설정

시작하기 전에

- 영역 생성, 2466 페이지에 설명된 대로 영역을 생성합니다.
- 인증, 권한 부여 및 감사(AAA)를 사용하려면, RADIUS 서버 그룹, 667 페이지에 설명된 대로 RADIUS 서버 그룹을 설정합니다.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **Devices(**디바이스**)** > **VPN** > **Remote Access(**원격 액세스**)**를 클릭합니다.

단계 **3** 새 Remote Access VPN 정책 생성, 1166 페이지의 내용을 참조하십시오.

다음에 수행할 작업

- ID 정책 생성, 2534 페이지에 설명된 대로 ID 정책을 사용하여 제어할 사용자 및 기타 옵션을 지정합니다.
- 액세스 제어에 다른 정책 연결, 1641 페이지에 설명된 대로 ID 규칙을 트래픽을 필터링하고 필요에 따라 검사하는 액세스 제어 규칙과 연결합니다.
- 컨피그레이션 변경 사항 구축, 498 페이지에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- VPN 세션 및 사용자 정보, 1232 페이지에 설명된 대로 VPN 사용자 트래픽을 모니터링합니다.

원격 액세스 VPN ID 소스 문제 해결

- 기타 관련 문제 해결 정보를 보려면 영역 및 사용자 다운로드 문제 해결, 2480 페이지, 사용자 제어 문제 해결, 549 페이지, Firepower Threat Defense VPN 문제 해결, 1235 페이지을 참조하십시오.
- Remote Access VPN 관련 문제가 발생한다면, Firepower Management Center 및 매니지드 디바이스 간의 연결을 확인하십시오. 연결에 실패했을 때, 사용자가 이전에 확인된 적이 있고 Firepower Management Center에 다운로드된 경우가 아니라면 다운타임 동안에는 디바이스에서 보고된 모든 원격 액세스 VPN 로그인을 식별할 수 없습니다.

  식별되지 않은 사용자는 Firepower Management Center에서 알 수 없는 사용자로 로깅됩니다. 다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.
- Kerberos 인증에 성공하려면 매니지드 디바이스의 호스트 이름이 15자 미만이어야 합니다.
- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 RFC 959를 참조하십시오.

RA VPN 기록

기능	버전	세부 사항
원격 액세스 VPN	6.2.1	기능이 도입되었습니다. RA VPN은 개별 사용자가 인터넷에 연결된 랩톱 또는 데스크톱, Android, Apple iOS 모바일 디바이스를 사용하여 전용 비즈니스 네트워크에 연결할 수 있게 합니다. 원격 사용자는 공유 미디어 및 인터넷을 통해 전송되는 데이터에 중요한 암호화 기술을 사용하여 안전하게, 자신 있게 데이터를 전송합니다.

101 장

TS 에이전트를 사용하여 사용자 제어

다음 주제는 TS 에이전트를 이용해 사용자 인식 및 사용자 제어를 수행하는 방법을 설명합니다.

- TS(Terminal Services) 에이전트 ID 소스, 2525 페이지
- TS 에이전트 가이드라인, 2525 페이지
- 사용자 제어에 대한 TS 에이전트 설정, 2526 페이지
- TS 에이전트 ID 소스 문제 해결, 2526 페이지
- TS 에이전트 기록, 2527 페이지

TS(Terminal Services) 에이전트 ID 소스

TS 에이전트는 패시브 인증 방법이자 Firepower System에서 지원하는 권한 있는 ID 소스 중 하나입니다. Windows 터미널 서버가 인증을 수행하면, TS 에이전트는 독립형 또는 고가용성Firepower Management Center에 이를 보고합니다.

Windows 터미널 서버에 설치된 경우, TS 에이전트는 개별 사용자가 모니터링되는 네트워크에 로그인 또는 로그아웃할 때 개별 사용자에게 고유의 포트 범위를 할당합니다. Firepower Management Center는 고유한 포트를 사용하여 Firepower System에서 개별 사용자를 식별합니다. TS 에이전트 1개를 사용하여 Windows 터미널 서버 1개에서 사용자 활동을 모니터링하고, 암호화된 데이터를 Firepower Management Center에 보낼 수 있습니다.

TS 에이전트는 실패한 로그인 시도를 보고하지 않습니다. TS 에이전트에서 수집한 데이터는 사용자 인식 및 사용자 제어에 사용할 수 있습니다.

Video(비디오**)** YouTube의 TS Agent 설정 비디오

TS 에이전트 가이드라인

TS 에이전트는 다단계 컨피그레이션이 필요하며 다음이 포함됩니다.

1. TS 에이전트가 설치 및 구성된 Windows 터미널 서버
2. 서버에서 모니터링 중인 사용자를 대상으로 하는 하나 이상의 ID 영역

Microsoft Windows 터미널 서버에 TS 에이전트를 설치합니다. 다단계 TS 에이전트 설치 및 컨피그레이션에 대한 자세한 내용과 서버 및 Firepower System 요건의 전체 내용을 보려면 *Cisco TS(Terminal Services)* 에이전트 가이드를 참조하십시오.

TS 에이전트 데이터는 Users(사용자), User Activity(사용자 활동), Connection Event(연결 이벤트) 테이블에 표시되며 사용자 인식 및 사용자 제어에 사용할 수 있습니다.

참고 TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE/ISE-PIC)로 모니터링할 경우, Firepower Management Center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 다른 수동 ID 소스가 동일한 IP 주소로 활동을 보고할 경우, TS 에이전트 데이터만 Firepower Management Center에 로깅됩니다.

사용자 제어에 대한 TS 에이전트 설정

TS 에이전트를 사용자 인식 및 사용자 제어를 위한 ID 소스로 사용하려면, *Cisco TS(Terminal Services)* 에이전트 가이드의 설명에 따라 TS 에이전트 소프트웨어를 설치하고 설정합니다.

다음 작업:

- ID 정책 생성, 2534 페이지에 설명된 대로 ID 정책을 사용하여 제어할 사용자 및 기타 옵션을 지정합니다.
- 액세스 제어에 다른 정책 연결, 1641 페이지에 설명된 대로 ID 규칙을 트래픽을 필터링하고 필요에 따라 검사하는 액세스 제어 규칙과 연결합니다.
- 컨피그레이션 변경 사항 구축, 498 페이지에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- 워크플로 사용, 2793 페이지에 설명된 대로 사용자 활동을 모니터링합니다.

TS 에이전트 ID 소스 문제 해결

기타 관련 문제 해결 정보를 보려면 영역 및 사용자 다운로드 문제 해결, 2480 페이지 및 사용자 제어 문제 해결, 549 페이지을 참조하십시오.

TS 에이전트와 Firepower System을 통합하는 데 문제가 발생한 경우 다음을 확인하십시오.

- TS 에이전트 서버의 시간을 Firepower Management Center의 시간과 동기화해야 합니다.
- TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE)로 모니터링할 경우, Firepower Management Center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 수동 ID 소스가 동일한 IP 주소별로 활동을 보고할 경우, TS 에이전트 데이터만 Firepower Management Center에 로깅됩니다.
-

- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 RFC 959를 참조하십시오.

전체 문제 해결 정보를 보려면 *Cisco TS(Terminal Services)* 에이전트 컨피그레이션 가이드를 참조하십시오.

TS 에이전트 기록

102 장

ID 정책 생성 및 관리

다음 주제는 ID 규칙과 ID 정책을 만들고 관리하는 방법을 설명합니다.

- ID 정책 정보, 2529 페이지
- ID 정책 라이선스 요구 사항, 2530 페이지
- ID 정책 요구 사항 및 사전 요건, 2530 페이지
- ID 규칙 생성, 2531 페이지
- ID 정책 생성, 2534 페이지
- ID 규칙 관리, 2535 페이지
- ID 정책 관리, 2536 페이지

ID 정책 정보

ID 정책에는 ID 규칙이 포함됩니다. ID 규칙은 트래픽 집합을 영역 및 인증 방법(패시브 인증, 활성 인증, 인증 없음)과 연결합니다.

다음 단락에서 언급하는 예외 사항이 아닌 이상, 사용하려는 영역과 인증 방법을 먼저 설정해야 ID 규칙에서 이를 호출할 수 있습니다.

- ID 정책 외부, **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**에서 영역을 설정합니다. 자세한 내용은 영역 생성, 2466 페이지를 참고하십시오.
- **System(**시스템**)** > **Integration(**통합**)** > **Identity Sources(ID** 소스**)**에서 인 사용자 에이전트와 를 설정합니다. 자세한 내용은 사용자 제어를 위한 ISE/ISE-PIC 설정, 2497 페이지를 참조하십시오.
- ID 정책 내에서 액티브 인증 ID 소스인 캡티브 포털을 설정합니다. 자세한 내용은 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지를 참고하십시오.
- Remote Access VPN 정책에서 액티브 인증 ID 소스인 Remote Access VPN을 설정합니다. 자세한 내용은 Remote Access VPN 인증, 1158 페이지를 참고하십시오.

여러 ID 규칙을 단일 ID 정책에 추가한 후, 규칙 순서를 지정합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

하나 이상의 ID 정책을 설정한 후에는 ID 정책 하나를 액세스 컨트롤 정책에 연결해야 합니다. 네트워크의 트래픽이 ID 규칙의 조건과 일치하면, 시스템은 트래픽을 지정된 영역과 연결하며 지정한 ID 소스를 사용하여 트래픽의 사용자를 인증합니다.

ID 정책을 구성하지 않으면 시스템은 사용자 인증을 수행하지 않습니다.

ID 정책 생성 예외 사항

ID 정책은 다음이 모두 참인 경우 필요하지 않습니다.

- ISE/ISE-PIC ID 소스를 사용합니다.
- 액세스 제어 정책에서 사용자 또는 그룹을 사용하지 않습니다.
- 액세스 제어 정책에서 SGT(Security Group Tag)를 사용합니다. 자세한 내용은 ISE SGT 및 맞춤형 SGT 규칙 조건 비교를 참고하십시오.

비디오 ID 정책 및 규칙 생성에 대한 YouTube 비디오.

관련 항목

ID 정책 설정 방법

ID 정책 라이선스 요구 사항

FTD 라이센스

Any(모든 상태)

기본 라이선스

제어

ID 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자

- Network Admin(네트워크 관리자)

ID 규칙 생성

ID 규칙의 설정 옵션에 대한 자세한 내용은 Identity Rule Fields(ID 규칙 필드), 2532 페이지 섹션을 참조하십시오.

시작하기 전에

영역 또는 영역 시퀀스를 생성하고 활성화해야 합니다.

- 영역 생성, 2466 페이지에 설명된 대로 를 생성합니다.
- (선택 사항). 영역 시퀀스 생성, 2477 페이지에 설명된 대로 영역 시퀀스를 생성합니다.
- 영역 디렉터리 설정, 2475 페이지에 설명된 대로 디렉터리를 생성합니다.
- 사용자 및 그룹 다운로드, 2476 페이지에 설명된 대로 사용자 및 그룹을 다운로드하고 영역을 활성화합니다.

프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)** 버튼을 클릭합니다.

단계 3 ID 규칙을 추가할 ID 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 5 **Name(**이름**)**을 입력합니다.

단계 6 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.

단계 7 기존 카테고리에 규칙을 추가하려면 규칙을 **Insert(**삽입**)**할 위치를 나타냅니다. 새 카테고리를 추가하려면 **Add Category(**카테고리 추가**)**를 클릭합니다.

단계 8 목록에서 규칙 **Action(**작업**)**을 선택합니다.

단계 9 **Realms & Settings(**영역 및 설정**)**를 클릭합니다.

단계 10 **Realms(**영역**)** 목록에서 ID 규칙에 대한 영역 또는 영역 시퀀스를 선택합니다. 영역 또는 영역 시퀀스를 모든 ID 규칙과 연결해야 합니다.

영역 요규사항의 유일한 예외는 ISE SGT 속성 태그만 사용하여 사용자 제어를 구현하는 것입니다. 이 경우에는 ISE 서버에 대한 영역 또는 영역 시퀀스는 설정하지 않아도 됩니다. 연결된 ID 정책이 포함되어 있거나 포함되지 않은 정책에서 ISE SGT 속성 조건을 설정할 수 있습니다.

단계 11 캡티브 포털을 설정하는 경우에는 사용자 제어에 대한 캡티브 포털 설정 방법, 2508 페이지 섹션을 참조하십시오.

단계 **12** (선택사항) ID 규칙에 조건을 추가하려면 규칙 조건 유형, 525 페이지 섹션을 참조하십시오.

단계 **13** **Add(**추가**)**를 클릭합니다.

단계 **14** 정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다. 규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

단계 **15** **Save(**저장**)**를 클릭합니다.

Identity Rule Fields(ID 규칙 필드)

ID 규칙을 구성하려면 다음 필드를 사용합니다.

Enabled(활성화**)**

이 옵션을 선택하면 ID 정책에서 ID 규칙이 활성화됩니다. 이 옵션을 선택 취소하면 ID 규칙이 비활성화됩니다.

작업

지정한 영역에 있는 사용자에 대해 실행할 인증 유형을 지정합니다. **Passive Authentication(**패시브 인증**)**(기본값), **Active Authentication(**액티브 인증**)** 또는 **No Authentication(**인증 없음**)**을 지정할 수 있습니다. 인증 방법, 즉 *ID* 소스를 완전히 구성해야 ID 규칙에서 이를 작업으로 선택할 수 있습니다.

또한 VPN이 활성화된 경우(최소 하나 이상의 매니지드 디바이스에서 구성됨) Remote Access VPN 세션은 VPN에 의해 액티브 인증됩니다. 다른 세션은 규칙 작업을 사용합니다. 즉, VPN이 활성화되면 선택한 작업에 관계없이 모든 세션에 대해 VPN ID 확인이 먼저 수행됩니다. 지정된 영역에 VPN ID가 있을 경우, 이를 ID 소스로 사용합니다. No additional captive portal active authentication is done, even if selected.

VPN ID 소스가 없는 경우, 지정된 작업에 따라 프로세스가 계속 진행됩니다. VPN ID 소스가 없는 경우 ID 정책을 VPN 인증에만 제한할 수 없으며, 선택한 작업에 따라 규칙이 적용됩니다.

⚠

주의 SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거함 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

액티브 인증 규칙에는 **Active Authentication(**액티브 인증**)** 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)**가 선택된 **Passive Authentication(**패시브 인증**)** 규칙 작업이 있음에 유의하십시오.

현재 보유한 버전의 Firepower System에서 어떤 수동 및 액티브 인증 방법을 지원하는지에 대한 내용은 사용자 ID 소스 정보를 참조하십시오.

Realm(영역**)**

지정된 **Action(**작업**)**을 수행할 사용자가 포함된 영역 또는 영역 시퀀스 . 영역 또는 영역 시퀀스을 완전히 설정해야 ID 규칙에서 이를 영역으로 선택할 수 있습니다.

참고 원격 액세스 VPN이 활성화되어 있고 구축에서 VPN 인증에 RADIUS 서버 그룹을 사용할 경우, 이 RADIUS 서버 그룹과 연결된 영역을 지정하십시오.

참고 **Kerberos**(Kerberos를 옵션으로 사용하려는 경우에는 **HTTP Negotiate(HTTP** 협상**)**)를 ID 규칙의 **Authentication Protocol(**인증 프로토콜**)**로 선택할 경우, Kerberos 캡티브 포털(captive portal) 액티브 인증을 수행하려면 선택한 **Realm(**영역**)**에 **AD Join Username((AD** 죠인 사용자 이름**)**과 **AD Join Password(AD** 죠인 비밀번호**)**를 구성해야 합니다.

Use active authentication if passive or VPN identity cannot be established(패시브 인증 또는 **VPN ID** 를 설정할 수 없는 경우 액티브 인증 사용**)**

패시브 또는 VPN 인증이 사용자를 식별하지 못할 경우, 이 옵션을 선택하면 캡티브 포털(captive portal) 액티브 인증을 통해 사용자를 인증합니다. 이 옵션을 선택하려면 ID 정책에서 캡티브 포털(captive portal) 액티브 인증을 구성해야 합니다.

이 옵션을 비활성화하면 VPN ID가 없거나 패시브 인증으로 식별할 수 없는 사용자는 Unknown(알 수 없음)으로 식별됩니다.

인증에서 사용자를 식별할 수 없는 경우 특수 **ID/**게스트로 식별함

이 옵션을 선택하면 지정된 횟수만큼 캡티브 포털(captive portal) 액티브 인증에 실패한 사용자가 네트워크에 게스트로 액세스할 수 있습니다. Firepower Management 콘솔에 표시되는 이러한 사용자는 사용자 이름(사용자 이름이 AD 또는 LDAP 서버에 있는 경우) 또는 **Guest(**게스트**)**(사용자 이름을 알 수 없는 경우)로 식별됩니다. 이 영역은 ID 규칙에 지정된 영역입니다. (기본 로그인 실패 횟수는 3회입니다.)

이 필드는 **Active Authentication(**액티브 인증**)**(즉 캡티브 포털 인증)을 규칙 **Action(**작업**)**으로 설정했을 때만 표시됩니다.

Authentication Protocol(인증 프로토콜**)**

캡티브 포털 액티브 인증을 수행하는 데 사용할 방법입니다. 선택 사항은 영역의 유형, LDAP 또는 AD에 따라 달라집니다.

- 암호화되지 않은 HTTP BA(Basic Authentication) 연결을 사용하여 사용자를 인증하려는 경우 **HTTP Basic(HTTP** 기본**)**을 선택합니다. 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.

  대부분의 웹 브라우저는 **HTTP Basic(HTTP** 기본**)** 로그인의 접속 정보를 캐시하며, 접속 정보를 사용하여 기존 세션의 시간이 초과하면 새 세션을 원활하게 시작합니다.

- NTLM(NT LAN Manager) 연결을 사용하여 사용자를 인증하려는 경우 **NTLM**을 선택합니다. 이 선택 사항은 AD 영역을 선택한 경우에만 사용 가능합니다. 사용자의 브라우저에 투명 인증이 구성된 경우, 사용자는 자동으로 로그인됩니다. 투명 인증이 구성되지 않은 경우, 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.
- 캡티브 포털(captive portal) 서버가 인증 연결에 HTTP Basic(HTTP 기본) 또는 NTLM 중에서 선택할 수 있도록 하려면 **HTTP Negotiate(HTTP** 협상**)**를 선택합니다. 이 선택 사항은 AD 영역을 선택한 경우에만 사용 가능합니다.

참고 HTTP 협상 캡티브 포털(captive portal)을 수행할 ID 규칙을 생성 중이고 DNS 확인을 구성한 경우, 캡티브 포털(captive portal) 디바이스의 FQDN(Fully Qualified Domain Name)을 확인할 DNS 서버를 구성해야 합니다. FQDN은 DNS를 구성할 때 제공된 호스트 이름과 일치해야 합니다.

ASA with FirePOWER Services, FQDN은 캡티브 포털(captive portal)에 사용된 라우팅 인터페이스의 IP 주소를 확인해야 합니다.

ID 정책 생성

시작하기 전에

액세스 컨트롤 정책의 영역에서 사용자와 그룹을 사용하려면 ID 정책이 있어야 합니다. 영역 생성, 2466 페이지에 설명된 대로 하나 이상의 영역을 생성하고 활성화합니다.

ID 정책은 다음이 모두 참인 경우 필요하지 않습니다.

- ISE/ISE-PIC ID 소스를 사용합니다.
- 액세스 제어 정책에서 사용자 또는 그룹을 사용하지 않습니다.
- 액세스 제어 정책에서 SGT(Security Group Tag)를 사용합니다. 자세한 내용은 ISE SGT 및 맞춤형 SGT 규칙 조건 비교를 참고하십시오.

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)** 을(를) 클릭하고 **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** **Name(**이름**)**을 입력하고 필요한 경우, **Description(**설명**)**을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 정책에 규칙을 추가하려면 ID 규칙 생성, 2531 페이지에 설명된 대로 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 6 규칙 카테고리를 생성하려면 **Add Category(**카테고리 추가**)**를 클릭합니다.

단계 7 종속 포털 액티브 인증을 설정하려면 캡티브 포털 설정 1부: ID 정책 생성, 2510 페이지에 설명된 대로 **Active Authentication(**액티브 인증**)**을 클릭합니다.

단계 8 **Save(**저장**)**를 클릭하여 ID 정책을 저장합니다.

다음에 수행할 작업

- 일치시킬 사용자를 지정하는 ID 정책과 기타 옵션을 규칙에 추가합니다(ID 규칙 생성, 2531 페이지 참조).
- ID 정책을 액세스 컨트롤 정책에 연결해 선택한 사용자가 지정된 리소스에 액세스하도록 허용하거나 액세스하지 못하게 합니다(액세스 제어에 다른 정책 연결, 1641 페이지 참조).
- 매니지드 디바이스에 설정 변경사항을 구축합니다(컨피그레이션 변경 사항 구축, 498 페이지 참조).

문제가 발생하는 경우에는 사용자 제어 문제 해결, 549 페이지 섹션을 참조하십시오.

관련 항목

캡티브 포털 설정 1부: ID 정책 생성, 2510 페이지
캡티브 포털(captive portal) 필드, 2516 페이지
사용자 제어 문제 해결, 549 페이지

ID 규칙 관리

프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)** 버튼을 클릭합니다.

단계 3 수정하려는 정책 옆에 있는 수정( )를 클릭합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 ID 규칙을 수정하려면 수정( )을 클릭하고 ID 정책 생성, 2534 페이지에 설명된 대로 규칙을 변경합니다.

단계 5 ID 규칙을 삭제하려면 삭제( )을 클릭합니다.

단계 6 규칙 카테고리를 생성하려면 **Add Category(**카테고리 추가**)**를 클릭하고 위치와 규칙을 선택합니다.

단계 7 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

ID 정책 관리

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)** 버튼을 클릭합니다.

단계 **3** 정책을 삭제하려면 삭제( )를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** 정책을 편집하려면 정책 옆에 있는 수정( )을 클릭하고 ID 정책 생성, 2534 페이지에 설명된 대로 변경합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **5** 정책을 복사하려면 복사 ( )을 클릭합니다.

단계 **6** 정책에 대한 보고서를 생성하려면 현재 정책 보고서 생성, 515 페이지에 설명된 대로 보고서( )을 클릭합니다.

단계 **7** 정책을 비교하려면 정책 비교, 514 페이지 섹션을 참조하십시오.

103 장

네트워크 검색 정책

다음 주제에서는 네트워크 검색 정책을 생성, 설정, 관리하는 방법을 설명합니다.

- 개요: 네트워크 검색 정책, 2537 페이지
- 네트워크 검색 정책 요구 사항 및 사전 요건, 2538 페이지
- 네트워크 검색 맞춤 설정, 2538 페이지
- 네트워크 검색 규칙, 2539 페이지
- 고급 네트워크 검색 옵션 설정, 2550 페이지
- 네트워크 검색 전략 문제 해결, 2560 페이지

개요: 네트워크 검색 정책

Firepower Management Center의 네트워크 검색 정책에서는 시스템이 조직의 네트워크 자산에서 데이터를 수집하는 방법과 모니터링해야 할 네트워크 세그먼트 및 포트를 제어합니다.

다중 도메인 구축의 경우, 각 리프 도메인에는 독립적인 네트워크 검색 정책이 있습니다. 네트워크 검색 정책 규칙 및 기타 설정은 도메인 간에 공유, 계승, 복사할 수 없습니다. 새 도메인을 생성할 때마다, 시스템은 기본 설정을 이용해 새 도메인의 네트워크 검색 정책을 생성합니다. 원하는 모든 사용자 설정을 새 정책에 명시적으로 적용해야 합니다.

정책 내의 검색 규칙은 트래픽의 네트워크 데이터를 바탕으로 검색 데이터를 생성하기 위해 Firepower System이 모니터링할 네트워크와 포트를, 그리고 정책을 구축할 영역을 지정합니다. 규칙 내에서는 호스트, 애플리케이션 및 신뢰할 수 없는 사용자의 검색 여부를 구성할 수 있습니다. 검색에서 네트워크와 영역을 제외하는 규칙을 생성할 수 있습니다. NetFlow 엑스포터에서 데이터 검색을 설정하고 네트워크에서 사용자 데이터가 검색되는 트래픽에 대한 프로토콜을 제한할 수 있습니다.

네트워크 검색 정책에는 관찰되는 모든 트래픽에서 애플리케이션을 검색하도록 설정되는, 단일 기본 규칙이 적용됩니다. 규칙은 네트워크, 영역 또는 포트를 제외하지 않으며, 호스트와 사용자 검색은 설정되지 않습니다. 그리고 규칙은 NetFlow 엑스포터를 모니터링하도록 설정되지 않습니다. 기본적으로 이 정책은 매니지드 디바이스가 Firepower Management Center에 등록될 때 구축됩니다. 호스트 또는 사용자 데이터 수집을 시작하려면, 검색 규칙을 추가 또는 수정하고 디바이스에 정책을 다시 적용해야 합니다.

네트워크 검색의 범위를 조정하려면 추가 검색 규칙을 생성하고 기본 규칙을 수정 또는 제거할 수 있습니다.

각각의 매니지드 디바이스에 대한 액세스 컨트롤 정책은 해당 디바이스에 대해 사용자가 허용하는 트래픽, 즉 네트워크 검색으로 모니터링할 수 있는 트래픽을 정의합니다. 액세스 컨트롤을 사용하여 특정 트래픽을 차단하면 시스템은 해당 트래픽에서 호스트, 사용자 또는 애플리케이션 활동을 검토할 수 없습니다. 예를 들어 액세스 컨트롤 정책이 소셜 네트워킹 애플리케이션에 대한 액세스를 차단하면, 시스템은 해당 애플리케이션에 대한 검색 데이터를 제공하지 않습니다.

검색 규칙에서 트래픽 기반 사용자 검색을 활성화하면, 애플리케이션 프로토콜 모음을 이용하는 트래픽 내 사용자 로그인 활동을 통해 신뢰할 수 없는 사용자를 탐지할 수 있습니다. 필요한 경우 모든 규칙에서 특정 프로토콜에서의 검색을 비활성화할 수 있습니다. 일부 프로토콜을 비활성화하면 Firepower Management Center 모델과 연결된 사용자 제한에 도달하는 것을 방지하여, 다른 프로토콜의 사용자에 대해 사용할 수 있는 사용자 카운트를 확보할 수 있습니다.

고급 네트워크 검색 설정을 사용하면 어떤 데이터를 기록할지, 검색 데이터를 어떻게 저장할지, 어떤 IOC(indications of compromise) 규칙을 활성화할지, 영향 평가에 어떤 취약성 매핑을 사용할지, 소스에서 충돌하는 검색 데이터를 제공할 경우 어떤 일이 발생할지를 관리할 수 있습니다. 모니터링할 호스트 입력 및 NetFlow 엑스포터의 소스를 추가할 수도 있습니다.

네트워크 검색 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

Leaf

사용자 역할

- 관리자
- 검색 관리자

네트워크 검색 맞춤 설정

Firepower System에서 수집하는 네트워크 트래픽에 대한 정보는 시스템이 이 정보를 연계하여 가장 소중하고 가장 중요한 네트워크의 호스트를 식별할 때 가장 가치 있게 사용됩니다.

예를 들어 SuSE Linux의 맞춤형 버전을 실행하는 디바이스가 네트워크에 여러 개 있는 경우 시스템은 해당 운영체제를 식별할 수 없으므로 호스트에 취약성을 매핑할 수 없습니다. 그러나 시스템에 SuSE Linux에 대한 취약성 목록이 있음을 알고 있다면, 호스트 중 하나에 대한 맞춤형 핑거프린트를 생성한 다음 동일한 운영체제를 실행하는 다른 호스트의 식별에 이를 사용할 수 있습니다. 핑거프린트에 SuSE Linux에 대한 취약성 목록의 매핑을 포함하여, 해당 목록을 핑거프린트와 일치하는 각 호스트와 연결할 수 있습니다.

호스트 입력 기능을 사용하여 서드파티 시스템의 호스트 데이터를 네트워크 맵에 직접 입력할 수도 있습니다. 그러나 서드파티 운영체제나 애플리케이션 데이터는 취약성 정보에 자동으로 매핑되지 않습니다. 서드파티 운영체제, 서버 및 애플리케이션 프로토콜 데이터를 사용하여 호스트에 대한 취약성을 보고 영향 상관관계를 수행하려면, 서드파티 시스템의 벤더 및 버전 정보를 VDB(취약성 데이터베이스)에 나열된 벤더 및 버전에 매핑해야 합니다. 호스트 입력 데이터를 지속적으로 유지 관리할 수도 있습니다. 애플리케이션 데이터를 Firepower System 벤더 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

시스템이 네트워크의 호스트에서 실행되는 애플리케이션 프로토콜을 식별할 수 없는 경우, 포트나 패턴을 기반으로 시스템이 애플리케이션을 식별하도록 하는 사용자 정의 애플리케이션 프로토콜 탐지기를 생성할 수 있습니다. 특정 애플리케이션 탐지기를 가져오고 활성화 및 비활성화하여 Firepower System의 애플리케이션 탐지 기능을 한층 더 맞춤화할 수 있습니다.

Nmap 활성 스캐너의 스캔 결과를 사용하여 운영체제 및 애플리케이션 데이터의 탐지를 교체하거나 취약성 목록을 서드파티 취약성으로 보강할 수도 있습니다. 시스템에서는 애플리케이션의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

네트워크 검색 정책 설정

다중 도메인 구축의 경우, 각 도메인에는 별도의 네트워크 검색 정책이 있습니다. 사용자 계정이 여러 도메인을 관리할 수 있다면, 정책을 설정할 리프 도메인으로 전환합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** 정책의 다음 구성 요소를 설정합니다.

- 검색 규칙 - 네트워크 검색 규칙 구성, 2540 페이지 섹션을 참조하십시오.
- 사용자에 대한 트래픽 기반 탐지 - 트래픽 기반 사용자 탐지 구성, 2549 페이지 섹션을 참조하십시오.
- 고급 네트워크 검색 옵션 - 고급 네트워크 검색 옵션 설정, 2550 페이지 섹션을 참조하십시오.
- 맞춤형 운영체제 정의(핑거프린트) - 클라이언트에 대한 맞춤형 핑거프린트 생성, 2401 페이지 및 서버에 대한 맞춤형 핑거프린트 생성, 2403 페이지 섹션을 참조하십시오.

네트워크 검색 규칙

네트워크 검색 규칙을 사용하면 원하는 특정 데이터만 포함하도록 네트워크 맵에 대해 검색되는 정보를 맞춤화할 수 있습니다. 네트워크 검색 정책의 규칙은 차례로 평가됩니다. 모니터링 기준을 중첩하여 규칙을 생성할 수 있지만, 그렇게 하면 시스템 성능에 영향이 미칠 수 있습니다.

호스트 또는 네트워크를 모니터링에서 제외하면 해당 호스트 또는 네트워크는 네트워크 맵에 나타나지 않으며 그에 대한 이벤트도 보고되지 않습니다. Cisco는 로드 밸런서(또는 로드 밸런서의 특정 포트) 및 NAT 디바이스를 모니터링에서 제외할 것을 권장합니다. 이러한 디바이스는 잘못된 이벤트를 과도하게 생성하여 데이터베이스를 채우고 Firepower Management Center에 과부하를 가져올 수 있습니다. 예를 들어 모니터링되는 NAT 디바이스는 단기간에 운영체제의 여러 업데이트를 표시할 수 있습니다. 로드 밸런서 및 NAT 디바이스의 IP 주소를 알고 있으면 모니터링에서 이들을 제외할 수 있습니다.

팁 시스템은 네트워크 트래픽을 검토하여 다수의 로드 밸런서 및 NAT 디바이스를 식별할 수 있습니다.

또한 맞춤형 서버 핑거프린트를 생성해야 할 경우, 핑거프린트 생성 중인 호스트와 통신하는 데 사용하는 IP 주소를 모니터링에서 일시적으로 제외해야 합니다. 이렇게 하지 않으면 네트워크 맵 및 검색 이벤트 보기가 해당 IP 주소로 표시되는 호스트에 대한 부정확한 정보와 뒤섞이게 됩니다. 핑거프린트를 생성한 후에는 IP 주소를 다시 모니터링하도록 정책을 구성할 수 있습니다.

또한 Cisco는 NetFlow 엑스포터 및 Firepower System 매니지드 디바이스를 이용해 같은 네크워트 세그먼트를 모니터링하지 않을 것을 권장합니다. 중첩되지 않는 규칙으로 네트워크 검색 정책을 구성하는 것이 이상적이지만, 시스템은 매니지드 디바이스에 의해 생성된 중복 연결 로그를 삭제합니다. 그러나 매니지드 디바이스와 NetFlow 엑스포터를 모두 이용해 탐지한 검색에 대한 중복되는 연결 로그는 삭제할 수 없습니다.

네트워크 검색 규칙 구성

호스트 및 애플리케이션 데이터의 검색을 요구에 맞춤화하도록 검색 규칙을 구성할 수 있습니다.

시작하기 전에

- 네트워크 데이터를 검색하려는 트래픽에 대한 연결을 로깅해야 합니다(연결 로깅 모범 사례, 2868 페이지 참조).
- 내보낸 NetFlow 레코드를 수집하려면 네트워크 검색 정책에 NetFlow 엑스포터 추가, 2556 페이지에 설명된 대로 NetFlow 엑스포터를 추가합니다.
- 검색 성능 그래프를 보려면 검색 규칙에서 호스트, 사용자, 애플리케이션을 활성화해야 합니다. (시스템 성능에 영향을 줄 수 있습니다.)

팁 대부분의 경우 Cisco는 RFC 1918에서 주소 검색을 제한합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** 규칙에 대한 **Action(**작업**)**을 작업 및 검색된 자산, 2541 페이지에 설명된 대로 설정합니다.

단계 **4** 선택적 검색 매개변수 설정:

- 특정 네트워크에 대한 규칙 작업을 제한합니다(모니터링되는 네트워크 제한, 2542 페이지 참조).
- 특정 영역의 트래픽에 대한 규칙 작업을 제한합니다(네트워크 검색 규칙의 영역 구성, 2547 페이지 참조).
- 모니터링에서 포트를 제외합니다(네트워크 검색 규칙에서 포트 제외, 2545 페이지 참조).
- NetFlow 데이터 검색에 대한 규칙을 구성합니다(NetFlow 데이터 검색에 대한 규칙 구성, 2543 페이지 참조).

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

작업 및 검색된 자산

검색 규칙을 구성할 때에는 규칙에 대한 작업을 선택해야 합니다. 이러한 작업의 영향은 매니지드 디바이스 또는 NetFlow 엑스포터에서 데이터를 검색하는 데 규칙을 사용하는지 여부에 따라 달라집니다.

다음 표에서는 이러한 두 시나리오에서 지정된 작업 설정과 함께 규칙에 의해 어떤 자산이 검색되는지에 대해 설명합니다.

표 ***251:*** 검색 규칙 작업

작업	옵션	매니지드 디바이스	**NetFlow** 엑스포터
제외	--	지정된 네트워크를 모니터링에서 제외합니다. 연결의 소스 또는 대상 호스트가 검색에서 제외되면 연결이 기록되기는 하지만 제외된 호스트에 대해 검색 이벤트가 생성되지 않습니다.	지정된 네트워크를 모니터링에서 제외합니다. 연결의 소스 또는 대상 호스트가 검색에서 제외되면 연결이 기록되기는 하지만 제외된 호스트에 대해 검색 이벤트가 생성되지 않습니다.
파악	호스트	검색 이벤트를 기반으로 호스트를 네트워크 맵에 추가합니다. (선택 사항, 사용자 검색이 활성화된 경우 필수.)	NetFlow 레코드를 기반으로 호스트를 네트워크 맵에 추가하고 연결을 로깅합니다. (필수)
파악	애플리케이션	애플리케이션 탐지기를 기반으로 애플리케이션을 네트워크 맵에 추가합니다. 애플리케이션 검색 없이는 규칙에서 호스트 또는 사용자를 검색할 수 없습니다. (필수)	NetFlow 레코드 및 `/etc/sf/services`의 포트 애플리케이션 프로토콜 상관관계를 기준으로 애플리케이션 프로토콜을 네트워크 맵에 추가합니다. (선택 사항)

작업	옵션	매니지드 디바이스	**NetFlow** 엑스포터
파악	사용자	사용자를 사용자 테이블에 추가하고, 네트워크 검색 정책에 구성된 사용자 프로토콜의 트래픽 기반 탐지를 기준으로 사용자 활동을 로깅합니다. (선택 사항)	해당 없음
NetFlow 연결 기록	--	해당 없음	NetFlow 연결만 기록합니다. 호스트나 애플리케이션은 검색하지 않습니다.

매니지드 디바이스 트래픽을 모니터링할 규칙을 사용하려면 애플리케이션 로깅이 필요합니다. 사용자를 모니터링할 규칙을 사용하려면 호스트 로깅이 필요합니다. 내보낸 NetFlow 레코드를 모니터링할 규칙을 사용하려면 사용자를 로깅하도록 규칙을 구성할 수 없으며, 로깅 애플리케이션은 선택 사항입니다.

참고 시스템은 네트워크 검색 정책의 **Action(**작업**)** 설정을 기준으로, 내보낸 NetFlow 레코드에서 연결을 탐지합니다. 시스템은 액세스 제어 정책 설정을 기준으로 매니지드 디바이스 트래픽에서 연결을 탐지합니다.

모니터링되는 네트워크

검색 규칙을 사용하면 지정된 네트워크의 호스트에서 나가고 들어오는 트래픽에서만 모니터링되는 자산의 검색이 이루어집니다. 검색 규칙에서는 모니터링할 네트워크 내 IP 주소에 대해서만 생성되는 이벤트와 함께, 지정된 네트워크 내에 하나 이상의 IP 주소를 가지고 있는 연결에 대해 검색이 이루어집니다. 기본 검색 규칙은 관찰하는 모든 트래픽(IPv4 트래픽은 `0.0.0.0/0`, IPv6 트래픽은 `::/0`)에서 애플리케이션을 검색합니다.

NetFlow 검색을 처리하고 연결 데이터만 기록하도록 규칙을 설정하면, 시스템은 지정된 네트워크의 IP 주소에 대한 연결도 기록합니다. 네트워크 검색 규칙은 NetFlow 네트워크 연결을 기록하는 유일한 방법입니다.

모니터링할 네트워크를 지정하기 위해 네트워크 개체 또는 개체 그룹을 사용할 수도 있습니다.

모니터링되는 네트워크 제한

모든 검색 규칙에는 하나 이상의 네트워크를 포함해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 3 열려 있지 않은 경우 **Networks(**네트워크**)**를 클릭합니다.

단계 4 필요한 경우, 검색 규칙 컨피그레이션 동안 네트워크 개체 생성, 2544 페이지에 설명된 대로 Available Networks(사용 가능한 네트워크) 목록에 네트워크 개체를 추가합니다.

참고 네트워크 검색 정책에서 사용된 네트워크 개체를 수정할 경우, 컨피그레이션 변경 사항을 구축할 때까지 변경 사항이 검색에 영향을 미치지 않습니다.

단계 5 네트워크를 지정합니다.

- **Available Networks(**사용 가능한 네트워크**)** 목록에서 네트워크를 선택합니다.

  팁 네트워크가 목록에 즉시 나타나지 않으면 다시 로드 아이콘(다시 로드( ))을 클릭하십시오.

- Available Networks(사용 가능한 네트워크) 라벨 아래의 텍스트 상자에 IP 주소를 입력합니다.

단계 6 **Add(**추가**)**를 클릭합니다.

단계 7 필요한 경우, 이전의 두 단계를 반복하여 네트워크를 더 추가합니다.

단계 8 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

NetFlow 데이터 검색에 대한 규칙 구성

Firepower System은 NetFlow 엑스포터의 데이터를 사용하여 연결 및 검색 이벤트를 생성하고, 호스트 및 애플리케이션 데이터를 네트워크 맵에 추가할 수 있습니다.

검색 규칙에서 NetFlow 엑스포터를 선택하면, 지정된 네트워크에 대한 NetFlow 데이터의 검색으로 규칙이 제한됩니다. NetFlow 디바이스를 선택하면 사용 가능한 규칙 작업이 변경되므로 규칙 동작의 다른 측면을 구성하기 전에 NetFlow 디바이스를 모니터링하도록 선택합니다. NetFlow 엑스포터 모니터링에는 포트 제외를 구성할 수 없습니다.

시작하기 전에

- 네트워크 검색 정책에 NetFlow 지원 디바이스를 추가합니다(네트워크 검색 정책에 NetFlow 엑스포터 추가, 2556 페이지 참조).

프로시저

단계 1 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **NetFlow Device(NetFlow** 디바이스**)**를 선택합니다.

단계 **4** **Netflow Device(NetFlow** 디바이스**)** 드롭다운 목록에서 모니터링할 NetFlow 엑스포터의 IP 주소를 선택합니다.

단계 **5** Firepower System의 매니지드 디바이스에서 수집할 NetFlow 데이터의 유형을 지정합니다.

- 연결 전용 — **Action(**작업**)** 드롭다운 목록에서 `Log NetFlow Connections(NetFlow 연결 로깅)`를 선택합니다.
- 호스트, 애플리케이션, 연결 — **Action(**작업**)** 드롭다운 목록에서 `Discover(검색)`를 선택합니다. 시스템에서 **Hosts(**호스트**)** 확인란을 자동으로 확인하고 연결 데이터의 수집을 활성화합니다. 필요한 경우, **Application(**애플리케이션**)** 확인란을 선택하여 애플리케이션 데이터를 수집할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

검색 규칙 컨피그레이션 동안 네트워크 개체 생성

재사용 가능한 네트워크 개체 및 그룹의 목록에 네트워크 개체를 추가하면, 검색 규칙에 표시되는 사용 가능한 네트워크 목록에 새로운 네트워크 개체를 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Networks(**네트워크**)**에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Available Networks(**사용 가능한 네트워크**)** 옆의 추가( )을 클릭합니다.

단계 **4** 네트워크 개체 생성, 571 페이지에 설명된 대로 네트워크 개체를 생성합니다.

단계 **5** 네트워크 검색 규칙 구성, 2540 페이지에 설명된 대로 네트워크 검색 규칙 추가를 완료합니다.

포트 제외

호스트를 모니터링에서 제외할 수 있는 것처럼, 특정 포트도 모니터링에서 제외할 수 있습니다. 예를 들면 다음과 같습니다.

- 로드 밸런서는 짧은 기간에 동일한 포트에서 여러 애플리케이션을 보고할 수 있습니다. 포트를 모니터링에서 제외하도록 네트워크 검색 규칙을 구성할 수 있습니다(예: 웹 팜을 처리하는 로드 밸런서의 포트 80 제외).
- 조직에서는 특정 포트 범위를 사용하는 맞춤형 클라이언트를 사용할 수 있습니다. 이 클라이언트의 트래픽이 잘못된 이벤트를 과도하게 생성하면 해당 포트를 모니터링에서 제외할 수 있습니다. 마찬가지로, DNS 트래픽을 모니터링하지 않도록 결정할 수도 있습니다. 이 경우 검색 정책이 포트 53을 모니터링하지 않도록 규칙을 설정할 수 있습니다.

제외할 포트를 추가할 때 Available Ports(사용 가능한 포트) 목록에서 재사용 가능한 포트 개체의 사용 여부를 결정하거나, 포트를 소스 또는 대상 제외 목록에 직접 추가하거나, 재사용 가능한 새 포트를 만든 다음 제외 목록으로 이동할 수 있습니다.

참고 NetFlow 데이터 검색을 처리하는 규칙에서는 포트를 제외할 수 없습니다.

네트워크 검색 규칙에서 포트 제외

NetFlow 데이터 검색을 처리하는 규칙에서는 포트를 제외할 수 없습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Port Exclusions(**포트 제외**)**를 클릭합니다.

단계 **4** 필요한 경우, 검색 규칙 컨피그레이션 동안 포트 개체 생성, 2546 페이지에 설명된 대로 Available Ports(사용 가능한 포트) 목록에 포트 개체를 추가합니다.

단계 **5** 다음 방법 중 하나를 사용하여 특정 소스 포트를 모니터링에서 제외합니다.

- **Available Ports(**사용 가능한 포트**)** 목록에서 하나 이상의 포트를 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다.
- 포트 개체를 추가하지 않고 특정 소스 포트로부터 트래픽을 제외하려면 **Selected Source Ports(**선택된 소스 포트**)** 목록에서 **Protocol(**프로토콜**)**을 선택하고 **Port(**포트**)** 번호(1 ~ 65535)를 입력하고 **Add(**추가**)**를 클릭합니다.

단계 **6** 다음 방법 중 하나를 사용하여 특정 대상 포트를 모니터링에서 제외합니다.

- **Available Ports(**사용 가능한 포트**)** 목록에서 하나 이상의 포트를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- 포트 개체를 추가하지 않고 특정 대상 포트로부터 트래픽을 제외하려면 **Selected Destination Ports(**선택된 대상 포트**)** 목록에서 **Protocol(**프로토콜**)**을 선택하고 **Port(**포트**)** 번호를 입력하고 **Add(**추가**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

검색 규칙 컨피그레이션 동안 포트 개체 생성

Firepower System의 어디서든 사용할 수 있는 재사용 가능한 포트 개체 및 그룹의 목록에 포트 개체를 추가하면, 검색 규칙에 표시되는 사용 가능한 포트 목록에 새로운 포트 개체를 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** Networks(네트워크)에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Port Exclusions(**포트 제외**)**를 클릭합니다.

단계 **4** Available Ports(사용 가능한 포트) 목록에 포트를 추가하려면 추가( )를 클릭합니다.

단계 **5** **Name(**이름**)**을 제공합니다.

단계 **6** 제외할 트래픽의 프로토콜을 **Protocol(**프로토콜**)** 필드에 지정합니다.

단계 **7** 모니터링에서 제외할 포트를 **Port(**포트**)** 필드에 입력합니다.

단일 포트를 지정할 수도 있고, 대시(-)를 사용하여 포트 범위를 지정하거나, 쉼표로 구분된 포트 목록 및 포트 범위를 지정할 수도 있습니다. 허용되는 값의 범위는 1~65535입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** 포트가 목록에 즉시 나타나지 않으면 **Refresh(**새로 고침**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 검색 규칙의 영역

성능 개선을 위해, 규칙 내 영역이 규칙에서 모니터링할 네트워크에 물리적으로 연결된 매니지드 디바이스에 센싱 인터페이스를 포함하도록 검색 규칙을 설정할 수 있습니다.

그러나 네트워크 설정 변경 사항에 대해 항상 지속적으로 알림을 받지는 못할 수도 있습니다. 네트워크 관리자는 별도의 알림 없이 라우팅 또는 호스트 변경을 통해 네트워크 설정을 수정할 수 있으며, 이 경우 적절한 네트워크 검색 정책 설정의 최신 상태를 유지하기가 어려울 수 있습니다. 매니지드 디바이스의 센싱 인터페이스가 네트워크에 어떻게 물리적으로 연결되는지 모른다면, 영역 설정을

기본값으로 유지하십시오. 이 기본값은 시스템이 검색 규칙을 구축 내 모든 영역에 구축하게 합니다. (제외되는 영역이 없다면, 시스템은 검색 정책을 모든 영역에 구축합니다.)

네트워크 검색 규칙의 영역 구성

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Zones(**영역**)**를 클릭합니다.

단계 **4** **Available Zones(**사용 가능한 영역**)** 목록에서 영역을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

트래픽 기반 탐지 ID 소스

트래픽 기반 탐지는 Firepower System에서 지원하는 유일한 권한 없는 ID 소스입니다. 매니지드 디바이스가 구성된 경우 지정한 네트워크에서 LDAP, AIM, POP3, IMAP, Oracle, SIP(VoIP), FTP, HTTP, MDNS 및 SMTP 로그인을 탐지합니다. 트래픽 기반 탐지에서 수집된 데이터는 사용자 인식에만 사용할 수 있습니다. 권한 있는 ID 소스와 달리, 네트워크 검색 정책의 트래픽 기반 탐지는 트래픽 기반 사용자 탐지 구성, 2549 페이지에 설명된 대로 구성합니다.

다음과 같은 제한 사항을 참고하십시오.

- 트래픽 기반 탐지는 LDAP 연결에 대한 Kerberos 로그인만 LDAP 인증으로 해석합니다. 매니지드 디바이스는 SSL이나 TLS 등의 프로토콜을 사용하는 암호화된 LDAP 인증을 탐지할 수 없습니다.
- 트래픽 기반 탐지는 OSCAR 프로토콜만을 사용하여 AIM 로그인을 탐지합니다. TOC2를 사용하여 AIM 로그인을 탐지할 수는 없습니다.
- 트래픽 기반 탐지는 SMTP 로깅을 제한할 수 없습니다. 이는 사용자가 SMTP 로그인을 기반으로 데이터베이스에 추가되지 않기 때문입니다. 시스템이 SMTP 로그인을 탐지하더라도 데이터베이스에 일치하는 이메일 주소의 사용자가 이미 있지 않으면 로그인이 기록되지 않습니다.

트래픽 기반 탐지는 실패한 로그인 시도도 기록합니다. 실패한 로그인 시도는 데이터베이스의 사용자 목록에 새 사용자를 추가하지 않습니다. 트래픽 기반 탐지로 탐지된 실패한 로그인 활동에 대한 사용자 활동 유형은 **Failed User Login(**실패한 사용자 로그인**)**입니다.

참고 시스템은 실패한 HTTP 로그인과 성공한 HTTP 로그인을 구분할 수 없습니다. HTTP 사용자 정보를 보려면 트래픽 기반 탐지 컨피그레이션에서 **Capture Failed Login Attempts(**실패한 로그인 시도 캡처**)**를 활성화해야 합니다.

주의 네트워크 검색 정책을 사용하여 HTTP, FTP 또는 MDNS 프로토콜을 통한 신뢰할 수 없는 트래픽 기반 사용자 탐지를 활성화하거나 비활성화 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

트래픽 기반 탐지 데이터

디바이스가 트래픽 기반 탐지를 사용하여 로그인을 탐지하면 다음 정보를 Firepower Management Center로 전송하여 사용자 활동으로 로깅됩니다.

- 로그인에서 확인된 사용자 이름
- 로그인 시간
- 로그인과 관련된 IP 주소. 사용자 호스트(LDAP, POP3, IMAP 및 AIM 로그인), 서버(HTTP, MDNS, FTP, SMTP 및 Oracle 로그인) 또는 세션 시작 주체(SIP 로그인)의 IP 주소일 수 있습니다.
- 사용자의 이메일 주소(POP3, IMAP, SMTP 로그인용)
- 로그인을 탐지한 디바이스의 이름

사용자가 이전에 탐지된 적이 있는 경우, Firepower Management Center에서는 해당 사용자의 로그인 기록을 업데이트합니다. Firepower Management Center는 POP3 및 IMAP 로그인의 이메일 주소를 사용하여 LDAP 사용자와의 상관관계를 분석합니다. 예를 들어 Firepower Management Center에서 새로운 IMAP 로그인을 탐지하고 IMAP 로그인의 이메일 주소가 기존 LDAP 사용자와 일치할 경우, IMAP 로그인에서는 신규 사용자를 생성하지 않고 해당 LDAP 사용자의 내역을 업데이트합니다.

사용자가 이전에 탐지된 적이 없는 경우, Firepower Management Center에서는 해당 사용자를 사용자 데이터베이스에 추가합니다. 이러한 로그인 이벤트에는 Firepower Management Center에서 다른 로그인 유형과의 상관관계를 분석할 수 있는 데이터가 없으므로, 고유한 AIM, SIP, Oracle 로그인에서는 항상 새로운 사용자 레코드를 생성합니다.

Firepower Management Center에서는 다음과 같은 경우 사용자 활동 또는 사용자 신원을 기록하지 않습니다.

- 해당 로그인 유형을 무시하도록 네트워크 검색 정책을 구성한 경우
- 매니지드 디바이스에서 SMTP 로그인을 탐지했지만 사용자 데이터베이스에 일치하는 이메일 주소를 보유한 이전에 탐지된 LDAP, POP3 또는 IMAP 사용자가 없는 경우

사용자 데이터가 사용자 테이블에 추가됩니다.

트래픽 기반 탐지 전략

가장 완전한 사용자 정보를 제공할 수 있을 것 같은 사용자들에게 집중할 수 있도록 사용자 활동을 검색하는 프로토콜을 제한하여 탐지되는 총 사용자 수를 줄일 수 있습니다. 프로토콜 탐지를 제한하면 정리되지 않은 사용자 이름을 최소화하고 Firepower Management Center의 스토리지 공간을 보존하는 데 도움이 됩니다.

트래픽 기반 탐지 프로토콜을 선택할 경우 다음 사항을 고려하십시오.

- AIM, POP3, IMAP 등의 프로토콜을 통해 사용자 이름을 가져오는 경우 계약직원, 방문자, 기타 손님 등의 네트워크 액세스 때문에 조직과 관련이 없는 사용자 이름이 포함될 수 있습니다.
- AIM, Oracle, SIP 로그인은 외부 사용자 레코드를 생성할 수 있습니다. 이러한 로그인 유형은 LDAP 서버에서 시스템이 가져오는 사용자 메타데이터와도 연결되지 않고, 매니지드 디바이스에서 탐지하는 기타 로그인 유형에 포함된 정보와도 연결되지 않으므로 이 문제가 발생합니다. 따라서 Firepower Management Center는 이러한 사용자를 다른 사용자 유형과 상호 연결할 수 없습니다.

트래픽 기반 사용자 탐지 구성

네트워크 검색 규칙에서 트래픽 기반 사용자 탐지를 활성화하면 호스트 검색이 자동으로 활성화됩니다. 트래픽 기반 탐지에 대한 자세한 내용은 트래픽 기반 탐지 ID 소스, 2547 페이지를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Users(**사용자**)**를 클릭합니다.

단계 **3** 수정( ) 버튼을 클릭합니다.

단계 **4** 로그인을 탐지하려는 프로토콜에 대한 확인란을 선택하거나, 로그인을 탐지하지 않으려는 프로토콜에 대한 확인란을 선택 취소합니다.

단계 **5** 선택적으로, LDAP, POP3, FTP 또는 IMAP 트래픽에서 탐지되는 실패한 로그인 시도를 기록하거나 HTTP 로그인에 대한 사용자 정보를 캡처하려면 **Capture Failed Login Attempts(**실패한 로그인 시도 캡처**)**를 활성화합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

주의 네트워크 검색 정책을 사용하여 HTTP, FTP 또는 MDNS 프로토콜을 통한 신뢰할 수 없는 트래픽 기반 사용자 탐지를 활성화하거나 비활성화 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오.

- 네트워크 검색 규칙 구성, 2540 페이지에 설명된 대로 사용자를 검색할 네트워크 검색 규칙을 구성합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

고급 네트워크 검색 옵션 설정

네트워크 검색 정책의 Advanced(고급)에서는 어떤 이벤트를 탐지할지, 검색 데이터를 얼마 동안 보존하고 얼마나 자주 업데이트할지, 영향 상관관계에 어떤 취약성 매핑을 사용할지, 운영체제 및 서버 ID 충돌을 어떻게 해결할지 등 정책 전반의 설정을 구성할 수 있습니다. 또한 다른 소스에서 데이터를 가져올 수 있도록 호스트 입력 소스 및 NetFlow 엑스포터를 추가할 수 있습니다.

참고 데이터베이스 이벤트는 검색 및 사용자 활동 이벤트가 시스템 설정에서 설정되도록 제한합니다.

프로시저

단계 **1** **Policies(정책)** > **Network Discovery(네트워크 검색)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Advanced(고급)**를 클릭합니다.

단계 **3** 수정할 설정 옆에 있는 수정( ) 또는 추가( )을 클릭합니다.

- 데이터 스토리지 설정 - 네트워크 검색 데이터 스토리지 설정, 2558 페이지에 설명된 대로 설정을 업데이트합니다.
- 이벤트 로깅 설정 - 네트워크 검색 이벤트 기록 설정, 2558 페이지에 설명된 대로 설정을 업데이트합니다.
- 일반 설정 - 네트워크 검색 일반 설정 구성, 2551 페이지에 설명된 대로 설정을 업데이트합니다.
- ID 충돌 설정 - 네트워크 검색 ID 충돌 확인 설정, 2553 페이지에 설명된 대로 설정을 업데이트합니다.
- 침해 지표 설정 - 보안 침해 지표 규칙 활성화, 2555 페이지에 설명된 대로 설정을 업데이트합니다.

- NetFlow 엑스포터 - 네트워크 검색 정책에 NetFlow 엑스포터 추가, 2556 페이지에 설명된 대로 설정을 업데이트합니다.
- 운영체제 및 서버 ID 소스 - 네트워크 검색 OS 및 서버 ID 소스 추가, 2559 페이지에 설명된 대로 설정을 업데이트합니다.
- 영향 평가에 사용할 취약성 - 네트워크 검색 취약성 영향 평가 활성화, 2554 페이지에 설명된 대로 설정을 업데이트합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

데이터베이스 이벤트 제한 수, 1351 페이지

네트워크 검색 일반 설정

일반 설정은 시스템이 네트워크 맵을 업데이트하는 빈도 및 검색 중 서버 배너의 캡처 여부를 제어합니다.

배너 캡처

시스템이 서버 벤더 및 버전("배너")을 광고하는 네트워크 트래픽에서 헤더 정보를 저장하도록 하려면 이 확인란을 선택합니다. 이 정보는 수집하는 정보에 추가 콘텍스트를 제공할 수 있습니다. 서버 상세정보에 액세스하여 호스트에 대해 수집된 서버 배너에 액세스할 수 있습니다.

업데이트 간격

호스트의 IP 주소 중 하나가 마지막으로 표시된 시간, 애플리케이션이 사용된 시간 또는 애플리케이션의 히트 수 등의 정보를 시스템이 업데이트하는 간격입니다. 기본 설정은 3,600초(1시간)입니다.

업데이트 시간 초과의 간격을 더 낮게 설정하면 호스트 표시에 더 정확한 정보가 제공되지만, 네트워크 이벤트가 더 많이 생성됩니다.

네트워크 검색 일반 설정 구성

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다.

단계 3 **General Settings(**일반 설정**)** 옆의 수정( )을(를) 클릭합니다.

단계 4 네트워크 검색 일반 설정, 2551 페이지에 설명된 대로 설정을 업데이트합니다.

단계 5 **Save(**저장**)**를 클릭하여 일반 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 검색 ID 충돌 설정

시스템은 운영체제와 서버에 대한 핑거프린트를 트래픽 내 패턴과 일치시켜, 호스트에서 실행 중인 운영체제와 애플리케이션을 확인합니다. 가장 신뢰할 수 있는 운영체제 및 서버 ID 정보를 제공하기 위해 시스템은 여러 소스에서 온 핑거프린트 정보를 맞춰봅니다.

시스템은 운영체제 ID를 도출하고 신뢰도 값을 할당하기 위해 모든 수동 데이터를 사용합니다.

기본적으로 ID 충돌이 없으면, 스캐너 또는 서드파티 애플리케이션에 의해 추가된 ID 데이터가 Firepower System에 의해 탐지된 ID 데이터를 재정의합니다. 우선순위별로 스캐너 및 서드파티 애플리케이션 핑거프린트 소스의 순위를 매기려면 Identity Sources 설정을 사용할 수 있습니다. 시스템은 각 소스에 대해 하나의 ID를 보유하지만, 우선순위가 가장 높은 서드파티 애플리케이션 또는 스캐너 소스의 데이터만 현재 ID로 사용됩니다. 그러나 우선순위와 상관없이 사용자 입력 데이터가 스캐너 및 서드파티 애플리케이션 데이터를 재정의한다는 점에 유의하십시오.

시스템이 Identity Sources 설정에 나열된 활성 스캐너나 서드파티 애플리케이션 소스 또는 Firepower System 사용자에게서 온 기존 ID와 충돌하는 ID를 탐지하면 ID 충돌이 발생합니다. 기본적으로 ID 충돌은 자동으로 해결되지 않으므로, 호스트 프로파일을 통해 또는 호스트를 다시 스캔하거나 새 ID 데이터를 다시 추가하여 수동 ID를 재정의함으로써 충돌을 해결해야 합니다. 하지만 수동 ID나 활성를 유지하여 충돌을 자동으로 해결하도록 시스템을 설정할 수 있습니다.

ID 충돌 이벤트 생성

ID 충돌이 발생할 때 시스템의 이벤트 생성 여부를 지정합니다.

충돌 자동 해결

Automatically Resolve Conflicts(충돌 자동 해결**)** 드롭다운 목록에서 다음 중 하나를 선택합니다.

- **Disabled(**비활성**)** - ID 충돌의 수동 충돌 해결을 강제 실행하려는 경우
- **Identity(ID)** - ID 충돌 발생 시 시스템이 수동 핑거프린트를 사용하게 하려는 경우
- **Keep Active(**활성 상태 유지**)** - ID 충돌 발생 시 시스템이 우선순위가 가장 높은 활성 소스의 현재 ID를 사용하게 하려는 경우

네트워크 검색 ID 충돌 확인 설정

프로시저

단계 1 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 2 **Advanced(**고급**)**를 클릭합니다.

단계 3 **Identity Conflict Settings(ID** 충돌 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 4 네트워크 검색 ID 충돌 설정, 2552 페이지에 설명된 대로 Edit Identity Conflict Settings(ID 충돌 설정 편집) 팝업 윈도우의 설정을 업데이트합니다.

단계 5 **Save(**저장**)**를 클릭하여 ID 충돌 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 검색 취약성 영향 평가 옵션

Firepower System에서 침입 이벤트로 영향 상관관계를 수행하는 방법을 구성할 수 있습니다. 선택 항목은 다음과 같습니다.

- 시스템 기반 취약성 정보를 사용하여 영향 상관관계를 수행하려면 **Use Network Discovery Vulnerability Mappings(**네트워크 검색 취약성 매핑 사용**)** 확인란을 선택합니다.
- 서드파티 취약성 참조를 사용하여 영향 상관관계를 수행하려면 **Use Third-Party Vulnerability Mappings(**서드파티 취약성 매핑 사용**)** 확인란을 선택합니다. 자세한 내용은 *Firepower System Host Input API* 설명서을 참조하십시오.

확인란 하나 또는 둘 다를 선택할 수 있습니다. 시스템이 침입 이벤트를 생성하며 선택한 취약성 매핑 집합의 취약성과 함께 이벤트 관련 호스트에 서버나 운영체제가 있는 경우, 침입 이벤트는 Vulnerable (level 1: red) 영향 아이콘으로 표시됩니다. 벤더 또는 버전 정보가 없는 서버의 경우 Firepower Management Center 설정에서 취약성 매핑을 활성화해야 합니다.

두 확인란을 모두 선택 취소한 경우 침입 이벤트는 Vulnerable (level 1: red) 영향 아이콘으로 표시되지 않습니다.

관련 항목

서드파티 취약성 매핑, 2410 페이지
서버의 취약성 매핑, 1389 페이지

네트워크 검색 취약성 영향 평가 활성화

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **Vulnerabilities to use for Impact Assessment(**충격 평가에 사용할 취약성**)** 옆의 수정( )을 클릭합니다.

단계 **4** 네트워크 검색 취약성 영향 평가 옵션, 2553 페이지에 설명된 대로 Edit Vulnerability Settings(취약성 설정 편집) 팝업 윈도우의 설정을 업데이트합니다.

단계 **5** 취약성 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

보안 침해 지표

Firepower System은 네트워크 검색 정책에서 IOC 규칙을 사용하여 악의적인 수단에 의해 침해될 가능성이 높은 호스트를 식별합니다. 호스트가 이러한 시스템 제공 규칙에 제정된 조건을 충족하면, 시스템은 호스트에 침해 지표(IOC) 태그를 지정합니다. 관련된 규칙을 *IOC* 규칙이라고 합니다. 각 IOC 규칙은 IOC 태그 유형 중 하나에 대응합니다. *IOC* 태그는 가능성이 높은 침해의 특성을 지정합니다.

Firepower Management Center은(는) 다음 중 하나가 발생하면 관련된 호스트 을(를) 태그할 수 있습니다.

- 시스템은 침입, 연결, Security Intelligence(보안 인텔리전스), 파일 또는 악성 이벤트를 이용해, 모니터링되는 네트워크 및 네트워크 트래픽과 관련해 수집한 데이터를 상호 연결하고 잠재 IOC 발생 여부를 확인합니다.
- Firepower Management Center은(는) AMP 클라우드를 통해 엔드포인트 구축을 위한 IOC 데이터를 AMP에서 가져올 수 있습니다. 이 데이터는 호스트 자체에 대한 활동(예: 개별 프로그램에 의해 또는 개별 프로그램에서 수행되는 작업)을 검토하므로, 네트워크 전용 데이터에서는 할 수 없는 위협 가능성에 대한 통찰력을 제공할 수 있습니다. 사용자 편의를 위해, Firepower Management Center은(는) Cisco가 AMP 클라우드를 통해 개발한 새로운 IOC 태그 일체를 자동으로 획득합니다.

이 기능을 설정하려면 보안 침해 지표 규칙 활성화, 2555 페이지 섹션을 참조하십시오.

IOC 태그가 있는 호스트를 설명하는 호스트 IOC 데이터와 규정준수 화이트리스트에 대한 상관관계 규칙을 작성할 수도 있습니다.

태그가 지정된 IOC를 조사하고 사용하는 방법은 보안 침해 지표 데이터, 3056 페이지 및 그 하위 항목을 참조하십시오.

보안 침해 지표 규칙 활성화

시스템에서 보안 침해 지표(Indications of compromise, IOC)를 탐지하고 태그하도록 하려면 먼저 네트워크 검색 정책에서 하나 이상의 IOC 규칙을 활성화해야 합니다. 각 IOC 규칙은 한 유형의 IOC 태그에 해당하며 모든 IOC 규칙은 Cisco에서 사전 정의합니다. 원본 규칙은 사용자가 생성할 수 없습니다. 네트워크 및 조직의 필요에 따라 규칙의 일부 또는 전체를 활성화할 수 있습니다. 예를 들어, Microsoft Excel과 같은 소프트웨어를 사용하는 호스트가 모니터링되는 네트워크에 나타나지 않으면 Excel 기반 위협에 해당하는 IOC 태그를 활성화하지 않을 수 있습니다.

팁 개별 호스트에 대한 IOC 규칙을 비활성화하려면 단일 호스트에 대한 보안 침해 지표 규칙 상태 수정, 3059 페이지을 참조하십시오.

시작하기 전에

IOC 규칙은 Firepower System의 기타 구성 요소 및 AMP for Endpoints에서 제공한 데이터를 기반으로 트리거되므로, 이러한 구성 요소는 IOC 규칙에 올바르게 라이선스를 부여하고 구성하여 IOC 태그를 설정해야 합니다. 활성화할 IOC 규칙과 연결된 Firepower System 기능을 활성화합니다(예: 침입 탐지 및 방지(IPS) 및 AMP(Advanced Malware Protection)). IOC 규칙의 연결된 기능이 활성화되지 않으면 관련 데이터가 수집되지 않으며 규칙을 트리거할 수 없습니다.

프로시저

단계 1 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 2 **Advanced(**고급**)**를 클릭합니다.

단계 3 **Indications of Compromise Settings(**감염 지표 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 4 전체 IOC 기능을 설정 또는 해제하려면 **Enable IOC** 옆에 있는 슬라이더를 클릭합니다.

단계 5 개별 IOC 규칙을 전역으로 활성화 또는 비활성화하려면 규칙의 **Enabled(**활성화됨**)** 열에 있는 슬라이더를 클릭합니다.

단계 6 IOC 규칙 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 검색 정책에 NetFlow 엑스포터 추가

시작하기 전에

- 사용하려는 NetFlow 엑스포터를 Firepower System의 Netflow 데이터, 2381 페이지에 설명된 대로 구성합니다.
- NetFlow 데이터를 사용하기 위한 요건, 2382 페이지에 설명된 기타 NetFlow 사전 요구 사항을 검토합니다.

프로시저

단계 1 **Policies(정책)** > **Network Discovery(네트워크 검색)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 2 **Advanced(고급)**를 클릭합니다.

단계 3 **NetFlow Devices(NetFlow 디바이스)** 옆의 추가( )을 클릭합니다.

단계 4 매니지드 디바이스로 NetFlow 데이터를 수집할 네트워크 디바이스의 IP 주소를 **IP Address(IP 주소)** 필드에 입력합니다.

단계 5 선택 사항:

- NetFlow 엑스포터를 더 추가하려면 이전의 두 단계를 반복합니다.
- 삭제( )를 클릭하여 NetFlow 엑스포터를 제거합니다. 검색 규칙에서 NetFlow 엑스포터를 사용할 경우, Advanced(고급) 페이지에서 디바이스를 삭제하려면 먼저 규칙을 삭제해야 합니다.

단계 6 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

- 네트워크 검색 규칙 구성, 2540 페이지에 설명된 대로 NetFlow 트래픽을 모니터링할 네트워크 검색 규칙을 구성합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 검색 데이터 스토리지 설정

검색 데이터 저장소 설정에는 호스트 제한 및 시간 초과 설정을 포함합니다.

호스트 제한 도달 시

Firepower Management Center가 모니터링할 수 있는 호스트, 즉 네트워크 맵에 저장할 수 있는 호스트 수는 모델에 따라 다릅니다. 호스트 제한 시 옵션은 호스트 제한에 도달했을 때 새 호스트를 탐지하는 경우의 동작을 제어합니다. 다음 작업을 수행할 수 있습니다.

호스트 제거

시스템은 오랫동안 비활성 상태인 호스트를 제거하고 새 호스트를 추가합니다. 이 설정이 기본 설정입니다.

새 호스트 추가 금지

시스템에서 새로 검색된 모든 호스트를 추적하지 않습니다. 시스템은 관리자가 도메인의 호스트 제한을 늘리거나 네트워크 맵에서 수동으로 호스트를 삭제하는 경우, 또는 시스템이 비활성화되어 시간 제한을 초과한 호스트를 식별하여 호스트가 제한 수 이하가 되면 새 호스트를 추적합니다.

다중 도메인 구축에서 리프 도메인은 모니터링되는 호스트의 사용 가능 풀을 공유합니다. 각 리프 도메인이 네트워크 맵을 채울 수 있도록 도메인 속성의 하위 도메인 레벨에서 호스트 제한을 설정할 수 있습니다. 각 리프 도메인에 자체 네트워크 검색 정책이 있으므로 각 리프 도메인은 시스템에서 새 호스트를 검색할 때 다음과 같이 고유한 동작을 제어합니다.

표 ***252:*** 멀티 테넌시의 호스트 제한 도달

설정	도메인 호스트 제한 설정은**?**	도메인 호스트 제한에 도달함	상위 도메인 호스트 제한에 도달함
호스트 제거	예	제한된 도메인에 있는 가장 오래된 호스트를 삭제합니다.	호스트를 삭제하도록 구성된 모든 하위 리프 도메인 중에서 가장 오래된 호스트를 삭제합니다. 호스트가 삭제되지 않는 경우 호스트를 추가하지 않습니다.
	아니요	해당 없음	일반 풀을 공유하고 호스트를 삭제하도록 구성된 모든 하위 리프 도메인 중 가장 오래된 호스트를 삭제합니다.
새 호스트 추가 금지	예 또는 아니오	호스트를 추가하지 않습니다.	호스트를 추가하지 않습니다.

호스트 시간 초과

시스템이 비활성화 상태의 호스트를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(1주일)입니다. 개별 호스트 IP 및 MAC 주소는 개별적으로 시간이 초과되지만 호스트는 관련된 모든 주소가 시간 초과되기 전에는 네트워크 맵에서 사라지지 않습니다.

호스트의 조기 시간 초과를 방지하려면 호스트의 시간 제한 값이 네트워크 검색 정책 일반 설정의 업데이트 간격보다 긴지 확인합니다.

서버 시간 초과

시스템이 비활성화 상태의 서버를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(1주일)입니다.

서버의 조기 시간 초과를 방지하려면 서비스의 시간 제한 값이 네트워크 검색 정책 일반 설정의 업데이트 간격보다 긴지 확인합니다.

클라이언트 애플리케이션 시간 초과

시스템이 비활성화 상태의 클라이언트를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(1주일)입니다.

클라이언트의 조기 시간 초과를 방지하려면 클라이언트의 시간 제한 값이 네트워크 검색 정책 일반 설정의 업데이트 간격보다 긴지 확인합니다.

관련 항목

Firepower System 호스트 제한, 2391 페이지
도메인 속성, 483 페이지

네트워크 검색 데이터 스토리지 설정

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **Data Storage Settings(**데이터 스토리지 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 **4** 네트워크 검색 데이터 스토리지 설정, 2556 페이지에 설명된 대로 Data Storage Settings(데이터 스토리지 설정) 대화 상자의 설정을 업데이트합니다.

단계 **5** **Save(**저장**)**를 클릭하여 데이터 스토리지 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 검색 이벤트 기록 설정

Event Logging Settings(이벤트 기록 설정)는 검색 및 호스트 입력 이벤트의 기록 여부를 제어합니다. 이벤트를 기록하지 않으면 이벤트 보기에서 검색할 수 없거나, 상관관계 규칙을 트리거하는 데 사용할 수 없습니다.

프로시저

단계 1 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 2 **Advanced(**고급**)**를 클릭합니다.

단계 3 **Event Logging Settings(**이벤트 기록 설정**)** 옆에 있는 수정( )을 클릭합니다.

단계 4 검색 이벤트 유형, 3039 페이지 및 호스트 입력 이벤트 유형, 3043 페이지에서 설명하는 것처럼, 데이터베이스에 기록할 검색 및 호스트 입력 이벤트 유형 옆에 있는 확인란을 선택하거나 선택 취소합니다.

단계 5 **Save(**저장**)**를 클릭하여 이벤트 기록 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

네트워크 검색 OS 및 서버 ID 소스 추가

네트워크 검색 정책의 Advanced(고급)에서 새 활성 소스를 추가하거나 기존 소스의 우선순위 또는 시간 초과 설정을 변경할 수 있습니다.

이 페이지에 스캐너를 추가한다고 해서 Nmap 스캐너에 대해 존재하는 모든 통합 기능이 추가되지는 않지만, 가져온 서드파티 애플리케이션 또는 스캔 결과를 통합하는 것은 가능합니다.

서드파티 애플리케이션 또는 스캐너에서 데이터를 가져오는 경우 소스의 취약성을 네트워크에서 탐지한 취약성에 매핑해야 합니다.

프로시저

단계 1 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 2 **Advanced(**고급**)**를 클릭합니다.

단계 3 **OS and Server Identity Sources(**운영체제 및 서버 **ID** 소스**)** 옆에 있는 수정( )을 클릭합니다.

단계 4 새 소스를 추가하려면 **Add Source(**소스 추가**)**를 클릭합니다.

단계 5 **Name(**이름**)**을 입력합니다.

단계 6 드롭다운 목록에서 입력 소스 **Type(**유형**)**을 선택합니다.

- AddScanResult 기능을 사용하여 스캔 결과를 가져오려면 **Scanner(**스캐너**)**를 선택합니다.
- 스캔 결과를 가져오지 않으려는 경우에는 **Application(**애플리케이션**)**을 선택합니다.

단계 **7** 이 소스가 네트워크 맵에 ID가 추가되는 시간과 해당 ID가 삭제되는 시간 사이의 간격을 지정하려면 **Timeout(**시간 초과**)** 드롭다운 목록에서 **Hours(**시간**)**, **Days(**일**)** 또는 **Weeks(**주**)**를 선택하고 적절한 기간을 입력합니다.

단계 **8** 선택 사항:

- 특정 소스를 승격하여 운영체제 및 애플리케이션 ID가 목록에서 그 아래에 있는 소스에 사용되도록 하려면, 해당 소스를 선택하고 위쪽 화살표를 클릭합니다.
- 특정 소스를 강등하여 목록에서 그 위에 있는 소스가 제공하는 ID가 없는 경우에만 운영체제 및 애플리케이션 ID가 사용되도록 하려면, 해당 소스를 선택하고 아래쪽 화살표를 클릭합니다.
- 소스를 삭제하려면 소스 옆에 있는 삭제( )을 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭하여 ID 소스 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

관련 항목

서드파티 취약성 매핑, 2410 페이지

네트워크 검색 전략 문제 해결

시스템의 기본 탐지 기능을 변경하려면 먼저 어떤 호스트가 올바르게 식별되지 않는지, 그 이유가 무엇인지를 분석해야 합니다. 그래야만 어떤 해결책을 구현할지 결정할 수 있습니다.

매니지드 디바이스의 배치가 올바릅니까?

로드 밸런서, 프록시 서버 또는 NAT 디바이스 같은 네트워크 디바이스가 매니지드 디바이스 및 식별되지 않는/잘못 식별된 호스트 사이에 상주하는 경우, 맞춤형 핑거프린트를 사용하기보다는 매니지드 디바이스를 잘못 식별된 호스트에 더 가까이 두십시오. Cisco는 이 시나리오에서 맞춤형 핑거프린트의 사용을 권장하지 않습니다.

식별되지 않은 운영체제에 고유한 TCP 스택이 있습니까?

시스템에서 호스트를 잘못 식별하면 호스트가 잘못 식별된 이유를 조사하여, 맞춤형 핑거프린트를 생성 및 활성화할지 아니면 검색 데이터 대신 Nmap 또는 호스트 입력 데이터를 사용할지를 결정해야 합니다.

⚠

주의 잘못 식별된 호스트를 발견하면 맞춤형 핑거프린트를 생성하기 전에 먼저 지원 부서에 문의하십시오.

기본적으로 호스트가 시스템에서 탐지되지 않는 운영체제를 실행 중이며 TCP 스택 특성 파악 내용을 기존의 탐지된 운영체제와 공유하지 않는 경우에는 맞춤형 핑거프린트를 생성해야 합니다.

예를 들어 시스템이 식별할 수 없는 고유한 TCP 스택의 맞춤형된 Linux 버전을 가지고 있는 경우 맞춤형 핑거프린트를 생성하면 도움이 될 수 있습니다. 이렇게 하면 시스템은 스캔 결과나 서드파티 데이터를 사용하는 대신 호스트를 식별하고 지속적으로 모니터링할 수 있습니다. 이 경우 사용자가 직접 지속적, 능동적으로 데이터를 업데이트해야 합니다.

많은 오픈 소스 Linux 배포에서 동일한 커널이 사용되며, 시스템은 Linux 커널 이름을 사용하여 이들을 식별합니다. Red Hat Linux 시스템에 대해 사용자 핑거프린트를 생성하는 경우, 동일한 핑거프린트가 여러 Linux 배포 제품과 일치하기 때문에 다른 운영체제(예: Debian Linux, Mandrake Linux, Knoppix 등)도 Red Hat Linux로 표시될 수 있습니다.

모든 상황에 핑거프린트를 사용해서는 안 됩니다. 예를 들어 호스트의 TCP 스택이 다른 운영체제와 유사하거나 동일하게 수정되었을 수 있습니다. 예를 들어 Apple Mac OS X 호스트가 변경되어 핑거프린트가 Linux 2.4 호스트와 일치하게 되면 시스템은 이를 Mac OS X가 아닌 Linux 2.4로 식별합니다. Mac OS X 호스트의 맞춤형 핑거프린트를 생성하면, 적합한 모든 Linux 2.4 호스트가 Mac OS X 호스트로 잘못 식별될 수 있습니다. 이 경우 Nmap이 호스트를 올바르게 식별하면 해당 호스트에 대해 주기적인 Nmap 스캔을 예약할 수 있습니다.

호스트 입력을 사용하여 서드파티 시스템의 데이터를 가져오는 경우, 서드파티가 서버 및 애플리케이션 프로토콜을 설명하는 데 사용하는 벤더, 제품 및 버전 문자열을 해당 제품의 Cisco 정의에 매핑해야 합니다. 애플리케이션 데이터를 Firepower System 벤더 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

시스템에서는 운영체제 또는 애플리케이션에 대한 현재 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

Nmap 데이터의 경우 정기적인 Nmap 스캔을 예약할 수 있습니다. 호스트 입력 데이터의 경우 가져오기 또는 명령줄 유틸리티에 대해 Perl 스크립트를 정기적으로 실행할 수 있습니다. 그러나 활성 스캔 데이터 및 호스트 입력 데이터는 검색 데이터의 빈도로 업데이트되지 않을 수 있습니다.

Firepower System이 모든 애플리케이션을 식별할 수 있습니까**?**

호스트가 시스템에서 올바르게 식별되지만 미확인 애플리케이션을 포함하고 있는 경우, 애플리케이션 식별에 도움이 되도록 사용자 정의 탐지기를 생성하여 시스템에 포트 및 패턴 매칭 정보를 제공할 수 있습니다.

취약성을 수정하는 패치를 적용했습니까**?**

시스템이 호스트를 올바르게 식별하지만 적용된 수정을 반영하지 않는 경우 호스트 입력 기능을 사용하여 패치 정보를 가져올 수 있습니다. 패치 정보를 가져오면 수정 이름을 데이터베이스의 수정에 매핑해야 합니다.

서드파티 취약성을 추적하고자 합니까**?**

영향 상관관계에 사용하고자 하는 서드파티 시스템의 취약성 정보를 가지고 있는 경우, 서버 및 애플리케이션 프로토콜에 대한 서드파티 취약성 식별자를 Cisco 데이터베이스의 취약성 식별자에 매핑한 다음 호스트 입력 기능을 사용하여 취약성을 가져올 수 있습니다. 호스트 입력 기능 사용에 관한 자세한 정보는 *Firepower System Host Input API* 설명서 섹션을 참조하십시오. 애플리케이션 데이터를 Firepower System 벤더 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

XXI 부

상관관계 및 컴플라이언스

- 컴플라이언스 화이트 목록, 2565 페이지
- 상관관계 정책, 2583 페이지
- 트래픽 프로파일, 2623 페이지
- 치료, 2637 페이지

104 장

컴플라이언스 화이트 목록

다음 주제에서는 상관관계 정책에 추가하기 전에 규정준수 화이트리스트를 설정하는 방법을 설명합니다.

- 컴플라이언스 화이트 목록 소개, 2565 페이지
- 컴플라이언스 요구 사항 및 사전 요건, 2571 페이지
- 규정준수 화이트 목록 생성, 2571 페이지
- 규정준수 화이트리스트 관리, 2577 페이지
- 공유 호스트 프로파일 관리, 2580 페이지

컴플라이언스 화이트 목록 소개

줄여서 화이트 목록이라고도 하는 컴플라이언스 화이트 목록은 네트워크의 호스트에서 허용할 운영체제, 애플리케이션(웹 및 클라이언트)을 지정하는 기준 모음입니다. 호스트가 이 목록에 없으면 시스템은 이벤트(위반)를 생성합니다.

컴플라이언스 화이트 목록은 다음과 같은 두 가지 주요 구성 요소로 이루어집니다.

- 대상은 컴플라이언스 평가를 위해 선택한 호스트입니다. 모니터링되는 전체 또는 일부 호스트를 서브넷, VLAN 및 호스트 속성으로 제한해 평가할 수 있습니다. 다중 도메인 구축의 경우에는 도메인과 도메인 내부 또는 사이에 있는 서브켓을 지정할 수 있습니다.
- 호스트 프로파일은 대상의 규정준수 기준을 지정합니다. 전역 호스트 프로파일은 운영체제의 구속을 받지 않습니다. 하나의 화이트 목록에 국한되거나 여러 화이트 목록이 공유하는 운영체제별 호스트 프로파일을 설정할 수도 있습니다.

Cisco Talos Intelligence Group(Talos)은(는) 권장 설정을 적용한 기본 화이트 목록을 제공합니다. 맞춤형 화이트 목록을 만들 수도 있습니다. 단순 맞춤형 목록은 특정 운영체제를 실행하는 호스트만 허용할 수 있습니다. 더 복잡한 목록은 모든 운영체제를 허용할 수 있지만, 특정 포트에서 특정 애플리케이션 프로토콜을 실행하기 위해 호스트가 사용해야 하는 운영체제를 지정합니다.

참고 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지의 내용을 참조하십시오.이러한 제한은 컴플라이언스 화이트 목록을 작성하는 방법에 영향을 미칠 수 있습니다.

컴플라이언스 화이트 목록 구현

화이트 목록을 구현하려면 해당 목록을 활성 상관관계 정책에 추가해야 합니다. 시스템은 대상을 평가하고 모든 호스트를 대응하는 속성에 할당합니다.

- 규정준수 - 호스트가 해당 목록을 위반하지 않습니다.
- 규정 미준수 - 호스트가 해당 목록을 위반합니다.
- 미평가 - 호스트가 해당 목록의 대상이 아니거나, 호스트가 현재 평가 중이거나, 정보가 부족해 시스템이 호스트의 규정준수 여부를 판단할 수 없습니다.

참고 호스트 속성을 삭제하려면 해당 화이트 목록을 삭제해야 합니다. 상관관계 정책에서 화이트 목록을 비활성화, 삭제 또는 제거하더라도 호스트 속성은 삭제되지 않으며, 각 호스트에 대한 속성의 값도 변경되지 않습니다.

최초 평가가 끝나면 시스템은 모니터링되는 호스트가 활성 화이트 목록에 대한 규정준수에서 벗어날 때마다 화이트 목록 이벤트를 생성하며, 화이트 목록 위반을 기록합니다.

워크플로우, 대시보드, 네트워크 맵을 이용해 시스템 전반의 규정준수 활동을 모니터링하여 개별 호스트가 화이트 목록을 언제 어떻게 위반하는지 확인할 수 있습니다. 그러한 위반에 대해 교정과 알림으로 자동 응답할 수도 있습니다.

예: **HTTP**를 웹 서버에 제한

보안 정책이 웹 서버만 HTTP를 실행하도록 규정합니다. 웹 팜을 제외한 전체 네트워크를 평가하는 화이트 목록을 생성하여 어떤 호스트가 HTTP를 실행 중인지 확인합니다.

네트워크 맵과 대시보그를 사용하여, 네트워크 규정준수 상태를 한 눈에 확인할 수 있습니다. 조직 내의 어떤 호스트가 정책을 위반한 상태로 HTTP를 실행 중인지 단 몇 초 만에 정확히 확인하고, 적절한 조치를 취할 수 있습니다.

그런 다음 상관관계 기능을 사용하면 웹 팜에 없는 호스트가 HTTP 실행을 시작할 때마다 사용자에게 알림이 전송되도록 시스템을 구성할 수 있습니다.

관련 항목

상관관계 정책 설정, 2585 페이지

규정준수 화이트리스트 대상 네트워크

대상 네트워크는 규정준수에 대해 평가할 호스트를 지정합니다. 화이트리스트는 하나 이상의 대상 네트워크를 가질 수 있으며, 대상 기준을 충족하는 호스트를 평가합니다.

처음에는 대상 네트워크를 IP 주소 또는 범위로 제한합니다. 다중 도메인 구축의 경우, 최초 제한에는 도메인도 포함됩니다.

시스템이 제공하는 기본 화이트리스트는 모니터링되는 모든 호스트, 즉 0.0.0.0/0과 ::/0을 지정합니다. 다중 도메인 구축의 경우, 기본 화이트리스트는 전역 도메인으로 제한됩니다. 그리고 전역 도메인에서만 사용할 수 있습니다.

대상 네트워크나 호스트를 수정하여 호스트가 화이트리스트의 유효한 대상이 되지 않게 하면 호스트는 해당 리스트로 평가되지 않으며 규정준수 또는 미준수로 간주되지 않습니다.

대상 네트워크 조사 및 개선

대상 네트워크를 화이트리스트를 추가하는 경우, 시스템은 규정준수 호스트를 특성화할 수 있도록 네트워크 맵을 조사하라는 프롬프트를 표시합니다. 조사를 통해 조사 대상인 호스트를 나타내는 대상이 화이트리스트에 추가됩니다.

서브넷 또는 개별 호스트를 조사할 수 있습니다. 다중 도메인 구축의 경우에는 전체 도메인을 조사하거나 여러 도메인에 걸쳐 조사를 진행할 수 있습니다. 상위 도메인을 조사하면 시스템은 해당 도메인의 하위 요소를 조사합니다.

추가한 대상 외에, 조사에서 탐지된 각 운영체제에 대해 하나의 호스트 프로파일과 화이트리스트도 채웁니다. 이러한 호스트 프로파일은 해당 운영체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

대상 네트워크 조사가 끝나면(또는 조사를 건너뛰면), 대상을 개선합니다. 호스트를 IP 주소를 기준으로 제외하거나, 대상 네트워크를 호스트 속성이나 VLAN을 기준으로 제한할 수 있습니다.

규정준수 화이트리스트를 이용한 도메인 지정

다중 도메인 구축의 경우, 도메인과 대상 네트워크는 밀접하게 연결됩니다.

- 리프 도메인 관리자는 자신의 리프 도메인 내에서 호스트를 평가하는 화이트리스트를 만들 수 있습니다.
- 상위 도메인 관리자가 도메인에 걸쳐 호스트를 평가하는 화이트리스트를 생성할 수 있습니다. 동일한 화이트 목록에서 다른 도메인에 있는 다른 서브넷을 대상으로 지정할 수 있습니다.

자신이 Global(전역) 도메인 관리자이며, 전체 구축의 웹 서버에 같은 규정준수 기준을 적용하는 상황을 고려해보십시오. 규정준수 기준을 정의하는 화이트리스트를 전역 도메인에서 생성합니다. 그런 다음 각 리프 도메인에 있는 웹 서버의 IP 공간(또는 개별 IP 주소)을 지정하는 대상 네트워크를 이용하여 화이트리스트를 제한합니다.

참고 리프 도메인의 IP 주소와 범위를 대상으로 지정할 수도 있지만, 상위 도메인을 이용해 대상 네트워크를 제한할 수도 있습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

규정준수 화이트 리스트 호스트 프로필

규정준수 화이트 리스트에서 호스트 프로파일은 대상 호스트에서 실행할 수 있는 운영체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다. 규정준수 화이트 리스트에서는 3가지 유형의 호스트 프로파일을 사용할 수 있습니다. 각 유형은 규정준수 편집기에서 다르게 표시됩니다.

표 ***253:*** 규정준수 화이트 리스트 호스트 프로파일 유형

호스트 프로파일 유형	모양	설명
전역글로벌	모든 운영체제	운영체제에 상관없이 대상 호스트에서 실행할 수 있는 요소를 지정
운영체제 한정	일반 텍스트로 나열됨	특정 운영체제의 대상 호스트에서 실행할 수 있는 요소를 지정
공유됨	기울임꼴로 나열	여러 화이트 리스트에서 사용할 수 있는 운영체제 기준을 지정

운영 체제별 호스트 프로파일

규정준수 화이트 목록에서 운영체제 한정 호스트 프로파일은 네트워크에서 실행할 수 있는 운영체제뿐만 아니라, 해당 운영체제에서 실행할 수 있는 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 나타냅니다.

예를 들어 규정준수 호스트가 특정 버전의 Microsoft Windows를 실행하도록 요구할 수 있습니다. 다른 예로, SSH가 포트 22의 Linux 호스트에서 실행되도록 허용하고 SSH 클라이언트의 벤더와 버전을 추가로 제한할 수 있습니다.

네트워크에서 허용하려는 각 운영체제에 대한 하나의 호스트 프로파일을 생성합니다. 네트워크에서 특정 운영체제를 허용하지 않으려면, 해당 운영체제에 대한 호스트 프로파일을 생성하지 마십시오. 예를 들어 네트워크의 모든 호스트가 Windows를 실행하게 하려면, 화이트 목록에 해당 운영체제에 대한 호스트 프로파일만 포함되도록 구성하십시오.

참고 확인되지 않은 호스트는 확인될 때까지 모든 화이트 목록을 준수하는 상태로 유지됩니다. 그러나 알 수 없는 호스트에 대한 화이트 목록 호스트 프로파일을 생성할 수 있습니다. *Unidentified(*미확인*)* 호스트는 시스템이 해당 호스트의 운영체제를 식별하기 위한 충분한 정보를 아직 수집하지 못한 호스트입니다. *Unknown(*알 수 없는*)* 호스트는 운영체제가 알려진 핑거프린트와 일치하지 않는 호스트입니다.

공유 호스트 프로파일

규정준수 화이트리스트에서 공유 호스트 프로파일은 특정 운영체제에 연결되지만, 각 공유 호스트 프로파일을 두 개 이상의 화이트리스트에서 사용할 수 있습니다.

예를 들어, 전 세계에 지사가 있고 각 위치에 별도의 화이트리스트를 적용하지만, Apple Mac OS X를 실행하는 모든 호스트에 동일한 프로파일을 사용하려면 해당 운영체제에 대한 공유 프로파일을 생성하고 이를 모든 화이트리스트에 사용할 수 있습니다.

기본 화이트리스트는 내장형 호스트 프로파일이라고 하는 특수 카테고리의 공유 호스트 프로파일을 사용합니다. 이러한 프로파일은 내장된 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜 및 클라이언트를 사용합니다. 규정준수 화이트리스트 편집기에서 시스템은 이러한 프로파일에 내장 호스트 프로파일 아이콘을 표시합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 공유 호스트 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 공유 호스트 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 공유 호스트 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경 사항은 이를 사용하는 모든 화이트리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

화이트 위반 트리거

호스트의 화이트리스트 규정준수는 시스템이 다음 작업을 할 때 변경할 수 있습니다.

- 호스트 운영체제의 변경 사항을 탐지한 경우
- 호스트의 운영체제 또는 호스트에 있는 애플리케이션 프로토콜의 ID 충돌을 탐지한 경우
- 호스트에서 새 TCP 서버 포트(예: SMTP 또는 웹 서버에서 사용된 포트)가 활성화되었거나, 호스트에서 새 UDP 서버가 실행 중인 것을 탐지한 경우
- 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버의 변경 사항을 탐지한 경우(예: 업그레이드로 인한 버전 변경)
- 호스트를 실행하는 새 클라이언트나 웹 애플리케이션을 탐지한 경우

- 비활성 상태인 클라이언트나 웹 애플리케이션을 데이터베이스에서 삭제하는 경우
- 새 네트워크 또는 전송 프로토콜과 통신하는 호스트를 탐지한 경우
- 새 탈옥 모바일 디바이스를 탐지한 경우
- 시스템에서 종료되거나 시간 초과된 TCP 또는 UDP 포트를 탐지한 경우

이와 더불어, 호스트 입력 기능 또는 호스트 프로파일을 사용하여 호스트의 규정준수 변경을 트리거할 수 있습니다.

- 호스트에 클라이언트, 프로토콜 또는 서버 추가
- 호스트에서 클라이언트, 프로토콜 또는 서버 삭제
- 호스트의 운영체제 정의 설정
- 해당 호스트가 더 이상 유효 대상이 되지 않도록 호스트의 호스트 속성 변경

참고 이벤트 과잉을 방지하기 위해, 시스템은 최초 평가 시에는 규정 미준수 호스트에 대한 화이트리스트 이벤트를 생성하지 않으며, 활성 화이트리스트 또는 공유 호스트 프로파일을 수정해도 호스트는 규정 미준수가 되지 않습니다. 그러나 위반 사항은 계속 기록됩니다. 모든 규정 미준수 대상에 대한 화이트리스트 이벤트를 생성하려면 검색 데이터를 비웁니다. 네트워크 자산을 재검색하면 화이트리스트 이벤트가 트리거될 수도 있습니다.

운영체제 규정준수

네트워크에서 Microsoft Windows 호스트만 허용하도록 화이트리스트를 지정할 경우, 시스템에서는 Mac OS X를 실행하는 호스트를 탐지하며 화이트리스트 이벤트를 생성합니다. 또한 화이트리스트와 연결된 호스트 속성은 해당 호스트에 대해 Compliant(규정준수)에서 Non-Compliant(규정 미준수)로 변경됩니다.

이 예시에 나온 호스트의 상태가 규정준수로 돌아가려면 다음 중 하나를 수행해야 합니다.

- Mac OS X 운영체제를 허용하도록 화이트리스트 편집
- 호스트의 운영체제 정의를 Microsoft Windows로 수동으로 변경
- 운영체제가 Microsoft Windows로 다시 변경된 사실을 시스템에서 탐지함

네트워크 맵에서 규정 미준수 자산 삭제

화이트리스트에서 FTP 사용이 허용되지 않고 사용자가 애플리케이션 프로토콜 네트워크 맵 또는 이벤트 보기에서 FTP를 삭제할 경우, FTP를 실행하는 호스트는 규정준수를 상태가 됩니다. 그러나 애플리케이션 프로토콜이 다시 탐지될 경우, 시스템에서는 화이트리스트 이벤트를 생성하며 호스트는 규정준수 위반 상태가 됩니다.

완전한 정보에서만 트리거

화이트리스트가 포트 21의 TCP FTP 트래픽만 허용하며 시스템이 포트 21/TCP에서의 불확정 활동을 탐지하면 화이트리스트는 트리거하지 않습니다. 화이트리스트는 시스템이 트래픽을 FTP가 아닌 다른 무언가로 식별하거나, 사용자가 호스트 입력 기능을 이용하여 트래픽을 비 FTP 트래픽으로 지정하는 경우에만 트리거합니다. 시스템은 부분적인 정보만 있는 위반은 기록하지 않습니다.

컴플라이언스 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자

규정준수 화이트 목록 생성

규정준수 화이트 목록을 생성하는 경우, 시스템은 최초 대상을 생성하고 규정준수 호스트 속성을 설명할 수 있도록 네트워크를 조사하라는 프롬프트를 표시합니다.

프로시저

단계 **1** 화이트리스트을(를) 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 새로 만들기화이트리스트를 클릭합니다.

단계 **3** 선택적으로, 최초 대상 네트워크의 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다. 다중 도메인 구축인 경우에는 대상 네트워크가 상주하는 **Domain(**도메인**)**을 선택합니다.

팁 전체 모니터링된 네트워크를 조사하려면, 기본값 0.0.0.0/0 및 ::/0을 사용합니다.

참고 대상 네트워크의 도메인은 선택이 끝나면 변경할 수 없습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 대상 네트워크 추가:

- Add(추가) - 조사하지 않고 대상 네트워크를 추가하려면 **Add(**추가**)**를 클릭합니다.
- Add and Survey Network(추가 및 네트워크 조사) - 대상 네트워크를 추가하고 조사하려면 **Add and Survey Network(**네트워크 추가 및 조사**)**를 클릭합니다.
- Skip(건너뛰기) - 네트워크를 조사하지 않고 화이트 목록을 생성하려면 **Skip(**건너뛰기**)**을 클릭합니다.

단계 **5** 선택적으로, 화이트 목록의 새 **Name(**이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **6** 선택적으로, 네트워크에서 탈옥 모바일 디바이스를 허용합니다. 이 옵션을 비활성화하면 탈옥한 디바이스가 화이트 목록 위반을 생성할 수 있습니다.

단계 **7** 규정준수 화이트 목록에 대한 대상 네트워크 설정, 2573 페이지에 설명된 대로 하나 이상의 **Target Network(**대상 네트워크**)**를 화이트 목록에 추가합니다.

단계 **8** **Allowed Host Profiles(**허용되는 호스트 프로파일**)**을 이용해 규정준수 호스트의 특성 설명:

- Global Host Profile(전역 호스트 프로파일) - 화이트 목록의 전역 호스트 프로파일을 편집하려면 **Any Operating System(**모든 운영체제**)**을 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Edit Surveyed Profiles(조사한 프로파일 편집) - 네트워크 조사로 생성한 기존 운영체제 한정 호스트 프로파일을 편집하려면, 해당 프로파일의 이름을 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Create New Profiles(새 프로파일 생성) - 이 화이트 목록에 대한 새로운 운영체제 한정 호스트 프로파일을 생성하려면, **Allowed Host Profiles(**허용되는 호스트 프로파일**)** 옆에 있는 추가( )을 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Add Shared Host Profile(공유 호스트 프로파일 추가) - 기존 공유 호스트 프로파일을 화이트 목록에 추가하려면, **Add Shared Host Profile(**공유 호스트 프로파일 추가**)**을 클릭하고 추가할 공유 호스트 프로파일을 선택한 다음 **OK(**확인**)**를 클릭합니다. 공유 호스트 프로파일은 기울임꼴로 표시됩니다.

단계 **9** **Save(**저장**)**화이트리스트를 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 설정, 2585 페이지에 설명된 대로 활성 상관관계 정책에 화이트 목록을 추가합니다. 시스템은 화이트 목록 평가와 위반 생성을 즉시 시작합니다.

관련 항목

규정준수 화이트리스트 대상 네트워크, 2567 페이지
선택한 호스트를 기반으로 규정준수 화이트리스트 생성, 3053 페이지
Firepower System IP 주소 규칙, 19 페이지

규정준수 화이트 목록에 대한 대상 네트워크 설정

대상 네트워크를 추가할 때 해당 네트워크를 조사해 규정준수 호스트의 특성을 설명할 수 있습니다. 조사에서 탐지된 각 운영체제에 대해 하나의 호스트 프로파일과 화이트 목록을 채웁니다. 이러한 호스트 프로파일은 해당 운영 체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

프로시저

단계 **1** 규정준수 화이트 목록 편집기에서 **Add Target Network(**대상 네트워크 추가**)**를 클릭합니다.

단계 **2** 대상 네트워크의 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다.

단계 **3** 다중 도메인 구축인 경우에는 대상 네트워크가 상주하는 **Domain(**도메인**)**을 선택합니다.

참고 대상 네트워크의 도메인은 선택이 끝나면 변경할 수 없습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 대상 네트워크 추가:

- Add(추가) - 조사하지 않고 대상 네트워크를 추가하려면 **Add(**추가**)**를 클릭합니다.
- Add and Survey Network(추가 및 네트워크 조사) - 대상 네트워크를 추가하고 조사하려면 **Add and Survey Network(**네트워크 추가 및 조사**)**를 클릭합니다.

단계 **5** 선택적으로, 추가 설정할 새 대상을 클릭합니다.

- Name(이름) - 새 **Name(**이름**)**을 입력합니다.
- Add Networks(네트워크 추가) - 추가 호스트를 대상으로 지정하려면, 추가(+)을 클릭하고 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다. 네트워크를 화이트 목록 규정준수에서 제외하려면, **Exclude(**제외**)**를 선택합니다.
- Add Host Attributes(호스트 속성 추가) - 호스트를 특정 호스트 속성과 함께 대상으로 지정하려면, 추가(+)을 클릭하고 **Attribute(**속성**)**와 그 **Value(**값**)**를 지정합니다.
- Add VLANs(VLAN 추가) - VLAN을 대상으로 지정하려면 추가(+)을 클릭하고 (802.1q VLAN에 대한) VLAN 번호를 입력합니다.
- Delete(삭제) — 대상 제한을 제거하려면 삭제(🗑)을 클릭합니다.

단계 **6** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**화이트리스트를 클릭합니다.

관련 항목

규정준수 화이트리스트 대상 네트워크, 2567 페이지
Firepower System IP 주소 규칙, 19 페이지

화이트 리스트 호스트 프로필 빌드

호스트 프로파일은 화이트 리스트의 규정준수 기준, 즉 대상 호스트에서 실행할 수 있는 운영체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다.

모든 화이트 리스트에는 운영체제에 구속되지 않는 전역 호스트 프로파일이 있습니다. 예를 들어 여러 개의 Microsoft Windows 및 Linux 호스트 프로파일을 수정하는 대신 Mozilla Firefox를 허용하려면, Firefox가 탐지되는 운영체제에 상관없이 Firefox를 허용하도록 전역 호스트 프로파일을 구성할 수 있습니다.

개별 화이트 리스트에 국한되거나 여러 화이트 리스트가 공유하는 운영체제 한정 호스트 프로파일을 설정할 수도 있습니다.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경사항은 이를 사용하는 모든 화이트리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

시작하기 전에

- 규정준수 화이트 목록 편집, 2578 페이지에 설명된 대로 화이트내에서 호스트 프로파일을 생성 또는 편집하거나, 공유 호스트 프로파일 관리, 2580 페이지에 설명된 대로 공유 호스트 프로파일을 생성 또는 편집합니다.

프로시저

단계 **1** 규정준수 화이트 리스트 호스트 프로파일 편집기에서 호스트 프로파일을 설정합니다.

- Name(이름) - **Name(**이름**)**을 입력합니다.
- Operating System(운영체제) - 호스트 프로파일을 특정 운영체제에 제한하려면, **OS Vendor(**운영체제 벤더**)**, **OS Name(**운영체제 이름**)**, **Version(**버전**)** 드롭다운 목록을 이용합니다. 운영체제 종류에 상관없이 운영체제를 실행하는 모든 호스트에 적용하는 것이 목표이므로, 전역 호스트 프로파일을 제한할 수는 없습니다.
- Application Protocol(애플리케이션 프로토콜) - 애플리케이션 프로토콜을 허용하려면 추가 아이콘(추가(+))을 클릭하고 규정준수 화이트리스트에 애플리케이션 프로토콜 추가, 2575 페이지에 설명된 대로 진행합니다.
- Client(클라이언트) - 클라이언트를 허용하려면 아이콘(추가(+))을 클릭하고 규정 준수 화이트 목록에 클라이언트 추가, 2576 페이지에 설명된 대로 진행합니다.
- Web Application(웹 애플리케이션) - 웹 애플리케이션을 허용하려면 추가 아이콘(추가(+))을 클릭하고 규정준수 화이트리스트에 웹 애플리케이션 추가, 2576 페이지에 설명된 대로 진행합니다.

- Protocol(프로토콜) - 프로토콜을 허용하려면 아이콘(추가( ))을 클릭하고 규정준수 화이트리스트에 프로토콜 추가, 2577 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 이전에 허용한 항목을 허용하지 않으려면 아이콘(삭제( ))을 클릭합니다.
- Edit Properties(속성 편집) - 허용되는 애플리케이션 프로토콜, 클라이언트 또는 프로토콜의 속성을 편집하려면 해당 요소의 이름을 클릭합니다. 변경사항은 해당 요소를 사용하는 모든 호스트 프로파일에 반영됩니다.

팁 적절한 **Allow all...(**모두 허용**...)** 확인란을 선택해 이 프로파일과 일치하는 호스트에 대한 모든 애플리케이션 프로토콜, 클라이언트 또는 웹 애플리케이션을 허용합니다.

단계 **2** 마지막으로 저장한 이후 적용된 모든 변경사항을 즉시 구현하려면 **Save(**저장**)**화이트리스트(공유 호스트 프로파일을 편집하는 경우에는 **Save All Profiles(**모든 프로파일 저장**))**를 클릭합니다.

규정준수 화이트리스트에 애플리케이션 프로토콜 추가

화이트 리스트 호스트 프로파일을 사용하면 애플리케이션 프로토콜을 전역적으로, 또는 특정 운영 체제에서만 허용할 수 있습니다. 선택적으로, 애플리케이션 프로토콜을 포트, 벤더 또는 버전으로 제한할 수도 있습니다. 예를 들어 OpenSSH 특정 버전이 포트 22/TCP의 Linux 호스트에서 실행되도록 허용할 수 있습니다.

프로시저

단계 **1** 컴플라이언스 화이트 리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Application Protocols(**허용되는 애플리케이션 프로토콜**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Application Protocols(**전역적으로 허용되는 애플리케이션 프로토콜**))** 옆에 있는 추가( )를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 애플리케이션 프로토콜이 목록에 있다면 해당 프로토콜을 선택합니다. 웹 인터페이스는 화이트 목록이 허용해 왔거나 현재 허용하는 애플리케이션 프로토콜을 나열합니다.
- 목록에 없는 애플리케이션 프로토콜을 허용하려면, **<New Application Protocol>**을 선택하고 **OK(**확인**)**를 클릭하여 애플리케이션 프로토콜 편집기를 표시합니다. 허용할 애플리케이션 프로토콜 **Type(**유형**)**과 **Protocol(**프로토콜**)**을 선택합니다. 선택적으로, 애플리케이션 프로토콜을 포트, **Vendor(**벤더**)**, **Version(**버전**)**으로 제한합니다.

  참고 애플리케이션의 테이블 보기에 표시되는 벤더와 버전을 정확하게 입력해야 합니다. 벤더 또는 버전을 지정하지 않을 경우, 화이트 목록에서는 유형 및 프로토콜이 매칭될 때까지 모든 벤더와 버전을 허용합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**화이트리스트를 클릭합니다.

규정 준수 화이트 목록에 클라이언트 추가

화이트 목록 호스트 프로파일을 사용하면 클라이언트를 전역적으로 또는 특정 운영체제에서만 허용할 수 있습니다. 선택적으로, 클라이어트가 특정 버전이길 요청할 수 있습니다. 예를 들어 Microsoft Internet Explorer 10에서만 Microsoft Windows 호스트를 실행하도록 허용할 수 있습니다.

프로시저

단계 **1** 컴플라이언스 화이트 리스트 호스트 프로파일을 생성하거나 수정할 경우 **Allowed Clients(**허용되는 클라이언트**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Clients(**전역적으로 허용되는 클라이언트**)**) 옆에 있는 추가(+)를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 클라이언트가 목록에 있다면 해당 클라이언트를 선택합니다. 웹 인터페이스는 화이트이 허용해 왔거나 현재 허용하는 클라이언트를 나열합니다.
- 목록에 없는 클라이언트를 허용하려면 **<New Client>**를 선택하고 **OK(**확인**)**를 클릭해 클라이언트 편집기를 표시합니다. 드롭다운 목록에서 허용할 **Client(**클라이언트**)**를 선택하고, 원한다면 클라이언트를 허용되는 **Version(**버전**)**에 제한합니다.

  참고 클라이언트의 테이블 보기에 표시되는 버전을 정확하게 입력해야 합니다. 버전을 지정하지 않으면 모든 버전이 허용됩니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**화이트리스트를 클릭합니다.

규정준수 화이트리스트에 웹 애플리케이션 추가

화이트리스트 호스트 프로파일을 사용하면 웹 애플리케이션을 전역적으로, 또는 특정 운영체제만 허용할 수 있습니다.

프로시저

단계 **1** 규정준수 화이트리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Web Applications(**허용되는 웹 애플리케이션**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Web Applications(**전역적으로 허용되는 웹 애플리케이션**)**) 옆에 있는 추가(+)를 클릭합니다.

단계 **2** 허용할 웹 애플리케이션을 선택합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**화이트리스트를 클릭합니다.

규정준수 화이트리스트에 프로토콜 추가

화이트리스트 호스트 프로파일을 사용하면 프로토콜을 전역적으로, 또는 특정 운영체제에서만 허용할 수 있습니다. ARP, IP, TCP, UDP는 항상 모든 호스트에서 허용되며 해당 프로토콜은 허용하지 않을 수 없습니다.

프로시저

단계 **1** 화이트리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Protocols(**허용되는 프로토콜**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Protocols(**전역적으로 허용되는 프로토콜**)**) 옆에 있는 추가( )를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 프로토콜이 목록에 있다면 해당 프로토콜을 선택합니다. 웹 인터페이스는 허용되어 왔거나 화이트리스트가 현재 허용하는 프로토콜을 나열합니다.
- 목록에 없는 프로토콜을 허용하려면, **<New Protocol>**을 선택하고 **OK(**확인**)**를 클릭하여 프로토콜 편집기를 표시합니다. **Type(**유형**)** 드롭다운 목록에서 프로토콜 유형**(Network(**네트워크**)** 또는 **Transport(**전송**))**을 선택하고, 드롭다운 목록에서 **Protocol(**프로토콜**)**을 선택합니다.

  팁 **Other (manual entry)(**기타**(**수동 입력**)**를 선택하여 목록에 없는 프로토콜을 지정합니다. 네트워크 프로토콜의 경우, http://www.iana.org/assignments/ethernet-numbers/에 나열된 적합한 번호를 입력합니다. 전송 프로토콜의 경우, http://www.iana.org/assignments/protocol-numbers/에 나열된 적합한 번호를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**화이트리스트를 클릭합니다.

규정준수 화이트리스트 관리

화이트List(화이트리스트) 페이지를 이용하여 규정준수 화이트리스트와 공유 호스트 프로파일을 관리할 수 있습니다. 기본 화이트리스트는 권장 설정을 표시하며 내장형 호스트 프로파일이라고 하는 특수 범주의 공유 호스트 프로파일을 사용합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 규정준수 화이트리스트를 표시하며, 이러한 리스트는 수정할 수 있습니다. 상위 도메인의 선택된 화이트리스트도 표시되지만, 이는 편집할 수 없습니다. 하위 도메인에서 생성된 화이트리스트를 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다. 기본 화이트리스트는 전역 도메인에서만 사용할 수 있습니다.

프로시저

단계 **1** 화이트리스트을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 다음과 같이 규정준수 화이트리스트를 관리합니다.

- Create(생성) - 새 화이트리스트를 생성하려면 **New(**신규**)**화이트리스트를 클릭하고 규정준수 화이트 목록 생성, 2571 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 사용하지 않는 화이트리스트를 삭제하려면 삭제( )를 클릭하고 화이트리스트 삭제 여부를 확인합니다. 화이트리스트를 삭제하면 관련된 호스트 속성이 네트워크의 모든 호스트에서 제거됩니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- Edit(편집) - 기존 화이트리스트를 수정하려면 수정( )을 클릭하고 규정준수 화이트 목록 편집, 2578 페이지에 설명된 대로 진행합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- Shared Host Profiles(공유 호스트 프로파일) - 화이트리스트의 공유 호스트 프로파일을 관리하려면 **Edit Shared Profiles(**공유 프로파일 편집**)**를 클릭하고 공유 호스트 프로파일 관리, 2580 페이지에 설명된 대로 진행합니다.

규정준수 화이트 목록 편집

활성 상관관계 정책에 포함된 규정준수 화이트 목록을 수정하고 저장하는 경우, 시스템은 화이트 목록의 대상 네트워크에 있는 호스트의 규정준수 여부를 즉시 다시 평가합니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수 또는 규정 미준수로 바뀔 수 있으나, 시스템은 어떤 화이트 목록 이벤트도 생성하지 않습니다.

프로시저

단계 **1** 화이트리스트을(를) 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 수정할 화이트 목록 옆의 수정( )를 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 규정준수 화이트 목록 편집:

- Name and Description(이름 및 설명) - 이름이나 설명을 변경하려면 왼쪽 패널에서 화이트 목록 이름을 클릭해 기본 화이트 목록 정보를 표시한 다음 새 정보를 입력합니다.
- Allow Jailbroken Devices(탈옥 디바이스 허용) - 네트워크에서 탈옥 모바일 디바이스를 허용하려면, 왼쪽 패널에서 화이트 목록 이름을 클릭해 기본 화이트 목록 정보를 표시하고 **Allow Jailbroken Mobile Devices(**탈옥 모바일 디바이스 허용**)**를 활성화합니다. 이 옵션을 비활성화하면 탈옥한 디바이스가 화이트 목록 위반을 생성할 수 있습니다.
- Add Allowed Host Profile(허용되는 호스트 프로파일 추가) - 화이트 목록에 대한 운영체제 한정 호스트 프로파일을 생성하려면, Allowed Host Profiles(허용되는 호스트 프로파일) 옆에 있는 추가( )을 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Add Shared Host Profile(공유 호스트 프로파일 추가) - 기존 공유 호스트 프로파일을 화이트 목록에 추가하려면, **Add Shared Host Profile(**공유 호스트 프로파일 추가**)**을 클릭하고 추가할 공유 호스트 프로파일을 선택한 다음 **OK(**확인**)**를 클릭합니다. 공유 호스트 프로파일은 기울임꼴로 표시됩니다.
- Add Target Network(대상 네트워크 추가) - 호스트 조사 없이 새 대상 네트워크를 추가하려면, Target Networks(대상 네트워크) 옆에 있는 추가( )을 클릭하고 규정준수 화이트 목록에 대한 대상 네트워크 설정, 2573 페이지에 설명된 대로 진행합니다.
- Delete Host Profile(호스트 프로파일 삭제) - 공유 또는 운영체제 한정 호스트 프로파일을 화이트 목록에서 삭제하려면, 호스트 프로파일 옆에 있는 삭제( )을 클릭하고 선택을 확인합니다. 공유 호스트 프로파일을 삭제하면 화이트 목록에서 해당 프로파일이 제거되지만, 이를 사용하는 다른 화이트 목록의 해당 프로파일은 삭제 또는 제거되지 않습니다. 화이트 목록의 전역 호스트 프로파일은 삭제할 수 없습니다.
- Delete Target Network(대상 네트워크 삭제) - 대상 네트워크를 화이트 목록에서 제거하려면, 네트워크 옆에 있는 삭제( )을 클릭하고 선택을 확인합니다.
- Edit Global Host Profile(전역 호스트 프로파일 편집) - 화이트 목록의 전역 호스트 프로파일을 편집하려면 **Any Operating System(**모든 운영체제**)**을 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Edit Other Host Profile(기타 호스트 프로파일 편집) - 공유 또는 운영체제 한정 호스트 프로파일을 편집하려면, 호스트 프로파일의 이름을 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Edit Target Network(대상 네트워크 편집) - 대상 네트워크를 편집하려면, 네트워크의 이름을 클릭하고 규정준수 화이트 목록에 대한 대상 네트워크 설정, 2573 페이지에 설명된 대로 진행합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**화이트리스트를 클릭합니다.

공유 호스트 프로파일 관리

규정준수 화이트리스트에서 공유 호스트 프로파일은 특정 운영체제에 연결되지만, 각 공유 호스트 프로파일을 두 개 이상의 화이트리스트에서 사용할 수 있습니다. 여러 개의 화이트리스트를 생성하지만 동일한 호스트 프로파일을 사용하여 화이트리스트 전반에 걸쳐 특정 운영체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로파일을 사용합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 공유 호스트 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 공유 호스트 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 공유 호스트 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경 사항은 이를 사용하는 모든 화이트리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 화이트리스트을(를) 클릭합니다.

단계 **2** **Edit Shared Profiles(**공유 프로파일 편집**)**를 클릭합니다.

단계 **3** 공유 호스트 프로파일 관리:

- Create Shared Host Profile(공유 호스트 프로파일 생성) - 호스트를 점검하지 않고 새 공유 호스트 프로파일을 생성하려면 Shared Host Profiles(공유 호스트 프로파일) 옆에 있는 추가( )를 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Create Shared Host Profile by Survey(조사를 통해 공유 호스트 프로파일 생성) - 네트워크를 조사해 여러 새 공유 호스트 프로파일을 생성하려면, **Add Target Network(**대상 네트워크 추가**)**를 클릭하고 규정준수 화이트 목록에 대한 대상 네트워크 설정, 2573 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 공유 호스트 프로파일을 삭제하려면 삭제( )를 클릭하고 선택을 확인합니다.
- Edit(편집) - 기존 공유 호스트 프로파일(내장된 공유 호스트 프로파일 포함)을 수정하려면, 이름을 클릭하고 화이트 리스트 호스트 프로필 빌드, 2574 페이지에 설명된 대로 진행합니다.
- Reset Built-In Host Profiles(내장 호스트 프로파일 재설정) - 모든 내장 호스트 프로파일을 공장 기본값으로 재설정하려면, **Built-in Host Profiles(**내장 호스트 프로파일**)**를 클릭하고 **Reset to Factory Defaults(**공장 기본값으로 재설정**)** 를 클릭한 다음 선택을 확인합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경사항을 즉시 구현하려면, **Save All Profiles(**모든 프로파일 저장**)**를 클릭합니다.

105 장

상관관계 정책

다음 주제에서는 상관관계 정책과 규칙을 설정하는 방법을 설명합니다.

- 상관관계 정책 및 규칙 소개, 2583 페이지
- 컴플라이언스 요구 사항 및 사전 요건, 2585 페이지
- 상관관계 정책 설정, 2585 페이지
- 상관관계 규칙 설정, 2587 페이지
- 상관관계 응답 그룹 설정, 2621 페이지

상관관계 정책 및 규칙 소개

상관관계 기능을 이용하면 상관관계 정책을 바탕으로 네트워크에 대한 위협에 실시간으로 반응할 수 있습니다.

상관관계 정책 위반은 네트워크 상의 활동이 활성 상관관계 정책 내의 상관관계 규칙이나 규정준수 화이트 목록을 트리거할 때 발생합니다.

상관관계 규칙

활성 상관관계 정책에서 상관관계 규칙이 트리거되면, 시스템은 상관관계 이벤트를 생성합니다. 상관관계 규칙은 다음 조건이 충족될 때 트리거됩니다.

- 시스템이 특정 유형의 이벤트(연결, 침입, 악성코드, 검색, 사용자 활동 등)를 생성합니다.
- 네트워크 트래픽이 자체 일반 프로파일에서 벗어납니다.

다음 방법으로 상관관계 규칙을 제한할 수 있습니다.

- 트리거링 이벤트와 관련된 호스트의 호스트 프로파일에서 정보를 사용하여 규칙을 제한하려면 호스트 프로파일 자격을 추가합니다.
- 규칙의 초기 기준이 충족된 후 시스템이 특정 연결 추적을 시작할 수 있도록 하려면 상관관계 규칙에 연결 추적기를 추가합니다. 그러면 추적된 연결이 추가 조건을 충족하는 경우에만 상관관계 이벤트가 생성됩니다.

- 특정 사용자 또는 사용자 그룹을 추적하려면 상관관계 규칙에 사용자 자격을 추가합니다. 예를 들어 특정 사용자의 트래픽 또는 특정 부서의 트래픽에 대해서만 트리거하도록 상관관계 규칙을 제한할 수 있습니다.
- 스누즈 기간을 추가합니다. 상관관계 규칙이 트리거될 때, 스누즈 기간 때문에 규칙이 지정된 간격 동안 다시 트리거되지 않을 수도 있습니다. 유휴 기간이 경과하면 규칙을 다시 트리거하고 새 스누즈 기간을 시작할 수 있습니다.
- 비활성 기간을 추가합니다. 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다.

구축을 허가받지 않고도 상관과계 규칙을 구성할 수 있지만, 허가받지 않은 구성 요소를 사용하는 규칙은 트리거되지 않습니다.

컴플라이언스 화이트 목록

규정준수 화이트 목록은 네트워크에서 허용할 운영체제, 애플리케이션(웹 및 클라이언트), 프로토콜을 지정합니다. 호스트가 활성 상관관계 정책에서 사용하는 화이트 목록을 위반하는 경우, 시스템은 화이트 목록 이벤트를 생성합니다.

상관관계 응답

상관관계 정책 위반에 대한 응답은 단순 알림 및 다양한 교정(호스트 스캔 등)을 포함합니다. 각 상관관계 규칙 또는 화이트 리스트를 단일 응답 또는 응답 그룹에 연결할 수 있습니다.

네트워크 트래픽이 여러 규칙 또는 화이트 리스트를 트리거하는 경우 각 규칙 및 화이트 리스트와 연결된 모든 응답이 시작됩니다.

상관관계 및 멀티 테넌시

다중 도메인 구축의 경우, 각 도메인 레벨에서 사용 가능한 규칙, 화이트 목록과 응답을 이용해 어떤 도메인 수준에서도 상관관계 정책을 생성할 수 있습니다. 상위 도메인 관리자는 도메인 내부 또는 도메인 간에서 상관관계를 수행할 수 있습니다.

- 도메인을 이용한 상관관계 규칙 제한은 해당 도메인의 하위 항목에서 보고하는 이벤트와 일치합니다.
- 상위 도메인 관리자는 도메인 간의 호스트를 평가하는 규정준수 화이트 목록을 생성할 수 있습니다. 동일한 화이트 목록에서 다른 도메인에 있는 다른 서브넷을 대상으로 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 일반적인 설정(IP 주소, VLAN 태그, 사용자 이름 등)으로 도메인 간 상관관계 규칙을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

관련 항목

컴플라이언스 화이트 목록 소개, 2565 페이지
Firepower Management Center 알림 응답, 2681 페이지
교정 소개, 2637 페이지

컴플라이언스 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자

상관관계 정책 설정

상관관계 규칙, 규정준수 화이트리스트, 알림 응답 및 교정을 사용하여 상관관계 정책을 만듭니다.

다중 도메인 구축의 경우에는, 각 도메인 레벨에서 사용 가능한 구성 요소 설정을 이용해 어떤 도메인 수준에서도 상관관계 정책을 생성할 수 있습니다.

각 상관관계 정책에, 그리고 해당 정책에서 사용하는 각 규칙과 화이트리스트에 우선순위를 할당할 수 있습니다. 규칙 및 화이트리스트 우선순위는 상관관계 정책 우선순위를 재정의합니다. 네트워크 트래픽이 상관관계 정책을 위반하는 경우, 그에 따른 상관관계 이벤트는 위반한 규칙이나 화이트리스트에 자체 우선순위가 없다면 정책 우선순위 값을 표시합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **3** **Policy Name(**정책 이름**)** 및 **Policy Desription(**정책 설명**)**을 입력합니다.

단계 **4** **Default Priority(**기본 우선순위**)** 드롭다운 목록에서 정책의 우선순위를 선택합니다. 규칙 우선순위만 사용하려면 **None(**없음**)**을 선택합니다.

단계 **5** **Add Rules(**규칙 추가**)**를 클릭하고, 정책에서 사용할 규칙 및 화이트리스트를 확인한 다음 **Add(**추가**)**를 클릭합니다.

단계 **6** 각 규칙 또는 화이트리스트의 **Priority(**우선순위**)** 목록에서 우선순위를 선택합니다.

- 1~5의 운선순위 값
- **None**
- **Default(**기본**)** - 정책의 기본 우선순위 사용

단계 **7** 규칙 및 화이트 리스트에 응답 추가, 2586 페이지에 설명된 대로 규칙 및 화이트리스트에 응답을 추가합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 슬라이더를 클릭하여 정책을 활성화합니다.

규칙 및 화이트 리스트에 응답 추가

각 상관관계 규칙 또는 화이트 리스트를 단일 응답 또는 응답 그룹에 연결할 수 있습니다. 네트워크 트래픽이 여러 규칙 또는 화이트 리스트를 트리거하는 경우 각 규칙 및 화이트 리스트와 연결된 모든 응답이 시작됩니다. 트래픽 프로파일 변경에 대한 응답으로 사용되는 경우에는 Nmap 치료가 시작되지 않습니다.

다중 도메인 구축에서는 현재 도메인 또는 상위 도메인에서 생성된 응답을 사용할 수 있습니다.

프로시저

단계 **1** 상관관계 정책 편집기에서 응답을 추가하려는 규칙 또는 화이트 리스트 옆에 있는 **Response(**응답**)**를 클릭합니다.

단계 **2** Unassigned Responses(미할당 응답) 아래에서 규칙 또는 화이트 리스트가 트리거될 때 시작할 응답을 선택하고 위로 화살표(^)를 클릭합니다.

단계 **3** **Update(**업데이트**)**를 클릭합니다.

관련 항목

Firepower Management Center 알림 응답, 2681 페이지
교정 소개, 2637 페이지

상관관계 정책 관리

활성 상관관계 정책에 적용된 변경사항은 즉시 적용됩니다.

상관관계 정책을 활성화하면, 시스템은 즉시 이벤트를 처리하고 응답을 트리거합니다. 시스템은 최초, 활성화 이후 평가에서는 규정 미준수 호스트에 대한 화이트리스트 이벤트를 생성하지 않습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 상관관계 정책을 표시하며, 이러한 정책은 편집할 수 있습니다. 상위 도메인의 선택된 상관관계 정책도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 상관관계 정책을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택합니다.

단계 **2** 상관관계 정책 관리:

- Activate(활성화) 또는 Deactivate(비활성화) - 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 생성 - **Create Policy(**정책 생성**)**를 클릭합니다(상관관계 정책 설정, 2585 페이지 참조).
- 편집 - 수정( )을(를) 클릭합니다. 상관관계 정책 설정, 2585 페이지의 내용을 참조하십시오. 보기( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - 삭제( )을(를) 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

상관관계 규칙 설정

단순한 상관관계 규칙은 특정 유형의 이벤트 발생만 요구합니다. 그 이상의 상세 조건은 입력하지 않아도 됩니다. 예를 들어 트래픽 프로파일 변경 기반의 상관관계 규칙에는 조건이 전혀 필요하지 않습니다. 여러 조건이 적용되며 제한이 추가된 복잡한 상관관계 규칙을 만들 수도 있습니다.

상관관계 규칙 트리거 기준, 호스트 프로파일 자격, 사용자 자격 또는 연결 추적기를 생성할 때 구문은 각기 다르지만 원리는 동일합니다.

참고 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 이벤트와 일치하는 상위 도메인을 기준으로 상관관계 규칙을 제한합니다.

시작하기 전에

- 구축이 상관관계 이벤트를 트리거하는 데 사용할 정보 유형을 수집하고 있는지 확인합니다. 예를 들어 개별 연결 또는 연결 요약 이벤트에 사용 가능한 정보는 탐지 방법, 로깅 방법, 이벤트 유형 등 여러 요인에 따라 달라집니다. 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Rule Management(**규칙 관리**)**을 클릭합니다.

단계 **2** **Create Rule(**규칙 생성**)**을 클릭합니다.

단계 **3** **Rule Name(**규칙 이름**)** 및 **Rule Description(**규칙 설명**)**을 입력합니다.

단계 **4** 원한다면 규칙에 대한 **Rule Group(**규칙 그룹**)**을 선택합니다.

단계 **5** 기본 이벤트 유형을 선택하고, 원한다면 상관관계 규칙에 대한 추가 트리거 기준을 지정합니다. 다음 기본 이벤트 유형을 선택할 수 있습니다.

- 침입 이벤트 발생 - 침입 이벤트 트리거 기준 구문, 2589 페이지 섹션을 참조하십시오.
- 악성 코드 이벤트 발생 - 악성코드 이벤트 트리거 기준 구문, 2592 페이지 섹션을 참조하십시오.
- 검색 이벤트 발생 - 검색 이벤트 트리거 기준 구문, 2594 페이지 섹션을 참조하십시오.
- 사용자 활동 탐지됨 - 사용자 활동 이벤트 트리거 기준 구문, 2597 페이지 섹션을 참조하십시오.
- 호스트 입력 이벤트 발생 - 호스트 입력 이벤트 트리거 기준 구문, 2598 페이지 섹션을 참조하십시오.
- 연결 이벤트 발생 - 연결 이벤트 트리거 기준 구문, 2599 페이지 섹션을 참조하십시오.
- 트래픽 프로파일 변경사항 - 트래픽 프로파일 변경 구문, 2603 페이지 섹션을 참조하십시오.

단계 **6** 선택적으로, 다음 중 하나 또는 전부를 추가해 상관관계 규칙을 추가로 제한합니다.

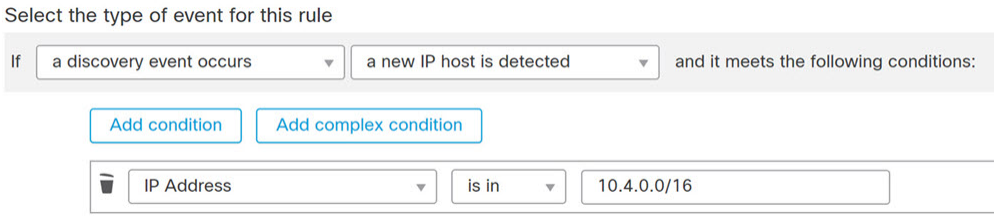
- 호스트 프로파일 자격 - **Add Host Profile Qualification(**호스트 프로파일 자격 추가**)**을 클릭합니다(상관관계 호스트 프로파일 자격 구문, 2605 페이지 참조).
- 연결 추적기 - **Add Connection Tracker(**연결 추적기 추가**)**를 클릭합니다(연결 추적기, 2608 페이지 참조).
- 사용자 자격 - **Add User Qualification(**사용자 자격 추가**)**을 클릭합니다(사용자 자격 구문, 2607 페이지 참조).
- 스누즈 기간 - Rule Options(규칙 옵션)에서 **Snooze(**스누즈**)** 텍스트 필드와 드롭다운 목록을 이용해 시스템에 규칙 트리거 후 상관관계 규칙을 다시 트리거할 때까지 기다려야 하는 기간을 정의합니다.
- 비활성 기간 - Rule Options(규칙 옵션)에서 **Add Inactive Period(**비활성 기간 추가**)**를 클릭합니다. 텍스트 필드와 드롭다운 목록을 사용하여, 시스템이 상관관계 규칙에 대한 네트워크 트래픽 평가를 억제하도록 할 시기와 빈도를 지정합니다.

팁 유휴 기간을 제거하려면 간격을 **0**으로 지정합니다(초, 분 또는 시간).

단계 **7** **Save Rule(**규칙 저장**)**을 클릭합니다.

단순 상관관계 규칙 예시

다음의 단순 상관관계 규칙은 특정 서브넷에서 새 호스트가 탐지되면 트리거됩니다. 카테고리가 IP 주소를 나타낼 때 **is in** 또는 **is not in**을 연산자로 선택하면, IP 주소가 CIDR 등의 특수 표기법으로 표현된 IP 주소 블록에서 *is in* 상태인지 *is not in* 상태인지를 지정할 수 있습니다.



다음에 수행할 작업

- 상관관계 정책 설정, 2585 페이지에 설명된 대로 상관관계 정책의 규칙을 사용합니다.

관련 항목

상관관계 규칙 관리, 2620 페이지
상관관계 규칙 작성 원리, 2617 페이지
스누즈 및 비활성 기간, 2617 페이지
NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지

침입 이벤트 트리거 기준 구문

다음 표에서는 기본 이벤트로 침입 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***254:*** 침입 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 컨트롤 정책을 하나 이상 선택합니다.
액세스 제어 규칙 이름	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다.
애플리케이션 프로토콜	침입 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
분류	하나 이상의 분류를 선택합니다.
Client(클라이언트)	침입 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	침입 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
목적지 IP, 소스 IP, 소스 IP 및 목적지 IP 모두, 또는 소스 IP 나 목적지 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
대상 포트/ICMP 코드 또는 소스 포트/ICMP 유형	소스 트래픽의 포트 번호나 ICMP 코드 또는 대상 트래픽의 포트 번호나 ICMP 유형을 입력합니다.
디바이스	이벤트를 생성했을 가능성이 있는 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
Egress Interface(이그레스 인터페이스) 또는 Ingress Interface(인그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Egress Security Zone(이그레스 보안 영역) 또는 Ingress Security Zone(인그레스 보안 영역)	보안 영역을 하나 이상 선택합니다.
생성자 ID	전처리기를 하나 이상 선택합니다.
영향 플래그	침입 이벤트에 할당된 영향 레벨을 선택합니다. NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.
인라인 결과	침입 정책 위반에 따라 시스템이 패킷을 삭제했는지 또는 삭제할 가능성이 있는지를 선택합니다. 시스템은 인라인, 스위치드 또는 라우티드 구축의 패킷을 삭제할 수 있습니다. 침입 규칙 상태나 침입 정책의 삭제 작업에 상관없이, 수동 구축(인라인 설정이 탭 모드에 있는 경우 포함)에서는 패킷을 삭제하지 않습니다.
침입 정책	침입 이벤트를 생성한 침입 정책을 하나 이상 선택합니다.
IOC 태그	침입 이벤트의 결과로 침해 지표 태그가 설정되었는지를 선택합니다.
Priority(우선순위)	규칙 우선순위를 선택합니다. 규칙 기반 침입 이벤트의 경우 우선순위는 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 기타 침입 이벤트의 경우, 우선순위는 디코더 또는 전처리기에 의해 결정됩니다.

다음을 지정할 경우...	연산자를 선택하고...
프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
규칙 메시지	규칙 메시지의 전체 또는 일부를 입력합니다.
규칙 SID	단일 Snort ID(SID) 또는 쉼표로 구분된 여러 SID를 입력합니다. 연산자로 **is in** 또는 **is not in**을 선택하는 경우 다중 선택 팝업 윈도우를 사용할 수 없습니다. 쉼표로 구분된 SID 목록을 입력해야 합니다.
규칙 유형	규칙이 로컬인지를 지정합니다. 로컬 규칙에는 맞춤형 표준 텍스트 침입 규칙, 수정된 표준 텍스트 규칙, 수정된 헤더 정보와 함께 규칙을 저장했을 때 생성된 공유 개체 규칙의 새 인스턴스가 포함됩니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
Username	침입 이벤트의 소스 호스트에 로그인한 사용자의 사용자 이름을 입력합니다.
VLAN ID	침입 이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID를 입력합니다.
웹 애플리케이션	침입 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

침입 이벤트 필드, 2912 페이지
Firepower System IP 주소 규칙, 19 페이지

악성코드 이벤트 트리거 기준 구문

악성코드 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 악성코드 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 중에서 선택할 수 있습니다.

- **by endpoint-based malware detection(**엔드포인트 기반 악성코드 탐지 이용**)**(엔드포인트용 AMP를 이용한 탐지)
- **by network-based malware detection(**네트워크 기반 악성코드 탐지 이용**)**(네트워크용 AMP를 이용한 탐지)
- **by retrospective network-based malware detection(**회귀적 네트워크 기반 악성코드 탐지 이용**)**(네트워크용 AMP를 이용한 회귀적 탐지)

다음 표에서는 기본 이벤트로 악성코드 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***255:*** 악성코드 이벤트 구문

다음을 지정할 경우**...**	연산자를 선택하고**...**
애플리케이션 프로토콜	악성코드 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
Client(클라이언트)	악성코드 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	악성코드 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
목적지 IP, 호스트 IP 또는 소스 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
대상 포트/ICMP 코드	대상 트래픽의 포트 번호 또는 ICMP 코드를 입력합니다.
속성	**Malware(**악성코드**)**나 **Custom Detection(**맞춤형 탐지**)** 중 하나 또는 둘 다를 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
이벤트 유형	엔드포인트용 AMP가 탐지한 악성코드 이벤트와 관련된 이벤트 유형을 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
파일 이름	파일의 이름을 입력합니다.
File Type(파일 유형)	파일 형식을 선택합니다.
파일 유형 카테고리	파일 유형 카테고리를 하나 이상 선택합니다.
IOC 태그	악성코드 이벤트의 결과로 침해 지표 태그가 **is** 또는 **is not**으로 설정되었는지를 선택합니다.
SHA-256	파일의 SHA-256 해시 값을 입력하거나 붙여넣습니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
소스 포트/ICMP 유형	소스 트래픽의 포트 번호 또는 ICMP 유형을 입력합니다.
웹 애플리케이션	악성코드 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

파일 및 악성코드 이벤트 필드, 2968 페이지
Firepower System IP 주소 규칙, 19 페이지

검색 이벤트 트리거 기준 구문

검색 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 검색 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 표는 선택할 수 있는 검색 이벤트 유형을 나열합니다.

홉이 변경되는 경우 또는 호스트 제한에 도달하여 시스템이 새 호스트를 삭제하는 경우에는 상관관계 규칙을 트리거할 수 없습니다. 그러나 유형과 상관없이 검색 이벤트가 발생할 때 규칙을 트리거하려면 **there is any type of event(**아무 유형의 이벤트가 존재함**)**를 선택합니다.

표 ***256:*** 상관관계 규칙 트리거 기준 대 검색 이벤트 유형

옵션 선택	이 검색 이벤트 유형 사용
클라이언트가 변경됨	클라이언트 업데이트
클라이언트의 시간이 초과됨	클라이언트 시간 초과
호스트 IP 주소 재사용됨	DHCP: IP 주소 재할당
호스트 한도에 도달하여 호스트가 삭제됨	호스트 삭제됨: 호스트 한도 도달함
호스트가 네트워크 장치로 식별됨	네트워크 디바이스로 호스트 유형 변경됨
호스트의 시간이 초과됨	호스트 시간 초과
호스트 IP 주소가 변경됨	DHCP: IP 주소 변경됨
NETBIOS 이름 변경이 탐지됨	NETBIOS 이름 변경
새 클라이언트가 탐지됨	새 클라이언트
새 IP 호스트가 탐지됨	새 호스트
새 MAC 주소가 탐지됨	호스트에 대해 추가 MAC 탐지됨
새 MAC 호스트가 탐지됨	새 호스트
새 네트워크 프로토콜이 탐지됨	새 네트워크 프로토콜
새 전송 프로토콜이 탐지됨	새 전송 프로토콜
aTCP 포트가 닫힘	TCP 포트 닫힘
TCP 포트의 시간이 초과됨	TCP 포트 시간 초과
UDP 포트가 닫힘	UDP 포트 닫힘
UDP 포트의 시간이 초과됨	UDP 포트 시간 초과
VLAN 태그가 업데이트됨	VLAN 태그 정보 업데이트

옵션 선택	이 검색 이벤트 유형 사용
IOC가 설정됨	보안 침해 지표
열린 TCP 포트가 탐지됨	새 TCP 포트
열린 UDP 포트가 탐지됨	새 UDP 포트
호스트에 대한 OS 정보가 변경됨	새 OS
호스트에 대한 OS 또는 서버 ID에 충돌이 발생함	ID 충돌
호스트에 대한 OS 또는 서버 ID의 시간이 초과됨	ID 시간 초과
아무 유형의 이벤트가 존재함	아무 이벤트 유형
MAC 주소에 대한 새 정보가 있음	MAC 정보 변경
TCP 서버에 대한 새 정보가 있음	TCP 서버 정보 업데이트
UDP 서버에 대한 새 정보가 있음	UDP 서버 정보 업데이트

다음 표에서는 기본 이벤트로 검색 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***257:*** 검색 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
Client(클라이언트)	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트의 버전 번호를 입력합니다.
디바이스	검색 이벤트를 생성했을 가능성이 있는 장치를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

다음을 지정할 경우...	연산자를 선택하고...
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 **`iPhone`**을 입력합니다.
Host Type(호스트 유형)	호스트 유형을 하나 이상 선택합니다. 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IP 주소 또는 새 IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC Address(MAC 주소)	호스트의 MAC 주소 전체 또는 일부를 입력합니다. 예를 들어 특정 하드웨어 제조업체 디바이스의 MAC 주소가 0A:12:34로 시작하는 것을 알고 있다면 연산자로 **begins with**를 선택하고 값으로 **`0A:12:34`**를 입력할 수 있습니다.
MAC 유형	MAC 주소가 **ARP/DHCP Detected**인지 여부를 선택합니다. 즉 시스템에서 MAC 주소를 호스트에 속한 것(**ARP/DHCP Detected**)으로 확실하게 식별했는지, 또는 매니지드 디바이스와 호스트 간에 라우터가 있다는 등의 이유로 여러 호스트가 해당 MAC 주소를 갖는지(**is not ARP/DHCP Detected**) 여부를 선택합니다.
MAC 벤더	검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 벤더 이름 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
NETBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
Network Protocol(네트워크 프로토콜)	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
OS Name	운영체제 이름을 하나 이상 선택합니다.
OS Vendor(OS 공급업체)	운영체제 벤더를 하나 이상 선택합니다.
OS Version(OS 버전)	운영체제 버전을 하나 이상 선택합니다.
프로토콜 또는전송 프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
소스	(운영체제와 서버 ID의 변경 및 시간 초과에 대한) 호스트 입력 데이터의 소스를 선택합니다.
소스 유형	(운영체제와 서버 ID의 변경 및 시간 초과에 대한) 호스트 입력 데이터의 소스 유형을 선택합니다.
VLAN ID	이벤트와 관련된 호스트 VLAN ID를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 선택합니다.

관련 항목

검색 이벤트 유형, 3039 페이지
검색 이벤트 필드, 3046 페이지
Firepower System IP 주소 규칙, 19 페이지

사용자 활동 이벤트 트리거 기준 구문

사용자 활동의 상관관계 규칙에 기반을 두려면, 먼저 사용할 사용자 활동의 유형을 선택해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 중에서 선택할 수 있습니다.

- 새 사용자 **ID**가 탐지됨
- 사용자가 호스트에 로그인함

다음 표에서는 기본 이벤트로 사용자 활동 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***258:*** 사용자 활동 구문

지정 항목	연산자 선택
디바이스	사용자 활동을 탐색했을 가능성이 있는 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
Username	사용자 이름을 입력합니다.

관련 항목

사용자 활동 데이터 필드

Firepower System IP 주소 규칙, 19 페이지

호스트 입력 이벤트 트리거 기준 구문

호스트 입력 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 호스트 입력 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 표는 선택할 수 있는 호스트 입력 이벤트 유형을 나열합니다.

사용자 정의 호스트 속성의 정의를 추가, 삭제 또는 변경할 때나 취약성 영향 자격을 설정할 때는 상관관계 규칙을 트리거할 수 없습니다.

표 ***259:*** 상관관계 규칙 트리거 기준 호스트 입력 이벤트 유형

옵션 선택	이 이벤트 유형에서 규칙을 트리거
클라이언트가 추가됨	클라이언트 추가
클라이언트가 삭제됨	클라이언트 삭제
호스트가 추가됨	호스트 추가
프로토콜이 추가됨	프로토콜 추가
프로토콜이 삭제됨	프로토콜 삭제
스캔 결과가 추가됨	스캔 결과 추가
서버 정의가 설정됨	서버 정의 설정
서버가 추가됨	포트 추가
서버가 삭제됨	포트 삭제
취약성이 유효하지 않음으로 표시됨	취약성 설정 유효하지 않음
취약성이 유효함으로 표시됨	취약성 설정 유효함
주소가 삭제됨	호스트/네트워크 삭제
속성 값이 삭제됨	호스트 특성 삭제 값
속성 값이 설정됨	호스트 특성 설정 값
운영체제 정의가 설정됨	운영 시스템 정의 설정
호스트 중요도가 설정됨	호스트 중요도 설정

다음 표에서는 기본 이벤트로 호스트 입력 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***260:*** 호스트 입력 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
소스	호스트 입력 데이터의 소스를 선택합니다.
소스 유형	호스트 입력 데이터의 소스 유형을 선택합니다.

관련 항목

호스트 입력 이벤트 유형, 3043 페이지
검색 이벤트 필드, 3046 페이지
Firepower System IP 주소 규칙, 19 페이지

연결 이벤트 트리거 기준 구문

연결 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 연결 이벤트의 유형을 지정해야 합니다. 연결 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다. 다음 중에서 선택할 수 있습니다.

- 연결 시작 또는 종료 시
- 연결 시작 시
- 연결 종료 시

다음 표에서는 기본 이벤트로 연결 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***261:*** 연결 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	연결을 로깅한 액세스 컨트롤 정책을 하나 이상 선택합니다.
Access Control Rule Action	연결을 로깅한 액세스 컨트롤 규칙과 관련된 작업을 하나 이상 선택합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 네트워크 트래픽이 Monitor 규칙의 조건과 일치할 때 상관관계 이벤트를 트리거하려면 **Monitor**를 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 규칙	연결을 로깅한 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 연결 기준으로 조건이 일치한 Monitor 규칙의 이름을 입력할 수 있습니다.
애플리케이션 프로토콜	연결과 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
Client(클라이언트)	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트의 버전 번호를 입력합니다.
연결 지속시간	연결 이벤트의 기간을 초 단위로 입력합니다.
연결 유형	연결 이벤트를 획득한 방법에 따라 상관관계 규칙을 트리거할지 여부를 지정합니다. • 내보낸 NetFlow 데이터에서 생성한 연결 이벤트에 대해 **is**와 **Netflow**를 선택합니다. • Firepower System 매니지드 디바이스가 탐지한 연결 이벤트에 대하 **is not**과 **Netflow**를 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	연결 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
디바이스	연결을 탐지했거나 (내보낸 NetFlow 기록에서 얻은 연결 데이터의 경우) 연결을 처리한 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
Egress Interface(이그레스 인터페이스) 또는 Ingress Interface(인그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Egress Security Zone(이그레스 보안 영역) 또는 Ingress Security Zone(인그레스 보안 영역)	보안 영역을 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
이니시에이터 바이트, 응답자 바이트 또는 전체 바이트	다음 중 하나를 입력합니다. • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) • 주고받은 바이트 수(전체 바이트)
이니시에이터 IP, 응답자 IP, 이니시에이터와 응답자 IP 모두, 또는 이니시에이터 IP나 응답자 IP	단일 IP 주소 또는 주소 블록을 지정합니다.
이니시에이터 패킷, 응답자 패킷 또는전체 패킷	다음 중 하나를 입력합니다. • 전송한 패킷 수(이니시에이터 패킷). • 수신한 패킷 수(응답자 패킷). • 주고받은 패킷 수(총 패킷)
이니시에이터 포트/ICMP 유형 또는 응답자 포트/ICMP 코드	이니시에이터 트래픽의 포트 번호나 ICMP 유형 또는 응답자 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	연결 이벤트 때문에 침해 지표 태그가 **is** 또는 **is not**으로 설정되었느지를 지정합니다.
NetBIOS Name(NetBIOS 이름)	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.
NetFlow 디바이스	상관관계 규칙을 트리거하는 데 사용할 NetFlow 엑스포터의 IP 주소를 선택합니다. 네트워크 검색 정책에 어떤 NetFlow 엑스포터도 추가하지 않았다면, **NetFlow Device(NetFlow** 디바이스**)** 드롭다운 목록에는 아무것도 표시되지 않습니다.
이유	연결 이벤트와 관련된 이유를 하나 이상 선택합니다.
보안 인텔리전스 카테고리	연결 이벤트와 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다. 보안 인텔리전스 카테고리를 연결 종료 이벤트의 조건으로 사용하려면, 액세스 컨트롤 정책에서 해당 카테고리를 **Block**이 아닌 **Monitor**로 설정합니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 지정합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 상태	세션 암호화에 사용된 인증서와 관련된 상태를 하나 이상 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 암호 그룹	세션 암호화에 사용된 암호 그룹을 하나 이상 선택합니다.
SSL 암호화된 세션	**Successfully Decrypted(**성공적으로 해독**)**를 선택합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
SSL 정책	암호화된 연결을 로깅한 SSL 정책을 하나 이상 선택합니다.
SSL 규칙 이름	암호화된 연결을 로깅한 SSL 규칙의 이름 전체 또는 일부를 입력합니다.
SSL 서버 이름	클라이언트가 암호화된 연결을 설정한 서버의 이름 전체 또는 일부를 입력합니다.
SSL URL 카테고리	암호화된 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
SSL 버전	세션 암호화에 사용된 SSL 또는 TLS 버전을 하나 이상 선택합니다.
TCP 플래그	상관관계 규칙을 트리거하기 위해 연결 이벤트에 포함해야 할 TCP 플래그를 선택합니다. NetFlow에서 생성한 연결 데이터만 TCP 플래그를 가지고 있습니다.
Transport Protocol(전송 프로토콜)	연결에 사용된 전송 프로토콜(**`TCP`** 또는 **`UDP`**)을 입력합니다.
URL	연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 범주	연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL Reputation(URL 평판)	연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.
Username	연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
웹 애플리케이션	연결과 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지
Firepower System IP 주소 규칙, 19 페이지

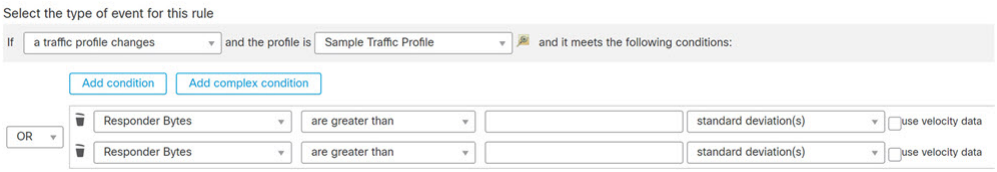
트래픽 프로파일 변경 구문

트래픽 프로파일 변경사항에 대한 상관관계 규칙을 기반으로 하려면, 먼저 사용할 트래픽 프로파일을 선택해야 합니다. 규칙은 네트워크 트래픽이 선택한 프로파일로 특성화되는 패턴에서 벗어날 때 트리거됩니다.

원시 데이터 또는 데이터에서 계산된 통계를 기반으로 규칙을 트리거할 수 있습니다. 예를 들어 네트워크를 통과하는 데이터의 양(바이트 단위로 측정됨)이 급증할 때(공격이나 기타 보안 정책 위반의 징후일 수 있음) 트리거되는 규칙을 작성할 수 있습니다. 다음의 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트 수가 특정 바이트 수 위로 급증하는 경우
- 네트워크를 통과하는 바이트 수가 평균 트래픽 양의 위 또는 아래에서 표준 편차의 특정 수치 위로 급증하는 경우

  네트워크를 통과하는 바이트의 수가 표준 편차의 특정 수치(위 또는 아래)를 벗어날 때 트리거되는 규칙을 생성하려면 다음 그림에 보이는 것처럼 상한 또는 하한을 지정해야 합니다.



  통과하는 바이트 수가 평균 위에서 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 그림에 보이는 첫 번째 조건만 사용하십시오.

  통과하는 바이트 수가 평균 아래에서 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 두 번째 조건만 사용하십시오.

데이터 포인트 간 변경 속도를 기반으로 상관관계 규칙을 트리거하려면 **use velocity data(**속도 데이터 사용**)** 확인란을 선택합니다. 위의 예에서 속도 데이터를 사용한다면 다음과 같은 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트의 양이 변경되어 평균 변경 속도 위에서 표준 편차의 특정 수치 위 또는 아래로 급증하는 경우
- 네트워크를 통과하는 바이트 수가 변경되어 특정 바이트 수 위로 급증하는 경우

다음 표에서는 기본 이벤트로 트래픽 프로파일 변경을 선택할 경우 상관관계 규칙에서 조건을 작성하는 방법에 대해 설명합니다.

표 ***262:*** 트래픽 프로파일 변경 구문

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.	그런 다음 다음 중 하나를 선택합니다.
연결 수	탐지된 총 연결 수 또는 규칙을 트리거하기 위해 탐지된 연결 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	연결 표준 편차
총 바이트, 이니시에이터 바이트 또는 응답자 바이트	다음 중 하나에 해당합니다. • 전송한 총 바이트(총 바이트) • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) 또는 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	바이트 표준 편차
총 패킷, 이니시에이터 패킷 또는 응답자 패킷	다음 중 하나에 해당합니다. • 전송한 총 패킷(총 패킷) • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷) 또는 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	packets 표준 편차
고유한 이니시에이터	세션을 시작한 고유한 호스트의 수 또는 규칙을 트리거하기 위해 탐지된 고유한 이니시에이터 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	개시자 표준 편차
고유한 응답자	세션에 응답한 고유한 호스트의 수 또는 규칙을 트리거하기 위해 탐지된 고유한 응답자 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	응답자 표준 편차

상관관계 호스트 프로파일 자격 구문

이벤트와 관련된 호스트의 호스트 프로파일을 기준으로 상관관계 규칙을 제한하려면 *host profile qualification(*호스트 프로파일 자격*)*을 추가합니다. 악성코드 이벤트, 트래픽 프로파일 변경 또는 새 IP 호스트 탐색에 대해 트리거되는 상관관계 규칙에 호스트 프로파일 자격을 추가할 수 없습니다.

호스트 프로파일 자격을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 호스트를 지정해야 합니다. 선택할 수 있는 호스트는 규칙의 기본 이벤트 유형에 따라 달라집니다 .

- 연결 이벤트 - **Responder Host(**응답자 호스트**)** 또는 **Initiator Host(**이니시에이터 호스트**)**를 선택합니다.
- 침입 이벤트 - **Destination Host(**목적지 호스트**)** 또는 **Source Host(**소스 호스트**)**를 선택합니다.
- 검색 이벤트, 호스트 입력 이벤트 또는 사용자 활동 - **Host(**호스트**)**를 선택합니다.

다음 표에서는 상관관계 규칙에 대한 호스트 프로파일 자격을 만드는 방법을 설명합니다.

표 ***263:*** 호스트 프로파일 자격 구문

다음을 지정할 경우**...**	연산자를 선택하고**...**
애플리케이션 프로토콜 >애플리케이션 프로토콜	애플리케이션 프로토콜을 선택합니다.
애플리케이션 프로토콜 >애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
애플리케이션 프로토콜 >프로토콜	Choose a protocol.
애플리케이션 프로토콜 카테고리	카테고리를 선택합니다.
클라이언트 > 클라이언트	클라이언트를 선택합니다.
클라이언트 > 클라이언트 버전	클라이언트 버전을 입력합니다.
클라이언트 카테고리	카테고리를 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다.이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 **`iPhone`**을 입력합니다.
Host Criticality(호스트 심각도)	호스트 중요도를 선택합니다.
Host Type(호스트 유형)	호스트 유형을 하나 이상 선택합니다. 일반 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.

다음을 지정할 경우...	연산자를 선택하고...
IOC 태그	침해 지표 태그를 하나 이상 선택합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC 주소 > MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다.
MAC 주소 > MAC 유형	MAC 유형이 ARP/DHCP Detected인지 여부를 선택합니다. • 시스템이 MAC 주소가 호스트에 속한 것으로 명확하게 확인함**(is ARP/DHCP Detected)** • 디바이스와 호스트 간에 라우터가 있다는 등의 이유로, 시스템이 MAC 주소가 있는 다양한 호스트를 확인함**(is not ARP/DHCP Detected)** • MAC 유형이 올바르지 않음**(is any)**
MAC 벤더	호스트에서 사용하는 하드웨어의 MAC 벤더 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
NetBIOS Name(NetBIOS 이름)	호스트의 NetBIOS 이름을 입력합니다.
Network Protocol(네트워크 프로토콜)	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
운영체제 > OS 벤더	운영체제 벤더 이름을 하나 이상 선택합니다.
운영체제 > OS 이름	운영체제 이름을 하나 이상 선택합니다.
운영체제 > OS 버전	운영체제 버전을 하나 이상 선택합니다.
Transport Protocol(전송 프로토콜)	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
VLAN ID	호스트의 VLAN ID 번호를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 선택합니다.
웹 애플리케이션 카테고리	카테고리를 선택합니다.
사용 가능한 모든 호스트 속성(기본 규정준수 화이트리스트 호스트 속성 포함)	호스트 속성 유형에 맞는 적절한 값을 입력하거나 선택합니다.

암시적 또는 일반 클라이언트를 사용하여 호스트 프로파일 자격 구축

시스템이 뒤에 클라이언트가 붙는 애플리케이션 프로토콜 이름(HTTPS 클라이언트 등)을 이용해 탐지 클라이언트를 보고하는 경우, 해당 클라이언트는 암시적 또는 일반 클라이언트가 됩니다. 이 경우 시스템은 특정 클라이언트를 탐지하지 않지만, 서버 응답 트래픽을 기준으로 클라이언트 존재를 추론합니다.

암시적 또는 일반 클라이언트를 사용하여 호스트 프로파일 자격을 생성하려면, 클라이언트가 아닌 응답자 호스트에서 실행하는 애플리케이션 프로토콜을 이용해 제한해야 합니다.

이벤트 데이터를 사용하여 호스트 프로파일 자격 작성

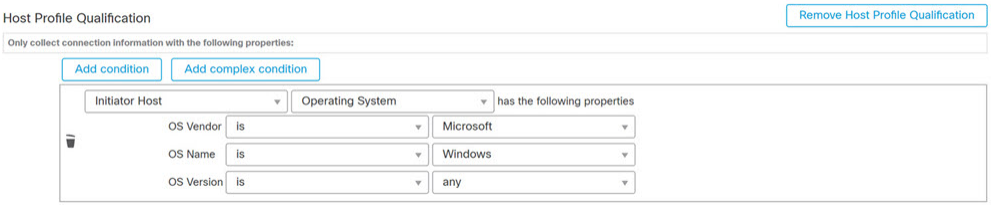
호스트 프로파일 자격을 구성할 때는 상관관계 규칙의 기본 이벤트에서 제공하는 데이터를 자주 사용하게 됩니다.

예를 들어 모니터링되는 호스트 중 하나에서 특정 브라우저를 사용하는 것을 시스템이 탐지할 때 상관관계 규칙이 트리거된다고 가정해보겠습니다. 그리고 이러한 사용을 탐지할 때, 브라우저 버전이 최신 버전이 아니라면 이벤트를 생성하려 합니다.

Client(클라이언트**)**가 **Event Client(**이벤트 클라이언트**)**지만 **Client Version(**클라이언트 버전**)**이 최신 버전이 아닐 경우에만 규칙이 트리거되도록 호스트 프로파일 자격을 이 상관관계 규칙에 추가할 수 있습니다.

호스트 프로파일 자격 예

다음 호스트 프로파일 자격은 규칙의 기반이 되는 검색 이벤트와 관련된 호스트가 Microsoft Windows 버전을 실행하는 경우에만 규칙이 트리거되는 방식으로 상관관계 규칙을 제한합니다.



관련 항목

호스트 데이터 필드, 3048 페이지

사용자 자격 구문

연결, 침입, 검색 또는 호스트 입력 이벤트를 사용하여 상관관계 규칙을 트리거하는 경우, 이벤트와 관련된 사용자의 ID를 기반으로 규칙을 제한할 수 있습니다. 이러한 제약을 *user qualification(*사용자 자격*)*이라고 합니다. 예를 들어 소스 또는 대상 사용자의 ID가 영업 부서 사용자인 경우에만 트리거되도록 상관관계 규칙을 제한할 수 있습니다.

트래픽 프로파일 변경 또는 사용자 활동 탐색에 대해 트리거되는 상관관계 규칙에 사용자 자격을 추가할 수 없습니다. 또한 시스템은 Firepower Management Center-ID 영역에서 형성된 서버 연결을 통해

사용자 상세정보를 획득합니다. 데이터베이스의 일부 사용자에 대해서는 이 정보를 이용하지 못할 수 있습니다.

사용자 자격을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 ID를 지정해야 합니다. 선택할 수 있는 ID는 규칙의 기본 이벤트 유형에 따라 달라집니다 .

- 연결 이벤트 - 이니시에이터에서의 **ID** 또는 응답자에서의 **ID**를 선택합니다.
- 침입 이벤트 - 목적지에서의 **ID** 또는 소스에서의 **ID**를 선택합니다.
- 검색 이벤트 - 호스트에서의 **ID**를 선택합니다.
- 호스트 입력 이벤트 - 호스트에서의 **ID**를 선택합니다.

다음 표에서는 상관관계 규칙에 대한 사용자 자격을 만드는 방법을 설명합니다.

표 ***264:*** 사용자 자격 구문

다음을 지정할 경우...	연산자를 선택하고...
Authentication Protocol(인증 프로토콜)	사용자 탐지에 사용한 인증 프로토콜(또는 사용자 유형) 프로토콜을 선택합니다.
Department(부서)	부서를 입력합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
Email(이메일)	이메일 주소를 입력합니다.
First Name(이름)	이름을 입력합니다.
Last Name(성)	성을 입력합니다.
Phone(전화 번호)	전화번호를 입력합니다.
Username	사용자 이름을 입력합니다.

관련 항목

사용자 데이터 필드

연결 추적기

규칙의 초기 기준이 충족되면(호스트 프로파일 및 사용자 자격 포함) 시스템이 특정 연결 추적을 시작할 수 있도록, 연결 추적기는 상관관계 규칙을 제한합니다. 추적된 연결이 지정 기간 동안 수집된 추가 기준을 충족할 경우 시스템은 규칙에 대해 상관관계 이벤트를 생성합니다.

팁 연결 추적기는 일반적으로 매우 구체적인 트래픽을 모니터링하며, 트리거될 경우 지정된 기간에만 실행됩니다. 일반적으로 폭넓은 네트워크 트래픽을 모니터링하고 영구적으로 실행되는 트래픽 프로파일을 연결 추적기와 비교해보십시오.

연결 추적기는 두 가지 방법으로 이벤트를 생성할 수 있습니다.

조건이 충족될 때 즉시 실행되는 연결 추적기

네트워크 트래픽이 추적기의 조건을 충족하자마자 상관관계 규칙이 실행되도록 연결 추적기를 구성할 수 있습니다. 이러한 상황이 발생하면 시스템은 시간 초과 기간이 만료되지 않았더라도 이 연결 추적기 인스턴스에 대한 연결 추적을 중지합니다. 상관관계 규칙을 트리거한 동일한 정책 위반 유형이 다시 발생하면 시스템은 새 연결 추적기를 생성합니다.

하지만 네트워크 트래픽이 연결 추적기의 조건을 충족하기 전에 시간이 만료되면 시스템은 상관관계 이벤트를 생성하지 않으며, 동시에 해당 규칙 인스턴스에 대한 연결 추적을 중지합니다.

예를 들어 연결 추적기는 특정 유형의 연결이 지정된 기간 내에 지정된 횟수보다 더 많이 발생하는 경우에만 상관관계 이벤트를 생성함으로써 일종의 이벤트 임계값 역할을 할 수 있습니다. 또는 초기 연결 이후 시스템에서 과도한 데이터 전송을 탐지하는 경우에만 상관관계 이벤트를 생성할 수 있습니다.

시간 초과 기간 끝에 실행되는 연결 추적기

전체 시간 초과 기간에 수집된 데이터에 의존하도록, 따라서 시간 초과 기간이 끝날 때까지 실행될 수 없도록 연결 추적기를 구성할 수 있습니다.

예를 들어 일정 기간 동안 특정 바이트 수 미만이 탐지될 때 실행되도록 연결 추적기를 구성하는 경우, 시스템은 기간이 지날 때까지 기다렸다가 네트워크 트래픽이 해당 조건을 충족하면 이벤트를 생성합니다.

연결 추적기 추가

시작하기 전에

- 연결, 침입, 검색, 사용자 ID 또는 호스트 입력 이벤트를 기반으로 상관관계 규칙을 생성합니다. 악성코드 이벤트 또는 트래픽 프로파일 변경을 기반으로 하는 규칙에는 연결 추적기를 추가할 수 없습니다.

프로시저

단계 **1** 상관관계 규칙 편집기에서 **Add Connection Tracker(**연결 추적기 추가**)**를 클릭합니다.

단계 **2** 추적할 연결을 지정합니다(연결 추적기 구문, 2610 페이지 참조).

단계 **3** 추적한 연결을 바탕으로, 상관관계 이벤트를 생성할 시점을 지정합니다(연결 추적기 이벤트 구문, 2613 페이지 참조).

단계 **4** 추적기의 조건을 달성해야 하는 간격(단위: 초, 분 또는 시간)을 지정합니다.

연결 추적기 구문

다음 표에서는 추적하고자 하는 연결의 종류를 지정하는 연결 추적기 조건을 작성하는 방법에 대해 설명합니다.

표 ***265:*** 연결 추적기 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	추적할 연결을 처리한 액세스 컨트롤 정책을 하나 이상 선택합니다.
Access Control Rule Action	추적할 연결을 로깅한 액세스 컨트롤 규칙과 관련된 액세스 컨트롤 규칙 작업을 하나 이상 선택합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, Monitor 규칙의 조건과 일치하는 연결을 추적하려면 **Monitor**를 선택합니다.
액세스 제어 규칙 이름	추적할 연결을 로깅한 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다. Monitor 규칙과 일치하는 연결을 추적하려면 Monitor 규칙의 이름을 입력하십시오. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이 시스템은 연결을 추적합니다.
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
Client(클라이언트)	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트 버전을 입력합니다.
연결 지속시간	연결 이벤트 지속시간을 초 단위로 입력합니다.
연결 유형	연결 이벤트를 획득한 방법에 따라 상관관계 규칙을 트리거할지 여부를 지정합니다. • 내보낸 NetFlow 기록에서 생성한 연결 이벤트에 대해 **is**와 **Netflow**를 선택합니다. • Firepower System 매니지드 디바이스가 탐지한 연결 이벤트에 대하 **is not**과 **Netflow**를 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	국가를 하나 이상 선택합니다.
디바이스	탐지된 연결을 추적하려는 디바이스를 하나 이상 선택합니다. NetFlow 연결을 추적하려면 내보낸 NetFlow 기록의 연결 데이터를 처리하는 디바이스를 선택합니다.
Ingress Interface(인그레스 인터페이스) 또는 Egress Interface(이그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Ingress Security Zone(인그레스 보안 영역) 또는 Egress Security Zone(이그레스 보안 영역)	보안 영역을 하나 이상 선택합니다.
이니시에이터 IP, 응답자 IP 또는 이니시에이터/응답자 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
이니시에이터 바이트, 응답자 바이트 또는 전체 바이트	다음 중 하나를 입력합니다. • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) • 전송 및 수신된 바이트 수(총 바이트)
이니시에이터 패킷, 응답자 패킷 또는 총 패킷	다음 중 하나를 입력합니다. • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷) • 전송 및 수신된 패킷 수(총 패킷)
이니시에이터 포트/ICMP 유형 또는 응답자 포트/ICMP 코드	이니시에이터 트래픽의 포트 번호나 ICMP 유형 또는 응답자 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	침해 지표 태그가 **is** 또는 **is not**으로 설정되었는지를 선택합니다.
NETBIOS 이름	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.
NetFlow 디바이스	추적할 NetFlow 엑스포터의 IP 주소를 선택합니다. 네트워크 검색 정책에 어떤 NetFlow 엑스포터도 추가하지 않았다면, NetFlow Device(NetFlow 디바이스) 드롭다운 목록에는 아무것도 표시되지 않습니다.
이유	추적할 연결과 관련된 이유를 하나 이상 선택합니다.
보안 인텔리전스 카테고리	추적할 연결과 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
TCP 플래그	추적을 위해 연결에 반드시 포함해야 하는 TCP 플래그를 선택합니다. 내보낸 NetFlow 기록에서 생성한 연결만 TCP 플래그 데이터를 가지고 있습니다.
Transport Protocol(전송 프로토콜)	연결에 사용된 전송 프로토콜을 선택합니다.
URL	추적할 연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 범주	추적할 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL Reputation(URL 평판)	추적할 연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.
Username	추적할 연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
웹 애플리케이션	웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

이벤트 데이터를 사용하여 연결 추적기 구축

연결 추적기를 구성할 때는 상관관계 규칙의 기본 이벤트에서 제공하는 데이터를 자주 사용하게 됩니다.

예를 들어 시스템이 새 클라이언트를 탐지할 때 상관관계 규칙이 트리거된다고 가정해 봅시다. 이러한 유형의 상관관계 규칙에 연결 추적기를 추가하면, 시스템은 기본 이벤트를 참조하는 제약 조건으로 추적기를 자동으로 채웁니다.

- **Initiator/Responder IP(**이니시에이터/응답자 **IP)**는 **Event IP Address(**이벤트 **IP** 주소**)**로 설정됩니다.
- **Client(**클라이언트**)**는 **Event Client(**이벤트 클라이언트**)**로 설정됩니다.

팁 특정 IP 주소 또는 IP 주소 블록의 연결을 추적하려면 **switch to manual entry(**수동 입력으로 전환**)**를 클릭하여 IP를 수동으로 지정하십시오. 이벤트의 IP 주소를 사용하는 방식으로 돌아가려면 **switch to event fields(**이벤트 필드로 전환**)**를 클릭합니다.

관련 항목

연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지
Firepower System IP 주소 규칙, 19 페이지

연결 추적기 이벤트 구문

다음 표에서는 추적 중인 연결을 기반으로 상관관계 이벤트를 생성하고자 하는 시기를 지정하는 연결 추적기 조건의 작성 방법에 대해 설명합니다.

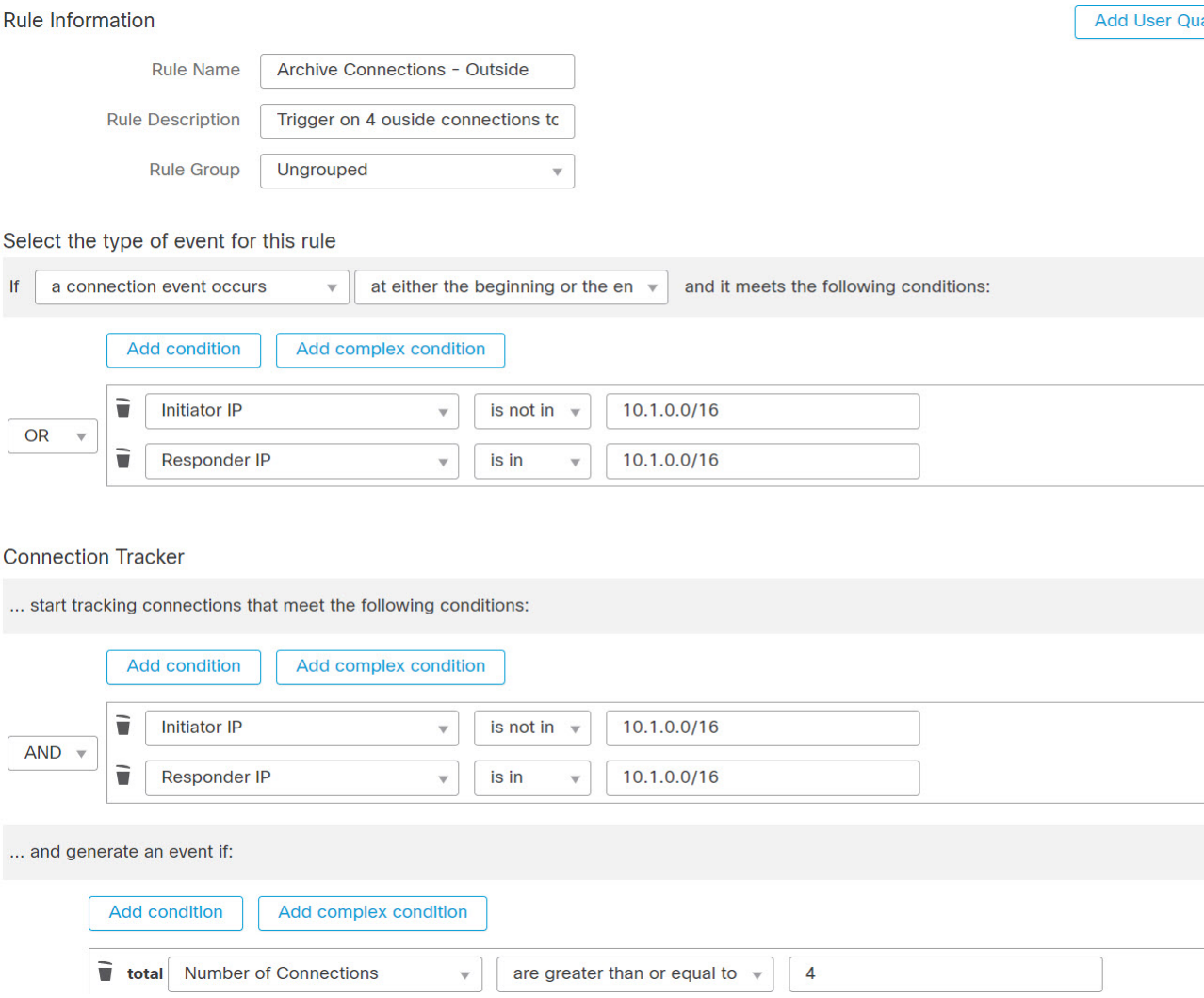
표 ***266:*** 연결 추적기 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.
연결 수	탐지된 총 연결 수
SSL 암호화된 세션 수	탐지된 총 SSL 또는 TLS 암호화 세션의 수를 입력합니다.
총 바이트, 이니시에이터 바이트 또는 응답자 바이트	다음 중 하나에 해당합니다. • 전송한 총 바이트(총 바이트) • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트)
총 패킷, 이니시에이터 패킷 또는 응답자 패킷	다음 중 하나에 해당합니다. • 전송한 총 패킷(총 패킷) • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷)
고유 이니시에이터 또는 고유 응답자	다음 중 하나에 해당합니다. • 탐지된 세션을 시작한 고유한 호스트의 수(고유 이니시에이터) • 탐지된 연결에 응답한 고유한 호스트의 수(고유 응답자)

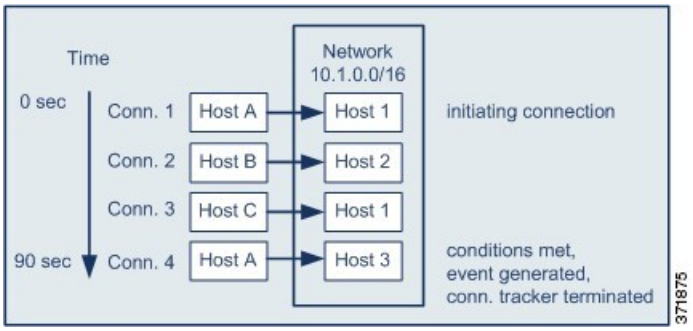
외부 호스트의 과도한 연결에 대한 샘플 설정

네트워크 10.1.0.0/16에 중요한 파일을 보관하며, 이 네트워크 외부의 호스트는 일반적으로 네트워크 내부의 호스트에 대해 연결을 시작하지 않는 시나리오를 고려해 보십시오. 네트워크 외부에서 더러 연결이 시작되었지만, 2분 내에 4개 이상의 연결이 시작되면 문제가 있는 것으로 판단했습니다.

다음 그림의 규칙에서는, 10.1.0.0/16 네트워크 외부에서 네트워크 내부로 연결이 시작될 때 시스템이 해당 조건을 충족하는 연결의 추적을 시작하는 것을 알 수 있습니다. 이제 시스템이 해당 서명과 일치하는 4개의 연결(원래 연결 포함)을 2분 내에 탐지할 경우 시스템은 상관관계 이벤트를 생성합니다.



다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 상관관계 규칙의 기본 조건을 충족한 연결, 즉 10.1.0.0/16 네트워크 외부 호스트에서 네트워크 내부 호스트로의 연결을 탐지했습니다. 여기에서 연결 추적기가 생성됩니다.

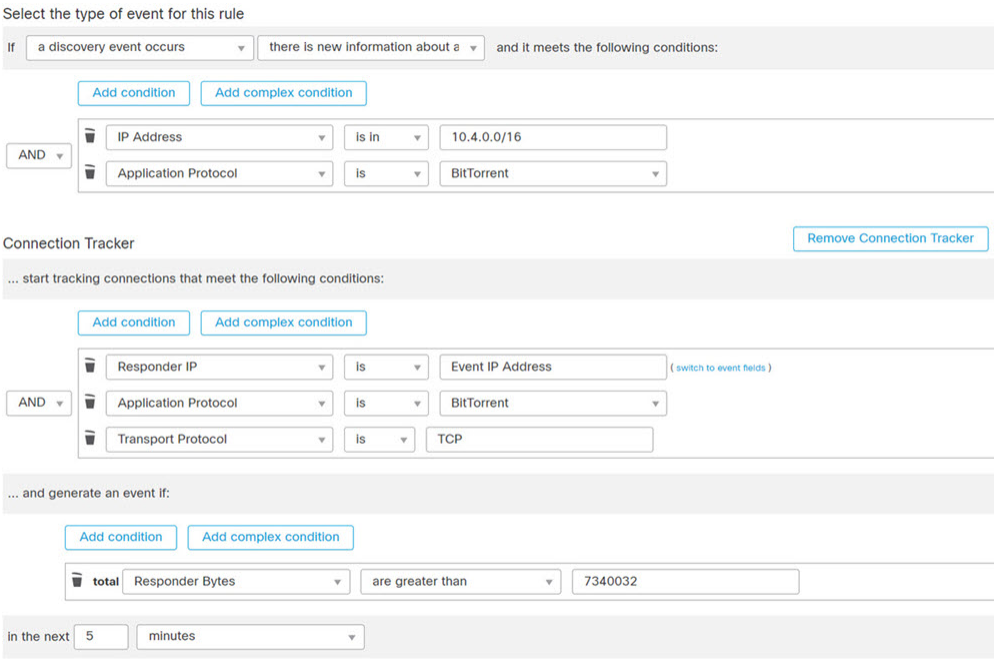
연결 추적기는 다음과 같이 처리됩니다.

- 먼저, 시스템은 네트워크 외부 Host A에서 네트워크 내부 Host 1로의 연결을 탐지하면 연결 추적을 시작합니다.
- 시스템은 연결 추적기 서명과 일치하는 연결을 2개 더 탐지합니다(Host B에서 Host 2, Host C에서 Host 1).
- 2분 시간 제한 내에 Host A가 Host 3에 연결되면 시스템은 4번째 해당 연결을 탐지하게 됩니다. 규칙 조건이 충족됩니다.
- 마지막으로, 시스템은 상관관계 이벤트를 생성하고 연결 추적을 중지합니다.

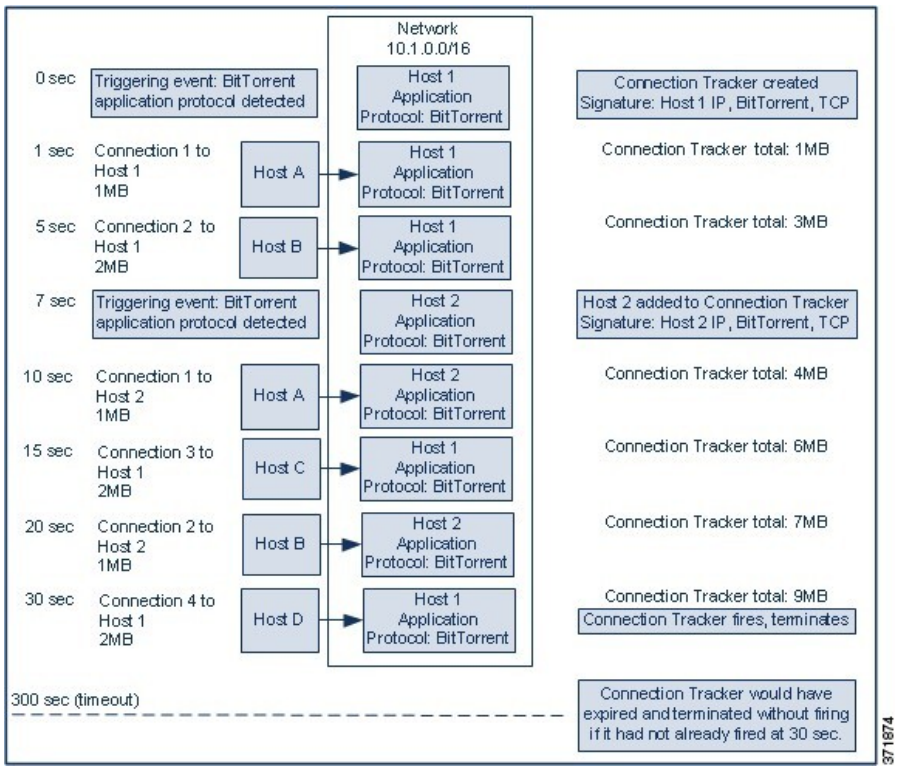
과도한 **BitTorrent** 데이터 전송에 대한 샘플 설정

모니터링되는 네트워크의 호스트에 대한 초기 연결 이후 시스템이 과도한 BitTorrent 데이터 전송을 탐지하는 경우 상관관계 이벤트를 생성하고자 하는 시나리오를 고려해보십시오.

다음 그림에서는 시스템이 모니터링되는 네트워크에서 BitTorrent 애플리케이션 프로토콜을 탐지할 때 트리거되는 상관관계 규칙을 보여줍니다. 이 규칙에는 모니터링되는 네트워크의 호스트(이 경우 10.1.0.0/16)가 초기 정책 위반 이후 5분 동안 BitTorrent를 통해 총 7MB(7340032바이트)가 넘는 데이터를 전송하는 경우 규칙이 트리거되도록 규칙을 제한하는 연결 추적기가 있습니다.



다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 두 호스트, 즉 Host 1과 Host 2에서 BitTorrent TCP 애플리케이션 프로토콜을 탐지했습니다. 이러한 두 호스트는 BitTorrent를 통해 4개의 다른 호스트(Host A, Host B, Host C, Host D)로 데이터를 전송합니다.

이 연결 추적기는 다음과 같이 처리됩니다.

- 먼저, 시스템은 Host 1에서 BitTorrent 애플리케이션 프로토콜을 탐지하면 0초 마커에서 연결 추적을 시작합니다. 시스템이 5분 내에(300초 마커까지) 7MB의 BitTorrent TCP 데이터가 전송되는 것을 탐지하지 못하면 연결 추적기가 만료됩니다.
- 5초에 Host 1이 서명과 일치하는 3MB의 데이터를 전송했습니다.
  - 1초 마커에 Host 1에서 Host A로 1MB(연결 추적기를 충족하기 위해 계산된 총 BitTorrent 트래픽 1MB)
  - 5초 마커에 Host 1에서 Host B로 2MB(총 3MB)
- 7초에 시스템은 Host 2에서 BitTorrent 애플리케이션 프로토콜을 탐지하고 해당 호스트에 대해서도 BitTorrent 연결 추적을 시작합니다.
- 20초에 시스템은 서명과 일치하는 추가 데이터가 Host 1과 Host2 모두에서 전송되는 것을 탐지했습니다.
  - 10초 마커에 Host 2에서 Host A로 1MB(총 4MB)
  - 15초 마커에 Host 1에서 Host C로 2MB(총 6MB)
  - 20초 마커에 Host 2에서 Host B로 1MB(총 7MB)

- Host 1과 Host 2에서 이제 총 7MB의 BitTorrent 데이터를 전송했지만, 전송된 총 바이트 수가 7MB(응답자 바이트가 **7340032** 초과**)**)보다 커야 하므로 규칙이 트리거되지 않습니다. 이 시점에 시스템이 추적기의 시간 초과 기간에 나머지 280초 동안 추가 BitTorrent 전송을 탐지하지 못하면, 추적기가 만료되고 시스템은 상관관계 이벤트를 생성하지 않습니다.
- 하지만 30초가 되면 시스템은 다른 BitTorrent 전송을 탐지하고, 규칙 조건이 충족됩니다.
  - 30초 마커에 Host 1에서 Host D로 2MB(총 9MB)
- 마지막으로, 시스템은 상관관계 이벤트를 생성합니다. 5분 기간이 만료되지 않았어도 시스템은 이 연결 추적기 인스턴스에 대한 연결 추적도 중지합니다. 이 시점에 BitTorrent TCP 애플리케이션 프로토콜을 사용하는 새 연결을 탐지하면 시스템은 새 연결 추적기를 생성합니다. 시스템은 세션이 끝날 때까지 연결 데이터를 집계하지 않으므로, Host 1이 총 2MB를 Host D로 전송한 후 상관관계 이벤트를 생성합니다.

스누즈 및 비활성 기간

상관관계 규칙에서 스누즈 기간을 구성할 수 있습니다. 상관관계 규칙이 트리거되면, 유휴 기간은 지정된 기간 동안(규칙 위반이 다시 발생해도) 규칙의 실행을 중지하도록 시스템에 지시합니다. 스누즈 기간이 경과하면 규칙을 다시 트리거할 수 있습니다(그리고 새 스누즈 기간을 시작할 수 있습니다).

예를 들면 트래픽을 생성해서는 안 되는 호스트가 네트워크에 있을지도 모릅니다. 시스템이 해당 호스트와 관련된 연결을 탐지할 때마다 트리거되는 간단한 상관관계 규칙은 호스트를 통과하는 네트워크 트래픽에 따라 짧은 기간에 여러 상관관계 이벤트를 생성할 수 있습니다. 정책 위반을 알리는 상관관계 이벤트의 수를 제한하려면 시스템이 해당 호스트와 관련하여 시스템이 탐지하는 첫 번째 연결(지정한 기간 내에)에 대해서만 상관관계 이벤트를 생성하도록 유휴 기간을 추가할 수 있습니다.

상관관계 규칙에서 비활성 시간도 설정할 수 있습니다. 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다. 비활성 기간이 매일, 매주 또는 매월 반복되도록 설정할 수 있습니다. 예를 들어 호스트 운영체제 변경 사항을 찾기 위해 내부 네트워크에서 야간 Nmap 스캔을 수행할 수 있습니다. 이 경우 규칙이 잘못 트리거되지 않도록 스캔 시간 및 기간에 영향받는 상관관계 규칙에 대해 일일 비활성 기간을 설정할 수 있습니다.

상관관계 규칙 작성 원리

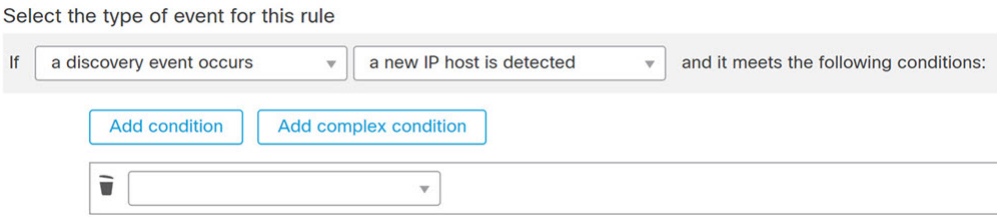
트리거 조건을 지정하여 상관관계 규칙을 작성합니다. 조건 내에서 사용할 수 있는 구문은 생성하는 요소에 따라 달라지지만, 그 원리는 동일합니다.

대부분의 조건은 카테고리, 연산자, 값이라는 3개 부분으로 구성됩니다.

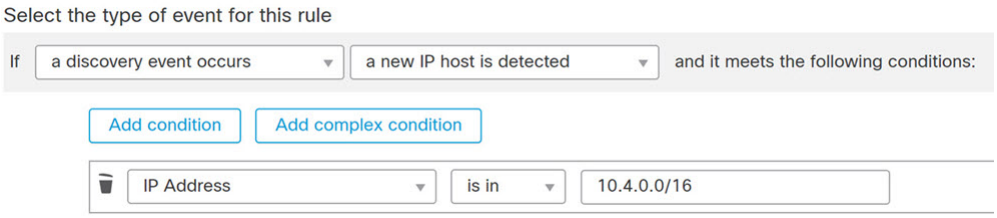
- 선택 가능한 카테고리는 상관관계 규칙 트리거, 호스트 프로파일 자격, 연결 추적기 또는 사용자 자격 중 어떤 것을 작성 중인지에 따라 달라집니다. 상관관계 규칙 트리거에서, 카테고리는 규칙에 대한 기본 이벤트 유형에 따라 달라집니다. 일부 조건은 여러 카테고리를 포함하는데, 각 카테고리마다 고유의 연산자와 값을 가질 수도 있습니다.
- 조건의 사용 가능한 연산자는 카테고리에 따라 달라집니다.

- 조건의 값을 지정하는 데 사용 가능한 구문은 카테고리와 연산자에 따라 달라집니다. 텍스트 필드에 직접 값을 입력해야 하는 경우도 있습니다. 그 외의 경우에는 드롭다운 목록에서 값(복수의 값 가능)을 선택할 수 있습니다.

예를 들어 새 호스트가 탐지될 때마다 상관관계 이벤트를 생성하려면, 어떤 조건도 없는 매우 단순한 규칙을 생성할 수 있습니다.



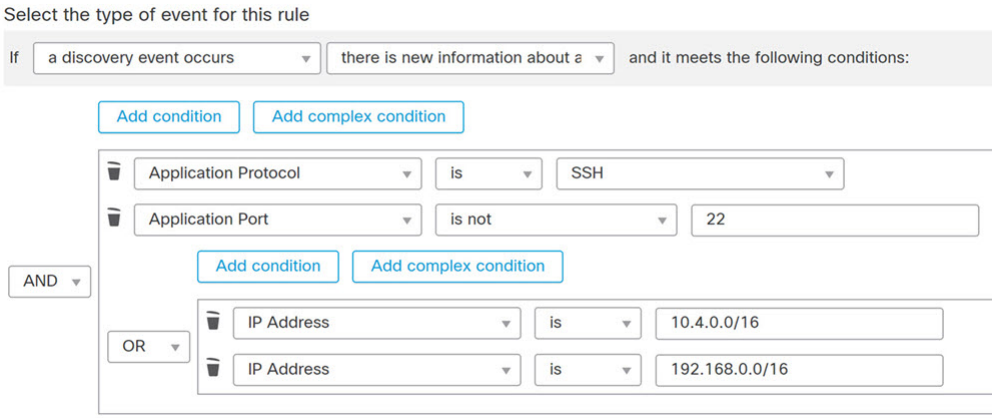
규칙을 더 제한하여 10.4.x.x 네트워크에서 새 호스트가 탐지되는 경우에만 이벤트를 생성하려는 경우 단일 조건을 추가할 수 있습니다.



여러 개의 조건을 포함할 경우 **AND** 또는 **OR** 연산자로 연결해야 합니다. 동일한 레벨의 조건은 함께 평가됩니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자를 사용하면 이 연산자가 제어하는 레벨의 조건 중 하나 이상을 충족해야 합니다.

10.4.x.x 네트워크 및 192.168.x.x 네트워크의 비표준 포트에서 SSH 활동을 탐지하는 다음 규칙에는 4개의 조건이 있으며, 그중 마지막 2개는 복합 조건입니다.



논리적으로, 이 규칙은 다음과 같이 평가됩니다.

```
(A and B and (C or D))
```

표 ***267:*** 규칙 평가

항목	조건의 내용
A	애플리케이션 프로토콜이 SSH임
B	애플리케이션 포트가 22가 아님
C	IP 주소는 10.0.0.0/8임
D	IP 주소가 196.168.0.0/16에 있음

주의 자주 발생하는 이벤트에 대해 트리거되는 복잡한 상관관계 규칙을 평가하면 시스템 성능이 저하될 수 있습니다. 예를 들어 로깅된 모든 연결에 대해 시스템에서 반드시 평가해야 하는 다중 조건 규칙은 리소스 과부하를 일으킬 수 있습니다.

상관관계 규칙에 조건 추가 및 연결

프로시저

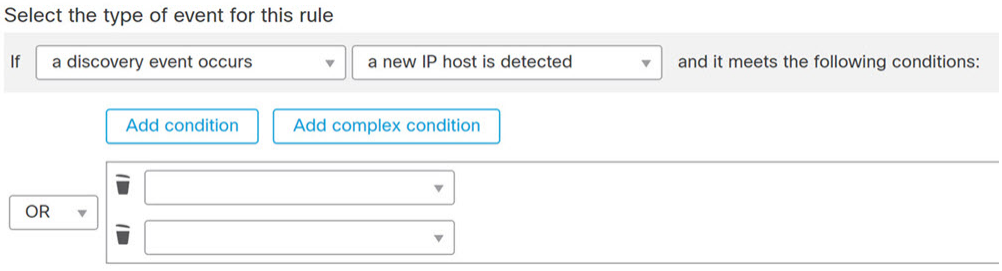
단계 **1** 상관관계 규칙 편집기에서 단순 또는 복합 조건을 추가합니다.

- 단순 - **Add condition(**조건 추가**)**을 클릭합니다.
- 복합 - **Add complex condition(**복합 조건 추가**)**을 클릭합니다.

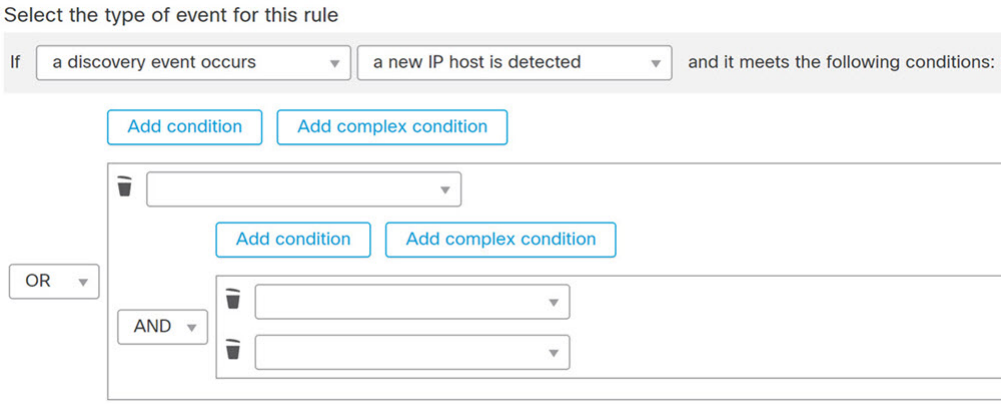
단계 **2** 조건 왼쪽에 있는 드롭다운 목록에서 **AND** 또는 **OR** 연산자를 선택해 조건을 연결합니다.

예**:** 단순 대 복합 조건

다음 그림은 두 가지 단순 조건이 **OR** 연산자로 결합된 상관관계 규칙을 보여줍니다.



다음 그림은 단순 조건 하나와 복합 조건 하나가 **OR** 연산자로 결합된 상관관계 규칙을 보여줍니다. 복합 조건은 **AND** 연산자로 결합된 단순 조건 2개로 구성됩니다.



상관관계 규칙 조건에 여러 값 사용

상관관계 조건을 작성할 때 조건 구문상 드롭다운 목록의 값 선택이 가능할 경우 대개는 목록에서 여러 값을 사용할 수 있습니다.

프로시저

단계 **1** 상관관계 규칙 편집기에서 조건을 작성하고, **is in** 또는 **is not in**을 연산자로 선택합니다.

단계 **2** 텍스트 필드의 아무 곳이나 클릭하거나 **Edit(**편집**)** 링크를 클릭합니다.

단계 **3** **Available(**사용 가능**)**에서 여러 값을 선택합니다. 클릭하고 드래그하여 인접한 여러 값을 선택할 수도 있습니다.

단계 **4** 오른쪽 화살표(>)를 클릭하여 선택한 항목을 **Selected**로 이동합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

상관관계 규칙 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 상관관계 규칙 및 그룹을 표시하며, 이러한 정책은 편집할 수 있습니다. 상위 도메인의 선택된 상관관계 규칙 및 그룹도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 상관관계 규칙 및 그룹을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다.

활성 상관관계 정책의 규칙에 적용된 변경사항은 즉시 적용됩니다.

시작하기 전에

- 규칙을 삭제하려면 상관관계 정책 관리, 2586 페이지에 설명된 대로 해당 규칙을 모든 상관관계 정책에서 삭제합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Rule Management(**규칙 관리**)**을 클릭합니다.

단계 **2** 규칙 관리:

- Create(생성) - **Create Rule(**규칙 생성**)**를 클릭합니다(상관관계 규칙 설정, 2587 페이지 참조).
- Create Group(그룹 생성) - **Create Group(**그룹 생성**)**을 클릭하고, 그룹의 이름을 입력하고, **Save(**저장**)**를 클릭합니다. 그룹에 규칙을 추가하려면 규칙을 편집합니다.
- 편집 - 수정( )을 클릭합니다. 상관관계 규칙 설정, 2587 페이지의 내용을 참조하십시오. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- Delete Rule or Rule Group(규칙 또는 규칙 그룹 삭제) - 삭제( )을 클릭합니다. 규칙 그룹을 삭제하면 규칙의 그룹이 해제됩니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

상관관계 응답 그룹 설정

알림 및 교정의 상관관계 응답 그룹을 만든 다음, 해당 그룹을 활성화해 활성 상관관계 정책 내의 상관관계 규칙에 할당할 수 있습니다. 시스템은 네트워크 트래픽이 상관관계 규칙과 일치할 때 모든 그룹화된 응답을 실행합니다.

활성 상관관계 정책에서 사용하는 경우, 활성 그룹 또는 그룹화된 응답에 대한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Groups(**그룹**)**를 클릭합니다.

단계 **2** **Create Group(**그룹 생성**)**을 클릭합니다.

단계 **3** **Name(**이름**)**을 입력합니다.

단계 **4** 생성 즉시 그룹을 활성화하려면 **Active(**활성**)** 확인란을 선택합니다.

비활성화된 그룹은 응답을 실행하지 않습니다.

단계 **5** 그룹에 대한 **Available Responses(**사용 가능한 응답**)**를 선택하고, 오른쪽 화살표(>)를 클릭해 응답을 **Responses in Group(**그룹 내 응답**)**으로 옮깁니다. 응답을 다른 방식으로 옮기려면 왼쪽 화살표(<)를 사용합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 생성과 동시에 활성화하지 않은 그룹을 지금 활성화하고 싶다면, 슬라이더를 클릭합니다.

관련 항목

Firepower Management Center 알림 응답, 2681 페이지
교정 소개, 2637 페이지

상관관계 응답 그룹 관리

상관관계 정책에서 사용하지 않는 응답 그룹을 삭제할 수 있습니다. 응답 그룹을 삭제하면 관련 응답의 그룹이 해제됩니다. 응답 그룹을 삭제하지 않고 일시적으로 비활성화할 수도 있습니다. 이렇게 하면 그룹은 시스템에서 삭제되지 않지만 정책 위반 시 실행되지도 않습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 그룹을 표시하며 이러한 그룹은 수정할 수 있습니다. 상위 도메인에서 생성된 그룹도 표시되지만, 이러한 그룹은 수정할 수 없습니다. 하위 도메인에서 생성된 그룹을 보고 수정하려면 해당 도메인으로 전환하십시오.

사용 중인 활성 응답 그룹에 대한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Groups(**그룹**)**를 클릭합니다.

단계 **2** 응답 그룹 관리:

- Activate(활성화) 또는 Deactivate(비활성화) - 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- Create(생성) - **Create Group(**그룹 생성**)**을 클릭합니다(상관관계 응답 그룹 설정, 2621 페이지 참조).
- 편집 - 수정( )을 클릭합니다. 상관관계 응답 그룹 설정, 2621 페이지의 내용을 참조하십시오. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - 삭제( )을(를) 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

106 장

트래픽 프로파일

다음 주제에서는 트래픽 프로파일을 설정하는 방법을 설명합니다.

- 트래픽 프로파일 소개, 2623 페이지
- 트래픽 프로필 요구 사항 및 사전 요건, 2627 페이지
- 트래픽 프로파일 관리, 2627 페이지
- 트래픽 프로파일 설정, 2628 페이지

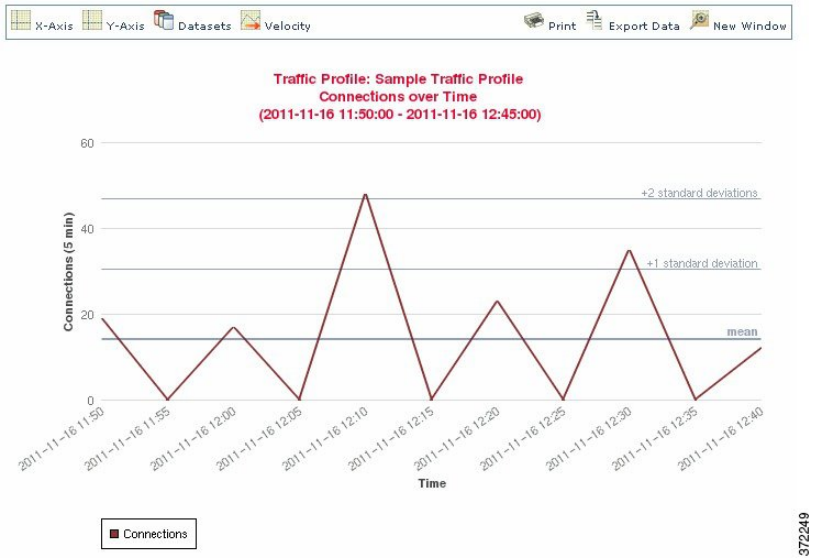
트래픽 프로파일 소개

트래픽 프로파일은 PTW(profiling time window) 동안 수집한 연결 데이터를 기반으로 하는 네트워크 트래픽 그래프입니다. 이 수치는 정상적인 네트워크 트래픽을 나타냅니다. 학습 기간이 지나면, 프로파일을 기준으로 새로운 트래픽을 평가해 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

기본 PTW는 1주이지만 짧게는 1시간, 길게는 몇 주까지 변경할 수 있습니다. 기본적으로 트래픽 프로파일은 시스템에서 발생한 연결 이벤트에 대한 통계를 5분 간격으로 생성합니다. 그러나 이 샘플링 속도는 최대 1시간까지 늘릴 수 있습니다.

팁 Cisco는 PTW에 100개 이상의 데이터 포인트가 포함되는 것을 권장합니다. 트래픽 프로파일에 통계적으로 유의미한 양의 데이터가 포함되도록 PTW와 샘플링 속도를 설정합니다.

다음 그림은 PTW가 1일, 샘플링 속도가 5분인 트래픽 프로파일을 보여줍니다.



트래픽 프로파일에서 비활성 시간도 설정할 수 있습니다. 트래픽 프로파일은 비활성 기간 동안 데이터를 수집하지만, 프로파일 통계를 계산할 때는 해당 데이터를 사용하지 않습니다. 시간 추이 트래픽 프로파일 그래프에서는 비활성 기간이 음영으로 나타납니다.

예를 들어 모든 워크스테이션이 매일 밤 자정에 백업되는 네트워크 인프라가 있습니다. 백업에는 약 30분이 소요되고 네트워크 트래픽이 급증합니다. 예약된 백업과 일치하도록 트래픽 프로파일에 대한 반복 비활성 기간을 설정할 수 있습니다.

참고 시스템은 연결 종료 시의 데이터를 사용하여 연결 그래프와 트래픽 프로파일을 생성합니다. 트래픽 프로파일을 사용하려면, Firepower Management Center 데이터베이스에 대한 연결 종료 시 이벤트를 기록하는지 확인하십시오.

트래픽 프로파일 구현

트래픽 프로파일을 활성화하면, 시스템은 사용자가 설정한 학습 기간(PTW) 동안 연결 데이터를 수집하고 평가합니다. 학습 기간이 지나면, 시스템은 트래픽 프로파일에 대해 작성된 상관관계 규칙을 평가합니다.

예를 들어 네트워크를 지나는 데이터의 양(패킷, KByte 또는 연결 수 단위로 측정됨)이 급증하여 트래픽 평균량보다 표준 편차의 3배만큼 많아질 때(공격이나 기타 보안 정책 위반의 징후일 수 있음) 트리거되는 규칙을 작성할 수 있습니다. 그런 다음 상관관계 정책에 그 규칙을 포함시켜 트래픽 급증을 알리거나 그에 대한 대응으로 개선 조치를 수행할 수 있습니다.

트래픽 프로파일을 대상으로 지정

프로파일 조건과 호스트 프로파일 자격은 트래픽 프로파일을 제한합니다.

프로파일 조건을 사용하면 모든 네트워크 트래픽의 프로파일을 생성하거나, 트래픽 프로파일을 제한해 도메인, 도메인 내부 또는 여러 도메인 사이에 있는 서브넷, 또는 개별 호스트를 모니터링하도록 제한할 수 있습니다. 다중 도메인 구축의 경우:

- 리프 도메인 관리자는 자신의 리프 도메인 내의 네트워크 트래픽에 대한 프로파일을 생성할 수 있습니다.
- 상위 도메인 관리자는 도메인 내부 또는 도메인 사이에 있는 트래픽에 대한 프로파일을 생성할 수 있습니다.

또한 프로파일 조건을 이용하면 연결 데이터를 기반으로 하는 기준을 사용하여 트래픽 프로파일을 제한할 수도 있습니다. 예를 들어 트래픽 프로파일이 반드시 특정 포트, 프로토콜 또는 애플리케이션을 사용하여 세션의 프로파일을 생성하도록 프로파일 조건을 설정할 수도 있습니다.

마지막으로, 추적한 호스트에 대한 정보를 이용해 트래픽 프로파일을 제한할 수 있습니다. 이러한 제약을 *host profile qualification(*호스트 프로파일 자격*)*이라고 합니다. 예를 들어 중요도가 높은 호스트의 연결 데이터만 수집할 수 있습니다.

참고 트래픽 프로파일을 상위 도메인에 제한하면 각각의 하위 리프 도메인에 있는 같은 유형의 트래픽을 집계하고 프로파일을 생성합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우, 도메인 사이의 트래픽에 대한 프로파일을 생성하면 예기치 않은 결과가 발생할 수 있습니다.

관련 항목

상관관계 정책 및 규칙 소개, 2583 페이지

트래픽 프로파일 조건

단순한 트래픽 프로파일 조건과 호스트 프로파일 자격을 생성하거나 조건을 연결하고 중첩시키는 방법으로 더 정교하게 구성할 수 있습니다.

대부분의 조건은 카테고리, 연산자, 값이라는 3개 부분으로 구성됩니다.

- 사용할 수 있는 카테고리는 트래픽 작성의 대상이 프로파일 조건인지 호스트 프로파일 자격인지에 따라 달라집니다.
- 사용할 수 있는 연산자는 선택한 카테고리에 따라 달라집니다.
- 조건의 값을 지정하는 데 사용 가능한 구문은 카테고리와 연산자에 따라 달라집니다. 텍스트 필드에 직접 값을 입력해야 하는 경우도 있습니다. 그 외의 경우에는 드롭다운 목록에서 하나 이상의 값을 선택할 수 있습니다.

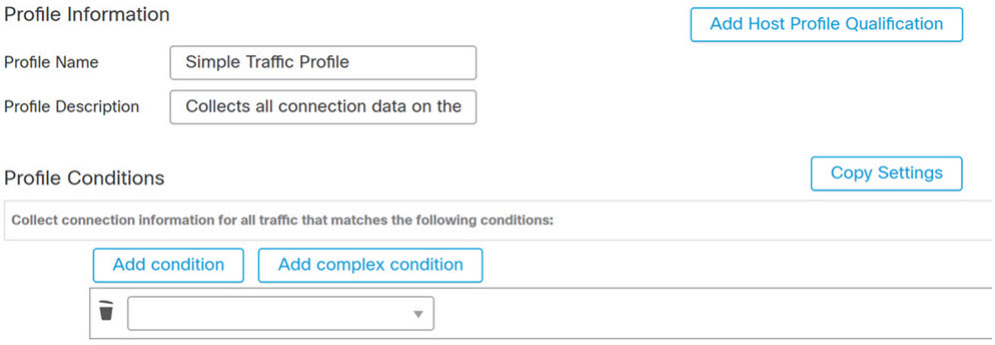
호스트 프로파일 자격의 경우에는, 이니시에이팅 또는 응답 호스트에 관한 정보 데이터를 사용하여 트래픽 프로파일을 제한하는지의 여부도 지정해야 합니다.

여러 개의 조건을 포함할 경우 **AND** 또는 **OR** 연산자로 연결해야 합니다. 동일한 레벨의 조건은 함께 평가됩니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자를 사용하면 이 연산자가 제어하는 레벨의 조건 중 하나 이상을 충족해야 합니다.

제한되지 않은 트래픽 프로파일

모니터링되는 전체 네트워크 세그먼트에 대해 데이터를 수집하는 트래픽 프로파일을 생성하려는 경우 다음 그림과 같이 조건 없는 매우 단순한 프로파일을 생성할 수 있습니다.



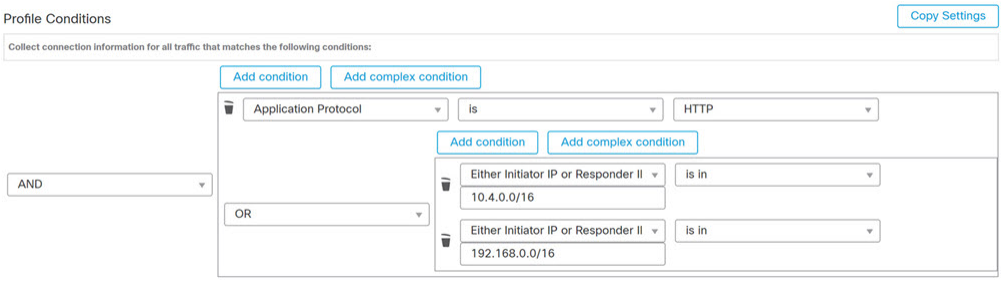
단순 트래픽 프로파일

프로파일을 제한하여 서브넷에 대해서만 데이터를 수집하게 하려는 경우 다음 그림과 같이 하나의 조건을 추가할 수 있습니다.

복합 트래픽 프로파일

다음 트래픽 프로파일에서는 2개의 조건이 **AND**로 연결되어 있습니다. 즉 이 트래픽 프로파일은 두 조건이 모두 참인 경우에만 연결 데이터를 수집합니다. 이 예에서는 IP 주소가 특정 서브넷에 있는 모든 호스트에 대해 HTTP 연결을 수집합니다.

반면 두 서브넷 중 하나의 HTTP 활동에 대한 연결 데이터를 수집하는 다음 트래픽 프로파일은 3개의 조건을 가지며, 그중 마지막은 복합 조건입니다.



논리적으로, 위 트래픽 프로파일은 다음과 같이 평가됩니다.

```
(A and (B or C))
```

항목	조건의 내용
A	Application Protocol Name(애플리케이션 프로토콜 이름)이 HTTP임
B	IP Address가 10.4.0.0/16에 있음
C	IP Address가 192.168.0.0/16에 있음

트래픽 프로필 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 검색 관리자

트래픽 프로파일 관리

활성 상태이며 온전한 트래픽 프로파일에 대해 작성한 규칙만 상관관계 정책 위반을 트리거할 수 있습니다. 각 트래픽 프로파일 옆에 있는 슬라이더는 프로파일이 활성 상태이며 데이터를 수집하고 있음을 나타냅니다. 진행 표시줄은 트래픽 프로파일의 학습 기간 상태를 보여줍니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 트래픽 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 선택된 트래픽 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 트래픽 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 프로파일 조건이 관련이 없는 도메인에 대한 이름이나 매니지드 디바이스 등의 정보를 표시하는 경우, 시스템은 상위 도메인의 프로파일은 표시하지 않습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Traffic Profiles(**트래픽 프로파일**)**을 클릭합니다.

단계 **2** 트래픽 프로파일 관리:

- Activate/Deactivate(활성화/비활성화) - 트래픽 프로파일을 활성화 또는 비활성화하려면 슬라이더를 클릭합니다. 트래픽 프로파일을 비활성화하면 관련 데이터가 삭제됩니다. 프로파일을 재활성화하면, 해당하는 PTW가 지나야 프로파일에 대해 작성한 규칙이 트리거됩니다.
- Create(생성) - 새 트래픽 프로파일을 생성하려면 **New Profile(**새 프로파일**)**을 클릭하고 트래픽 프로파일 설정, 2628 페이지에 설명된 대로 진행합니다. 복사 ( )를 클릭하여 기존 트래픽 프로파일의 복사본을 편집할 수도 있습니다.
- Delete(삭제) - 트래픽 프로파일을 삭제하려면 삭제( )를 클릭하고 선택을 확인합니다.
- Edit(편집) - 기존 트래픽 프로파일을 수정하려면 수정( )을 클릭하고 트래픽 프로파일 설정, 2628 페이지에 설명된 대로 진행합니다. 트래픽 프로파일이 활성 상태인 경우에는 이름과 설명만 바꿀 수 있습니다.
- Graph(그래프) - 트래픽 프로파일을 그래프로 보려면 그래프( )를 클릭합니다. 다중 도메인 구축의 경우, 그래프가 상관 없는 도메인 관련 정보를 표시한다면 상위 도메인에 속한 트래픽 프로파일의 그래프는 볼 수 없습니다.

트래픽 프로파일 설정

트래픽 프로파일을 상위 도메인에 제한하면 각각의 하위 리프 도메인에 있는 같은 유형의 트래픽을 집계하고 프로파일을 생성합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우, 도메인 사이의 트래픽에 대한 프로파일을 생성하면 예기치 않은 결과가 발생할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Traffic Profiles(**트래픽 프로파일**)**을 클릭합니다.

단계 **2** **New Profile(**새 프로파일**)**을 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)**을 입력하고, 필요한 경우 **Profile Description(**프로파일 설명**)**을 입력합니다.

단계 **4** 선택적으로, 트래픽 프로파일을 제한합니다.

- Copy Settings(설정 복사) - 기본 트래픽 프로파일의 설정을 복사하려면 **Copy Settings(**설정 복사**)**를 클릭하고 사용할 트래픽 프로파일을 선택한 다음 **Load(**불러오기**)**를 클릭합니다.
- Profile Conditions(프로파일 조건) - 추적한 연결이 제공하는 정보를 사용하여 트래픽 프로파일을 제한하려면, 트래픽 프로파일 조건 추가, 2629 페이지에 설명된 대로 진행합니다.
- Host Profile Qualification(호스트 프로파일 자격) - 추적한 호스트가 제공하는 정보를 사용하여 트래픽 프로파일을 제한하려면, 트래픽 프로파일에 호스트 프로파일 자격 추가, 2630 페이지에 설명된 대로 진행합니다.
- PTW(Profiling Time Window) - **Profiling Time Window**를 변경하려면 시간 단위를 입력하고 **hour(s)(**시간**)**, **day(s)(**일**)** 또는 **week(s)(**주**)**를 선택합니다.
- Sampling Rate(샘플링 속도) - **Sampling Rate(**샘플링 속도**)**를 분 단위로 선택합니다.
- Inactive Period(비활성 기간) - **Add Inactive Period(**비활성 기간 추가**)**를 클릭하고 드롭다운 목록을 사용하여 트래픽 프로파일이 비활성 상태를 유지할 시점과 방법을 지정합니다. 비활성 트래픽 프로파일은 상관관계 규칙을 트리거하지 않습니다. 트래픽 프로파일은 비활성 기간에 속하는 데이터는 프로파일 통계에 포함하지 않습니다.

단계 **5** 트래픽 프로파일 저장:

- 프로파일을 저장하고 즉시 데이터 수집을 시작하려면 **Save & Activate(**저장 및 활성화**)**를 클릭합니다.
- 프로파일을 활성화하지 않고 저장하려면 **Save(**저장**)**를 클릭합니다.

트래픽 프로파일 조건 추가

프로시저

단계 **1** Profile Conditions(프로파일 조건)의 트래픽 프로파일 편집기에서 추가할 각 조건에 대해 **Add condition(**조건 추가**)** 또는 **Add complex condition(**복합 조건 추가**)**을 클릭합니다. 수준이 같은 조건은 함께 평가됩니다.

- 연산자가 제어하는 레벨의 모든 조건을 충족해야 하는 경우에는 **AND**를 선택합니다.
- 연산자가 제어하는 레벨의 조건 중 하나만 충족하면 되는 경우에는 **OR**를 선택합니다.

단계 **2** 트래픽 프로파일 조건 구문, 2631 페이지 및 트래픽 프로파일 조건, 2625 페이지에 설명된 대로 각 조건에 대한 카테고리, 연산자, 값을 지정합니다.

is in 또는 **is not in**을 연산자로 선택하면, 트래픽 프로파일 조건에서 여러 값 사용, 2635 페이지에 설명된 대로 단일 조건에서 여러 값을 선택할 수 있습니다.

카테고리가 IP 주소를 나타낼 때 **is in** 또는 **is not in**을 연산자로 선택하면, IP 주소가 IP 주소 범위에서 *is in* 상태인지 *is not in* 상태인지를 지정할 수 있습니다.

예

다음 트래픽 프로파일은 특정 서브넷에 대한 정보를 수집합니다. 이 조건의 카테고리는 **Initiator/Responder IP**, 연산자는 **is in**, 값은 `10.4.0.0/16`입니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

트래픽 프로파일에 호스트 프로파일 자격 추가

프로시저

단계 **1** 트래픽 프로파일 편집기에서 **Add Host Profile Qualification(**호스트 프로파일 조건 추가**)**을 클릭합니다.

단계 **2** Host Profile Qualification(호스트 프로파일 자격)에서 추가할 각 조건에 대해 **Add condition(**조건 추가**)** 또는 **Add complex condition(**복합 조건 추가**)**을 클릭합니다. 수준이 같은 조건은 함께 평가됩니다.

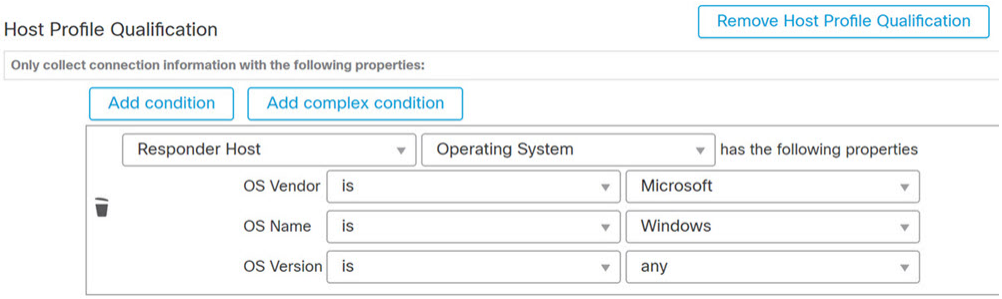
- 연산자가 제어하는 레벨의 모든 조건을 충족해야 하는 경우에는 **AND**를 선택합니다.
- 연산자가 제어하는 레벨의 조건 중 하나만 충족하면 되는 경우에는 **OR**를 선택합니다.

단계 **3** 트래픽 프로파일의 호스트 프로파일 자격 구문, 2632 페이지 및 트래픽 프로파일 조건, 2625 페이지에 설명된 대로 각 조건에 대한 호스트 유형, 카테고리, 연산자, 값을 지정합니다.

is in 또는 **is not in**을 연산자로 선택하면, 트래픽 프로파일 조건에서 여러 값 사용, 2635 페이지의 설명대로 단일 조건에서 여러 값을 선택할 수 있습니다.

예

다음 호스트 프로파일 자격은 탐지된 연결의 응답 호스트가 어떤 버전의 Microsoft Windows를 실행하는 경우에만 연결 데이터를 수집하도록 트래픽 프로파일을 제한합니다.



트래픽 프로파일 조건 구문

다음 표에서는 트래픽 프로파일 조건을 작성하는 방법을 설명합니다. 트래픽 프로파일 작성에 사용할 수 있는 연결 데이터는 트래픽 특성과 탐지 방법을 포함한 다양한 요소에 따라 달라집니다.

표 ***268:*** 트래픽 프로파일 조건 구문

다음을 선택하면...	연산자를 선택하고...
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
Client(클라이언트)	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트 카테고리를 하나 이상 선택합니다.
연결 유형	프로파일이 Firepower System 매니지드 디바이스로 모니터링하는 트래픽의 연결 데이터를 사용하는지, 내보낸 NetFlow 기록의 연결 데이터를 사용하는지를 선택합니다. 연결 유형을 지정하지 않는 경우 트래픽 프로파일은 둘 항목을 모두 포함합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	국가를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다.

다음을 선택하면...	연산자를 선택하고...
이니시에이터 IP, 응답자 IP 또는 이니시에이터/응답자 IP	IP 주소 또는 IP 주소 범위를 입력합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.
NetFlow 디바이스	데이터를 사용해 트래픽 프로파일을 생성할 NetFlow 엑스포터를 선택합니다.
응답자 포트/ICMP 코드	포트 번호 또는 ICMP 코드를 입력합니다.
보안 인텔리전스 카테고리	보안 인텔리전스 카테고리를 하나 이상 선택합니다. 트래픽 프로파일 조건에 대한 보안 인텔리전스 카테고리를 사용하려면, 액세스 컨트롤 정책에서 카테고리를 **Block**이 아닌 **Monitor**로 설정해야 합니다.
SSL 암호화된 세션	**Successfully Decrypted(**성공적으로 해독**)**를 선택합니다.
Transport Protocol(전송 프로토콜)	전송 프로토콜로 **`TCP`** 또는 **`UDP`**를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

연결 이벤트 필드 채우기 요구 사항, 2895 페이지
Firepower System IP 주소 규칙, 19 페이지

트래픽 프로파일의 호스트 프로파일 자격 구문

호스트 프로파일 자격 조건을 작성할 때 먼저 트래픽 프로파일을 제한하는 데 사용할 호스트를 선택해야 합니다. **Responder Host(**응답자 호스트**)** 또는 **Initiator Host(**이니시에이터 호스트**)** 중 하나를 선택할 수 있습니다. 호스트 역할 선택이 끝나면, 호스트 프로파일 자격 조건 작성을 계속 진행합니다.

NetFlow 기록을 사용하여 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. 예를 들어 호스트 입력 기능을 사용하여 제공하지 않는 한, 이러한 호스트에 대해서는 어떤 운영체제 데이터도 사용할 수 없습니다. 또한 트래픽 프로파일이 내보낸 NetFlow 기록에의 연결 데이터를 사용할 경우, NetFlow 기록은 연결의 어떤 호스트가 이니시에이터이고 어떤 호스트가 응답자인지에 대한 정보를 포함하지 않습니다. 시스템은 NetFlow 기록을 처리할 때 특정 알고리즘을 사용하여 각 호스트에서 사용 중인 포트 및 해당 포트가 잘 알려진 포트인지 여부를 기반으로 이 정보를 확인합니다.

암시된 클라이언트 또는 일반 클라이언트에 매칭하려면, 클라이언트에 응답하는 서버에서 사용하는 애플리케이션 프로토콜에 따라 호스트 프로파일 자격을 생성합니다. 연결의 initiator 또는 소스가 되는 호스트의 클라이언트 목록에서 어떤 애플리케이션 프로토콜 이름 다음에 클라이언트가 올 경우

그 클라이언트는 암시된 클라이언트일 수 있습니다. 즉 시스템은 탐지된 클라이언트 트래픽이 아니라 해당 클라이언트에 대해 애플리케이션 프로토콜을 사용하는 서버 응답 트래픽을 기반으로 클라이언트를 보고합니다.

예를 들어 시스템에서 호스트의 클라이언트로 **HTTPS client(HTTPS** 클라이언트**)**를 보고할 경우 **Responder Host(**응답자 호스트**)**에 대한 호스트 프로파일 자격을 생성하며, 여기서 **Application Protocol(**애플리케이션 프로토콜**)**은 **HTTPS**로 설정됩니다. 응답자 또는 목적지 호스트에서 보낸 HTTPS 서버 응답 트래픽에 따라 HTTPS 클라이언트가 일반 클라이언트로 보고되기 때문입니다.

표 ***269:*** 호스트 프로파일 자격 구문

다음을 선택하면...	연산자를 선택하고...
애플리케이션 프로토콜 >애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 >애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
애플리케이션 프로토콜 >프로토콜	프로토콜을 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트 > 클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 > 클라이언트 버전	클라이언트 버전을 입력합니다.
클라이언트 카테고리	클라이언트 카테고리를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다.
하드웨어	모바일 디바이스 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 `iPhone`을 입력합니다.
Host Criticality(호스트 심각도)	호스트 중요도를 선택합니다.
Host Type(호스트 유형)	호스트 유형을 하나 이상 선택합니다. 일반 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IOC 태그	IOC 태그를 하나 이상 선택합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC 주소 > MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다.

다음을 선택하면...	연산자를 선택하고...
MAC 주소 > MAC 유형	MAC 유형이**ARP/DHCP Detected**인지, 즉 다음인지를 선택합니다. • 시스템이 MAC 주소가 호스트에 속한 것으로 명확하게 확인함(**is ARP/DHCP Detected**) • 디바이스와 호스트 간에 라우터가 있다는 등의 이유로, 시스템이 MAC 주소가 있는 다양한 호스트를 확인함(**is not ARP/DHCP Detected**) • MAC 유형이 올바르지 않음(**is any**)
MAC 벤더	호스트에서 사용하는 하드웨어의 MAC 벤더 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
NETBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
Network Protocol(네트워크 프로토콜)	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
운영체제 > OS 벤더	운영체제 벤더 이름을 하나 이상 선택합니다.
운영체제 > OS 이름	운영체제 이름을 하나 이상 선택합니다.
운영체제 > OS 버전	운영체제 버전을 하나 이상 선택합니다.
Transport Protocol(전송 프로토콜)	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
VLAN ID	호스트의 VLAN ID 번호를 입력합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.
웹 애플리케이션	웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

다음을 선택하면...	연산자를 선택하고...
사용 가능한 모든 호스트 속성(기본 규정준수 화이트리스트 호스트 속성 포함)	선택하는 호스트 속성의 유형에 따라 알맞은 값을 지정합니다. • 호스트 속성 유형이 Integer(정수)일 경우 그 특성에 대해 정의된 범위의 정수 값을 입력합니다. • 호스트 속성 유형이 Text(텍스트)일 경우 텍스트 값을 입력합니다. • 호스트 속성 유형이 List(목록)일 경우 유효한 목록 문자열을 선택합니다. • 호스트 속성 유형이 URL일 경우 URL 값을 입력합니다.

트래픽 프로파일 조건에서 여러 값 사용

조건을 작성할 때 조건 구문상 드롭다운 목록의 값 선택이 가능할 경우, 대개는 목록에서 여러 값을 사용할 수 있습니다.

예를 들어 호스트가 UNIX의 특정 버전을 실행해야한다는 조건을 호스트 프로파일 자격으로 트래픽 프로파일에 추가하려는 경우, 여러 조건을 OR 연산자로 연결하는 대신 다음 절차를 사용합니다.

프로시저

단계 **1** 트래픽 프로파일 또는 호스트 프로파일 자격 조건을 작성할 때, **is in** 또는 **is not in**을 연산자로 선택합니다.
드롭다운 목록이 텍스트 필드로 바뀝니다.

단계 **2** 텍스트 필드의 아무 곳이나 클릭하거나 **Edit(**편집**)** 링크를 클릭합니다.

단계 **3** **Available(**사용 가능**)**에서 여러 값을 선택합니다.

단계 **4** 오른쪽 화살표를 클릭하여 선택한 항목을 **Selected**로 옮깁니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

107 장

치료

다음 주제는 교정 설정 관련 정보를 제공합니다.

- 교정 요구 사항 및 사전 요건, 2637 페이지
- 교정 소개, 2637 페이지
- 교정 모듈 관리, 2646 페이지
- 교정 인스턴스 관리, 2646 페이지
- 단일 교정 모듈 인스턴스 관리, 2647 페이지

교정 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 검색 관리자

교정 소개

교정은 Firepower System이 상관관계 위반에 대한 응답으로 실행하는 프로그램입니다.

교정을 실행하면, 시스템은 교정 상태 이벤트를 생성합니다. 교정 상태 이벤트는 교정 이름, 상관관계 정책 및 이를 트리거한 규칙, 종료 상태 메시지 등의 상세정보를 포함합니다.

시스템은 여러 교정 모듈을 지원합니다.

- Cisco ISE ANC(Adaptive Network Control) - 상관관계 정책 위반과 관련된 ISE 설정 ANC 정책을 적용하거나 지웁니다.
- Cisco IOS Null Route - 상관관계 정책 위반과 관련된 호스트 또는 네트워크로 전송된 트래픽을 차단(Cisco IOS 버전 12.0 이상 필수)
- Nmap Scanning(Nmap 스캐닝) - 호스트를 스캔해 실행 중인 운영체제와 서버 확인
- Set Attribute Value(속성 값 설정) - 상관관계 정책 위반과 관련된 호스트에서 호스트 속성 설정

팁 다른 작업을 수행하는 맞춤형 모듈을 설치할 수 있습니다(*Firepower System Remediation API* 설명서 참조).

교정 구현

교정을 구현하려면, 먼저 선택한 모듈에 대한 인스턴스를 하나 이상 만들어야 합니다. 모듈당 여러 인스턴스를 만들 수 있으며, 이때 각 인스턴스는 저마다 다르게 설정됩니다. 예를 들어 Cisco IOS Null Route 교정 모듈을 사용하여 여러 라우터와 통신하려면, 해당 모듈이 인스턴스 다수를 설정해야 합니다.

그런 다음 정책 위반 시 수행할 작업을 설명하는 여러 교정을 각 인스턴스에 추가합니다.

마지막으로, 교정을 상관관계 정책에 있는 규칙과 연결해 시스템이 상관관계 정책 위반에 대한 응답으로 교정을 실행하게 합니다.

교정 및 멀티 테넌시

다중 도메인 구축의 경우에는, 어떤 도메인 레벨에서도 맞춤형 교정 모듈을 설치할 수 있습니다. 시스템 제공 모듈은 Global(전역) 도메인에 속합니다.

상위 도메인에서 생성한 인스턴스에는 교정을 추가할 수 없지만, 비슷하게 설정한 인스턴스를 현재 도메인에 생성하고 해당 인스턴스에 교정을 추가할 수는 있습니다. 상위 도메인에서 생성한 교정을 상관관계 응답으로 사용할 수도 있습니다.

관련 항목

Firepower Management Center 알림 응답, 2681 페이지
Nmap 스캐닝, 2414 페이지
규칙 및 화이트 리스트에 응답 추가, 2586 페이지

Cisco IOS Null Route 교정

Cisco IOS Null Route 교정 모듈을 이용하면 Cisco의 “null route” 명령을 사용하여 IP 주소 또는 주소 범위를 차단할 수 있습니다. 이렇게 하면 라우터의 NULL 인터페이스로 라우팅하여 호스트나 네트워크에 전송한 모든 트래픽이 삭제됩니다. 위반 호스트 또는 네트워크에서 전송된 트래픽은 차단되지 않습니다.

참고 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

주의 Cisco IOS 교정이 활성화되는 경우에는 시간 초과 기간이 없습니다. IP 주소 또는 네트워크를 차단 해제하려면, 라우팅 변경사항을 라우터에서 수동으로 삭제해야 합니다.

Cisco IOS 라우터에 대한 교정 설정

참고 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

주의 Cisco IOS 교정이 활성화되는 경우에는 시간 초과 기간이 없습니다. IP 주소 또는 네트워크를 차단 해제하려면, 라우팅 변경사항을 라우터에서 수동으로 삭제해야 합니다.

시작하기 전에

- Cisco 라우터가 Cisco IOS 12.0 이상을 실행 중인지 확인합니다.
- 라우터에 대한 레벨 15 관리 액세스가 있는지 확인합니다.

프로시저

단계 **1** Cisco 라우터 또는 IOS 소프트웨어와 함께 제공된 문서에 설명된 대로 Cisco 라우터에서 텔넷을 활성화합니다.

단계 **2** Firepower Management Center에서, 사용할 각 Cisco IOS 라우터에 대해 Cisco IOS Null Route 인스턴스를 추가합니다(Cisco IOS 인스턴스 추가, 2640 페이지 참조).

단계 **3** 상관관계 정책이 위반될 때 라우터에서 이끌어낼 응답의 유형을 기반으로 각 인스턴스에 대한 교정을 생성합니다.

- Cisco IOS Block Destination 교정 추가, 2641 페이지
- Cisco IOS Block Destination Network 교정 추가, 2641 페이지
- Cisco IOS Block Source 교정 추가, 2642 페이지
- Cisco IOS Block Source Network 교정 추가, 2643 페이지

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 화이트 리스트에 응답 추가, 2586 페이지를 참조하십시오.

Cisco IOS 인스턴스 추가

여러 라우터로 교정을 전송하려는 경우 각 라우터에 대해 개별 인스턴스를 생성합니다.

시작하기 전에

- Cisco 라우터 또는 IOS 소프트웨어와 함께 제공된 문서에 설명된 대로 Cisco 라우터에서 텔넷 액세스를 설정합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **Cisco IOS Null Route**를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **4** 교정에 대해 사용하려는 Cisco IOS 라우터의 IP 주소를 **Router IP** 필드에 입력합니다.

단계 **5** 라우터에 대한 텔넷 사용자 이름을 **Username(**사용자 이름**)** 필드에 입력합니다. 이 사용자는 라우터에 대한 레벨 15 관리 액세스 권한이 있어야 합니다.

단계 **6** 텔넷 사용자의 사용자 비밀번호를 **Connection Password(**연결 비밀번호**)** 필드에 입력합니다.

단계 **7** 텔넷 사용자의 활성 비밀번호를 **Enable Password(**비밀번호 활성화**)** 필드에 입력합니다. 이 비밀번호는 라우터의 특권 모드로 들어가기 위해 사용되는 비밀번호입니다.

단계 **8** 교정에서 제외할 IP 주소 또는 범위를 한 줄에 하나씩 **White List(**화이트리스트**)** 필드에 입력합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **9** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- Cisco IOS Block Destination 교정 추가, 2641 페이지, Cisco IOS Block Destination Network 교정 추가, 2641 페이지, Cisco IOS Block Source 교정 추가, 2642 페이지, Cisco IOS Block Source Network 교정 추가, 2643 페이지에 설명된 대로 상관관계 정책이 사용할 특정 교정을 추가합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

Cisco IOS Block Destination 교정 추가

Cisco IOS Block Destination 교정은 라우터에서 상관관계 정책 위반과 관련된 목적지 호스트로 전송된 트래픽을 차단합니다. 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 2640 페이지에 설명된 대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 보기 ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Destination(**목적지 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 화이트 리스트에 응답 추가, 2586 페이지를 참조하십시오.

Cisco IOS Block Destination Network 교정 추가

Cisco IOS Block Destination Network 교정은 라우터에서 상관관계 정책 위반과 관련된 목적지 호스트의 네트워크로 전송된 트래픽을 차단합니다. 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 2640 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 2 교정을 추가하려는 인스턴스 옆에 있는 보기 ( )를 클릭합니다.

단계 3 **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Destination Network(**목적지 네트워크 차단**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 4 **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 5 **Netmask(**넷마스크**)** 필드에 서브넷 마스크를 입력하거나 CIDR 표기법을 사용하여 트래픽을 차단할 네트워크를 설명합니다.

예를 들어 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면 (권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과 `10.1.1.30` 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나, `32`를 입력하거나, `255.255.255.255`를 입력합니다.

단계 6 **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 화이트 리스트에 응답 추가, 2586 페이지를 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

Cisco IOS Block Source 교정 추가

Cisco IOS Block Source 교정은 라우터에서 상관관계 정책 위반과 관련된 소스 호스트로 전송된 트래픽을 차단합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 2640 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 보기 ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Source(**소스 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 화이트 리스트에 응답 추가, 2586 페이지를 참조하십시오.

Cisco IOS Block Source Network 교정 추가

Cisco IOS Block Source Network 교정은 라우터에서 상관관계 정책 위반과 관련된 소스 호스트의 네트워크로 전송된 트래픽을 차단합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 2640 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 보기 ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Source Network(**소스 네트워크 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** **Netmask(**넷마스크**)** 필드에 서브넷 마스크를 입력하거나 트래픽을 차단할 네트워크를 설명하는 CIDR 표기법을 입력합니다.

예를 들어 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면 (권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과

10.1.1.30 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나, 32를 입력하거나, 255.255.255.255를 입력합니다.

단계 **6** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 화이트 리스트에 응답 추가, 2586 페이지를 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

Nmap 스캔 교정

Firepower System은 네트워크 탐색 및 보안 감사를 위한 오픈 소스 활성 스캐너인 Nmap™과 통합됩니다. Nmap 교정을 사용하여 상관관계 정책 위반에 응답할 수 있으며, 이 경우 Nmap 스캔 교정이 트리거됩니다.

Nmap 스캔에 대한 자세한 정보는 Nmap 스캐닝, 2414 페이지 섹션을 참조하십시오.

속성 값 교정 설정

트리거링 이벤트가 발생한 호스트에서 호스트 속성 값을 설정하여 상관관계 정책 위반에 응답할 수 있습니다. 텍스트 호스트 속성의 경우에는 이벤트의 설명을 속성 값으로 사용할 수 있습니다.

세트 속성값 교정 구성

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 속성값 설정 인스턴스 추가, 2645 페이지에 설명된 대로 세트 속성 인스턴스를 생성합니다.

단계 **3** 속성값 설정 교정 추가, 2645 페이지에 설명된 대로 세트 속성 교정을 추가합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 화이트 리스트에 응답 추가, 2586 페이지를 참조하십시오.

관련 항목

사전 정의된 호스트 속성, 3019 페이지
사용자 정의 호스트 속성, 3020 페이지

속성값 설정 인스턴스 추가

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **Set Attribute Value(**속성 값 설정**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **4** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- 속성값 설정 교정 추가, 2645 페이지에 설명된 대로 속성 설정 교정을 생성합니다.

속성값 설정 교정 추가

Set Attribute Value(속성 값 설정) 교정은 상관관계 정책 위반과 관련된 호스트에서 호스트 속성을 설정합니다. 설정할 각 속성값에 대한 교정을 생성합니다. 텍스트 속성의 경우에는 트리거링 이벤트의 설명을 속성 값으로 사용할 수 있습니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- 속성값 설정 인스턴스 추가, 2645 페이지에 설명된 대로 속성 설정 인스턴스를 생성합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 보기 ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Set Attribute Value(**속성값 설정**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** 소스 및 목적지 데이터가 있는 이벤트에 대한 응답으로 이 교정을 사용하려면, **Update Which Host(s) From Event(**이벤트의 호스트 업데이트**)** 옵션을 선택합니다.

단계 **6** 텍스트 속성의 경우에는 **Use Description From Event For Attribute Value(**속성값으로 이벤트의 설명 사용**)** 여부를 지정합니다.

- 이벤트의 설명을 속성값으로 사용하려면 **On(**설정**)**을 클릭하고 설정할 **Attribute Value(**속성값**)**를 입력합니다.
- 교정에 대한 **Attribute Value(**속성값**)** 설정을 속성값으로 사용하려면 **Off(**해제**)**를 선택합니다.

단계 **7** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 화이트 리스트에 응답 추가, 2586 페이지를 참조하십시오.

교정 모듈 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에 설치된 Nmap 교정 모듈을 표시하며, 이러한 모듈은 삭제할 수 있습니다. 상위 도메인에 설치된 모듈도 표시되지만, 이러한 모듈은 수정할 수 없습니다. 하위 도메인의 교정 모듈을 관리하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Modules(**모듈**)**을(를) 선택합니다.

단계 **2** 교정 모듈 관리:

- Configure(설정) - 모듈에 대한 Module Detail(모듈 상세정보) 페이지를 확인하고 모듈의 인스턴스와 교정을 설정하려면, 보기( )을 클릭합니다. 다중 도메인 구축의 경우에는 Module Detail(모듈 상세정보) 페이지를 사용하여 상위 도메인에 설치된 모듈의 현재 도메인에 있는 인스턴스를 추가, 삭제 또는 편집할 수 없습니다. 대신 Instances(인스턴스) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**)를 사용하십시오(교정 인스턴스 관리, 2646 페이지 참조).
- Delete(삭제) - 사용하지 않은 맞춤형 모듈을 삭제하려면 삭제( )을 클릭합니다. 시스템 제공 모듈은 삭제할 수 없습니다.
- Install(설치) - 맞춤형 모듈을 설치하려면 **Choose File(**파일 선택**)**을 클릭하고, 모듈을 찾은 다음 **Install(**설치**)**을 클릭합니다. 자세한 내용은 *Firepower System Remediation API* 설명서를 참조하십시오.

교정 인스턴스 관리

Instances(인스턴스) 페이지는 모든 교정 모듈을 대상으로, 설정된 인스턴스를 모두 열거합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 교정 인스턴스를 표시하며 이러한 인스턴스는 편집할 수 있습니다. 상위 도메인에서 생성된 인스턴스도 표시되지만, 이러한 인스턴스는 편집할 수 없습니다. 하위 도메인의 교정 인스턴스를 관리하려면 해당 도메인으로 전환하십시오.

상위 도메인에서 생성한 인스턴스에는 교정을 추가할 수 없지만, 비슷하게 설정한 인스턴스를 현재 도메인에 생성하고 해당 인스턴스에 교정을 추가할 수는 있습니다. 상위 도메인에서 생성한 교정을 상관관계 응답으로 사용할 수도 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정 인스턴스 관리:

- Add(추가) - 인스턴스를 추가하려면 인스턴스를 추가할 교정 모듈을 선택하고 **Add(**추가**)**를 클릭합니다. 시스템 제공 모듈의 경우에는 다음을 참조하십시오.
  - Cisco IOS 인스턴스 추가, 2640 페이지
  - Nmap 스캔 인스턴스 추가, 2427 페이지
  - 속성값 설정 인스턴스 추가, 2645 페이지

  맞춤형 모듈 추가 관련 도움이 필요하다면 해당 모듈의 설명서(존재하는 경우)를 참조하십시오.
- Configure(구성) - 인스턴스 상세정보를 구성하고 교정을 인스턴스에 추가하려면 보기 ( )를 클릭합니다.
- Delete(삭제) - 사용하지 않는 인스턴스를 삭제하려면 삭제( )를 클릭합니다.

단일 교정 모듈 인스턴스 관리

Module Detail(모듈 상세정보) 페이지는 특정 교정 모듈에 대해 설정된 인스턴스와 교정을 모두 표시합니다.

다중 도메인 구축의 경우에는, 현재 도메인과 상위 도메인에 설치된 교정 모듈에 대한 Module Detail(모듈 상세정보) 페이지에 액세스할 수 있습니다. 그러나 Module Detail(모듈 상세정보) 페이지를 사용하여 상위 도메인에 설치된 모듈의 현재 도메인에 있는 인스턴스를 추가, 삭제 또는 편집할 수는 없습니다. 대신 Instances(인스턴스) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**)를 사용하십시오(교정 인스턴스 관리, 2646 페이지 참조).

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Modules(**모듈**)**을(를) 선택합니다.

단계 **2** 관리할 인스턴스가 있는 교정 모듈 옆에 있는 보기 ( )를 클릭합니다.

단계 **3** 교정 인스턴스 관리:

- Add(추가) - 인스턴스를 추가하려면 **Add(**추가**)**를 클릭합니다. 시스템 제공 모듈의 경우에는 다음을 참조하십시오.
  - Cisco IOS 인스턴스 추가, 2640 페이지
  - Nmap 스캔 인스턴스 추가, 2427 페이지
  - 속성값 설정 인스턴스 추가, 2645 페이지

  맞춤형 모듈을 위한 인스턴스 추가 관련 도움이 필요하다면 해당 모듈의 설명서(존재하는 경우)를 참조하십시오.
- Configure(구성) - 인스턴스 상세정보를 구성하고 교정을 인스턴스에 추가하려면 보기 ( )를 클릭합니다.
- Delete(삭제) - 사용하지 않는 인스턴스를 삭제하려면 삭제( )를 클릭합니다.

XXII 부

보고 및 알림

- 보고서 작업, 2651 페이지
- 알림 응답을 사용한 외부 알림, 2681 페이지
- 침입 이벤트에 대한 외부 알림, 2691 페이지

108 장

보고서 작업

다음 주제에서는 Firepower System의 보고서를 이용하는 방법을 설명합니다.

- 보고서 요구 사항 및 사전 요건, 2651 페이지
- 보고서 소개, 2651 페이지
- 위험 보고서, 2652 페이지
- Introduction to Reports(보고서 소개), 2653 페이지
- 생성된 보고서 작업 정보, 2675 페이지
- 보고 기록, 2679 페이지

보고서 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 유지 보수 사용자 (위험 보고서만 해당)
- 보안 분석가

보고서 소개

Firepower System은 두 가지 유형의 보고서를 제공합니다.

- 위험 보고서, 2652 페이지 - 네트워크에서 발견한 위험에 대한 개괄적인 요약

- Introduction to Reports(보고서 소개), 2653 페이지 - Firepower 의 모든 요소에 대한 상세하고 맞춤형 가능한 보고서

위험 보고서

위험 보고서는 조직에서 발견한 리스트에 대한 휴대 가능하며, 개괄적이고, 쉽게 해석할 수 있는 요약입니다. 이러한 보고서를 이용하면 위험 영역 관련 정보와 이러한 위험 해결을 위한 권장사항을 사용자 시스템에 대한 액세스 권한이 없으며, 네트워크 보안 전문 지식이 없을 수도 있는 사람과 공유할 수 있습니다. 보고서는 네트워크 보안에 대한 투자 영역 관련 논의를 촉진할 용도로 제작됩니다.

위험 보고서 생성, 보기 및 인쇄

표준 보고서용 템플릿은 위험 보고서에는 적용되지 않습니다.

보고서는 현재 도메인에만 적용됩니다.

각각의 위험 보고서는 HTML 파일을 생성합니다.

위험 보고서 생성을 예약하는 방법은 보고서 생성 자동화, 254 페이지 섹션을 참조하십시오.

시작하기 전에

- 요약할 위험을 탐지하도록 시스템이 설정돼 있는지 확인하십시오.
- 보고서를 이메일로 전송하고 싶지만 아직 Relay Host(릴레이 호스트)를 설정하지 않았다면 , 지금 설정하십시오. 자세한 내용은 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지를 참조하십시오.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 원하는 보고서의 **Generate Report(**보고서 생성**)**를 클릭합니다.

단계 **4** 정보를 입력합니다.

- Input Parameters(입력 파라미터) 섹션에 입력하는 정보는 보고서의 제목 페이지에 표시됩니다. 이러한 필드는 입력하지 않아도 됩니다.

단계 **5** **Generate(**생성**)**를 클릭합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 위험 보고서를 보고, 다운로드하고, 옮기고 삭제하는 방법은 생성된 보고서 작업 정보, 2675 페이지 섹션을 참조하십시오.
- 지원되는 대부분의 브라우저에서 위험 보고서를 PDF 형식으로 인쇄할 수 있습니다. 최상의 결과를 얻으려면 브라운저의 인쇄 또는 인쇄 미리보기 설정에서 배경색과 이미지를 활성화하고, 원한다면 머리글과 바닥글도 활성화하십시오. 지원되는 페이지 크기는 A4 및 US 레터입니다.

Introduction to Reports(보고서 소개)

Firepower System은 Firepower Management Center에 나타나는 대시보드 또는 이벤트 보기와 함께 다중 섹션의 보고서를 빠르고 쉽게 생성할 수 있는 유연한 보고 시스템을 제공합니다. 맞춤형 보고서를 처음부터 디자인할 수도 있습니다.

보고서는 전달할 내용이 포함된 PDF, HTML 또는 CSV 형식의 문서 파일입니다. 보고서 템플릿은 보고서 및 보고서 섹션에 대한 데이터 검색과 형식을 지정합니다. Firepower System에는 보고서 템플릿의 디자인을 자동화하는 강력한 보고서 디자이너가 포함되어 있습니다. 웹 인터페이스에 표시되는 이벤트 보기 테이블 또는 대시보드 그래픽의 내용을 복제할 수 있습니다.

보고서 템플릿을 필요한 만큼 작성할 수 있습니다. 각 보고서 템플릿은 보고서의 개별 섹션을 정의하며, 보고서의 내용을 생성하는 데이터베이스 검색은 물론 표시 형식(테이블, 차트, 상세 보기 등)과 시간 프레임도 지정합니다. 템플릿은 또한 커버 페이지와 목차, 문서 페이지에 머리글과 바닥글 포함(PDF 형식의 보고서에서만 사용 가능) 여부 등의 문서 속성도 지정합니다. 단일 설정 패키지 파일로 보고서 템플릿을 내보내고, 다른 Firepower Management Center에서 재사용하기 위해 가져올 수 있습니다.

유용성 확장을 위해 템플릿에 입력 파라미터를 포함할 수 있습니다. 입력 파라미터를 사용하면 동일한 보고서를 원하는 형태로 변형할 수 있습니다. 입력 파라미터로 보고서를 생성할 경우 생성 과정 중에 각 입력 파라미터의 값을 입력하라는 프롬프트가 표시됩니다. 입력하는 값은 1회 기반으로 보고서 내용을 제한합니다. 예를 들어 침입 이벤트 보고서를 생성하는 검색의 목적지 IP 필드에 입력 파라미터를 둘 수 있습니다. 보고서 생성 시 목적지 IP 주소를 입력하라는 프롬프트가 표시될 때 부서의 네트워크 세그먼트를 지정할 수 있습니다. 그러면 생성된 보고서에는 해당 특정 부서와 관련된 정보만 포함됩니다.

설계 보고서 정보

보고서 템플릿

보고서 템플릿을 사용하면 각 보고서 섹션에서 데이터의 내용과 형식을 정의하는 것은 물론, 보고서 파일의 문서 특성(커버 페이지, 목차, 페이지 머리글과 바닥글)도 정의할 수 있습니다. 보고서를 생성한 후 템플릿은 삭제될 때까지 계속 재사용 가능합니다.

보고서에는 하나 이상의 정보 섹션이 포함되어 있습니다. 각 섹션의 형식(텍스트, 테이블 또는 차트)을 개별적으로 선택합니다. 한 섹션에 대해 선택한 형식은 포함 가능한 데이터를 제한할 수 있습니다.

예를 들어 원 그래프 형식을 사용하는 특정 테이블에는 시간 기반 정보를 표시할 수 없습니다. 최적의 상태로 표시하기 위해 언제든지 섹션의 형식 또는 데이터 기준을 변경할 수 있습니다.

사전 정의된 이벤트 보기를 기반으로 보고서의 초기 디자인을 작성할 수도 있고, 정의된 대시보드, 워크플로 또는 요약에서 내용을 가져와 디자인을 시작할 수도 있습니다. 빈 템플릿에서 시작하여 하나씩 섹션을 추가하고 특성을 정의할 수도 있습니다.

참고 다중 도메인 구축에서는 상위 도메인에 속한 보고서 템플릿을 볼 수는 있지만 편집할 수는 없습니다. 이러한 템플릿에서 보고서를 생성하려면 현재 도메인에 템플릿을 복사해야 합니다.

보고서 템플릿 필드

다음 표에서는 보고서 템플릿의 섹션을 작성하는 데 사용할 수 있는 필드를 설명합니다. 섹션 유형에 따라 사용할 수 없는 필드도 있습니다. 섹션 형식을 선택하면 시스템은 적절한 필드를 표시합니다.

필드 이름	섹션 유형	정의
형식	해당 없음	섹션 데이터의 형식을 선택합니다. 막대그래프( ): 선택한 변수의 수량을 비교합니다. 선형 차트( ): 선택한 변수의 시간에 따른 추세/변경 사항을 표시합니다. 시간 기반 테이블에만 사용할 수 있습니다. 원도표( ): 선택한 각 변수를 전체의 비율로 표시합니다. 수량이 0인 변수는 차트에서 삭제됩니다. 매우 소량의 항목들은 **Other(**기타**)**라는 카테고리로 묶입니다. 테이블 보기( ): 각 레코드의 속성값을 표시합니다. 요약 또는 통계 데이터에는 사용할 수 없습니다. 상세정보 보기 ( ): 패킷(침입 이벤트의 경우) 및 호스트 프로파일(호스트 이벤트의 경우) 등 특정 이벤트와 관련된 복잡한 개체 데이터를 표시합니다. 이 형식은 해당 개체와 관련된 특정 이벤트 유형에 대해서만 사용할 수 있습니다. 요청 수가 많을 경우 출력 성능이 저하될 수 있습니다.
표	All(모두)	섹션 데이터를 추출하는 테이블을 선택합니다.
프리셋	All(모두)	사전 정의된 검색입니다. 새 검색을 정의할 때 검색 기준을 시작할 적절한 프리셋을 선택합니다.
Search(검색) 또는 Filter(필터)	All(모두)	대부분의 테이블에서 사전 정의 또는 저장된 **Search(**검색**)**를 사용하여 보고서를 제한할 수 있습니다. 또한 수정( )을 클릭하여 새 검색을 생성할 수 있습니다. Application Statistics(애플리케이션 통계) 테이블에서는 사용자 정의 애플리케이션 **Filter(**필터**)**를 이용해 보고서를 제한할 수 있습니다.

필드 이름	섹션 유형	정의
X축	막대 그래프 라인 차트 원형 차트	선택한 차트의 X축에 대해 사용할 수 있는 데이터입니다. 선 그래프의 경우 X축 값은 항상 **Time(**시간**)**입니다. 막대 및 원도표의 경우 X축 값으로 **Time(**시간**)**을 선택할 수 없습니다.
Y축	막대 그래프 라인 차트 원형 차트	선택한 차트의 Y축에 대해 사용할 수 있는 데이터입니다.
섹션 설명	All(모두)	섹션의 검색 데이터 앞에 오는 설명 텍스트입니다. 텍스트 및 입력 파라미터의 조합을 입력합니다. 새로운 섹션의 기본값은 `$<Time Window>` 및 `$<Constraints>`입니다.
기간	All(모두)	섹션에 나타나는 데이터의 시간 창입니다. 섹션에서 시간 기반 테이블을 검색하는 경우, 보고서의 전역 시간 창을 상속하는 확인란을 선택할 수 있습니다. 또는 섹션에 대한 특정 시간 창을 설정할 수 있습니다.
최대 결과 수	테이블 보기 세부 정보 보기	포함할 일치하는 레코드의 최대 수입니다.
결과	막대 그래프 원형 차트	**Top(**위쪽**)** 또는 **Bottom(**아래쪽**)**을 선택하고 차트 작성에 사용할 일치하는 레코드의 수를 입력합니다.
색상	막대 그래프 라인 차트	섹션에서 그래프로 표시하는 데이터의 색상입니다.

보고서 템플릿 생성

보고서 템플릿은 섹션의 프레임워크이며, 각각은 자체 데이터베이스 쿼리에서 독립적으로 작성됩니다.

새 보고서 템플릿은 새 템플릿을 만들거나, 기존 템플릿을 이용하거나, 이벤트 보기의 템플릿을 기반으로 하거나, 대시보드 또는 워크플로를 가져와 작성합니다.

기존 보고서 템플릿을 복사하지 않으려는 경우 완전히 새로운 템플릿을 생성할 수 있습니다. 템플릿 생성의 첫 단계는 섹션을 추가하고 형식을 지정할 수 있는 프레임워크를 생성하는 것입니다. 그런 다음 원하는 순서대로 개별 템플릿 섹션을 디자인하고 보고서 문서의 속성을 설정합니다.

각 템플릿 섹션은 검색 또는 필터에 의해 생성된 데이터 집합으로 구성되며, 표시 모드를 결정하는 형식 사양(테이블, 원도표 등)을 가지고 있습니다. 출력에 포함하려는 데이터 레코드의 필드 및 표시할 레코드의 시간 프레임과 수를 선택하여 섹션 내용을 더 자세히 지정할 수 있습니다.

참고 윈도표 색상 등 출력 특성과 열 선택을 확인하려면 섹션 미리 보기 유틸리티를 사용할 수 있지만, 구성한 검색의 정확성이 신뢰할 수 있는 수준으로 표시되지는 않습니다.

템플릿에서 생성하는 보고서에는 커버 페이지, 머리글과 바닥글, 페이지 번호 지정 등 모든 섹션 및 제어 기능에 해당하는 몇 가지 문서 속성이 있습니다.

문서 형식으로 CSV를 선택한 경우에는 문서 속성을 설정하지 않아도 됩니다.

기존 템플릿 중에서 좋은 모델을 찾은 경우 해당 템플릿을 복사하고 특성을 수정하여 새 보고서 템플릿을 생성할 수 있습니다. Cisco에서는 사전 정의 보고서 템플릿 집합도 제공하며, 템플릿 목록의 **Reports Tab(**보고서 탭**)**에서 확인할 수 있습니다.

이벤트 보기에서는 보고서 템플릿을 만들고 필요에 맞게 수정할 수 있습니다. 섹션을 더 추가하고, 포함된 섹션을 자동으로 수정하고, 섹션을 삭제할 수 있습니다.

대시보드, 워크플로 및 통계 요약을 가져와서 새 보고서를 빠르게 생성할 수 있습니다. 가져오기를 수행하면 대시보드 및 워크플로의 각 이벤트 보기에 각 위젯 그래픽에 대한 섹션이 생성됩니다. 가장 중요한 정보에 집중할 수 있도록 불필요한 섹션을 모두 삭제할 수 있습니다.

맞춤형 보고서 템플릿 생성

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**를 선택합니다.

단계 **2** **Report Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** **Create Report Template(**보고서 템플릿 생성**)**을 클릭합니다.

단계 **4** **Report Title(**보고서 제목**)** 필드에 새 템플릿의 이름을 입력합니다.

단계 **5** 보고서 제목에 입력 매개변수를 추가하려면 매개변수의 값이 나타나야 할 제목에 커서를 두고 입력 입력 매개변수(+)를 클릭합니다.

단계 **6** Report Sections(보고서 섹션) 제목 표시줄 아래에 있는 추가 집합을 사용하여 필요한 만큼 섹션을 삽입합니다.

단계 **7** 보고서 템플릿 설정, 2659 페이지에 설명된 대로 섹션 콘텐츠를 설정합니다.

팁 섹션 창 아래에 있는 **Preview(**미리보기**)**를 클릭하면 선택한 열 배치나 그래픽 형식을 볼 수 있습니다.

단계 **8** **Advanced(**고급**)**를 클릭하고 보고서 템플릿의 문서 속성, 2668 페이지에 설명된 대로 PDF와 HTML 보고서의 속성을 설정합니다 .

단계 **9** **Save(**저장**)**를 클릭합니다.

오류가 표시되는 경우에는 각 섹션의 결과 값 옆에 노란색 삼각표가 있는지 확인하십시오. 삼각형이 보인다면 다음 중 하나를 수행합니다.

- 노란색 화살표가 있는 각 필드에서 삼각형 위에 마우스 포인터를 올리고 결과 값을 표시되는 값으로 줄입니다.
- **Generate(**생성**)**를 클릭하고 PDF 이외의 출력 형식을 포함합니다.

기존 템플릿에서 보고서 템플릿 생성

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**를 선택합니다.

단계 **2** **Report Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 복사할 보고서 템플릿 옆에 있는 아이콘(복사 ( ))을 클릭합니다.

단계 **4** **Report Title(**보고서 제목**)** 필드에 이름을 입력합니다.

단계 **5** 필요한 대로 템플릿을 변경합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이벤트 보기에서 보고서 템플릿 생성

프로시저

단계 **1** 보고서에 표시할 이벤트를 이용해 이벤트 보기를 채웁니다.

- 확인할 이벤트를 이벤트 검색을 사용하여 정의합니다.
- 이벤트 보기에 적절한 이벤트가 표시될 때까지 워크플로에서 드릴다운합니다.

단계 **2** 이벤트 보기 페이지에서 **Report Designer(**보고서 디자이너**)**를 클릭합니다.

캡처한 워크플로의 각 보기에 대한 섹션과 함께 Report Sections(보고서 섹션) 페이지가 표시됩니다.

단계 **3** 선택적으로, **Report Title(**보고서 제목**)** 필드에 새 이름을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **4** 다음 작업을 수행할 수 있습니다.

- 커버 페이지, 목차, 시작 페이지 번호 또는 머리글과 바닥글 텍스트 추가 - **Advanced(**고급**)** 설정을 클릭합니다.
- 페이지 나누기 추가 - 페이지 구분 추가( )을 클릭하고, 새 페이지 나누기 개체를 템플릿 아래쪽에서 새 페이지를 시작할 섹션 앞으로 드래그합니다.
- 텍스트 섹션 추가 - 텍스트 섹션 추가(T)을 클릭하고, 새 텍스트 섹션을 템플릿 아래쪽에서 보고서 템플릿에 표시할 위치까지 드래그합니다.
- 섹션 제목 변경 - 제목 표시줄에 있는 섹션 제목을 클릭하고, 섹션 제목을 입력하고, **OK(**확인**)**를 클릭합니다.

- 보고서 섹션 설정 - 각 섹션의 필드 설정을 조정합니다.

  팁 섹션의 현재 열 레이아웃 또는 차트 형식을 보려면 해당 섹션의 **Preview(**미리보기**)** 링크를 클릭하십시오.

- 보고서에서 템플릿 섹션 제외 - 섹션의 제목 표시줄에서 삭제 ( )을 클릭하고 삭제 여부를 확인합니다.

  참고 일부 워크플로의 마지막 보고서 섹션에는 워크플로에 따라 패킷, 호스트 프로파일 또는 취약성을 보여주는 상세정보 보기가 포함됩니다. 보고서를 생성할 때 이러한 상세정보 보기가 있는 다수의 이벤트를 검색하면 Firepower Management Center의 성능이 저하될 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

대시보드 또는 워크플로를 가져와 보고서 템플릿 생성

프로시저

단계 **1** 보고서에서 복제할 대시보드, 워크플로 또는 요약을 식별합니다.

단계 **2** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **3** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **4** **Create Report Template(**보고서 템플릿 생성**)**을 클릭합니다.

단계 **5** **Report Title(**보고서 제목**)** 필드에 새 보고서 템플릿의 이름을 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 가져오기 섹션 ( ) 버튼을 클릭합니다. 보고서 가져오기 섹션의 데이터 소스 옵션, 2659 페이지에서 설명하는 데이터 소스 중 하나를 선택할 수 있습니다.

단계 **8** 드롭다운 메뉴에서 대시보드, 워크플로 또는 요약을 선택합니다.

단계 **9** 추가할 데이터 소스에 대해 **Import(**가져오기**)**를 클릭합니다.

대시보드의 경우 각 위젯 그래픽이 자체 섹션을 가지며, 워크플로의 경우 각 이벤트 보기가 자체 섹션을 가집니다.

단계 **10** 필요한 대로 섹션의 내용을 변경합니다.

참고 일부 워크플로의 마지막 보고서 섹션에는 워크플로에 따라 패킷, 호스트 프로파일 또는 취약성을 보여주는 상세정보 보기가 포함됩니다. 보고서를 생성할 때 이러한 상세정보 보기가 있는 다수의 이벤트를 검색하면 Firepower Management Center의 성능이 저하될 수 있습니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

보고서 가져오기 섹션의 데이터 소스 옵션

표 ***270:*** 보고서 가져오기 섹션 창의 데이터 소스 옵션

이 옵션 선택	가져오기
대시보드 가져오기	선택한 대시보드의 맞춤형 분석 위젯
워크플로 가져오기	사전 정의 또는 맞춤형 워크플로 선택 형식은 다음과 같습니다. `Table - Workflow name` 예를 들어 `Connection Events - Traffic by Port`는 Connection Events(연결 이벤트) 테이블에서 생성된 Traffic by Port(포트별 트래픽) 워크플로의 보기를 가져옵니다.
Import Summary Sections(요약 섹션 가져오기)	다음 일반 요약 중 하나: • Intrusion Detailed Summary(침입 상세 요약) • Intrusion Short Summary(침입 짧은 요약) • Discovery Detailed Summary(검색 짧은 요약) • Discovery Short Summary(검색 짧은 요약)

보고서 템플릿 설정

생성한 보고서 템플릿은 수정하거나 맞춤형할 수 있습니다. 다양한 보고서 섹션 속성을 수정하여, 섹션의 내용과 해당 데이터 표시 방식을 조정할 수 있습니다.

보고서 템플릿의 각 섹션은 데이터베이스 테이블을 쿼리하여 해당 섹션의 내용을 생성합니다. 섹션의 데이터 형식을 변경할 경우 동일한 데이터 쿼리가 사용되지만, 형식 유형의 분석 목적에 따라 섹션에 나타나는 필드가 수정됩니다. 예를 들어 침입 이벤트의 테이블 보기는 이벤트 레코드당 다수의 데이터 필드로 섹션을 채우는 반면, 원도표 섹션에는 개별 이벤트에 대한 상세정보 없이 선택한 각 특성이 나타내는 모든 일치하는 레코드의 일부가 표시됩니다. 막대 그래프는 특정 속성이 있는 일치하는 레코드의 총 수를 비교합니다. 선 그래프는 단일 특성을 기준으로 일치하는 레코드의 시간에 따른 변경 사항을 요약합니다. 선 그래프는 시간 기반의 데이터에만 사용할 수 있으며 호스트, 사용자, 서드파티 취약성 등에 대한 정보에는 사용할 수 없습니다.

보고서 섹션의 검색 또는 필터는 섹션 내용의 기반이 되는 데이터베이스 쿼리를 지정합니다. 대부분의 테이블에서 사전 정의 검색 또는 저장된 검색을 사용하여 보고서를 제한하거나, 즉석에서 새 검색을 생성할 수 있습니다.

- 사전 정의된 검색은 특정 이벤트 테이블을 검색하는 예제로 제공되며, 보고서에 포함할 네트워크 관련 중요 정보에 빠르게 액세스할 수 있습니다.
- 저장된 이벤트에는 자신이나 타인이 생성한 모든 공개 이벤트 검색은 물론, 자신이 저장한 모든 비공개 이벤트 검색도 포함됩니다.

- 현재 보고서 템플릿에 대해 저장된 검색은 보고서 템플릿 자체에서만 액세스 가능합니다. 저장한 보고서 템플릿 검색의 검색 이름은 “Custom Search” 문자열로 끝납니다. 사용자는 보고서를 디자인하는 도중 이러한 검색을 생성합니다.

Application Statistics(애플리케이션 통계) 테이블에서는 사용자 정의 애플리케이션 필터를 이용해 보고서를 제한할 수 있습니다.

섹션에 테이블 데이터를 포함하는 경우 데이터 레코드에 어떤 필드를 표시할지를 선택할 수 있습니다. 테이블의 모든 필드를 포함하거나 제외할 수 있습니다. 보고서 목적을 달성하는 필드를 선택한 다음 적절히 순서를 지정하고 정렬합니다.

전체 보고서 또는 개별 섹션에 대해 맞춤형 텍스트(예: 소개)를 제공하려면 템플릿에 텍스트 섹션을 추가할 수 있습니다.

템플릿의 섹션 전후에 페이지 나누기를 추가할 수 있습니다. 이 기능은 다양한 섹션을 소개하는 텍스트 페이지가 있는 다중 섹션 보고서에서 특히 유용합니다.

보고서 템플릿의 시간 창은 템플릿의 보고 기간을 정의합니다.

참고 보안 분석가는 자신이 생성한 보고서 템플릿만 수정할 수 있습니다. 다중 도메인 구축의 경우에는 상위 도메인의 보고서 템플릿은 편집할 수 없지만, 복사해서 하위 버전을 만들 수 있습니다.

보고서 템플릿 섹션에 대한 테이블 및 데이터 형식 설정

프로시저

단계 **1** 보고서 템플릿 섹션에서 **Table(**테이블**)** 드롭다운 메뉴를 사용하여, 쿼리할 테이블을 선택합니다.

Format(형식**)** 필드는 선택한 테이블에 사용할 수 있는 각 출력 형식을 나타냅니다.

단계 **2** 섹션에 해당하는 출력 형식을 선택합니다.

단계 **3** 검색 제약 조건을 변경하려면 **Section description(**섹션 설명**)** 필드 또는 **Filter(**필터**)** 필드 옆에 있는 수정( )을 클릭합니다.

단계 **4** 그래픽 출력 형식(원도표, 막대 그래프 등)에 대해 드롭다운 메뉴를 사용하여 **X-Axis(X**축**)** 및 **Y-Axis(Y**축**)** 파라미터를 조정합니다.

X축에 대한 값을 선택하면 호환되는 값만 Y축 드롭다운 메뉴에 나타나고, 그 반대의 경우도 마찬가지입니다.

단계 **5** 테이블 출력에서는 열, 나타나는 순서 및 출력의 정렬 순서를 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

보고서 템플릿 필드, 2654 페이지

보고서 템플릿 섹션에 대한 검색 또는 필터 지정

프로시저

단계 **1** 보고서 템플릿 섹션에서 **Table(**테이블**)** 드롭다운 메뉴를 사용하여, 쿼리할 데이터베이스 테이블을 선택합니다.

- 대부분의 테이블에 대해 **Search(**검색**)** 드롭다운 목록이 나타납니다.
- Application Statistics(애플리케이션 통계) 테이블의 경우 **Filter(**필터**)** 드롭다운 목록이 나타납니다.

단계 **2** 보고서를 제한하기 위해 사용할 검색 또는 필터를 선택합니다.

검색 기준을 볼 수도 있고 수정( )을 클릭하여 새 검색을 생성할 수도 있습니다.

관련 항목

애플리케이션 필터, 574 페이지

테이블 형식 섹션에 표시되는 검색 필드 설정

프로시저

단계 **1** 테이블 형식 보고서 섹션에서 **Fields(**필드**)** 매개변수 옆에 있는 수정( )을 클릭합니다.

단계 **2** 섹션을 수정하려는 경우, 필드를 추가 및 삭제하고 필드를 원하는 열 순서대로 끌어와야 합니다.

단계 **3** 특정 열의 정렬 순서를 변경하려는 경우에는 각 필드의 드롭다운 목록을 사용하여 정렬 순서와 우선순위를 설정해야 합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

보고서 템플릿에 텍스트 섹션 추가

텍스트 섹션에서는 여러 글꼴 크기와 스타일(굵게, 기울임 등)의 풍부한 텍스트는 물론 입력 파라미터와 가져온 이미지도 사용할 수 있습니다.

팁 텍스트 섹션은 보고서 또는 보고서 섹션을 소개할 때 유용합니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 텍스트 섹션 추가( )을 클릭합니다.

단계 **2** 보고서 템플릿의 원하는 위치로 새 텍스트 섹션을 끌어옵니다.

단계 **3** 텍스트 섹션을 페이지 처음이나 끝 부분에 배치하는 경우에는, 텍스트 섹션 앞이나 뒤에 페이지 나누기를 추가합니다.

단계 **4** 텍스트 섹션의 일반 이름을 변경하려는 경우에는 제목 표시줄에서 섹션의 이름을 클릭하고 새 이름을 입력합니다.

단계 **5** 텍스트 섹션의 본문에 서식이 지정된 텍스트와 이미지를 추가합니다.

보고서를 생성할 때 동적으로 업데이트되는 입력 파라미터를 포함할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

입력 매개변수, 2664 페이지

보고서 템플릿에 페이지 나누기 추가

프로시저

단계 **1** 보고서 템플릿 편집기에서 페이지 구분 추가( )을 클릭합니다.

템플릿의 아래쪽에 페이지 나누기가 나타납니다.

단계 **2** 페이지 나누기를 섹션 전후의 원하는 위치로 끌어옵니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

글로벌 시간 창 및 보고서 템플릿 섹션

시간 기반 데이터(예: 침입 또는 검색 이벤트)가 포함된 보고서 템플릿에는 전역 시간 창이 있으며, 템플릿의 시간 기반 섹션은 생성될 때 기본적으로 이를 상속합니다. 전역 시간 창을 변경하면 전역 시간 창을 상속하도록 구성된 섹션에 대한 로컬 시간 창이 변경됩니다. **Inherit Time Window(**시간 창 상속**)** 확인란의 선택을 취소하여 개별 섹션에 대해 시간 창 상속을 비활성화할 수 있습니다. 그러면 로컬 시간 창을 편집할 수 있습니다.

참고 전역 시간 창 상속은 시간 기반 테이블의 데이터(예: 침입 이벤트 및 검색 이벤트)와 함께 보고서 섹션에만 적용됩니다. 네트워크 자산(호스트와 디바이스) 및 관련 정보(예: 취약성)에 대해 보고하는 섹션의 경우 각 시간 창을 개별적으로 설정해야 합니다.

보고서 템플릿 및 관련 섹션에 대한 글로벌 시간 창 설정

팁 보고서에서 섹션마다 다른 시간 범위를 사용할 수 있습니다. 예를 들어 첫 번째 섹션에는 월 요약을 포함하고, 나머지 섹션에는 각 주의 상세정보을 포함할 수 있습니다. 이 경우 섹션 레벨 시간 창을 개별적으로 설정합니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Generate(**생성**)**를 클릭합니다.

단계 **2** 전역 시간 창을 수정하려면 시간 창( )을 클릭합니다.

단계 **3** **Events Time Window(**이벤트 시간 창**)**에서 시간 설정을 수정합니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

단계 **5** **Generate(**생성**)**을 클릭해 보고서를 생성하고 **Yes(**예**)**를 클릭해 확인합니다.

보고서 템플릿 섹션에 대한 보고서 템플릿 섹션에 로컬 시간 창 설정

프로시저

단계 **1** 템플릿의 Report Sections 페이지에서 섹션에 대한 **Inherit Time Window(**시간 창 상속**)** 확인란(있는 경우)의 선택을 취소합니다.

단계 **2** 섹션의 로컬 시간 창을 변경하려면 시간 창( )를 클릭합니다.

참고 통계 테이블의 데이터가 있는 섹션에는 슬라이딩 시간 창만 포함할 수 있습니다.

단계 **3** Events Time Window(이벤트 시간 창)에서 **Apply(**적용**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

보고서 템플릿 섹션 이름 변경

프로시저

단계 **1** 보고서 템플릿 편집기에서 섹션 헤더에 있는 현재 섹션 이름을 클릭합니다.

단계 **2** 섹션의 새 이름을 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

보고서 템플릿 섹션 미리 보기

미리 보기 기능은 테이블 보기의 필드 레이아웃과 정렬 순서, 그리고 원도표 색상과 같은 그래픽의 중요한 가독성 특성을 보여줍니다.

프로시저

단계 **1** 보고서 템플릿 섹션을 편집하는 동안 섹션에 대한 **Preview(**미리보기**)**를 클릭합니다.

단계 **2** **OK(**확인**)**를 클릭하여 미리보기를 닫습니다.

보고서 템플릿 섹션에서 검색

성공적인 보고서 생성의 핵심은 보고서 섹션을 채우는 검색을 정의하는 것입니다. Firepower System에서는 보고서 템플릿에서 사용할 수 있는 검색을 보고 새 맞춤형 검색을 정의할 수 있는 검색 편집기를 제공합니다.

보고서 템플릿 섹션에서 검색

프로시저

단계 **1** 보고서 템플릿의 관련 섹션에서 **Search(**검색**)** 필드 옆에 있는 수정( )을 클릭합니다.

단계 **2** 사전 정의한 검색에서 맞춤형 검색을 기반으로 하려면, **Saved Searches(**저장된 검색**)** 드롭다운 목록에서 사정 정의한 검색을 선택해야 합니다.

이 목록에는 해당 테이블에 대해 사용할 수 있는 모든 사전 정의 검색(시스템 전체에 또는 특정 보고서에만 적용되는 검색 포함)이 포함됩니다.

단계 **3** 해당 필드에서 검색 기준을 수정합니다.

특정 필드에서는 제약 조건으로 이벤트 검색과 동일한 연산자(<, <> 등)를 포함할 수 있습니다. 여러 기준을 입력하면 모든 기준과 일치하는 레코드만 반환됩니다.

단계 **4** 제한 값을 입력하는 대신 드롭다운 메뉴에서 입력 매개변수를 삽입하려는 경우에는 입력 매개변수( )를 클릭해야 합니다.

참고 보고 검색의 제약 조건을 수정하면 시스템은 수정된 검색을 *section* `custom search` 이름으로 저장합니다. 여기서 *section*은 섹션 제목 표시줄의 이름이며, 그 뒤에 `custom search` 문자열이 옵니다. 저장된 맞춤형 검색에 대해 의미 있는 이름을 지정하려면 수정된 검색을 저장하기 전에 섹션 이름을 변경해야 합니다. 저장된 보고 검색의 이름은 변경할 수 없습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

입력 매개변수

생성 시 보고서가 동적으로 업데이트할 수 있는 입력 파라미터를 보고서 템플릿에서 사용할 수 있습니다. 입력 매개변수( )는 처리 가능한 필드를 나타냅니다. 두 가지 종류의 입력 파라미터가 있습니다.

- 사전 정의 입력 파라미터는 내부 시스템 함수 또는 설정 정보에 의해 확인됩니다. 예를 들어 보고서 생성 시 시스템은 `$<Time>` 파라미터를 현재 날짜 및 시간과 교체합니다.
- 사용자 정의 입력 파라미터는 섹션 검색에서 제약을 제공합니다. 입력 파라미터로 검색을 제약하면 시스템은 보고서를 요청하는 사용자의 생성 시간에 값을 수집합니다. 이렇게 하면 템플릿을 변경하지 않고도 데이터의 특별한 일부를 표시하도록 생성 시 보고서를 동적으로 맞춤화할

수 있습니다. 예를 들어 보고서 섹션 검색의 **Destination IP(**목적지 **IP)** 필드에 입력 파라미터를 제공할 수 있습니다. 그런 다음 보고서를 생성할 때 특정 부서의 데이터만 가져오려면 해당 부서의 IP 네트워크 세그먼트를 입력할 수 있습니다.

이메일(제목이나 본문), 보고서 파일 이름, 텍스트 섹션 등 보고서의 특정 필드에 동적 텍스트를 추가하려면 문자열 유형의 입력 파라미터를 정의할 수 있습니다. 동일한 템플릿을 사용하되 맞춤형된 보고서 파일 이름, 이메일 주소, 이메일 메시지 등을 사용하여 부서별로 보고서를 개별 설정할 수 있습니다.

사전 정의 입력 파라미터

표 ***271:*** 사전 정의 입력 파라미터

삽입할 파라미터	템플릿에 포함할 정보:
`$<Logo>`	선택한 업로드된 로고
`$<Report Title>`	보고서 제목
`$<Time>`	보고서가 실행된 날짜와 시간(1초 단위)
`$<Month>`	현재 월
`$<Year>`	현재 연도
`$<System Name>`	이름 Firepower Management Center
`$<Model Number>`	모델 번호 Firepower Management Center
`$<Time Window>`	현재 보고서 섹션에 적용된 시간 창
`$<Constraints>`	현재 보고서 섹션에 적용 된 검색 제약 조건

표 ***272:*** 사전 정의 입력 파라미터 사용법

매개변수	보고서 템플릿 커버 페이지	보고서 템플릿 보고서 제목	보고서 템플릿 섹션 설명	보고서 템플릿 텍스트 섹션	보고서 파일 이름 생성	보고서 이메일 제목, 본문 생성
`$<Logo>`	예	아니요	아니요	아니요	아니요	아니요
`$<Report Title>`	예	아니요	예	예	예	예
`$<Time>`	예	예	예	예	예	예
`$<Month>`	예	예	예	예	예	예
`$<Year>`	예	예	예	예	예	예
`$<System Name>`	예	예	예	예	예	예

매개변수	보고서 템플릿 커버 페이지	보고서 템플릿 보고서 제목	보고서 템플릿 섹션 설명	보고서 템플릿 텍스트 섹션	보고서 파일 이름 생성	보고서 이메일 제목, 본문 생성
`$<Model Number>`	예	예	예	예	예	예
`$<Time Window>`	아니요	아니요	예	아니요	아니요	아니요
`$<Constraints>`	아니요	아니요	예	아니요	아니요	아니요

사용자 정의 입력 파라미터

입력 파라미터를 사용하면 검색의 활용 범위를 확장할 수 있습니다. 입력 파라미터는 보고서를 요청하는 사용자의 생성 시간에 시스템에 값을 수집하도록 지시합니다. 이렇게 하면 검색을 변경하지 않고도 데이터의 특별한 일부를 표시하도록 생성 시 보고서를 동적으로 제한할 수 있습니다. 예를 들어 부서 수준에서 보안 이벤트를 드릴다운하는 보고서 섹션의 **Destination IP(**목적지 **IP)** 필드에 입력 파라미터를 제공할 수 있습니다. 보고서를 생성할 때 특정 부서의 데이터만 가져오려면 해당 부서의 IP 네트워크 세그먼트를 입력합니다.

입력 파라미터의 유형은 사용 가능한 검색 필드를 결정합니다. 유형은 적절한 필드에서만 사용할 수 있습니다. 예를 들어 문자열 유형으로 정의하는 사용자 파라미터는 텍스트 필드에 삽입할 수 있지만, IP 주소가 필요한 필드에는 사용할 수 없습니다.

정의하는 각 입력 파라미터에는 이름과 유형이 존재합니다.

표 ***273:*** 사용자 정의 입력 파라미터 유형

사용할 파라미터 유형	다음 데이터가 포함된 필드
네트워크/IP	CIDR 형식의 IP 주소 또는 네트워크 세그먼트
애플리케이션	애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 웹 애플리케이션의 이름
이벤트 메시지	이벤트 보기 메시지
디바이스	FMC 또는 매니지드 디바이스
Username	사용자 식별(예: 이니시에이터 사용자 및 응답자 사용자)
번호(VLAN ID, Snort ID, Vuln ID)	VLAN ID, Snort ID 또는 취약성 ID
문자열	애플리케이션이나 OS 버전, 메모, 설명 등의 텍스트 필드

사용자 정의 입력 파라미터 생성

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** 매개변수 입력 추가( ) 버튼을 클릭합니다.

단계 **3** 파라미터 **Name(**이름**)**을 입력합니다.

단계 **4** **Type(**유형**)** 드롭다운 목록에서 값을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 파라미터를 추가합니다.

단계 **6** **OK(**확인**)**를 클릭하여 편집기로 돌아갑니다.

사용자 정의 입력 파라미터 수정

보고서 템플릿의 **Input Parameters(**입력 파라미터**)** 섹션은 템플릿에 대해 사용할 수 있는 모든 사용자 정의 파라미터를 열거합니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** 수정할 매개변수 옆에 있는 수정( )을 클릭합니다.

단계 **3** 새 **Name(**이름**)**을 입력합니다.

단계 **4** **Type(**유형**)** 드롭다운 목록을 사용하여 파라미터 유형을 변경합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **6** 입력 매개 변수를 삭제하려는 경우에는 입력 매개변수 옆에 있는 삭제( )을 클릭하고 확인합니다.

단계 **7** **OK(**확인**)**를 클릭하여 보고서 템플릿 편집기로 돌아갑니다.

사용자 정의 입력 파라미터로 검색 제한

정의하는 입력 파라미터는 해당 파라미터 유형과 일치하는 검색 필드에서만 사용할 수 있습니다. 예를 들어 **Network/IP** 유형의 파라미터는 IP 주소 또는 CIDR 형식의 네트워크 세그먼트가 허용되는 필드에만 사용할 수 있습니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 섹션의 **Search(**검색**)** 필드 옆에 있는 수정( )을 클릭합니다.

입력 매개변수를 사용할 수 있는 필드는 입력 매개변수( )로 표시됩니다.

단계 **2** 필드 옆에 있는 입력 매개변수( )를 클릭한 다음 드롭다운 메뉴에서 입력 매개변수를 선택합니다.

사용자 정의 입력 매개변수는 아이콘( )으로 표시됩니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

보고서 템플릿의 문서 속성

보고서를 생성하기 전에 보고서 모양에 영향을 주는 문서 속성을 설정할 수 있습니다. 이러한 특성에는 선택적인 커버 페이지 및 목차가 포함됩니다. 일부 특성에 대한 지원은 선택한 보고서 형식(PDF, HTML 또는 CSV)에 따라 달라집니다.

표 ***274:*** 문서 속성 지원

특성	**PDF** 지원 여부	**HTML** 지원 여부	**CSV** 지원 여부
커버 페이지	예(로고 및 맞춤형 모양은 선택 사항)	예(로고 및 맞춤형 모양은 선택 사항)	아니요
목차	예	예	아니요
페이지 머리글 및 바닥글	예(필드의 텍스트 또는 로고는 선택 사항)	아니요	아니요
맞춤형 시작 페이지 번호	예	아니요	아니요
첫 페이지의 번호 억제 옵션	예	아니요	아니요

보고서 템플릿의 문서 속성 수정

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Add cover page(커버 페이지 추가) - 커버 페이지를 추가하려면 **Include Cover Page(**커버 페이지 추가**)** 확인란을 선택합니다.
- Customize cover page(커버 페이지 맞춤형) - 커버 페이지 디자인을 편집하는 방법은 커버 페이지 맞춤 설정, 2669 페이지 섹션을 참조하십시오.
- Add table of contents(목차 추가) - 목차를 추가하라면 **Include Table of Contents(**목차 넣기**)** 확인란을 선택합니다.
- Manage logos(로고 관리) - 템플릿과 관련된 로고 이미지를 관리하는 방법은 보고서 템플릿 로고 관리, 2669 페이지 섹션을 참조하십시오.
- Configure header and footer(머리글 및 바닥글 설정) - 템플릿의 머리글과 바닥글에 대한 요소를 지정하려면, **Header(**머리글**)** 및 **Footer(**바닥글**)** 필드의 드롭다운 목록을 사용하십시오.
- Set first page number(첫 번째 페이지 번호 설정) - 보고서 첫 번째 페이지의 페이지 번호를 지정하려면 **Page Number Start(**페이지 번호 시작**)** 값을 입력합니다.
- Show first page number(첫 번째 페이지 번호 표시) - 보고서 첫 번째 페이지에서 페이지 번호를 표시하려면 **Number First Page?(**첫 번째 페이지 번호 표시**)** 확인란을 선택합니다. 이 옵션을 선택하면 커버 페이지에는 번호가 지정되지 않습니다.

단계 **3** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

커버 페이지 맞춤 설정

보고서 템플릿의 커버 페이지를 맞춤형할 수 있습니다. 커버 페이지에서는 여러 글꼴 크기와 스타일(굵게, 기울임 등)의 풍부한 텍스트는 물론 입력 파라미터와 가져온 이미지도 사용할 수 있습니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Cover Page Design(**커버 페이지 디자인**)** 옆에 있는 수정( )을 클릭합니다.

단계 **3** 풍부한 텍스트 편집기 내에서 커버 페이지 디자인을 편집합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

보고서 템플릿 로고 관리

Firepower Management Center에 여러 로고를 저장하고 서로 다른 보고서 템플릿과 연결할 수 있습니다. 템플릿을 디자인할 때 로고 연결을 설정합니다. 템플릿을 내보내면 내보내기 패키지에 로고가 포함됩니다.

로고를 Firepower Management Center에 업로드하면 다음 대상에서 로고를 사용할 수 있습니다.

- Firepower Management Center의 모든 보고서 템플릿 또는
- 다중 도메인 구축의 경우에는 현재 도메인에 있는 모든 보고서 템플릿

로고 이미지는 GIF, JPG 또는 PNG 형식입니다.

보고서의 로고를 Firepower Management Center에 업로드된 JPG 이미지로 변경할 수 있습니다. 예를 들어 템플릿을 재사용하려면 다른 조직의 로고를 보고서와 연결할 수 있습니다.

업데이트된 로그는 삭제할 수 이습니다. 로고를 삭제하면 로고를 사용하는 모든 템플릿에서 해당 로고가 제거됩니다. 삭제는 취소할 수 없습니다. 사전 정의된 Cisco 로고는 삭제할 수 없습니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

현재 템플릿과 연결된 로고는 **General Settings(**일반 설정**)**의 **Logo(**로고**)** 아래에 나타납니다.

단계 **2** 로고 옆에 있는 수정( )을 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Add(추가) - 새 로고 추가, 2670 페이지에 설명된 대로 새 로고를 추가합니다.

- Change(변경) - 보고서 템플릿에 대한 로고 변경, 2670 페이지에 설명된 대로 보고서 템플릿의 로고를 변경합니다.
- Delete(삭제) - 로고 삭제, 2670 페이지에 설명된 대로 로고를 삭제합니다.

새 로고 추가

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.
단계 **2** **Logo(**로고**)** 필드 옆에 있는 수정( )를 클릭합니다.
단계 **3** **Upload Logo(**로고 업로드**)**를 클릭합니다.
단계 **4** **Browse(**찾기**)**를 클릭하고 파일의 위치로 이동한 다음 **Open(**열기**)**을 클릭합니다.
단계 **5** **Upload(**업로드**)**를 클릭합니다.
단계 **6** 새 로고를 현재 템플릿에 연결하려면 항목을 선택하고 **OK(**확인**)**를 클릭합니다.

보고서 템플릿에 대한 로고 변경

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.
단계 **2** **Logo(**로고**)** 필드 옆에 있는 수정( )을 클릭합니다.
단계 **3** Select Logo(로고 선택) 대화 상자에서 보고서 템플릿에 연결할 로고를 선택합니다.
단계 **4** **OK(**확인**)**를 클릭합니다.

로고 삭제

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.
단계 **2** **Logo(**로고**)** 필드 옆에 있는 수정( )을 클릭합니다.
단계 **3** Select Logo(로고 선택) 대화상자에서 삭제할 로고를 선택합니다.
단계 **4** **Delete Logo(**로고 삭제**)**를 클릭합니다.
단계 **5** **OK(**확인**)**를 클릭합니다.

보고서 템플릿 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 보고서 템플릿을 표시하며, 이러한 템플릿은 편집할 수 있습니다. 상위 도메인에서 생성된 보고서 템플릿도 표시되지만, 이러한 템플릿은 편집할 수 없습니다. 하위 도메인에서 생성된 보고서 템플릿을 보고 편집하려면 해당 도메인으로 전환하십시오. 시스템은 현재 도메인에 생성된 보고서만 표시합니다.

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**를 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Delete(삭제) - 삭제할 템플릿 옆에 있는 삭제( )을 클릭하고 확인합니다.

  시스템 제공 보고서 템플릿은 삭제할 수 없습니다. 보안 분석가는 자신이 생성한 보고서 템플릿만 삭제할 수 있습니다. 다중 도메인 구축의 경우에는 현재 도메인에 속한 보고서 템플릿만 삭제할 수 있습니다.

- Edit(편집) - 보고서 템플릿을 편집하는 방법은 보고서 템플릿 수정, 2671 페이지 섹션을 참조하십시오.
- Export(내보내기) - 보고서 템플릿을 내보내는 방법은 보고서 템플릿 내보내기, 2672 페이지 섹션을 참조하십시오.

  팁 표준 설정 내보내기 프로세스를 사용하여 보고서 템플릿을 내보낼 수도 있습니다(컨피그레이션 내보내기, 240 페이지 참조).

- Import(가져오기) - 보고서 템플릿을 가져오는 방법은 컨피그레이션 가져오기, 240 페이지 섹션을 참조하십시오.

보고서 템플릿 수정

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 보고서 템플릿을 표시하며, 이러한 템플릿은 편집할 수 있습니다. 상위 도메인에서 생성된 보고서 템플릿도 표시되지만, 이러한 템플릿은 편집할 수 없습니다. 하위 도메인에서 생성된 보고서 템플릿을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 편집할 템플릿의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 다음 옵션을 이용할 수 있습니다.

- 페이지 나누기를 추가합니다(보고서 템플릿에 페이지 나누기 추가, 2662 페이지 참조).
- 텍스트 섹션을 추가합니다(보고서 템플릿에 텍스트 섹션 추가, 2661 페이지 참조).
- 보고서 템플릿 설정, 2659 페이지의 설명대로 섹션 콘텐츠를 설정합니다.
- 입력 파라미터를 생성합니다(사용자 정의 입력 파라미터 생성, 2666 페이지 참조).
- 입력 파라미터를 편집합니다(사용자 정의 입력 파라미터 수정, 2667 페이지 참조).
- 문서 속성을 편집합니다(보고서 템플릿의 문서 속성 수정, 2668 페이지 참조).
- 템플릿 섹션을 검색합니다(보고서 템플릿 섹션에서 검색, 2664 페이지 참조).
- **Advanced(**고급**)**를 클릭하여 보고서 템플릿의 문서 속성, 2668 페이지에 설명된 대로 문서 속성을 설정합니다.
- 글로벌 타임 창을 설정합니다(보고서 템플릿 및 관련 섹션에 대한 글로벌 시간 창 설정, 2662 페이지 참조).
- 로컬 타임 창을 설정합니다(보고서 템플릿 섹션에 대한 보고서 템플릿 섹션에 로컬 시간 창 설정, 2663 페이지 참조).
- 검색 필드를 설정합니다(테이블 형식 섹션에 표시되는 검색 필드 설정, 2661 페이지 참조).
- 테이블 및 데이터 형식을 설정합니다(보고서 템플릿 섹션에 대한 테이블 및 데이터 형식 설정, 2660 페이지 참조).
- 검색 및 필터를 지정합니다(보고서 템플릿 섹션에 대한 검색 또는 필터 지정, 2661 페이지 참조).

보고서 템플릿 내보내기

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**를 선택합니다.

단계 **2** **Report Templates(**보고서 템플릿**)**을 선택합니다.

단계 **3** 내보내려는 템플릿에 대해 **YouTube EDU(**)을 클릭합니다.

단계 **4** **Save file(**파일 저장**)** 및 **OK(**확인**)**를 선택하여 파일을 로컬 컴퓨터에 저장합니다.

보고서 생성 정보

보고서 생성

보고서 템플릿을 생성 및 맞춤형했으면 이제 보고서를 생성할 준비가 된 것입니다. 생성 프로세스에서는 보고서의 형식(HTML, PDF 또는 CSV)을 선택할 수 있습니다. 제외한 섹션 이외의 모든 섹션에 일관된 기간을 적용하는 보고서의 전역 시간 창을 조정할 수도 있습니다.

PDF 보고서의 경우:

- 유니코드(UTF-8) 문자를 사용한 파일 이름은 지원되지 않습니다.
- 특정 유니코드 파일 이름(예: 파일 또는 악성코드 이벤트에 나타나는 이름)이 포함된 보고서 섹션에는 이러한 파일 이름이 음역 형식으로 표시됩니다.

보고서 템플릿의 검색 사양에 사용자 입력 파라미터가 포함된 경우 일반 프로세스에서는 값을 입력하라는 프롬프트가 표시됩니다. 이러한 값은 데이터 일부에 대한 보고서 실행을 맞춤화합니다.

DNS 서버가 구성되어 있고 IP 주소 확인이 활성화된 경우 확인에 성공하면 보고서에 호스트 이름이 포함됩니다.

다중 도메인 구축의 경우 상위 도메인에서 보고서를 생성할 때, 모든 하위 도메인의 결과가 포함될 수 있습니다. 특정 리프 도메인에 대한 보고서를 생성하려면 해당 도메인으로 전환합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Report Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 보고서를 생성하는 데 사용할 템플릿 옆에 있는 보고서( )를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

팁 상위 템플릿의 보고서를 생성하려면 템플릿을 현재 도메인으로 복사합니다.

단계 **4** 선택적으로, 보고서 이름을 설정합니다.

- 새 **File Name(**파일 이름**)**을 입력합니다. 새 이름을 입력하지 않는 경우 시스템은 보고서 템플릿에 지정된 이름을 사용합니다.
- 파일 이름에 하나 이상의 입력 매개변수를 추가하려면 입력 매개변수( )를 사용하십시오.

단계 **5** HTML, PDF 또는 CSV를 클릭하여 보고서의 출력 형식을 선택합니다.

단계 **6** 전역 시간 창을 변경하려면 시간 창( )를 클릭합니다.

참고 개별 보고서 섹션이 전역 설정을 상속하도록 구성된 경우에만 전역 시간 창 설정이 개별 보고서 섹션의 내용에 영향을 미칩니다.

단계 **7** **Input Parameters(**입력 파라미터**)** 섹션에 나타나는 필드의 값을 입력합니다.

팁 필드에 * 와일드카드 문자를 입력하여 사용자 파라미터를 무시할 수 있습니다. 이 경우 검색에 대한 사용자 파라미터의 제약 조건이 제거됩니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 리터럴 IP 주소 또는 VLAN 태그를 사용하여 보고서 결과를 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **8** Firepower Management Center 설정에서 이메일 릴레이 호스트를 활성화한 경우, **Email(**이메일**)**을 클릭해 생성되는 보고서의 이메일 전송을 자동으로 처리하십시오.

단계 **9** 프롬프트가 표시되면 **OK(**확인**)** 를 클릭하고 확인합니다.

Generate(생성**)**를 클릭하면 일반 설정을 보고서 템플릿과 함께 저장합니다.

Cancel(취소**)**을 클릭하면 선택한 내용은 세션 기간 동안에만 저장됩니다.

단계 **10** 다음 옵션을 이용할 수 있습니다.

- 보고서 링크를 클릭해 보고서를 새 창에서 표시합니다.
- **OK(**확인**)**를 클릭하여 보고서 템플릿 편집기로 돌아갑니다.

보고서 생성 옵션

보고서 생성 옵션을 설정해 다음 작업을 할 수 있습니다.

- 향후 보고서 생성을 일회 또는 반복 예약합니다. 보고서 생성 자동화, 254 페이지의 내용을 참조하십시오. 일별, 주별, 월별 등 전체 기간에 대한 일정을 맞춤형할 수 있습니다.
- 일정 관리기를 사용하여 이메일 보고서를 배포합니다. 작업을 예약하기 전에 먼저 보고서 템플릿과 메일 릴레이 호스트를 설정해야 합니다.
- 보고서를 생성할 때 보고서를 이메일 첨부파일로 수신자 목록에 자동으로 전송합니다. 보고서를 이메일로 전달하려면 메일 릴레이 호스트를 적절히 구성해야 합니다.
- 새로 생성한 보고서 파일을 설정된 원격 스토리지 위치에 저장합니다. 원격 스토리지를 사용하려면 먼저 원격 스토리지 위치를 설정해야 합니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

생성 시 이메일로 보고서 배포

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**를 선택합니다.

단계 **2** **Report Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 보고서를 생성하는 데 사용할 템플릿 옆에 있는 보고서( )를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

팁 상위 템플릿의 보고서를 생성하려면 템플릿을 현재 도메인으로 복사합니다.

단계 **4** 창의 **Email(**이메일**)** 섹션을 확장합니다.

단계 **5** **Email Options(**이메일 옵션**)** 필드에서 **Send Email(**이메일 전송**)**을 선택합니다.

단계 **6** **Recipient List**, **CC** 및 **BCC** 필드에서 쉼표로 구분된 목록에 수신자의 이메일 주소를 입력합니다.

단계 **7** **Subject(**제목**)** 필드에 이메일 제목을 입력합니다.

팁 타임스탬프나 Firepower Management Center의 이름과 같은 정보를 이메일에서 동적으로 생성하려면 **Subject(**제목**)** 필드 및 메시지 본문에 입력 파라미터를 제공할 수 있습니다.

단계 **8** 필요에 따라 이메일 본문에 설명 내용을 입력합니다.

단계 **9** **OK(**확인**)**를 클릭하고 확인합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지

향후 보고서 예약

보고서 생성 자동화, 254 페이지의 내용을 참조하십시오.

생성된 보고서 작업 정보

Reports(보고서) 탭 페이지에 있는 이전에 생성한 보고서에 액세스하고 관련 작업을 합니다.

보고서 보기

Reports(보고서)에는 보고서 이름, 생성 날짜와 시간, 생성 사용자, 보고서가 로컬에 저장되었는지 원격에 저장되었는지 등의 정보와 함께 전에 생성된 모든 보고서가 나열됩니다. 상태 열에는 보고서가 이미 생성되었는지, 생성 대기열에 있는지(예: 예약된 작업) 또는 (디스크 공간 부족 등의 이유로) 생성에 실패했는지 등이 나타납니다.

Administrator(관리자) 액세스 권한이 있는 사용자는 모든 보고서를 볼 수 있습니다. 다른 사용자는 자신이 생성한 보고서만 볼 수 있습니다.

다중 도메인 구축의 경우에는 현재 도메인에서 생성한 보고서만 볼 수 있습니다.

Reports(보고서) 페이지에는 로컬에 저장된 모든 보고서가 표시됩니다. 현재 원격 스토리지가 구성된 경우 원격으로 저장된 보고서도 표시됩니다. 원격으로 저장한 보고서의 **Location(**위치**)** 열 데이터는 `Remote(원격)`입니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 클릭합니다.

단계 **3** 확인할 보고서를 클릭합니다.

보고서 다운로드

원하는 보고서 파일을 로컬 컴퓨터로 다운로드할 수 있습니다. 이곳에서는 보고서 파일을 이메일로 전송하거나 다른 사용 가능한 수단을 통해 전자 방식으로 배포할 수 있습니다.

다중 도메인 구축의 경우에는 현재 도메인에서 생성한 보고서만 다운로드할 수 있습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 클릭합니다.

단계 **3** 다운로드할 보고서 옆에 있는 확인란을 선택하고 **Download(**다운로드**)**를 선택합니다.

팁 페이지의 모든 보고서를 다운로드하려면 페이지 상단 왼쪽에 있는 확인란을 클릭합니다. 보고서에 여러 페이지가 있는 경우 클릭하면 모든 페이지의 모든 보고서를 다운로드하는 두 번째 확인란이 나타납니다.

단계 **4** 브라우저의 프롬프트에 따라 보고서를 다운로드합니다. 여러 보고서를 선택하면 단일 `.zip` 파일로 다운로드됩니다.

보고서 원격 저장

현재 구성된 보고서 스토리지의 위치는 Overview(개요)> Reporting(보고) > Reports(보고서) 아래쪽에 로컬, NFS 및 SMB 스토리지에 대한 디스크 사용량과 함께 나타납니다. SSH를 사용하여 원격 스토리지에 액세스하는 경우 디스크 사용량 데이터를 사용할 수 없습니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

시작하기 전에

- 원격 스토리지 관리, 1363 페이지에 설명된 대로 원격 스토리지 위치를 설정합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 선택합니다.

단계 **3** 페이지 아래쪽에서 **Enable Remote Storage of Reports(**보고서의 원격 스토리지 활성화**)** 확인란을 선택합니다.

다음에 수행할 작업

- 보고서를 원격 스토리지에서 원격 스토리지로 옮깁니다(원격 스토리지로 보고서 이동, 2677 페이지 참조).

관련 항목

원격 스토리지 관리, 1363 페이지
원격 스토리지로 보고서 이동, 2677 페이지

원격 스토리지로 보고서 이동

배치 모드에서 또는 단독으로 로컬 스토리지의 보고서를 원격 스토리지 위치로 옮길 수 있습니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

시작하기 전에

- 원격 스토리지 관리, 1363 페이지에 설명된 대로 원격 스토리지 위치를 설정합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 선택합니다.

단계 **3** 이동할 보고서 옆에 있는 확인란을 선택하고 **Move(**이동**)**를 클릭합니다.

팁 페이지의 모든 보고서를 옮기려면 페이지 상단 왼쪽에 있는 확인란을 선택합니다. 보고서에 여러 페이지가 있는 경우 선택하면 모든 페이지의 모든 보고서를 옮길 수 있는 두 번째 확인란이 나타납니다.

단계 **4** 보고서 이동 여부를 확인합니다.

보고서 삭제

언제든지 보고서 파일을 삭제할 수 있습니다. 이 절차를 수행하면 파일이 완전히 제거되며 복구할 수 없습니다. 보고서를 생성 한 보고서 템플릿이 여전히 있지만 시간 창이 확장 또는 슬라이딩 되는 경우 특정 보고서 파일을 다시 생성 하기 어려울 수 있습니다. 템플릿에서 입력 파라미터를 사용하는 경우에도 재생성이 어려울 수 있습니다.

다중 도메인 구축의 경우에는 현재 도메인에서 생성한 보고서만 삭제할 수 있습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Delete selected(선택사항 삭제) - 삭제할 보고서 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.
- Delete all(모두 삭제) - 페이지의 모든 보고서를 삭제하려면 페이지 상단 왼쪽에 있는 확인란을 선택합니다. 보고서에 여러 페이지가 있는 경우 선택하면 모든 페이지의 모든 보고서를 삭제할 수 있는 두 번째 확인란이 나타납니다.

단계 **4** 삭제를 확인합니다.

보고 기록

기능	버전	세부 사항
취약점 보고서의 변경 사항	6.7	보고서 출력이 Bugtraq 데이터의 가용성이 부족하도록 조정되었습니다.

109 장

알림 응답을 사용한 외부 알림

다음 주제에서는 알림 응답을 사용하여 외부 이벤트 알림을 Firepower Management Center에서 전송하는 방법을 설명합니다.

- Firepower Management Center 알림 응답, 2681 페이지
- 알림 응답 요구 사항 및 사전 요건, 2682 페이지
- SNMP 알림 응답 생성, 2683 페이지
- Syslog 알림 응답 생성, 2684 페이지
- 이메일 알림 응답 생성, 2687 페이지
- 영향 플래그 알림 설정, 2688 페이지
- 검색 이벤트 알림 설정, 2688 페이지
- AMP for Networks 알림 설정, 2689 페이지

Firepower Management Center 알림 응답

SNMP, 시스템 로그 또는 이메일을 통한 외부 이벤트 알림으로 중요 시스템 모니터링을 지원할 수 있습니다. Firepower Management Center은(는) 설정 가능한 알림 응답을 이용해 외부 서버와 상호작용합니다. 알림 응답은 이메일, SNMP 또는 시스템 로그 서버와의 연결을 나타나는 설정입니다. 응답이라고 부르는데, 이들을 이용해 Firepower가 탐지한 이벤트에 대한 응답으로 알림을 보낼 수 있기 때문입니다. 여러 알림 응답을 설정해 다양한 유형의 알림을 다양한 모니터링 서버 또는 사람에게 전송할 수 있습니다.

참고 디바이스와 Firepower 버전에 따라, 알림 응답이 시스템 로그 메시지를 전송하는 최상의 방법이 아닐 수도 있습니다. Syslog 정보, 1445 페이지 및 보안 이벤트 시스템 로그 메시지 구성 모범 사례, 2755 페이지를 참조하십시오.

참고 알림 응답을 사용하는 알림은 Firepower Management Center(으)로 전송합니다. 알림 응답을 사용하지 않는 침입 이메일 알림도 Firepower Management Center(으)로 전송합니다. 반면 개별 침입 규칙 트리거링에 기반을 두는 SNMP와 시스템 로그 알림은 매니지드 디바이스가 직접 전송합니다. 자세한 내용은 침입 이벤트에 대한 외부 알림, 2691 페이지를 참고하십시오.

대부분의 경우 외부 알림에 있는 정보는 데이터베이스에 기록한 연결된 이벤트에 있는 정보와 동일합니다. 하지만 상관관계 규칙이 연결 추적기를 포함하는 상관관계 이벤트 알림의 경우, 수신하는 정보는 기본 이벤트 유형에 상관없이 트래픽 프로파일 변경에 대한 알림에 대한 정보와 동일합니다.

Alerts(알림) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**)에서 알림 응답을 생성하고 관리합니다. 새 알림 응답은 자동으로 활성화됩니다. 알림 생성을 일시적으로 중단하려면, 알림 응답을 삭제하지 말고 비활성화하면 됩니다.

알림 응답 변경 사항은 즉시 적용되지만, 연결 로그를 SNMP 트랩 또는 시스템 로그 서버로 전송할 때는 예외입니다.

다중 도메인 구축의 경우에는, 알림 응답을 생성하면 해당 응답은 현재 도메인에 속하게 됩니다. 이 알림 응답은 하위 도메인이 사용할 수도 있습니다.

알림 응답 지원 설정

알림 응답 생성이 끝나면 이를 이용해 다음과 같은 외부 알림을 Firepower Management Center에서 전송할 수 있습니다.

알림/이벤트 유형	추가 정보
영향 플래그별 침입 이벤트	영향 플래그 알림 설정, 2688 페이지
유형별 검색 이벤트	검색 이벤트 알림 설정, 2688 페이지
MP for Networks(네트워크용 AMP)("네트워크 기반")로 탐지한 악성코드 및 회귀 악성코드 이벤트	AMP for Networks 알림 설정, 2689 페이지
상관관계 정책 위반별 상관관계 이벤트	규칙 및 화이트 리스트에 응답 추가, 2586 페이지
로깅 규칙 또는 기본 작업별 연결 이벤트(이메일 알림은 지원되지 않음)	로깅할 수 있는 기타 연결, 2861 페이지
상태 모듈 및 심각도 수준별 상태 이벤트	상태 모니터 알림 생성, 405 페이지

알림 응답 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

SNMP 알림 응답 생성

를 제외하고 디바이스 유형에 대해 SNMPv1, SNMPv2 또는 SNMPv3FTD를 사용하여 SNMP 알림 응답을 만들 수 있습니다.

참고 SNMP 프로토콜을 위한 SNMP 버전을 선택하는 경우, SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3는 읽기 전용 사용자만 지원한다는 사실을 유념하십시오. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

SNMP로 64비트 값을 모니터링하려는 경우, SNMPv2 또는 SNMPv3을 사용해야 합니다. SNMPv1은 64비트 모니터링을 지원하지 않습니다.

시작하기 전에

- 네트워크 관리 시스템에 Firepower Management Center의 관리 정보 베이스(MIB) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create SNMP Alert(SNMP** 알림 생성**)**을 선택합니다.

단계 **3** SNMP 응답 식별을 위한 **Name(**이름**)**을 입력합니다.

단계 **4** **Trap Server(**트랩 서버**)** 필드에 SNMP 트랩 서버의 호스트 이름 또는 IP 주소를 입력합니다.

참고 이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.169.1.456)를 입력한다고 해도 시스템에서 경고하지 않는다는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

단계 **5** **Version(**버전**)** 드롭다운 목록에서 사용하려는 SNMP 버전을 선택합니다. SNMP v3은 기본값입니다.

단계 **6** 사용하는 SNMP의 버전에 따라 다음 중 하나를 수행합니다.

- **Version(**버전**) 1** 또는 **Version(**버전**) 2**: 커뮤니티 문자열 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뜁니다.

  참고 SNMP 커뮤니티 문자열 이름에는 특수문자(< > / % # & ? ', 등)를 포함하지 않습니다.

- SNMP v3의 경우, **User Name(**사용자 이름**)** 필드에 SNMP 서버로 인증하려는 사용자 이름을 입력하고 다음 단계로 넘어갑니다.

단계 **7** **Authentication Protocol(**인증 프로토콜**)** 드롭다운 목록에서 인증을 위해 사용하려면 프로토콜을 선택합니다.

단계 **8** **Authentication Password(**인증 비밀번호**)** 필드에 SNMP 서버 인증에 필요한 비밀번호를 입력합니다.

단계 **9** **Privacy Protocol(**프라이버시 프로토콜**)** 목록에서 **None(**없음**)**을 선택하여 프라이버시 프로토콜을 사용하지 않거나 **DES**를 선택하여 데이터 암호화 표준을 프라이버시 프로토콜로 사용할 수 있습니다.

단계 **10** **Privacy Password(**프라이버시 비밀번호**)** 필드에 SNMP 서버에 필요한 프라이버시 비밀번호를 입력합니다.

단계 **11** **Engine ID(**엔진 **ID)** 필드에 짝수를 사용하여 16진법으로 SNMP 엔진을 위한 식별자를 입력합니다.

SNMPv3을 사용할 때, 시스템은 엔진 ID 값을 사용하여 메시지를 암호화합니다. SNMP 서버에서는 메시지를 해독하는 데 이 값이 필요합니다.

Cisco에서는 Firepower Management Center IP 주소의 16진수 버전을 사용할 것을 권장합니다. 예를 들어, Firepower Management Center의 IP 주소가 10.1.1.77이면 0a01014D0을 사용합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

변경 사항은 즉시 적용됩니다. 단,

알림 응답을 사용해 연결 로그를 보내는 경우 해당 알림 응답을 편집한 후 설정 변경 사항을 구축해야 합니다.

Syslog 알림 응답 생성

syslog 알림 응답을 설정할 때, syslog 메시지와 연결된 심각도 및 기능을 지정하여 syslog 서버에 의해 제대로 처리되었음을 확인할 수 있습니다. 기능은 메시지를 생성하는 하위 시스템을 나타내며, 심각도는 메시지의 심각도를 정의합니다. 기능 및 심각도는 syslog에 나타나는 실제 메시지에 표시되지 않지만, syslog 메시지를 수신하는 시스템에 메시지 카테고리화 방법을 전달하는 데 사용됩니다.

팁 syslog의 작동 방식 및 구성 방법에 대한 자세한 내용은 시스템에 대한 설명서를 참고하십시오. UNIX 시스템에서는 `syslog` 및 `syslog.conf`의 `man` 페이지에서 개념 정보 및 구성 지침을 제공합니다.

시스템 로그 알림 응답을 생성할 때에는 어떤 유형의 기능이든 선택할 수 있지만, 모든 기능을 지원하는 모든 시스템 로그 서버가 아니라 현재의 시스템 로그 서버를 기반으로 합리적인 하나의 기능을 선택해야 합니다. UNIX syslog 서버의 경우, `syslog.conf` 파일은 어느 기능이 서버의 어느 로그 파일에 저장되는지 나타냅니다.

시작하기 전에

- 이 절차는 다양한 상황의 시스템 로그 메시지를 전송하기 위한 방법으로는 권장하지 않습니다. 자세한 내용은 보안 이벤트 시스템 로그 메시지 구성 모범 사례, 2755 페이지를 참조하십시오.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create Syslog Alert(**시스템 로그 알림 생성**)**을 선택합니다.

단계 **3** 알림의 **Name(**이름**)**을 입력합니다.

단계 **4** **Host(**호스트**)** 필드에 시스템 로그 서버의 IP 주소나 호스트 이름을 입력합니다.

참고 이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.168.1.456)를 입력한다고 해도 시스템에서 경고하지 않는다는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

단계 **5** 서버가 시스템 로그 메시지에 사용할 포트를 **Port(**포트**)** 필드에 입력합니다. 기본적으로 이 값은 514로 설정됩니다.

단계 **6** **Facility(**시설**)** 목록에서 시스템 로그 알림 시설, 2685 페이지에 설명된 시설을 선택합니다.

단계 **7** **Severity(**심각도**)** 목록에서에 Syslog 심각도 레벨, 2686 페이지에 설명된 심각도를 선택합니다.

단계 **8** **Tag(**태그**)** 필드에 시스템 로그 메시지와 함께 표시할 태그 이름을 입력합니다.

예를 들어 시스템 로그로 전송된 모든 메시지를 `FromMC` 앞에 오도록 하는 경우, 필드에 `FromMC`를 입력합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

변경 사항은 즉시 적용됩니다. 단,

알림 응답을 사용해 시스템 로그 서버로 연결 로그를 보내는 경우 해당 알림 응답을 편집한 후 설정 변경 사항을 구축해야 합니다.

이 알림 응답을 보안 이벤트를 위해 사용하려는 경우에는, 정책에서 알림 응답을 지정해야 합니다. 보안 이벤트 시스템 로그에 대한 설정 위치, 2760 페이지의 내용을 참조하십시오.

시스템 로그 알림 시설

다음 표에는 선택 가능한 syslog 기능이 나와 있습니다.

표 *275:* 사용 가능한 *Syslog* 기능

기능	설명
ALERT	알림 메시지입니다.
AUDIT	감사 하위 시스템에 의해 생성된 메시지입니다.
AUTH	보안 및 인증과 관련된 메시지입니다.
AUTHPRIV	보안 및 인증과 관련된 제한적 액세스 메시지입니다. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다.
CLOCK	클록 데몬에 의해 생성된 메시지입니다. Windows 운영 체제를 실행하는 syslog 서버는 `CLOCK` 기능을 사용합니다.
CRON	클록 데몬에 의해 생성된 메시지입니다. Linux 운영 체제를 실행하는 syslog 서버는 `CRON` 기능을 사용합니다.
DAEMON	시스템 데몬에서 생성된 메시지입니다.
FTP	FTP 데몬에 의해 생성된 메시지입니다.
KERN	커널에 의해 생성된 메시지입니다. 여러 시스템에서 이 메시지가 나타나면 콘솔에 인쇄됩니다.
LOCAL0-LOCAL7	내부 프로세스에 의해 생성된 메시지입니다.
LPR	인쇄 하위 시스템에 의해 생성된 메시지입니다.
MAIL	메일 시스템에 의해 생성된 메시지입니다.
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지입니다.
NTP	NTP 데몬에 의해 생성된 메시지입니다.
SYSLOG	syslog 데몬에 의해 생성된 메시지입니다.
USER	사용자 레벨 프로세스에 의해 생성된 메시지입니다.
UUCP	UUCP 하위 시스템에 의해 생성된 메시지입니다.

Syslog 심각도 레벨

다음 표에는 선택 가능한 표준 syslog 심각도 레벨이 나와 있습니다.

표 ***276: Syslog*** 심각도 레벨

레벨	설명
ALERT	즉시 해결해야 하는 상태입니다.
CRIT	심각한 상태입니다.
DEBUG	디버깅 정보를 포함하는 메시지입니다.
EMERG	모든 사용자에게 알려진 위험 상태입니다.
ERR	오류 상태입니다.
INFO	정보를 제공하는 메시지입니다.
NOTICE	오류 상태는 아니지만 주의가 필요한 상태입니다.
WARNING	경고 메시지입니다.

이메일 알림 응답 생성

시작하기 전에

- Firepower Management Center이(가) 자체 IP 주소를 역확인할 수 있는지 확인합니다.
- 메일 릴레이 호스트를 메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지에 설명된 대로 설정합니다.

참고 이메일 알림을 이용해 연결을 기록할 수는 없습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create Email Alert(**이메일 알림 생성**)**을 선택합니다.

단계 **3** 알림 응답의 **Name(**이름**)**을 입력합니다.

단계 **4** **To(**수신인**)** 필드에 알림을 전송할 이메일 주소를 쉼표로 구분하여 입력합니다.

단계 **5** **From(**발신인**)** 필드에 알림 전송자로 표시할 이메일 주소를 입력합니다.

단계 **6** **Relay Host(**릴레이 호스트**)** 옆에 나열된 메일 서버가 알림을 전송하는 데 사용하려는 서버인지 확인합니다.

팁 이메일 서버를 변경하려면 수정( )을 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

영향 플래그 알림 설정

특정 영향 플래그의 침입 이벤트가 발생할 때마다 알림을 전송하도록 시스템을 설정할 수 있습니다. 영향 플래그는 침입 데이터, 네트워크 검색 데이터 및 취약성 정보를 상호 연결하여, 침입이 네트워크에 미치는 영향을 평가하는 데 도움이 됩니다.

이러한 알림을 설정하려면 위협 스마트 라이센스 또는 보호 클래식 라이센스가 있어야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**를 선택합니다.

단계 **2** **Impact Flag Alerts(**영향 플래그 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Impact Configuration(**영향 설정**)** 섹션에서 적절한 확인란을 선택하여 각 영향 플래그에 대해 수신할 알림을 지정합니다.

영향 플래그 정의는 침입 이벤트 영향 레벨, 2924 페이지 섹션을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

검색 이벤트 알림 설정

특정 유형의 검색 이벤트가 발생할 때마다 알리도록 시스템을 설정할 수 있습니다.

시작하기 전에

- 네트워크 검색 이벤트 기록 설정, 2558 페이지에 설명된 대로 알림을 설정할 검색 이벤트 유형을 기록하도록 네트워크 검색 정책을 설정합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Discovery Event Alerts(**검색 이벤트 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Events Configuration(**이벤트 설정**)** 섹션에서 각 검색 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

AMP for Networks 알림 설정

AMP for Networks(네트워크용 AMP)가 회귀 이벤트를 포함한 악성코드 이벤트를 생성할 때마다(즉 "네트워크 기반 악성코드 이벤트"가 생성될 때마다) 알림을 전송하도록 시스템을 설정할 수 있습니다. AMP for Endpoints(엔드포인트용 AMP)("엔드포인트 기반 악성코드 이벤트")가 생성한 악성코드 이벤트에 대한 알림은 만들 수 없습니다.

시작하기 전에

- 액세스 제어의 이해, 1609 페이지에 설명된 대로 악성코드 클라우드 조회를 수행하고 정책을 액세스 컨트롤 규칙과 연결하도록 파일 정책을 설정합니다.
- 이러한 알림을 설정하려면 악성 코드 라이선스가 있어야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Advanced Malware Protections Alerts(**고급 악성코드 보호 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Event Configuration(**이벤트 설정**)** 섹션에서 각 악성코드 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

All network-based malware events(모든 네트워크 기반 악성코드 이벤트**)**에는 **Retrospective Events(**회귀 이벤트**)**가 포함된다는 점에 유의하십시오.

(정의상, 네트워크 기반 악성코드 이벤트는 AMP for Endpoints(엔드포인트용 AMP)가 생성한 이벤트는 포함하지 않습니다.)

단계 **5** **Save(**저장**)**를 클릭합니다.

110 장

침입 이벤트에 대한 외부 알림

다음 주제에서는 침입 이벤트에 대한 외부 경고 설정 방법을 설명합니다.

- 침입 이벤트에 대한 외부 알림 정보, 2691 페이지
- 침입 이벤트 외부 알림 라이선스 요구 사항, 2692 페이지
- 침입 이벤트 외부 알림 요구 사항 및 사전 요건, 2692 페이지
- 침입 이벤트에 대한 SNMP 알림 설정, 2692 페이지
- 침입 이벤트를 위한 시스템 로그 알림 설정, 2694 페이지
- 침입 이벤트에 대한 이메일 알림 설정, 2696 페이지

침입 이벤트에 대한 외부 알림 정보

외부 침입 이벤트 알림으로 중요 시스템 모니터링을 지원할 수 있습니다.

- SNMP - 침입 정책별로 설정되며 매니지드 디바이스에서 전송됩니다. 침입 규칙별로 SNMP 알림을 활성화할 수 있습니다.
- Syslog(시스템 로그) - 침입 정책별로 설정되며 매니지드 디바이스에서 전송됩니다. 침입 규칙에서 시스템 로그 알림을 설정하는 경우, 정책의 모든 규칙에 대해 알림을 설정하게 됩니다.
- Email(이메일) - 모든 침입 정책에서 설정되며 Firepower Management Center에서 전송합니다. 침입 규칙별로 이메일 알림을 활성화하고, 알림의 길이와 빈도를 제한할 수 있습니다.

침입 이벤트 억제 또는 임계값 설정을 설정하는 경우, 시스템은 규칙이 트리거될 때마다 침입 규칙을 생성하지는 않는다는 점을(그리고 그에 따라 알림을 전송하지 않을 수도 있음을) 유의하십시오.

다중 도메인 구축의 경우, 모든 도메인에서 외부 알림을 설정할 수 있습니다. 상위 도메인의 경우, 시스템은 하위 도메인의 침입 이벤트에 대한 알림을 생성합니다.

참고

또한 Firepower Management Center은(는) SNMP, 시스템 로그, 이메일 알림 응답을 사용하여 다양한 유형의 외부 알림을 전송합니다(Firepower Management Center 알림 응답, 2681 페이지 참조). 시스템은 알림 응답을 이용해 개별 침입 이벤트를 바탕으로 알림을 보내지는 않습니다.

관련 항목

침입 정책의 침입 이벤트 알림 필터, 2025 페이지

침입 이벤트 외부 알림 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

침입 이벤트 외부 알림 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 이벤트에 대한 **SNMP** 알림 설정

침입 정책에서 외부 SNMP 알림을 활성화하면, 개별 규칙을 설정해 트리거 시 SNMP 알림을 보낼 수 있습니다. 이러한 알림은 매니지드 디바이스에서 전송됩니다.

프로시저

단계 **1** 침입 정책 편집기의 탐색창에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **SNMP Alerting(SNMP** 알림**)**이 **Enabled(**활성화**)**인지 확인하고 **Edit(**편집**)**를 클릭합니다.
페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다.

단계 **3** **SNMP** 버전을 클릭하고 침입 SNMP 알림 옵션, 2693 페이지에 설명된 대로 설정 옵션을 지정합니다.

단계 **4** 탐색 창에서 **Rules(**규칙**)**를 클릭합니다.

단계 5 규칙 창에서 SNMP 알림을 설정할 규칙을 선택하고 **Alerting(**알림**)** > **Add SNMP Alert(SNMP** 알림 추가**)**을(를) 선택합니다.

단계 6 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

침입 SNMP 알림 옵션

네트워크 관리 시스템에 Firepower Management Center의 MIB(Management Information Base) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

SNMP v2 옵션

옵션	설명
트랩 유형	경고에 나타나는 IP 주소를 사용할 트랩 유형입니다. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(**이진으로**)**을(를) 선택합니다. 그렇지 않은 경우에는 **as String(**문자열로**)**을 선택합니다. 예를 들어 HP OpenView는 **as String(**문자열로**)** 옵션이 필요합니다.
트랩 서버	SNMP 트랩 알림을 받을 서버입니다. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
커뮤니티 문자열	커뮤니티 이름입니다.

SNMP v3 옵션

매니지드 디바이스는 SNMPv3 알림을 Engine ID 값으로 인코딩합니다. 알림을 디코딩할 때 SNMP 서버는 이 값을 요구합니다. 이 값은 전송하는 디바이스의 인터페이스 IP 주소의 16진수 버전으로, "01"이 붙습니다.

예를 들어 SNMP 알림을 전송하는 디바이스의 관리 인터페이스 IP 주소가 172.16.1.50인 경우, Engine ID 값은 0xAC10013201입니다.

옵션	설명
트랩 유형	경고에 나타나는 IP 주소를 사용할 트랩 유형입니다. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(**이진으로**)**을(를) 선택합니다. 그렇지 않은 경우에는 **as String(**문자열로**)**을 선택합니다. 예를 들어 HP OpenView는 **as String(**문자열로**)** 옵션이 필요합니다.
트랩 서버	SNMP 트랩 알림을 받을 서버입니다. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
인증 비밀번호	인증을 위해 필요한 비밀번호입니다. SNMP v3은 이 비밀번호를 암호화하기 위해 메시지 다이제스트 5(MD5) 해시 함수 또는 보안 해시 알고리즘(SHA) 해시 함수를 사용하며, 이는 구성에 따른 것입니다. 인증 비밀번호를 지정한 경우, 인증이 활성화됩니다.
개인 비밀번호	프라이버시를 위한 SNMP 키입니다. SNMP v3은 이 비밀번호를 암호화하기 위해 데이터 암호화 표준(DES) 블록 암호를 사용합니다. SNMP v3 비밀번호를 입력할 때, 해당 비밀번호는 초기 구성 중에 일반 텍스트로 표시되지만 암호화된 형식으로 저장됩니다. 개인 비밀번호를 지정한 경우 프라이버시가 활성화되며, 인증 비밀번호도 반드시 지정해야 합니다.
User Name(사용자 이름)	SNMP 사용자 이름입니다.

침입 이벤트를 위한 시스템 로그 알림 설정

침입 정책에서 시스템 로그 알림을 활성화하면, 시스템은 모든 침입 이벤트를 매니지드 디바이스 자체 또는 외부 호스트의 시스템 로그로 전송합니다. 외부 호스트를 지정하는 경우, 시스템 로그 알림은 매니지드 디바이스에서 전송됩니다.

프로시저

단계 **1** 침입 정책 편집기의 탐색창에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **Syslog Alerting(**시스템 로그 알림**)**이 **Enabled(**활성화**)**인지 확인하고 **Edit(**편집**)**를 클릭합니다.
페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. **Syslog Alerting(**시스템 로그**)** 알림 페이지가 **Advanced Settings(**고급 설정**)**에 추가됩니다.

단계 **3** 시스템 로그 알림을 전송할 **Logging Hosts(**기록 호스트**)**의 IP 주소를 입력합니다.

Logging Hosts(기록 호스트**)** 필드를 입력하지 않는 경우 기록 호스트 상세정보는 연결된 Access Control Policy(액세스 컨트롤 정책)의 Logging(기록)에서 가져옵니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **4** 침입 시스템 로그 알림에 대한 시설 및 Severities(심각도), 2695 페이지에 설명된 대로 **Facility(**시설**)** 및 **Severity(**심각도**)**을(를) 선택합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

침입 시스템 로그 알림에 대한 시설 및 **Severities(**심각도**)**

매니지드 디바이스는 기록 호스트가 알림을 분류할 수 있도록, 특정 시설 및 **Severity(**심각도**)**를 사용하여 침입 이벤트를 시스템 로그 알림으로 전송할 수 있습니다. 시설은 이를 생성한 하위 시스템을 지정합니다. 이러한 시설 및 **Severity(**심각도**)** 값은 실제 시스템 로그 메시지에는 표시되지 않습니다.

환경에 맞는 합리적인 값을 선택합니다. 로컬 설정 파일(UNIX 기반 기록 호스트에서의 syslog.conf 등)은 어떤 시설이 어떤 로그 파일에 저장되는지를 나타내기도 합니다.

시스템 로그 알림 시설

기능	설명
AUTH	보안 및 인증과 관련된 메시지입니다.
AUTHPRIV	보안 및 인증과 관련된 제한적 액세스 메시지입니다. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다.
CRON	클록 데몬에 의해 생성된 메시지입니다.
DAEMON	시스템 데몬에서 생성된 메시지입니다.
FTP	FTP 데몬에 의해 생성된 메시지입니다.
KERN	커널에 의해 생성된 메시지입니다. 여러 시스템에서 이 메시지가 나타나면 콘솔에 인쇄됩니다.
LOCAL0-LOCAL7	내부 프로세스에 의해 생성된 메시지입니다.
LPR	인쇄 하위 시스템에 의해 생성된 메시지입니다.

기능	설명
MAIL	메일 시스템에 의해 생성된 메시지입니다.
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지입니다.
SYSLOG	syslog 데몬에 의해 생성된 메시지입니다.
USER	사용자 레벨 프로세스에 의해 생성된 메시지입니다.
UUCP	UUCP 하위 시스템에 의해 생성된 메시지입니다.

시스템 로그 알림 심각도

레벨	설명
EMERG	모든 사용자에게 브로드캐스팅되는 공황 상태
ALERT	즉시 수정되어야 하는 상태
CRIT	심각한 상태
ERR	오류 상태
WARNING	경고 메시지
NOTICE	오류 상태는 아니지만 주의 필요
INFO	정보를 제공하는 메시지
DEBUG	디버그 정보를 포함하는 메시지

침입 이벤트에 대한 이메일 알림 설정

침입 이메일 알림을 활성화한 경우, 시스템은 침입을 매니지드 디바이스가 탐지했는지 침입 정책이 탐지했지와는 상관없이, 침입 이벤트 생성 시 이메일을 전송할 수 있습니다. 이러한 알림은 Firepower Management Center에서 전송됩니다.

시작하기 전에

- 이메일 알림을 받을 메일 호스트 설정합니다(메일 릴레이 호스트 및 알림 주소 구성, 1374 페이지 참조).
- Firepower Management Center이(가) 자체 IP 주소를 역확인할 수 있는지 확인합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Intrusion Email(**침입 이메일**)**을 클릭합니다.

단계 **3** 알림을 생성할 침입 규칙 또는 규칙 그룹을 포함한, 알림 옵션을 침입 이메일 알림 옵션, 2697 페이지에 설명된 대로 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

침입 이메일 알림 옵션

On/Off(켜기/끄기**)**

침입 이메일 알림을 활성화 또는 비활성화합니다.

참고 활성화하면 개별 규칙을 선택하기 전에는 모든 규칙에 대한 알림이 활성화됩니다.

From/To Addresses(발신자/수신자 주소**)**

이메일 발신자 및 수신자입니다. 쉼표로 구분된 수신자 목록을 지정할 수 있습니다s.

최대 알림 및 빈도

Firepower Management Center이(가) 시간 간격(**Frequency(**빈도**)**)마다 전송할 이메일 알림의 최대 수(**Max Alerts(**최대 알림**)**)입니다.

알림 병합

같은 소스 IP와 규칙 ID를 이용하는 알림을 그룹화하여 전송하는 알림 수를 줄입니다.

요약 출력

텍스트 제한 디바이스에 적합한 짧은 알림을 활성화합니다. 짧은 알림은 다음 정보를 포함합니다.

- 타임스탬프
- 프로토콜
- 소스 및 목적지 IP와 포트
- Message
- 동일한 소스 IP에 대해 생성되는 침입 이벤트의 수

예: `2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: 알 수 없는 Datagram 디코딩 문제! (116:108)`

Summary Output(요약 출력**)**을 활성화하는 경우에는 **Coalesce Alerts(**알림 병합**)** 활성화도 고려해보십시오. 텍스트 메시지 제한 초과 예방을 위해 **Max Alerts(**최대 알림**)**를 낮춰야 할 수도 있습니다.

표준 시간대

알림 타임스탬프의 시간대입니다.

특정 규칙 설정에 관한 이메일 알림

이메일 알림을 설정할 규칙을 선택할 수 있습니다.

XXIII 부

이벤트 및 자산 분석 툴

- Context Explorer 사용, 2701 페이지
- 네트워크 맵 사용, 2727 페이지
- 인시던트, 2739 페이지
- 조회 사용, 2747 페이지
- 외부 툴을 사용하여 이벤트 분석, 2749 페이지

111 장

Context Explorer 사용

다음 주제에서는 Firepower System에서 Context Explorer(상황 탐색기)를 사용하는 방법을 설명합니다.

- Context Explorer(상황 탐색기) 정보, 2701 페이지
- Context Explorer 요구 사항 및 사전 요건, 2716 페이지
- Context Explorer(상황 탐색기) 새로 고침, 2717 페이지
- Context Explorer(상황 탐색기) 시간 범위 설정, 2717 페이지
- Context Explorer(상황 탐색기) 섹션 최소화 및 최대화, 2718 페이지
- Context Explorer(상황 탐색기) 데이터에 대해 드릴다운, 2718 페이지
- Context Explorer의 필터, 2719 페이지

Context Explorer(상황 탐색기) 정보

Firepower System Context Explorer(상황 탐색기)는 애플리케이션에 대한 데이터, 애플리케이션 통계, 연결, 지리위치, IOC, 침입 이벤트, 호스트, 서버, 보안 인텔리전스, 사용자, 파일(악성코드 파일 포함), 관련 URL 등 모니터링 중인 네트워크의 상태에 대한 자세한 인터랙티브 그래픽 정보를 콘텍스트에 맞게 표시합니다. 개별 섹션은 이 데이터를 선명한 선, 막대, 파이, 도넛 그래프 형식과 자세한 목록으로 표시합니다. 첫 번째 섹션인 시간 경과에 따른 트래픽 및 이벤트 카운트의 선 그래프는 네트워크 활동의 최신 추세를 한눈에 볼 수 있는 그림을 제공합니다.

간편하게 맞춤형 필터를 만들고 적용하여 정밀 분석을 수행할 수 있으며, 그래프 영역을 클릭하거나 커서를 올려놓기만 하면 데이터 섹션을 자세히 확인할 수 있습니다. 또한 탐색기의 시간 범위를 마지막 시간 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수도 있습니다. Administrator(관리자), Security Analyst(보안 분석가) 또는 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 사용자 역할이 있는 사용자만 Context Explorer(상황 탐색기)에 액세스할 수 있습니다.

Firepower System 대시보드는 세부적으로 맞춤화 및 구획화할 수 있으며 실시간으로 업데이트됩니다. 반면 Context Explorer(상황 탐색기)는 수동으로 업데이트되고, 데이터에 대한 더 넓은 범위의 콘텍스트를 제공하도록 설계되었으며, 활성 사용자 탐색에 편리하도록 일관된 단일 레이아웃을 제공합니다.

특정 요구에 맞게 네트워크 및 어플라이언스에서 실시간 활동을 모니터링하려면 대시보드를 사용합니다. 반대로, 매우 세분화되고 분명한 상황에서 사전 정의된 최신 데이터 세트를 조사하려면 Context

Explorer(상황 탐색기)를 사용합니다. 예를 들어 네트워크의 호스트 중 15%만 Linux를 사용하지만 여기에서 거의 모든 YouTube 트래픽이 생성되는 경우 필터를 신속하게 적용하여 Linux 호스트 또는 YouTube 관련 애플리케이션 데이터만 보거나 두 가지 데이터를 모두 볼 수 있습니다. 간결하고 매우 집중적인 대시보드 위젯과는 달리 Context Explorer(상황 탐색기) 섹션은 시스템 활동을 Firepower System의 전문가는 물론 일반 사용자도 알기 쉬운 유용한 형식으로 시각적으로 표시하도록 설계되었습니다.

표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다. 필터를 적용해 모든 Context Explorer(상황 탐색기) 섹션에 표시되는 데이터를 제한할 수도 있습니다.

다중 도메인 구축의 경우, Context Explorer(상황 탐색기)는 사용자가 상위 도메인에서 데이터를 확인할 때 모든 하위 도메인에서 집계된 데이터를 표시합니다. 리프 도메인의 경우에는 해당 도메인과 관련된 데이터만 확인할 수 있습니다.

대시보드 및 **Context Explorer** 간 차이

다음 표에는 대시보드와 Context Explorer(상황 탐색기)의 주요 차이점이 요약되어 있습니다.

표 ***277:*** 비교*:* 대시보드 및 ***Context Explorer(***상황 탐색기***)***

기능	대시보드	**Context Explorer(**상황 탐색기**)**
표시 가능한 데이터	Firepower System이 모니터링하는 모든 데이터	애플리케이션, 애플리케이션 통계, 지리 위치, 침해 지표, 침입 이벤트, 파일(악성 코드 파일 포함), 호스트, Security Intelligence(보안 인텔리전스) 이벤트, 서버, 사용자, URL
맞춤형 가능	• 대시보드를 맞춤형할 수 있는 위젯 선택 • 개별 위젯은 다양한 수준으로 맞춤형할 수 있음	• 기본 레이아웃은 변경 불가 • 적용된 필터는 탐색기 URL에 나타나며 나중에 사용하도록 북마크 처리 가능
데이터 업데이트 빈도	자동(기본값): 사용자가 구성함	수동
데이터 필터링	일부 위젯에 대해 가능(위젯 환경설정을 수정해야 함)	(탐색기의 모든 부분에 대해 가능하며 다중 필터 지원
그래픽 콘텍스트	일부 위젯(특히 Custom Analysis)은 데이터를 그래픽 형식으로 표시 가능	매우 자세한 도넛 그래프를 포함하여 폭넓은 그래픽 콘텍스트로 모든 데이터 표시 가능
관련 웹 인터페이스 페이지에 대한 링크	일부 위젯에서	모든 섹션에서
표시된 데이터의 시간 범위	사용자가 구성함	사용자가 구성함

관련 항목

대시보드 정보, 363 페이지

트래픽 및 침입 이벤트 횟수 시간 그래프

Context Explorer(상황 탐색기) 상단에는 시간 경과에 따른 트래픽 및 침입 이벤트의 선 그래프가 있습니다. X축은 시간 간격을 나타냅니다(선택한 시간 창에 따라 5분에서 1개월까지). Y축은 킬로바이트 단위의 트래픽(파란색 선) 및 침입 이벤트 카운트(빨간색 선)를 나타냅니다.

X축의 최소 간격은 5분입니다. 이를 위해 시스템에서는 선택한 기간의 시작 지점과 종료 지점을 가장 가까운 5분 간격으로 반올림합니다.

기본적으로 이 섹션에는 선택한 기간의 모든 네트워크 트래픽 및 생성된 모든 침입 이벤트가 표시됩니다. 필터를 적용하면 필터에 지정된 기준과 관련이 있는 트래픽 및 침입 이벤트만 표시하도록 차트가 변경됩니다. 예를 들어 `Windows`의 **OS Name**으로 필터링하면 시간 그래프에는 Windows 운영체제를 사용하는 호스트와 관련된 트래픽 및 이벤트만 표시됩니다.

침입 이벤트 데이터로 Context Explorer(상황 탐색기)를 필터링하면(예: **Priority**가 `High`) 침입 이벤트에 더 집중할 수 있도록 파란색 트래픽 선이 숨겨집니다.

트래픽 및 이벤트 카운트에 대한 정확한 정보를 보려면 포인터를 그래프 선의 특정 지점에 올려놓을 수 있습니다. 색이 있는 선 중 하나로 포인터를 가져가면 해당 선이 그래프 앞으로 이동하므로 콘텍스트를 더 자세히 볼 수 있습니다.

이 섹션에서는 주로 Intrusion Events(침입 이벤트) 및 Connection Events(연결 이벤트) 테이블의 데이터를 보여줍니다.

보안 침해 지표 섹션

Context Explorer의 IOC(Indications of Compromise, 보안 침해 지표) 섹션에는 모니터링되는 네트워크에서 감염 가능성이 있는 호스트를 전체적으로 보여주는 두 개의 인터랙티브 섹션이 있습니다. 이 둘은 각각 트리거된 가장 일반적인 IOC 유형의 비례 보기 및 트리거된 지표 수 기준의 호스트 보기입니다.

IOC에 관한 자세한 내용은 보안 침해 지표 데이터, 3056 페이지 섹션을 참조하십시오.

지표별 호스트 그래프

도넛 형식의 Hosts by Indication 그래프는 모니터링되는 네트워크에서 호스트별로 트리거된 IOC의 비례 보기를 제공합니다. 내부 원에는 카테고리(예: `CnC Connected` 또는 `Malware Detected`)로 구분된 내용이 표시되며, 외부 원에는 특정 이벤트 유형(예: `Impact 2 Intrusion Event - attempted-admin` 또는 `Threat Detected in File Transfer`)별로 그러한 데이터가 더 자세히 구분되어 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 IOC 테이블의 데이터를 주로 보여줍니다.

호스트별 지표 그래프

막대 형식의 Indications by Host 그래프에는 모니터링되는 네트워크에서 IOC가 가장 높은 호스트 15개에 의해 트리거된 고유한 보안 침해 지표(IOC)의 개수가 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 IOC 테이블의 데이터를 주로 보여줍니다.

네트워크 정보 섹션

Context Explorer(상황 탐색기)의 Network Information(네트워크 정보) 섹션에는 소스, 목적지, 사용자, 트래픽과 관련된 보안 영역, 네트워크의 호스트에서 사용하는 운영체제 구분, Firepower System이 네트워크에서 수행한 액세스 컨트롤 작업의 비례 보기 등 모니터링되는 네트워크의 연결 트래픽을 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다.

운영 체제 그래프

도넛 형식의 Operating Systems 그래프는 모니터링하는 네트워크의 호스트에서 탐지한 운영체제의 비율을 표시합니다. 내부 원에는 OS 이름(예: `Windows` 또는 `Linux`)으로 구분된 내용이 표시되며, 외부 원에는 특정 운영체제 버전(예: `Windows Server 2008` 또는 `Linux 11.x`)별 데이터가 더 자세히 구분되어 표시됩니다. 일부 긴밀하게 연결된 운영체제(예: Windows 2000, Windows XP 및 Windows Server 2003)는 그룹화됩니다. 매우 드물거나 인식되지 않는 운영체제는 **Other(**기타**)**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 그래프는 변경되지 않습니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 테이블의 데이터를 주로 보여줍니다.

소스 **IP**별 트래픽 그래프

막대 형식의 Traffic by Source IP 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source IP 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

소스 사용자별 트래픽 그래프

막대 형식의 Traffic by Source User 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 사용자 15명에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source User 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다. 신뢰할 수 있는 사용자 데이터를 표시합니다.

액세스 제어 작업별 연결 그래프

원 형식의 Connections by Access Control Action 그래프는 Firepower System이 모니터링되는 트래픽에서 수행한 액세스 컨트롤 작업(예: `Block(차단)` 또는 `Allow(허용)`)의 비례 보기를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source User 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

대상 **IP**별 트래픽 그래프

막대 형식의 Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 가장 활발한 목적지 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 목적지 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Destination IP 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

인그레스/이그레스 보안 영역별 트래픽 그래프

막대 형식의 Traffic by Ingress/Egress Security Zone 그래프는 모니터링되는 네트워크에 구성된 각 보안 영역에 대한 들어오는 또는 나가는 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카

운트를 보여줍니다. 필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

나열된 각 보안 영역에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Ingress/Egress Security Zone 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

애플리케이션 정보 섹션

Context Explorer(상황 탐색기)의 Application Information(애플리케이션 정보) 섹션에는 모니터링되는 네트워크에서 전반적인 애플리케이션 활동 내용을 보여주는 인터랙티브 그래프 3개 및 테이블 형식의 목록 1개가 있습니다. 트래픽, 침입 이벤트, 애플리케이션과 관련된 호스트 등은 각 애플리케이션에 할당된 비즈니스 연관성 또는 추정 위험 단위로 더 세부적으로 구성됩니다. Application Details List(애플리케이션 상세정보 목록)는 위험, 비즈니스 연관성, 카테고리 및 호스트 카운트의 인터랙티브 목록을 제공합니다.

이 섹션의 모든 "애플리케이션" 인스턴스에서 기본적으로 애플리케이션 정보 그래프 집합은 특별히 애플리케이션 프로토콜(예: DNS 또는 SSH)을 검사합니다. 특별히 클라이언트 애플리케이션(예: PuTTY 또는 Firefox) 또는 웹 애플리케이션(예: Facebook 또는 Pandora)을 검사하도록 Application Information(애플리케이션 정보) 섹션을 설정할 수도 있습니다.

애플리케이션 정보 섹션 초점

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** **Application Protocol Information(**애플리케이션 프로토콜 정보**)** 섹션으로 포인터를 이동합니다.

참고 동일한 Context Explorer(상황 탐색기) 세션에서 전에 이 설정을 변경한 경우에는 섹션 제목이 **Client Application Information(**클라이언트 애플리케이션 정보**)** 또는 **Web Application Information(**웹 애플리케이션 정보**)**으로 표시될 수 있습니다.

단계 **3** **Application Protocol(**애플리케이션 프로토콜**)**, **Client Application(**클라이언트 애플리케이션**)** 또는 **Web Application(**웹 애플리케이션**)**을 클릭합니다.

위험/비즈니스 관련성 및 애플리케이션별 트래픽 그래프

도넛 형식의 Traffic by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크에서 탐지되는 애플리케이션 트래픽의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 그래프는 변경되지 않습니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Risk/Business Relevance and Application 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 및 Application Statistics(애플리케이션 통계) 테이블의 데이터를 주로 보여줍니다.

위험/비즈니스 관련성 및 애플리케이션별 침입 이벤트 그래프

도넛 형식의 Intrusion Events by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 침입 이벤트의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 침입 이벤트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 및 Application Statistics(애플리케이션 통계) 테이블의 데이터를 주로 보여줍니다.

위험/비즈니스 관련성 및 애플리케이션별 호스트 그래프

도넛 형식의 Hosts by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 호스트의 비례 표시를 관련 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`) 별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Applications(애플리케이션) 테이블의 데이터를 주로 보여줍니다.

애플리케이션 상세정보 목록

Application Information(애플리케이션 정보) 섹션 아래쪽에는 Application Details List(애플리케이션 상세정보 목록)가 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 애플리케이션에 대한 예상 위험, 예상 비즈니스 연관성, 카테고리 및 호스트 카운트 정보를 제공하는 테이블입니다. 애플리케이션은 관련 호스트 카운트의 내림차순으로 나열됩니다.

Application Details List(애플리케이션 상세정보 목록) 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다. 이 테이블에서는 Applications(애플리케이션) 테이블의 데이터를 주로 보여줍니다.

이 목록은 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 목록은 변경되지 않습니다.

보안 인텔리전스 섹션

상황 탐색기의 Security Intelligence(보안 인텔리전스) 섹션에는 보안 인텔리전스에서 모니터링하거나 차단한 모니터링되는 네트워크의 트래픽을 전체적으로 보여주는 세 개의 인터랙티브 막대 그래프가 있습니다. 그래프에서 그러한 트래픽은 카테고리, 소스 IP 주소, 대상 IP 주소로 각각 정렬됩니다. 트래픽의 양(초당 킬로바이트 단위) 및 해당 연결 수가 모두 나타납니다.

카테고리별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Category 그래프는 모니터링되는 네트워크에서 상위 보안 인텔리전스 카테고리에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Category 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

소스 IP별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Source IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 소스 IP 주소에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Source IP 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

대상 IP별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 목적지 IP 주소에 대한 네트워크 트래픽(초당 킬로바이

트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Destination IP 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

침입 정보 섹션

Context Explorer(상황 탐색기)의 Intrusion Information(침입 정보) 섹션에는 모니터링되는 네트워크의 침입 이벤트를 전체적으로 보여주는 인터랙티브 그래프 6개와 테이블 형식의 목록 1개가 있습니다. 여기에는 영향 레벨, 공격 소스, 대상 목적지, 사용자, 우선순위 레벨, 침입 이벤트와 관련된 보안 영역과 더불어 침입 이벤트 분류, 우선순위 및 카운트의 자세한 목록이 포함됩니다.

영향별 침입 이벤트 그래프

원 형식의 Intrusion Events by Impact 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 영향 레벨(0~4)로 그룹화하여 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프는 침입 탐지(IDS 통계) 및 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 공격자 그래프

막대 형식의 Top Attackers 그래프는 모니터링되는 네트워크에서 상위 공격 호스트 IP 주소(이벤트를 일으키는)에 대한 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 사용자 그래프

막대 형식의 Top Users 그래프는 최고 침입 이벤트 카운트와 관련된 모니터링되는 네트워크의 사용자를 이벤트 카운트 단위로 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프는 침입 탐지(IDS) 사용자 통계 및 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다. 신뢰할 수 있는 사용자 데이터를 표시합니다.

우선 순위별 침입 이벤트 그래프

원 형식의 Intrusion Events by Priority 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 우선순위 레벨(예: `High`, `Medium` 또는 `Low`)로 그룹화하여 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 대상 그래프

막대 형식의 Top Targets 그래프는 모니터링되는 네트워크에서 상위 대상 호스트 IP 주소(이벤트를 일으키는 연결의 대상)에 대한 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 인그레스/이그레스 보안 영역 그래프

막대 형식의 Top Ingress/Egress Security Zones 그래프는 모니터링되는 네트워크에 설정된 각 보안 영역(그래프 설정에 따라 Ingress 또는 Egress)과 관련된 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

침입 이벤트 상세정보 목록

Intrusion Information(침입 섹션 아래쪽에는 Intrusion Event Details List(침입 이벤트 상세정보 목록)이 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 침입 이벤트에 대한 분류, 예상 우선순위 및 이벤트 카운트 정보를 제공하는 테이블입니다. 이벤트는 이벤트 카운트의 내림차순으로 나열됩니다.

Intrusion Event Details List(침입 이벤트 상세정보 목록) 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 이 테이블에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

파일 정보 섹션

Context Explorer의 Files Information(파일 정보) 섹션에는 모니터링되는 네트워크의 파일 및 악성코드 이벤트를 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다.

6개 중 5개 그래프에는 AMP for Networks (구 AMP for Firepower) 관련 데이터, 즉 네트워크 트래픽에서 탐지되는 파일의 악성코드 속성, 파일 형식, 파일 이름과 이러한 파일을 보내는(업로드) 호스트 및 받는(다운로드) 호스트가 표시됩니다. 마지막 그래프에는 AMP for Networks 또는 AMP for Endpoints가 조직에서 탐지한 모든 악성코드 위협이 표시됩니다.

참고 침입 정보에 대해 필터링하는 경우 전체 Files Information(파일 정보) 섹션은 표시되지 않습니다.

상위 파일 유형 그래프

도넛 형식의 Top File Types 그래프는 네트워크 트래픽에서 탐지되는 파일 형식(외부 원)의 비례 보기를 파일 카테고리(내부 원)로 그룹화하여 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 파일 이름 그래프

막대 형식의 Top File Names 그래프는 네트워크 트래픽에서 탐지되는 고유한 상위 파일 이름의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

성향별 파일 그래프

원 형식의 Top File Types 그래프는 AMP for Networks 기능(구 AMP for Firepower)으로 탐지한 악성코드 성향의 비율을 표시합니다. 성향은 Firepower Management Center이(가) 악성코드 클라우드 조회를 수행한 파일에만 있습니다. 클라우드 조회를 트리거하지 않은 파일은 `N/A` 성향을 갖습니다. `Unavailable` 성향은 Firepower Management Center에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 호스트 전송 파일 그래프

막대 형식의 Top Hosts Sending Files 그래프는 상위 파일 전송 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 전송 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware(**악성코드**)**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files(**파일**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 파일 보기로 돌아갑니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 호스트 수신 파일 그래프

막대 형식의 Top Hosts Receiving Files 그래프는 상위 파일 수신 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 수신 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware(**악성코드**)**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files(**파일**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 파일 보기로 돌아갑니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 악성코드 탐지 그래프

막대 형식의 op Malware Detections 그래프에는 AMP for Networks 또는 AMP for Endpoints가 조직에서 탐지한 상위 악성코드 위협 숫자가 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 및 Malware Events(악성코드 이벤트) 테이블의 데이터를 주로 보여줍니다.

지리위치 정보 섹션

Context Explorer(상황 탐색기)의 Geolocation Information(지리위치 정보) 섹션에는 모니터링되는 네트워크의 호스트가 데이터를 교환하는 국가를 전체적으로 보여주는 3개의 인터랙티브 도넛 그래프가 있습니다. 이러한 그래프는 각각 이니시에이터 또는 응답자 국가 단위의 고유한 연결, 소스 또는 대상 국가 단위의 침입 이벤트, 수신 또는 송신 국가 단위의 파일 이벤트에 대한 것입니다.

이니시에이터/응답자 국가별 연결 그래프

도넛 형식의 Connections by Initiator/Responder Country 그래프는 이니시에이터(기본값) 또는 응답자로서 네트워크의 연결과 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 응답자 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Responder(**응답자**)**를 클릭합니다. 기본 보기로 돌아가려면 **Initiator(**이니시에이터**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Initiator 보기로 돌아갑니다.

이 그래프에서는 Connection Summary Data(연결 요약 데이터) 테이블의 데이터를 주로 보여줍니다.

소스/목적지 국가별 침입 이벤트 그래프

도넛 형식의 Intrusion Events by Source/Destination Country 그래프는 이벤트의 소스(기본값) 또는 목적지로서 네트워크의 침입 이벤트와 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 침입 이벤트의 목적지 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Destination(**목적지**)**을 클릭합니다. 기본 보기로 돌아가려면 **Source(**소스**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Source 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

전송/수신 국가별 파일 이벤트 그래프

도넛 형식의 File Events by Sending/Receiving Country 그래프는 네트워크의 파일 이벤트에서 파일을 전송하거나(기본값) 수신하는 것으로 탐지되는 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 파일 수신 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Receiver(**수신자**)**를 클릭합니다. 기본 보기로 돌아가려면 **Sender(**발신자**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Sender 보기로 돌아갑니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 정보 섹션

Context Explorer의 URL Information 섹션에는 모니터링되는 사용자 네트워크의 호스트가 데이터를 교환하는 URL을 전체적으로 보여주는 3개의 인터랙티브 막대 그래프가 있습니다. 여기에는 URL과 연결된 트래픽 및 고유한 연결이 포함되며 개별 URL, URL 카테고리 및 URL 평판 단위로 정렬됩니다. URL 정보에 대해서는 필터링할 수 없습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 전체 URL Information(URL 정보) 섹션은 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

URL별 트래픽 그래프

막대 형식의 Traffic by URL 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL 그래프는 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 카테고리별 트래픽 그래프

막대 형식의 Traffic by URL Category 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 카테고리(예: `Search Engines(검색 엔진)` 또는 `Streaming Media(스트리밍 미디어)`)에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL Category 그래프는 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

이 그래프에서는 URL Statistics(URL 통계) 및 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 평판별 트래픽 그래프

막대 형식의 Traffic by URL Reputation(URL 평판별 트래픽) 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 평판 그룹(예: , Trusted(신뢰할 수 있는), 또는 , Neutral(보통))에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL 평판에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL Reputation 그래프는 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

이 그래프에서는 URL Statistics(URL 통계) 및 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

Context Explorer 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 보안 분석가

Context Explorer(상황 탐색기) 새로 고침

Context Explorer(상황 탐색기)는 표시되는 정보를 자동으로 업데이트하지 않습니다. 새로운 데이터를 표시하려면 탐색기를 수동으로 새로 고쳐야 합니다.

Context Explorer(상황 탐색기) 자체를 다시 고치면(브라우저 프로그램을 새로 고치거나 Context Explorer(상황 탐색기)에서 나간 후 다시 돌아오는 방법 사용) 표시되는 모든 정보를 새로 고칠 수 있지만, 섹션 설정에 대해 변경한 내용(예: Ingress/Egress 그래프 및 애플리케이션 정보 섹션)이 유지되지 않으며 로딩에 지연이 발생할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 오른쪽 위에 있는 **Reload(**다시 로드**)**를 클릭합니다.

새로 고침이 완료되기 전까지 **Reload(**다시 로드**)**는 흐리게 표시됩니다.

Context Explorer(상황 탐색기) 시간 범위 설정

Context Explorer(상황 탐색기)의 시간 범위를 마지막 시간 단위(기본값)로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다. 시간 범위를 변경해도 변경 사항을 반영하여 Context Explorer(상황 탐색기)가 자동으로 업데이트되지는 않습니다. 새로운 시간 범위를 적용하려면 탐색기를 수동으로 새로 고쳐야 합니다.

Context Explorer(상황 탐색기)에서 빠져나가거나 로그인 세션을 종료해도 시간 범위에 대한 변경 사항은 유지됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** **Show the last(**마지막 선택 표시**)** 드롭다운 목록에서 시간 범위를 선택합니다.

단계 **3** 선택적으로, 새 시간 범위의 데이터를 보려면 **Reload(**다시 로드**)**를 클릭합니다.

팁 **Apply Filters(**필터 적용**)**를 클릭해도 시간 범위 업데이트가 적용됩니다.

Context Explorer(상황 탐색기) 섹션 최소화 및 최대화

하나 이상의 Context Explorer(상황 탐색기) 섹션을 최소화할 수 있습니다. 이는 특정 섹션에만 집중하거나 더 간단한 보기를 원하는 경우 유용합니다. Traffic and Intrusion Event Counts Time 그래프는 최소화할 수 없습니다.

페이지를 새로 고치거나 어플라이언스에서 로그아웃해도 최소화 또는 최대화 구성 상태는 Context Explorer(상황 탐색기) 섹션에서 그대로 유지됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 섹션을 최소화하려는 경우에는 섹션 제목 표시줄의 최소화(−)를 클릭합니다.

단계 **3** 섹션을 최대화하려면 최소화된 섹션에서 제목 표시줄의 최대화(최대화(□))를 클릭합니다.

Context Explorer(상황 탐색기) 데이터에 대해 드릴다운

Context Explorer(상황 탐색기)에서 허용하는 것보다 더 자세히 그래프 또는 목록의 데이터를 검사하려면 관련 데이터의 테이블 보기로 드릴다운할 수 있습니다. (Traffic and Intrusion Events over Time 그래프에서는 드릴다운할 수 없습니다.) 예를 들어 Traffic by Source IP 그래프에서 IP 주소를 드릴다운하면 Connection Events(연결 이벤트) 테이블의 Connections with Application Details(애플리케이션 상세정보 연결) 보기가 표시되며, 선택한 소스 IP 주소와 연결된 데이터만 포함됩니다.

검사하는 데이터 유형에 따라 콘텍스트 메뉴에 추가 옵션이 표시될 수 있습니다. 특정 IP 주소와 관련된 데이터 포인트는 선택하는 IP 주소에서 호스트 또는 whois 정보를 볼 수 있는 옵션을 제공합니다. 특정 애플리케이션과 관련된 데이터 포인트는 선택하는 애플리케이션에 대한 애플리케이션 정보를 볼 수 있는 옵션을 제공합니다. 특정 사용자와 관련된 데이터 포인트는 해당 사용자의 사용자 프로파일 페이지를 볼 수 있는 옵션을 제공합니다. 침입 이벤트 메시지와 관련된 데이터 포인트는 해당 이

벤트와 관련된 침입 규칙에 대한 규칙 문서를 볼 수 있는 옵션을 제공하며, 특정 IP 주소와 관련된 데이터 포인트는 해당 주소를 차단 또는 차단 금지 목록에 추가할 수 있는 옵션을 제공합니다. 이 목록에 대한 자세한 내용은 글로벌 및 도메인 보안 인텔리전스 목록, 598 페이지와 그 하위 항목을 참조하십시오.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(분석)** > **Context Explorer(상황 탐색기)**을(를) 선택합니다.

단계 **2** **Traffic and Intrusion Events over Time**을 제외한 임의의 섹션에서 조사하려는 데이터 포인트를 클릭합니다.

단계 **3** 선택한 데이터 포인트에 따라 여러 가지 옵션이 표시됩니다.

- 테이블 보기에서 이 데이터를 더 자세히 살펴보려면 **Drill into Analysis(분석을 위해 드릴다운)**를 선택합니다.
- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 관련 호스트에 대해 자세히 알아보려면 **View Host Information(호스트 정보 보기)**을 선택합니다.
- 특정 IP 주소의 데이터 포인트를 선택했으며 해당 주소에서 whois 검색을 수행하려면 **Whois**를 선택합니다.
- 특정 애플리케이션과 관련된 데이터 포인트를 선택했으며 해당 애플리케이션에 대해 자세히 알아보려면 **View Application Information(애플리케이션 정보 보기)**을 선택합니다.
- 특정 사용자와 관련된 데이터 포인트를 선택했으며 해당 사용자에 대해 자세히 알아보려면 **View User Information(사용자 정보 보기)**을 선택합니다.
- 특징 침입 이벤트 사용자와 관련된 데이터 포인트를 선택했으며 관련된 침입 규칙에 대해 자세히 알아보려면 **View Rule Documentation(규칙 문서 보기)**을 선택합니다. 원한다면 **Rule Documentation(규칙 문서)**을 클릭해 더 구체적인 규칙 상세정보를 확인합니다.
- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 해당 IP 주소를 보안 인텔리전스 전역 차단 및 차단 금지 목록에 추가하려면 적절한 옵션을 선택합니다.

Context Explorer의 필터

Context Explorer(상황 탐색기)에 처음 표시되는 기본적인 광범위한 데이터를 이용해 네트워크의 활동에 대해 좀 더 세부적인 콘텍스트를 얻기 위해 이러한 데이터를 필터링할 수 있는 옵션이 제공됩니다. 필터는 모든 유형의 Firepower System 데이터(URL 정보 제외)를 포괄하며, 포함과 제외를 지원하고, Context Explorer(상황 탐색기) 그래프 데이터 포인트에서 클릭하여 빠르게 적용될 수 있으며, 전체 Explorer에 영향을 미칩니다. 한 번에 최대 20개의 필터를 적용할 수 있습니다.

Context Explorer(상황 탐색기) 데이터에 여러 방법으로 필터를 추가할 수 있습니다.

- Add Filter(필터 추가) 대화 상자에서

- 탐색기에서 데이터 포인트를 선택한 경우 콘텍스트 메뉴에서
- 특정 상세정보 보기 페이지(Application Detail, Host Profile, Rule Detail 및 User Profile)에 나타나는 텍스트 링크에서 이러한 링크를 클릭하면 상세정보 보기 페이지의 관련 데이터에 따라 Context Explorer(상황 탐색기)가 자동으로 열리고 필터링이 수행됩니다. 예를 들어 사용자 `jenkins`에 대한 사용자 상세정보 페이지에서 Context Explorer(상황 탐색기) 링크를 클릭하면 해당 사용자와 관련된 데이터만 표시하도록 탐색기가 제한됩니다.

일부 필터 유형은 다른 유형과 호환되지 않습니다. 예를 들어 침입 이벤트(예: **Device** 및 **Inline Result**)와 관련된 필터는 연결 이벤트와 관련된 필터(예: **Access Control Action**)와 동시에 적용할 수 없습니다. 시스템에서 연결 이벤트 데이터와 침입 이벤트 데이터를 정렬할 수 없기 때문입니다. 시스템에서는 호환되지 않는 필터가 동시에 적용되는 것을 방지합니다. 한 필터 유형이 좀 더 최근에 활성화되었으면, 비호환성이 존재하는 한 호환되지 않는 유형의 필터는 표시되지 않습니다.

여러 필터가 활성화된 경우 동일한 데이터 유형에 대한 값은 OR 검색 기준으로 취급되므로, 적어도 하나의 값과 일치하는 모든 데이터가 표시됩니다. 서로 다른 데이터 유형에 대한 값은 AND 검색 기준으로 취급되므로, 데이터는 필터링하는 각 데이터 유형에 대해 적어도 하나의 값과 일치해야 합니다. 예를 들어 `Application: 2channel`, `Application: Reddit` 및 `User: edickinson` 필터 집합에 대해 나타나는 데이터는 사용자 `edickinson` 및**(AND)** 애플리케이션 `2channel` 또는**(OR)** 애플리케이션 `Reddit`과 관련이 있어야 합니다.

다중 도메인 구축의 경우 상위 도메인에서 Context Explorer(상황 탐색기)를 볼 때 여러 하위 도메인을 필터링할 수 있습니다. 이 경우 **IP Address(IP 주소)** 필터를 추가할 때 주의해야 합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 리터럴 IP 주소를 사용하여 이 설정을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다.

참고 필터는 필요한 정확한 Firepower 데이터 콘텍스트를 특정 시간에 얻기 위한 간단하고 민첩한 툴 역할을 합니다. 필터의 목적은 영구적인 설정 설정이 아니며, Context Explorer(상황 탐색기)에서 빠져나가거나 세션을 종료하면 필터도 사라집니다. 나중에 사용하기 위해 필터 설정을 보존하려면 필터링된 Context Explorer(상황 탐색기) 보기 저장, 2724 페이지 섹션을 참조하십시오.

데이터 유형 필드 옵션

다음 표에는 필터로 이용할 수 있는 데이터 유형과 각 유형에 대한 예제 및 간단한 정의가 나열되어 있습니다.

표 ***278:*** 필터 데이터 유형

유형	값 예	정의
액세스 컨트롤 작업	`Allow(허용)`, `Block(차단)`	트래픽을 허용 또는 차단하기 위해 액세스 컨트롤 정책에서 수행하는 작업입니다.

유형	값 예	정의
애플리케이션 범주	web browser(웹 브라우저), email(이메일)	애플리케이션의 가장 핵심적인 기능에 대한 일반 분류입니다.
애플리케이션 이름	Facebook, HTTP	애플리케이션의 이름입니다.
애플리케이션 위험성	Very High(매우 높음), Medium(중간)	애플리케이션의 예상 보안 위험입니다.
애플리케이션 태그	encrypts communications(통신 암호화), sends mail(메일 전송)	애플리케이션에 대한 추가 정보(애플리케이션에는 0부터 원하는 수만큼의 태그 포함 가능)입니다.
애플리케이션 유형	Client(클라이언트), Web Application(웹 애플리케이션)	애플리케이션 유형(application protocol, client 또는 web application)입니다.
사업 타당성	Very Low(매우 낮음), High(높음)	비즈니스 활동에 대한 애플리케이션의 예상 연관성(레크리에이션과 반대)입니다.
대륙	North America(북미), Asia(아시아)	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 대륙입니다.
Country	Canada(캐나다), Japan(일본)	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 국가입니다.
디바이스	device1.example.com, 192.168.1.3	모니터링되는 네트워크에 있는 디바이스의 이름 또는 IP 주소입니다.
도메인	Asia Division(아시아 부서), Europe Division(유럽 부서)	네트워크 활동을 그래프로 작성할 디바이스의 도메인입니다. 이 데이터 유형은 다중 도메인 구축에서만 표시됩니다.
이벤트 분류	Potential Corporate Policy Violation(잠재적 기업 정책 위반), Attempted Denial of Service(시도된 서비스 거부)	침입 이벤트에 대한 설명으로, 침입 이벤트를 트리거한 규칙, 디코더 또는 전처리기의 분류에 의해 결정됩니다.
이벤트 메시지	dns response(dns 응답), P2P	이벤트에 의해 생성되는 메시지로, 이벤트를 트리거한 규칙, 디코더 또는 전처리기에 의해 결정됩니다.
파일 속성	Malware(악성코드), Clean(클린)	Firepower Management Center가 악성코드 클라우드 조회를 수행한 파일의 성향입니다.
파일 이름	Packages.bz2	네트워크 트래픽에서 탐지되는 파일의 이름입니다.

유형	값 예	정의
파일 SHA256	임의의 32비트 문자열	Firepower Management Center에서 악성 코드 클라우드 조회를 수행한 파일의 SHA-256 해시 값입니다.
File Type(파일 유형)	GZ, SWF, MOV	네트워크 트래픽에서 탐지되는 파일 형식입니다.
파일 유형 카테고리	Archive(아카이브), Multimedia(멀티미디어), Executables(실행파일)	네트워크 트래픽에서 탐지되는 파일 형식의 일반 카테고리입니다.
IP 주소	192.168.1.3, 2001:0db8:85a3::0000/24	IPv4 또는 IPv6 주소, 주소 범위 또는 주소 블록입니다. IP 주소를 검색하면 이벤트가 반환되는데, 여기서 해당 주소는 이벤트의 소스 또는 대상입니다.
영향 레벨	Impact Level 1(영향 레벨 1), Impact Level 2(영향 레벨 2)	모니터링되는 네트워크에서 이벤트의 예상 영향입니다.
인라인 결과	dropped(삭제됨), would have dropped(삭제된 것으로 추정됨)	트래픽이 삭제되었는지, 삭제된 것으로 추정되는지 또는 시스템에 의해 작동되지 않았는지의 여부입니다.
IOC 카테고리	High Impact Attack(강력한 공격), Malware Detected(악성코드 탐지)	트리거된 IOC(Indications of Compromise) 이벤트에 대한 카테고리입니다.
IOC 이벤트 유형	exploit-kit, malware-backdoor	특정 IOC(Indications of Compromise)와 관련된 식별자로, 이를 트리거한 이벤트를 가리킵니다.
악성코드 위협 이름	W32.Trojan.a6b1	악성코드 위협의 이름입니다.
OS Name	Windows, Linux	운영체제의 이름입니다.
OS Version(OS 버전)	XP, 2.6	운영체제의 특정 버전입니다.
Priority(우선순위)	high(높음), low(낮음)	이벤트의 예상 긴급도입니다.
보안 인텔리전스 카테고리	Malware(악성코드), Spam(스팸)	보안 인텔리전스로 확인된 위험 트래픽의 카테고리입니다.
보안 영역	My Security Zone(내 보안 영역), Security Zone X(보안 영역 X)	트래픽이 분석되고 통과되는(인라인 구축의 경우) 인터페이스 집합입니다.
SSL	yes, no	SSL 또는 TLS 암호화 트래픽입니다.

유형	값 예	정의
User	`wsmith`, `mtwain`	모니터링되는 네트워크의 호스트에 로그인하는 사용자의 ID입니다.

추가 필터 창에서 필터 생성

이 절차를 사용하면 Add Filter(필터 추가) 창에서 필터를 처음부터 만들 수 있습니다. (콘텍스트 메뉴를 사용하여 빠른 필터를 만들 수도 있습니다.)

Context Explorer(상황 탐색기) 왼쪽 위의 **Filters(**필터**)** 아래에 있는 더하기(+)를 클릭하여 액세스할 수 있는 Add Filter(필터 추가) 창에는 필터가 2개만 있습니다.

- **Data Type(**데이터 유형**)** 드롭다운 목록에는 Context Explorer(상황 탐색기)를 제한하는 데 사용할 수 있는 많은 유형의 Firepower System 데이터가 포함되어 있습니다. 데이터 유형을 선택한 다음 **Filter(**필터**)** 필드에서 해당 유형에 대한 특정 값(예: **Continent** 유형에 대해 `Asia` 값)을 입력합니다. 사용자에게 도움이 되도록 선택 가능한 데이터 유형에 대한 몇 가지 예제 값이 Filter(필터) 필드에 회색으로 표시됩니다. (필드에 데이터를 입력하면 이러한 값이 지워집니다.)
- 필터 필드 `*` 같은 특수 한 검색 파라미터 입력과 `!` 이벤트의 수를 기본적으로 검색 합니다. 필터 파라미터 앞에 `!` 기호를 추가하면 제외하는 필터를 만들 수 있습니다.

참고 추가하는 필터는 자동으로 적용되지 않습니다. Context Explorer(상황 탐색기)에서 필터를 보려면 **Apply Filters(**필터 적용**)**를 클릭해야 합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 왼쪽 위의 **Filters(**필터**)** 아래에서 더하기(+)를 클릭합니다.

단계 **3** **Data Type(**데이터 유형**)** 드롭다운 목록에서 필터링할 데이터 유형을 선택합니다.

단계 **4** **Filter(**필터**)** 필드에 필터링할 데이터 유형 값을 입력합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 선택적으로, 원하는 필터 집합이 구성될 때까지 이전 단계를 반복하여 필터를 더 추가합니다.

단계 **7** **Apply Filters(**필터 적용**)**을 클릭합니다.

관련 항목

데이터 유형 필드 옵션, 2720 페이지

검색 제약 조건, 2826 페이지

콘텍스트 메뉴에서 빠른 필터 생성

Context Explorer(상황 탐색기) 그래프 및 목록 데이터를 탐색할 때 데이터 포인트를 클릭한 다음 콘텍스트 메뉴를 사용하여 해당 데이터를 기반으로 빠르게 필터를 만들 수 있습니다(포함 또는 제외). 콘텍스트 메뉴를 사용하여 데이터 유형(애플리케이션, 사용자, 침입 이벤트 메시지, 개별 호스트 등)의 정보에 대해 필터링하면 필터 위젯에는 해당 데이터 유형에 대한 관련 세부 사항 페이지(예: 애플리케이션 데이터의 경우 Application Detail(애플리케이션 세부 사항))로 연결되는 위젯 정보가 포함됩니다. URL 데이터에 대해서는 필터링할 수 없습니다.

특정 그래프나 목록 데이터를 좀 더 자세히 조사하려는 경우에도 콘텍스트 메뉴를 사용할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(분석)** > **Context Explorer(상황 탐색기)**을(를) 선택합니다.

단계 **2** Traffic and Intrusion Events over Time을 제외한 탐색기 섹션 또는 URL 데이터가 포함된 섹션에서 필터링할 데이터 포인트를 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 이 데이터에 대한 필터를 추가하려면 **Add Filter(필터 추가)**를 클릭합니다.
- 이 데이터에 대한 제외 필터를 추가하려면 **Add Exclude Filter(제외 필터 추가)**를 클릭합니다. 필터를 적용하면 제외된 값과 관련된 데이터 외의 모든 데이터가 표시됩니다. 제외 필터는 필터 값 앞에 느낌표(!)를 표시합니다.

필터링된 **Context Explorer(상황 탐색기)** 보기 저장

Context Explorer(상황 탐색기)에서 나오거나 세션 종료 후 필터 설정을 Context Explorer(상황 탐색기)에 저장하려면, 원하는 필터가 적용된 Context Explorer(상황 탐색기)의 브라우저 즐겨찾기를 생성합니다. 적용된 필터는 Context Explorer(상황 탐색기) 페이지 URL에 통합되므로 해당 페이지의 즐겨찾기를 로드하면 해당 필터도 로드됩니다.

프로시저

원하는 필터가 적용된 Context Explorer(상황 탐색기)의 브라우저 즐겨찾기를 생성합니다.

필터 데이터 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**를 선택합니다.

단계 **2** 해당 필터 위젯에서 **Information(**정보**)**을 클릭합니다.

필터 삭제

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**를 선택합니다.

단계 **2** 왼쪽 위의 **Filters(**필터**)** 아래에서 아무 필터 위젯의 지우기(✕)을 클릭합니다.

팁 모든 필터를 동시에 삭제하려면 **Clear(**지우기**)** 버튼을 클릭합니다.

112 장

네트워크 맵 사용

다음 주제에서는 네트워크 맵을 사용하는 방법을 설명합니다.

- 네트워크 맵 요구 사항 및 사전 요건, 2727 페이지
- 네트워크 맵, 2727 페이지
- 맞춤형 네트워크 토폴로지, 2734 페이지

네트워크 맵 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

Leaf

사용자 역할

- 관리자
- 검색 관리자

네트워크 맵

Firepower System은 네트워크를 통해 이동하는 트래픽을 모니터링하고, 트래픽 데이터를 디코딩한 다음 데이터를 설정된 운영체제 및 핑거프린트와 비교합니다. 그런 다음 시스템은 이 데이터를 사용하여 네트워크 맵이라고 하는, 네트워크의 자세한 표현을 작성합니다. 다중 도메인 구축의 경우, 시스템은 각 리프 도메인에 대한 개별 네트워크 맵을 생성합니다.

시스템은 네트워크 검색 정책에서 모니터링용으로 식별된 매니지드 디바이스에서 데이터를 수집합니다. 매지니드 디바이스는 네트워크 자산을 모니터링하는 트래픽에서는 직접적으로, 처리된 NetFlow

기록에서는 간접적으로 탐지합니다. 여러 디바이스가 동일한 네트워크 자산을 탐지하면 시스템은 하나의 복합 자산 표현으로 정보를 결합합니다.

수동 탐지에서 데이터를 보강하는 방법은 다음과 같습니다.

- 오픈 소스 스캐너인 Nmap™을 이용해 호스트를 적극적으로 스캔하고, 스캔 결과를 네트워크 맵에 추가합니다.
- 호스트 입력 기능을 이용해 타사 애플리케이션의 호스트 데이터를 수동으로 추가합니다.

네트워크 맵은 탐지한 호스트 및 네트워크 디바이스를 중심으로 네트워크 토폴로지를 표시합니다.

네트워크 맵을 사용하면 다음 작업을 수행할 수 있습니다.

- 전체 네트워크를 빠르게 확인.
- 수행할 분석에 맞게 각기 다른 보기 선택. 네트워크 맵의 각 보기는 확장 가능한 카테고리 및 하위 카테고리가 있는 계층적 트리의 동일한 형식을 가지고 있습니다. 카테고리를 클릭하면 그 아래의 하위 카테고리가 표시되도록 카테고리가 확장됩니다.
- 맞춤형 토폴로지 기능을 통해 서브넷 구성 및 식별. 예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 맞춤형 토폴로지 기능을 사용하여 친숙한 레이블을 서브넷에 할당할 수 있습니다.
- 임의의 모니터링 호스트의 호스트 프로파일로 드릴다운하여 상세 정보 확인
- 더 이상 조사하지 않으려는 자산 삭제

참고 네트워크 맵에서 삭제된 호스트와 관련된 활동이 탐지되면, 해당 호스트는 네트워크 맵에 다시 추가됩니다. 마찬가지로, 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하면 삭제된 애플리케이션이 네트워크 맵에 다시 추가됩니다. 호스트를 취약하게 만드는 변경 사항이 탐지되면 특정 호스트에서 취약성이 다시 활성화됩니다.

팁 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오. 과도하거나 관련 없는 이벤트를 생성하는 것으로 확인된 로드 밸런서와 NAT 디바이스는 모니터링에서 제외할 수 있습니다.

관련 항목

네트워크 검색 정책 설정, 2539 페이지

호스트 네트워크 맵

Hosts(호스트) 탭의 네트워크 맵은 호스트 카운트와 호스트 IP 주소 및 기본 MAC 주소 목록을 표시합니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다. 이 네트워크 맵 보기는 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 호스트의 카운트를 제공합니다.

호스트 네트워크 맵을 사용하면 계층적 트리에 서브넷으로 구성된 네트워크의 호스트를 볼 수 있으며, 특정 호스트에 대한 호스트 프로파일로 드릴다운할 수도 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지의 내용을 참조하십시오.

네트워크에 대한 맞춤형 토폴로지를 생성하면, 부서 이름과 같은 의미 있는 레이블(예: 부서 이름)을 서브넷에 할당할 수 있으며, 이는 호스트 네트워크 맵에 나타납니다. 또한 맞춤형 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다.

호스트 네트워크 맵에서 전체 네트워크, 서브넷 또는 개별 호스트를 삭제할 수 있습니다. 특정 호스트가 네트워크에 더 이상 연결되어 있지 않음을 알고 있다면 분석을 간소화하기 위해 해당 호스트를 삭제할 수 있습니다. 삭제된 호스트와 관련된 활동이 이후에 탐지되면 해당 호스트는 네트워크 맵에 다시 추가됩니다. 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오.

주의 네트워크 맵에서 네트워크 디바이스를 삭제하지 마십시오. 시스템은 이러한 디바이스를 이용해 네트워크 토폴로지를 확인합니다.

호스트 네트워크 맵 페이지에서는 기본 MAC 주소만 검색할 수 있으며, Hosts [MAC] 카운트에는 기본 MAC 주소만 포함됩니다. 기본 및 보조 MAC 주소에 대한 설명은 호스트 프로파일의 기본 호스트 정보, 3004 페이지 섹션을 참조하십시오.

네트워크 디바이스 네트워크 맵

Network Devices(네트워크 디바이스) 탭의 네트워크 맵은 네트워크의 세그먼트를 다른 세그먼트와 연결하는 네트워크 디바이스(브리지, 라우터, NAT 디바이스, 로드 밸런서)를 표시합니다. 맵에는 IP 주소로 식별한 디바이스를 나열하는 섹션과 MAC 주소로 식별한 디바이스를 나열하는 섹션이 있습니다.

또한 맵은 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 네트워크 디바이스의 카운트도 제공합니다.

네트워크에 대해 맞춤형 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 네트워크 디바이스 네트워크 맵에 나타납니다.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스가 CDP를 사용하여 통신하는 경우 IP 주소가 하나 이상일 수 있습니다. STP를 사용하여 통신하는 경우 MAC 주소가 하나뿐일 수 있습니다.

네트워크 맵에서는 네트워크 디바이스를 삭제할 수 없습니다. 시스템은 이러한 디바이스의 위치를 이용해 네트워크 토폴로지를 결정하기 때문입니다.

네트워크 디바이스의 호스트 프로파일에는 Operating Systems 섹션이 아닌 Systems 섹션이 있습니다. 여기에는 네트워크 디바이스 뒤에서 탐지되는 모바일 디바이스에 대한 하드웨어 플랫폼을 반영하는 Hardware 열이 포함됩니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

모바일 디바이스 네트워크 맵

Mobile Devices(모바일 디바이스) 탭의 네트워크 맵은 네트워크에 연결된 모바일 디바이스를 표시합니다. 이 네트워크 맵은 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 모바일 디바이스의 카운트도 제공합니다.

각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다. 서브넷이나 IP 주소를 삭제할 수도 있습니다. 시스템이 디바이스를 다시 검색하면, 디바이스는 네트워크 맵에 다시 추가됩니다.

드릴다운을 통해 모바일 디바이스에 대한 호스트 프로파일을 확인할 수도 있습니다.

모바일 디바이스 식별을 위해 시스템은 다음을 수행합니다.

- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 User-Agent(사용자 에이전트) 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크에 대해 맞춤형 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 모바일 디바이스 네트워크 맵에 나타납니다.

보안 침해 지표 네트워크 맵

Indications of Compromise(보안 침해 지표) 탭의 네트워크 맵은 IOC 카테고리별로 조직화된, 네트워크 상의 침해된 호스트를 표시합니다. 영향받는 호스트는 각 카테고리 아래에 나열됩니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다.

IOC 네트워크 맵에서는 특정 방법으로 침해된 것으로 판단된 각 호스트의 호스트 프로파일을 볼 수 있습니다. 특정 IOC 카테고리 또는 특정 호스트를 삭제(또는 해결된 것으로 표시)할 수 있는데, 그렇게 하면 관련 호스트에서 IOC 태그가 제거됩니다. 예를 들어 문제가 해결되어 재발하지 않을 것으로 판단한 경우 네트워크 맵에서 IOC 카테고리를 삭제할 수 있습니다.

네트워크 맵에서 호스트 또는 IOC 카테고리를 해결된 것으로 표시하더라도 해당 항목이 네트워크에서 제거되지는 않습니다. 해당 IOC를 트리거하는 정보가 새로 탐지되면 네트워크 맵에 해결된 호스트 또는 IOC 카테고리가 다시 나타납니다.

시스템이 보안 침해 지표를 결정하는 방법에 대한 자세한 내용은 보안 침해 지표 데이터, 3056 페이지 및 하위 항목을 참조하십시오.

애플리케이션 프로토콜 네트워크 맵

Application Protocols(애플리케이션 프로토콜) 탭의 네트워크 맵은 애플리케이션 이름, 벤더, 버전별로, 그리고 마지막에는 각 애플리케이션을 실행하는 호스트별로 계층형 트리에 구성되어 있는, 네트워크 상의 애플리케이션을 표시합니다.

시스템 소프트웨어와 VDB가 업데이트되는 경우, 그리고 애드온 탐지기를 가져오는 경우 시스템에서 탐지하는 애플리케이션이 변경될 수 있습니다. 각 시스템 또는 VDB 업데이트에 대한 릴리스 정보나 자문 텍스트에는 새 탐지기 및 업데이트된 탐지기에 대한 정보가 포함되어 있습니다. 포괄적인 최신 탐지기 목록은 Cisco 지원 사이트(http://www.cisco.com/cisco/web/support/index.html)를 참조하십시오.

이 네트워크 맵에서는 특정 애플리케이션을 실행하는 각 호스트의 호스트 프로파일을 확인할 수 있습니다.

또한 모든 애플리케이션 카테고리, 모든 호스트에서 실행 중인 모든 애플리케이션, 특정 호스트에서 실행 중인 모든 애플리케이션을 삭제할 수 있습니다. 예를 들어 애플리케이션이 호스트에서 비활성화된 것을 알고 있으며 시스템이 영향 레벨 자격에 애플리케이션을 사용하지 않도록 하려면 네트워크 맵에서 해당 애플리케이션을 삭제할 수 있습니다.

네트워크 맵에서 애플리케이션을 삭제해도 네트워크에서 제거되지는 않습니다. 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하거나 시스템의 검색 기능을 다시 시작하는 경우 삭제된 애플리케이션이 네트워크 맵에 다시 나타납니다.

삭제한 내용에 따라 동작이 달라집니다.

- 애플리케이션 카테고리 - 삭제하면 네트워크 맵에서 애플리케이션 카테고리가 제거됩니다. 카테고리에 속하는 모든 애플리케이션이 해당 호스트 프로파일에서 제거됩니다.

  예를 들어 **http**를 삭제하면 **http**로 식별되는 모든 애플리케이션이 모든 호스트 프로파일에서 제거되며, 네트워크 맵의 애플리케이션 보기에 **http**가 더 이상 나타나지 않습니다.

- 특정 애플리케이션, 벤더 또는 버전 - 삭제하면 영향받는 애플리케이션이 네트워크 맵 및 해당 호스트 프로파일에서 제거됩니다.

  예를 들어 **http** 카테고리를 확장하고 **Apache**를 삭제하면, Apache 아래에 나열된 버전과 상관없이 Apache로서 나열된 모든 애플리케이션이 해당 호스트 프로파일에서 제거됩니다. 마찬가지로, **Apache**를 삭제하는 대신 특정 버전(예: **1.3.17**)을 삭제하면 선택한 버전만이 영향받는 호스트 프로파일에서 삭제됩니다.

- 특정 IP 주소 - 삭제하면 애플리케이션 목록에서 해당 IP 주소가 제거되며, 선택한 IP 주소의 호스트 프로파일에서 애플리케이션 자체도 제거됩니다.

  예를 들어 **http**, **Apache**, **1.3.17(Win32)**을 확장한 다음 **172.16.1.50:80/tcp**를 삭제하면 Apache 1.3.17(Win32) 애플리케이션이 IP 주소 172.16.1.50의 호스트 프로파일에서 삭제됩니다.

취약성 네트워크 맵

Vulnerabilities(취약성) 탭의 네트워크 맵은 시스템이 네트워크에서 탐지한 취약성을 레거시 취약성 ID(SVID), CVE ID 또는 Snort ID별로 조직화해 표시합니다.

이 네트워크 맵에서는 특정 취약성의 상세정보와, 특정 취약성에 대한 호스트의 호스트 프로파일을 확인할 수 있습니다. 이 정보는 해당 취약성이 영향받는 특정 호스트에 미치는 위협을 평가하는 데 도움이 됩니다.

특정 취약성이 (패치 적용 등의 이유로) 네트워크의 호스트에 영향을 미치지 않는 것 같다면 해당 취약성을 비활성화할 수 있습니다. 비활성화된 취약성은 여전히 네트워크 맵에 나타나지만 영향받는 이전 호스트의 IP 주소는 회색의 기울임꼴로 나타납니다. 그러한 호스트의 호스트 프로파일은 비활성화된 취약성을 무효 상태로 표시합니다(개별 호스트에 대해 수동으로 취약성을 유효 상태로 표시할 수는 있음).

호스트에서 애플리케이션이나 운영체제의 ID 충돌이 있는 경우 시스템은 잠재적인 두 ID에 대한 취약성을 나열합니다. ID 충돌이 해결되면 취약성과 현재 ID의 연결 상태가 유지됩니다.

기본적으로, 패킷에 애플리케이션의 벤더 및 버전이 포함된 경우에만 네트워크 맵에 탐지된 애플리케이션의 취약성이 표시됩니다. 그러나 Firepower Management Center 설정에서 애플리케이션에 대한 취약성 매핑 설정을 활성화함으로써, 벤더 및 버전 데이터가 없는 애플리케이션에 대한 취약성을 나열하도록 시스템을 구성할 수 있습니다.

취약성 ID(또는 취약성 ID의 범위) 옆에 있는 숫자는 두 개의 카운트를 나타냅니다.

영향받은 호스트

첫 번째 숫자는 취약성의 영향을 받는 고유하지 않은 호스트의 카운트입니다. 하나의 호스트가 둘 이상의 취약성에 의해 영향을 받으면 여러 번으로 계산됩니다. 따라서 카운트가 네트워크에 있는 호스트의 수보다 클 수 있습니다. 취약성을 비활성화하면 해당 취약성의 영향을 받을 가능성이 있는 호스트의 수만큼 이 카운트가 줄어듭니다. 취약성 또는 취약성 범위의 영향을 받을 가능성이 있는 호스트에 대해 취약성을 비활성화하지 않은 경우 이 카운트가 표시되지 않습니다.

영향받았을 가능성이 있는 호스트

두 번째 숫자는 시스템이 취약성의 영향을 받을 가능성이 있는 것으로 판단한, 고유하지 않은 총 호스트의 카운트입니다.

취약성을 비활성화하면 지정한 호스트에 대해서만 비활성이 적용됩니다. 취약한 것으로 판단한 모든 호스트에 대해 또는 취약한 개별 지정 호스트에 대해 취약성을 비활성화할 수 있습니다. 취약성이 비활성화되면, 해당하는 호스트의 IP 주소가 네트워크 맵에서 회색 기울임꼴로 표시됩니다. 또한 그러한 호스트의 호스트 프로파일에는 비활성화된 취약성이 무효 상태로 표시됩니다.

그 후 비활성화되지 않은 호스트(예: 네트워크 맵의 새 호스트)에서 취약성이 탐지되면, 시스템은 해당 호스트에 대해 취약성을 활성화합니다. 새로 검색된 취약성은 명시적으로 비활성화해야 합니다. 또한 호스트에 대해 운영체제 또는 애플리케이션 변경이 탐지되면 시스템은 비활성화된 관련 취약성을 다시 활성화할 수 있습니다.

호스트 속성 네트워크 맵

Host Attributes(호스트 속성) 탭의 네트워크 맵은 네트워크 상의 호스트를 사용자 정의 또는 규정준수 화이트 목록 호스트 속성 중 하나를 기준으로 조직화해 표시합니다. 이 화면에서는 사전 정의된 호스트 속성을 이용해 호스트를 조직화할 수는 없습니다.

호스트를 구성하는 데 사용할 호스트 속성을 선택하면, Firepower Management Center은(는) 네트워크 맵에서 해당 특성에 대해 사용할 수 있는 값을 나열하고 할당된 값을 기반으로 호스트를 그룹화합니다. 예를 들어 화이트 목록 호스트 속성을 기준으로 호스트를 조직화하는 경우, 시스템은 호스트를 Compliant(규정준수), Non-Compliant(규정 미준수), Not Evaluated(미평가) 카테고리로 구분해 표시합니다.

또한 특정 호스트 속성 값이 할당된 호스트의 호스트 프로파일을 볼 수도 있습니다.

관련 항목

호스트 프로파일의 호스트 속성, 3019 페이지

네트워크 맵 보기

네트워크 맵을 보려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(분석)** > **Hosts(호스트)** > **Network Map(네트워크 맵)**를 선택합니다.

단계 **2** 보려는 네트워크 맵을 클릭합니다.

단계 **3** 해당하는 작업을 계속 진행합니다.

- 도메인 선택 — 다중 도메인 환경의 경우, **Domain(도메인)** 드롭다운 목록에서 리프 도메인을 선택합니다.
- 호스트 필터링 — IP 주소 또는 MAC 주소로 필터링하려는 경우, 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기( )을 클릭합니다.
- 드릴다운 — 카테고리 또는 호스트 프로파일을 조사하려는 경우, 맵의 카테고리 또는 서브넷을 드릴다운합니다. 맞춤형 토폴로지가 정의된 경우 보려는 **Hosts(호스트)**에서 **(topology)(토폴로지)**를 클릭한 다음, 기본 보기로 다시 토글하려면 **(hosts)(호스트)**를 클릭합니다.
- 삭제 — 해당 요소 옆에 있는 삭제( )을 클릭합니다.
  - **Hosts(호스트)**, **Network Devices(네트워크 디바이스)**, **Mobile Devices(모바일 디바이스)** 또는 **Application Protocols(애플리케이션 프로토콜)** 의 맵에서 요소를 제거합니다.
  - **Indications of Compromise(보안 침해 지표)**에서 확인된 IOC 카테고리, 보안 침해된 호스트 또는 보안 침해된 호스트 그룹을 표시합니다.
  - **Vulnerabilities(취약점)**에서 모든 호스트 또는 단일 호스트의 취약점을 비활성화합니다.
- 취약점 등급 지정 — **Vulnerabilities(취약점)**의 **Type(유형)** 드롭다운 목록에서 보려는 취약점 등급을 선택합니다.

- 구성 속성 지정 — **Host Attributes(**호스트 속성**)**의 **Attribute(**속성**)** 드롭다운 목록에서 속성을 선택합니다.

관련 항목

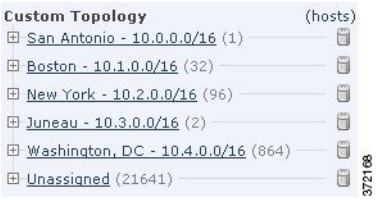
맞춤형 네트워크 토폴로지, 2734 페이지
호스트 프로파일, 3002 페이지

맞춤형 네트워크 토폴로지

맞춤형 토폴로지 기능을 사용하면 호스트 및 네트워크 디바이스 네트워크 맵에서 서브넷을 구성 및 식별하는 데 도움이 될 수 있습니다.

예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 맞춤형 토폴로지 기능을 사용하여 서브넷에 레이블을 지정할 수 있습니다.

또한 사용자 정의 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다.



다음 방법 중 하나 또는 모두를 사용하여 맞춤형 토폴로지의 네트워크를 지정할 수 있습니다.

- 네트워크 검색 정책에서 네트워크를 가져와 시스템이 모니터링하도록 설정한 네트워크에 추가할 수 있습니다.
- 네트워크를 수동으로 네트워크 토폴로지에 추가할 수 있습니다.

Custom Topology(맞춤형 토폴로지) 페이지는 맞춤형 토폴로지와 토폴로지의 상태를 열거합니다. 정책 이름 옆에 있는 전구 아이콘이 밝게 표시되면 토폴로지가 활성 상태이며 네트워크 맵에 영향을 미치게 됩니다. 아이콘 흐리게 표시된다면, 토폴로지는 비활성 상태입니다.

관련 항목

호스트 네트워크 맵, 2728 페이지
네트워크 디바이스 네트워크 맵, 2729 페이지

맞춤형 토폴로지 생성

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** 툴바에서 **Custom Topology(**맞춤형 토폴로지**)**를 클릭합니다.

단계 **3** **Create Topology(**토폴로지 생성**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** 네트워크를 토폴로지에 추가합니다. 다음의 전략 중 하나 또는 모두를 사용할 수 있습니다.

- 네트워크 검색 정책에서 네트워크 가져오기, 2735 페이지에 설명된 대로 네트워크 검색 정책에서 네트워크를 가져옵니다.
- 맞춤형 토폴로지에 수동으로 네트워크 추가, 2736 페이지에 설명된 대로 네트워크를 수동으로 추가합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 2736 페이지에 설명된 대로 토폴로지를 활성화합니다.

네트워크 검색 정책에서 네트워크 가져오기

프로시저

단계 **1** 네트워크를 가져올 맞춤형 토폴로지에 액세스합니다.

- 맞춤형 토폴로지를 생성합니다(맞춤형 토폴로지 생성, 2734 페이지 참조).
- 기존 맞춤형 토폴로지를 편집합니다(맞춤형 토폴로지 편집, 2737 페이지 참조).

단계 **2** **Import Policy Networks(**정책 네트워크 가져오기**)**를 클릭합니다.

단계 **3** **Load(**로드**)**를 클릭합니다. 시스템은 네트워크 검색 정책에 대한 토폴로지 정보를 표시합니다.

단계 **4** 토폴로지를 정리하려면

- 네트워크 옆에 있는 수정( )을 클릭하고, 이름을 입력하고, **Rename(**이름 변경**)**을 클릭해 토폴로지의 네트워크 이름을 변경합니다.
- 삭제( )을 클릭하고 **OK(**확인**)**를 클릭해 토폴로지에서 네트워크를 제거합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 2736 페이지에 설명된 대로 토폴로지를 활성화합니다.

맞춤형 토폴로지에 수동으로 네트워크 추가

프로시저

단계 **1** 네트워크를 추가할 맞춤형 토폴로지에 액세스합니다.

- 맞춤형 토폴로지를 생성합니다(맞춤형 토폴로지 생성, 2734 페이지 참조).
- 기존 맞춤형 토폴로지를 편집합니다(맞춤형 토폴로지 편집, 2737 페이지 참조).

단계 **2** **Add Network(**네트워크 추가**)**를 클릭합니다.

단계 **3** 호스트 및 네트워크 디바이스 네트워크 맵에 네트워크에 대한 맞춤형 라벨을 추가하려면, **Name(**이름**)**을 입력합니다.

단계 **4** 추가할 네트워크를 나타내는 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**(IPv4)를 입력합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 2736 페이지에 설명된 대로 토폴로지를 활성화합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

맞춤형 토폴로지 활성화 및 비활성화

참고 언제든 하나의 맞춤형 토폴로지만 활성 상태를 유지할 수 있습니다. 여러 토폴로지를 생성한 경우 하나를 활성화하면 현재 활성 상태인 토폴로지는 자동으로 비활성화됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Topology(**맞춤형 토폴로지**)**를 선택합니다.

단계 **3** 토폴로지 옆에 있는 슬라이더를 클릭하여 토폴로지를 활성화 또는 비활성화합니다.

맞춤형 토폴로지 편집

활성 토폴로지에 적용한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Topology(**맞춤형 토폴로지**)**를 클릭합니다.

단계 **3** 편집할 토폴로지 옆에 있는 수정( )을 클릭합니다.

단계 **4** 맞춤형 토폴로지 생성, 2734 페이지에 설명된 대로 토폴로지를 편집합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

113 장

인시던트

다음 주제에서는 인시던트 처리를 설정하는 방법을 설명합니다.

- 인시던트 처리 정보, 2739 페이지
- 인시던트 라이선스 요구 사항, 2743 페이지
- 인시더트 요구 사항 및 사전 요건, 2743 페이지
- 맞춤형 인시던트 유형 생성, 2743 페이지
- 인시던트 생성, 2744 페이지
- 인시던트 편집, 2744 페이지
- 인시던트 보고서 생성, 2745 페이지

인시던트 처리 정보

인시던트 처리란 보안 정책 위반이 의심될 때 조직에서 취하는 대응을 가리킵니다. Firepower System에는 인시던트의 조사와 관련된 정보의 수집 및 처리를 지원하는 기능이 포함되어 있습니다. 이러한 기능을 통해 인시던트와 관련이 있을 수 있는 침입 이벤트와 패킷을 수집할 수 있습니다. 공격의 효과를 완화하기 위해 Firepower System의 외부에서 수행하는 활동에 대한 메모의 저장소로 인시던트를 사용할 수도 있습니다. 예를 들어 감염된 호스트를 네트워크에서 격리하도록 보안 정책에서 요구하는 경우 인시던트에 그 내용을 메모할 수 있습니다.

또한 Firepower System은 인시던트 라이프사이클을 지원하며, 따라서 공격에 대한 대응을 진행할 때 인시던트의 상태를 변경할 수 있습니다. 인시던트를 종료할 때 학습 내용의 결과로서 보안 정책에 대해 변경한 내용을 메모할 수 있습니다.

인시던트의 정의

일반적으로 인시던트는 보안 정책 위반과 관련이 있을 것으로 의심되는 하나 이상의 침입 이벤트로 정의됩니다. 또한 Firepower System에서 이 단어는 인시던트에 대한 응답을 추적하는 데 사용할 수 있는 기능을 말합니다.

일부 침입 이벤트는 네트워크 자산의 가용성, 기밀성 및 무결성에서 다른 이벤트보다 더 중요합니다. 예를 들어 포트 스캔 탐지 기능은 네트워크에서의 포트 스캐닝 활동을 지속적으로 알려줄 수 있습니다. 그러나 보안 정책에서는 포트 스캐닝을 명시적으로 금지하지 않거나 우선순위가 높은 위협으로

간주하지 않을 수 있으며, 따라서 직접적인 조치를 취하기보다는 향후 포렌식 연구를 위해 포트 스캐닝의 로그를 보존하고자 할 수 있습니다.

반면 네트워크 내 호스트가 감염되었으며 DDoS(Distributed Denial-of-Service)에 참여하고 있음을 나타내는 이벤트가 생성되면, 이 활동은 명백한 보안 정책 위반이 될 수 있으므로 해당 이벤트의 조사를 추적하는 데 도움이 되도록 Firepower System에서 인시던트를 생성해야 합니다.

일반 인시던트 처리 프로세스

준비

두 가지 방법으로 인시던트를 준비할 수 있습니다.

- 분명하고 포괄적인 보안 정책과 더불어 이를 적용할 하드웨어 및 소프트웨어 리소스를 지정합니다.
- 확실하게 정의된 인시던트 대응 계획을 세우고, 계획을 구현할 수 있도록 적절하게 팀을 훈련합니다.

인시던트 처리의 중요한 부분은 네트워크의 어떤 부분이 가장 위험한가를 파악하는 것입니다. 그러한 네트워크 세그먼트에 Firepower System 구성 요소를 구축하면 인시던트가 언제 어떻게 발생하는지를 더 잘 인지할 수 있습니다. 또한 각각의 매니지드 디바이스에 대해 침입 정책을 세부적으로 조정하면, 최고의 품질로 이벤트가 생성되도록 보장할 수 있습니다.

탐지 및 알림

인시던트를 탐지하지 못하면 인시던트에 대응할 수 없습니다. 인시던트 처리 프로세스에는 탐지할 수 있는 보안 관련 이벤트의 종류와 탐지에 사용되는 메커니즘(소프트웨어와 하드웨어 모두)을 명시해야 합니다. 또한 보안 정책의 위반을 어디서 탐지할 수 있는지도 명시해야 합니다. 네트워크에 능동적으로 또는 수동적으로 모니터링되지 않는 세그먼트가 포함되어 있으면 그러한 내용도 명시해야 합니다.

네트워크에 구축한 매니지드 디바이스는 각각 설치된 세그먼트에서 트래픽을 분석하여 침입을 탐지하고 이를 설명하는 이벤트를 생성해야 합니다. 매니지드 디바이스 각각에 구축하는 액세스 컨트롤 정책은 탐지할 활동의 종류 및 우선순위 지정 방법을 결정합니다. 인시던트 팀이 수백 개의 인시던트를 엄밀히 조사하지 않아도 되도록 특정 침입 이벤트 유형에 대한 알림 옵션을 설정할 수 있습니다. 특정 레벨의 우선순위, 특정 레벨의 심각도 이벤트가 탐지될 때 자동으로 알림을 전송하도록 지정할 수 있습니다.

조사 및 자격

인시던트 처리 프로세스에는 보안 인시던트가 탐지된 이후 조사를 수행하는 방법을 지정해야 합니다. 일부 조직에서는 팀의 신입이 모든 인시던트를 분류하고 심각도나 우선순위가 낮은 사건을 처리하며, 선임자는 심각도나 우선순위가 높은 인시던트를 처리합니다. 각 팀 멤버가 인시던트의 중요도를 결정하는 기준을 이해할 수 있도록 에스컬레이션 프로세스를 신중하게 정리해두어야 합니다.

에스컬레이션 프로세스의 일부는 탐지된 이벤트가 네트워크 자산의 보안에 어떤 영향을 미칠 수 있는지를 파악하는 것과 연결됩니다. 예를 들어 Microsoft SQL 서버를 실행하는 호스트에 대한 공격은

다른 데이터베이스 서버를 사용하는 조직에서는 우선순위가 높지 않습니다. 마찬가지로 이 공격은 네트워크에서 SQL Server를 사용하는 경우에도 덜 중요하지만, 모든 서버가 패치되었고 공격에 취약하지 않은지를 확인해야 합니다. 그러나 누군가가 최근에 (아마도 테스트 목적으로) 취약한 소프트웨어 버전을 설치했다면, 피상적인 조사에서 제시하는 것보다 문제가 더 클 수 있습니다.

Firepower System은 조사 및 자격 프로세스의 지원에서 특별히 뛰어납니다. 사용자는 고유한 이벤트 분류를 생성한 다음 네트워크 취약성에 가장 적합하게 적용할 수 있습니다. 네트워크의 트래픽이 이벤트를 트리거하면 특수 지표를 통해 해당 이벤트에 대한 우선순위와 자격이 자동으로 지정되어, 어떤 공격이 취약한 것으로 알려진 호스트로 향하는지를 알 수 있습니다.

또한 Firepower System의 인시던트 추적 기능에는 어떤 인시던트가 에스컬레이션되었는지를 표시하기 위해 변경할 수 있는 상태 지표도 포함됩니다.

의사소통

모든 인시던트 처리 프로세스에는 인시던트 처리 팀과 내부 및 외부 담당자 간 인시던트의 커뮤니케이션 방법을 지정해야 합니다. 예를 들면, 관리 개입이 필요한 인시던트 종류 및 해당 레벨을 고려해야 합니다. 외부 조직과의 커뮤니케이션 방법 및 시기에 대해서도 프로세스에 명시해야 합니다. 다음과 같은 변화에 주목하십시오.

- 일부 인시던트의 경우 법 집행 기관에 알려야 합니까?
- 호스트가 원격 사이트에 대한 DDoS(distributed denial of service)에 참여하고 있는 경우 해당 사이트에 알려야 합니까?
- CERT/CC(CERT Coordination Center) 또는 FIRST 등의 조직과 정보를 공유하고자 합니까?

Firepower System에는 타인과 손쉽게 공유할 수 있도록 침입 데이터를 HTML, PDF, CSV(comma-separated values) 등의 표준 형식으로 수집할 수 있는 기능이 있습니다.

예를 들어 CERT/CC는 웹사이트의 보안 인시던트에 대한 표준 정보를 수집합니다. CERT/CC는 Firepower System에서 손쉽게 추출할 수 있는 다음과 같은 유형의 정보를 찾습니다.

- 영향을 받는 시스템에 대한 다음과 같은 정보:
  - 호스트 이름 및 IP
  - 표준 시간대
  - 호스트의 목적 또는 기능
- 공격 소스에 대한 다음과 같은 정보:
  - 호스트 이름 및 IP
  - 표준 시간대
  - 공격자와 접촉이 있었는지 여부
  - 인시던트 처리 예상 비용
- 인시던트에 대한 다음과 같은 설명:

- 날짜
- 침입 방법
- 관련 된 침입자 도구
- 소프트웨어 버전 및 패치 레벨
- 침입자 툴 출력
- 악용된 취약성 상세정보
- 공격의 소스
- 기타 관련 정보

인시던트의 코멘트 섹션을 사용하여 문제에 대해 누구와 언제 커뮤니케이션했는지를 기록할 수 있습니다.

봉쇄 및 복구

인시던트 처리 프로세스에는 호스트 또는 다른 네트워크 구성 요소가 손상될 때 어떤 단계를 따라야 하는지를 분명히 명시해야 합니다. 봉쇄 및 복구 옵션의 범위는 취약한 호스트에 패치를 적용하는 것부터 대상을 종료하고 네트워크에서 제거하는 것까지 다양합니다. 또한 공격의 본질과 심각도에 따라, 형사 고발로 이어질 경우에 대비하여 증거 보존의 중요도를 고려해야 합니다.

인시던트의 봉쇄 및 복구 단계 중에 취한 작업의 레코드를 유지 관리하려면 Firepower System의 인시던트 기능을 사용할 수 있습니다.

습득한 교훈

성공적인 공격이든 아니든, 각 보안 인시던트는 보안 정책을 검토할 수 있는 기회입니다. 방화벽 규칙을 업데이트해야 합니까? 패치 관리에 대해 좀 더 구조적인 접근 방식이 필요합니까? 무단 무선 액세스 포인트가 새로운 보안 문제입니까? 각각의 습득한 교훈을 보안 정책에 반영하여 다음 인시던트에 더 잘 대비해야 합니다.

Firepower System의 인시던트 유형

생성하는 각 인시던트에 인시던트 유형을 할당할 수 있습니다. Firepower System에서는 기본적으로 다음 유형을 지원합니다.

- 침입
- Denial of Service(서비스 거부)
- 무단 관리자 액세스
- 웹사이트 파손
- 시스템 무결성 손상
- 사기

- 도난
- 손상
- 알 수 없음

자체 인시던트 유형을 생성할 수도 있습니다.

인시던트 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

인시더트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

맞춤형 인시던트 유형 생성

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** **Create Incident(**인시던트 생성**)**를 클릭합니다.

단계 **3** **Type(**유형**)** 영역에서 **Types(**유형**)**를 클릭합니다.

기본 인시던트 유형이 페이지 하단에 나열됩니다.

단계 **4** **Incident Type Name(**인시던트 유형 이름**)** 필드에 새 인시던트 유형의 이름을 입력합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Done(**완료**)**을 클릭합니다.

다음에 인시던트를 생성하거나 수정할 때 새 인시던트 유형을 사용할 수 있습니다.

인시던트 생성

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 인시던트만 보고 수정할 수 있습니다. 상위 도메인의 경우에는 모든 하위 도메인의 인시던트에 이벤트를 추가할 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** **Create Incident(**인시던트 생성**)**를 클릭합니다.

단계 **3** **Type(**유형**)** 드롭다운 메뉴에서 인시던트를 가장 잘 설명하는 옵션을 선택합니다.

단계 **4** 인시던트에 사용한 시간을 #d #h #m #s 형식으로 **Time Spent(**사용한 시간**)** 필드에 입력합니다. #은 일수, 시간, 분 또는 초를 나타냅니다.

단계 **5** 인시던트에 대한 짧은 설명을 **Summary(**요약**)** 텍스트 상자에 입력합니다(최대 255자의 영숫자 문자, 공백 및 기호).

단계 **6** 인시던트에 대한 좀 더 완전한 설명을 **Add Comment(**코멘트 추가**)** 텍스트 상자에 입력합니다(최대 8,191자의 영숫자 문자, 공백 및 기호).

단계 **7** 인시턴트에 이벤트 추가:

- 선택한 이벤트를 추가하려면 클립보디에서 이벤트를 선택하고 **Add to Incident(**인시던트에 추가**)**를 클릭합니다.
- 클립보드의 이벤트를 모두 추가하려면 **Add All to Incident(**모두 인시던트에 추가**)**를 클릭합니다.

참고 둘 이상의 클립보드 페이지에서 개별 이벤트를 추가하려는 경우, 먼저 한 페이지의 이벤트를 추가한 후 다른 페이지의 이벤트를 별도로 추가해야 합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

인시던트 편집

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 인시던트만 보고 수정할 수 있습니다. 상위 도메인의 경우에는 모든 하위 도메인의 인시던트에 이벤트를 추가할 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** 편집할 인시던트 옆에 있는 수정( )을 클릭합니다.

단계 **3** 인시던트의 다음과 같은 부분을 수정할 수 있습니다.

- 상태 변경
- 유형 변경
- 클립보드에서 이벤트 추가
- 이벤트 삭제

단계 **4** 인시던트에 사용한 추가 시간을 **Time Spent(**사용한 시간**)** 필드에 입력합니다.

단계 **5** 인시던트에 대한 변경 사항의 설명을 **Add Comment(**코멘트 추가**)** 텍스트 상자에 입력합니다(최대 8,191자의 영숫자 문자, 공백 및 기호).

단계 **6** 선택적으로, 인시던트에서 이벤트를 추가 또는 삭제할 수 있습니다.

- 클립보드의 이벤트를 추가하려면 클립보드에서 원하는 이벤트를 선택하고 **Add to Incident(**인시던트에 추가**)**를 클릭합니다.
- 클립보드의 이벤트를 모두 추가하려면 **Add All to Incident(**모두 인시던트에 추가**)**를 클릭합니다.
- 인시던트에서 특정 이벤트를 삭제하려면 이벤트를 선택하고 **Delete(**삭제**)**를 클릭합니다.
- 인시던트에서 모든 이벤트를 삭제하려면 **Delete All(**모두 삭제**)**을 클릭합니다.
- 이벤트를 추가 또는 삭제하지 않고 인시던트를 업데이트하려면 **Save(**저장**)**를 클릭합니다.

인시던트 보고서 생성

Firepower System을 사용하여 인시던트 보고서를 생성할 수 있습니다. 이러한 보고서는 인시던트에 추가한 이벤트의 정보와 함께 인시던트 요약, 인시던트 상태 및 코멘트를 포함할 수 있습니다. 또한 보고서에 이벤트 요약 정보를 포함할지 여부를 지정할 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** 보고서에 포함할 인시던트 옆에 있는 수정( )을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 인시던트의 모든 이벤트를 보고서에 포함하려면 **Generate Report All(**모든 보고서 생성**)**을 클릭합니다.

- 인시던트의 특정 이벤트를 보고서에 포함하려면 원하는 이벤트 옆의 확인란을 선택하고 **Generate Report(**보고서 생성**)**를 클릭합니다.

단계 **4** 보고서의 이름을 입력합니다.

단계 **5** **Incident Report Sections(**인시던드 보고서 섹션**)**에서, 보고서에 포함할 인시던트의 부분에 대한 확인란(**status**, **summary**, 및 **comments**)을 선택합니다.

단계 **6** 보고서에 이벤트 정보를 포함하려면 사용하려는 워크플로를 선택하고, **Report Sections(**보고서 섹션**)**에서 이벤트 요약 정보의 포함 여부를 지정합니다.

단계 **7** 보고서에 포함할 워크플로 페이지 옆에 있는 확인란을 선택합니다.

단계 **8** 보고서에 대해 사용할 출력 형식(**PDF**, **HTML** 및 **CSV**) 옆에 있는 확인란을 선택합니다.

참고 CSV 기반 인시던트 보고서에는 이벤트 정보만 포함됩니다. 인시던트의 상태, 요약 또는 코멘트는 포함되지 않습니다.

단계 **9** **Generate Report(**보고서 생성**)**를 클릭하고 보고서 프로파일 업데이트를 확인합니다.

114 장

조회 사용

다음 주제에서는 Firepower System이 알거나 알지 못하는 개체 관련 정보를 조회하는 방법을 설명합니다.

- 조회 소개, 2747 페이지
- Whois 조회 수행, 2747 페이지
- IP 주소에 대한 지리위치 정보 찾기, 2748 페이지

조회 소개

Firepower Management Center이(가) 인터넷에 연결된 경우, 수동 조회 기능으로 다음 정보를 찾을 수 있습니다.

- 모든 IP 주소에 대한 RIR(Regional Information Registries) 정보(whois)
- 모든 IP 주소에 대한 지리위치 정보: 국가 이름, 국가 코드, 대륙 이름 (최신 지리위치 정보 사용을 위해, Cisco는 Firepower Management Center의 GeoDB(Geolocation Database)를 정기적으로 업데이트할 것을 강력하게 권장합니다.)

관련 항목

GeoDB(지리위치 데이터베이스) 업데이트, 183 페이지

Whois 조회 수행

시작하기 전에

- Firepower Management Center이(가) 인터넷에 액세스할 수 있는지 확인합니다(보안, 인터넷 액세스 및 통신 포트, 3107 페이지 참조).

프로시저

단계 1 **Analysis(분석)** > **Advanced(고급)** > **Whois**을(를) 선택합니다.

단계 **2** IP 주소를 입력하고 **Search(**검색**)**를 클릭합니다.

관련 항목

상황 메뉴, 14 페이지

IP 주소에 대한 지리위치 정보 찾기

지리위치 조회 기능을 이용해 국가 이름, ISO 3166-1 3자리 국가 코드 및 특정 IP 주소와 관련된 대륙 이름을 찾을 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Geolocation(**지리위치**)**을(를) 선택합니다.

단계 **2** 하나 이사의 IP 주소에 대한 지리위치 정보를 보려면 주소 또는 주소 모음을 입력하고 **Search(**검색**)**를 클릭합니다. IPv4 주소나 IPv6 주소, 또는 둘 다를 지정할 수 있습니다. 쉼표, 세미콜론, 리턴, 또는 모든 공백 문자를 사용하여 여러 주소를 구분하십시오.

팁 텍스트 상자를 비우려면 **Clear(**지우기**)**를 클릭합니다.

단계 **3** 선택적으로, 열 제목을 클릭하여 데이터를 정렬합니다. IP 주소를 제외한 모든 필드별로 정렬할 수 있습니다.

관련 항목

GeoDB(지리위치 데이터베이스) 업데이트, 183 페이지

115 장

외부 툴을 사용하여 이벤트 분석

- Cisco SecureX와의 통합, 2749 페이지
- 다음을 이용한 이벤트 분석 Cisco SecureX Threat Response, 2749 페이지
- 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지
- 다음에 대한 교차 실행 링크 설정 Stealthwatch, 2754 페이지
- Security Events(보안 이벤트)에 대한 시스템 로그 메시지 전송 정보, 2755 페이지
- eStreamer 서버 스트리밍, 2769 페이지
- Splunk의 이벤트 분석, 2773 페이지
- IBM QRadar의 이벤트 분석, 2773 페이지
- 외부 툴을 사용한 이벤트 데이터 분석 기록, 2774 페이지

Cisco SecureX와의 통합

단일한 보안 창인 SecureX 클라우드 포털을 통해 모든 Cisco 보안 제품의 데이터를 보고 작업할 수 있습니다. SecureX를 통해 제공되는 툴을 사용하여 위협 추적 및 조사 등을 강화하십시오.

SecureX에 대한 자세한 내용은 http://www.cisco.com/c/en/us/products/security/securex.html의 내용을 참조하십시오.

Firepower를 SecureX와 통합하려면 https://cisco.com/go/firepower-securex-documentation에 있는 *Firepower* 및 *SecureX* 통합 가이드를 참조하십시오.

다음을 이용한 이벤트 분석 Cisco SecureX Threat Response

Cisco SecureX Threat Response는 이전에는 CTR (Cisco Threat Response)로 알려졌습니다.

Firepower를 포함해 여러 제품에서 집계한 데이터를 사용하여 인시던트를 분석할 수 있는, Cisco Cloud의 통합 플랫폼인 Cisco SecureX Threat Response을(를) 사용하여 위협을 빠르게 탐지하고, 조사하고 응답할 수 있습니다.

- Cisco SecureX Threat Response에 대한 일반 정보는 다음을 참조하십시오

  https://www.cisco.com/c/en/us/products/security/threat-response.html.

- Cisco SecureX Threat Response과 Firepower 통합에 대한 자세한 지침은 다음을 참조하십시오.
- https://cisco.com/go/firepower-ctr-integration-docs의 *Firepower* 및 *Cisco SecureX Threat Response* 통합 가이드.

Cisco SecureX Threat Response에서 이벤트 데이터 보기

시작하기 전에

- https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html의 *Firepower* 및 *Cisco SecureX Threat Response* 통합 가이드의 설명과 같이 통합을 설정합니다.
- Cisco SecureX Threat Response의 온라인 도움말을 검토해 위협을 찾고, 조사하고, 조치하는 방법을 확인하십시오.
- Cisco SecureX Threat Response에 액세스하려면 자격 증명이 필요합니다.

프로시저

단계 **1** Firepower Management Center에서 다음 중 하나를 수행합니다.

- 특정 이벤트에서 Cisco SecureX Threat Response(으)로 피벗하는 방법:

  a. **Analysis(분석) > Intrusions(침입)** 메뉴에서 지원되는 이벤트를 나열하는 페이지로 이동합니다.

  b. 소스 또는 대상 IP 주소를 마우스 오른쪽 버튼으로 클릭하고 **View in SecureX(SecureX**에서 보기**)**를 선택합니다.

- 일반적인 이벤트 정보 확인 방법:

  a. **System(**시스템**) > Integrations(**통합**) > Cloud Services(**클라우드 서비스**)**로 이동합니다.

  b. 링크를 클릭해 Cisco SecureX Threat Response의 이벤트를 확인합니다.

단계 **2** 메시지가 표시되면 Cisco SecureX Threat Response에 로그인합니다.

웹 기반 리소스를 사용한 이벤트 조사

상황별로 크로스 실행 기능을 사용하면 Firepower Management Center 외부에 있는 웹 기반 리소스의 잠재 위협에 관한 자세한 정보를 빠르게 확인할 수 있습니다. 예를 들어 다음 작업을 할 수 있습니다.

- 알려졌거나 의심스러운 위협에 관한 정보를 게시하는, Cisco 또는 서드파티 클라우드가 호스트한 서비스에서 의심스러운 소스 IP 주소를 조회합니다.

- 조직의 기록 로그에서 특정 위협의 과거 인스턴스를 찾습니다(조직이 해당 데이터를 SIEM(Security Information and Event Management) 애플리케이션에 저장하는 경우).
- 파일 경로 정보를 포함한 특정 파일 관련 정보를 찾습니다(조직이 Cisco AMP for Endpoints를 구축한 경우).

이벤트를 조사할 때, Firepower Management Center의 이벤트 뷰어나 대시보드에서 이벤트를 클릭하면 외부 리소스의 관련 정보로 바로 이동할 수 있습니다. 이렇게 하면 특정 이벤트 관련 정보를 해당 이벤트의 IP 주소, 포트, 프로토콜, 도메인 및 SHA 256 해시를 기반으로 빠르게 수집할 수 있습니다.

예를 들어 Top Attackers(상위 공격자) 대시보드 위젯을 찾는 중이며, 나열된 소스 IP 주소 중 하나에 관한 자세한 정보를 찾고 싶다고 가정하겠습니다. Talos가 이 IP 주소에 대해 게시하는 정보를 봐야 하니, "Talos IP" 리소스를 선택합니다. Talos 웹 사이트가 이 특정 IP 주소 관련 정보가 있는 페이지를 엽니다.

Cisco와 서드파티 위협 정보 서비스에 대한 사정 정의된 링크 모음에서 하나를 선택하고, 맞춤형 링크를 다른 웹 기반 서비스에 추가하고, SIEM 또는 웹 인터페이스가 있는 다른 제품에 추가합니다. 일부 리소스는 계정 또는 제품 구매를 요구할 수도 있습니다.

상황별 크로스 실행 리소스 관리 정보

Analysis(분석) > Advanced(고급) > Contextual Cross-Launch(상황별 크로스 실행) 페이지를 이용해 외부 웹 기반 리소스를 관리합니다.

예외: 다음에 대한 교차 실행 링크 설정 Stealthwatch, 2754 페이지의 절차에 따라 Stealthwatch 어플라이언스에 대한 교차 실행 링크를 관리합니다.

Cisco가 제공하는 사정 정의된 리소스에는 Cisco 로고가 표시됩니다. 나머지 링크는 서드파티 리소스입니다.

필요 없는 리소스는 비활성화하거나 삭제할 수 있으며, 이름을 변경할 수도 있습니다. 리소스가 목록 맨 아래에 정렬되도록 소문자 "z"로 시작하는 이름을 지정하는 식입니다. 교차 실행 리소스를 비활성화하면 모든 사용자에 대해 비활성화됩니다. 삭제한 리소스는 다시 설치할 수 없지만 다시 만들 수는 있습니다.

리소스를 추가하려면 상황별 크로스 실행 리소스 추가, 2752 페이지 섹션을 참조하십시오.

맞춤형 상황별 크로스 실행 리소스 요구 사항

맞춤형 상황별로 크로스 실행 리소스를 추가하는 경우:

- 웹 브라우저를 통해 리소스를 액세스할 수 있어야 합니다.
- Http 및 https 프로토콜만 지원됩니다.
- GET 요청만 지원됩니다. POST 요청은 지원되지 않습니다.
- URL의 변수 인코딩은 지원되지 않습니다. IPv6 주소는 콜론 구분자 인코딩을 요구할 수 있지만, 대부분의 서비스는 이러한 인코딩을 요구하지 않습니다.
- 사전 정의된 리소스를 포함한 리소스를 100개까지 설정할 수 있습니다.

- 교차 실행을 생성하려면 관리자 또는 보안 분석가 사용자여야 하지만 읽기 전용 보안 분석가로 사용할 수도 있습니다.

상황별 크로스 실행 리소스 추가

보안 인텔리전스 서비스나 SIEM(Security Information and Event Management) 툴 같은 상황별로 크로스 실행 리소스를 추가할 수 있습니다.

다중 도메인 구축의 경우, 상위 도메인의 리소스는 보고 사용할 수 있지만 현재 도메인의 리소스는 생성 및 편집만 할 수 있습니다. 전체 도메인의 총 리소스 수는 100개로 제한됩니다.

시작하기 전에

- Stealthwatch 어플라이언스에 링크를 추가하는 경우 이 절차를 생략하고 다음에 대한 교차 실행 링크 설정 Stealthwatch, 2754 페이지의 내용을 참조하십시오..
- 맞춤형 상황별 크로스 실행 리소스 요구 사항, 2751 페이지의 내용을 참조하십시오.
- 링크할 리소스에 필요하다면, 계정과 액세스에 필요한 자격 증명을 생성 또는 획득합니다. 선택적으로, 액세스가 필요한 각 사용자에게 자격 증명을 할당하고 배포합니다.
- 링크할 리소스에 대한 쿼리 링크의 구문을 확인합니다.

  브라우저를 통해 리소스에 액세스하고, 필요에 따라 해당 리소스에 대한 문서를 사용하여 쿼리 링크가 찾아야 할 정보 유형(예 IP 주소)의 샘플을 검색하는 데 필요한 쿼리 링크를 작성합니다

  쿼리를 실행하고 브라우저의 위치 표시줄에서 결과 URL을 복사합니다.

  예를 들어 쿼리 URL이 **`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`**일 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**) > Advanced(**고급**) > Contextual Cross-Launch(**상황별 크로스 실행**)**를 선택합니다.

단계 **2** **New Cross-Launch(**새 크로스 실행**)**를 클릭합니다.

표시되는 양식에서, 별표가 있는 필드는 값을 입력해야 합니다.

단계 **3** 고유한 리소스 이름을 입력합니다.

단계 **4** 리소스의 작업 URL 문자열을 복사해 **URL Template(URL** 템플릿**)** 필드에 붙여넣습니다.

단계 **5** 쿼리 문자열의 특정 데이터(IP 주소 등)를 적절한 변수로 교체합니다. 커서를 놓은 다음 변수(예: **ip**)를 한 번 클릭하여 변수를 삽입합니다.

위의 "Before You Begin(시작하기 전에)" 색션에서, 결과 URL은 **`https://www.talosintelligence.com/reputation_center/lookup?search={ip}`**일 것입니다. 상황별로 크로스 실행 링크를 사용하는 경우, URL의 {ip} 변수는 이벤트 뷰어 또는 대시보드에서 사용자가 오른쪽 클릭한 IP 주소로 교체됩니다.

각 변수에 대한 설명을 보려면 커서를 변수 위에 올리십시오.

하나의 툴이나 서비스로 여러 상황별로 크로스 실행 링크를 만들 수 있으며, 이 경우 각 항목에 다른 변수를 사용해야 합니다.

단계 **6** 예시 데이터로 링크를 테스트하려면 예제 데이터를 사용한 테스트( )을 클릭합니다.

단계 **7** 문제를 해결합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

상황별 크로스 실행을 이용한 이벤트 조사

시작하기 전에

액세스하는 리소스가 자격 증명을 요구하는 경우, 해당 자격 증명이 있는지 확인하십시오.

프로시저

단계 **1** 이벤트를 표시하는 Firepower Management Center의 다음 페이지 중 하나로 이동합니다.

- 대시보드(**Overview(**개요**) > Dashboards(**대시보드**)**) 또는
- 이벤트 뷰어 페이지(이벤트의 테이블을 포함하는 **Analysis(**분석**)** 메뉴의 아무 메뉴 옵션)

단계 **2** 관심 있는 이벤트를 오른쪽 클릭하고 사용할 상황별로 크로스 실행 리소스를 선택합니다.

필요한 경우 콘텍스트 메뉴를 내려 사용할 수 있는 옵션을 모두 확인합니다

오른쪽 클릭한 데이터 유형에 따라 표시되는 옵션이 달라집니다. 예를 들어 IP 주소를 오른쪽 클릭하면 IP 주소 관련 상황별로 크로스 실행 옵션만 표시됩니다.

따라서 예를 들어 Cisco Talos에서 Top Attackers(상위 공격자) 대시보드 위젯의 소스 IP 주소 관련 위협 정보를 얻으려면, **Talos SrcIP** 또는 **Talos IP**를 선택합니다.

리소스에 여러 변수가 있는 경우, 해당 리소스를 선택하는 옵션은 포함된 각 변수에 대한 단일 유효 값이 있는 이벤트에서만 사용할 수 있습니다.

별도의 브라우저 창에 상황별로 크로스 실행 리소스가 열립니다.

쿼리하는 데이터 양, 리소스의 속도 및 요구 등의 요소에 따라 쿼리 처리에 시간이 오래 걸릴 수도 있습니다.

단계 **3** 필요한 경우 리소스에 로그인합니다.

다음에 대한 교차 실행 링크 설정 **Stealthwatch**

Firepower의 이벤트 데이터에서 Stealthwatch 어플라이언스의 관련 데이터로 교차 실행할 수 있습니다. Stealthwatch 제품에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html의 내용을 참조하십시오.

상황별 교차 실행에 대한 일반적인 정보는 상황별 크로스 실행을 이용한 이벤트 조사, 2753 페이지의 내용을 참조하십시오.

Stealthwatch 어플라이언스에 대한 일련의 교차 실행 링크를 빠르게 설정하려면 이 절차를 사용합니다.

참고

- 나중에 해당 링크를 변경해야 하는 경우 이 절차로 돌아갑니다. 상황별 교차 실행 목록 페이지에서는 직접 변경할 수 없습니다.
- 상황별 크로스 실행 리소스 추가, 2752 페이지의 절차를 사용하여 Stealthwatch 어플라이언스에 교차 실행하는 추가 링크를 수동으로 생성할 수 있지만 해당 링크는 자동으로 생성된 리소스와 무관하므로 수동으로 관리(삭제, 업데이트 등)해야 합니다.

시작하기 전에

Stealthwatch 어플라이언스가 구축되어 실행되고 있어야 합니다.

Cisco Security Analytics 및 로깅(온프레미스) 을 사용하여 Stealthwatch 어플라이언스에 Firepower 데이터를 전송하려면 Stealthwatch 어플라이언스의 원격 데이터 스토리지, 273 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**) > Logging(**로깅**) > Security Analytics & Logging(**보안 분석 및 로깅**)**을 선택합니다.

단계 **2** 기능을 활성화합니다.

단계 **3** Stealthwatch 어플라이언스의 호스트 이름이나 IP 주소, 포트를 입력합니다.

기본 포트는 443입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 새 교차 실행 링크를 확인합니다. **Analysis(**분석**) > Advanced(**고급**) > Contextual Cross-Launch(**상황별 교차 실행**)**를 선택합니다.

변경이 필요한 경우 이 절차로 돌아갑니다. 상황별 교차 실행 목록 페이지에서는 직접 변경할 수 없습니다.

다음에 수행할 작업

이벤트에서 Stealthwatch 이벤트 뷰어로 교차 실행하려면 Stealthwatch 자격 증명이 필요합니다.

FMC 이벤트 뷰어 또는 대시보드의 이벤트에서 교차 실행하려면 관련 이벤트의 테이블 셀을 마우스 오른쪽 버튼으로 클릭하고 적절한 옵션을 선택합니다.

쿼리하는 데이터 양, Stealthwatch 관리 콘솔의 속도 및 요구 등에 따라 쿼리를 처리하는 데 시간이 오래 걸릴 수도 있습니다.

Security Events(보안 이벤트)에 대한 시스템 로그 메시지 전송 정보

연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트 관련 데이터를 시스템 로그를 통해 SIEM(Security Information and Event Management) 툴 또는 에 전송할 수 있습니다.

때로는 이러한 이벤트를 Snort® 이벤트라고 지칭하기도 합니다.

보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보

보안 이벤트 시스템 로그를 전송하도록 시스템을 설정하려면, 다음 항목을 알고 있어야 합니다.

- 보안 이벤트 시스템 로그 메시지 구성 모범 사례, 2755 페이지
- 보안 이벤트 시스템 로그에 대한 설정 위치, 2760 페이지
- 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지
- 정책에서 시스템 로그 설정을 변경하는 경우, 변경사항은 재구축해야 효력을 발휘합니다.

보안 이벤트 시스템 로그 메시지 구성 모범 사례

디바이스 및 버전	설정 위치
모두	시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

디바이스 및 버전	설정 위치
Firepower Threat Defense	1. **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**) > Threat Defense Settings(**위협 방어 설정**) > Syslog(**시스템 로그**)**에서 FTD 플랫폼 설정을 구성합니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지도 참조하십시오. 2. 액세스 컨트롤 정책 Logging(로깅) 탭에서, FTD 플랫폼 설정 사용을 선택합니다. 3. (침입 이벤트의 경우) 액세스 제어 정책 Logging(로깅) 탭의 설정을 사용하도록 침입 정책을 구성합니다. (기본값입니다.) 이런 설정을 재정의하는 것은 권장하지 않습니다. 자세한 내용은 FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 2756 페이지의 내용을 참조하십시오.
기타 모든 디바이스	1. 알림 응답을 생성합니다. 2. 알림 응답을 사용하도록 액세스 제어 정책 Logging(로깅)을 설정합니다. 3. (침입 이벤트) 침입 정책에서 시스템 로그 설정을 구성합니다. 자세한 내용은 클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 2759 페이지의 내용을 참조하십시오.

FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기

이 절차에서는 FTD 디바이스에서 보안 이벤트(연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트)에 대한 시스템 로그 메시지를 전송하기 위한 모범 사례 설정을 설명합니다.

참고 대부분의 FTD 시스템 로그 설정은 보안 이벤트에 적용되지 않습니다. 이 절차에 설명된 옵션만 설정하십시오.

시작하기 전에

- Firepower Management Center에서 보안 이벤트를 생성하도록 정책을 설정하고 표시될 것으로 예상되는 이벤트가 Analysis(분석) 메뉴의 해당 테이블에 나타나는지 확인합니다.
- 시스템 로그 서버 IP 주소, 포트 및 프로토콜(UDP 또는 TCP)을 수집합니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.

- 연결 로깅에 대한 중요 정보는 연결 로깅, 2859 페이지의 관련 챕터를 참조하십시오.

프로시저

단계 **1** FTD 디바이스에 대한 시스템 로그 설정을 구성합니다.

a) **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**를 클릭합니다.
b) FTD 디바이스와 연결된 플랫폼 설정 정책을 편집합니다.
c) 왼쪽 탐색 창에서 시스템 로그를 클릭합니다.
d) **Syslog Servers(**시스템 로그 서버**)**를 클릭하고 **Add(**추가**)**를 클릭하여 서버, 프로토콜, 인터페이스 및 관련 정보를 입력합니다.

   이 페이지의 옵션에 대한 질문이 있는 경우 Syslog 서버 설정, 1459 페이지을 참조하십시오.

e) **Syslog Settings(**시스템 로그 설정**)**를 클릭하고 다음 설정을 구성합니다.
   - **Syslog** 메시지에서 타임스탬프 활성화
   - 타임스탬프 형식
   - **Syslog** 디바이스 **ID** 활성화

f) **Logging Setup(**로깅 설정**)**을 클릭합니다.
g) **Send syslogs in EMBLEM format(EMBLEM** 형식으로 시스템 로그 전송**)** 여부를 선택합니다.
h) 설정을 **Save(**저장**)**합니다.

단계 **2** 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 구성합니다.

a) **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.
b) 해당 액세스 제어 정책을 편집합니다.
c) **Logging(**로깅**)**을 클릭합니다.
d) **FTD 6.3** 이상**:** 디바이스에 구축된 **FTD** 플랫폼 설정 정책에 설정된 시스템 로그 설정을 사용합니다**.**를 선택합니다.
e) (선택 사항) **Syslog Severity(**시스템 로그 심각도**)**를 선택합니다.
f) 파일 및 악성코드 이벤트를 전송하려면 **Send Syslog messages for File and Malware(**파일 및 악성코드 이벤트에 대해 시스템 로그 메시지 전송**)**를 선택합니다.
g) **Save(**저장**)**를 클릭합니다.

단계 **3** 액세스 제어 정책에 대한 보안 인텔리전스 이벤트에 대한 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Security Intelligence(**보안 인텔리전스**)** 탭을 클릭합니다.
b) 다음 각 위치에서 로깅( )를 클릭하여 연결의 시작과 끝 및 시스템 로그 서버를 활성화합니다.
   - **DNS Policy(DNS** 정책**)** 옆.
   - **Block List(**차단 목록**)** 상자에서 **Networks(**네트워크**)** 및 **URL**에 대해.

c) **Save(**저장**)**를 클릭합니다.

단계 **4** 액세스 제어 정책에서 각 규칙에 대해 syslog 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Rules(**규칙**)** 탭을 클릭합니다.
b) 편집할 규칙을 클릭합니다.
c) 규칙에서 **Logging(**로깅**)** 탭을 클릭합니다.
d) 연결의 시작 또는 종료를 기록할지 아니면 둘 다 기록 할지를 선택합니다.

(연결 로깅은 많은 양의 데이터를 생성합니다. 시작과 끝을 모두 로깅하면 데이터 양이 약 2배 증가합니다. 모든 연결을 처음과 끝에서 모두 로깅할 수있는 것은 아닙니다.)

e) 파일 이벤트를 로깅할 경우 **Log Files(**로그 파일**)**를 선택합니다.
f) **Syslog Server(**시스템 로그 서버**)**를 활성화합니다.
g) 규칙이 "**Using default syslog configuration in Access Control Logging(**세스 제어 기록에서 기본 시스템 로그 컨피그레이션 사용**)**"인지 확인합니다.
h) **Add(**추가**)**를 클릭합니다.
i) 정책의 각 규칙에 대해 반복합니다.

단계 **5** 침입 이벤트를 전송할 경우, 다음을 수행합니다.

a) 액세스 제어 정책과 연결된 침입 정책으로 이동합니다.
b) 침입 정책에서 **Advanced Settings(**고급 설정**) > Syslog Alerting(**시스템 로그 알림**) > Enabled(**활성화**)**를 선택합니다.
c) 필요한 경우 **Edit(**편집**)**을 클릭합니다.
d) 옵션을 입력합니다.

옵션	값
로깅 호스트	다른 시스템 로그 메시지를 전송하는 것 이외의 다른 시스템 로그 서버로 침입 이벤트 시스템 로그 메시지를 보내지 않는 한 위에서 구성한 설정을 사용하려면 이 필드를 비워 두십시오.
기능	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 자세한 내용은 시스템 로그 알림 시설, 2685 페이지를 참조하십시오.
심각도	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 자세한 내용은 Syslog 심각도 레벨, 2686 페이지를 참조하십시오.

e) **Back(**뒤로**)**을 클릭합니다.
f) 탐색창에서 **Policy Information(**정책 정보**)**을 클릭합니다.
g) **Commit Changes(**변경 커밋**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) 개별 정책 및 규칙에 대해 서로 다른 로깅 설정을 구성합니다.

연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 2760 페이지의 해당 테이블 행을 참조하십시오.

이러한 설정에는 시스템 로그 알림 응답이 필요하며, 이는 Syslog 알림 응답 생성, 2684 페이지에 설명된 대로 구성됩니다. 이 절차에서 설정한 플랫폼 설정은 사용하지 않습니다.

- 클래식 디바이스에 대한 보안 이벤트 시스템 로그 로깅을 설정하려면 클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 2759 페이지의 내용을 참조하십시오.
- 변경을 완료한 경우, 매니지드 디바이스에 변경 사항을 구축합니다.

클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기

시작하기 전에

- 보안 이벤트를 생성하도록 정책을 설정합니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.
- 연결 로깅에 대한 중요 정보는 연결 로깅, 2859 페이지의 관련 챕터를 참조하십시오.

프로시저

단계 **1** 클래식 디바이스에 대한 알림 응답을 설정합니다.

Syslog 알림 응답 생성, 2684 페이지의 내용을 참조하십시오.

단계 **2** 액세스 제어 정책에서 시스템 로그 설정을 구성합니다.

a) **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.
b) 해당 액세스 제어 정책을 편집합니다.
c) **Logging(**로깅**)**을 클릭합니다.
d) **Send using specific syslog alert(**특정 시스템 로그 알림을 사용하여 전송**)**을 선택합니다.
e) 위에서 생성한 시스템 로그 알림을 선택합니다.
f) **Save(**저장**)**를 클릭합니다.

단계 **3** 파일 및 악성코드 이벤트를 전송할 경우, 다음을 수행합니다.

a) **Send Syslog messages for File and Malware events(**파일 및 악성코드 이벤트에 대한 시스템 로그 메시지 전송**)**를 선택합니다.
b) **Save(**저장**)**를 클릭합니다.

단계 **4** 침입 이벤트를 전송할 경우, 다음을 수행합니다.

a) 액세스 제어 정책과 연결된 침입 정책으로 이동합니다.
b) 침입 정책에서 **Advanced Settings(**고급 설정**) > Syslog Alerting(**시스템 로그 알림**) > Enabled(**활성화**)**를 선택합니다.
c) 필요한 경우, **Edit(**편집**)**을 클릭합니다.

d) 옵션을 입력합니다.

옵션	값
로깅 호스트	다른 시스템 로그 메시지를 전송하는 것 이외의 다른 시스템 로그 서버로 침입 이벤트 시스템 로그 메시지를 보내지 않는 한 위에서 구성한 설정을 사용하려면 이 필드를 비워 두십시오.
기능	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 시스템 로그 알림 시설, 2685 페이지의 내용을 참조하십시오.
심각도	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. Syslog 심각도 레벨, 2686 페이지의 내용을 참조하십시오.

e) **Back(**뒤로**)**을 클릭합니다.
f) 탐색창에서 **Policy Information(**정책 정보**)**을 클릭합니다.
g) **Commit Changes(**변경 커밋**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) 개별 액세스 제어 규칙에 대해 서로 다른 로깅 설정을 구성합니다. 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 2760 페이지의 해당 테이블 행을 참조하십시오. 이러한 설정에는 Syslog 알림 응답 생성, 2684 페이지에 설명된 대로 구성된 시스템 로그 알림 응답이 필요합니다. 위에서 구성한 설정은 사용하지 않습니다.
- FTD 디바이스에 대한 보안 이벤트 시스템 로그 로깅을 설정하려면 FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 2756 페이지의 내용을 참조하십시오.

보안 이벤트 시스템 로그에 대한 설정 위치

- 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 2760 페이지
- 침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 디바이스), 2762 페이지
- 침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 이전 버전의 디바이스), 2763 페이지
- 파일 및 악성코드 이벤트에 대한 시스템 로그 설정 위치, 2764 페이지

연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스)

로깅 설정은 여러 곳에서 설정할 수 있습니다. 아래 표를 사용하여 필요한 옵션을 설정했는지 확인합니다.

중요

- 시스템 로그 설정은 신중하게 수행해야 하며, 다른 설정에서 상속받은 기본값을 사용할 때는 특히 주의해야 합니다. 아래 표에서 설명하듯이, 매니지드 디바이스 모델과 소프트웨어 버전에 따라 사용할 수 없는 옵션도 있습니다.
- 연결 로깅 설정 관련 중요 정보는 연결 로깅, 2859 페이지의 관련 챕터를 참조하십시오.

설정 위치	설명 및 상세정보
Devices(장치**) > Platform Settings(**플랫폼 설정**)**, Threat Defense Settings(위협 방어 설정) 정책, **Syslog(**시스템 로그**)**	이 옵션은 Firepower Threat Defense(Firepower 위협 방어) 디바이스에만 적용됩니다. 여기서 구성하는 설정은 Access Control(액세스 컨트롤) 정책에 대한 Logging(기록) 설정에서 지정할 수 있으며, 이 표에 있는 나머지 정책과 규칙에서 사용하거나 재정의할 수 있습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지, Syslog 정보, 1445 페이지 및 하위 항목을 참조하십시오.
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Logging(**기록**)**	여기서 구성하는 설정은 모든 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그의 기본 설정입니다. 단 이 표의 나머지 행에서 지정하는 위치에 있는 하위 정책 및 규칙에서 기본값을 재정의하는 경우는 예외입니다. FTD 디바이스의 권장 설정입니다. FTD Platform Settings(FTD 플랫폼 설정)를 사용합니다. 자세한 정보는 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지, Syslog 정보, 1445 페이지 및 하위 항목을 참조하십시오. 다른 모든 디바이스의 필수 설정입니다. 시스템 로그 알림을 사용합니다. 시스템 로그 알림을 지정하는 경우에는 Syslog 알림 응답 생성, 2684 페이지 섹션을 참조하십시오. Logging(기록) 탭의 설정에 관한 자세한 내용은 액세스 제어 정책용 로깅 설정, 1636 페이지섹션을 참조하십시오.
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Rules(**규칙**)**, **Default Action(**기본 작업**)** 행, 로깅( )	액세스 컨트롤 정책과 관련된 기본 작업의 기록 설정입니다. 액세스 제어 규칙, 1645 페이지 챕터 및 정책 기본 작업으로 연결 로깅, 2873 페이지의 기록 관련 정보를 참조하십시오.
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Rules(**규칙**)**, <각 규칙>, **Logging(**기록**)**	액세스 컨트롤 정책의 특정 규칙에 대한 기록 설정입니다. 액세스 제어 규칙, 1645 페이지 챕터의 기록 관련 정보를 참조하십시오.

설정 위치	설명 및 상세정보
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Security Intelligence(**보안 인텔리전스**)**, 로깅( )	보안 인텔리전스 차단 목록의 기록 설정입니다. 버튼을 클릭해 다음을 설정합니다. • DNS 차단 목록 로깅 옵션 • URL 차단 목록 로깅 옵션 • 네트워크 차단 목록 기록 옵션(차단 목록의 IP 주소용) 사전 요구 사항 섹션, 하위 항목 및 링크를 포함한 보안 인텔리전스 설정, 1698 페이지의 정보를 참조하십시오.
Policies(정책**) > SSL**, <각 정책>, **Default Action(**기본 작업**)** 행, 로깅( )	SSL 정책과 관련된 기본 작업의 기록 설정입니다. 정책 기본 작업으로 연결 로깅, 2873 페이지의 내용을 참조하십시오.
Policies(정책**) > SSL**, <각 정책>, <각 규칙>, **Logging(**로깅**)**	SSL 규칙에 대한 기록 설정입니다. TLS/SSL 규칙 구성 요소, 1776 페이지의 내용을 참조하십시오.
Policies(정책**) > Prefilter(**사전 필터**)**, <각 정책>, **Default Action(**기본 작업**)** 행, 로깅( )	사전 필터 정책과 관련된 기본 작업의 기록 설정입니다. 정책 기본 작업으로 연결 로깅, 2873 페이지의 내용을 참조하십시오.
Policies(정책**) > Prefilter(**사전 필터**)**, <각 정책>, <각 사전 필터 규칙>, **Logging(**기록**)**	사전 필터 정책의 각 사전 필터 규칙에 대한 기록 설정입니다. 터널 및 사전 필터 규칙 구성 요소, 1731 페이지의 내용을 참조하십시오.
Policies(정책**) > Prefilter(**사전 필터**)**, <각 정책>, <각 터널 규칙>, **Logging(**기록**)**	사전 필터 정책의 각 터널 규칙에 대한 기록 설정입니다. 터널 및 사전 필터 규칙 구성 요소, 1731 페이지의 내용을 참조하십시오.
FTD 클러스터 설정에 대한 추가 시스템 로그 설정:	Firepower Threat Defense 클러스터링, 917 페이지 챕터에는 시스템 로그에 대한 여러 참조자료가 있습니다. 챕터에서 "syslog"를 검색해 보십시오.

침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 디바이스)

다양한 위치에서 침입 정책의 시스템 로그 설정을 지정할 수 있으며, 선택적으로 액세스 컨트롤 정책 또는 FTD Platform Settings(FTD 플랫폼 설정)이나 양쪽 모두의 설정을 상속할 수도 있습니다.

설정 위치	설명 및 상세정보
Devices(장치**) > Platform Settings(**플랫폼 설정**)**, Threat Defense Settings(위협 방어 설정) 정책, **Syslog(**시스템 로그**)**	여기서 구성하는 시스템 로그 대상은 침입 정책의 기본값이 될 수 있는, 액세스 컨트롤 정책의 Logging(기록) 탭에서 지정할 수 있습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지, Syslog 정보, 1445 페이지 및 하위 항목을 참조하십시오.
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Logging(**기록**)**	침입 정책이 다른 기록 호스트를 지정하지 않는 경우, 침입 이벤트에 대한 시스템 로그 대상의 기본 설정입니다. 액세스 제어 정책용 로깅 설정, 1636 페이지의 내용을 참조하십시오.
Policies(정책**) > Intrusion(**침입**)**, <각 정책>, **Advanced Settings(**고급 설정**)**에서 **Syslog Alerting(**시스템 로그 알림**)**을 활성화하고 **Edit(**편집**)** 클릭	Logging(기록) 탭의 액세스 컨트롤 정책에 지정된 대상이 아닌 다른 시스템 로그 수집기를 지정하고 시설과 심각도를 지정하려면, 침입 이벤트를 위한 시스템 로그 알림 설정, 2694 페이지 섹션을 참조하십시오. 침입 정책에 설정된 **Severity(**심각도**)**나 **Facility(**시설**)** 또는 둘 다를 사용하고 싶다면, 정책에서 기록 호스트를 설정해야 합니다. 액세스 컨트롤 정책에서 지정하는 기록 호스트를 사용하는 경우, 침입 규칙에 지정된 심각도와 시설은 사용하지 않습니다.

침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 이전 버전의 디바이스)

- (기본값) 액세스 컨트롤 정책액세스 제어 정책용 로깅 설정, 1636 페이지, 시스템 로그 알림을 지정하는 경우(Syslog 알림 응답 생성, 2684 페이지 참조)
- 또는 침입 이벤트를 위한 시스템 로그 알림 설정, 2694 페이지 섹션을 참조하십시오.

기본적으로, 침입 정책은 액세스 컨트롤 정책의 Logging(로깅) 탭에 있는 설정을 사용합니다. FTD 이아닌 디바이스에 적용 가능한 설정이 구성되어 있지 않다면, 시스템 로그는 FTD 이외의 디바이스에는 전송되지 않으며 경고도 표시되지 않습니다.

파일 및 악성코드 이벤트에 대한 시스템 로그 설정 위치

설정 위치	설명 및 상세정보
액세스 컨트롤 정책에서 **Policies(**정책**) > Access Control(**액세스 컨트롤**),** <각 정책>, **Logging(**기록**)**	파일 및 악성코드 이벤트에 대한 시스템 로그를 전송하도록 시스템을 설정하는 기본 위치입니다. FTD Platform Settings(FTD 플랫폼 설정)에서 시스템 로그 설정을 사용하지 않는다면, 알림 응답도 생성해야 합니다. Syslog 알림 응답 생성, 2684 페이지의 내용을 참조하십시오.
Firepower Threat Defense 플랫폼 설정에서 **Devices(**장치**) > Platform Settings(**플랫폼 설정**),** Threat Defense Settings(위협 방어 설정) 정책, **Syslog(**시스템 로그**)**	이러한 설정은 지원되는 버전을 실행하는 Firepower Threat Defense(Firepower 위협 방어) 디바이스에만 적용되며, FTD 플랫폼 설정을 사용할 액세스 컨트롤 정책에서 Logging(기록) 탭을 설정한 경우에만 적용됩니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, 1452 페이지, Syslog 정보, 1445 페이지 및 하위 항목을 참조하십시오.
액세스 컨트롤 규칙에서 **Policies(**정책**) > Access Control(**액세스 컨트롤**),** <각 정책>, <각 규칙>, **Logging(**기록**)**	FTD Platform Settings(FTD 플랫폼 설정)에서 시스템 로그 설정을 사용하지 않는다면, 알림 응답도 생성해야 합니다. Syslog 알림 응답 생성, 2684 페이지의 내용을 참조하십시오.

Security(보안) 이벤트 시스템 로그 메시지 구조

FTD 에서 전송하는 보안 이벤트 메시지 예시(침입 이벤트)

```
 0        1              2              3        4   5     6
___   ___________   ___________   _______   ___  __  ______

<37>2018-06-27 192.168.0.81 SFIMS : %FTD-5-430001:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Rev
Message: "DCE2_EVENT   SMB_INVALID_DSIZE", Classif
Potentially Bad Traffic, User: No Authentication R
Client: NetBIOS-ssn (SMB) client, ApplicationProto
(SMB), ACPolicy: test, NAPPolicy: Balanced Securit
Connectivity, InlineResult: Blocked
```

표 279: 보안 이벤트 시스템 로그 메시지의 구성 요소

샘플 메시지의 항목 수	헤더 요소	설명
0	PRI	알림의 기능 및 심각도를 모두 나타내는 우선 순위 값입니다. 이 값은 FMC 플랫폼 설정을 사용하여 EMBLEM 형식으로 로깅을 활성화한 경우에만 시스템 로그 메시지에 나타납니다. 액세스 제어 정책 Logging(로깅) 탭을 통해 침입 이벤트 로깅을 활성화하면 PRI 값이 시스템 로그 메시지에 자동으로 표시됩니다. EMBLEM 형식을 활성화하는 방법에 대한 자세한 내용은 로깅 활성화 및 기본 설정, 1452 페이지의 내용을 참조하십시오. PRI에 대한 자세한 내용은 RFC5424를 참조하십시오.
1	타임스탬프	디바이스에서 시스템 로그 메시지가 전송된 날짜와 시간입니다. • (FTD 장치에서 전송된 시스템 로그) 액세스 컨트롤 정책 및 그 하위 항목의 설정의 경우, 또는 이 형식을 FTD Platform Settings(FTD 플랫폼 설정)에서 사용하도록 지정한 경우 날짜 형식은 RFC 5424에 지정하는 ISO 8601 타임스탬프 형식에서 정의하는 형식(yyyy-MM-ddTHH:mm:ssZ)입니다. 여기서 Z는 UTC 시간대를 의미합니다. • (다른 모든 장치에서 전송된 시스템 로그) 액세스 컨트롤 정책 및 그 하위 항목의 설정의 경우, 날짜 형식은 RFC 5424에 지정하는 ISO 8601 타임스탬프 형식에서 정의하는 형식(yyyy-MM-ddTHH:mm:ssZ)입니다. 여기서 Z는 UTC 시간대를 의미합니다. • 그렇지 않은 경우에는 UTC 시간대의 월, 일, 시간이 되지만, 시간대는 표시되지 않습니다. FTD Platform Settings(FTD 플랫폼 설정)에서 타임스탬프 설정을 구성하는 방법은 Syslog 설정, 1458 페이지 섹션을 참조하십시오.

샘플 메시지의 항목 수	헤더 요소	설명
2	메시지를 보낸 디바이스 또는 인터페이스입니다. 다음을 선택할 수 있습니다. • 인터페이스의 IP 주소 • 디바이스 호스트 이름 • 맞춤형 디바이스 식별자	(FTD 디바이스 전송된 시스템 로그 전용) 시스템 로그 메시지가 FTD Platform Settings(FTD 플랫폼 설정)을 사용하여 전송된 경우, 이것은 **Enable Syslog Device ID(**시스템 로그 디바이스 **ID)** 옵션(지정한 경우)의 **Syslog Settings(**시스템 로그 설정**)**에서 설정한 값입니다. 그렇지 않은 경우, 이 요소는 헤더에 존재하지 않습니다. FTD Platform Settings(FTD 플랫폼 설정)에서 이 설정을 구성하는 방법은 Syslog 설정, 1458 페이지 섹션을 참조하십시오.
3	맞춤형 값	알림 응답을 사용하여 메시지를 전송한 경우, 이것은 메시지를 전송한 알림 응답에서 설정한 **Tag(**태그**)** 값입니다(설정한 경우). (Syslog 알림 응답 생성, 2684 페이지 참조) 그렇지 않은 경우, 이 요소는 헤더에 존재하지 않습니다.
4	%FTD %NGIPS	메시지를 전송한 디바이스의 유형입니다. • %FTD는 Firepower Threat Defense(Firepower 위협 방어)입니다. • %NGIPS는 다른 모든 디바이스입니다.
5	심각도	메시지를 트리거한 정책의 시스템 로그 설정에서 지정한 심각도입니다. 심각도 설명은 심각도 레벨, 1446 페이지 또는 Syslog 심각도 레벨, 2686 페이지 섹션을 참조하십시오.
6	이벤트 유형 식별자	• 430001: 침입 이벤트 • 430002: 연결 시작 시 기록된 연결 이벤트 • 430003: 연결 종료 시 기록된 연결 이벤트 버전 6.4 이상을 실행하는 디바이스에서 전송한 메시지의 경우, 다음 이벤트 유형 ID도 사용합니다. • 430004: 파일 이벤트 • 430005: 파일 악성코드 이벤트

샘플 메시지의 항목 수	헤더 요소	설명
--	기능	보안 이벤트 시스템 로그 메시지의 시설, 2767 페이지의 내용을 참조하십시오.
--	메시지의 나머지 부분	필드와 값은 콜론으로 구분합니다. 비어 있거나 알 수 없는 값이 있는 필드는 메시지에서 생략됩니다. 필드 설명은 다음을 참조하십시오. • 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지. • 침입 이벤트 필드, 2912 페이지 • 파일 및 악성코드 이벤트 필드, 2968 페이지 참고 필드 설명 목록은 시스템 필드와 이벤트 뷰어(Firepower Management Center 웹 인터페이스의 Analysis(분석) 메뉴에 있는 메뉴 옵션)에 표시되는 필드를 모두 포함합니다. 시스템 로그를 통해 사용할 수 있는 필드에는 다음과 같은 레이블이 지정됩니다. 이벤트 뷰어에 표시되는 필드 중 일부는 시스템 로그를 통해 사용할 수 없습니다. 또한 이벤트 뷰어에 포함되지 않는(하지만 검색을 통해 사용할 수 있는) 시스템 로그 필드도 있으며, 결합되거나 분리된 필드도 존재합니다.

보안 이벤트 시스템 로그 메시지의 시설

일반적으로 시설 값은 보안 이벤트의 시스템 로그 메시지와는 무관합니다. 그러나 Facility(시설)이 필요하다면, 다음 표를 사용하십시오.

디바이스	시설을 연결 이벤트에 포함하는 방법	시설을 침입 이벤트에 포함하는 방법	시스템 로그 메시지에서의 위치
FTD	FTD Platform Settings(FTD 플랫폼 설정)에서 EMBLEM 옵션을 사용합니다. FTD Platform Settings(FTD 플랫폼 설정)를 사용하여 시스템 로그 메시지를 전송하는 경우, 연결 이벤트에 대한 시설은 언제나 **ALERT**입니다.	FTD Platform Settings(FTD 플랫폼 설정)에서 EMBLEM 옵션을 사용하거나 침입 규칙의 시스템 로그 설정을 사용하여 기록을 구성합니다. 침입 정책을 사용하는 경우에는 침입 정책 설정에서 기록 호스트를 지정해야 합니다.	시설은 메시지 헤더에는 표시되지 않지만, 시스템 수집기는 RFC 5424, 섹션 6.2.1을 바탕으로 값을 끌어낼 수 있습니다.
FTD 이외의 디바이스	알림 응답을 사용합니다.	침입 정책 고급 설정의 시스템 로그 설정을 사용하거나 액세스 컨트롤 정책 Logging(기록) 탭에서 식별한 응답 알림을 사용합니다.	

자세한 내용은 침입 시스템 로그 알림에 대한 시설 및 Severities(심각도), 2695 페이지 및 Syslog 알림 응답 생성, 2684 페이지의 내용을 참조하십시오.

Firepower System 로그 메시지 유형

Firepower는 다음 테이블에서 설명하는 것처럼 여러 시스템 로그 데이터 유형을 전송할 수 있습니다.

시스템 로그 데이터 유형	확인
FMC의 감사 로그	시스템 로그로의 감사 로그 스트리밍 및 시스템 감사, 449 페이지 챕터
기본 디바이스(7000/8000 시리즈, ASA FirePOWER, NGIPSv)의 감사 로그	클래식 디바이스에서의 감사 로그 스트리밍, 1408 페이지 및 시스템 감사, 449 페이지 챕터 CLI 명령: syslog
디바이스 상태 및 FTD의 네트워크 관련 로그	Syslog 정보, 1445 페이지 및 하위 항목
연결, 보안 인텔리전스 및 FTD 디바이스의 침입 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보, 2755 페이지.
연결, 보안 인텔리전스 및 기본 디바이스의 침입 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보, 2755 페이지

시스템 로그 데이터 유형	확인
파일 및 악성코드 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보, 2755 페이지

보안 이벤트에 대한 시스템 로그 제한 사항

- 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.
- 이벤트가 시스템 로그 수집기에 표시될 때까지 최대 15분이 걸릴 수 있습니다.
- 다음 파일 및 악성코드 이벤트의 데이터는 시스템 로그를 통해 사용할 수 없습니다.
  - 회귀 이벤트
  - AMP for Endpoints(엔드포인트용 AMP)가 생성한 이벤트

eStreamer 서버 스트리밍

Event Streamer(eStreamer)를 사용하면 여러 종류의 이벤트 데이터를 Firepower Management Center 또는 7000 또는 8000 Series 디바이스에서 맞춤 개발된 클라이언트 애플리케이션으로 스트리밍할 수 있습니다. 자세한 내용은 *Firepower System Event Streamer* 통합 가이드를 참고하십시오.

eStreamer 서버로 사용할 어플라이언스가 외부 클라이언트로 eStreamer 이벤트의 스트리밍을 시작하기 전에 이벤트를 클라이언트로 전송하고, 클라이언트에 대한 정보를 제공하고, 통신 설정 시 사용할 인증 자격 증명 집합을 생성하도록 eStreamer 서버를 구성해야 합니다. 어플라이언스의 사용자 인터페이스에서 이 모든 작업을 수행할 수 있습니다. 설정이 저장되면, 선택한 이벤트는 요청 시 eStreamer 클라이언트에 전달됩니다.

eStreamer 서버가 이벤트를 요청하는 클라이언트에 전송할 수 있는 이벤트 유형을 제어할 수 있습니다.

표 ***280: eStreamer*** 서버가 전송할 수 있는 이벤트 유형

이벤트 유형	설명
침입 이벤트	매니지드 디바이스에서 생성된 침입 이벤트
침입 이벤트 패킷 데이터	침입 이벤트와 관련된 패킷
침입 이벤트 추가 데이터	HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소와 같은 침입 이벤트와 관련된 추가 데이터
검색 이벤트	네트워크 검색 이벤트

이벤트 유형	설명
상관관계 및 화이트리스트 이벤트	상관관계 및 컴플라이언스 화이트 목록 이벤트
영향 플래그 알림	다음이 생성한 영향 알림 FMC
사용자 이벤트	사용자 이벤트
악성코드 이벤트	악성코드 이벤트
파일 이벤트	파일 이벤트
연결 이벤트	모니터링되는 호스트와 기타 모든 호스트 간의 세션 트래픽에 대한 정보입니다.

시스템 로그 및 eStreamer의 보안 이벤트 비교

일반적으로, eStreamer에 큰 투자를 하지 않은 조직은 시스템 로그 대신 eStreamer를 사용하여 보안 이벤트 데이터를 외부적으로 관리해야 합니다.

시스템 로그	**eStreamer**
맞춤형 필요 없음	각 릴리스의 변경사항을 수용하려면 상당한 수준의 맞춤형 및 유지관리가 필요함
표준	Proprietary
시스템 로그 표준은 데이터 손실을 방지하지 않으며, UDP를 사용할 때는 더욱 그렇습니다.	데이터 손실 방지
디바이스에서 직접 전송	FMC에서 전송하며, 처리 오버헤드 추가
파일 및 악성코드 이벤트, 연결 이벤트(보안 인텔리전스 이벤트 포함) 및 침입 이벤트를 지원합니다.	eStreamer 서버 스트리밍, 2769 페이지에 나열된 모든 이벤트 유형을 지원합니다.
일부 이벤트 데이터는 FMC에서만 전송할 수 있습니다. (시스템 로그가 아닌) eStreamer로만 전송된 데이터, 2770 페이지의 내용을 참조하십시오.	디바이스에서 시스템 로그를 통해 직접 전송될 수 없는 데이터를 포함합니다. (시스템 로그가 아닌) eStreamer로만 전송된 데이터, 2770 페이지의 내용을 참조하십시오.

(시스템 로그가 아닌) eStreamer로만 전송된 데이터

다음 데이터는 에서만 사용할 수 있으며, 따라서 디바이스에서 시스템 로그를 통해 전송할 수 없습니다.Firepower Management Center

- 패킷 로그
- 침입 이벤트 추가 데이터 이벤트

자세한 내용은 eStreamer 서버 스트리밍, 2769 페이지의 내용을 참조하십시오.

- 통계 및 통합 이벤트
- 네트워크 검색 이벤트
- 사용자 활동 및 로그인 이벤트
- 상관관계 이벤트
- 악성코드 이벤트:
  - 회귀 판정
  - 관련 SHA 정보가 디바이스에 이미 동기화되어 있지 않은 경우 ThreatName 및 분류
- 다음 필드:
  - Impact 및 ImpactFlag 필드

    자세한 내용은 eStreamer 서버 스트리밍, 2769 페이지의 내용을 참조하십시오.
  - IOC_Count 필드
- 대부분의 원시 ID 및 UUID입니다.

  예외
  - 연결 이벤트에 대한 시스템 로그는 FirewallPolicyUUID, FirewallRuleID, TunnelRuleID, MonitorRuleID, SI_CategoryID, SSL_PolicyUUID, SSL_RuleID가 포함됩니다.
  - 침입 이벤트의 시스템 로그는 IntrusionPolicyUUID, GeneratorID, SignatureID를 포함합니다.
- 확장 메타데이터(다음을 포함하되 이에 제한되지 않음):
  - LDAP에서 제공한 사용자 상세정보(전체 이름, 부서, 전화 번호 등)

    시스템 로그는 이벤트의 사용자 이름만 제공합니다.
  - SSL 인증 상세정보 같은 상태 기반 정보

    시스템 로그는 인증서 지문과 같은 기본 정보를 제공하지만, cert CN 같은 다른 인증서 세부 정보는 제공하지 않습니다.
  - 앱 태그 및 범주 같은 자세한 애플리케이션 정보

    시스템 로그는 애플리케이션 이름만 제공합니다.

  일부 메타데이터 메시지에는 개체에 대한 추가 정보도 포함됩니다.
- 지오로케이션 정보

eStreamer 이벤트 유형 선택

eStreamer Event Configuration(eStreamer 이벤트 설정**)** 확인란는 eStreamer 서버가 전송할 수 있는 이벤트를 제어합니다. 클라이언트에서는 여전히 eStreamer 서버로 전송하는 요청 메시지에서 수신하고자 하는 이벤트 유형을 구체적으로 요청해야 합니다. 자세한 내용은 *Firepower System Event Streamer* 통합 가이드을 참조하십시오.

다중 도메인 구축에서는 어떤 도메인 수준에서도 eStreamer 이벤트 설정을 구성할 수 있습니다. 그러나 상위 도메인이 특정 이벤트 유형을 활성화했다면, 하위 도메인에서는 이벤트 유형을 비활성화할 수 없습니다.

FMC 및 7000 및 8000 Series 디바이스에 대해 이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Integration(**통합**)**를 선택합니다.

단계 **2** **eStreamer**를 클릭합니다.

단계 **3** eStreamer 서버 스트리밍, 2769 페이지에 설명된 대로, **eStreamer Event Configuration(eStreamer** 이벤트 설정**)**에서 eStreamer가 요청 클라이언트로 전달하도록 할 이벤트 유형 옆에 있는 확인란을 선택하거나 선택 해제합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

eStreamer 클라이언트 커뮤니케이션 설정

eStreamer가 eStreamer 이벤트를 클라이언트에 전송하려면, 먼저 eStreamer 페이지에서 클라이언트를 eStreamer 서버의 피어 데이터베이스에 추가해야 합니다. 또한 eStreamer 서버에서 생성된 인증 인증서를 클라이언트에 복사해야 합니다. 이상의 단계를 완료하면 eStreamer 서비스를 다시 시작하지 않고도 클라이언트를 eStreamer 서버에 연결할 수 있습니다.

다중 도메인 구축에서는 모든 도메인에서 eStreamer 클라이언트를 만들 수 있습니다. 인증 인증서를 이용하면 클라이언트가 클라이언트 인증서의 도메인 및 하위 도메인의 이벤트만 요청하게 할 수 있습니다. eStreamer 설정 페이지는 현재 도메인과 연결된 클라이언트만 표시하므로, 인증서를 다운로드하거나 취소하려면 클라이언트가 생성된 도메인으로 전환해야 합니다.

FMC 및 7000 및 8000 Series 디바이스에 대해 이 작업을 수행하려면 관리자 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Integration(**통합**)**를 선택합니다.

단계 **2** **eStreamer**를 클릭합니다.

단계 **3** **Create Client(**클라이언트 생성**)**를 클릭합니다.

단계 **4** **Hostname(**호스트 이름**)** 필드에 eStreamer 클라이언트를 실행하는 호스트의 IP 주소 또는 호스트 이름을 입력합니다.

참고 DNS 확인을 설정하지 않은 경우, IP 주소를 사용해야 합니다.

단계 **5** 인증서 파일을 암호화하려면, **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.
이제 eStreamer 서버는 호스트가 eStreamer 서버의 포트 8302에 액세스하는 것을 허용하고 클라이언트-서버 인증 중에 사용할 인증 인증서를 만듭니다.

단계 **7** 인증서 파일을 다운로드하려면 클라이언트 호스트 이름 옆에 있는 다운로드( )을 클릭합니다.

단계 **8** SSL 인증을 위해 클라이언트가 사용한 적절한 디렉터리에 인증서 파일을 저장합니다.

단계 **9** 클라이언트에 대한 액세스를 취소하려면, 제거할 호스트 옆에 있는 삭제( )을 클릭합니다.

eStreamer 서비스를 다시 시작할 필요가 없으며, 액세스는 즉시 취소됩니다.

Splunk의 이벤트 분석

Splunk용 Cisco Secure Firewall(f.k.a. Firepower)(이전 명칭: Splunk용 Cisco Firepower App)를 외부 툴로 사용하여 Firepower 이벤트 데이터를 표시하고 사용하여 네트워크에서 위협을 추적하고 조사할 수 있습니다.

eStreamer가 필요합니다. 고급 기능입니다. eStreamer 서버 스트리밍, 2769 페이지를 참조하십시오.

자세한 내용은 https://cisco.com/go/firepower-for-splunk를 참고하십시오.

IBM QRadar의 이벤트 분석

IBM QRadar용 Cisco Firepower 앱을 대체 방법으로 사용하여 이벤트 데이터를 표시하고 네트워크에 대한 위협을 분석, 추적 및 조사할 수 있습니다.

eStreamer가 필요합니다. 이는 고급 기능입니다. eStreamer 서버 스트리밍, 2769 페이지를 참조하십시오.

자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html를 참고하십시오.

외부 툴을 사용한 이벤트 데이터 분석 기록

기능	버전	세부 사항
데이터를 보기 위한 교차 실행 Stealthwatch	6.7	이 기능을 사용하면 Analysis(분석) > Contextual Cross-Launch(상황별 교차 실행) 페이지에서 Stealthwatch 어플라이언스에 대한 여러 항목을 빠르게 생성할 수 있습니다. 이러한 항목을 사용하면 관련 이벤트를 마우스 오른쪽 버튼으로 클릭하여 Stealthwatch를 교차 실행하고 교차 시작한 데이터 지점과 관련된 정보를 표시할 수 있습니다. 새 메뉴 항목: System(시스템) > Logging(로깅) > Security Analytics and Logging(보안 분석 및 로깅) Stealthwatch로 이벤트 전송을 설정할 새 페이지입니다.
추가 필드 유형에서 상황별 교차 실행	6.7	이제 다음과 같은 추가 이벤트 데이터 유형을 사용하여 외부 애플리케이션으로 교차 실행할 수 있습니다. • 액세스 제어 정책 • 침입 정책 • 애플리케이션 프로토콜 • 클라이언트 애플리케이션 • 웹 애플리케이션 • 사용자 이름(영역 포함) 새로운 메뉴 옵션: 이제 Analysis(분석) 메뉴 아래의 페이지에서 대시보드 위젯 및 이벤트 테이블의 이벤트에 대한 위의 데이터 유형을 마우스 오른쪽 버튼으로 클릭하면 상황별 교차 실행 옵션을 사용할 수 있습니다. 지원되는 플랫폼: Firepower Management Center

기능	버전	세부 사항
IBM QRadar와의 통합	6.0 이상	IBM QRadar 사용자는 새로운 Firepower 전용 앱을 통해 이벤트 데이터를 분석할 수 있습니다. 사용 가능한 기능은 Firepower 버전에 따라 달라집니다. IBM QRadar의 이벤트 분석, 2773 페이지의 내용을 참조하십시오.

개선 사항은 다음에 통합됩니다. Cisco SecureX Threat Response	6.5	• 지역 클라우드 지원:
		  • 미합중국(북미)
		  • 유럽
		• 추가 이벤트 유형 지원:
		  • 파일 및 악성코드 이벤트
		  • 높은 우선순위 연결 이벤트
		  다음과 관련된 연결 이벤트입니다.
		  • 침입 이벤트
		  • 보안 인텔리전스 이벤트
		  • 파일 및 악성코드 이벤트
		수정된 화면: **System(**시스템**) > Integration(**통합**) > Cloud Service(**클라우드 서비스**)**의 새 옵션
		지원 플랫폼: 이 버전에서는 직접 통합 또는 시스템 로그의 형태로 모든 디바이스를 지원합니다.

시스템 로그	6.5	이제 AccessControlRuleName 필드를 침입 이벤트 시스템 로그 메시지에서 사용할 수 있습니다.
통합 Cisco Security Packet Analyzer	6.5	이 기능의 지원은 삭제되었습니다.

기능	버전	세부 사항
통합 Cisco SecureX Threat Response	6.3(시스템 로그를 통해, 프록시 수집기 사용) 6.4(직접)	Firepower 침입 이벤트 데이터를 다른 소스의 데이터와 통합해 Cisco SecureX Threat Response의 강력한 분석 도구를 사용하여 네트워크상의 위협을 통합적으로 확인합니다. 수정된 화면(버전 6.4): **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)**의 새 옵션 지원되는 플랫폼: 버전 6.3(시스템 로그를 통해) 또는 6.4를 실행하는 Firepower Threat Defense 디바이스
파일 및 악성코드 이벤트에 대한 시스템 로그 지원	6.4	이제 완전히 인증된 파일 및 악성코드 이벤트 데이터를 시스템 로그를 통해 매니지드 디바이스에서 전송할 수 있습니다. 수정된 화면: **Policies(**정책**) > Access Control(**액세스 제어**) > Access Control(**액세스 제어**) > Logging(**로깅**)** 지원 되는 플랫폼: 버전 6.4를 실행하는 모든 매니지드 디바이스
Splunk와의 통합	모든 6.x 버전 지원.	Splunk 사용자는 새로운 별도의 Splunk 앱인 Splunk용 Cisco Secure Firewall(f.k.a. Firepower)을(를) 사용하여 이벤트를 분석할 수 있습니다. 사용 가능한 기능은 Firepower 버전에 따라 달라집니다. Splunk의 이벤트 분석, 2773 페이지의 내용을 참조하십시오.

기능	버전	세부 사항
통합 Cisco Security Packet Analyzer	6.3	도입된 기능: 이벤트와 관련된 패킷의 Cisco Security Packet Analyzer을(를) 즉시 쿼리하고, 클릭하여 Cisco Security Packet Analyzer의 결과를 검사하거나 다운로드해 다른 외부 도구에서 분석합니다. 새 화면: **System(**시스템**)** > **Integration(**통합**)** > **Packet Analyzer(**패킷 분석기**)** **Analysis(**분석**)** > **Advanced(**고급**)** > **Packet Analyzer Queries(**패킷 분석기 쿼리**)** 새 메뉴 옵션: Dashboard(대시보드) 페이지와 Analysis(분석) 메뉴의 페이지에 있는 이벤트를 오른쪽 클릭할 때 나타나는 **Query Packet Analyzer(**쿼리 패킷 분석기**)** 지원되는 플랫폼: Firepower Management Center
상황별 크로스 실행	6.3	도입된 기능: 이벤트를 오른쪽 클릭해 사전 정의 또는 맞춤형 URL 기반 외부 리소스에서 관련 정보를 찾습니다. 새 화면: **Analysis(**분석**)** > **Advanced(**고급**)** > **Contextual Cross-Launch(**상황별 크로스 실행**)** 새 메뉴 옵션: Dashboard(대시보드) 페이지와 Analysis(분석) 메뉴의 페이지에 있는 이벤트를 오른쪽 클릭할 때 나타나는 여러 옵션 지원되는 플랫폼: Firepower Management Center

기능	버전	세부 사항
연결 및 침입 이벤트용 시스템 로그 메시지	6.3	통합되고 단순화된 새로운 설정을 사용하여, 시스템 로그를 통해 완전히 인증된 연결 및 침입 이벤트를 외부 스토리지로 전송하는 기능 이제 메시지 헤더가 표준화되었고 이벤트 유형 식별자를 포함하며, 알 수 없거나 값이 없는 필드는 생략되기 때문에 미시지가 서로 비슷해집니다. 지원되는 플랫폼: • 모든 새 기능: 버전 6.3을 실행하는 FTD 디바이스 • 일부 새 기능: 버전 6.3을 실행하는 FTD 이외의 디바이스 • 소수의 새 기능: 버전 6.3 미만을 실행하는 모든 디바이스. 자세한 내용은 Security Events(보안 이벤트)에 대한 시스템 로그 메시지 전송 정보, 2755 페이지 및 하위 항목의 주제를 참조하십시오.
eStreamer	6.3	eStreamer 콘텐츠를 Host Identity Sources(호스트 ID 소스) 챕터에서 이 챕터로 옮기고, eStreamer와 시스템 로그를 비교한 요약을 추가했습니다.

XXIV 부

워크플로

- 워크플로, 2781 페이지
- 이벤트 검색, 2825 페이지
- 사용자 지정 워크플로, 2837 페이지
- 사용자 지정 표, 2845 페이지

116 장

워크플로

다음 주제에서는 워크플로를 사용하는 방법을 설명합니다.

- 개요: 워크플로, 2781 페이지
- 사전 정의 워크플로, 2782 페이지
- 맞춤형 테이블 워크플로, 2792 페이지
- 워크플로 사용, 2793 페이지
- 북마크, 2822 페이지
- 워크플로우 히스토리, 2823 페이지

개요: 워크플로

워크플로는 Firepower Management Center 웹 인터페이스에 있는 일련의 맞춤 데이터 페이지이며, 분석가는 시스템에서 생성된 이벤트를 평가하는 데 이를 사용할 수 있습니다.

다음 워크플로 유형은 Firepower Management Center에서 사용할 수 있습니다.

사전 정의 워크플로

시스템으로 전달한 미리 설정된 워크플로입니다. 사전 정의한 워크플로는 편집하거나 삭제할 수 없습니다. 하지만 사전 정의한 워크플로를 복사하고 맞춤형 워크플로의 기반으로 사용하는 것은 가능합니다.

저장된 맞춤형 워크플로

Firepower Management Center(으)로 전달한 저장된 맞춤형 테이블을 기반으로 하는 맞춤형 워크플로입니다. 이러한 워크플로는 편집, 삭제, 복사할 수 있습니다.

사용자 지정 워크플로

생성하고 필요에 맞게 맞춤형한 워크플로 또는 맞춤형 테이블을 생성할 때 시스템이 자동으로 생성한 워크플로입니다. 이러한 워크플로는 편집, 삭제, 복사할 수 있습니다.

많은 경우 워크플로에 표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다.

사전 정의 워크플로

다음 섹션에서 설명하는 사전 정의된 워크플로는 시스템을 통해 전달됩니다. 사전 정의된 워크플로는 편집하거나 삭제할 수 없지만, 사전 정의한 워크플로를 복사하고 맞춤형 워크플로의 기반으로 사용하는 것은 가능합니다.

사전 정의 침입 이벤트 워크플로

다음 표에서는 Firepower System에 포함된 사전 정의 침입 이벤트 워크플로에 대해 설명합니다.

표 ***281:*** 사전 정의 침입 이벤트 워크플로

워크플로 이름	설명
대상 포트	대상 포트가 대개 애플리케이션과 연결되므로, 이 워크플로는 알림의 양이 비정상적으로 많은 애플리케이션을 탐지하는 데 사용할 수 있습니다. Destination Port(대상 포트) 열은 네트워크에 있어서는 안 될 애플리케이션을 식별하는 데에도 도움이 됩니다.
이벤트 관련	이 워크플로는 두 가지의 유용한 기능을 제공합니다. 자주 발생하는 이벤트는 다음을 의미할 수 있습니다. • 오탐 • 웜 • 잘못 구성된 네트워크 드물게 발생하는 이벤트는 표적 공격의 증거일 가능성이 높으므로 각별한 주의가 필요합니다.
우선순위 및 분류별 이벤트	이 워크플로는 이벤트와 그 유형을 이벤트 우선순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다.
대상에 대한 이벤트	이 워크플로는 어떤 호스트 IP 주소가 공격받고 있으며 공격의 특성이 어떠한지 총괄적으로 보여줍니다. 가능한 경우 공격 관련 국가에 대한 정보도 볼 수 있습니다.
IP 관련	이 워크플로에서는 어떤 호스트 IP 주소가 가장 많은 알림을 생성하는지를 보여줍니다. 이벤트 수가 가장 많은 호스트는 일반에게 공개되는 수신 웜 유형 트래픽이거나(튜닝을 위한 조사 대상으로 적합), 알림의 원인을 확인하기 위해 추가 조사가 필요한 곳입니다. 카운트가 가장 낮은 호스트 역시 조사가 필요한데, 표적 공격의 주체일 가능성이 있습니다. 카운트가 낮으면 네트워크에 속하지 않는 호스트일 수도 있습니다.

워크플로 이름	설명
영향 및 우선순위	이 워크플로에서는 영향이 큰 반복적 이벤트를 신속하게 찾을 수 있습니다. 보고된 영향 레벨은 이벤트가 발생한 횟수와 함께 표시됩니다. 이 정보를 사용 하면 가장 자주 재발 하는 영향력이 큰 이벤트를 식별 하 여 네트워크에 대 한 광범위 한 공격의 지표가 될 수 있습니다.
영향 및 소스	이 워크플로는 진행 중인 공격의 출처를 파악하는 데 도움이 될 수 있습니다. 보고된 영향 레벨은 이벤트의 소스 IP 주소와 함께 표시됩니다. 예를 들어 영향 레벨이 1인 이벤트가 동일한 IP 주소에서 반복적으로 발생하는 경우, 공격자가 취약한 시스템을 찾아내 표적으로 삼고 있음을 의미할 수 있습니다.
대상에 대한 영향	이 워크플로를 통해 취약한 컴퓨터에서 반복적으로 발생하는 이벤트를 식별할 수 있어 시스템의 취약성을 해결하고 진행 중인 공격이 있을 경우 공격을 중지시킬 수 있습니다.
소스 포트	이 워크플로는 어떤 서버에서 가장 많은 알림을 생성하는지 나타냅니다. 튜닝이 필요한 영역을 식별하고 주의가 필요한 서버를 확인하는 데 이 정보를 사용할 수 있습니다.
소스 및 대상	이 워크플로는 높은 수준의 알림을 공유하는 호스트 IP 주소를 식별합니다. 목록 맨 위의 쌍은 오탐일 가능성이 있으며, 따라서 튜닝이 필요한 영역을 나타내는 것일 수도 있습니다. 목록 맨 아래의 쌍은 표적 공격, 권한이 없는 리소스에 액세스하는 사용자, 네트워크에 속하지 않는 호스트인지의 여부에 대해 조사할 수 있습니다.

사전 정의 악성코드 워크플로

다음 표에서는 Firepower Management Center에 포함된 사전 정의 악성코드 워크플로에 대해 설명합니다. 모든 사전 정의 악성코드 워크플로에서는 악성코드 이벤트의 테이블 보기를 사용합니다.

표 ***282:*** 사전 정의 악성코드 워크플로

워크플로 이름	설명
악성코드 요약	이 워크플로는 네트워크 트래픽에서 또는 엔드포인트 기반 AMP for Endpoints Connector에 의해 탐지된 악성코드를 개별 위협을 기준으로 그룹화한 목록을 제공합니다.
악성코드 이벤트 요약	이 워크플로에서는 다양한 악성 코드 이벤트 유형 및 하위 유형을 신속하게 분석할 수 있습니다.

워크플로 이름	설명
악성코드를 수신하는 호스트 수	이 워크플로는 악성코드를 수신한 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
악성코드를 송신하는 호스트 수	이 워크플로는 악성코드를 전송한 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
Applications Introducing Malware	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 파일 워크플로

다음 표에서는 Firepower Management Center에 포함된 사전 정의 파일 이벤트 워크플로에 대해 설명합니다. 모든 사전 정의 파일 이벤트 워크플로에서는 파일 이벤트의 테이블 보기를 사용합니다.

표 ***283:*** 사전 정의 파일 워크플로

워크플로 이름	설명
파일 요약	이 워크플로에서는 다양한 파일 이벤트 카테고리와 유형을 신속하게 분석할 수 있으며, 관련 악성코드 성향도 표시합니다.
파일을 수신하는 호스트 수	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.
파일을 송신하는 호스트 수	이 워크플로는 파일을 전송한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 캡처 파일 워크플로

다음 표에서는 Firepower Management Center에 포함된 사전 정의 캡처 파일 워크플로에 대해 설명합니다. 모든 사전 정의 캡처 파일 워크플로에서는 캡처 파일의 테이블 보기를 사용합니다.

표 ***284:*** 사전 정의 캡처 파일 워크플로

워크플로 이름	설명
캡처된 파일 요약	이 워크플로에서는 유형, 카테고리, 위협 점수를 기준으로 캡처 파일을 분석할 수 있습니다.
동적 분석 상태	이 워크플로에서는 캡처 파일이 동적 분석을 위해 제출되었는지 여부에 따라 그 카운트를 제공합니다.

사전 정의 연결 데이터 워크플로

다음 표에서는 Firepower Management Center에 포함된 사전 정의 연결 데이터 워크플로에 대해 설명합니다. 모든 사전 정의 연결 데이터 워크플로에서 연결 데이터의 테이블 보기를 사용합니다.

표 ***285:*** 사전 정의 연결 데이터 워크플로

워크플로 이름	설명
연결 이벤트	이 워크플로에서는 기본 연결 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 테이블 보기로 드릴다운할 수 있습니다.
애플리케이션별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다.
이니시에이터를 이용한 연결	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트가 연결 트랜잭션을 시작한 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
포트별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.
응답자별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트 IP 주소가 연결 트랜잭션의 응답자인 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
시간에 따른 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 연결 수를 그래프로 나타냅니다.

워크플로 이름	설명
애플리케이션별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다. 애플리케이션 카운트는 애플리케이션 연결과 일치하는 각 탐지기를 반영합니다. 트래픽과 일치하는 것이 애플리케이션 프로토콜, 웹 애플리케이션, 클라이언트 탐지기, 내부 탐지기 중 무엇인지에 따라, 그리고 트래픽이 모바일 디바이스에서 발생했는지 암호화된 세션의 일부인지에 따라 같은 애플리케이션 세션이 목록에서 여러번 나타날 수도 있습니다. 클라이언트 플로우에 애플리케이션이 표시되며 특별한 클라이언트 탐지기가 존재하지 않는다면, 일반 클라이언트가 보고될 수 있습니다. 예를 들어 (YouTube 웹 애플리케이션 탐지기와 일치하기 때문에) **YouTube**로 보고되거나, (내부 YouTube 탐지기가 클라이언트 세션에서 일반적으로 표시되는 특성과 일치하기 때문에) **YouTube** 클라이언트로 보고된 YouTube 트래픽과 같은 세션이 표시될 수 있습니다. 네트워크의 연결 이벤트와 네트워크 맵에 있는 정보를 사용하여 특정 애플리케이션 연결에 대한 추가 정보를 확인합니다.
이니시에이터별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소로부터 전송된 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
포트별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.
응답자별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 수신한 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
시간에 따른 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 전송 킬로바이트 수를 그래프로 나타냅니다.
응답자별 고유 이니시에이터	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소에 연결한 고유 initiator 수를 기준으로 가장 활동적인 10개의 응답 호스트 IP 주소를 그래프로 나타냅니다.
이니시에이터별 고유 응답자	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 연결한 고유 responder 수를 기준으로 가장 활동적인 10개의 발신 호스트 IP 주소를 그래프로 나타냅니다.

사전 정의 보안 인텔리전스 워크플로

다음 표에서는 Firepower Management Center에 포함된 사전 정의 보안 인텔리전스 워크플로에 대해 설명합니다. 모든 사전 정의 보안 인텔리전스 워크플로에서는 보안 인텔리전스 이벤트의 테이블 보기를 사용합니다.

표 ***286:*** 사전 정의 보안 인텔리전스 워크플로

워크플로 이름	설명
보안 인텔리전스 이벤트	이 워크플로에서는 기본 보안 인텔리전스 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 테이블 보기로 드릴다운할 수 있습니다.
보안 인텔리전스 요약	이 워크플로는 Security Intelligence Events(보안 인텔리전스 이벤트) 워크플로와 동일하지만 보안 인텔리전스 이벤트를 카테고리 및 카운트별로만 나열하는 Security Intelligence Summary(보안 인텔리전스 요약) 페이지로 시작합니다.
DNS 상세정보가 있는 보안 인텔리전스	이 워크플로는 Security Intelligence Events(보안 인텔리전스 이벤트) 워크플로와 동일하지만 Security Intelligence(보안 인텔리전스) 이벤트를 카테고리 및 DNS 관련 특성별로만 나열하는 Security Intelligence with DNS Details(DNS 상세정보가 있는 보안 인텔리전스) 페이지로 시작합니다.

사전 정의 호스트 워크플로

다음 표에서는 호스트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***287:*** 사전 정의 호스트 워크플로

워크플로 이름	설명
호스트	이 워크플로에서는 호스트의 테이블 보기에 이어 호스트 보기가 표시됩니다. 호스트 테이블 기반의 워크플로 보기에서는 어떤 호스트와 관련된 모든 IP 주소의 데이터를 편리하게 볼 수 있습니다.
운영 체제 요약	이 워크플로를 사용하여 네트워크에서 사용 중인 운영체제를 분석할 수 있습니다.

사전 정의 보안 침해 지표 워크플로

다음 표에서는 IOC 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***288:*** 사전 정의 보안 침해 지표 워크플로

워크플로 이름	설명
보안 침해 지표	이 워크플로는 IOC 데이터를 카운트 및 카테고리별로 그룹화한 요약 보기로 시작하며, 요약 데이터를 이벤트 유형별로 세분화하는 세부사항 보기를 제공합니다. **Analysis(**분석**) > Hosts(**호스트**)** 메뉴를 통해 이 워크플로에 액세스합니다.
호스트별 보안 침해 지표	이 워크플로를 사용하여 네트워크의 어떤 호스트가 공격받을 가능성이 가장 높은지 (IOC 데이터를 기반으로) 평가할 수 있습니다. **Analysis(**분석**) > Hosts(**호스트**)** 메뉴를 통해 이 워크플로에 액세스합니다.

사전 정의 애플리케이션 워크플로

다음 표에서는 애플리케이션 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***289:*** 사전 정의 애플리케이션 워크플로

워크플로 이름	설명
애플리케이션 비즈니스 관련성	이 워크플로를 사용하여 네트워크의 예상 비즈니스 타당성 레벨별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다.
애플리케이션 범주	이 워크플로를 사용하여 네트워크에서 카테고리(예: 이메일, 검색 엔진, 소셜 네트워킹)별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다.
애플리케이션 위험성	이 워크플로를 사용하여 네트워크에서 각 예상 보안 위험 레벨의 실행 중인 애플리케이션을 분석함으로써 사용자 활동의 잠재적 리스크를 추정하고 적절한 조치를 취할 수 있습니다.
애플리케이션 요약	이 워크플로를 사용하여 네트워크의 애플리케이션 및 해당 호스트에 대한 세부 정보를 얻어 호스트 애플리케이션 활동을 면밀하게 조사할 수 있습니다.
애플리케이션	이 워크플로를 사용하여 네트워크에서 실행 중인 애플리케이션을 분석함으로써 네트워크가 어떻게 사용되고 있는가를 개괄적으로 파악할 수 있습니다.

사전 정의 애플리케이션 상세정보 워크플로

다음 표에서는 애플리케이션 상세정보 및 클라이언트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***290:*** 사전 정의 애플리케이션 상세정보 워크플로

워크플로 이름	설명
애플리케이션 세부사항	이 워크플로를 사용하여 네트워크의 클라이언트 애플리케이션을 더 자세히 분석할 수 있습니다. 그런 다음 클라이언트 애플리케이션의 테이블 보기와 호스트 보기로 이어집니다.
클라이언트	이 워크플로에서는 클라이언트 애플리케이션의 테이블 보기에 이어 호스트 보기가 표시됩니다.

사전 정의 서버 워크플로

다음 표에서는 서버 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***291:*** 사전 정의 서버 워크플로

워크플로 이름	설명
카운트별 네트워크 애플리케이션	이 워크플로를 사용하여 네트워크에서 가장 자주 사용되는 애플리케이션을 분석할 수 있습니다.
히트별 네트워크 애플리케이션	이 워크플로를 사용하여 네트워크에서 가장 활동적인 애플리케이션을 분석할 수 있습니다.
서버 세부 정보	이 워크플로를 사용하여 탐지된 서버 애플리케이션 프로토콜의 벤더 및 버전을 더 자세히 분석할 수 있습니다.
서버	이 워크플로에서는 애플리케이션의 테이블 보기에 이어 호스트 보기가 표시됩니다.

사전 정의 호스트 속성 워크플로

다음 표에서는 호스트 속성 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***292:*** 사전 정의 호스트 속성 워크플로

워크플로 이름	설명
특성	이 워크플로를 사용하여 네트워크에 있는 호스트의 IP 주소 및 호스트의 상태를 모니터링할 수 있습니다.

사전 정의 검색 이벤트 워크플로

다음 표에서는 검색 및 ID 데이터를 확인하는 데 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***293:*** 사전 정의 검색 이벤트 워크플로

워크플로 이름	설명
검색 이벤트	이 워크플로에서는 검색 이벤트의 세부 목록을 테이블 보기 형태로 제공하고 이어서 호스트 보기를 표시합니다.

사전 정의 사용자 워크플로

다음 표에서는 사용자 검색 및 사용자 ID 데이터를 확인하는 데 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***294:*** 사전 정의 사용자 워크플로

워크플로 이름	설명
활성 세션	이 워크플로는 사용자 ID 소스가 수집한 활성 세션 목록을 제공합니다.
사용자	이 워크플로는 사용자 ID 소스가 수집한 사용자 정보 목록을 제공합니다.

사전 정의 취약성 워크플로

다음 표에서는 Firepower Management Center에 포함된 사전 정의 취약성 워크플로에 대해 설명합니다.

표 ***295:*** 사전 정의 취약성 워크플로

워크플로 이름	설명
취약성	이 워크플로를 이용하면 네트워크에서 탐지된 호스트에 적용되는 활성 취약성만 표시하는 테이블 보기 등을 이용해, 데이터베이스에 있는 취약성을 검토할 수 있습니다. 또한 제약 조건에 부합하는 모든 취약성에 대해 자세히 설명하는 취약성 세부사항 보기도 제공합니다.

사전 정의 서드파티 취약성 워크플로

다음 표에서는 Firepower Management Center에 포함된 사전 정의 서드파티 취약성 워크플로에 대해 설명합니다.

표 ***296:*** 사전 정의 서드파티 취약성 워크플로

워크플로 이름	설명
IP 주소별 취약성	이 워크플로를 사용하여 모니터링되는 네트워크의 호스트 IP 주소별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다.
소스별 취약성	이 워크플로를 사용하여 서드파티 취약성 소스(예: QualysGuard Scanner)별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다.

사전 정의 상관관계 및 화이트 목록 워크플로

상관관계 데이터, 화이트 목록 이벤트, 화이트 목록 위반, 교정 상태 이벤트의 유형별로 사전 정의 워크플로가 있습니다.

표 ***297:*** 사전 정의 상관관계 워크플로

워크플로 이름	설명
Correlation Events	이 워크플로는 상관관계 이벤트의 테이블 보기로 구성됩니다.
화이트 이벤트 나열	이 워크플로는 화이트 목록 이벤트의 테이블 보기로 구성됩니다.
호스트 위반 카운트	이 워크플로는 하나 이상의 화이트 목록을 위반하는 모든 호스트 IP 주소를 나열하는 일련의 페이지로 구성됩니다.

워크플로 이름	설명
화이트 위반 목록	이 워크플로에는 모든 위반을 나열하는 화이트 목록 위반의 테이블 보기가 포함되는데, 가장 최근에 탐지된 위반이 맨 위에 옵니다. 테이블의 각 행에는 탐지된 위반 사항이 하나씩 포함되어 있습니다.
상태	이 워크플로는 교정 상태의 테이블 보기로 구성됩니다. 여기에는 위반한 정책의 이름, 적용된 교정의 이름과 상태가 포함됩니다.

사전 정의 시스템 워크플로

Firepower System에서는 몇 가지 추가 워크플로를 제공하는데, 여기에는 감사 이벤트 및 상태 이벤트와 같은 시스템 이벤트 뿐만 아니라 규칙 업데이트 가져오기 및 활성 검사의 결과를 나열하는 워크플로도 포함됩니다.

표 ***298:*** 추가 사전 정의 워크플로

워크플로 이름	설명
감사 로그	이 워크플로는 감사 이벤트를 나열하는 감사 로그의 테이블 보기로 구성됩니다.
Health Events	이 워크플로에서는 상태 모니터링 정책에 의해 트리거되는 이벤트를 표시합니다.
규칙 업데이트 가져오기 로그	이 워크플로는 성공한 규칙 업데이트 가져오기 및 실패한 규칙 업데이트 가져오기에 대한 정보를 나열하는 테이블 보기로 구성됩니다.
스캔 결과	이 워크플로는 완료된 각 스캔을 나열하는 테이블 보기로 구성됩니다.

맞춤형 테이블 워크플로

맞춤형 테이블 기능을 사용하여 이벤트 유형 2가지 이상의 데이터를 사용하는 테이블을 생성할 수 있습니다. 이를테면 침입 이벤트 데이터를 검색 데이터와 연계하여 중요 시스템에 영향을 주는 이벤트의 단순 검색을 지원하는 테이블과 워크플로를 만들 때 유용한 기능입니다.

맞춤형 테이블을 생성하는 경우, 시스템은 테이블과 관련된 이벤트를 볼 수 있는 워크플로를 자동으로 생성합니다. 워크플로의 기능은 사용하는 테이블 유형에 따라 달라집니다. 예를 들어 침입 이벤트 테이블을 기반으로 하는 맞춤형 테이블 워크플로는 항상 패킷 보기로 끝납니다. 그러나 검색 이벤트를 기반으로 하는 맞춤형 테이블 워크플로는 호스트 보기로 끝납니다.

사전 정의 이벤트 테이블 기반의 워크플로와 달리 맞춤형 테이블 기반의 워크플로는 다른 워크플로 유형에 대한 링크가 없습니다.

워크플로 사용

프로시저

단계 **1** 워크플로 선택, 2795 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택합니다.

단계 **2** 현재 워크플로 내에서 이동:

- 선택한 이벤트 데이터 유형에서 사용 가능한 행을 모두 보려면 테이블 보기 페이지를 사용하십시오(테이블 보기 페이지 사용, 2802 페이지 참조).
- 선택한 이벤트 데이터 유형에서 사용 가능한 행의 하위 집합을 보려면 드릴다운 페이지를 사용하십시오(드릴다운 페이지 사용, 2801 페이지 참조).
- 워크플로우의 다음 페이지에 해당 행을 표시하려면 아래쪽 화살표( )을 클릭합니다.
- 여러 페이지가 있는 워크플로의 페이지 사이를 이동하려면 각 페이지 하단에 있는 툴을 사용하십시오(워크플로 페이지 이동 툴, 2798 페이지 참조).
- 다른 유형의 워크플로에 적용된 같은 제약을 보려는 경우, **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.

단계 **3** 현재 워크플로의 표시 화면을 수정합니다.

- 페이지에서 하나 이상의 열 옆에 있는 체크 박스를 선택해 영향받는 열을 표시하고, 페이지 하단의 버튼 중 하나(예: **View(**보기**)**)를 클릭해 선택한 열 전체에 작업을 수행합니다.
- 열 상단에 있는 체크 박스를 선택해 페이지의 모든 열을 선택하고, 페이지 하단의 버튼 중 하나(예: **View(**보기**)**)를 클릭해 페이지의 열 전체에 작업을 수행합니다.
- 표시하지 않을 컬럼 헤드의 닫기( )을 클릭하여 화면에 표시되는 열을 제한합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 선택한 필드의 선택된 값을 이용해 데이터 보기를 제한합니다. 자세한 내용은 이벤트 보기 제약 조건, 2818 페이지 및 복합 이벤트 보기 제약, 2820 페이지 섹션을 참고하십시오.
- 이벤트 보기의 시간 제약을 변경합니다. 페이지의 오른쪽 위에 있는 날짜 범위는 워크플로에 포함할 이벤트의 시간 범위를 설정합니다. 자세한 내용은 이벤트 시간 제약 조건, 2811 페이지 섹션을 참조하십시오.

참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 열을 기준으로 데이터를 정렬하려면 열의 이름을 클릭합니다. 정렬 순서를 반대로 하려면 열 이름을 다시 클릭합니다. 방향 아이콘은 데이터가 정렬되는 열과 정렬이 오름차순인지 내림차순인지를 표시합니다.
- 워크플로 페이지 링크를 클릭하여 활성 제약 조건을 사용해 해당 페이지를 표시합니다. 사전 정의된 워크플로 테이블 보기 및 드릴다운 페이지의 왼쪽 위에서 이벤트 위, 워크플로 이름 아래에 워크플로 페이지 링크가 나타납니다.

단계 **4** 현재 워크플로 내의 추가 데이터를 확인합니다.

- 파일의 경로 맵을 새 창에서 보려면, 파일 이름과 SHA-256 해시 값 열에서 네트워크 파일 경로를 클릭합니다. 아이콘은 파일 상태에 따라 달라집니다(파일 경로 아이콘, 2799 페이지 참조).
- IP 주소와 관련된 호스트 프로파일의 팝업 윈도우를 표시하려는 경우, 아무 IP 주소 열의 호스트 프로파일을 클릭합니다. 아이콘은 파일 상태에 따라 달라집니다(호스트 프로파일 아이콘, 2799 페이지 참조).
- 파일의 최고 위협 점수에 대한 Dynamic Analysis Summary(동적 분석 요약) 보고서를 보려는 경우, 위협 점수 열에 나타나는 위협 점수를 클릭합니다. 아이콘은 파일의 최고 위협 점수에 따라 달라집니다(위협 점수 아이콘, 2800 페이지 참조).
- 사용자 프로파일 정보를 보려는 경우에는 아무 사용자 ID 열의 사용자 또는 보안 침해 지표와 관련된 사용자의 경우에는 빨간색 사용자를 클릭합니다. 해당 사용자가 데이터베이스에 존재할 수 없다면(즉 AMP for Endpoints Connector 사용자려면) 사용자 아이콘은 흐리게 표시됩니다.
- 서드파티 취약성의 취약성 상세정보를 보려는 경우네는 아무 서드파티 취약성 ID 열의 취약성을 클릭합니다.
- 집계된 데이터 포인트를 볼 때 마우스 포인터를 플래그 위에 올리면 국가 이름을 볼 수 있습니다.
- 개별 데이터 포인트를 볼 때 플래그를 클릭하면 지리위치, 2802 페이지에서 설명하는 추가 지리위치 상세정보를 볼 수 있습니다.

단계 **5** 다른 워크플로로 이동합니다.

다른 워크플로를 이용하는 같은 이벤트 유형을 보려는 경우, 워크플로 제목 옆에 있는 **(switch workflow)**을 클릭하고 사용할 워크플로를 선택합니다. 스캔 결과에 대해 다른 워크플로를 사용할 수는 없습니다.

사용자 역할별 워크플로 액세스

워크플로에 대한 액세스는 사용자의 역할에 따라 결정됩니다. 자세한 내용은 아래 표를 참고하십시오.

사용자 역할	액세스 가능한 워크플로
관리자	어떤 워크플로에도 액세스할 수 있으며, 감사 로그, 검사 결과, 규칙 업데이트 가져오기 로그에 액세스할 수 있는 유일한 사용자입니다.
유지 보수 사용자	상태 이벤트에 액세스할 수 있습니다.
Security Analyst 및 Security Analyst(읽기 전용)	침입, 악성코드, 파일, 연결, 검색, 취약성, 상관관계, 상태 워크플로에 액세스할 수 있습니다.

워크플로 선택

Firepower System에서는 다음 표에 나열된 데이터 유형에 대해 사전 정의된 워크플로를 제공합니다.

표 ***299:*** 워크플로를 사용하는 기능

기능	메뉴 경로	옵션
침입 이벤트	분석 > 침입	이벤트 검사된 이벤트 클립보드 인시던트
악성코드 이벤트	분석 > 파일	악성코드 이벤트
파일 이벤트	분석 > 파일	파일 이벤트
캡처된 파일	분석 > 파일	캡처된 파일
연결 이벤트	분석 > 연결	이벤트
보안 인텔리전스 이벤트	분석 > 연결	보안 인텔리전스 이벤트

기능	메뉴 경로	옵션
호스트 이벤트	분석 > 호스트	네트워크 맵 호스트 보안 침해 지표 애플리케이션 애플리케이션 세부사항 서버 호스트 속성 검색 이벤트
사용자 이벤트	분석 > 사용자	활성 세션 사용자의 활동 사용자
취약성 이벤트	분석 > 호스트	취약성 서드파티 취약성
상관관계 이벤트	분석 > 상관관계	상관관계 이벤트 화이트 이벤트 나열 화이트 위반 목록 상태
감사 이벤트	시스템 > 모니터링	감사
상태 이벤트	System(시스템) > Health(상태) > Events(이벤트)	해당 없음
규칙 업데이트 가져오기 로그	시스템 > 업데이트	해당 없음
스캔 결과	정책 > 작업 > 스캐너	해당 없음

위 표에 있는 데이터 유형을 표시할 경우 그 데이터의 기본 워크플로 중 첫 페이지에 이벤트가 나타납니다. 이벤트 보기 설정을 구성하여 다른 기본 워크플로를 지정할 수 있습니다. 워크플로 액세스는 사용자 역할에 따라 달라집니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

관련 항목

이벤트 보기 구성, 41 페이지

워크플로 페이지

각 워크플로 유형의 데이터는 저마다 다르지만, 모든 워크플로가 공유하는 공통 기능이 있습니다. 워크플로는 페이지의 여러 유형을 포함할 수 있습니다. 워크플로 페이지에서 수행할 수 있는 작업은 페이지 유형에 따라 달라집니다.

워크플로의 드릴다운 및 테이블 보기 페이지를 통해 신속하게 데이터 보기의 범위를 한정하여 분석에 중요한 이벤트에 초점을 맞출 수 있습니다. 테이블 보기 페이지 및 드릴다운 페이지는 표시할 이벤트 집합을 제한하거나 워크플로를 이동하는 데 사용할 수 있는 여러 기능을 지원합니다. 워크플로의 드릴다운 페이지나 테이블 보기에서 데이터를 볼 때, 사용 가능한 아무 열을 기준으로 데이터를 오름차순이나 내림차순으로 정렬할 수 있습니다. 데이터베이스가 단일 워크플로 페이지에 표시할 수 있는 것보다 많은 이벤트를 포함할 경우, 페이지 맨 아래의 링크를 클릭하여 추가 이벤트를 표시할 수 있습니다. 이 링크 중 하나를 클릭할 때 동일한 이벤트가 두 번 표시되지 않도록 시장 창이 자동으로 일시 중지합니다. 언제라도 타임 윈도우의 일시 중지를 취소할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

테이블 보기

페이지가 기본적으로 활성화되는 경우, 테이블 보기에는 워크플로가 기반으로 하는 데이터베이스의 각 필드에 대한 열이 포함됩니다.

최상의 성능을 위해 필요한 열만 표시합니다. 열이 많이 표시될수록 데이터를 표시하는 데 더 많은 리소스가 필요합니다.

테이블 보기에서 어떤 열을 비활성화할 경우 그 열을 비활성화함으로써 둘 이상의 동일한 행이 생성되고 6개 미만의 열이 표시된다면(Count 열 제외) Firepower System에서는 이벤트 보기에 Count 열을 추가합니다.

테이블 보기 페이지에서 어떤 값을 클릭하면 그 값으로 제한할 수 있습니다.

맞춤형 워크플로를 생성할 때 **Add Table View(**테이블 보기 추가**)**를 클릭하여 여기에 테이블 보기를 추가합니다.

드릴다운 페이지

일반적으로 드릴다운 페이지는 보기 페이지로 이동하기 전에 조사 범위를 몇몇 이벤트로 한정하는 데 사용하는 중간 단계의 페이지입니다. 드릴다운 페이지는 데이터베이스에서 제공하는 열의 일부를 포함합니다.

예를 들어 검색 이벤트의 드릴다운 페이지에 IP Address, MAC Address, Time 열만 포함될 수 있습니다. 한편 침입 이벤트의 드릴다운 페이지는 Priority, Impact Flag, Inline Result, Message 열이 포함될 수 있습니다.

드릴다운 페이지에서는 표시하는 이벤트의 범위를 좁히고 워크플로에서 다음으로 진행할 수 있습니다. 이를테면 드릴다운 페이지에서 어떤 값을 클릭할 경우 그 값을 기준으로 제한하고 워크플로의 다음 페이지로 이동함으로써, 선택한 값과 매칭하는 이벤트에 더 초점을 맞출 수 있습니다. 드릴다운 페이지에서 어떤 값을 클릭하더라도 그 값이 있는 열이 비활성화되지 않습니다. 진행할 페이지가 테이블 보기인 경우도 마찬가지입니다. 사전 정의 워크플로의 드릴다운 페이지에는 항상 Count 열이 있

습니다. 맞춤형 워크플로를 생성할 때 **Add Page(**페이지 추가**)**를 클릭하여 드릴다운 페이지를 추가합니다.

Graphs(그래프**)**

연결 데이터 기반의 워크플로는 연결 그래프라고도 하는 그래프 페이지를 포함할 수 있습니다.

예를 들어 연결 그래프에서 시간의 경과에 따른 탐지된 연결 수를 나타내는 선 그래프가 표시될 수 있습니다. 일반적으로 연결 그래프는 드릴다운 페이지처럼 조사 범위를 한정하는 데 사용하는 중간 단계의 페이지입니다.

최종 페이지

워크플로의 최종 페이지는 워크플로의 기반이 되는 이벤트의 유형에 따라 달라집니다.

- 호스트 보기는 애플리케이션, 애플리케이션 상세정보, 검색 이벤트, 호스트, 보안 침해 지표(IOC), 서버, 화이트 목록 위반, 호스트 속성 또는 서드파티 취약성을 기반으로 하는 워크플로의 최종 페이지입니다. 이 페이지에서 호스트 프로파일을 보면서 다중 주소를 갖는 호스트의 모든 IP 주소에 대한 데이터를 편리하게 볼 수 있습니다.
- 사용자 상세정보 보기는 사용자 및 사용자 활동를 기반으로 하는 워크플로의 최종 페이지입니다.
- 취약성 상세정보 보기는 Cisco 취약성을 기반으로 하는 워크플로의 최종 페이지입니다.
- 패킷 보기는 침입 이벤트를 기반으로 하는 워크플로의 최종 페이지입니다.

다른 종류의 이벤트(예: 감사 로그 이벤트, 악성코드 이벤트)를 기반으로 하는 워크플로는 최종 페이지가 없습니다.

워크플로의 마지막 페이지에서 세부사항 섹션을 확장하여 초점 대상인 집합의 각 개체에 대해 워크플로의 진행에 따른 구체적인 정보를 볼 수 있습니다. 웹 인터페이스에서는 워크플로의 최종 페이지에 제약 조건을 나열하지 않지만, 이미 설정된 제약 조건이 유지되어 데이터 집합에 적용됩니다.

워크플로 페이지 탐색 툴

워크플로 페이지는 각 페이지를 손쉽게 탐색하고 이벤트 분석 동안 표시할 정보를 선택하는 데 도움이 되는 시각적 단서를 제공합니다.

워크플로 페이지 이동 툴

워크플로에 여러 페이지의 데이터가 있는 경우, 각 페이지 하단에 워크플로의 페이지 숫자가 표시되며, 아래 표에 나열된 툴을 이용해 페이지를 이동할 수 있습니다.

표 ***300:*** 워크플로 페이지 이동 툴

페이지 이동 툴	조치
페이지 번호 (다른 페이지를 보려는 경우 확인할 페이지 번호를 입력하고 Enter를 누릅니다.)	다른 페이지 보기
>	다음 페이지 보기
<	이전 페이지 보기
>|	마지막 페이지로 바로 이동
|<	첫 페이지로 바로 이동

파일 경로 아이콘

워크플로 페이지에서 파일의 경로 맵을 새 창에서 볼 수 있다면, 네트워크 경로 아이콘이 표시됩니다. 이 아이콘은 파일 상태에 따라 달라집니다.

표 ***301:*** 파일 경로 아이콘

파일 경로 아이콘	파일 상태
정상	정상
악성코드	악성코드
맞춤형 탐지	맞춤형 탐지
알 수 없음	알 수 없음
사용 불가능	사용 불가능

호스트 프로파일 아이콘

워크플로 페이지에서 IP 주소와 연결된 호스트 프로파일을 팝업 윈도우에서 볼 수 있다면, 호스트 프로파일 아이콘이 표시됩니다. 호스트 프로파일 아이콘이 흐리게 표시될 경우 호스트가 네트워크 맵에 포함될 수 없으므로(예: `0.0.0.0`) 호스트 프로파일을 볼 수 없습니다. 이 아이콘은 호스트의 상태에 따라 다르게 표시됩니다.

표 ***302:*** 호스트 프로파일 아이콘

호스트 프로파일 아이콘	**Host Status(**호스트 상태**)**
	호스트가 침해 가능성 있음으로 태그되지 않았습니다.

호스트 프로파일 아이콘	**Host Status**(호스트 상태)
	호스트가 트리거된 보안 침해 지표(IOC) 규칙에 의해 침해 가능성 있음으로 태그되었습니다.
	차단 목록에 추가됨(보안 인텔리전스 데이터를 바탕으로 트래픽 필터링을 수행하는 경우에만 표시됩니다.)
	차단 목록에 추가됨, 모니터링하도록 설정(보안 인텔리전스 데이터를 바탕으로 트래픽 필터링을 수행하는 경우에만 표시됩니다.)

위협 점수 아이콘

워크플로 페이지를 제공 하는 경우 가장 높은 위협 점수에 대 한 동적 분석 요약 보고서를 볼 수 있는 기회와 연결 파일을 위협 점수 아이콘 위에 표시 됩니다. 아이콘은 파일의 최고 위협 점수에 따라 다릅니다.

표 ***303:*** 위협 점수 아이콘

위협 점수 아이콘	위협 점수 레벨
낮음	낮음
보통	보통
높음	높음
매우 높음	매우 높음

워크플로 툴바

워크플로의 각 페이지에는 관련 기능에 빠르게 액세스할 수 있는 툴바가 있습니다. 다음 표에서는 툴바의 각 링크에 대해 설명합니다.

표 ***304:*** 워크플로 툴바 링크

기능	설명
이 페이지를 즐겨찾기에 추가	현재 페이지에 북마크를 지정하여 나중에 다시 돌아올 수 있게 합니다. 북마크는 현재 보고 있는 페이지에 적용된 제약 조건을 캡처하므로 나중에 (데이터가 그대로 있을 경우) 동일한 데이터로 돌아올 수 있습니다.
보고서 디자이너	현재 제약 조건이 적용된 워크플로를 선택 기준으로 하는 보고서 디자인 도구를 엽니다.

기능	설명
대시보드	현재 워크플로와 관련된 대시보드를 엽니다. 예를 들어 Connection Events(연결 이벤트) 워크플로는 Connection Summary(연결 요약) 대시보드와 연결됩니다.
즐겨찾기 보기	선택 가능한 저장된 즐겨찾기의 목록을 표시합니다.
검색	워크플로의 데이터에 대한 고급 검색을 수행할 수 있는 Search(검색) 페이지를 표시합니다. 아래쪽 화살표 아이콘을 클릭하여 저장된 검색을 선택하고 사용할 수도 있습니다.

관련 항목

이벤트 보기에서 보고서 템플릿 생성, 2657 페이지
대시보드 정보, 363 페이지
이벤트 검색, 2825 페이지
북마크, 2822 페이지
즐겨찾기 생성, 2822 페이지
즐겨찾기 보기, 2823 페이지

드릴다운 페이지 사용

프로시저

단계 **1** 워크플로를 사용하는 기능에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 모든 워크플로에는 다음 옵션이 있습니다.

- 특정 값으로 제한하여 다음 워크플로 페이지로 드릴다운하려면 행 내의 값을 클릭합니다. 이 방법은 드릴다운 페이지에만 적용됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한될 뿐이고 다음 페이지로 드릴다운되지 않습니다.
- 일부 이벤트로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 이벤트의 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다.
- 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All(**모두 보기**)**을 클릭합니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

테이블 보기 페이지 사용

테이블 보기 페이지는 드릴다운, 호스트 보기, 패킷 보기 또는 취약성 세부사항 페이지에 없는 기능을 제공합니다. 이러한 기능은 아래 설명대로 사용하십시오.

프로시저

단계 **1** 워크플로 선택, 2795 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 워크플로 이름 아래에 표시된 워크플로 경로에서 테이블 보기를 선택합니다.

단계 **3** 필요에 따라 아래 나열된 기능을 사용하여 테이블 보기를 정렬하고 내부를 이동합니다.

- 비활성화된 열의 목록을 표시하려면 Search Constraints(검색 제약 조건) 확장 화살표( )를 클릭합니다.
- 비활성화된 열의 목록을 숨기려면 Search Constraints(검색 제약 조건) 축소 화살표( )를 클릭합니다.
- 비활성화된 열을 이벤트 보기에 다시 추가하려면 Search Constraints(검색 제약 조건) 확장 화살표( )를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.
- 열을 표시하거나 숨기려면(비활성화하려면) 아무 열 이름 옆에 있는 지우기( )를 클릭합니다. 표시되는 팝업 윈도우에서 적절한 체크 박스를 선택하거나 선택 취소해 표시할 열을 나타낸 다음, **Apply(**적용**)**를 클릭합니다.

지리위치

지리위치 기능은 라우팅 가능한 IP 주소(국가, 대륙 등)의 지리위치적 소스에 대한 데이터를 제공합니다. 이 정보는 이벤트, 자산 프로파일, Context Explorer(상황 탐색기), 대시보드 및 기타 분석 툴에서 사용할 수 있습니다.

참고 한 국가에서 다른 국가로 이동하는 모바일 디바이스 및 다른 탐지된 호스트의 경우, 시스템은 특정 국가 대신 대륙을 보고하기도 합니다.

지리위치 데이터를 사용하여 네트워크 트래픽을 필터링할 수 있습니다. 예를 들어 연결이 해당 조직과 연결되지 않은 국가에서 시작하거나 종료하는지 여부를 확인할 수 있습니다. 인라인 구축의 경우에는 이러한 연결을 차단하거나 속도를 제한할 수 있습니다.

시스템은 지리위치 데이터를 자체 지리위치 데이터베이스(GeoDB)에 저장합니다. Cisco는 GeoDB에 주기적인 업데이트를 제공합니다. About(정보) 페이지(**Help** > **About**)에서 현재 GeoDB 업데이트 버전을 확인할 수 있습니다.

GeoDB 업데이트를 수락하면, Firepower Management Center에서 작은 국기 아이콘과 ISO 국가 번호를 클릭하여 특정 IP 주소 관련 지리위치 상세정보를 얻을 수 있습니다(지리위치 상세정보, 2803 페이지 참조). 서드파티 지도 툴을 사용하여, 탐지된 위치를 정확히 표시할 수도 있습니다. GeoDB를 업데이트하지 않으면 이러한 상세정보는 사용할 수 없습니다.

Connection Summary(연결 요약) 대시보드 등에서는 종합 지리위치 정보에 대한 상세정보를 볼 수 없습니다.

관련 항목

네트워크 조건, 530 페이지
지리위치 개체, 576 페이지
상관관계 정책 및 규칙 소개, 2583 페이지
트래픽 프로파일 조건, 2625 페이지
GeoDB(지리위치 데이터베이스) 업데이트, 183 페이지

지리위치 상세정보

가용성에 따라 다수의 필드가 Geolocation Details(지리위치 상세정보) 페이지에 표시될 수 있습니다. 다음 표에서는 이러한 필드에 대해 설명합니다. (정보가 없는 필드는 표시되지 않습니다.)

표 ***305: Geolocation Details(지리위치 상세정보) 필드***

필드	목차
Country	호스트의 IP 주소와 관련된 국가이며 국기가 함께 나타납니다. 대륙은 괄호 안에 표시됩니다. 예: `United States (North America)`, `Equatorial Guinea (Africa)`
지역	호스트가 위치한 국가의 주, 시/도, 기타 지역입니다. 예: `VA`, `35`
도시	호스트가 위치한 도시입니다. 예: `Seattle`, `Fukuoka`
Postal Code(우편번호)	호스트가 위치한 지역의 우편 번호입니다. 예: `361000`, `90210`
위도/경도	호스트 위치의 정확한 좌표입니다. 예: `40.0375, -76.1053`; `53.4050, -0.5484`
지도	외부 지도 사이트(Google Maps, Yahoo Maps, Bing Maps, OpenStreetMap)로 가는 링크입니다. 링크를 클릭하면 호스트의 대략적인 위치에 대한 콘텍스트 지도가 표시됩니다.
Timezone표준 시간대	호스트 위치의 시간대로, Daylight Savings Time(일광 절약 시간)이 표시되어 있습니다. 예: `GMT+8:00`, `GMT-4:00 (In DST)`

필드	목차
ASN	호스트의 IP 주소와 관련된 ASN 및 해당 ASN에 대한 추가 정보입니다. 예: `14618 (Amazon.com Inc.)`; `4837 (Cncgroup China169 Backbone)`
ISP	호스트의 IP 주소와 관련된 ISP입니다. 예: `Atlantic Broadband`; `China Unicom Ip Network`
집/직장	호스트의 연결이 `Home(집)` 또는 `Business(비즈니스)` 용도인지를 나타냅니다.
조직	호스트의 IP 주소와 관련된 조직입니다. 예: `Amazon.com`, `Bank of America`
도메인 이름	호스트의 IP 주소와 관련된 도메인 이름입니다. 예: `amazonaws.com`, `xmcnc.net`
연결 유형	호스트의 IP 주소와 관련된 연결 유형입니다. 예: `Broadband`, `DSL`
프록시 유형	사용된 프록시의 유형입니다. 예: `Anonymous`, `Corporate`

연결 이벤트 그래프

표 드릴다운 페이지와 이벤트의 최종 테이블 보기를 사용하는 워크플로 외에도, 시스템은 5분 간격으로 집계한 데이터를 이용해 특정 연결 데이터를 그래픽으로 표시할 수 있습니다. 데이터를 집계하는 데 사용한 정보, 즉 소스 및 목적지 IP 주소(및 해당 호스트와 연결된 사용자), 대상 포트, 전송 프로토콜, 애플리케이션 프로토콜만 그래프로 표시할 수 있습니다.

팁 Security Intelligence(보안 인텔리전스) 이벤트를 관련된 연결 이벤트와 별도로 그래프로 표시할 수는 없습니다. Security Intelligence(보안 인텔리전스) 필터링 활동에 대한 그래픽 개요를 보려면 대시보드와 Context Explorer(맥락 탐색기)를 사용하십시오.

연결 그래프는 세 가지 유형이 있습니다.

- 원도표는 불연속 카테고리로 그룹화한 단일 데이터 집합의 데이터를 표시합니다.
- 막대 그래프는 불연속 카테고리로 그룹화한 하나 이상의 데이터 집합의 데이터를 표시합니다.
- 선 그래프는 표준 또는 속도(변경 속도) 보기 중 하나를 사용하여, 하나 이상의 데이터 집합에서 얻은 데이터의 시간에 따른 변화를 표시합니다.

참고 시스템은 트래픽 프로파일을 선 그래프로 표시하며, 이 그래프는 몇 가지 제한 사항은 있지만 다른 연결 그래프와 같은 방식으로 조작할 수 있습니다. 트래픽 프로파일을 보려면 관리자 액세스 권한이 있어야 합니다.

워크플로 테이블처럼, 워크플로 그래프도 분석에 집중할 수 있도록 드릴다운하고 제한할 수 있습니다.

막대 그래프와 선 그래프는 모두 여러 데이터 집합을 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다. 예를 들어 고유한 이니시에이터 및 응답자의 총 수를 표시할 수 있습니다. 원도표는 데이터 집합을 하나만 표시할 수 있습니다.

x축, y축 또는 두 축을 모두 변경하여 연결 그래프에 다른 데이터와 데이터 집합을 표시할 수 있습니다. 원도표의 경우, x축을 변경하면 독립 변수가 변경되고 y축을 변경하면 종속 변수가 변경됩니다.

관련 항목

연결 요약(그래프에 대한 집계된 데이터), 2876 페이지

연결 이벤트 그래프 사용

Firepower Management Center에서는 연결 이벤트 그래프를 보고, 찾는 정보에 맞게 그래프를 조작할 수 있습니다.

연결 그래프에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 연결 이벤트의 테이블 보기에서 종료되는 사전 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(분석)** > **Connections(연결)** > **Events(이벤트)**을(를) 선택합니다.

참고 그래프 대신 연결 이벤트 테이블이 표시되거나 다른 그래프를 보려는 경우, 워크플로 제목별로 **(switch workflow)**을 클릭하고 그래프를 포함하는 사전 정의된 워크플로 또는 맞춤형 워크플로를 선택합니다. 미리 정의된 연결 이벤트 워크플로(연결 그래프 포함)는 연결의 테이블 보기에서 종료됩니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Time Range(시간 범위) - 시간 범위를 조정합니다. 그래프에 아무것도 표시되지 않는 경우에 유용합니다(타임 윈도우 변경, 2815 페이지 참조).
- Field Names(필드 이름) - 그래프로 표시할 수 있는 데이터에 관한 자세한 정보는 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지 섹션을 참조하십시오.

- Host Profile(호스트 프로파일) - IP 주소에 대한 호스트 프로파일을 보려면, 연결 데이터를 이니시에이터 또는 응답자별로 표시하는 그래프에서 막대 그래프의 막대나 원도표의 쐐기를 클릭하고 **View Host Profile(**호스트 프로파일 보기**)**을 선택합니다.
- User Profile(사용자 프로파일) - 사용자 프로파일 정보를 보려면, 연결 데이터를 이니시에이터 사용자별로 표시하는 그래프에서 막대 그래프의 막대나 원도표의 쐐기를 클릭하고 **View User Profile(**사용자 프로파일 보기**)**을 선택합니다.
- Other Information(기타 정보) - 그래프로 표시한 데이터에 관해 자세히 알고 싶다면, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기에 마우스 포인터를 올립니다.
- Constrain(제한) - 워크플로를 다음 페이지로 진행하지 않고 아무 X축(독립 변수) 기준을 이용해 연결 그래프를 제한하려는 경우, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기를 클릭하고 **View by...(**보기 기준**)** 옵션을 선택합니다.
- Data Selection(데이터 선택) - 그래프에 표시되는 데이터를 변경하려면 **X-Axis(X**축**)** 또는 **Y-Axis(Y**축**)**를 클릭하고 그래프로 표시한 새 데이터를 선택합니다. X축을 **Time(**시간**)**으로 변경하거나 시간에서 다른 항목으로 변경하면 그래프 유형도 변경됩니다. Y축을 변경하면 표시되는 데이터 집합도 영향을 받습니다.
- Datasets(데이터 집합) - 그래프의 데이터 집합을 변경하는 경우, **Datasets(**데이터 집합**)**를 클릭하고 새 데이터 집합을 선택합니다.
- Detach(분리) - 기본 시간 범위에 영향을 주지 않고 추가 분석을 수행할 수 있도록 연결 그래프를 분리하려면 **Detach(**분리**)**를 클릭합니다.

  팁 분리된 그래프에서 **New Window(**새 창**)**를 클릭하여 복사본을 만듭니다. 그러면 각각의 분리된 그래프에 서로 다른 분석을 수행할 수 있습니다. 트래픽 프로파일은 분리된 그래프라는 점을 유의하십시오.

- Drill Down(드릴다운) - 워크플로의 다음 페이지로 드릴다운하려면, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기를 클릭하고 **Drill-down(**드릴다운**)**을 선택합니다. 선 그래프의 특정 지점을 클릭하면 이 클릭한 지점을 중심으로 다음 페이지의 시간 범위가 10분 간격으로 제한됩니다. 막대 그래프의 막대를 클릭하거나 원도표의 쐐기 모양을 클릭하면 막대 또는 쐐기 모양에 따라 표시된 기준에 의해 다음 페이지가 제한됩니다.
- Export(내보내기) - 그래프에 대한 연결 데이터를 CSV(쉼표로 구분된 값) 파일로 내보내려면 **Export Data(**데이터 내보내기**)**를 클릭합니다. 그런 다음 **Download CSV File(CSV** 파일 다운로드**)**을 클릭하고 파일을 저장합니다.
- Graph Type(그래프 유형): 선 - 표준 또는 속도(변경 속도) 그래프로 전환하려면 **Velocity(**속도**)**를 클릭하고 **Standard(**표준**)** 또는 **Velocity(**속도**)**를 선택합니다.
- Graph Type(그래프 유형): 막대 및 원 - 막대 그래프 또는 원도표로 전환하려면 **Switch to Bar(**막대 그래프로 전환**)** 또는 **Switch to Pie(**원도표로 전환**)**를 클릭합니다. 원도표에는 여러 데이터 집합을 표시할 수 없으며, 따라서 여러 데이터 집합이 있는 막대 그래프에서 원도표로 전환하면 원도표에는 자동으로 선택되는 데이터 집합 하나만 표시됩니다. 표시할 데이터세트를 선택할 경우, Firepower Management Center은(는) 이니시에이터 및 응답자 통계보다 전체 통계를 우선시하고, 응답자 통계보다는 이니시에이터 통계를 우선시합니다.

- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.
- Recenter(중앙으로 지정) - 시간 범위를 변경하지 않고 특정 시간 지점을 선 그래프의 중앙으로 지정하려면, 해당 지점을 클릭하고 **Recenter(**중앙으로 지정**)**를 선택합니다.
- Zoom(확대/축소) - 확대 또는 축소하지 않고 특정 시간 지점을 선 그래프의 중앙으로 지정하려면, 해당 지점을 클릭하고 **Zoom(**확대/축소**)**을 선택한 다음 새 기간을 선택합니다.

참고 제한, 중앙으로 지정, 확대/축소 작업은 Firepower Management Center의 기본 시간 범위를 변경합니다. 단 분리된 그래프를 이용해 작업하는 경우는 예외입니다.

예: 연결 그래프 제한

예: 원도표의 **X**축과 **Y**축 변경

시간 추이에 따른 연결 그래프를 고려해 보십시오. 포트에 따라 그래프의 포인트를 제한할 경우, 탐지된 연결 이벤트 수를 기준으로 가장 활성화된 포트 10개가 제시되지만, 사용자가 클릭한 포인트를 중심으로 한 10분 간격으로 제한된 막대 그래프가 표시됩니다.

막대 중 하나를 클릭하고 **View by Initiator IP(**이니시에이터 **IP**별로 보기**)**를 선택하여 그래프를 추가로 제한할 경우, 이전과 동일한 10분 간격뿐만 아니라 클릭한 막대에 따라 표시되는 포트를 기준으로 제한된 새로운 막대 그래프가 표시됩니다.

포트당 킬로바이트 단위로 그래프를 작성하는 원도표를 고려해보십시오. 이 경우 x축은 **Responder Port**이고 y축은 **KBytes**입니다. 이러한 원도표는 특정 간격 동안 모니터링되는 네트워크를 통해 전송된 데이터의 총 킬로바이트를 나타냅니다. 원의 쐐기 모양은 각 포트에서 탐지된 데이터의 비율을 나타냅니다.

- **Application Protocol(**애플리케이션 프로토콜**)**에 대한 차트의 x축을 변경할 경우 원도표에는 전송된 총 킬로바이트가 계속 표시되지만, 원형의 쐐기 모양은 각 탐지된 애플리케이션 프로토콜에 전송된 데이터의 비율을 나타냅니다.
- 도표의 y축을 **Packets**로 변경할 경우 원도표는 특정 간격 동안 모니터링되는 네트워크를 통해 전송된 총 패킷 수를 나타내며, 원의 쐐기 모양은 각 포트에서 탐지된 총 패킷 수의 비율을 나타냅니다.

관련 항목

워크플로 사용, 2793 페이지
이벤트 보기 구성, 41 페이지

연결 그래프 데이터 옵션

x축, y축 또는 두 축을 모두 변경하여 연결 그래프에 다른 데이터를 표시할 수 있습니다. 원 그래프의 경우, x축을 변경하면 독립 변수가 변경되고 y축을 변경하면 종속 변수가 변경됩니다.

표 ***306: X***축 옵션

X축 옵션	그래프 유형	이 데이터를 그래프로 표시
애플리케이션 프로토콜	막대 또는 원	가장 활성화된 10가지 애플리케이션 프로토콜별
디바이스	막대 또는 원	가장 활성화된 10가지 매니지드 디바이스별
초기자 IP	막대 또는 원	가장 활성화된 10가지 이니시에이터 호스트 IP 주소별
이니시에이터 사용자	막대 또는 원	가장 활성화된 10가지 이니시에이터 사용자별
응답기 IP	막대 또는 원	가장 활성화된 10가지 응답자 호스트 IP 주소별
응답자 포트	막대 또는 원	가장 활성화된 10가지 응답자 포트별
Source Device	막대 또는 원	가장 활성화된 10가지 NetFlow 데이터 엑스포터, 그리고 Firepower System 매니지드 디바이스가 탐지한 모든 연결에 대한 `Firepower`라는 이름의 소스 디바이스별
시간	라인	시간 추이 y축을 **Time(**시간**)**으로 변경하거나 시간에서 다른 항목으로 변경하면 그래프 유형도 변경되며, 데이터 집합이 변경될 수도 있습니다.

표 ***307: Y***축 옵션

Y축 옵션	**X**축 기준을 사용하여 이 데이터를 그래프로 표시
바이트	전송된 바이트
Connections	연결 수

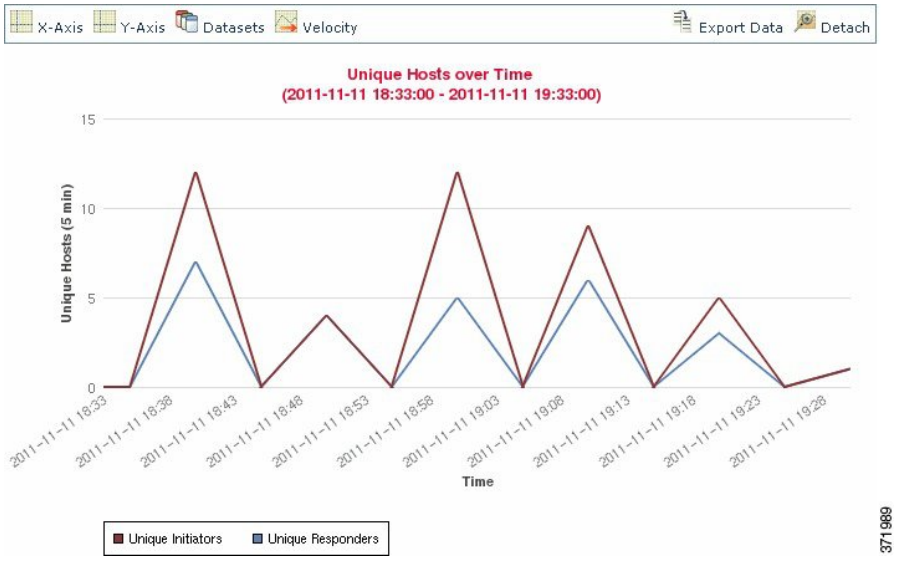
Y축 옵션	**X**축 기준을 사용하여 이 데이터를 그래프로 표시
KB	전송된 킬로바이트
초당 KB	초당 킬로바이트
패킷	전송된 패킷 수
고유 호스트	탐지한 고유 호스트 수
고유한 애플리케이션 프로토콜	고유 애플리케이션 프로토콜 수
고유한 사용자	고유한 사용자 수

여러 데이터 집합이 포함된 연결 그래프

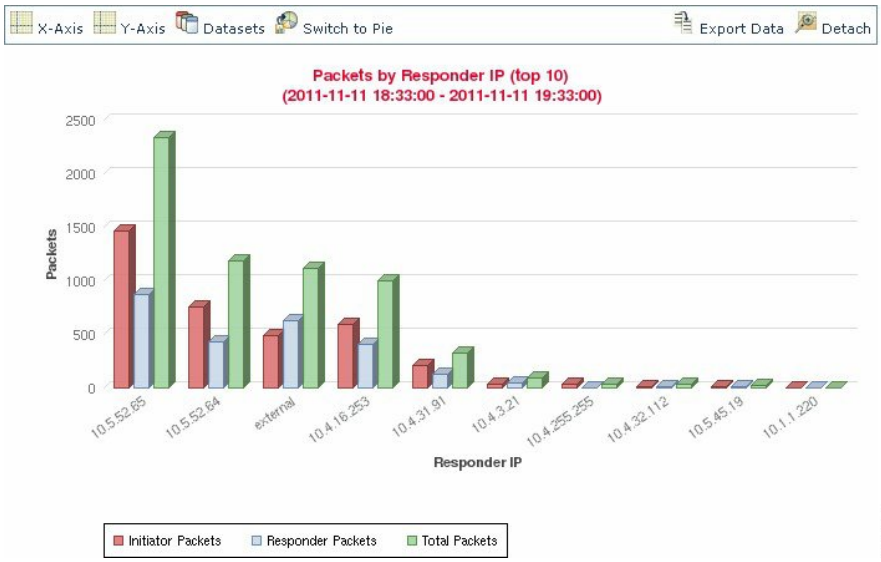
막대 그래프와 선 그래프는 모두 여러 데이터 집합을 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다. 예를 들어 고유한 이니시에이터 및 응답자의 총 수를 표시할 수 있습니다.

참고 원도표에서는 여러 데이터세트를 표시할 수 없습니다. 여러 데이터세트가 있는 막대 그래프에서 원도표로 전환할 경우, 원도표에는 자동으로 선택된 하나의 데이터세트만 표시됩니다. 표시할 데이터세트를 선택할 경우, Firepower Management Center은(는) 이니시에이터 및 응답자 통계보다 전체 통계를 우선시하고, 응답자 통계보다는 이니시에이터 통계를 우선시합니다.

선 그래프에서 여러 데이터세트는 각기 다른 색상의 여러 선으로 표시됩니다. 예를 들어 다음 그래픽에는 1시간 간격 동안 모니터링된 네트워크에서 탐지된 고유한 개시자의 총수 및 고유한 응답자의 총수가 표시됩니다.



막대 그래프에서 여러 데이터세트는 각 x축 데이터 포인트의 색상 막대로 표시됩니다. 예를 들어 다음 막대 그래프에는 모니터링된 네트워크에서 전송된 총 패킷, 이니시에이터가 전송한 패킷, 응답자가 전송한 패킷이 표시됩니다.



연결 그래프 데이터 집합 옵션

다음 표에서는 연결 그래프의 x축에 표시할 수 있는 데이터세트를 설명합니다.

표 ***308:*** 데이터 집합 옵션

y축에 표시되는 내용	선택 가능한 데이터 집합
Connections	기본값 전용 - 모니터링되는 네트워크에서 탐지된 연결의 수(**Connections**) 이는 트래픽 프로파일 그래프의 유일한 옵션입니다.
KB	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 킬로바이트(**Total KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 킬로바이트 수(**Initiator KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 킬로바이트 수(**Responder KBytes**)
초당 KB	기본값 전용 - 모니터링되는 네트워크에서 전송된 초당 총 킬로바이트(**Total KBytes Per Second**)

y축에 표시되는 내용	선택 가능한 데이터 집합
패킷	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 패킷(**Total Packets**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 패킷 수(**Initiator Packets**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 패킷 수(**Responder Packets**)
고유 호스트	다음을 조합하여 선택 • 모니터링되는 네트워크의 고유한 세션 개시자 수(**Unique Initiators**) • 모니터링되는 네트워크의 고유한 세션 응답자 수(**Unique Responders**)
고유한 애플리케이션 프로토콜	기본값 전용 - 모니터링되는 네트워크의 고유한 애플리케이션 프로토콜 수(**Unique Application Protocols**)
고유한 사용자	기본값 전용 - 모니터링되는 네트워크의 세션 개시자에 로깅된 고유한 사용자 수(**Unique Initiator Users**)

이벤트 시간 제약 조건

각 이벤트에는 이벤트가 발생한 시점을 나타내는 타임스탬프가 있습니다. 시간 범위라고도 하는 타임 윈도우를 설정하여 일부 워크플로에 나타나는 정보를 제한할 수 있습니다.

시간을 기준으로 제한할 수 있는 이벤트를 기반으로 하는 워크플로는 페이지 상단에 시간 범위 줄이 나타납니다.

기본적으로 워크플로는 지난 시간으로 설정된 확장 타임 윈도우를 사용합니다. 예를 들어 오전 11:30분에 로그인할 경우 오전 10:30분부터 오전 11:30분까지의 이벤트를 볼 수 있습니다. 시간이 경과하면서 타임 윈도우가 확장됩니다. 오후 12:30분에는 오전 10:30분부터 오후 12:30분까지의 이벤트를 볼 수 있습니다.

이 동작은 이벤트 보기 설정에서 자체 기본 타임 윈도우를 설정해 변경할 수 있습니다. 이것은 세 가지 속성을 제어합니다.

- 타임 윈도우 유형(고정, 확장, 슬라이딩)
- 타임 윈도우 길이
- 타임 윈도우 개수(다중 타임 윈도우 또는 단일 글로벌 타임 윈도우)

기본 타임 윈도우 설정과 무관하게 이벤트 분석 과정에서 페이지 맨 위의 시간 범위를 클릭하면 표시되는 Date/Time(시간/날짜) 팝업 창에서 수동으로 타임 윈도우를 변경할 수 있습니다. 구성한 타임 윈도우의 개수 및 사용 중인 어플라이언스의 유형에 따라 Date/Time(시간/날짜) 창을 사용하여 현재 보고 있는 이벤트 유형의 기본 타임 윈도우를 변경할 수도 있습니다.

마지막으로, 슬라이딩 또는 확장 워크플로를 보는 도중 타임 윈도우를 일시 중지할 수 있습니다. 타임 윈도우 일시 중지로 데이터 집합 임시 중지, 2815 페이지의 내용을 참조하십시오.

관련 항목

이벤트 보기 구성, 41 페이지
연결 및 보안 인텔리전스 이벤트 테이블 사용, 2900 페이지

이벤트에 대한 세션별 타임 윈도우 맞춤 설정

기본 타임 윈도우과 무관하게 이벤트 분석 과정에서 타임 윈도우를 수동으로 변경할 수 있습니다.

참고 수동 타임 윈도우 설정은 현재 세션에만 유효합니다. 로그아웃하고 다시 로그인하면 타임 윈도우는 기본값으로 돌아갑니다.

구성된 타임 윈도우의 수에 따라 어떤 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에 영향을 줄 수 있습니다. 예를 들어 단일 글로벌 타임 윈도우가 있을 경우 한 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에서도 변경됩니다. 이와 달리 다중 타임 윈도우를 사용하는 경우 감사 로그 또는 상태 이벤트 워크플로의 타임 윈도우를 변경하더라도 다른 타임 윈도우에 영향을 주지 않습니다. 반면에 다른 이벤트 종류의 타임 윈도우를 변경하면 (감사 이벤트 및 상태 이벤트를 제외하고) 시간의 제한을 받을 수 있는 모든 이벤트에 적용됩니다.

일부 워크플로는 시간의 제한을 받지 않을 수 있으므로 타임 윈도우 설정은 호스트, 호스트 속성, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 또는 화이트 목록 위반을 기반으로 한 워크플로에는 적용되지 않습니다.

Date/Time(시간/날짜) 창의 Time Window(타임 윈도우) 탭을 사용하여 수동으로 타임 윈도우를 구성합니다. 기본 타임 윈도우 설정에서 구성한 타임 윈도우의 수에 따라 탭의 제목은 다음 중 하나가 됩니다.

- **Events Time Window(**이벤트 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 감사 로그 또는 상태 이벤트 워크플로가 아닌 워크플로의 타임 윈도우를 설정하는 경우
- **Health Monitoring Time Window(**상태 모니터링 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 상태 이벤트 워크플로의 타임 윈도우를 설정하는 경우
- **Audit Log Time Window(**감사 로그 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 감사 로그에 대한 타임 윈도우를 설정하는 경우
- **Global Time Window(**전역 타임 윈도우**)** - 단일 타임 윈도우를 구성한 경우

타임 윈도우를 구성할 때는 사용할 타임 윈도우 유형을 가장 먼저 결정해야 합니다.

- 고정(*static*) 타임 윈도우는 특정 시작 시간부터 종료 시간까지의 모든 이벤트를 표시합니다.

- 확장(*expanding*) 타임 윈도우는 특정 시작 시간부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 타임 윈도우가 확장되고 새 이벤트가 이벤트 보기에 추가됩니다.
- 슬라이딩(*sliding*) 타임 윈도우는 특정 시작 시간(예: 1주일 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 페이지를 새로고침하면 타임 윈도우가 "슬라이딩"하므로 구성된 범위(이 예에서는 지난주)의 이벤트만 볼 수 있습니다. 검사하는 동안 데이터 집합의 업데이트를 일시 중단하는 방법은 타임 윈도우 일시 중지로 데이터 집합 임시 중지, 2815 페이지 섹션을 참조하십시오.

선택하는 유형에 따라 Date/Time(시간/날짜) 창이 바뀌어 각기 다른 설정 옵션을 제공합니다.

참고 Firepower System에서는 시간대 환경설정에서 지정한 시간에 따라 24시간 시계를 사용합니다.

타임 윈도우 설정

다음 표에서는 Time Window 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 ***309:*** 타임 윈도우 설정

설정	타임 윈도우 유형	설명
타임 윈도우 유형 드롭다운 목록	해당 없음	사용할 타임 윈도우의 유형을 고정, 확장, 슬라이딩 중에서 선택합니다. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
타임 캘린더 시작	고정, 확장	타임 윈도우의 시작 날짜와 시간을 지정합니다. 모든 타임 윈도우의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. 달력 대신 아래에서 설명하는 미리 설정 옵션을 사용할 수 있습니다.

설정	타임 윈도우 유형	설명
타임 캘린더 종료	고정	타임 윈도우의 종료 날짜와 시간을 지정합니다. 모든 타임 윈도우의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. 확장 타임 윈도우를 사용하는 경우 End Time 달력이 회색으로 표시되어 종료 시간이 "현재"임을 나타냅니다. 달력 대신 아래에서 설명하는 미리 설정 옵션을 사용할 수 있습니다.
최종 필드 및 드롭다운 목록 보기	슬라이딩	슬라이딩 타임 윈도우의 길이를 구성합니다.
미리 설정: 모두	모두	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간에 따라 타임 윈도우를 변경합니다. 예를 들어 **1 week(1** 주**)**클릭하면 지난주를 나타내도록 타임 윈도우가 변경됩니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다.
미리 설정: 현재	고정, 확장	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간 및 날짜에 따라 타임 윈도우를 변경합니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다. 다음을 참고하십시오. • 현재 요일은 자정에 시작합니다. • 현재 주는 일요일 자정에 시작합니다. • 현재 월은 월의 첫날 자정에 시작합니다.

설정	타임 윈도우 유형	설명
미리 설정: 동기화	모두(글로벌 타임 윈도우를 사용하는 경우에는 사용 불가)	다음 중 하나를 클릭합니다. • **Events Time Window(**이벤트 타임 윈도우**)** - 현재 타임 윈도우를 이벤트 타임 윈도우dhk 동기화합니다. • **Health Monitoring Time Window(**상태 모니터링 타임 윈도우**)** - 현재 타임 윈도우를 상태 모니터링 타임 윈도우와 동기화합니다. • **Audit Log Time Window(**감사 로그 타임 윈도우**)** - 현재 타임 윈도우를 감사 로그 타임 윈도우와 동기화합니다.

타임 윈도우 변경

프로시저

단계 **1** 시간으로 제한된 워크플로에서 시간 범위( )를 클릭하여 Date/Time(날짜/시간) 창으로 이동합니다.

단계 **2** **Events Time Window(**이벤트 타임 윈도우**)**에서 타임 윈도우 설정, 2813 페이지에 설명된 대로 타임 윈도우를 설정합니다.

팁 **Reset**을 클릭하여 타임 윈도우를 기본 설정으로 변경합니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

타임 윈도우 일시 중지로 데이터 집합 임시 중지

슬라이딩 또는 확장 타임 윈도우를 사용하는 경우, 타임 윈도우를 일시 중지해 워크플로가 제공하는 데이터의 스냅샷을 조사할 수 있습니다. 중지하지 않은 워크플로가 업데이트되면 조사할 이벤트가 제거되거나 조사 대상이 아닌 이벤트가 추가될 수 있습니다. 이 기능은 이런 경우에 유용합니다.

페이지 하단의 링크를 클릭해 다른 이벤트 페이지를 표시하면 타임 윈도우는 자동으로 일시 중지됩니다. 준비가 끝나면 타임 윈도우의 일시 중지를 취소하면 됩니다.

분석을 마치면 타임 윈도우의 일시 중지를 취소할 수 있습니다. 타임 윈도우 일시 중지를 취소하면 환경설정에 따라 업데이트되며, 이벤트 보기도 업데이트되어 일시 중지 취소된 타임 윈도우가 반영됩니다.

이벤트 타임 윈도우를 일시 중지하더라도 대시보드에 아무런 영향이 없으며, 또한 대시보드를 일시 중지하더라도 이벤트 타임 윈도우 일시 중지는 영향받지 않습니다.

프로시저

시간 기준으로 제한되는 워크플로에서, 원하는 시간 범위 제어를 선택합니다.

- 시간 창을 일시 중지하려면 시간 범위 제어 아이콘(일시 중지( ))을 클릭합니다.
- 시간 창 일시 중지를 취소하려면 시간 범위 제어 아이콘(재생( ))을 클릭합니다.

이벤트에 대한 기본 타임 윈도우

이벤트 분석 과정에서 Date/Time(날짜/시간) 창의 Preferences(환경설정) 탭을 사용하면 이벤트 보기 설정을 사용하지 않고도 현재 표시하는 이벤트 유형의 기본 타임 윈도우를 변경할 수 있습니다.

이렇게 기본 타임 윈도우를 변경하면 현재 보고 있는 이벤트 유형의 기본 타임 윈도우만 바뀝니다. 예를 들어 다중 타임 윈도우를 구성한 경우 Preferences(환경설정) 탭에서 기본 타임 윈도우를 변경하면 이벤트, 상태 모니터링 또는 감사 로그 창, 즉 첫 번째 탭에 표시된 타임 윈도우의 설정이 바뀝니다. 단일 타임 윈도우를 구성한 경우 Preferences(환경설정) 탭에서 기본 타임 윈도우를 변경하면 모든 이벤트 유형의 기본 타임 윈도우가 바뀝니다.

관련 항목

기본 시간대, 44 페이지

이벤트 유형에 대한 기본 타임 윈도우 옵션

다음 표에서는 Preferences(환경설정) 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 ***310:*** 타임 윈도우 환경설정

기본 설정	설명
간격 새로고침	이벤트 보기의 새로 고침 간격을 분 단위로 설정합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다.
타임 윈도우 수	사용할 타임 윈도우의 개수를 지정합니다. • 감사 로그, 상태 이벤트, 시간의 제한이 가능한 이벤트 기반 워크플로에 각각 기본 타임 윈도우를 구성하려면 **Multiple**을 선택합니다. • 모든 이벤트에 적용되는 글로벌 타임 윈도우를 사용하려면 **Single**을 선택합니다.

기본 설정	설명
Default Time Window: Show the Last - Sliding	이 설정에서는 지정하는 길이의 슬라이딩 기본 타임 윈도우를 구성할 수 있습니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하면 시간대가 "슬라이딩"하므로 항상 지난 1시간의 이벤트가 표시됩니다.
Default Time Window: Show the Last - Static/Expanding	이 설정에서는 지정하는 길이의 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 고정되어 있으므로 고정 시간 창에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 현재 시간으로 확장됩니다.
Default Time Window: Current Day - Static/Expanding	이 설정에서는 현재 일에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 날짜는 현재 세션의 표준 시간대 설정에 따라 자정에 시작합니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 고정되어 있으므로 고정 시간 창에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대가 현재 시간으로 확장됩니다. 로그아웃하기 전 24시간 이상 분석이 계속될 경우 이 시간대가 24시간을 초과할 수 있습니다.

기본 설정	설명
Default Time Window: Current Week - Static/Expanding	이 설정에서는 현재 주에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 주는 현재 세션의 표준 시간대 설정에 따라 이전 일요일 자정에 시작합니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 고정되어 있으므로 고정 시간 창에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 일요일 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대는 현재 시간으로 확장됩니다. 로그아웃하기 전 1주일 이상 분석이 계속될 경우, 시간대는 1주를 초과할 수 있습니다.

이벤트 유형에 대한 기본 타임 윈도우 변경

프로시저

단계 **1** 시간으로 제한된 워크플로우에서 시간 범위( )를 클릭하여 Date/Time(날짜/시간) 창으로 이동합니다.

단계 **2** **Preferences(**환경설정**)**를 클릭하고 이벤트 유형에 대한 기본 타임 윈도우 옵션, 2816 페이지에 설명된 대로 환경설정을 변경합니다.

단계 **3** **Save Preferences(**환경설정 저장**)**를 클릭합니다.

단계 **4** 다음 2가지 옵션을 사용할 수 있습니다.

- 보고 있는 이벤트 보기에 새 기본 타임 윈도우 설정을 적용하려면 **Apply(**적용**)**를 클릭하여 Date/Time(날짜/시간) 창을 닫고 이벤트 보기를 새로 고칩니다.
- 기본 타임 윈도우 설정을 적용하지 않고 분석을 계속하려면 **Apply(**적용**)**를 클릭하지 않고 Date/Time(날짜/시간) 창을 닫습니다.

이벤트 보기 제약 조건

워크플로 페이지에 표시되는 정보는 지정된 제약 조건에 따라 결정됩니다. 예를 들어 초기에 이벤트 워크플로를 열 때 그 정보는 이전 시간 동안 생성된 이벤트로 제한됩니다.

워크플로의 다음 페이지로 이동하고 표시되는 데이터를 특정 값으로 제한하려면 페이지에서 해당 값의 행을 선택하고 **View(**보기**)**를 클릭합니다. 워크플로에서 다음 페이지로 이동하되 현재 제약 조건을 유지하고 모든 이벤트를 이월하려면 **View All(**모두 보기**)**을 선택합니다.

참고 카운트가 아닌 다중 값을 포함한 행을 선택하고 **View(**보기**)**를 클릭하면 복합 제약 조건이 생성됩니다.

워크플로에서 데이터를 제한하는 3번째 방법이 있습니다. 선택한 값의 행으로 페이지를 제한하고 선택한 값을 페이지 맨 위의 제약 조건 목록에 추가하려면 페이지에서 특정 행의 값을 클릭합니다. 예를 들어 로깅된 연결의 목록을 보는 중에 액세스 컨트롤을 통해 허용된 연결로 목록을 제한하려면 **Action(**작업**)** 열에서 **Allow(**허용**)**를 클릭합니다. 또 다른 예로 침입 이벤트를 보는 중에 목적지 포트가 80인 이벤트로 제한하려는 목록을 제한하려는 경우 **Destination Port/ICMP Code(**대상 포트**/ICMP** 코드**)** 열에서 **80 (http)/tcp**를 클릭합니다.

팁 모니터 규칙 기준에 따라 연결 이벤트를 제한하는 절차는 약간 다르며 추가 단계가 필요할 수 있습니다. 또한 관련된 파일 또는 침입 정보를 기준으로 연결 이벤트를 제한할 수는 없습니다.

검색을 사용하여 워크플로의 정보를 제한할 수도 있습니다. 단일 열에서 다중 값을 대상으로 제한하려면 이 기능을 사용합니다. 예를 들어 두 IP 주소와 관련된 이벤트를 보려는 경우 **Edit Search(**검색 편집**)**를 클릭하고 Search(검색) 페이지에서 해당 IP 주소 필드를 수정하여 두 주소를 모두 포함하게 한 다음 **Search(**검색**)**를 클릭합니다.

검색 페이지에 입력하는 검색 기준은 페이지 맨 위에 제약 조건으로 나열되며, 그에 따라 결과 이벤트가 제한됩니다. Firepower Management Center에서는 현재 제약 조건이 다른 워크플로로 이동할 때에도 적용됩니다. 단, 복합 제약 조건인 경우는 제외합니다.

검색할 때 검색 제약 조건이 검색 중인 테이블에 적용될 것인지를 각별히 주의해야 합니다. 예를 들어 클라이언트 데이터는 연결 요약에서 사용할 수 없습니다. 연결에서 탐지된 클라이언트를 기반으로 연결 이벤트를 검색한 다음 그 결과를 연결 요약 이벤트 보기에 표시할 경우 Firepower Management Center에서는 아무런 제한을 받지 않은 것처럼 연결 데이터를 표시합니다. 잘못된 제약 조건은 N/A(not applicable) 레이블이 지정되고 취소선으로 표시됩니다.

이벤트 제약

프로시저

단계 **1** 워크플로 선택, 2795 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 모든 워크플로에는 다음 옵션이 있습니다.

- 단일 값과 일치하는 이벤트만 보도록 제한하려면, 페이지의 행에서 원하는 값을 클릭합니다.

- 여러 값과 일치하는 이벤트만 보도록 제한하려면, 해당 값이 있는 이벤트의 확인란을 선택하고 **View(**보기**)**를 클릭합니다.

  참고 행에 카운트가 아닌 다중 값이 있을 경우 복합 제약 조건이 추가됩니다.

- 제약 조건을 제거하려면 Search Constraints(검색 제약 조건) 확장 화살표( )를 클릭하고 확장된 Search Constraints(검색 제약 조건) 목록에서 제약 조건 이름을 클릭합니다.
- Search(검색) 페이지를 사용하여 제약 조건을 편집하려면 **Edit Search(**검색 편집**)**를 클릭합니다.
- 제약 조건을 저장된 검색으로 저장하려면 **Save Search(**저장 검색**)**를 클릭하고 쿼리에 이름을 지정합니다.

  참고 복합 제약 조건을 포함한 쿼리는 저장할 수 없습니다.

- 동일한 제약 조건을 다른 이벤트 보기와 함께 사용하려면 **Jump to(**이동**)**를 클릭하고 이벤트 보기를 선택합니다.

  참고 다른 워크플로로 전환하는 경우 복합 제약 조건은 유지되지 않습니다.

- 제약 조건 표시를 전환하려면 Search Constraints(검색 제한 조건) 확장 화살표( ) 또는 Search Constraints(검색 제약 조건) 축소 화살표( )를 클릭합니다. 제약 조건의 목록이 커서 화면의 대부분을 차지할 때 유용한 기능입니다.

복합 이벤트 보기 제약

복합 제약 조건은 특정 이벤트에 대해 카운트가 아닌 모든 값을 기반으로 합니다. 카운트가 아닌 다중 값이 있는 행을 선택할 때 해당 페이지에서 그 행의 카운트가 아닌 모든 값과 매칭하는 이벤트만 가져오는 복합 제약조건이 설정됩니다. 예를 들어 소스 IP 주소 `10.10.31.17`, 목적지 IP 주소 `10.10.31.15`를 포함하는 행 및 소스 IP 주소가 `172.10.10.17`, 목적지 IP 주소가 `172.10.10.15`인 행을 선택할 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15인 이벤트

복합 제약 조건을 단순 제약 조건과 결합할 경우 단순 제약 조건은 복합 제약 조건의 전 범위에 배포됩니다. 예를 들어 프로토콜 값이 `tcp`인 단순 제약 조건을 위에 소개된 복합 제약 조건에 추가한 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15이며 프로토콜이 tcp인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15이며 프로토콜이 tcp인 이벤트

복합 제약 조건에 대해서는 검색을 수행하거나 검색을 저장할 수 없습니다. 또한 이벤트 보기 링크를 사용하거나 **(switch workflow)**을 클릭하여 다른 워크플로로 전환할 때 복합 제약 조건을 유지할 수 없습니다. 복합 제약 조건이 적용된 이벤트 보기에 즐겨찾기를 지정할 경우 제약 조건은 즐겨찾기와 함께 저장되지 않습니다.

복합 이벤트 보기 제약 사용

프로시저

단계 **1** 워크플로 선택, 2795 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 복합 제약 조건은 다음 방법으로 관리할 수 있습니다.

- 복합 제약 조건을 생성하려면 카운트가 아닌 다중 값을 포함한 행을 하나 이상 선택하고 **View(**보기**)**를 클릭합니다.
- 복합 제약 조건을 지우려면 Search Constraints(검색 제약 조건) 확장 화살표( )를 클릭하고 **Compound Constraints(**복합 제약 조건**)**를 클릭합니다.

워크플로 간 탐색

워크플로 페이지에서 **Jump to...(**이동**...)** 드롭다운 목록의 링크를 사용하여 다른 워크플로로 이동할 수 있습니다. 드롭다운 목록을 선택하여 추가 워크플로를 표시하고 선택합니다.

새 워크플로를 선택하면 선택한 행에서 공유하는 속성 및 설정된 제약 조건이 새 워크플로에서 사용됩니다(적용 가능한 경우). 구성된 제약 조건 또는 이벤트 속성이 새 워크플로의 필드에 매핑되지 않을 경우 삭제됩니다. 또한 복합 제약 조건은 다른 워크플로로 전환할 때 유지되지 않습니다. 캡처 파일 워크플로의 제약 조건은 파일 및 악성코드 이벤트 워크플로로만 전송됩니다.

참고 어떤 시간 범위의 이벤트 수를 볼 때 총 이벤트 수가 세부사항 데이터가 있는 이벤트의 수를 반영하지 않을 수 있습니다. 이는 디스크 공간 사용량을 관리하기 위해 때때로 오래된 이벤트의 세부사항을 삭제하기 때문입니다. 이벤트 세부사항이 삭제되는 경우를 최소화하기 위해 이벤트 로깅을 세밀하게 조정하여 구축에 가장 중요한 이벤트만 로깅하게 할 수 있습니다.

타임 윈도우를 일시 중지하거나 고정 타임 윈도우를 구성한 경우를 제외하고 타임 윈도우는 워크플로를 변경할 때 바뀝니다.

이 기능으로 의심스러운 활동을 더 효과적으로 조사할 수 있습니다. 예를 들어 연결 데이터를 보는 중에 내부 호스트가 비정상적으로 많은 양의 데이터를 외부 사이트에 보내는 것이 확인될 경우 responder IP 주소와 포트를 제약 조건으로 선택한 다음 **Applications(**애플리케이션**)** 워크플로로 바로 이동할 수 있습니다. 애플리케이션 워크플로는 responder IP 주소와 포트를 IP Address 및 Port 제약 조건으로 사용하면서 애플리케이션에 대한 추가 정보, 이를테면 어떤 종류의 애플리케이션인가를 표

시합니다. 페이지 맨 위의 **Hosts(**호스트**)**를 클릭하여 원격 호스트의 호스트 프로파일을 볼 수도 있습니다.

애플리케이션에 대한 추가 정보를 얻은 다음 **Correlation Events(**상관관계 이벤트**)**를 클릭하여 연결 데이터 워크플로로 돌아가거나 제약 조건에서 Responder IP를 제거하거나 제약 조건에 Initiator IP를 추가하거나 **Application Details(**애플리케이션 세부사항**)**를 선택하여 시작 호스트의 사용자가 원격 호스트에 데이터를 전송할 때 사용한 클라이언트를 확인할 수 있습니다. Port 제약 조건은 Application Details 페이지에 전송되지 않습니다. 로컬 호스트를 제약 조건으로 유지하지만 다른 탐색 버튼을 사용하여 추가 정보를 찾을 수도 있습니다.

- 로컬 호스트가 어떤 정책을 위반했는지 알아보려면 IP 주소를 제약 조건으로 유지하고 **Jump to(**이동**)** 드롭다운 목록에서 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.
- 호스트에 대해 침입 규칙이 트리거되었는지(공격 지표) 확인하려면 **Jump to(**이동**)** 드롭다운 목록에서 **Intrusion Events(**침입 이벤트**)**를 선택합니다.
- 로컬 호스트에 대한 호스트 프로파일을 보고 호스트가 만일의 익스플로잇 취약성을 갖고 있는지 확인하려면 **Jump to(**이동**)** 드롭다운 목록에서 **Hosts(**호스트**)**를 선택합니다.

북마크

이벤트 분석의 특정 위치 및 시점으로 신속하게 돌아갈 수 있게 하려면 즐겨찾기를 생성합니다. 즐겨찾기는 다음 사항에 대한 정보를 유지합니다.

- 사용 중인 워크플로
- 워크플로에서 표시 중인 부분
- 워크플로 내의 페이지 번호
- 모든 검색 제약 조건
- 모든 비활성 열
- 사용 중인 시간 범위

생성하는 즐겨찾기는 즐겨찾기 액세스 권한이 있는 모든 사용자 계정에서 사용할 수 있습니다. 즉 심층 분석이 필요한 이벤트 모음을 발견할 경우 편리하게 즐겨찾기를 생성한 다음 알맞은 권한을 가진 다른 사용자에게 조사를 맡길 수 있습니다.

참고 즐겨찾기에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 즐겨찾기는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

즐겨찾기 생성

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 즐겨찾기만 볼 수 있습니다.

프로시저

단계 **1** 이벤트를 분석할 때 관심 이벤트가 표시된 상태에서 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다.

단계 **2** **Bookmark Name(**즐겨찾기 이름**)** 필드에 이름을 입력합니다.

단계 **3** **Save Bookmark(**즐겨찾기 저장**)**를 클릭합니다.

즐겨찾기 보기

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 즐겨찾기만 볼 수 있습니다.

프로시저

모든 이벤트 보기는 두 가지 옵션을 제공합니다.

- **View Bookmarks(**즐겨찾기 보기**)**에 마우스 포인터를 올리고, 드롭다운 메뉴에서 원하는 즐겨찾기를 클릭합니다.
- View Bookmarks(즐겨찾기 보기) 페이지에서 **View Bookmarks(**즐겨찾기 보기**)**를 클릭하고, 원하는 즐겨찾기 이름이나 옆에 있는 보기 ( )을 클릭합니다.

  참고 원래 즐겨찾기에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 즐겨찾기는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

워크플로우 히스토리

기능	버전	세부 사항
특정 경우에 워크플로우 테이블의 개선된 로딩 속도	6.6	이제 워크플로우 페이지의 테이블에는 열이 6개 이하로 표시되는 경우에만 동일한 행에 대한 개수 열이 표시됩니다. 이렇게 하면 필요한 계산량이 최소화되므로 테이블 로드 속도가 향상됩니다. 신규/수정 페이지: Analysis(분석) 메뉴 아래의 모든 페이지에서 워크플로우 테이블을 표시합니다. 지원되는 플랫폼: Firepower Management Center

117 장

이벤트 검색

다음 주제에서는 워크플로내의 이벤트를 검색하는 방법을 설명합니다.

- 이벤트 검색, 2825 페이지
- 셀을 통해 쿼리 재정의, 2833 페이지
- 이벤트 검색 히스토리, 2835 페이지

이벤트 검색

Firepower System은 데이터베이스 테이블에 이벤트로 저장되는 정보를 생성합니다. 이벤트에는 어플라이언스가 이벤트를 생성하도록 만든 활동을 설명하는 여러 필드가 포함되어 있습니다. 다양한 이벤트 유형에 대해 환경에 맞춤 설정된 검색을 생성하고 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

검색을 저장할 때 이름을 지정하고 검색을 사용자만 사용할 수 있는지 어플라이언스의 모든 사용자가 사용할 수 있는지 지정합니다. 맞춤형 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다. 전에 검색을 저장한 경우, 이를 로드하여 필요한 수정을 한 다음 검색을 시작할 수 있습니다. 맞춤형 분석 대시보드 위젯, 보고서 템플릿, 사용자 지정 사용자 역할도 저장된 검색을 사용할 수 있습니다. 저장한 검색은 Search(검색) 페이지에서 삭제할 수 있습니다.

일부 이벤트 유형의 경우, Firepower System은 예제 역할을 하고 네트워크에 대한 중요한 정보에 빠르게 액세스하도록 도와주는 사전 정의된 검색을 제공합니다. 네트워크 환경에 대해 사전 정의된 검색 내에서 필드를 수정한 다음 나중에 다시 사용하기 위해 저장할 수 있습니다.

사용할 수 있는 검색 기준은 검색 유형에 따라 다를 수 있지만 원리는 동일합니다. 검색은 모든 필드에 지정된 검색 기준에 일치하는 레코드만 반환합니다.

참고 맞춤형 테이블을 검색하려면 약간 다른 절차가 필요합니다.

관련 항목

맞춤형 테이블 검색, 2853 페이지

검색 제약 조건

각 데이터베이스 테이블에는 테이블에 대해 정의된 필드에 적용할 검색 제약 조건 값을 입력할 수 있는, 자체 검색 페이지가 있습니다. 필드 유형에 따라 와일드필드 문자 또는 숫자 값 범위 같은 특수 구문을 사용해 기준을 지정할 수 있습니다.

검색 결과는 열 레이아웃의 각 테이블 필드를 표시하는 워크플로 페이지에 표시됩니다. 워크플로 페이지에 열로 표시되지 않는 필드를 이용해 일부 데이터베이스 테이블을 추가로 검색할 수도 있습니다. 워크플로 페이지 상의 결과를 볼 때 검색 결과에 적용되는 제약을 확인하려면, 확장 화살표(▸)을 클릭하여 활성 검색 제약을 확인합니다.

일반 검색 제약 조건

이벤트를 검색하는 경우 다음 일반 지침을 따르십시오.

- 대부분의 필드에는 부분 일치 검색에 와일드 카드가 필요합니다. 모든 필드에서 이러한 검색에 와일드 카드를 사용할 수 있습니다.

  검색 내 와일드카드 및 특수문자, 2827 페이지의 내용을 참조하십시오.

- 모든 필드에 부정(`!`)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 많은 숫자 필드 앞에 초과(`>`), 이상(`>=`), 미만(`<`), 이하(`<=`), 같음(`=`) 또는 같지 않음(`<>`) 연산자를 붙일 수 있습니다.

팁 길고 복잡한 값(SHA-256 해시 값 등)을 이용해 필드를 검색하는 경우, 소스 자료에서 검색 기준을 복사해 검색 페이지의 적절한 필드에 붙여넣을 수 있습니다.

검색 내 와일드카드 및 특수문자

연결 및 보안 인텔리전스 이벤트의 모든 텍스트 필드 및 기타 이벤트 유형의 대부분의 텍스트 필드에서 검색할 때 텍스트 필드에서 부분 일치를 검색하려면 문자열에서 지정되지 않은 문자를 나타내는 별표(*)가 필요합니다. 별표가 없는 검색은 이러한 필드의 정확한 일치 검색입니다. 와일드 카드가 필요하지 않은 필드에서도 부분 일치 검색에는 항상 와일드 카드를 사용하는 것이 좋습니다.

예를 들어 `example.com`, `www.example.com` 또는 `department.example.com`을 찾으려면 `*.example.com`으로 검색합니다. 대부분의 경우 `example.com`을 검색하면 `example.com`만 반환됩니다.

영숫자 외의 문자를 검색하려면(별표 문자 포함) 검색 문자열을 따옴표로 감싸십시오. 예를 들어 다음 문자열을 검색하려면

```
Find an asterisk (*)
```

다음을 입력합니다.

```
"Find an asterisk (*)"
```

검색 내 개체 및 애플리케이션 필터

Firepower System에서는 네트워크 설정의 일부로 사용할 수 있는 명명된 개체, 개체 그룹 및 애플리케이션 필터를 생성할 수 있습니다. 검색을 수행하거나 저장할 때 이러한 개체, 그룹 및 필터를 검색 기준으로 사용할 수 있습니다.

검색을 수행하면 개체, 개체 그룹 및 애플리케이션 필터가 `${object_name}`의 형식으로 나타납니다. 예를 들어 개체 이름이 `ten_ten_network`인 네트워크 개체는 검색에 `${ten_ten_network}`로 나타납니다.

검색 기준으로 개체를 사용할 수 있는 검색 필드 옆에 나타나는 개체( )를 클릭할 수 있습니다.

관련 항목

개체 관리자, 560 페이지

검색 내 시간 제약 조건

시간 값을 입력하는 검색 기준 필드에서 허용되는 형식은 다음 표에 나와 있습니다.

표 ***311:*** 검색 필드의 시간 사양

시간 형식	예
`today [at HH:MMam|pm]`	현재 `today at 12:45pm`
*YYYY-DD*MM- *HH:MM:SS*	`2006-03-22 14:22:59`

다음 연산자 중 하나를 시간 값 앞에 사용할 수 있습니다.

표 312: 시간 사양 연산자

운영자	예	설명
<	`< 2006-03-22 14:22:59`	2006년 3월 22일 오후 2:23 이전 타임스탬프의 이벤트를 반환합니다.
>	`> today at 2:45pm`	오늘 오후 2:45 이후 타임스탬프의 이벤트를 반환합니다.

검색 내 IP 주소

검색에서 IP 주소를 지정할 때에는 개별 IP 주소, 쉼표로 구분된 주소 목록, 주소 블록, 또는 하이픈(-)으로 구분된 IP 주소 범위를 입력할 수 있습니다. 또한 부정을 사용할 수 있습니다.

침입 이벤트, 연결 데이터 및 상관 관계 이벤트 검색과 같은 IPv6을 지 원하는 검색의 경우 IPv4 및 IPv6 주소와 CIDR/접두사 길이 주소 블록을 임의의 조합으로 입력할 수 있습니다. IP 주소별로 호스트를 검색하면 하나 이상의 IP 주소가 검색 기준과 일치하는 모든 호스트가 결과에 포함됩니다. 즉, IPv6 주소를 검색하면 기본 주소가 IPv4인 호스트가 반환될 수 있습니다.

CIDR 또는 접두사 길이 표기법을 사용하여 IP 주소 블록을 지정하려는 경우, Firepower System은 마스크 또는 접두사 길이에 의해 지정된 네트워크 IP 주소의 일부만 사용합니다. 예를 들어 `10.1.2.3/8`을 입력한 경우 Firepower System은 `10.0.0.0/8`을 사용합니다.

IP 주소는 네트워크 개체로도 표현할 수 있으므로, IP 주소 검색 기준으로 네트워크 개체를 사용하려면 IP 주소 검색 필드 옆에 나타나는 네트워크 추가 개체(+)을 클릭할 수 있습니다.

표 313: 허용되는 IP 주소 구문

지정할 주소	입력할 내용	예시
단일 IP 주소	IP 주소	`192.168.1.1` `2001:db8::abcd`
목록을 사용하여 여러 IP 주소	쉼표로 구분된 IP 주소의 목록 쉼표 전후에 공백을 추가하지 마십시오.	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
CIDR 블록 또는 접두사 길이로 지정할 수 있는 IP 주소의 범위	IPv4 CIDR 또는 IPv6 접두사 길이 표기법으로 IP 주소 블록	`192.168.1.0/24` 192.168.1.0 네트워크에서 255.255.255.0(즉, 192.168.1.0~192.168.1.255)의 IP를 지정합니다.
CIDR 블록 또는 접두사로 지정할 수 없는 IP 주소의 범위	하이픈을 사용하여 IP 주소 범위 하이픈 전후에 공백을 추가하지 마십시오.	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

지정할 주소	입력할 내용	예시

IP 주소 또는 IP 주소 범위를 지정하기 위한 기타 방법의 표기법	IP 주소, 블록 또는 범위 앞에 느낌표	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

차단되었거나 모니터링되는(하지만 차단되었을 수 있는) 호스트 호스트 프로파일 아이콘, 2799 페이지의 내용을 참조하십시오.	연결 및 보안 인텔리전스 이벤트의 이니시에이터 IP 및 응답자 IP 필드: • 블랙리스트 • • 모니터	--

관련 항목

Firepower System IP 주소 규칙, 19 페이지

검색의 URL

URL을 검색할 때 와일드 카드를 포함합니다. 예를 들어 **`*example.com*`**을 사용하여 도메인의 모든 변형(예: **`https://example.com`**, **`division.example.com`** 및 **`example.com/division/`**)을 찾습니다.

검색 내 매니지드 디바이스

FMC에서만, 또는 실제 고가용성 또는 확장성 구성을 통해 디바이스를 그룹화하면 그룹의 이름을 검색했을 때 그룹 내의 모든 디바이스를 결과로 올바르게 반환합니다.

그룹, 디바이스 고가용성 쌍 또는 스택에 대한 일치를 발견하면, 시스템은 검색 수행을 위해 그룹, 디바이스 고가용성 쌍 또는 스택 이름을 적절한 회원 디바이스 이름으로 교체합니다. 장치 필드에 디바이스 그룹, 디바이스 고가용성 쌍 또는 스택을 사용하는 검색을 저장하면, 시스템은 장치 필드에 지정된 이름을 저장하고 검색이 실행될 때마다 디바이스 이름 교체를 수행합니다.

검색 내 포트

Firepower System은 검색에서 포트 번호에 대한 특정 구문을 허용합니다. 다음을 입력할 수 있습니다.

- 단일 포트 번호
- 쉼표로 구분된 포트 번호 목록
- 대시로 구분된 두 개의 포트 번호(포트 번호의 범위를 나타냄)
- 포트 번호 뒤에는 (침입 이벤트를 검색할 때만) 슬래시 (/)로 구분 된 프로토콜 약어
- 앞에 느낌표가 있는 포트 번호 또는 포트 번호의 범위(지정된 포트의 부정을 나타냄)

참고 포트 번호 또는 범위를 지정할 때는 공백을 사용하지 마십시오.

표 ***314:*** 포트 구문 예

예	설명
`21`	TCP와 UDP 이벤트를 비롯한 포트 21의 모든 이벤트를 반환합니다.
`!23`	포트 23의 이벤트를 제외한 모든 이벤트를 반환합니다.
`25/tcp`	포트 25의 모든 TCP 관련 침입 이벤트를 반환합니다.
`21/tcp,25/tcp`	포트 21과 25의 모든 TCP 관련 침입 이벤트를 반환합니다.
`21-25`	포트 21~25의 모든 이벤트를 반환합니다.

검색 내 이벤트 필드

이벤트를 검색하는 경우 검색 기준으로 다음 필드를 사용할 수 있습니다.

- 감사 로그 워크플로 필드, 453 페이지
- 애플리케이션 데이터 필드, 3065 페이지
- 애플리케이션 세부사항 데이터 필드, 3067 페이지
- 캡처된 파일 필드, 2986 페이지
- 화이트 목록 이벤트 필드, 3099 페이지
- 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지
- 상관관계 이벤트 필드, 3095 페이지
- 검색 이벤트 필드, 3046 페이지
- 상태 이벤트 테이블, 426 페이지
- 호스트 속성 데이터 필드, 3055 페이지
- 호스트 데이터 필드, 3048 페이지
- 파일 및 악성코드 이벤트 필드, 2968 페이지
- 침입 이벤트 필드, 2912 페이지
- 침입 규칙의 필드에 로그를 업데이트합니다., 193 페이지

- 교정 상태 테이블 필드, 3104 페이지
- Nmap 스캔 결과 필드, 2436 페이지
- 서버 데이터 필드, 3061 페이지
- 서드파티 취약성 데이터 필드, 3074 페이지
- 사용자 관련 필드, 3076 페이지
- 취약성 데이터 필드, 3069 페이지
- 화이트 목록 위반 필드, 3101 페이지

검색 수행

검색을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Search(**검색**)**를 선택합니다.

팁 워크플로의 아무 페이지에서 **Search(**검색**)**를 클릭해도 됩니다.

단계 **2** 테이블 드롭다운 목록에서 검색할 이벤트 또는 데이터 유형을 선택합니다.

단계 **3** 해당 필드에 검색 기준을 입력합니다. 사용 가능한 검색 기준에 대해 자세히 알아보려면 다음 섹션을 참조하십시오.

- 검색 제약 조건, 2826 페이지
- 감사 로그 워크플로 필드, 453 페이지
- 애플리케이션 데이터 필드, 3065 페이지
- 애플리케이션 세부사항 데이터 필드, 3067 페이지
- 캡처된 파일 필드, 2986 페이지
- 화이트 목록 이벤트 필드, 3099 페이지
- 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지
- 상관관계 이벤트 필드, 3095 페이지
- 검색 이벤트 필드, 3046 페이지
- 상태 이벤트 테이블, 426 페이지
- 호스트 속성 데이터 필드, 3055 페이지
- 호스트 데이터 필드, 3048 페이지

- 파일 및 악성코드 이벤트 필드, 2968 페이지
- 침입 이벤트 필드, 2912 페이지
- 침입 규칙의 필드에 로그를 업데이트합니다., 193 페이지
- 교정 상태 테이블 필드, 3104 페이지
- Nmap 스캔 결과 필드, 2436 페이지
- 서버 데이터 필드, 3061 페이지
- 서드파티 취약성 데이터 필드, 3074 페이지
- 사용자 데이터 필드
- 사용자 활동 데이터 필드
- 취약성 데이터 필드, 3069 페이지
- 화이트 목록 위반 필드, 3101 페이지

단계 **4** 검색을 나중에 다시 사용하려면 검색 저장, 2832 페이지에 설명된 대로 검색을 저장합니다.

단계 **5** 검색을 시작하려면 **Search(**검색**)**를 클릭합니다. 검색 결과가 시간으로 제한되어(적용 가능한 경우) 검색 중인 테이블에 대한 기본 워크플로우에 나타납니다.

다음에 수행할 작업

- 워크플로를 사용하여 검색 결과를 분석하는 방법은 워크플로 사용, 2793 페이지 섹션을 참조하십시오.

관련 항목

이벤트 보기 구성, 41 페이지

검색 저장

검색을 저장하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 저장된 검색을 표시하며 이러한 검색은 수정할 수 있습니다. 상위 도메인에서 저장된 검색도 표시되지만, 이러한 검색은 수정할 수 없습니다. 하위 도메인에서 생성된 검색을 보고 수정하려면 해당 도메인으로 전환하십시오.

시작하기 전에

- 검색 수행, 2831 페이지에 설명된 대로 검색 기준을 설정하거나, 저장된 검색 로드, 2833 페이지에 설명된 대로 저장된 검색을 로드합니다.

프로시저

단계 **1** 자신만 액세스할 수 있도록 검색을 비공개로 저장하려면, Search(검색) 페이지에서 **Private(**비공개**)** 확인란을 선택합니다.

팁 맞춤형 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 로드한 검색의 새 버전을 저장하려는 경우에는 **Save As New(**신규로 저장**)**를 클릭합니다.
- 새 검색을 저장하거나 같은 이름을 이용해 맞춤형 검색을 덮어쓰려는 경우에는 **Save(**저장**)**를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

저장된 검색 로드

저장된 검색을 로드하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 저장된 검색을 표시하며 이러한 검색은 수정할 수 있습니다. 상위 도메인에서 저장된 검색도 표시되지만, 이러한 검색은 수정할 수 없습니다. 하위 도메인에서 생성된 검색을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Search(**검색**)**을(를) 선택합니다.

팁 워크플로의 아무 페이지에서 **Search(**검색**)**를 클릭해도 됩니다.

단계 **2** 테이블 드롭다운 목록에서 검색할 이벤트 또는 데이터 유형을 선택합니다.

단계 **3** **Custom Searches(**맞춤형 검색**)** 목록 또는 **Predefined Searches(**사전 정의된 검색**)** 목록에서 로드하려는 검색을 선택합니다.

단계 **4** 다른 검색 기준을 사용하려는 경우에는 검색 제약 조건을 변경합니다.

단계 **5** 변경된 검색을 나중에 다시 사용하려면, 검색 저장, 2832 페이지에 설명된 대로 검색을 저장합니다.

단계 **6** **Search(**검색**)**를 클릭합니다.

셸을 통해 쿼리 재정의

시스템 관리자는 Linux 셸 기반 쿼리 관리 도구를 사용해 오래 실행되는 쿼리를 찾아서 중지할 수 있습니다.

쿼리 관리 툴을 사용하면 지정된 기간(분)보다 오래 실행되는 쿼리를 찾아 중지할 수 있습니다. 쿼리를 중지하면 이벤트가 감사 로그 및 시스템 로그에 기록됩니다.

관리자 내부 사용자는 FMC CLI에 액세스할 수 있습니다. CLI 액세스를 허용하는 외부 인증 개체를 사용하는 경우 셸 액세스 필터와 일치하는 사용자는 CLI에도 로그인할 수 있습니다.

참고 웹 인터페이스에 검색 페이지를 열어 두면 쿼리가 중지되지 않습니다. 반환에 오랜 시간이 걸리는 쿼리는 쿼리 실행 중에 전체 시스템 성능에 영향을 미칩니다.

셸 기반 쿼리 관리 구문

장기 쿼리는 다음 구문을 사용하여 관리합니다.

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

표 ***315: query_manager Options(옵션)***

옵션	설명
`-h, --help`	간략한 도움말 메시지를 인쇄합니다.
`-l, --list [minutes]`	지정된 기간(분)보다 오래 걸린 모든 쿼리를 나열합니다. 기본적으로, 1분 이상 걸리는 모든 쿼리가 표시됩니다.
`-k, --kill query_id [...]`	전달된 ID가 있는 쿼리를 중단합니다. 이 옵션은 여러 ID를 이용할 수 있습니다.
`--kill-all minutes`	지정된 기간(분)보다 오래 걸린 모든 쿼리를 중단합니다.
`-v, --verbose`	전체 SQL 쿼리를 포함하여 출력을 자세히 표시합니다.

주의 시스템 보안을 위해 Cisco에서는 Linux 셸 사용자를 어플라이언스에서 추가로 설정하지 않도록 권장합니다.

오래 실행되는 쿼리 중지

CLI 액세스 권한이 있는 관리자 사용자 또는 외부 인증된 사용자여야 합니다.

프로시저

단계 **1** `ssh`를 통해 Firepower Management Center에 연결합니다.

단계 **2** CLI `expert` 명령을 사용하여 Linux 셸에 액세스합니다.

단계 **3** 셸 기반 쿼리 관리 구문, 2834 페이지에 설명한 구문을 사용하여 `sudo` 아래에서 `query_manager`를 실행합니다.

이벤트 검색 히스토리

기능	버전	세부 사항
많은 필드에서 부분 일치 검색시 이제 와일드 카드가 필요합니다.	6.6	예를 들어 URL을 검색할 때 **`example.com`**의 모든 변형을 찾으려면 **`* example.com*`**을 사용합니다. 이 동작 변경 사항은 **Analysis(분석) > Search(검색)** 페이지에서 연결 또는 보안 인텔리전스 이벤트를 검색할 때 적용됩니다. 이 검색 페이지는 다른 페이지의 링크를 통해 액세스할 수도 있습니다. 부분 일치 검색에 와일드 카드가 필요하지 않은 필드에서는 선택적으로 사용할 수 있습니다. 영향을 받는 플랫폼: FMC

118 장

사용자 지정 워크플로

다음 주제에서는 맞춤형 워크플로를 사용하는 방법을 설명합니다.

- 맞춤형 워크플로 소개, 2837 페이지
- 저장된 맞춤형 워크플로, 2837 페이지
- 맞춤형 워크플로 생성, 2839 페이지
- 맞춤형 워크플로 사용 및 관리, 2842 페이지

맞춤형 워크플로 소개

사전 정의된 워크플로와 Cisco에서 제공하는 맞춤형 워크플로가 필요에 부합하지 않을 경우, 맞춤형 워크플로를 생성하고 관리해야 합니다.

맞춤형 워크플로는 조직의 고유한 필요에 맞게 생성하는 워크플로입니다. 맞춤형 워크플로를 생성할 때 워크플로의 기반이 되는 이벤트(또는 데이터베이스 테이블)의 종류를 선택합니다. Firepower Management Center에서 맞춤형 테이블을 맞춤형 워크플로의 기반으로 선택할 수 있습니다. 또한 맞춤형 워크플로에 포함되는 페이지를 선택할 수 있습니다. 맞춤형 워크플로는 드릴다운, 테이블 보기, 호스트 또는 패킷 보기 페이지로 구성될 수 있습니다.

이벤트 평가 프로세스가 변경될 경우 새 필요에 맞게 맞춤형 워크플로를 수정할 수 있습니다. 사전 정의 워크플로는 수정할 수 없습니다.

팁 어떤 이벤트 유형에서도 맞춤형 워크플로를 기본 워크플로로 설정할 수 없습니다.

저장된 맞춤형 워크플로

수정 불가한 사전 정의 워크플로 외에도 Firepower Management Center에는 여러 저장된 맞춤형 워크플로가 있습니다. 이 워크플로 각각은 맞춤형 테이블을 기반으로 하며 수정 가능합니다.

다중 도메인 구축의 경우, 이러한 저장된 워크플로는 Global(전역) 도메인에 속하며 하위 도메인에서는 수정할 수 없습니다.

표 ***316:*** 저장된 맞춤형 워크플로

워크플로 이름	설명
Events by Impact, Priority, and Host Criticality(영향, 우선순위, 호스트 중요도별 이벤트)	이 워크플로를 사용하여 네트워크에 중요한 호스트, 현재 취약한 호스트, 현재 공격을 받고 있는 호스트를 신속하게 선별하여 집중할 수 있습니다. 이 워크플로는 Intrusion Events with Destination Criticality(대상 중요도가 있는 침입 이벤트) 맞춤형 테이블을 기반으로 합니다.
우선순위 및 분류별 이벤트	이 워크플로는 이벤트와 그 유형을 이벤트 우선순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다. 이 워크플로는 Intrusion Events(침입 이벤트) 맞춤형 테이블을 기반으로 합니다.
Events with Destination, Impact, and Host Criticality(대상, 영향, 호스트 중요도가 있는 이벤트)	이 워크플로를 사용하여 현재 취약한 상태이며 네트워크에 중요한 호스트에서 발생한 최근의 공격을 확인할 수 있습니다. 이 워크플로는 Intrusion Events with Destination Criticality 사용자 정의 테이블을 기반으로 합니다.
Hosts with Servers Default Workflow(서버 기본 워크플로가 있는 호스트)	이 워크플로를 사용하여 Hosts with Servers(서버가 있는 호스트) 맞춤형 테이블의 기본 정보를 신속하게 볼 수 있습니다. 이 워크플로는 Hosts with Servers(서버가 있는 호스트) 맞춤형 테이블을 기반으로 합니다.
Intrusion Events with Destination Criticality Default Workflow(대상 중요도 기본 워크플로가 있는 침입 이벤트)	이 워크플로를 사용하여 Intrusion Events with Destination Criticality(대상 중요도가 있는 침입 이벤트) 맞춤형 테이블의 기본 정보를 신속하게 볼 수 있습니다. 이 워크플로는 Intrusion Events with Destination Criticality 사용자 정의 테이블을 기반으로 합니다.
Intrusion Events with Source Criticality Default Workflow(소스 중요도 기본 워크플로가 있는 침입 이벤트)	이 워크플로를 사용하여 Intrusion Events with Source Criticality(소스 중요도가 있는 침입 이벤트) 맞춤형 테이블의 기본 정보를 신속하게 볼 수 있습니다. 이 워크플로는 Intrusion Events with Source Criticality(소스 중요도가 있는 침입 이벤트) 맞춤형 테이블을 기반으로 합니다.

워크플로 이름	설명
Server and Host Details(서버 및 호스트 상세정보)	이 워크플로를 사용하여 네트워크에서 어떤 서버가 가장 많이 사용되었는지 그리고 어떤 호스트에서 이 서버를 실행하고 있는지를 확인할 수 있습니다. 이 워크플로는 Hosts with Servers(서버가 있는 호스트) 사용자 지정 테이블을 기반으로 합니다.

맞춤형 워크플로 생성

사전 정의된 워크플로와 Cisco에서 제공하는 맞춤형 워크플로가 필요에 부합하지 않을 경우, 맞춤형 워크플로를 생성해야 합니다.

팁 새 맞춤형 워크플로를 생성하지 않고 다른 어플라이언스에서 맞춤형 워크플로를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 워크플로를 필요에 맞게 수정할 수 있습니다.

맞춤형 워크플로를 생성할 때는 다음을 수행합니다.

- 워크플로의 소스가 될 테이블 선택
- 워크플로 이름 지정
- 워크플로에 드릴다운 페이지 및 테이블 보기 페이지 추가

워크플로의 각 드릴다운 페이지에 대해 다음을 수행할 수 있습니다.

- 웹 인터페이스에서 페이지의 맨 위에 나타날 이름 지정
- 페이지당 최대 5개의 열 포함
- 기본 정렬 순서 지정, 오름차순 또는 내림차순

일련의 워크플로 페이지에서 임의의 위치에 테이블 보기 페이지를 추가할 수 있습니다. 여기에는 페이지 이름, 정렬 순서, 맞춤형 열 위치와 같은 수정 가능한 속성이 없습니다.

참고 하나 이상의 드릴다운 페이지 또는 이벤트 테이블 보기를 맞춤형 워크플로에 추가해야 합니다.

참고 테이블 유형으로 **Vulnerabilities(**취약성**)**를 선택한 경우, **IP Address(IP** 주소**)**를 테이블 열로 추가하면 맞춤형 워크플로에서 취약성을 볼 때 IP Address 열이 나타나지 않습니다. 단, 검색 기능을 사용하여 특정 IP 주소 또는 주소 영역을 표시하도록 워크플로를 제한하는 경우는 제외합니다.

맞춤형 워크플로의 최종 페이지는 다음 표에서 설명하는 것처럼 워크플로의 기반이 되는 테이블에 따라 달라집니다. 이 최종 페이지는 워크플로 생성 시 기본적으로 추가됩니다.

표 ***317:*** 맞춤형 워크플로의 최종 페이지

이벤트/자산 유형	최종 페이지
검색 이벤트	호스트
취약성	취약성 상세정보
서드파티 취약성	호스트
사용자	사용자
보안 침해 지표	호스트
침입 이벤트	패킷

시스템은 다른 종류의 이벤트(예: 감사 로그, 악성 코드 이벤트)를 기반으로 한 맞춤형 워크플로에는 최종 페이지를 추가하지 않습니다.

연결 데이터를 기반으로 하는 맞춤형 워크플로는 다른 맞춤형 워크플로와 동일하지만, 연결 요약 데이터가 있는 드릴다운 페이지와 연결 데이터 그래프 페이지, 개별 연결 및 테이블 보기 페이지가 있는 드릴다운 페이지를 포함할 수 있습니다.

비 연결 데이터 기반 맞춤형 워크플로 생성

비 연결 데이터를 기반으로 맞춤형 워크플로우를 생성하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**맞춤형 워크플로**)**을(를) 선택합니다.

단계 **2** **Create Custom Workflow(**맞춤형 워크플로 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 워크플로의 이름을 입력합니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** **Table(**테이블**)** 드롭다운 목록에서 추가할 표를 선택합니다.

단계 **6** 워크플로에 드릴다운 페이지를 하나 이상 추가하려는 경우에는 **Add Page(**페이지 추가**)**를 클릭합니다.

단계 **7** **Page Name(**페이지 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **8** Column 1에서 정렬 우선순위와 테이블 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다.

예제**:**

예를 들어 대상이 된 대상 포트를 표시하는 페이지를 생성하고 그 페이지를 카운트 순으로 정렬하려면, **Sort Priority(**정렬 우선순위**)** 드롭다운 목록에서 **2**를 선택하고 **Field(**필드**)**드롭다운 목록에서 **Destination Port/ICMP Code(**대상 포트**/ICMP** 코드**)**를 선택합니다.

단계 **9** 페이지에 표시할 필드가 모두 지정될 때까지, 포함할 필드를 선택하고 정렬 우선순위를 설정합니다.

단계 **10** 테이블 보기 페이지 워크플로를 추가 하려는 경우 추가 테이블 보기를 클릭 합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

맞춤형 연결 데이터 워크플로 생성

연결 데이터 기반의 맞춤형 워크플로는 다른 맞춤형 워크플로와 비슷하지만, 드릴다운 페이지 및 테이블 보기 페이지뿐 아니라 연결 데이터 그래프 페이지까지 포함할 수 있습니다. 각 페이지 유형을 원하는 개수와 순서로 워크플로에 포함할 수 있습니다. 각 연결 데이터 그래프 페이지는 단일 그래프를 포함하는데, 이는 선 그래프, 막대 그래프 또는 원도표가 될 수 있습니다. 선 그래프와 막대 그래프는 둘 이상의 데이터 집합을 포함할 수 있습니다.

연결 데이터를 기반으로 맞춤형 워크플로우를 생성하려면 관리자 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**맞춤형 워크플로**)**을(를) 선택합니다.

단계 **2** **Create Custom Workflow(**맞춤형 워크플로 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 워크플로의 이름을 입력합니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** **Table(**표**)** 드롭다운 목록에서 **Connection Events(**연결 이벤트**)**를 선택합니다.

단계 **6** 워크플로에 드릴다운 페이지를 하나 이상 추가하려는 경우에는 두 가지 방법을 사용할 수 있습니다.

- **Add Page(**페이지 추가**)**를 클릭하여 개별 연결의 데이터를 포함하는 드릴다운 페이지를 추가합니다.
- **Add Summary Page(**요약 페이지 추가**)**를 클릭하여 연결 요약 데이터를 포함하는 드릴다운 페이지를 추가합니다.

단계 **7** **Page Name(**페이지 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **8** **Column 1**에서 정렬 우선순위와 테이블 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다.

단계 **9** 페이지에 표시할 필드가 모두 지정될 때까지, 포함할 필드를 선택하고 정렬 우선순위를 설정합니다.

예제**:**

예를 들어 모니터링되는 네트워크를 통해 전송된 트래픽의 양을 표시하는 페이지를 생성하고 가장 많은 트래픽을 전송한 응답자의 순으로 페이지를 정렬하려면 **Sort Priority(**정렬 우선순위**)** 드롭다운 목록에서 **1**을 선택하고 **Field(**필드**)** 드롭다운 목록에서 **Responder Bytes(**응답자 바이트**)**를 선택합니다.

단계 **10** 워크플로에 그래프 페이지를 하나 이상 추가하려는 경우에는 **Add Graph(**그래프 추가**)**를 클릭합니다.

단계 **11** **Graph Name(**그래프 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **12** 페이지에 포함하려는 그래프의 유형을 선택합니다.

- 선 그래프(선형 차트( ))
- 막대 그래프(막대그래프( ))
- 원도표원도표( ))

단계 **13** 그래프의 X축과 Y축을 선택하여 그래프에 표시할 데이터 종류를 지정합니다.

원도표에서 X축은 독립 변수를, Y축은 종속 변수를 나타냅니다.

단계 **14** 그래프에 포함할 데이터 집합을 선택합니다.

원도표는 하나의 데이터 집합만 포함할 수 있습니다.

단계 **15** 연결 데이터의 테이블 보기를 추가하려는 경우에는 **Add Table View(**테이블 보기 추가**)**를 클릭합니다.

테이블 보기를 구성할 수 없습니다.

단계 **16** **Save(**저장**)**를 클릭합니다.

맞춤형 워크플로 사용 및 관리

워크플로를 표시하는 데 사용하는 방법은 워크플로가 사전 정의 이벤트 테이블 중 하나 또는 맞춤형 테이블을 기반으로 하느냐에 따라 달라집니다.

맞춤형 워크플로가 사전 정의 이벤트 테이블을 기반으로 할 경우 어플라이언스와 함께 제공되는 워크플로에 액세스하는 것과 동일한 방법으로 액세스합니다. 예를 들어 Hosts(호스트) 테이블을 기반으로 하는 맞춤형 워크플로에 액세스하려면 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Hosts(**호스트**)**을(를) 선택합니다. 반대로 맞춤형 워크플로가 맞춤형 테이블을 기반으로 한다면, Custom Tables(맞춤형 테이블) 페이지에서 액세스해야 합니다.

이벤트 평가 프로세스가 변경될 경우 새 필요에 맞게 맞춤형 워크플로를 수정할 수 있습니다. 사전 정의 워크플로는 수정할 수 없습니다.

팁 어떤 이벤트 유형에서도 맞춤형 워크플로를 기본 워크플로로 설정할 수 없습니다.

사전 정의 테이블 기반 맞춤형 워크플로 보기

맞춤형 워크플로우를 보려면 관리자, 유지 보수 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** 워크플로 선택, 2795 페이지에서 설명한 대로 맞춤형 워크플로의 기반이 되는 테이블에 적합한 메뉴 경로와 옵션을 선택합니다.

단계 **2** 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 현재 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **3** 어떤 이벤트도 발생하지 않으며 워크플로를 시간으로 제한할 수 있다면, 시간 범위 조정이 필요할 수 있습니다. 이벤트 시간 제약 조건, 2811 페이지 섹션을 참조하십시오.

맞춤형 테이블 기반 맞춤형 워크플로 보기

맞춤형 테이블을 기반으로 하는 맞춤형 워크플로우를 보려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 워크플로를 표시하며 이러한 워크플로는 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 워크플로도 표시되지만, 이러한 워크플로는 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 워크플로를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**를 선택합니다.

단계 **2** 확인할 맞춤형 테이블 옆의 보기 ( )를 클릭하거나 맞춤형 테이블의 이름을 클릭합니다.

단계 **3** 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **4** 어떤 이벤트도 발생하지 않으며 워크플로를 시간으로 제한할 수 있다면, 시간 범위 조정이 필요할 수 있습니다. 이벤트 시간 제약 조건, 2811 페이지 섹션을 참조하십시오.

맞춤형 워크플로

맞춤형 워크 플로우를 편집하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 워크플로를 표시하며 이러한 워크플로는 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 워크플로도 표시되지만, 이러한 워크플로는 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 워크플로를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**맞춤형 워크플로**)**를 선택합니다.

단계 **2** 편집하려는 워크플로 이름 옆의 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 원하는 변경사항을 워크플로에 적용합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

119 장

사용자 지정 표

다음 주제에서는 맞춤형 테이블을 사용하는 방법을 설명합니다.

- 맞춤형 테이블 소개, 2845 페이지
- 사전 정의 맞춤형 테이블, 2845 페이지
- 사용자 정의 맞춤형 테이블, 2850 페이지
- 맞춤형 테이블 검색, 2853 페이지
- 맞춤형 테이블 기록, 2855 페이지

맞춤형 테이블 소개

Firepower System이 네트워크에 대한 정보를 수집하면 Firepower Management Center은(는) 이를 일련의 데이터베이스 테이블에 저장합니다. 워크플로를 사용하여 결과 정보를 볼 경우 Firepower Management Center은(는) 이러한 테이블 중 하나에서 데이터를 가져옵니다. 예를 들어 Count 워크플로의 각 Network Applications(네트워크 애플리케이션) 페이지에 있는 열은 Applications(애플리케이션) 테이블의 필드에서 옵니다.

서로 다른 테이블의 필드를 조합하여 네트워크에서의 활동 분석을 개선할 수 있다고 생각되는 경우 맞춤형 테이블을 생성할 수 있습니다.

사전 정의 테이블 또는 맞춤형 테이블에 대한 맞춤형 워크플로를 생성할 수 있습니다.

사전 정의 맞춤형 테이블

맞춤형 테이블에는 둘 이상의 사전 정의 테이블에서 오는 필드가 포함됩니다. Firepower System에서는 다수의 시스템 정의 맞춤형 테이블을 제공하지만, 사용자는 특정 요구에 맞는 정보만 포함하는 맞춤형 테이블을 추가로 생성할 수 있습니다.

예를 들어 Firepower System에서는 침입 이벤트 데이터를 호스트 데이터와 상호 연결하는 시스템 정의 맞춤형 테이블을 제공하므로, 중요 시스템에 영향을 미치는 이벤트를 검색하고 하나의 워크플로에서 검색 결과를 볼 수 있습니다.

다중 도메인 구축의 경우, 사전 정의된 맞춤형 테이블은 Global(전역) 도메인에 속하며 하위 도메인에서는 수정할 수 없습니다.

다음 표에서는 시스템에서 제공하는 맞춤형 테이블에 대해 설명합니다.

표 ***318:*** 시스템 정의 맞춤형 테이블

표	설명
서버가 있는 호스트	Hosts(호스트) 및 Servers(서버) 테이블의 필드를 포함하며, 네트워크에서 실행 중인 탐지된 애플리케이션에 대한 정보는 물론 그러한 애플리케이션을 실행하는 호스트에 대한 기본 운영체제 정보도 제공합니다.
대상 중요도가 있는 침입 이벤트	Intrusion Events(침입 이벤트) 및 Hosts(호스트) 테이블의 필드를 포함하며, 침입 이벤트에 대한 정보는 물론 각 침입 이벤트와 관련된 대상 호스트의 호스트 중요도도 제공합니다. 이 테이블을 사용해 호스트 중요도가 높은 대상 호스트와 관련된 침입 이벤트를 검색할 수 있습니다.
소스 중요도가 있는 침입 이벤트	Intrusion Events(침입 이벤트) 및 Hosts(호스트) 테이블의 필드를 포함하며, 침입 이벤트에 대한 정보 및 각 침입 이벤트와 관련된 소스 호스트의 호스트 중요도를 확인할 수 있습니다. 이 테이블을 사용해 호스트 중요도가 높은 소스 호스트와 관련된 침입 이벤트를 검색할 수 있습니다.

가능한 테이블 조합

맞춤형 테이블을 만들 때에는 관련 데이터가 포함된 사전 정의 테이블의 필드를 조합할 수 있습니다. 다음 표에는 새 맞춤형 테이블 생성을 위해 조합할 수 있는 사전 정의 테이블이 나열되어 있습니다. 둘 이상의 사전 정의된 맞춤형 테이블에서 오는 필드를 조합하는 맞춤형 테이블을 생성할 수 있습니다.

표 ***319:*** 맞춤형 테이블 조합

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
애플리케이션	• 상관 관계 이벤트 • 침입 이벤트 • 연결 요약 데이터 • 호스트 속성 • 애플리케이션 세부사항 • 검색 이벤트 • 호스트 • 서버 • 화이트 이벤트 나열
Correlation Events	• 애플리케이션 • 호스트 속성 • 호스트
침입 이벤트	• 애플리케이션 • 호스트 속성 • 호스트 • 서버
Connection Summary Data(연결 요약 데이터)	• 애플리케이션 • 호스트 속성 • 호스트 • 서버

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
보안 침해 지표	• 애플리케이션 • 애플리케이션 세부사항 • 캡처된 파일 • Connection Summary Data(연결 요약 데이터) • Correlation Events • 검색 이벤트 • 호스트 속성 • 호스트 • 침입 이벤트 • 보안 인텔리전스 이벤트 • 서버 • 화이트 이벤트 나열
호스트 속성	• 애플리케이션 • Correlation Events • 침입 이벤트 • Connection Summary Data(연결 요약 데이터) • 애플리케이션 세부사항 • 검색 이벤트 • 호스트 • 서버 • 화이트 이벤트 나열
애플리케이션 세부사항	• 애플리케이션 • 호스트 속성 • 호스트
검색 이벤트	• 애플리케이션 • 호스트 속성 • 호스트

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
보안 인텔리전스 이벤트	• 애플리케이션 • 호스트 속성 • 호스트 • 서버
호스트	• 애플리케이션 • Correlation Events • 침입 이벤트 • Connection Summary Data(연결 요약 데이터) • 호스트 속성 • 애플리케이션 세부사항 • 검색 이벤트 • 서버 • 화이트 이벤트 나열
서버	• 애플리케이션 • 침입 이벤트 • Connection Summary Data(연결 요약 데이터) • 호스트 속성 • 호스트
화이트 이벤트 나열	• 애플리케이션 • 호스트 속성 • 호스트

때때로 한 테이블의 한 필드가 또 다른 테이블의 둘 이상의 필드에 매핑됩니다. 예를 들어 사전 정의된 **Intrusion Events with Destination Criticality(**대상 중요도가 있는 침입 이벤트**)** 맞춤형 테이블은 Events(이벤트) 테이블과 Hosts(호스트) 테이블의 필드를 결합합니다. Intrusion Events(침입 이벤트) 테이블의 각 이벤트에는 두 개의 관련 IP 주소(소스 IP 주소 및 목적지 IP 주소)가 있습니다. 그러나 Hosts(호스트) 테이블의 "이벤트"는 각각 단일 호스트 IP 주소를 나타냅니다(호스트에 여러 IP 주소가 있을 수 있음). 따라서 Intrusion Events(침입 이벤트) 테이블과 Hosts(호스트) 테이블을 기반으로 맞춤형 테이블을 생성할 때에는 Hosts(호스트) 테이블에서 표시하는 데이터가 Intrusion Events(침입 이벤

트) 테이블의 호스트 소스 IP 주소 또는 호스트 목적지 IP 주소에 적용되는지 여부를 선택해야 합니다.

새 맞춤형 테이블을 생성하면 테이블의 모든 열을 표시하는 기본 워크플로가 자동으로 생성됩니다. 또한 사전 정의 테이블과 마찬가지로, 네트워크 분석에서 사용할 데이터에 대한 맞춤형 테이블을 검색할 수 있습니다. 사전 정의 테이블과 마찬가지로, 맞춤형 테이블을 기반으로 보고서를 생성할 수 있습니다.

사용자 정의 맞춤형 테이블

팁 새 맞춤형 테이블을 생성하는 대신, 다른 Firepower Management Center에서 맞춤형 테이블을 내보낸 다음 현재 Firepower Management Center로 가져올 수 있습니다.

맞춤형 테이블을 생성하려면, Firepower System과 함께 제공된 사전 정의 테이블 중 어떤 것에 맞춤형 테이블에 포함할 필드가 포함되어 있는지를 확인해야 합니다. 그런 다음, 포함하고자 하는 필드를 선택하고 필요한 경우 공통 필드에 대한 필드 매핑을 구성할 수 있습니다.

팁 Hosts(호스트) 테이블과 관련된 데이터에서는 하나의 특정 IP 주소보다는 한 호스트의 모든 IP 주소와 연결된 데이터를 볼 수 있습니다.

예를 들어 Correlation Events(상관관계 이벤트) 테이블과 Hosts(호스트) 테이블의 필드를 조합하는 맞춤형 테이블이 있다고 가정해보겠습니다. 이 맞춤형 테이블을 사용하면 상관관계 정책의 위반과 관련된 호스트에 대한 자세한 정보를 얻을 수 있습니다. Correlation Events(상관관계 이벤트) 테이블의 소스 IP 주소 또는 목적지 IP 주소와 일치하는 Hosts(호스트) 테이블의 데이터를 표시할지 여부를 결정해야 합니다.

이 맞춤형 테이블에 대한 이벤트를 테이블 보기로 보면 한 행에 하나씩 상관관계 이벤트가 표시됩니다. 다음 정보를 포함하도록 맞춤형 테이블을 설정할 수 있습니다.

- 이벤트가 생성된 날짜 및 시간
- 위반된 상관관계 정책의 이름
- 위반을 트리거한 규칙의 이름
- 상관관계 이벤트와 관련된 소스 또는 시작 호스트와 연결된 IP 주소
- 소스 호스트의 NetBIOS 이름
- 소스 호스트가 실행 중인 운영체제 및 버전
- 소스 호스트 중요도

팁 대상 또는 응답 호스트에 대한 동일한 정보를 표시하는 유사한 맞춤형 테이블을 생성할 수 있습니다.

맞춤형 테이블 생성

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**을(를) 선택합니다.

단계 **2** **Create Custom Table(**맞춤형 테이블 생성**)**을 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 맞춤형 테이블의 이름을 입력합니다.

예제**:**

예를 들어 `Correlation Events with Host Information (Src IP)`을 입력할 수 있습니다.

단계 **4** **Tables(**테이블**)** 드롭다운 목록에서 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.

단계 **5** **Fields(**필드**)**에서 **Time(**시간**)**을 선택하고 **Add(**추가**)**를 클릭하여 상관관계 이벤트가 생성된 날짜와 시간을 추가합니다.

단계 **6** 5단계를 반복하여 **Policy(**정책**)** 및 **Rule(**규칙**)** 필드를 추가합니다.

팁 여러 필드를 선택하려면 Ctrl 또는 Shift 키를 누른 상태에서 클릭합니다. 클릭하고 드래그하여 인접한 여러 값을 선택할 수도 있습니다. 그러나 테이블과 연결된 이벤트의 테이블 보기에 필드가 나타나는 순서를 지정하려면, 필드를 한 번에 하나씩 추가해야 합니다.

단계 **7** **Tables(**테이블**)** 드롭다운 목록에서 **Hosts(**호스트**)**를 선택합니다.

단계 **8** 맞춤형 테이블에 **IP Address(IP** 주소**)**, **NetBIOS Name(NetBIOS** 이름**)**, **OS Name(**운영체제 이름**)**, **OS Version(**운영체제 버전**)** 및 **Host Criticality(**호스트 중요도**)** 필드를 추가합니다.

단계 **9** **Common Fields(**공통 필드**)** 아래의 **Correlation Events(**상관관계 이벤트**)** 옆에 있는 **Source IP(**소스 **IP)**를 선택합니다.

상관관계 이벤트와 관련된 소스 또는 시작 호스트에 대해 8단계에서 선택한 호스트 정보를 표시하도록 맞춤형 테이블이 구성됩니다.

팁 이 절차를 수행하되 **Source IP(**소스 **IP)** 대신 **Destination IP(**목적지 **IP)**를 선택하여, 상관관계 이벤트와 관련된 대상 또는 응답 호스트에 대한 자세한 호스트 정보를 표시하는 맞춤형 테이블을 생성할 수 있습니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

맞춤형 테이블 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며 이러한 테이블은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 수정

할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**를 선택합니다.

단계 **2** 편집하려는 테이블 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 선택적으로, 제거하려는 필드 옆에 있는 삭제( )을 클릭하여 테이블에서 필드를 제거합니다.

참고 보고서에 현재 사용되고 있는 필드를 삭제하는 경우, 해당 보고서에서 해당 필드를 사용하는 섹션을 제거할 것인지 묻는 메시지가 표시됩니다.

단계 **4** 필요에 따라 다른 변경사항을 적용합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

맞춤형 테이블 삭제

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며, 이러한 테이블은 삭제할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 삭제할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 삭제하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**을(를) 선택합니다.

단계 **2** 삭제하고자 하는 맞춤형 테이블 옆에 있는 아이콘(삭제( ))을 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

맞춤형 테이블 기반 워크플로 보기

맞춤형 테이블을 생성하면 시스템은 자동으로 이에 대한 기본 워크플로를 생성합니다. 이 워크플로의 첫 번째 페이지에는 이벤트의 테이블 보기가 표시됩니다. 맞춤형 테이블에 침입 이벤트를 포함하면 워크플로의 두 번째 페이지는 패킷 보기 페이지가 됩니다. 그렇지 않으면 워크플로의 두 번째 페

이지는 호스트 페이지가 됩니다. 맞춤형 테이블을 기반으로 고유한 맞춤형 워크플로를 생성할 수도 있습니다.

팁 맞춤형 테이블을 기반으로 맞춤형 워크플로를 만드는 경우이를 해당 테이블의 기본 워크플로로 지정할 수 있습니다.

사전 정의 테이블을 기반으로 이벤트 보기에 대해 사용하는 맞춤형 테이블에서 이벤트를 보려면 이 방법을 사용할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며 이러한 테이블은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**을(를) 선택합니다.

단계 **2** 확인할 워크플로와 관련된 맞춤형 테이블 옆에 있는 보기 ( )을 클릭합니다.

맞춤형 테이블 검색

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며 이러한 테이블은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**를 선택합니다.

단계 **2** 검색할 맞춤형 테이블 옆에 있는 보기 ( )을 클릭합니다.

팁 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **3** **Search(**검색**)**를 클릭합니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트 또는 데이터를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

단계 **4** 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

팁 검색 기준으로 개체를 사용하려면 검색 필드 옆에 있는 개체( )을 클릭합니다.

단계 **5** 선택적으로, 검색을 저장하려면 **Private(**비공개**)** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 마십시오.

팁 사용자 지정 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다.

단계 **6** 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save(**저장**)**를 클릭합니다. **Private(**비공개**)** 확인란을 선택해야 검색이 계정에 표시됩니다.
- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New(**신규로 저장**)**를 클릭합니다. **Private(**비공개**)** 확인란을 선택해야 검색이 저장되고 계정에 표시됩니다.

단계 **7** 검색을 시작하려면 **Search(**검색**)**를 클릭합니다.

검색 결과가 현재 시간과 범위로 제한되어(적용 가능한 경우) 맞춤형 테이블에 대한 기본 워크플로에 나타납니다.

맞춤형 테이블 기록

기능	버전	세부 사항
맞춤형 테이블의 연결 이벤트 지원은 삭제되었습니다.	6.6	이제 연결 이벤트가 포함된 맞춤형 테이블을 생성할 수 없습니다. 6.6 버전으로 업그레이드한 경우: 연결 이벤트가 있는 기존 테이블은 사용되지 않음으로 표시되며 데이터가 표시되지 않고 테이블을 내보내거나 편집할 수 없습니다. 기존 보고서, 맞춤형 워크플로, 대시보드가 사용되지 않는 테이블을 포함할 수 있으며 사용자는 이를 검토할 수 있습니다. 수정된 화면: **Analysis(**분석**) > Advanced(**고급**) > Custom Tables(**맞춤형 테이블**)**과 맞춤형 테이블 추가 및 편집 페이지 영향을 받는 플랫폼: FMC

XXV 부

이벤트 및 자산

- 연결 로깅, 2859 페이지
- 연결 및 보안 인텔리전스 이벤트, 2875 페이지
- 침입 이벤트 작업, 2909 페이지
- 파일/악성코드 이벤트 및 네트워크 파일 경로 분석, 2963 페이지
- 호스트 프로파일 사용, 3001 페이지
- 검색 이벤트 작업, 3031 페이지
- 상관관계 및 규정 준수 이벤트, 3093 페이지

120 장

연결 로깅

다음 주제에서는 모니터링하는 네트워크 상의 호스트가 실행한 연결을 기록하도록 Firepower System을 설정하는 방법을 설명합니다.

- 연결 로깅 정보, 2859 페이지
- 연결 로깅 제한사항, 2867 페이지
- 연결 로깅 모범 사례, 2868 페이지
- 연결 로깅 요구 사항 및 사전 요건, 2870 페이지
- 연결 로깅 설정, 2870 페이지

연결 로깅 정보

시스템은 자신의 매니지드 디바이스가 탐지한 연결의 로그를 생성할 수 있습니다. 이러한 로그를 연결 이벤트라고 합니다. 규칙 및 정책의 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다. *Security Intelligence(*보안 인텔리전스*)* 이벤트라는 특수한 연결 이벤트는 평판 기반 Security Intelligence(보안 인텔리전스) 기능이 차단한 연결을 나타냅니다.

연결 이벤트에는 탐지된 세션에 관한 데이터가 포함되어 있습니다. 모든 개별 연결 이벤트에 대한 정보는 몇 가지 요소에 따라 가용성이 결정되지만, 일반적으로는 다음과 같습니다.

- 기본 연결 속성: 타임 스탬프, 소스 및 대상 IP 주소, 인그레스 및 이그레스 영역, 연결을 처리한 디바이스 등
- 시스템에서 검색하거나 유추한 추가 연결 속성: 애플리케이션, 요청된 URL 또는 연결과 관련된 사용자 등
- 연결이 로깅된 사유에 대한 메타데이터: 어떤 설정이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지, 암호화 및 해독된 연결에 대한 상세정보 등

조직의 보안 및 컴플라이언스 요구 사항에 따라 연결을 로깅해야 합니다. 연결 로깅을 설정할 때는 시스템이 여러 가지 이유로 연결을 로깅할 수 있으며, 따라서 한 곳의 로깅을 비활성화해도 일치하는 연결이 로깅되지 않는 것은 아님을 유의하십시오.

연결 이벤트에 있는 정보는 트래픽 특성, 연결을 마지막으로 처리한 설정 등의 다양한 요소에 따라 달라집니다.

참고 내보낸 NetFlow 기록에서 생성한 연결 데이터를 이용해, 매니지드 디바이스가 수집한 연결 로그를 보완할 수 있습니다. 이는 Firepower System 매니지드 디바이스가 모니터링할 수 없는 네트워크에서 NetFlow 지원 라우터 또는 기타 디바이스를 구축한 경우에 특히 유용합니다.

관련 항목

Firepower System의 Netflow 데이터, 2381 페이지

항상 로깅되는 연결

연결 이벤트 스토리지를 비활성화하지 않는 한, 시스템은 다른 로깅 설정과 관계없이 다음의 연결 종료 이벤트를 Firepower Management Center 데이터베이스에 자동으로 저장합니다.

침입과 연관된 연결

시스템은 연결이 액세스 제어 정책의 기본 작업에 의해 처리되지 않는 한, 침입 이벤트와 연관된 연결을 자동으로 로깅합니다.

액세스 제어 기본 작업과 관련된 침입 정책이 침입 이벤트를 생성할 때 시스템은 결합된 연결의 종료를 자동으로 로깅하지 않습니다. 대신, 사용자는 반드시 기본 작업 연결 로깅을 명시적으로 활성화해야 합니다. 이는 사용자가 연결 데이터를 로깅하는 것을 원하지 않을 때 침입 방지 전용 배포에 유용합니다.

그러나 기본 작업에 대한 연결 시작 로깅을 활성화하면, 시스템은 연결의 시작을 로깅하는 것 이외에도 관련 침입 정책이 작동을 이끌어낼 때 연결 종료를 분명히 로깅합니다.

파일 및 악성코드 이벤트와 연관된 연결

시스템은 파일 및 악성코드 이벤트와 연관된 연결을 자동으로 로깅합니다.

참고 클라이언트와 서버에 지속적인 연결이 설정되어 있기 때문에 NetBIOS-SSN(SMB) 트래픽 검사에 의해 생성된 파일 이벤트가 즉시 연결 이벤트를 생성하지는 않습니다. 시스템은 클라이언트 또는 서버가 세션을 종료한 후 연결 이벤트를 생성합니다.

지능형 애플리케이션 우회와 연관된 연결

시스템은 우회했거나 우회했을 가능성이 있는 IAB 관련 연결을 자동으로 로깅합니다.

모니터링되는 연결

트래픽이 다른 어느 규칙과도 일치하지 않고 기본 작업 로깅을 사용자가 활성화하지 않은 경우에도, 시스템은 모니터링되는 트래픽의 연결 종료를 로깅합니다. 자세한 내용은 모니터링된 연결에 대한 로깅, 2862 페이지를 참고하십시오.

로깅할 수 있는 기타 연결

중요한 연결만 로깅하려면 규칙별로 연결 로깅을 활성화합니다. 규칙에 대한 연결 로깅을 활성화할 경우, 시스템은 해당 규칙에서 처리하는 모든 연결을 로깅합니다.

정책 기본 작업이 처리하는 연결을 로깅할 수도 있습니다. 규칙 또는 기본 작업(액세스 제어의 경우, 규칙의 검사 설정)에 따라 로깅 옵션이 달라집니다.

SSL 정책**:** 규칙 및 기본 작업

SSL 규칙 또는 SSL 정책 기본 작업과 일치하는 연결을 로깅할 수 있습니다.

차단된 연결의 경우 시스템에서 즉시 세션을 종료하고 이벤트를 생성합니다. 모니터링된 연결 및 액세스 제어 규칙으로 전달하는 연결의 경우 시스템에서 세션 종료 시 이벤트를 생성합니다.

액세스 제어 정책**:** 보안 인텔리전스 결정

평판 기능 보안 인텔리전스 기능에 의해 연결이 차단될 때마다 해당 연결을 로깅할 수 있습니다.

원한다면 보안 인텔리전스 필터링에 모니터 한정 설정을 사용할 수 있으며, 이는 수동 구축에서 권장됩니다. 이를 통해 시스템은 차단되었을 수도 있지만 여전히 일치를 로깅하는 연결을 추가로 분석할 수 있습니다. 보안 인텔리전스 모니터링을 사용하면 또한 사용자가 보안 인텔리전스 정보를 사용하여 트래픽 프로파일을 작성할 수 있습니다.

보안 인텔리전스 필터링의 결과로 연결 이벤트를 로깅할 때 시스템은 일치하는 보안 인텔리전스 이벤트도 로깅합니다. 이 이벤트는 사용자가 별도로 보고 분석할 수 있는 특수한 연결 이벤트이며 별도로 저장되고 잘립니다. 연결에서 일치하는 IP 주소를 식별할 수 있도록 **Analysis(**분석**)** > **Connections(**연결**)** 메뉴 아래 페이지의 테이블에서 차단된 IP 주소 옆의 호스트 아이콘과 모니터링되는 IP 주소 옆의 호스트 아이콘은 약간 다르게 보입니다.

액세스 제어 정책**:** 규칙 및 기본 작업

액세스 제어 규칙 또는 액세스 제어 정책 기본 작업과 일치하는 연결을 로깅할 수 있습니다.

관련 항목

규칙 및 정책 작업이 로깅에 미치는 영향, 2861 페이지

규칙 및 정책 작업이 로깅에 미치는 영향

연결 이벤트에는 어느 구성이 트래픽을 처리했는지를 포함하여 연결이 로깅된 이유에 관한 메타데이터가 포함됩니다. 연결 로깅, 규칙 작업, 정책 기본 작업을 구성할 수 있는 경우, 시스템이 일치하는 트래픽을 검사하고 처리하는 방법뿐 아니라 일치하는 트래픽에 대한 상세정보를 로깅할 수 있는 시기와 방법도 결정하십시오.

관련 항목

TLS/SSL 규칙 작업, 1819 페이지
액세스 제어 규칙 작업, 1658 페이지
연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지

모니터링된 연결에 대한 로깅

트래픽이 다른 어느 규칙과도 일치하지 않고 기본 작업 로깅을 사용자가 활성화하지 않은 경우에도 시스템은 항상 다음 구성과 일치하는 트래픽의 연결 종료를 로깅합니다.

- 보안 인텔리전스 — 모니터링(또한 보안 인텔리전스도 생성)하도록 설정된 차단 목록
- SSL 규칙 — 모니터링 작업
- 액세스 제어 규칙 — 모니터링 작업

시스템은 단일 연결이 모니터 규칙과 일치할 때마다 별도의 이벤트를 생성하지 않습니다. 단일 연결이 여러 모니터 규칙과 일치할 수 있으므로 각 연결 이벤트는 일치하는 첫 번째 SSL 모니터 규칙뿐 아니라 연결과 일치하는 처음 8개의 모니터 액세스 제어 규칙에 대한 정보를 포함하고 표시합니다.

마찬가지로, 사용자가 외부 syslog 또는 SNMP 트랩 서버에 연결 이벤트를 보낼 경우, 시스템은 단일 연결이 모니터링 규칙에 일치할 때마다 별도의 경고를 보내지는 않습니다. 그보다, 연결 종료 시 시스템이 보내는 경고는 연결과 일치하는 모니터링 규칙에 관한 정보를 포함합니다.

신뢰할 수 있는 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하는 신뢰할 수 있는 연결의 시작과 종료를 로깅할 수 있습니다.

- 액세스 제어 규칙 — 신뢰 작업
- 액세스 제어 기본 작업 — 모든 트래픽 신뢰

참고 신뢰할 수 있는 연결을 로깅할 수 있더라도 로깅하지 않는 것이 좋습니다. 신뢰할 수 있는 연결은 심층 검사 또는 검색 대상이 아니므로 신뢰할 수 있는 연결 이벤트에는 제한된 정보가 포함되어 있기 때문입니다.

첫 번째 패킷의 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

시스템은 신뢰 액세스 제어 규칙이 처리하는 TCP 연결을 연결을 탐지한 디바이스에 따라 다르게 로깅합니다.

- 7000 및 8000 Series 디바이스의 경우, 첫 번째 패킷에서 신뢰 규칙에 의해 탐지된 TCP 연결은 선행 활성 모니터 규칙의 유무에 따라 다른 이벤트를 생성합니다. 모니터 규칙이 활성 상태일 경우, 시스템은 패킷을 평가하고 연결 시작 및 종료 이벤트를 모두 생성합니다. 활성 상태의 모니터 규칙이 없을 경우, 시스템은 연결 종료 이벤트만 생성합니다.
- 그 밖의 모든 모델에서는 첫 번째 패킷에서 신뢰 규칙에 의해 탐지된 TCP 연결이 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

차단된 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하는 차단된 연결을 로깅할 수 있습니다.

- 보안 인텔리전스 - 모니터링(보안 인텔리전스 이벤트도 생성)하도록 설정되지 않은 차단 목록
- SSL 규칙 — 차단 및 차단 후 재설정
- SSL 기본 작업 — 차단 및 차단 후 재설정
- 액세스 제어 규칙 — 차단, 차단 후 재설정, 인터랙티브 차단
- 액세스 제어 기본 작업 — 모든 트래픽 차단

인라인이 구축된(즉, 라우팅, 스위칭 또는 투명 인터페이스 혹은 인라인 인터페이스 페어링을 사용하는) 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다.

주의 DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. Block(차단) 규칙에 대한 로깅을 활성화하기 전에, 해당 규칙이 인터넷에 연결된 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하고 있는지 여부를 고려하시기 바랍니다.

차단된 연결의 연결 시작 또는 종료 로깅

차단된 연결을 로깅할 때 그 로깅 방식은 연결이 차단된 이유에 따라 달라집니다. 연결 로그를 기반으로 상관관계 규칙을 구성할 때 이 점을 기억해야 합니다.

- 암호화된 트래픽을 차단하는 SSL 규칙 및 SSL 정책 기본 작업의 경우, 연결 종료 이벤트가 로깅됩니다. 이는 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없기 때문입니다.
- 다른 차단 작업은 연결 시작 이벤트가 로깅됩니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.

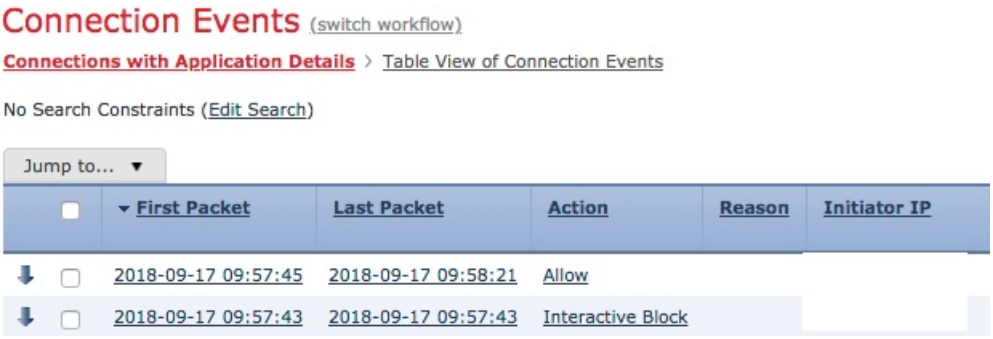
우회된 인터랙티브 차단 로깅

사용자가 금지된 웹사이트로 이동할 때 경고 페이지가 표시되도록 하는 인터랙티브 차단 액세스 제어 규칙을 사용하여 연결 종료 로깅을 구성할 수 있습니다. 이는 사용자가 경고 페이지를 클릭할 경우, 이 연결은 시스템이 모니터링 및 로깅할 수 있는 새롭게 허용된 연결로 간주되기 때문입니다.

따라서 인터랙티브 차단 또는 인터랙티브 차단 후 재설정 규칙과 일치하는 패킷의 경우, 시스템은 다음 연결 이벤트를 생성할 수 있습니다.

- 사용자 요구가 초기에 차단되고 경고 페이지가 표시되는 연결 시작 이벤트. 이 이벤트에는 `인터랙티브 차단` 또는 `인터랙티브 차단 후 재설정`이라는 연결된 작업이 있습니다.
- 사용자가 경고 페이지를 통해 클릭하고 원래 요청된 페이지를 로드하는 경우, 다중 연결 시작 또는 종료 이벤트. 이 이벤트에는 `허용` 및 `사용자 우회`의 이유라는 연결된 작업이 있습니다.

  다음 그림은 허용 다음의 인터랙티브 차단의 예를 보여줍니다.


Connection Events (switch workflow)

Connections with Application Details › Table View of Connection Events

No Search Constraints (Edit Search)

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP
	2018-09-17 09:57:45	2018-09-17 09:58:21	Allow		
	2018-09-17 09:57:43	2018-09-17 09:57:43	Interactive Block		

허용된 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하 허용된 연결을 로깅할 수 있습니다.

- SSL 규칙 —**Decrypt(**암호 해독**)** 작업
- SSL 규칙 —**Do not decrypt(**암호 해독 안 함**)** 작업
- SSL 기본 작업—**Do not decrypt(**암호 해독 안 함**)**
- 액세스 제어 규칙—**Allow(**허용**)** 작업
- 액세스 제어 기본 작업 —**Network Discovery Only(**네트워크 검색 전용**)** 및 침입 방지 옵션

이러한 구성에 대한 로깅을 활성화하면 연결이 기록되며 다음 단계인 검사 및 트래픽 처리를 허가(또는 지정)합니다. SSL 로깅 시 항상 연결이 종료되며, 액세스 제어 구성에서 연결 시작 로깅을 다시 할 수 있습니다.

액세스 제어 규칙 또는 기본 작업을 사용하여 트래픽을 허용하는 경우, 연결된 침입 정책을 사용하여 트래픽을 추가 검사하고 침입을 차단할 수 있습니다. 액세스 제어 규칙의 경우, 파일 정책을 사용하여 악성코드를 비롯한 금지된 파일을 탐지하고 차단할 수도 있습니다. 연결 이벤트 스토리지를 비활성화하지 않으면 시스템은 침입, 파일, 악성코드 이벤트에 연결된 허용되는 연결 대부분을 자동으로 로깅합니다. 자세한 내용은 항상 로깅되는 연결, 2860 페이지를 참조하십시오.

암호화된 페이로드와의 연결은 심층 검사 대상이 아니므로 암호화된 연결의 연결 이벤트에는 제한된 정보가 포함되어 있습니다.

허용된 연결에 대한 파일 및 악성코드 이벤트 로깅

파일 정책이 파일을 탐지하거나 차단하면 다음 이벤트 중 하나를 Firepower Management Center 데이터베이스에 로깅합니다.

- 파일 이벤트 - 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냅니다.
- 악성코드 이벤트 - 탐지되거나 차단된 악성코드 파일만 나타냅니다.
- 회귀적 악성코드 이벤트 - 이전에 탐지된 파일에 대한 악성코드 속성이 변경되는 경우 생성됩니다.

액세스 제어 규칙마다 이 로깅을 비활성화할 수 있습니다. 파일 및 악성코드 이벤트 스토리지를 완전히 비활성화할 수도 있습니다.

참고 파일 및 악성코드 이벤트 로깅 활성화를 유지하는 것이 좋습니다.

연결 시작 또는 종료 로깅

연결은 시작 또는 종료 시에 로깅할 수 있으며, 차단된 트래픽의 경우에는 다음 예외가 적용됩니다.

- 차단된 트래픽 - 차단된 트래픽은 추가 검사 없이 즉시 거부되기 때문에, 일반적으로는 차단된 트래픽의 연결 시작 이벤트만 로깅할 수 있습니다. 로깅할 고유 연결 종료는 존재하지 않습니다.
- 블랙리스트에 포함된 암호화된 트래픽-SSL 정책에서 연결 로깅을 활성화하면 연결 시작이 아닌 연결 종료가 로깅됩니다. 이는 시스템에서 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없고 따라서 즉시 암호화 세션을 차단할 수 없기 때문입니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다. 어떤 이유로든 연결을 모니터링하면 반드시 연결 종료가 로깅됩니다. 차단되지 않은 단일 연결의 경우 연결 종료 이벤트는 연결 시작 이벤트의 모든 정보 및 세션 과정에서 수집된 정보를 포함합니다.

다음 표에서는 연결 시작 및 연결 종료 이벤트의 차이점과 각 로깅의 장점을 설명합니다.

표 ***320:*** 연결 시작 이벤트와 연결 종료 이벤트 비교

	연결 시작 이벤트	연결 종료 이벤트
생성 가능 대상	연결 시작이 탐지될 때(또는 애플리케이션이나 URL 식별에 따라 이벤트가 생성되는 경우 처음 몇 개의 패킷 이후에)	시스템이 다음을 수행하는 경우 • 연결 차단을 탐지하는 경우 • 일정 시간이 지난 후 연결 종료를 탐지하지 않는 경우 • 메모리 제약 조건 때문에 더 이상 세션을 추적할 수 없는 경우
로깅 가능 대상	SSL 정책에 의해 차단된 연결을 제외한 모든 연결	대부분의 연결
포함 대상	첫 번째 패킷(또는 이벤트 생성이 애플리케이션 또는 URL ID에 의존하는 경우 처음 몇 패킷)에서 확인될 수 있는 정보만	연결 시작 이벤트의 모든 정보와 세션 기간에 트래픽을 검사하여 확인한 정보(예: 총 데이터 전송량, 연결의 마지막 패킷의 타임스탬프)

	연결 시작 이벤트	연결 종료 이벤트
유용한 경우	다음을 로깅하려는 경우 • 차단된 연결 • 연결 종료 정보가 사용자에게 상관 없기 때문에 연결의 시작 한정	다음을 원하는 경우 • SSL 정책이 처리한 암호화된 연결을 로깅하려는 경우 • 세션 기간 동안 수집된 정보에 관한 모든 종류의 상세 분석 작업을 수행하거나, 해당 정보를 사용하여 상호 규칙을 이끌어내려는 경우 • 연결 개요(집계된 연결 데이터)를 살펴보고, 그래픽 형식으로 연결 데이터를 살펴보기 트래픽 프로파일을 만들고 사용하려는 경우

Firepower Management Center 대 외부 로깅

연결 및 Security Intelligence(보안 인텔리전스) 이벤트 로그를 Firepower Management Center에 저장하는 경우, Firepower System의 보고, 분석, 데이터 상관광계 기능을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- 대시보드 및 컨텍스트 탐색기에서는 시스템에서 로깅한 연결을 그래픽 화면에서 한눈에 볼 수 있습니다.
- 이벤트 보기(Analysis(분석) 메뉴에서 사용할 수 있는 대부분의 옵션)는 시스템이 로깅한 연결에 대한 상세정보를 제공하며, 이러한 정보는 그래프 또는 표 형식 포맷으로 표시하거나 보고서로 요약할 수 있습니다.
- 트래픽 프로파일에서는 정상적인 네트워크 트래픽에 대한 프로파일을 생성하는 데 연결 데이터를 사용합니다. 그런 다음 이 프로파일을 비정상적인 동작을 탐지하고 추적하는 데 기준으로 사용할 수 있습니다.
- 상관관계 정책에서는 특정 유형의 연결 또는 트래픽 프로파일 변경에 대한 이벤트를 생성하고 응답(예: 알림, 외부 교정)을 트리거할 수 있습니다.

Firepower Management Center에서 저장할 수 있는 이벤트 숫자는 모델에 따라 달라집니다.

참고 이 기능을 사용하려면 반드시 연결을 (대부분의 경우에는 연결 시작이 아닌 연결 종료를) 로깅해야 합니다. 따라서 중요한 연결, 즉 로깅된 침입, 금지된 파일, 악성코드와 관련된 연결은 자동으로 로깅됩니다.

다음을 사용하여 외부 시스템 로그나 SNMP 트랩 서버 또는 다른 외부 툴에 이벤트를 로깅할 수도 있습니다.

- 모든 디바이스에서 외부 로깅:

  설정한 연결은 경고 응답이라고 합니다.

- FTD 디바이스에서 외부 로깅:

  시스템 로그 구성 관련 정보, 1445 페이지 및 SNMP 트랩 구성, 1442 페이지를 참조하십시오.

- 외부 로깅과 관련된 추가 옵션:

  외부 툴을 사용하여 이벤트 분석, 2749 페이지의 내용을 참조하십시오.

관련 항목

Firepower Management Center 알림 응답, 2681 페이지

연결 로깅 제한사항

다음 항목은 로깅할 수 없음:

- 8000 Series 단축 경로 규칙으로 단축 경로가 지정된 연결
- 일반 텍스트의 외부 세션, 캡슐화된 연결이 액세스 제어로 검사되는 통과 터널
- 3방향 핸드셰이크가 완료되지 않은 경우의 TCP 연결입니다.

  이러한 연결은 실행 시 Firepower 구축에 대한 서비스 거부 공격의 기회를 제공할 것으로 로깅되지는 않습니다.

  그러나 다음 해결 방법을 사용하여 실패한 연결을 모니터링하거나 디버깅할 수는 있습니다.

  - 명령줄 인터페이스에서 **show asp drops** 사용 명령을 사용합니다.

연결 이벤트에 있어야 할 정보가 존재하지 않는다면, 연결 이벤트 필드 채우기 요구 사항, 2895 페이지 및 연결 이벤트 필드에서 제공되는 정보, 2896 페이지 섹션을 참조하십시오.

이벤트가 이벤트 뷰어에 표시되는 경우

다음 내용은 모든 유형의 이벤트에 적용됩니다.

- Analysis(분석) 메뉴의 페이지를 찾는 경우에는 페이지를 새로고침해야 새 이벤트가 표시됩니다.
- 일반적으로 이벤트는 트래픽이 탐지된 시점에서 몇 초 이내에 확인할 수 있습니다. 그러나 외부의 과도한 트래픽 조건, 낮은 대역폭 네트워크에서 많은 디바이스를 관리하는 FMC, 이벤트 백업 등의 작업 중에 이벤트 처리가 일시 중지되는 등의 상황에서는 임의 지연이 발생할 수 있습니다.

연결 로깅 모범 사례

로깅하려는 연결만 로깅하려면 다음 모범 사례를 사용하십시오.

중요한 연결만 로깅하려면 액세스 제어 규칙별로 연결 로깅을 활성화합니다.

항상 로깅되는 연결

시스템이 자동으로 다음을 로깅합니다.

- 탐지된 파일, 악성코드, 침입, Intelligent Application Bypass(IAB)와 관련된 일부 연결.

  자세한 내용은 항상 로깅되는 연결, 2860 페이지를 참고하십시오.

- 모니터링되는 연결.

  자세한 내용은 모니터링된 연결에 대한 로깅, 2862 페이지를 참고하십시오.

로깅하지 않을 연결

다음에 대한 로깅을 활성화하지 마십시오.

- 신뢰 작업이 포함된 액세스 제어 규칙.

  신뢰할 수 있는 연결은 심층 검사 또는 검색 대상이 아니므로 신뢰할 수 있는 연결 이벤트에는 제한된 정보가 포함되어 있습니다.

- 수동 구축에서 차단 규칙에 대한 로깅을 활성화하지 마십시오. 디바이스가 인라인으로 구축되었다면 시스템이 차단했을 연결을 로깅하려면 차단 규칙 대신 모니터링 규칙을 사용합니다.

  인라인이 구축된(즉, 라우팅, 스위칭 또는 투명 인터페이스 혹은 인라인 인터페이스 페어링을 사용하는) 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다.

- 관심이 없는 트래픽. 예는 다음과 같습니다.
  - 신뢰할 수 있는 DNS 호스트에 대한 DNS 요청과 같은 허용되는 특정 트래픽.
  - 서비스 솔루션과 관련이 없는 인프라 트래픽.

  (앞서 언급했듯이 이 트래픽에서 위협을 계속 모니터링할 수 있습니다.)

항상 로깅되는 연결, 2860 페이지에서 설명한 것처럼 위 항목에 대한 로깅을 비활성화하더라도 침입 이벤트, 악성코드, IAB는 여전히 로깅됩니다.

다른 곳에서 로깅되는 것은 로깅하지 마십시오.

다른 디바이스 또는 서비스가 네트워크 세그먼트의 연결 데이터를 로깅하고 있는 경우, Firepower Management Center에서 해당 세그먼트의 데이터에 대한 로깅을 비활성화합니다. 예는 다음과 같습니다.

- 라우터가 Firepower Management Center와 동일한 네트워크 세그먼트에서 연결 이벤트를 로깅하는 경우, 상관관계 정책 또는 트래픽 프로파일 같은 다른 목적으로 이러한 연결 이벤트를 로깅해야 하는 경우가 아니라면 Firepower Management Center에서 동일한 연결을 로깅하지 마십시오.

  상관관계 정책에 대한 자세한 내용은 상관관계 정책 및 규칙 소개, 2583 페이지를 참조하십시오. 트래픽 프로파일에 대한 자세한 내용은 트래픽 프로파일 소개, 2623 페이지의 내용을 참조하십시오.

- Stealthwatch를 사용하여 스위치와 라우터에서 보고되는 NetFlow 레코드를 활용해 잠재적인 동작 이상 징후와 의심스러운 트래픽 패턴을 식별하는 경우, 이러한 세그먼트를 모니터링하는 규칙에 대한 연결 로깅을 비활성화하고 대신 네트워크의 해당 부분에 대한 동작 분석을 Stealthwatch에 의존할 수 있습니다.

  자세한 내용은 Stealthwatch 설명서를 참조하십시오.

연결의 시작 또는 종료를 로깅합니다**(**둘 다가 아니라**).**

연결 시작 또는 종료 로깅 중에서 선택할 수 있는 경우, 연결 종료 로깅을 활성화합니다. 이것은 연결 종료가 세션 기간 동안 수집된 정보뿐 아니라 연결 시작 이벤트의 정보도 로깅하기 때문입니다.

차단된 연결을 로깅하려고 하거나 연결 종료 정보가 중요하지 않은 경우에만 연결 시작을 로깅하십시오.

자세한 내용은 연결 시작 또는 종료 로깅, 2865 페이지를 참고하십시오.

차단된 트래픽에 대한 로깅

차단된 트래픽은 추가 검사 없이 즉시 거부되기 때문에 일반적으로는 연결 시작 이벤트만 로깅할 수 있습니다.

자세한 내용은 차단된 연결에 대한 로깅, 2863 페이지를 참고하십시오.

외부 위치에 이벤트 로깅

회사 보안 정책에서 허용하는 경우, 다음 중 하나를 사용하여 로그를 외부 소스에 스트리밍하면 Firepower Management Center에서 디스크 공간을 절약할 수 있습니다.

- Firepower Management Center 또는 7000 또는 8000 시리즈 디바이스에서 맞춤 개발된 클라이언트 애플리케이션으로 로그를 스트리밍할 수 있는 eStreamer입니다. 자세한 내용은 *Firepower eStreamer* 통합 가이드를 참조하십시오.
- 알림 응답이라고 하는 Syslog 또는 SNMP 트랩. 자세한 내용은 Firepower Management Center 알림 응답, 2681 페이지를 참고하십시오.

이벤트 레코드의 최대 수를 지정합니다.

데이터베이스에 저장될 수 있는 레코드의 최소 및 최대 수를 고려하십시오. 예를 들어 가상 Firepower Management Center는 기본적으로 천만 개의 이벤트를 저장하지만 이벤트 최대 수는 5천만 개입니다. **System(**시스템**)** > **Configuration(**구성**)** > **Database(**데이터베이스**)**로 이동하여 필요에 맞게 크기를 조정하십시오.

모든 Firepower Management Center 모델 목록과 이벤트 데이터베이스 크기는 데이터베이스 이벤트 제한 수, 1351 페이지의 내용을 참조하십시오.

연결 이벤트에 표시되는 항목 제어

연결 이벤트에 표시되는 행 수를 지정하려면 Firepower Management Center 오른쪽 상단에서 사용자 이름을 클릭하고 **User Preferences(**사용자 환경 설정**)** > **Event View Settings(**이벤트 보기 설정**)**를 클릭합니다. 페이지당 최대 1,000개의 이벤트를 설정할 수 있습니다.

연결 이벤트 보고서 설정

연결 이벤트가 누락되지 않도록 .csv 형식의 자동화된 보고서를 설정하여 필요에 따라 일정한 간격으로 생성되도록 예약할 수 있습니다. 자세한 내용은 다음을 참고하십시오.

- 리포트 디자이너(**Analysis(**분석**)** > **Connection(**연결**)** > **Events(**이벤트**)** > **Report Designer(**리포트 디자이너**)**): 보고서 템플릿 생성, 2655 페이지 사용.
- 작업 예약(**System(**시스템**)** > **Tools(**도구**)** > **Scheduling(**예약**)**): 작업 예약 관련 정보, 245 페이지.

연결 로깅 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

연결 로깅 설정

다음 섹션에서는 다양한 규칙 및 조건에 맞게 연결 로깅을 설정하는 방법을 설명합니다.

SSL 규칙으로 암호 해독 가능 연결 로깅

SSL 규칙은 NGIPSv 디바이스에 적용되지 않습니다.

프로시저

단계 **1** SSL 정책 편집기에서 로깅을 설정하려는 규칙 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **2** **Logging(**로깅**)**을 클릭합니다.

단계 **3** **Log at End of Connection(**연결 종료 시 로깅**)** 확인란을 선택합니다.

모니터링되는 트래픽의 경우, 연결 종료 로깅이 필요합니다.

단계 **4** 연결 이벤트를 전송할 위치를 지정합니다.

이러한 연결 이벤트에서 Firepower Management Center 기반의 분석을 수행하려는 경우 이벤트 뷰어로 이벤트를 전송합니다. 이것은 모니터링되는 트래픽의 경우에 필요합니다.

단계 **5** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

보안 인텔리전스로 연결 로깅

보안 인텔리전스 정책에는 Threat Smart 라이선스 또는 Protection Classic 라이센스가 필요합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

단계 **2** 로깅( )을 클릭하여 다음 기준을 바탕으로 Security Intelligenge(보안 인텔리전스) 로깅을 활성화합니다.

- IP 주소 기준 - **Networks(**네트워크**)** 옆에 있는 로깅을 클릭합니다.
- URL 기준 - **URLs** 옆에 있는 로깅을 클릭합니다.
- 도메인 이름 기준 - **DNS Policy(DNS** 정책**)** 드롭다운 목록 옆에 있는 로깅을 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Log Connections(**로그 연결**)** 확인란을 선택합니다.

단계 **4** 연결 및 보안 인텔리전스 이벤트를 전송할 위치를 지정합니다.

Firepower Management Center 기반 분석을 수행하거나 차단 목록에 있는 개체를 모니터링 전용으로 설정하려면, 이벤트를 이벤트 뷰어로 전송합니다.

단계 **5** **OK(**확인**)**를 클릭하여 로깅 옵션을 설정합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

액세스 제어 규칙으로 연결 로깅

어떤 규칙 작업 및 심층 검사 옵션을 선택했는가에 따라 로깅 옵션이 달라집니다(규칙 및 정책 작업이 로깅에 미치는 영향, 2861 페이지 참조).

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 로깅을 구성하려는 규칙 옆에 있는 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **2** **Logging(**로깅**)** 탭을 클릭합니다.

단계 **3** **Log at Beginning of Connection(**연결 시작 시 로그**)** 또는 **Log at End of Connection(**연결 종료 시 로그**)** 중 원하는 로그 방식을 선택합니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다.

단계 **4** (선택 사항) **Log Files(**로그 파일**)** 확인란을 선택하여 연결과 결합된 파일 및 악성코드 이벤트를 로깅합니다.

이 옵션은 활성화된 상태로 유지하는 것이 좋습니다.

단계 **5** 연결 이벤트를 전송할 위치를 지정합니다.

- **Event Viewer(**이벤트 뷰어**)**: 이러한 연결 이벤트를 대상으로 Firepower Management Center 기반 분석을 수행하고 싶거나 규칙 작업이 **Monitor(**모니터링**)**일 경우, 연결 이벤트를 Firepower Management Center 웹 인터페이스로 전송합니다.
- **Syslog Server(**시스템 로그 서버**)**: 연결 이벤트를 Access Control Policy(액세스 컨트롤 정책)의 Logging(로깅) 탭에 설정된 시스템 로그 서버로 전송합니다(재정의한 경우는 예외).

  Show Overrides(재정의 표시**)**: 액세스 컨트롤 정책에 구성한 설정을 오버라이드하는 옵션을 표시합니다.

- **Override Severity(**심각도 재정의**)**: 이 옵션을 선택하고 규칙의 심각도를 선택하면, 해당 규칙에 대한 연결 이벤트는 Access Control Policy(액세스 컨트롤 정책)의 Logging(로깅) 탭에 설정된 심각도와는 상관없이 선택된 심각도를 갖게 됩니다.
- **Override Default Syslog Destination(**기본 시스템 로그 대상 재정의**)**: 이 규칙의 연결 이벤트에 대해 생성된 시스템 로그를 이 알림에서 지정하는 대상으로 전송합니다.

- **SNMP Trap(SNMP** 트랩**)**: 연결 이벤트는 선택된 SNMP 트랩으로 전송됩니다.

단계 **6** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

정책 기본 작업으로 연결 로깅

정책의 기본 작업은 시스템이 정책 내 규칙 중 어느 것과도 일치하지 않는 트래픽을 어떻게 처리할 것인지 결정합니다(일치 및 로깅되지만 트래픽을 검사하거나 처리하지 않는의 모니터링 규칙은 예외).

SSL 정책 기본 작업의 로깅 설정은 해독 불가능한 세션을 로깅하는 방법도 제어합니다.

프로시저

단계 **1** 정책 편집기에서 **Default Action(**기본 작업**)** 드롭다운 목록 옆에 있는 로깅( )을 클릭합니다.

단계 **2** 일치하는 연결을 언제 로깅할지 지정합니다.

- Log at Beginning of Connection(연결 시작 시 로깅) — SSL 기본 작업에는 지원되지 않습니다.
- Log at End of Connection(연결 종료 시 로깅) — 액세스 제어 **Block All Traffic(**모든 트래픽 차단**)** 기본 작업을 선택한 경우 지원되지 않습니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다. 액세스 제어 정책의 경우, 상위 정책에서 컨피그레이션을 상속할 수도 있습니다.

단계 **3** 연결 이벤트를 전송할 위치를 지정합니다.

이러한 연결 이벤트에서 Firepower Management Center 기반의 분석을 수행하려는 경우 이벤트 뷰어로 이벤트를 전송합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

긴 URL의 로깅 제한

HTTP 트래픽에 대한 연결 종료 이벤트는 모니터링되는 호스트가 요청한 URL을 기록합니다. 저장된 URL 문자 수를 비활성화하거나 제한하면 시스템 성능을 높일 수 있습니다. URL 로깅을 비활성화해도(어떤 문자도 보관하지 않아도) URL 필터링은 영향받지 않습니다. 시스템은 요청된 URL을 기반으로 트래픽을 필터링하며, 시스템이 해당 URL을 기록하지 않는 경우도 마찬가지입니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭한 다음 **General Settings(**일반 설정**)** 옆에 있는 수정( )을 클릭합니다.

보기 ( )가 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 연결 이벤트에 저장하고자 하는 최대 **URL** 문자를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 498 페이지의 내용을 참조하십시오.

121 장

연결 및 보안 인텔리전스 이벤트

다음 주제에서는 연결 및 보안 이벤트 테이블을 사용하는 방법을 설명합니다.

- 연결 이벤트 정보, 2875 페이지
- 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지
- 연결 및 보안 인텔리전스 이벤트 테이블 사용, 2900 페이지
- 연결 요약 페이지 보기, 2905 페이지
- 연결 및 보안 인텔리전스 이벤트 기록, 2906 페이지

연결 이벤트 정보

시스템은 자신의 매니지드 디바이스가 탐지한 연결의 로그를 생성할 수 있습니다. 이러한 로그를 연결 이벤트라고 합니다. 연결 이벤트는 *Security Intelligence*(보안 인텔리전스) 이벤트(평판 기반 Security Intelligence(보안 인텔리전스) 기능이 차단한 연결)를 포함합니다.

연결 이벤트는 일반적으로 다음이 탐지한 트랜잭션을 포함합니다.

- Access Control(액세스 컨트롤) 정책
- SSL 정책
- 사전 필터 정책(사전 필터나 터널 규칙이 캡처함)
- DNS 차단 목록
- URL 차단 목록
- 네트워크(IP 주소) 차단 목록

규칙 및 정책의 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다.

자세한 내용은 연결 로깅, 2859 페이지를 참조하십시오.

관련 항목

보안 인텔리전스 정보, 1695 페이지

연결 또는 보안 인텔리전스 이벤트

*Security Intelligence(*보안 인텔리전스*)* 이벤트는 평판 기반 Security Intelligence(보안 인텔리전스) 기능으로 세션을 차단하거나 모니터링할 때마다 생성되는 연결 이벤트입니다.

그러나 모든 Security Intelligence(보안 인텔리전스 이벤트)에는 동일한 연결 이벤트가 존재합니다. Security Intelligence(보안 인텔리전스) 이벤트는 독립적으로 보고 분석할 수 있습니다. 또한 시스템은 Security Intelligence(보안 인텔리전스) 이벤트를 개별적으로 저장하고 정리합니다.

시스템은 리소스 집약적인 평가를 실행하기 전에 먼저 Security Intelligence(보안 인텔리전스)를 실행합니다. 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

참고 아 가이드에서, 연결 이벤트에 대한 일반 정보는 별도로 지정하지 않는 한 Security Intelligence(보안 인텔리전스) 이벤트와도 관련이 있습니다.

NetFlow 연결

매니지드 디바이스에 의해 수집된 연결 데이터를 보완하기 위해 NetFlow 엑스포터가 브로드캐스트하는 레코드를 사용하여 연결 이벤트를 생성할 수 있습니다. 이는 매니지드 디바이스에 의해 모니터링되는 것과 다른 네트워크를 NetFlow 엑스포터가가 모니터링하고 있는 경우 특히 유용합니다.

시스템은 NetFlow 레코드를 단방향 연결 종료 이벤트로 Firepower Management Center 데이터베이스에 로깅합니다. 이 연결에 사용 가능한 정보는 액세스 제어 정책이 탐지하는 연결의 정보와 약간 다릅니다(NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지 참조).

관련 항목

Firepower System의 Netflow 데이터, 2381 페이지

연결 요약(그래프에 대한 집계된 데이터)

Firepower System에서는 5분 간격으로 수집된 연결 데이터를 연결 요약으로 취합하며, 시스템에서는 이 정보를 사용하여 연결 그래프 및 트래픽 프로파일을 생성합니다. 선택적으로, 연결 요약 데이터를 기준으로 맞춤형 워크플로를 생성할 수 있으며 이는 개별 연결 이벤트에 기반한 워크플로를 사용할 때와 같은 방식으로 사용합니다.

해당하는 연결 종료 이벤트를 연결 요약 데이터로 취합할 수는 있지만, 보안 인텔리전스 이벤트에 대한 연결 요약 정보가 따로 제공되지는 않습니다.

여러 연결을 취합하려면 연결의 조건은 다음을 충족해야 합니다.

- 연결의 종료를 나타냄
- 소스 및 대상 IP 주소가 동일하며, 응답자(대상) 호스트에서 동일한 포트를 사용함
- 동일한 프로토콜을 사용함(TCP 또는 UDP)

- 동일한 애플리케이션 프로토콜을 사용함
- 동일한 Firepower System 매니지드 디바이스나 동일한 NetFlow 엑스포터를 사용하여 탐지함

각 연결 요약에는 총 트래픽 통계 및 요약에 나와 있는 연결 수가 포함됩니다. NetFlow 엑스포터는 단방향 연결을 생성하므로, 요약의 연결 수는 NetFlow 데이터를 기준으로 모든 연결마다 2배로 증가합니다.

연결 요약에는 요약의 취합된 연결과 관련된 모든 정보가 포함되지는 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

오래 실행되는 연결

모니터링되는 세션이 연결 데이터가 집계되는 5분 간격 2회 이상에 걸쳐 있는 경우, 해당 연결은 *long-running* 연결로 간주됩니다. 연결 요약의 연결 수를 계산할 때 long-running 연결이 시작된 5분 간격에 대해서만 수가 증가합니다.

또한 long-running 연결에서 이니시에이터 및 응답자가 전송한 패킷과 바이트 수를 계산할 때 각 5분 간격 동안 실제로 전송된 패킷과 바이트 수는 보고되지 않습니다. 그 대신, 시스템에서는 일정한 전송 속도를 추정하며 전송된 패킷과 바이트의 총 개수, 연결의 길이, 각 5분 간격 동안 발생한 연결의 부분을 기준으로 예측 수치를 계산합니다.

외부 응답자의 연결 요약 통합

연결 데이터를 저장하는 데 필요한 공간을 줄이고 연결 그래프의 렌더링 속도를 높이기 위해, 시스템에서는 다음과 같은 경우 연결 요약을 통합합니다.

- 모니터링되는 네트워크에 연결과 관련된 호스트 중 하나가 없는 경우
- 외부 호스트의 IP 주소를 제외하고 요약의 연결이 요약 어그리게이션 기준을 충족하는 경우

Analysis(분석) > Connections(연결) 하위 메뉴 페이지에서 연결 요약을 보고 연결 그래프 작업을 할 때 시스템은 모니터링되지 않는 호스트의 IP 주소 대신 외부 를 표시합니다.

이 어그리게이션으로 인해 외부 응답자와 관련된 연결 요약 또는 그래프에서 연결 데이터(즉, 개별 연결에 대한 액세스 데이터)의 테이블 보기로 드릴다운하려고 할 경우, 테이블 보기에 아무런 정보가 포함되지 않습니다.

연결 및 보안 인텔리전스 이벤트 필드

참고 연결/보안 인텔리전스 이벤트 검색 페이지를 사용하여 연결과 관련된 이벤트를 검색할 수 없습니다.

액세스 제어 정책**(**시스템 로그**: ACPolicy)**

연결을 모니터링하는 액세스 제어 정책.

액세스 제어 규칙**(**시스템 로그**: AccessControlRuleName)**

연결을 처리한 액세스 제어 규칙 또는 기본 작업이자, 해당 연결과 일치한 최대 8개의 Monitor(모니터링) 규칙.

연결이 하나의 Monitor(모니터링) 규칙과 매칭될 경우, Firepower Management Center에는 연결을 처리한 규칙의 이름이 표시되며 그 뒤에 Monitor(모니터링) 규칙 이름이 표시됩니다. 연결에 하나 이상의 Monitor(모니터링) 규칙과 매칭될 경우, 매칭되는 Monitor(모니터링) 규칙 수가 표시되며 `Default Action + 2 Monitor Rules`(기본 작업 + 2개 모니터링 규칙)가 그러한 예입니다.

팝업 창에 연결과 매칭되는 처음 8개 Monitor(모니터링) 규칙 목록을 표시하려면 ***N(***개수***)* Monitor Rules(**모니터링 규칙**)**를 클릭합니다.

작업**(**시스템 로그**: AccessControlRuleAction)**

연결을 로깅한 구성과 관련된 작업.

보안 인텔리전스로 모니터링된 연결의 경우, 작업은 연결에 의해 트리거되는 첫 번째 비 Monitor 액세스 제어 규칙 또는 기본 작업입니다. 이와 마찬가지로, Monitor(모니터링) 규칙과 매칭되는 트래픽은 항상 후속 규칙 또는 기본 규칙에 의해 처리되므로 Monitor(모니터링) 규칙에 의해 로깅된 연결과 관련된 작업은 Monitor(모니터링)가 될 수 없습니다. 그러나 Monitor(모니터링) 규칙과 매칭되는 연결에서 상관관계 정책 위반을 트리거할 수 있습니다.

작업	설명
허용	액세스 제어에 의해 명시적으로 허용되거나 사용자가 인터랙티브 차단을 우회했기 때문에 허용된 연결.
차단, 차단 후 재설정	차단된 연결. 예: • 보안 인텔리전스에 의해 차단된 연결 • SSL 정책에 의해 차단된 암호화된 연결 • 침입 정책에 따라 익스플로잇이 차단된 연결 • 파일 정책에 따라 파일(악성코드 포함)이 차단된 연결 시스템이 침입 또는 파일을 차단하는 연결의 경우, 액세스 제어 Allow(허용) 규칙을 사용하여 심층 검사를 호출하더라도 시스템에 `Block`(차단)이 표시됩니다.
Interactive Block, Interactive Block with reset(인터랙티브 차단, 인터랙티브 차단 후 재설정)	시스템이 Interactive Block(인터랙티브 차단) 규칙을 사용해 사용자의 HTTP 요청을 초기에 차단하는 경우 로깅된 연결. 사용자가 시스템에 표시된 경고 페이지를 클릭할 경우, 해당 세션에 로깅된 추가 연결에는 Allow(허용) 작업이 포함됩니다.
신뢰	액세스 제어에서 신뢰하는 연결. 시스템은 기기 모델에 따라 신뢰하는 TCP 연결을 다르게 기록합니다.

작업	설명
기본 작업	액세스 제어 정책 기본 작업에서 처리한 연결
(Blank/empty)	규칙과 일치하기에 충분한 패킷이 전달되기 전에 연결이 종료되었습니다. 이는 침입 방지 등의 액세스 제어 이외의 기능으로 인해 연결이 로깅되는 경우에만 발생할 수 있습니다.

애플리케이션 프로토콜**(**시스템 로그**: ApplicationProtocol)**

Firepower Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

호스트 간 통신을 나타내며 연결에서 탐지되는 애플리케이션 프로토콜

애플리케이션 프로토콜 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

사업 타당성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

클라이언트 및 클라이언트 버전**(**시스템 로그**:** 클라이언트**, ClientVersion)**

연결에서 탐지된 클라이언트 애플리케이션 및 클라이언트 버전

시스템이 연결에 사용된 특정 클라이언트를 식별하지 못할 경우, 이 필드에는 애플리케이션 프로토콜 이름에 추가된 단어 "클라이언트"가 표시되어 일반 이름을 제공합니다(예:FTP 클라이언트).

클라이언트 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

Connection Counter(시스템 로그 전용**)**

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

Connection Instance ID(시스템 로그 전용**)**

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

ConnectionDuration(시스템 로그만 있음**)**

이 필드는 시스템 로그 필드로만 존재합니다. Firepower Management Center 웹 인터페이스에서는 존재하지 않습니다. (웹 인터페이스는 First Packet and Last PAcket(첫 번째 패킷 및 마지막 패킷) 열을 사용하여이 정보를 전달합니다.)

이 필드는 연결 종료 시 로깅이 발생하는 경우에만 값을 갖습니다. 연결 시작 시스템 로그 메시지의 경우, 이 필드는 해당 시점에 값을 알 수 없으므로 출력하지 않습니다.

연결 종료 시스템 로그 메시지의 경우, 이 필드는 첫 번째 패킷과 마지막 패킷 사이의 초 수를 나타내며 짧은 연결인 경우 0이 될 수 있습니다. 예를 들어, 시스템 로그의 타임스탬프가 12:34:56이며 ConnectionDuration이 5인 경우 첫 번째 패킷은 12:34:51입니다.

Connections

연결 요약의 연결 개수. 여러 연결 요약 간격에 걸쳐 있는 long-running 연결의 경우, 첫 번째 연결 요약 간격만 증가합니다. **Connections(**연결**)** 기준을 사용하여 유의미한 검색 결과를 보려면 연결 요약 페이지가 있는 맞춤형 워크플로를 사용해야 합니다.

개수

각 행에 표시되는 정보와 매칭되는 연결의 개수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count(**개수**)** 필드가 나타납니다. 사용자 지정 워크플로를 생성하고 **Count(**카운트**)** 열을 드릴다운 페이지에 추가하지 않은 경우, 각 연결은 개별적으로 낭려되고 패킷과 바이트는 합산되지 않습니다.

대상 포트**/ICMP** 코드**(**시스템 로그**:** 별도 필드**- DstPort, ICMPCode)**

Firepower Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 responder가 사용하는 포트 또는 ICMP 코드

DestinationSecurityGroup(시스템 로그 전용**)**

이 필드는 사용 가능한 경우 **DestinationSecurityGroupTag**의 숫자 값과 연결된 텍스트 값을 보유합니다. 그룹 이름을 텍스트 값으로 사용할 수 없는 경우 이 필드에는 DestinationSecurityGroupTag 필드와 동일한 정수 값이 포함됩니다.

DestinationSecurityGroupType(시스템 로그만 해당**)**

이 필드는 보안 그룹 태그를 가져온 소스를 표시합니다.

값	설명
인라인	대상 SGT 값이 패킷에서 나옴
세션 디렉토리	대상 SGT 값이 세션 디렉토리 주제를 통해 ISE에서 제공됨
SXP	대상 SGT 값이 SXP 주제를 통해 ISE에서 제공됨

대상 **SGT(**시스템 로그**: DestinationSecurityGroupTag)**

연결에 사용되는 대상의 숫자 보안 그룹 태그(SGT) 속성입니다.

대상 SGT 값은 **DestinationSecurityGroupType** 필드에 지정된 소스에서 가져옵니다.

디바이스

Firepower Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

연결을 탐지한 매니지드 디바이스, 또는 NetFlow 데이터에서 생성된 연결의 경우 해당 데이터를 처리하는 매니지드 디바이스.

DeviceUUID(시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

DNS 쿼리**(**시스템 로그**: DNSQuery)**

연결에서 도메인 이름을 조회하기 위해 해당 이름 서버로 제출된 DNS 쿼리.

이 필드는 DNS 필터링이 활성화된 경우 URL 필터링 일치에 대한 도메인 이름을 포함할 수도 있습니다. 이 경우 URL 필드는 비어 있으며 URL 범주 및 URL 평판 필드에는 도메인과 연결된 값이 포함됩니다.

DNS 필터링에 대한 자세한 내용은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별(베타), 1678 페이지의 내용을 참조하십시오.

DNS 레코드 종류**(**시스템 로그**: DNSRecordType)**

연결에서 제출된 DNS 쿼리 해결에 사용된 DNS 리소스 레코드의 유형.

DNS 응답**(**시스템 로그**: DNSResponseType)**

연결에서 쿼리를 받은 경우 이름 서버로 반환되는 DNS 응답.

DNS 싱크홀 이름**(**시스템 로그**: DNS_Sinkhole)**

시스템이 연결을 재전송한 싱크홀 서버의 이름.

DNS TTL(시스템 로그**: DNS_TTL)**

DNS 서버가 DNS 리소스 레코드를 캐시하는 초 수.

도메인

연결을 탐지한 매니지드 디바이스의 도메인, 또는 NetFlow 데이터에서 생성된 연결의 경우 해당 데이터를 처리하는 매니지드 디바이스의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Endpoint Location(엔드포인트 위치**)**

ISE에서 식별된 사용자를 인증하기 위해 ISE가 사용되는 네트워크 디바이스의 IP 주소.

엔드포인트 프로파일**(**시스템 로그**: Endpoint Profile)**

ISE에서 식별된 사용자의 엔드포인트 디바이스 유형.

이벤트 우선 순위**(**시스템 로그만 해당**)**

연결 이벤트가 우선 순위가 높은 이벤트인지 여부입니다. 우선 순위가 높은 이벤트는 침입, 보안 인텔리전스, 파일, 악성코드 이벤트와 관련된 연결 이벤트입니다. 이 외의 이벤트는 우선 순위가 낮은 이벤트입니다.

파일**(**시스템 로그**: FileCount)**

하나 이상의 파일 이벤트와 관련된 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수.

Firepower Management Center 웹 인터페이스에서 파일 보기 아이콘이 파일 목록에 링크됩니다. 아이콘의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다.

첫 번째 패킷 또는 마지막 패킷**(**시스템 로그**: ConnectionDuration** 필드를 참조하십시오**.)**

세션의 첫 번째 또는 마지막 패킷이 표시된 날짜 및 시간.

첫 번째 패킷 시간**(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

HTTP 참조자**(**시스템 로그**: HTTPReferer)**

연결(다른 URL에 링크를 제공하는 웹사이트 또는 다른 URL에서 링크를 가져온 웹사이트 등)에서 탐지된 HTTP 트래픽에 대해 요청된 URL의 참조 페이지를 나타내는 HTTP 참조 페이지

HTTP 응답 코드**(**시스템 로그**: HTTPResponse)**

연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드

인그레스/이그레스 인터페이스**(**시스템 로그**: IngressInterface, EgressInterface)**

연결과 관련된 인그레스 또는 이그레스 인터페이스. 배포에 비대칭 라우팅 구성이 포함되어 있는 경우, 인그레스 및 이그레스 인터페이스가 동일한 인라인 쌍에 속하지 않을 수 있습니다.

인그레스/이그레스 보안 영역**(**시스템 로그**: IngressZone, EgressZone)**

연결과 관련된 인그레스 또는 이그레스 보안 영역

인그레스 가상 라우터/이그레스 가상 라우터**(**시스템 로그**: IngressVRF, EgressVRF**
가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크를 진입하거나 벗어날 때 통과하는 가상 라우터의 이름입니다.

개시자/응답자 바이트**(**시스템 로그**: InitiatorBytes, ResponderBytes)**

세션 개시자가 전송했거나 세션 응답자가 수신한 총 바이트 수.

개시자/응답자 대륙

라우팅 가능한 IP가 탐지되는 경우 세션 개시자 또는 응답자의 IP 주소와 관련된 대륙.

개시자/응답자 국가

라우팅 가능한 IP가 탐지되는 경우 세션 개시자 또는 응답자의 IP 주소와 관련된 국가. 시스템에 해당 국가의 플래그 및 ISO 3166-1 alpha-3 국가 코드 아이콘이 표시됩니다. 국가의 전체 이름을 보려면 플래그 아이콘 위에 포인터를 올려놓습니다.

개시자/응답자 **IP(**시스템 로그**: SrcIP, DstIP)**

Firepower Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 이니시에이터 또는 응답기의 호스트 IP 주소(DNS 확인을 활성화한 경우 호스트 이름)

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

Firepower Management Center 웹 인터페이스에서 호스트 아이콘은 연결을 차단한 IP 주소를 식별합니다.

개시자/응답자 패킷**(**시스템 로그**: InitiatorPackets, ResponderPackets)**

세션 개시자가 전송했거나 세션 응답자가 수신한 총 패킷 수.

개시자 사용자**(**시스템 로그**: User)**

Firepower Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

세션 개시자에 로그인한 사용자. 이 필드에 **No Authentication(**인증 없음**)**이 입력된 경우, 사용자 트래픽은 다음과 같습니다.

- 관련 ID 정책 없이 액세스 제어 정책과 매칭
- ID 정책에서 모든 규칙과 매칭되지 않음

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

침입 이벤트**(**시스템 로그**: IPSCount)**

연결과 관련된 침입 이벤트의 수(해당되는 경우).

Firepower Management Center 웹 인터페이스에서 침입 이벤트 보기 아이콘이 이벤트 목록에 링크됩니다.

IOC

이벤트가 연결과 관련된 호스트에 대해 IOC(indication of compromise)를 트리거했는지 여부.

NetBIOS 도메인**(**시스템 로그**: NetBIOSDomain)**

세션에서 사용되는 NetBIOS 도메인

NetFlow SNMP 인풋/아웃풋

NetFlow 데이터에서 생성된 연결에서 연결 트래픽이 입력되거나 NetFlow 엑스포터를 종료하는 경우 인터페이스에 대한 인터페이스 인덱스.

NetFlow 소스/대상 자동 시스템

NetFlow 데이터에서 생성된 연결에서 트래픽 소스 또는 대상에 대한 경계 게이트웨이 프로토콜 자동 시스템 번호.

NetFlow 소스/대상 접두사

NetFlow 데이터에서 생성된 연결에서 소스 또는 대상 접두사 마스크로 AND 처리된 소스 또는 대상 IP 주소.

NetFlow 소스/대상 **TOS**

NetFlow 데이터에서 생성된 연결에서 연결 트래픽이 입력되거나 NetFlow 엑스포터를 종료하는 경우 서비스 유형(TOS) 바이트에 대한 설정.

네트워크 분석 정책**(**시스템 로그**: NAPPolicy)**

이벤드 생성과 관련된 NAP(네트워크 분석 정책) (해당되는 경우).

원래 클라이언트 **IP(**시스템 로그**: originalClientSrcIP)**

XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더에서 추출된 원래 클라이언트 IP 주소. 이 필드를 입력하려면 네트워크 분석 정책에서 HTTP 전처리기 **Extract Original Client IP Address(**원래 클라이언트 **IP** 주소 추출**)** 옵션을 활성화해야 합니다. 또한 네트워크 분석 정책에서 최대 6개의 맞춤형 클라이언트 IP 헤더를 지정할 수 있으며 시스템이 Original Client IP 이벤트 필드에 대한 값을 선택하는 우선순위 순서를 설정할 수 있습니다.

프로토콜**(**시스템 로그**: Protocol)**

Firepower Management Center 웹 인터페이스:

- 이 값은 요약과 그래프를 제한합니다.
- 이 필드는 검색 필드로만 사용할 수 있습니다.

연결에 사용된 전송 프로토콜 특정 프로토콜을 검색하려면 http://www.iana.org/assignments/protocol-numbers에 열거된 이름 또는 번호 프로토콜을 사용합니다.

QoS-적용 인터페이스
속도가 제한되는 연결에서 속도 제한이 적용되는 인터페이스 이름.

QoS-손실 개시자/응답자 바이트
속도 제한으로 인해 세션 개시자 또는 세션 응답자에서 삭제된 바이트 수.

QoS-손실 개시자/응답자 패킷
속도 제한으로 인해 세션 개시자 또는 세션 응답자에서 삭제된 패킷의 수.

QoS 정책
연결 속도를 제한하는 QoS 정책.

QoS 규칙
연결 속도를 제한하는 QoS 규칙.

이유**(**시스템 로그**: AccessControlRuleReason)**

다양한 상황에서 연결이 로깅된 이유. 전체 목록은 연결 이벤트 이유, 2893 페이지를 참조하십시오.

IP Block(IP 차단), DNS Block(DNS 차단), URL Block(URL 차단) 이유와의 연결은 고유 개시자-응답자 쌍당 임계값이 15초입니다. 시스템이 이러한 연결 중 하나를 차단하는 경우, 포트 또는 프로토콜에 관계없이 다음 15초 동안 이러한 두 호스트 간에 추가로 차단된 연결에 대한 연결 이벤트는 생성되지 않습니다.

참조된 호스트**(**시스템 로그**: ReferencedHost)**

연결의 프로토콜이 HTTP, 또는 HTTPS인 경우 이 필드에는 각 프로토콜이 사용했던 호스트 이름이 표시됩니다.

SecIntMatchingIP(시스템 로그만 있음**)**

매칭되는 IP 주소.

가능한 값: **None (**없음**)**, **Destination(**대상**)** 또는 **Source(**소스**)**.

보안 상황**(**시스템 로그**: Context)**

여러 상황 모드에서 ASA FirePOWER가 처리한 연결의 경우 트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터.

보안 인텔리전스 카테고리**(**시스템 로그**: URLSICategory, DNSSICategory, IPReputationSICategory)**

연결 차단의 원인이 된 IP 주소를 나타내거나 포함하는 개체의 이름입니다. 보안 인텔리전스 카테고리는 네트워크 개체 또는 그룹, 차단 목록, 맞춤형 보안 인텔리전스 목록이나 피드, 인텔리전스 피드 내 카테고리 중 하나의 이름일 수 있습니다.

Firepower Management Center 웹 인터페이스에서 DNS, 네트워크(IP 주소) 및 URL 보안 인텔리전스 연결 이벤트는 단일 카테고리 필드에 통합됩니다. 시스템 로그 메시지에서 해당 이벤트는 유형별로 지정됩니다.

Intelligence Feed 카테고리에 대한 자세한 내용은 보안 인텔리전스 카테고리, 1702 페이지를 참조하십시오.

Source Device

Firepower Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

연결 생성에 사용된 데이터를 브로드캐스트하는 NetFlow 엑스포터의 IP 주소. 매니지드 디바이스에서 연결이 탐지된 경우 이 필드에 `Firepower`가 표시됩니다.

소스 포트**/ICMP** 유형**(**시스템 로그**: SrcPort, ICMPType)**

Firepower Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 이니시에이터가 사용하는 포트 또는 ICMP 유형

SourceSecurityGroup(시스템 로그만 해당**)**

이 필드는 사용 가능한 경우 **SourceSecurityGroupTag**의 숫자 값과 연결된 텍스트 값을 보유합니다. 그룹 이름을 텍스트 값으로 사용할 수 없는 경우이 필드에는 SourceSecurityGroupTag 필드와 동일한 정수 값이 포함됩니다. 태그는 인라인 디바이스(소스 SGT 이름이 지정되지 않음) 또는 ISE(소스를 지정 함)에서 가져올 수 있습니다.

SourceSecurityGroupType (시스템 로그만 해당**)**

이 필드는 보안 그룹 태그를 가져온 소스를 표시합니다.

값	설명
인라인	소스 SGT 값이 패킷에서 나옴
세션 디렉토리	소스 SGT 값이 세션 디렉토리 주제를 통해 ISE에서 제공됨
SXP	소스 SGT 값은 SXP 주제를 통해 ISE에서 제공됨

소스 **SGT(**시스템 로그**: SourceSecurityGroupTag)**

연결에 사용되는 패킷의 보안 그룹 태그(SGT) 속성에 대한 숫자값 SGT는 신뢰할 수 있는 네트워크 내의 트래픽 소스 권한을 지정합니다. Cisco TrustSec 및 Cisco ISE 둘 다에서 제공되는 기능인 SGA(Security Group Access)는 패킷이 네트워크로 들어오면 속성을 적용합니다.

SSL 실제 작업**(**시스템 로그**: SSLActualAction)**

Firepower Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

시스템에서 검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

시스템이 SSL 정책에서 암호화된 트래픽에 적용하는 작업.

작업	설명
차단/차단 및 재설정	차단된 암호화된 연결을 나타냅니다.
암호 해독(재서명)	다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(대체 키)	대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(알려진 키)	알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.
기본 작업	연결이 기본 작업에 의해 처리되었음을 나타냅니다.
암호해독안함	시스템이 암호 해독하지 않은 연결을 나타냅니다.

SSL 인증서 정보**(**시스템 로그**: SSLCertificate)**

Firepower Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)
- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)

- Serial Number(일련 번호)
- Certificate Fingerprint(인증서 지문)
- Public Key Fingerprint(공개 키 지문)

SSL 인증서 상태**(**시스템 로그**: SSLServerCertStatus)**

이는 인증서 상태 SSL 규칙 조건을 구성한 경우에만 적용됩니다. 암호화된 트래픽이 SSL 규칙과 일치할 경우, 이 필드에는 다음 서버 인증서 상태 값 중 하나 이상이 표시됩니다.

- Self Signed(셀프 서명)
- Valid(유효)
- Invalid Signature(잘못된 서명)
- Invalid Issuer(잘못된 발급자)
- Expired(만료됨)
- Unknown(알 수 없음)
- Not Valid Yet(아직 유효하지 않음)
- Revoked(취소됨)

해독 불가능한 트래픽이 SSL 규칙과 매칭될 경우, 이 필드는 `Not Checked(확인되지 않음)`로 표시됩니다.

SSL 암호화 그룹**(**시스템 로그**: SSSLCipherSuite)**

연결을 암호화하는 데 사용되는 암호화 그룹을 나타내는 매크로 값. 암호 그룹 값 지정에 대한 내용은 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml을 참조하십시오.

연결에 적용된 **SSL** 암호화

이 필드는 Firepower Management Center 웹 인터페이스에서 검색 필드로만 사용할 수 있습니다.

`Yes`(예) 또는 **`no`(아니오)**를 **SSL** 검색 필드에 입력하고 TLS/SSL-암호화 또는 비암호화 연결을 확인합니다.

SSL 예상 작업**(**시스템 로그**: SSLExpectedAction)**

Firepower Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

유효한 SSL 규칙을 감안해 시스에서 트래픽 암호화에 적용할 것으로 예상되는 작업.

SSL Actual Action(SSL 실제 작업**)**에 나열된 값 중 하나를 입력합니다.

SSL 실패 이유**(**시스템 로그**: SSLFlowStatus)**

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)

- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)
- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 플로우 오류

TLS/SSL 세션 도중 오류가 발생하는 경우 오류 이름 및 16진수 코드, 오류가 발생하지 않는 경우 `Success`(성공).

SSL 플로우 플래그

암호화된 연결에 대한 처음 10개의 디버깅 수준 플래그입니다. 워크플로 페이지에서 모든 플래그를 보려면 줄임표(**...**)를 클릭합니다.).

SSL 플로우 메시지

아래 키워드는 암호화된 트래픽이 TLS/SSL 핸드셰이크 중 클라이언트와 서버 간에 교환된 지정 메시지 유형과 관련되어 있음을 나타냅니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246를 참조하십시오.

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER
- SERVER_NAME_MISMATCH

세션에 표시되는 서버 인증서는 대상 도메인 이름과 일치하지 않는 공통 이름 또는 SAN 값을 갖습니다.

- CERTIFICATE_CACHE_HIT

  대상 도메인 이름과 일치하는 인증서가 캐시에 있습니다.

- CERTIFICATE_CACHE_MISS

  대상 도메인 이름과 일치하는 인증서가 캐시에 없습니다.

SSL 정책**(**시스템 로그**: SSLPolicy)**

연결을 처리한 SSL 정책.

TLS 서버 ID 검색이 액세스 제어 정책 고급 설정에서 활성화되어 있고 액세스 제어 정책과 연결된 SSL 정책이 없는 경우 이 필드는 모든 SSL 이벤트에 대해 아무것도 유지하지 않습니다.

SSL 규칙**(**시스템 로그**: SSLRuleName)**

연결을 처리한 SSL 규칙 또는 기본 작업이자 해당 연결과 매칭된 첫 번째 Monitor(모니터링) 규칙입니다. 연결이 하나의 Monitor(모니터링) 규칙과 매칭된 경우, 연결을 처리한 규칙의 이름이 필드에 표시되며 그 뒤에 Monitor(모니터링) 규칙 이름이 표시됩니다.

SSLServerName(시스템 로그만 있음**)**

이 필드는 시스템 로그 필드로만 존재합니다. Firepower Management Center 웹 인터페이스에서는 존재하지 않습니다.

클라이언트가 암호화된 연결을 설정한 서버의 호스트 이름.

SSL 세션 **ID(**시스템 로그**: SSLSessionID)**

TLS/SSL 핸드셰이크 도중 클라이언트와 서버 간에 협상된 16진수 Session ID.

SSL Status

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)** (SSL 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업. 잠금 아이콘은 SSL 인증서 세부 정보에 링크됩니다. 인증서를 사용할 수 없는 경우(예: TLS/SSL 핸드셰이크 오류로 연결 차단), 잠금 아이콘이 흐리게 표시됩니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`(암호 해독 하지 않음(알려지지 않은 암호화 그룹))로 표시됩니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL 대상자/발급자 국가

이 필드는 Firepower Management Center 웹 인터페이스에서만 검색 필드로만 사용 가능합니다.

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

SSL 티켓 **ID(**시스템 로그**: SSLTicketID)**

TLS/SSL 핸드셰이크 도중 전송된 세션 티켓 정보의 16진수 해시 값

SSLURLCategory(시스템 로그만 있음**)**

암호화된 연결에서 방문한 URL의 URL 카테고리.

이 필드는 시스템 로그 필드로만 존재합니다. Firepower Management Center 웹 인터페이스에서 이 필드의 값은 URL 카테고리 열에 포함됩니다.

URL도 참조하십시오.

SSL 버전**(**시스템 로그**: SSLVersion)**

연결 암호화에 사용되는 TLS/SSL 프로토콜 버전:

- 알 수 없음
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSV1.2

TCP 플래그**(**시스템 로그**: TCPFlags)**

NetFlow 데이터에서 생성된 연결에서 탐지된 TCP 플래그.

이 필드를 검색할 때 쉼표로 구분된 TCP 플래그 목록을 입력하면 이러한 플래그 중 최소한 하나를 보유한 모든 연결을 볼 수 있습니다.

시간

연결 요약에서 연결을 취합하기 위해 시스템이 사용한 5분 간격의 종료 시간. 이 필드는 검색할 수 없습니다.

총 패킷

이 필드는 검색 필드로만 사용할 수 있습니다.

연결에서 전송된 패킷의 총 수.

트래픽**(KB)**

이 필드는 검색 필드로만 사용할 수 있습니다.

연결에서 전송된 데이터의 총량(단위: 킬로바이트)

URL, URL 카테고리 및 **URL** 평판**(**시스템 로그**: URL, URLCategory** 및 **SSLURLCategory, URLReputation)**

세션 중에 모니터링된 호스트에서 요청한 URL, 관련 카테고리 및 평판(해당되는 경우)

URL 열이 비어 있고 DNS 필터링이 활성화된 경우 DNS Query(DNS 쿼리) 필드에 도메인이 표시되고 URL 범주 및 URL 평판 값이 도메인에 적용됩니다.

시스템에서 TLS/SSL 애플리케이션을 식별하거나 차단한 경우, 요청한 URL은 암호화된 트래픽에 있으므로 시스템은 SSL 인증서를 기준으로 해당 트래픽을 식별합니다. 따라서 TLS/SSL 애플리케이션의 경우, 이 필드는 인증서에 포함된 공용 이름을 나타냅니다.

위 **SSLURLCategory**도 참조하십시오.

사용자 에이전트**(**시스템 로그**: UserAgent)**

연결에서 탐지된 HTTP 트래픽에서 추출된 사용자 에이전트 문자열 애플리케이션 정보.

VLAN ID (시스템 로그**: VLAN_ID)**

연결을 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID.

웹 애플리케이션**(**시스템 로그**: WebApplication)**

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청한 URL을 나타내는 웹 애플리케이션

웹 애플리케이션이 이벤트의 URL과 매칭되지 않을 경우, 해당 트래픽은 참조 트래픽(예: 광고 트래픽)일 가능성이 높습니다. 시스템이 참조 트래픽을 탐지할 경우, 시스템은 제공되는 참조 애플리케이션을 저장하고 해당 애플리케이션을 웹 애플리케이션으로 나열합니다.

시스템이 HTTP 트래픽에서 특정 웹 애플리케이션을 식별하지 못할 경우, 이 필드는 `Web Browsing(웹 브라우징)`으로 표시됩니다.

웹 애플리케이션 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

연결 및 보안 인텔리전스 이벤트 필드 정보

Firepower Management Center 웹 인터페이스에서 **Analysis(**분석**) > Connections(**연결**)** 하위 메뉴의 테이블 형식 및 그래픽 워크플로를 사용하여 연결 및 보안 인텔리전스 이벤트를 보고 검색할 수 있습니다.

참고 보안 인텔리전스 이벤트마다 별도로 저장되는 동일한 연결 이벤트가 있습니다. 모든 보안 인텔리전스 이벤트에는 내용이 채워진 **Security Intelligence Category(**보안 인텔리전스 카테고리**)** 필드가 있습니다.

개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다.

검색 제약 조건

검색 페이지에서 별표**(*)**로 표시된 필드는 연결 그래프 및 연결 요약을 제한 합니다. 연결 그래프는 연결 요약에 기반하므로, 연결 요약을 제한하는 동일한 기준은 연결 그래프도 제한합니다. 잘못된 검

색 제한을 사용하여 연결 요약을 검색하고 맞춤형 워크플로의 연결 요약 페이지를 사용하여 결과를 볼 경우, 잘못된 제한은 해당 사항 없음(N/A)이라는 레이블로 표시되고 취소선이 그어집니다.

Syslog 필드

대부분의 필드는 Firepower Management Center 웹 인터페이스와 syslog 메시지에 모두 표시됩니다. 나열된 동등한 syslog가 없는 필드는 syslog 메시지에서 사용할 수 없습니다. 언급한 것처럼 일부 필드는 syslog 전용이며, 그 밖의 소수의 필드는 syslog 메시지에서는 별도의 필드이지만 웹 인터페이스에서는 통합된 필드이며, 그 반대의 경우도 있습니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침

표 ***321:*** 용어 비교

필드	이벤트 유형	설명
이니시에이터/응답자	연결	연결의 이니시에이터/응답자. 연결의 이니시에이터가 침입 소스 또는 악성 코드 파일의 발신자와 반드시 같을 필요는 없습니다.
소스/대상	침입	공격의 소스/대상입니다. 침입 이벤트의 소스는 연결의 이니시에이터 또는 응답자일 수 있습니다.
발신자/수신자 (전송 중..., 수신 중...)	파일, 악성 코드	파일 또는 악성 코드의 발신자/수신자. 파일을 업로드하거나 다운로드할 수 있으므로 파일의 발신자가 반드시 연결의 이니시에이터일 필요는 없습니다.

연결 이벤트 이유

연결 이벤트의 Reason(이유) 필드는 다음과 같은 상황에서 연결이 로깅된 이유를 표시합니다.

이유	설명
DNS 차단	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. DNS 차단 이유는 DNS 규칙 작업에 따라 차단, 도메인을 찾을 수 없음 또는 싱크홀과 페어링됩니다.
DNS 모니터링	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.
파일 차단	시스템이 전송을 차단한 파일 또는 악성코드 파일이 연결에 포함되었습니다. 파일 차단 이유는 항상 차단 작업과 페어링됩니다.

이유	설명
파일 맞춤형 탐지	시스템이 전송을 차단한 맞춤형 탐지 목록의 파일이 연결에 포함되었습니다.
파일 모니터링	시스템이 연결에서 특정 파일 유형을 탐지했습니다.
파일 재시작 허용	파일 전송이 파일 차단 또는 악성코드 차단 파일 규칙에 의해 원래 차단되었다가, 해당 파일을 허용하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 재시작되었습니다. 이 이유는 인라인 구축에서만 표시됩니다.
파일 재시작 차단	파일 전송이 파일 탐지 또는 악성코드 클라우드 조회 파일 규칙에 의해 원래 허용되었다가, 해당 파일을 차단하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 중지되었습니다. 이 이유는 인라인 구축에서만 표시됩니다.
인텔리전트 애플리케이션 바이패스	인텔리전트 애플리케이션 우회(IAB) 모드: • 작업이 Trust(신뢰)인 경우, IAB는 우회 모드였습니다. 일치하는 트래픽은 추가 검사 없이 통과합니다. • 작업이 Allow(허용)인 경우, IAB는 테스트 모드였습니다. 일치하는 트래픽은 추가 검사가 가능했습니다.
침입 차단	시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단할 수도 있었음을 나타냅니다. 침입 차단 이유는 차단된 익스플로잇의 경우 차단 작업과, 차단될 수도 있었던 익스플로잇의 경우 허용과 페어링됩니다.
침입 모니터링	시스템이 연결에서 탐지된 익스플로잇을 탐지했지만 차단하지는 않았습니다. 트리거된 침입 규칙의 상태가 이벤트 생성으로 설정되어 있으면 이러한 현상이 나타납니다.
IP 차단	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. IP 차단 이유는 항상 차단 작업과 페어링됩니다.
IP Monitor	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.
SSL 차단	시스템에서 TLS/SSL 검사 구성에 기반하여 암호화된 연결을 차단했습니다. SSL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 차단	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. URL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 모니터링	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.

이유	설명
User Bypass	시스템에서 사용자의 HTTP 요청을 처음에 차단했지만 사용자가 경고 페이지를 클릭하여 사이트를 봤습니다. 사용자 바이패스 이유는 항상 허용 작업과 페어링됩니다.

연결 이벤트 필드 채우기 요구 사항

연결 이벤트, 보안 인텔리전스 이벤트 또는 연결 요약에 사용할 수 있는 정보는 여러 요인에 따라 달라집니다.

어플라이언스 모델 및 라이선스

대다수의 기능은 대상 디바이스에서 특정 라이선스 기능을 활성화해야 하며, 특정 모델에서만 사용 가능한 기능도 많습니다.

예를 들어 NGIPSv 디바이스는 TLS/SSL 검사를 지원하지 않습니다. 이들은 암호화된 트래픽을 검사할 수 없습니다. 로깅된 연결 이벤트에는 암호화된 연결에 대한 정보가 포함되지 않습니다.

트래픽 특성

시스템은 네트워크 트래픽에 존재하고 탐지 가능한 정보만 보고합니다. 예를 들어 이니시에이터 호스트와 연결된 사용자가 없거나, 프로토콜이 DNS, HTTP 또는 HTTPS가 아닌 연결에서 참조 호스트가 탐지되지 않을 수 있습니다.

기원/탐지 방법: 트래픽 기반 탐지 대 **NetFlow**

NetFlow 전용 필드를 제외하고, NetFlow 기록에서 사용 가능한 정보는 트래픽 기반 탐지가 생성한 정보에 비해 더욱 제한됩니다(NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지 참조).

평가 단계

각 유형의 트래픽 검사와 제어는 유연성과 성능을 최대화할 수 있는 방식으로 발생합니다.

예를 들어 시스템은 리소스 집약적인 평가를 실행하기 전에 먼저 보안 인텔리전스를 실행합니다. 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

로깅 방법: 연결의 시작 또는 종료

시스템이 연결을 탐지한 경우, 연결의 시작/종료(또는 두 시점 모두) 시점 중 연결을 언제 로깅할 수 있는지는 사용자가 시스템의 연결 탐지 및 처리 방식을 어떻게 구성하느냐에 따라 달라집니다.

Beginning-of-connection 이벤트에는 세션 기간 중에 트래픽을 검사하여 확인해야 하는 정보(예: 전송된 총 데이터의 양, 연결의 마지막 패킷의 타임스탬프)가 포함되지 않습니다. Beginning-of-connection 이벤트에는 세션의 애플리케이션 또는 URL 트래픽에 대한 정보가 없을 수 있으며, 세션의 암호화에 대한 세부 정보도 포함되지 않습니다. 일반적으로 Beginning-of-connection 로깅은 차단된 연결에 대한 유일한 옵션입니다.

연결 이벤트 유형: 개별 대 요약

연결 요약에는 취합된 연결과 관련된 모든 정보가 포함되지 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

연결 그래프는 연결 종료 로그만 사용하는 연결 요약 데이터를 기준으로 합니다. 연결 시작 데이터만 기록하도록 시스템을 설정하는 경우, 연결 그래프 및 연결 요약 이벤트 보기에 데이터가 포함되지 않습니다.

기타 설정

연결에 영향을 주는 기타 설정으로는 다음과 같은 항목이 있습니다.

- ISE 관련 필드는 Active Directory 도메인 컨트롤러를 통해 인증한 사용자와 관련된 연결에서 ISE를 설정하는 경우에만 채워집니다. 연결 이벤트는 LDAP, RADIUS, 또는 RSA 도메인 컨트롤러를 통해 인증한 사용자의 ISE 데이터는 포함하지 않습니다.
- TLS/SSL관련 필드는 SSL 정책을 통해 처리되는 암호화된 연결에서만 채워집니다. 트래픽을 암호화하지 않아도 된다면 Do Not Decrypt 규칙 작업을 사용하여 필드의 값을 확인할 수 있습니다.
- 파일 정보 필드는 파일 정책과 관련된 액세스 컨트롤 규칙이 기록한 연결에서만 채워집니다.
- 침입 정보 필드는 침입 정책과 관련되거나 기본 작업을 사용하는 액세스 컨트롤 규칙이 기록한 연결에서만 채워집니다.
- QoS 관련 필드는 속도 제한의 영향을 받는 연결에서만 채워집니다.
- Reason(원인) 필드는 사용자가 Interactive Block(인터랙티브 차단) 설정을 우회하는 경우 같은 특정 상황에서만 채워집니다.
- Domain(도메인) 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
- 액세스 컨트롤 정책의 고급 설정에서는 HTTP 세션에서 모니터링된 호스트에서 요청한 각 URL의 연결 로그에 저장되는 특성의 수를 제어합니다. 이 설정을 사용하여 URL 로깅을 비활성화할 경우, 카테고리 및 평판 데이터가 존재하고 이를 계속 볼 수 있는 경우에도 시스템에서는 연결 로그에 개별 URL을 표시하지 않습니다.

관련 항목

NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지

연결 이벤트 필드에서 제공되는 정보

이 항목의 표에는 시스템이 연결 및 보안 인텔리전스 필드를 채울 수 있는 경우가 나와 있습니다. 표의 열은 다음 이벤트 유형을 나타냅니다.

- 출처: 직접 - Firepower System 매니지드 디바이스에서 탐지 및 처리된 연결을 나타내는 이벤트
- 출처: NetFlow - NetFlow 엑스포터에서 내보낸 연결을 나타내는 이벤트
- 로깅: 시작 - 시작 시에 로깅되는 연결을 나타내는 이벤트

• 로깅: 종료 - 종료 시에 로깅되는 연결을 나타내는 이벤트

표에서 "예"는 시스템이 연결 이벤트 필드를 채워야 한다는 의미가 아니라 채울 수 있다는 의미입니다. 시스템은 네트워크 트래픽에 존재하고 탐지 가능한 정보만 보고합니다. 예를 들어 TLS/SSL 관련 필드는 SSL 정책을 통해 처리되는 암호화된 연결의 기록에 대해서만 채워집니다.

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
액세스 제어 정책	예	아니요	예	예
Access Control Rule	예	아니요	예	예
작업	예	아니요	예	예
Application Protocol(애플리케이션 프로토콜)	예	예	사용 가능한 경우	예
애플리케이션 프로토콜 카테고리 및 태그	예	아니요	사용 가능한 경우	예
애플리케이션 위험성	예	아니요	사용 가능한 경우	예
Business Relevance	예	아니요	사용 가능한 경우	예
Client(클라이언트)	예	아니요	사용 가능한 경우	예
클라이언트 카테고리 및 태그	예	아니요	사용 가능한 경우	예
클라이언트 버전	예	아니요	사용 가능한 경우	예
Connections	예	예	아니요	예
개수	예	예	예	예
대상 포트/ICMP 유형	예	예	예	예
Destination SGT(대상 SGT)	예	아니요	예	예
디바이스	예	예	예	예
도메인	예	예	예	예
DNS Query(DNS 쿼리)	예	아니요	예	예
DNS 레코드 유형	예	아니요	예	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
DNS 응답	예	아니요	예	예
DNS 싱크홀 이름	예	아니요	예	예
DNS TTL	예	아니요	예	예
이그레스 인터페이스	예	아니요	예	예
이그레스 보안 영역	예	아니요	예	예
엔드포인트 위치	예	아니요	예	예
Endpoint Profile(엔드포인트 프로파일)	예	아니요	예	예
파일	예	아니요	아니요	예
첫 번째 패킷	예	예	예	예
HTTP 참조 페이지	예	아니요	아니요	예
HTTP 응답 코드	예	아니요	예	예
인그레스 인터페이스	예	아니요	예	예
인그레스 보안 영역	예	아니요	예	예
초기자 바이트	예	예	유용하지 않음	예
Initiator Country	예	아니요	예	예
초기자 IP	예	예	예	예
초기자 패킷	예	예	유용하지 않음	예
이니시에이터 사용자	예	예	예	예
침입 이벤트	예	아니요	아니요	예
침입 정책	예	아니요	예	예
IOC(보안 침해 지표)	예	아니요	예	예
마지막 패킷	예	예	아니요	예
NetBIOS 도메인	예	아니요	예	예
NetFlow 소스/대상 자동 시스템	아니요	예	아니요	예
NetFlow 소스/대상 접두사	아니요	예	아니요	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
NetFlow 소스/대상 TOS	아니요	예	아니요	예
NetFlow SNMP 인풋/아웃풋	아니요	예	아니요	예
Network Analysis Policy	예	아니요	예	예
QoS-적용 인터페이스	예	아니요	아니요	예
QoS-손실 이니시에이터 바이트	예	아니요	아니요	예
QoS-손실 이니시에이터 패킷	예	아니요	아니요	예
QoS-손실 Responder 바이트	예	아니요	아니요	예
QoS-손실 Responder 패킷	예	아니요	아니요	예
QoS 정책	예	아니요	아니요	예
QoS 규칙	예	아니요	아니요	예
이유	예	아니요	예	예
참조된 호스트	예	아니요	아니요	예
응답기 바이트	예	예	유용하지 않음	예
Responder Country	예	아니요	예	예
응답기 IP	예	예	예	예
응답기 패킷	예	예	유용하지 않음	예
보안 상황 (ASA 전용)	예	아니요	예	예
Security Intelligence Category	예	아니요	예	예
Source Device	예	예	예	예
Source Port/ICMP Type	예	예	예	예
Source SGT(소스 SGT)	예	아니요	예	예
SSL Certificate Status	예	아니요	아니요	예
SSL Cipher Suite	예	아니요	아니요	예
SSL Flow Error	예	아니요	아니요	예
SSL Flow Flags	예	아니요	아니요	예
SSL Flow Messages	예	아니요	아니요	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
SSL 정책	예	아니요	아니요	예
SSL Rule	예	아니요	아니요	예
SSL Session ID	예	아니요	아니요	예
SSL Status	예	아니요	아니요	예
SSL Version	예	아니요	아니요	예
TCP 플래그	아니요	예	아니요	예
시간	예	예	아니요	예
URL	예	아니요	사용 가능한 경우	예
URL Category(URL 범주)	예	아니요	사용 가능한 경우	예
URL Reputation(URL 평판)	예	아니요	사용 가능한 경우	예
사용자 에이전트	예	아니요	아니요	예
VLAN ID	예	아니요	예	예
웹 애플리케이션	예	아니요	사용 가능한 경우	예
웹 애플리케이션 카테고리 및 태그	예	아니요	사용 가능한 경우	예

연결 및 보안 인텔리전스 이벤트 테이블 사용

Firepower Management Center을(를) 사용하여 연결 또는 보안 인텔리전스 이벤트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

연결 그래프에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 이벤트의 테이블 보기에서 종료되는 미리 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

연결 또는 보안 인텔리전스 워크플로 테이블을 사용하는 경우, 여러 일반적인 작업을 수행할 수 있습니다.

드릴다운 페이지에서 연결 이벤트를 제한할 경우, 동일한 이벤트의 패킷 및 바이트가 합산됩니다. 하지만 맞춤형 워크플로를 사용 중이고 드릴다운 페이지에 **Count(**카운트**)** 열을 추가하지 않은 경우, 이벤트가 개별적으로 나열되고 패킷과 바이트는 합산되지 않습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** 다음 중 하나를 선택합니다.

- **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)** (연결 이벤트의 경우)
- **Analysis(**분석**)** > **Connections(**연결**)** > **Security Intelligence Events(**보안 인텔리전스 이벤트**)**

참고 테이블 대신 연결 그래프가 표시되는 경우, 워크플로 제목별로 **(**워크플로 전환**)**을 클릭하고 미리 정의된 **Connection Events(**연결 이벤트**)** 워크플로 또는 맞춤형 워크플로를 선택합니다. 미리 정의된 연결 이벤트 워크플로(연결 그래프 포함)는 연결의 테이블 보기에서 종료됩니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Time Range(시간 범위) - 시간 범위를 조정합니다. 이벤트가 표시되지 않는 경우에 유용합니다. 타임 윈도우 변경, 2815 페이지 참조.
- Field Names(필드 이름) - 테이블 열의 콘텐츠에 대해 자세히 알아봅니다. 연결 및 보안 인텔리전스 이벤트 필드, 2877 페이지 참조.

  팁 이벤트의 테이블 보기에서는 각 애플리케이션의 Category(카테고리) 및 Tag(태그) 필드, NetFlow 관련 필드, TLS/SSL 관련 필드 등 몇 가지 필드가 기본적으로 숨겨져 있습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면 검색 제한 사항을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 필드 이름을 클릭합니다.

- Firepower 시스템 외부의 사용 가능한 소스에 있는 데이터를 보려면 이벤트 값을 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지 섹션을 참조해 주십시오.
- 외부 인텔리전스 - 이벤트에 대한 정보를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지를 참고하십시오.
- 호스트 프로필 - IP 주소의 호스트 프로필을 보려면 **Host Profile(**호스트 프로필**)**을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 **Compromised Host(**보안 침해된 호스트**)**를 클릭합니다.

- 사용자 프로파일 - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘를 클릭합니다.
- 파일 및 악성코드 - 연결에서 탐지되거나 차단된 악성코드를 포함한 파일을 보려면 **View Files(**파일 보기**)**을 클릭하고 연결 내에서 탐지된 파일 및 악성코드 보기, 2903 페이지에 설명된 대로 계속합니다.
- 침입 이벤트 - 연결에 연결된 침입과 우선 순위 및 영향을 보려면 **Intrusion Events(**침입 이벤트**)** 열에서 **Intrusion Events(**침입 이벤트**)**을 클릭하고 연결에 연결된 침입 이벤트 보기, 2904 페이지에 설명된 대로 계속합니다.

  팁 하나 이상의 연결에 연결된 침입, 파일 또는 악성코드 이벤트를 빠르게 보려면 테이블의 확인란을 사용하여 연결을 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 적절한 옵션을 선택합니다. 액세스 제어 규칙 평가 전에 차단되기 때문에 보안 인텔리전스에 의해 차단된 연결에 연결된 파일 또는 침입이 없을 수도 있습니다. 연결을 차단하기보다는 모니터링하도록 보안 인텔리전스를 구성했다면 보안 인텔리전스 이벤트의 경우에만 이 정보를 볼 수 있습니다.

- 인증서 - 연결을 암호화하는 데 사용할 수 있는 인증서에 대한 상세정보를 보려면 **SSL Status(SSL** 상태**)** 열에서 **Enabled Lock(**활성화된 잠금**)**을 클릭합니다.
- 제한 - 표시되는 열을 제한하려면 숨기려는 열 머리글의 닫기 아이콘(닫기( ))을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 검색 제약 조건을 확장한 다음 Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 이벤트 삭제 - (보안 인텔리전스 이벤트 테이블만 해당) 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.
- 드릴다운 - 드릴다운 페이지 사용, 2801 페이지 참조.

  팁 로깅된 연결과 일치한 여러 모니터 규칙 중 하나를 사용하여 드릴다운하려면 *N* **Monitor Rules** 값을 클릭합니다. 표시되는 팝업 창에서 연결 이벤트를 제한하는 데 사용할 모니터 규칙을 클릭합니다.

- 이 페이지 탐색 - 워크플로 페이지 이동 툴, 2798 페이지 참조.
- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.

- 정렬 - 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.

관련 항목

개요: 워크플로, 2781 페이지
이벤트 보기 구성, 41 페이지

연결 내에서 탐지된 파일 및 악성코드 보기

파일 정책과 하나 이상의 액세스 제어 규칙을 연결할 경우, 시스템은 일치하는 트래픽에서 파일(악성코드 포함)을 탐지할 수 있습니다. 이러한 규칙에 의해 로깅된 연결과 연결된 파일 이벤트(있는 경우)를 보려면 Analysis(분석) > Connections(연결) 메뉴 옵션을 사용하십시오. Firepower Management Center에서는 파일 목록 대신 **Files(**파일**)** 열에 파일 보기( )를 표시합니다. 파일 보기의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다.

모든 파일 및 악성코드 이벤트가 연결에 연결되는 것은 아닙니다. 구체적으로 말씀드리면,

- AMP for Endpoints가 탐지하는 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")는 연결에 연결되지 않습니다. 이러한 이벤트는 AMP for Endpoints 구축에서 가져옵니다.
- 많은 IMAP 지원 이메일 클라이언트는 사용자가 애플리케이션을 종료해야 종료되는 단일 IMAP 세션을 사용합니다. long-running 연결은 시스템에 의해 로깅되지만 세션에서 다운로드된 파일은 세션이 종료될 때까지 연결에 연결되지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**) > Connections(**연결**)**로 이동하여 관련 옵션을 선택합니다.

단계 **2** 연결 이벤트 테이블을 사용할 때 **View Files(**파일 보기**)**를 클릭합니다.
연결에서 탐지된 파일 목록과 그 유형 및 (해당되는 경우) 악성코드 속성이 포함된 팝업 창이 표시됩니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 보기 - 파일 이벤트의 테이블 보기를 보려면 파일의 **View(**보기**)**를 클릭합니다.
- 보기 - 악성코드 이벤트의 테이블 보기에서 세부 사항을 보려면 악성코드 악성코드 파일의 **View(**보기**)**를 클릭합니다.
- 추적 - 네트워크를 통한 파일의 전송을 추적하려면 파일의 **Trajectory(**경로 전송**)**를 클릭합니다.

- 보기 - AMP for Networks에 의해 탐지된 모든 연결의 탐지된 파일 또는 악성코드 이벤트("네트워크 기반 악성코드 이벤트")의 세부 정보를 보려면 **View File Events(**파일 이벤트 보기**)** 또는 **View Malware Events(**악성코드 이벤트 보기**)**를 클릭합니다.

연결에 연결된 침입 이벤트 보기

침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 경우, 시스템은 일치하는 트래픽에서 익스플로잇을 탐지할 수 있습니다. 로깅된 연결에 연결된 침입 이벤트(있는 경우)와 우선 순위 및 영향을 보려면 Analysis(분석) > Connections(연결) 메뉴 옵션을 사용하십시오.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**) > Connections(**연결**)**로 이동하여 관련 옵션을 선택합니다.

단계 **2** 연결 이벤트 테이블을 사용할 때 **Intrusion Events(**침입 이벤트**)** 열에서 **Intrusion Events(**침입 이벤트**)**를 클릭합니다.

단계 **3** 나타나는 팝업 창에서 다음 옵션을 이용할 수 있습니다.

- **Listed Event's View(**나열된 이벤트의 보기**)**를 클릭하여 패킷 보기에서 세부 정보를 확인합니다.
- **View Intrusion Events(**침입 이벤트 보기**)**를 클릭하여 연결에 연결된 모든 침입 이벤트에 대한 세부 정보를 봅니다.

암호화된 연결 인증서 세부 정보

Analysis(분석) > Connections(연결) 메뉴 아래의 옵션을 사용하여 시스템이 처리하는 연결을 암호화하는 데 사용되는 공개 키 인증서(사용할 수 있는 경우)를 표시할 수 있습니다. 인증서에는 다음 정보가 포함됩니다.

표 ***322:*** 암호화된 연결 인증서 상세정보

속성	설명
Subject/Issuer Common Name(주체/발급자 공용 이름)	인증서 주체 또는 인증서 발급자의 호스트 및 도메인 이름입니다.

속성	설명
Subject/Issuer Organization(주체/발급자 조직)	인증서 주체 또는 인증서 발급자가 속한 조직입니다.
Subject/Issuer Organization Unit(주체/발급자 조직 단위)	인증서 주체 또는 인증서 발급자가 속한 조직 단위입니다.
Not Valid Before/After(유효기간)	인증서가 유효한 날짜입니다.
일련 번호	발급 CA가 할당한 일련번호입니다.
Certificate Fingerprint(인증서 지문)	인증서를 인증하는 데 사용되는 SHA 해시 값입니다.
Public Key Fingerprint(공개 키 지문)	인증서 내에 있는 공개 키를 인증하는 데 사용되는 SHA 해시 값입니다.

연결 요약 페이지 보기

Connection Summary(연결 요약) 페이지는 연결 이벤트에 대한 검색에 의해 제한되는 맞춤형 역할이 있고 Connection Summary(연결 요약) 페이지에 대한 명시적인 메뉴 기반 액세스 권한이 부여된 사용자에게만 표시됩니다. 이 페이지는 다양한 기준으로 구성된 모니터링되는 네트워크에서의 활동 그래프를 제공합니다. 예를 들어 Connections over Time 그래프에는 사용자가 선택한 간격 동안 모니터링되는 네트워크에서의 총 연결 수가 표시됩니다.

연결 요약 그래프에서는 연결 그래프에서 수행할 수 있는 작업을 거의 모두 동일하게 수행할 수 있습니다. 하지만 Connection Summary(연결 요약) 페이지의 그래프는 집계된 데이터를 기반으로 하기 때문에 그래프가 기반하는 개별 연결 이벤트를 검사할 수는 없습니다. 즉, 연결 요약 그래프에서는 연결 데이터 테이블 보기로 드릴다운할 수 없습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Connection Summary(**연결 요약**)**을(를) 선택합니다.

단계 **2** **Select Device(**디바이스 선택**)** 목록에서 요약을 보려는 디바이스를 선택하거나 **All(**모두**)**을 선택하여 모든 디바이스의 요약을 봅니다.

단계 **3** 연결 그래프를 조작하고 분석하려면 연결 이벤트 그래프 사용, 2805 페이지에 설명된 대로 진행합니다.

팁 기본 시간 범위에 영향을 주지 않고 추가 분석을 수행할 수 있도록 연결 그래프를 분리하려면 **View(**보기**)**를 클릭합니다.

관련 항목

사용자 역할 에스컬레이션
사용자 역할 확대 활성화, 130 페이지

연결 및 보안 인텔리전스 이벤트 기록

기능	버전	세부 사항
DNS 필터링	6.7(베타 기능)	DNS 필터링이 활성화된 경우: • DNS Query(DNS 쿼리) 필드에는 DNS 필터링 일치와 관련된 도메인이 포함될 수 있습니다. • URL 필드가 비어 있더라도 DNS 쿼리, URL 범주 및 URL 평판에 값이 있는 경우, DNS 필터링 기능으로 인해 이벤트가 생성되고 범주 및 평판이 DNS 쿼리에 지정된 도메인에 적용됩니다. • DNS 필터링 및 이벤트, 1679 페이지도 참조하십시오.
사용자 지정 테이블의 연결 이벤트 지원 제거	6.6	이제 연결 이벤트에 대한 사용자 지정 테이블을 생성할 수 없습니다. 업그레이드하는 경우, 연결 이벤트에 대한 기존 사용자 지정 테이블을 계속 사용할 수 있으나 결과가 항상 반환되지 않습니다. 다른 유형의 사용자 지정 테이블에는 변화가 없습니다. 신규/수정된 화면: **Analysis(분석) > Advanced(고급) > Custom Tables(사용자 지정 테이블)**의 Tables(테이블) 옵션 플랫폼: FMC

기능	버전	세부 사항
삭제 및 모든 연결 이벤트 삭제 기능 제거	6.6	삭제 및 모두 삭제 버튼이 연결 이벤트 테이블 페이지에서 제거되었습니다. 모든 연결 이벤트를 제거하려면 데이터 스토리지, 269 페이지의 내용을 참조하십시오. 신규/수정된 화면: **Analysis(분석) > Connections(연결) > Events(이벤트)** 플랫폼: FMC
VRF 및 SGT의 새 필드	6.6	• 인그레스 가상 라우터(시스템 로그: IngressVRF) • 이그레스 가상 라우터(시스템 로그: EgressVRF) • DestinationSecurityGroupType(시스템 로그만 해당) • SourceSecurityGroupType(시스템 로그만 해당)
신규 및 변경된 보안 그룹 태그 필드	6.5	FMC 웹 인터페이스의 필드 변경 사항: • 변경된 필드: 보안 그룹 태그가 소스 SGT로 변경 • 새 필드: 대상 SGT 시스템 로그 필드 변경 사항: • 변경된 필드: SecurityGroup이 SourceSecurityGroupTag로 변경 • 새 필드: • SourceSecurityGroup • DestinationSecurityGroup • DestinationSecurityGroupTag 지원되는 플랫폼: FMC 및 매니지드 디바이스

기능	버전	세부 사항
새 시스템 로그 필드: 이벤트 우선순위	6.5	이 필드는 침입, 파일, 악성코드 또는 보안 인텔리전스 이벤트와 연관된 연결 이벤트를 높은 우선순위로 식별합니다.
시스템 로그의 연결 이벤트 통합 식별자	6.4.0.4	다음 시스템 로그 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

122 장

침입 이벤트 작업

다음 주제에서는 침입 이벤트 작업 방법을 설명합니다.

- 침입 이벤트 정보, 2909 페이지
- 침입 이벤트 검토 및 평가용 도구, 2910 페이지
- 침입 이벤트 라이선스 요구 사항, 2910 페이지
- 침입 이벤트 요구 사항 및 사전 요건, 2910 페이지
- 침입 이벤트 보기, 2911 페이지
- 침입 이벤트 워크플로 페이지, 2931 페이지
- 침입 이벤트 클립보드, 2951 페이지
- 침입 이벤트 통계 보기, 2952 페이지
- 침입 이벤트 성능 그래프 보기, 2955 페이지
- 침입 이벤트 그래프 보기, 2960 페이지
- 침입 이벤트 기록, 2961 페이지

침입 이벤트 정보

Firepower System을 사용하면 네트워크에서 호스트와 호스트 데이터의 가용성, 무결성 및 신뢰성에 영향을 줄 수 있는 트래픽을 모니터링할 수 있습니다. 주요 네트워크 세그먼트에 매니지드 디바이스를 배치하면 악의적인 활동을 위해 네트워크에서 이동하는 패킷을 검토할 수 있습니다. 시스템에는 공격자들이 개발한 광범위한 익스플로잇을 찾는 데 사용하는 몇 가지 메커니즘에 있습니다.

시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트(이전 용어인 'IPS 이벤트'라고 부르기도 함)를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다. 매니지드 디바이스는 Firepower Management Center에 자체 이벤트를 전송합니다. 여기서는 집계된 데이터를 보고 네트워크 자산에 대한 공격을 더 잘 이해할 수 있습니다.

또한 매니지드 디바이스를 인라인, 스위치드 또는 라우티드 침입 시스템으로 구축할 수 있으며, 이를 통해 해로운 것으로 알려진 패킷을 삭제 또는 교체하도록 디바이스를 구성할 수도 있습니다.

침입 이벤트 검토 및 평가용 도구

다음 도구를 사용하여 침입 이벤트를 검토하고 네트워크 환경 및 보안 정책의 컨텍스트에서 중요성을 평가하는 데 필요한 도구를 제공합니다.

- 매니지드 디바이스에서 현재 활동을 검토할 수 있는 이벤트 요약 페이지
- 선택한 기간에 대해 생성할 수 있는 텍스트 기반 보고서와 그래프 보고서. 사용자는 자신만의 보고서를 계획하고 정해진 간격으로 실행되도록 구성할 수 있습니다.
- 공격과 관련된 이벤트 데이터를 수집하기 위해 사용할 수 있는 인시던트 처리 툴. 조사와 응답을 추적하는 데 도움이 되도록 메모를 추가할 수도 있습니다.
- SNMP, 이메일 및 시스템 로그를 위해 구성할 수 있는 자동화된 알림
- 특정 침입 이벤트에 대한 응답과 교정에 사용할 수 있는 자동화된 상관관계 정책
- 더 자세히 조사할 이벤트를 식별하기 위해 데이터에서 드릴다운할 수 있는 사전 정의 및 사용자 지정 워크플로
- 데이터 관리 및 분석을 위한 외부 툴. 시스템 로그 또는 eStreamer를 사용할 수 있습니다. 자세한 내용은 다음을 참조하십시오. 외부 툴을 사용하여 이벤트 분석, 2749 페이지

또한 **Analysis(분석) > Advanced(고급) > Contextual Cross-Launch(상황별 크로스 실행)** 페이지에서 사전 정의된 리소스 등 공개적으로 이용 가능한 정보를 사용하여 악의적인 엔터티에 대해 자세히 알아볼 수 있습니다.

특정 메시지 문자열을 검색하고 이벤트를 생성한 규칙에 대한 설명서를 검색하려면 https://www.snort.org/rule_docs/을 참조하십시오.

침입 이벤트 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

침입 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 이벤트 보기

침입 이벤트를 보고 네트워크 보안에 위협이 있는지 판단할 수 있습니다.

초기 침입 이벤트 보기는 페이지에 액세스하는 데 사용하는 워크플로에 따라 다릅니다. 하나 이상의 드릴다운 페이지, 침입 이벤트의 테이블 보기, 종료 패킷 보기 등 사전 정의 워크플로 중 하나를 사용할 수도 있고 자체 워크플로를 생성할 수도 있습니다. 침입 이벤트가 포함되어 있을 수 있는 맞춤형 테이블을 기반으로 하는 워크플로를 볼 수도 있습니다.

포함된 IP 주소가 많고 **Resolve IP Addresses(IP** 주소 확인**)** 이벤트 보기 설정을 활성화한 경우, 이벤트 보기가 표시되는 속도가 느려질 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 시간 범위 조정 - 타임 윈도우 변경, 2815 페이지의 설명에 따라 이벤트 보기의 시간 범위를 조정합니다.
- 워크플로 변경 - 침입 이벤트 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(**워크플로 전환**)**를 클릭하여 시스템 제공 워크플로 중에서 선택합니다.
- 제한 - 분석에 중요한 침입 이벤트로 보기 범위를 좁히려면 침입 이벤트 워크플로 사용, 2932 페이지를 참조하십시오.
- 이벤트 삭제 - 데이터베이스에서 이벤트를 삭제하려면 **Delete(**삭제**)**를 클릭하여 패킷을 보고 있는 이벤트를 삭제하거나 **Delete All(**모두 삭제**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 삭제합니다.
- 검토 표시 - 검토한 침입 이벤트에 표시하려면 검토된 침입 이벤트 표시, 2926 페이지를 참조하십시오.
- 연결 데이터 보기 - 침입 이벤트에 연결된 연결 데이터를 보려면 침입 이벤트 관련 연결 데이터 보기, 2925 페이지를 참조하십시오.

- 콘텐츠 보기 - 테이블에서 열의 콘텐츠를 보려면 침입 이벤트 필드, 2912 페이지의 설명에 따릅니다.

관련 항목

침입 이벤트 패킷 보기 사용, 2935 페이지

침입 이벤트 필드 정보

시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다.

Firepower Management Center 웹 인터페이스 **Analysis(**분석**) > Intrusions(**침입**) > Events(**이벤트**)**에서 침입 이벤트 데이터를 보거나 외부 도구에서 사용할 수 있도록 일부 필드에서 데이터를 syslog 메시지로 내보낼 수 있습니다. Syslog 필드는 아래 목록에 표시됩니다. 나열된 동등한 syslog가 없는 필드는 syslog 메시지에서 사용할 수 없습니다.

침입 이벤트를 검색할 때 개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다. 예를 들면 해독된 트래픽에 대해 트리거된 침입 이벤트에만 TLS/SSL 정보가 포함됩니다.

참고 Firepower Management Center 웹 인터페이스에서 침입 이벤트 테이블 보기의 일부 필드는 기본적으로 비활성화되어 있습니다. 세션 기간 동안 필드를 활성화하려면 검색 제약 조건을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 열 이름을 클릭합니다.

침입 이벤트 필드

액세스 제어 정책**(**시스템 로그**: ACPolicy)**

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책과 관련된 액세스 제어 정책.

액세스 제어 규칙**(**시스템 로그**: AccessControlRuleName)**

이벤트를 생성한 침입 정책을 호출한 액세스 제어 규칙. `Default Action(기본 작업)`은 규칙이 활성화된 침입 정책이 특정 액세스 제어 규칙과 연결되지 않았지만, 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다.

다음의 경우 (또는 시스템 로그 메시지의 경우 생략됨) 이 필드는 비어 있습니다.

- 관련 규칙/기본 작업 없음: 침입 검사가 액세스 제어 규칙 및 기본 작업과 모두 연결되지 않은 경우(예: 시스템이 어떤 규칙을 적용할지를 결정하기 전에 반드시 통과해야 하는 것으로서 패킷 처리를 위해 지정된 침입 정책에 의해 검토된 경우) (이 정책은 액세스 제어 정책의 Advanced (고급) 탭에서 지정됩니다.)

- 관련 연결 이벤트 없음: 세션에 로깅된 연결 이벤트가 데이터베이스에서 삭제된 경우(예: 연결 이벤트가 침입 이벤트보다 턴오버가 높은 경우)

애플리케이션 프로토콜(시스템 로그: **ApplicationProtocol**)

침입 이벤트를 트리거한 트래픽에서 탐지된 호스트 간 통신을 나타내는 애플리케이션 프로토콜(사용 가능한 경우).

애플리케이션 프로토콜 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 위험성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음). 연결에서 탐지된 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그 중 가장 높은 위험이 표시됩니다.

사업 타당성

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 비즈니스 연관성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음). 연결에서 탐지된 각 애플리케이션 유형에는 관련된 비즈니스 연관성이 있습니다. 이 필드에는 그 중 가장 낮은(가장 연관성이 적은) 값이 표시됩니다.

분류(시스템 로그: **Classification**)

이벤트를 생성한 규칙이 속하는 분류

침입 이벤트 세부 정보, 2072 페이지에서 가능한 분류 값 목록을 참조하십시오.

이 필드를 검색하는 경우, 확인하려는 이벤트를 생성한 규칙의 분류 번호 또는 분류 이름이나 설명의 전체 또는 일부를 입력합니다. 쉼표로 구분된 숫자, 이름 또는 설명의 목록을 입력할 수도 있습니다. 마지막으로, 사용자 지정 분류를 추가하는 경우 이름이나 설명의 전체 또는 일부를 사용하여 검색할 수도 있습니다.

클라이언트(시스템 로그: **Client**)

침입 이벤트를 트리거한 트래픽에서 탐지된 모니터링되는 호스트에서 실행 중인 소프트웨어를 나타내는 클라이언트 애플리케이션(사용 가능한 경우).

클라이언트 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

Connection Counter (시스템 로그만 해당)

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

Connection Instance ID (시스템 로그만 해당)

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

Count(개수)

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

CVE ID

이 필드는 검색 전용입니다.

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)에서 취약성과 관련된 식별 번호에 의한 검색.

Destination Continent(대상 대륙)

침입 이벤트와 관련된 수신 호스트의 대륙.

Destination Country(대상 국가)

침입 이벤트와 관련된 수신 호스트의 국가.

대상 **IP**(시스템 로그: **DstIP**)

침입 이벤트와 관련된 수신 호스트가 사용하는 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

대상 포트/**ICMP** 코드(시스템 로그: **DstPort, ICMPCode**)

트래픽을 수신하는 호스트의 포트 번호. ICMP 트래픽에서 포트 번호가 없는 경우 이 필드에 ICMP 코드가 표시됩니다.

대상 사용자

연결 이벤트의 응답자 IP와 연결된 사용자 이름입니다. 이 호스트는 익스플로잇을 수신하는 호스트일 수도 있고 아닐 수도 있습니다. 이 값은 일반적으로 네트워크의 사용자에게만 알려져 있습니다.

선택합니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

디바이스

액세스 제어 정책이 구축된 매니지드 디바이스입니다.

스태킹된 구성의 기본 및 보조 디바이스는 마치 별도의 디바이스인 것처럼 침입 이벤트를 보고합니다.

DeviceUUID (시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

도메인

침입을 탐지한 디바이스의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

이그레스 인터페이스**(**시스템 로그**: EgressInterface)**

이벤트를 트리거한 패킷의 이그레스 인터페이스. 패시브 인터페이스에 대해서는 이 인터페이스 열이 채워지지 않습니다.

이그레스 보안 영역**(**시스템 로그**: EgressZone)**

이벤트를 트리거한 패킷의 이그레스 보안 영역. 패시브 구축에서는 이 보안 영역 필드가 채워지지 않습니다.

이그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에서 벗어날 때 사용하는 가상 라우터의 이름입니다.

이메일 첨부 파일

MIME Content-Disposition 헤더에서 추출된 MIME 첨부 파일 이름. 첨부 파일 이름을 표시하려면 SMTP 프리프로세서 **Log MIME Attachment Names** 옵션을 활성화해야 합니다. 여러 첨부 파일 이름이 지원됩니다.

Email Headers(이메일 헤더**)**

이 필드는 검색 전용입니다.

이메일 헤더에서 추출된 데이터.

이메일 헤더를 SMTP 트래픽의 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers(**헤더 로깅**)** 옵션을 활성화해야 합니다.

Email Recipient(이메일 수신자**)**

SMTP RCPT TO 명령에서 추출된 이메일 수신자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log To Addresses(**주소로 로깅**)** 옵션을 활성화해야 합니다. 여러 수신자 주소가 지원됩니다.

Email Sender(이메일 발신자**)**

SMTP MAIL FROM 명령에서 추출된 이메일 발신자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log From Addresses(**주소에서 로깅**)** 옵션을 활성화해야 합니다. 여러 발신자 주소가 지원됩니다.

첫 번째 패킷 시간 **(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

Generator(생성기**)**

이벤트를 생성한 구성 요소.

다음에 나오는 침입 이벤트 필드인 GID, Message(메시지) 및 Snort ID에 대한 정보도 참조하십시오.

GID(시스템 로그만 있음**)**

Generator ID(생성기 ID)로, 이벤트를 생성한 구성 요소의 ID.

다음에 나오는 침입 이벤트 필드인 Generator(생성기), Message(메시지) 및 Snort ID에 대한 정보도 참조하십시오.

HTTP Hostname(HTTP 호스트네임**)**

HTTP 요청 Host 헤더에서 추출된 호스트 이름(해당되는 경우). 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다.

호스트 이름을 HTTP 클라이언트 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log Hostname(**호스트네임 로깅**)** 옵션을 활성화해야 합니다.

테이블 보기에서 이 열에는 추출된 호스트 이름의 첫 50자가 표시됩니다. 약식 호스트 이름의 표시된 부분 위로 마우스 포인터를 이동하여 최대 256바이트까지 전체 이름을 표시할 수 있습니다. 패킷 보기에서 전체 호스트 이름을 최대 256바이트까지 표시할 수 있습니다.

HTTP 응답 코드**(**시스템 로그**: HTTPResponse)**

이벤트를 트리거한 연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 요청 패킷에 항상 URI가 포함되는 것은 아닙니다.

URI를 HTTP 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log URI(URI** 로깅**)** 옵션을 활성화해야 합니다.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports(**양쪽 포트에서 스트림 리어셈블리 수행**)** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다.

이 열에는 추출된 URI의 첫 50자가 표시됩니다. 약식 URI의 표시된 부분 위로 마우스 포인터를 이동하여 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

영향

이 필드의 영향 레벨은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관 관계를 나타냅니다.

이 필드를 검색하는 경우 영향 아이콘이 색상 또는 부분 문자열을 지정하지 않습니다. 예를 들어, 파란색, 레벨 **1**또는 **0**을 사용하지 마십시오. 대/소문자 유효한 값은 다음과 같습니다.

- 영향 0, 영향 레벨 0
- 영향 1, 영향 레벨 1
- 영향 2, 영향 레벨 2
- 영향 3, 영향 레벨 3
- 영향 4, 영향 레벨 4

NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

인그레스 인터페이스**(**시스템 로그**: IngressInterface)**

이벤트를 트리거한 패킷의 인그레스 인터페이스입니다. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다.

인그레스 보안 영역**(**시스템 로그**: IngressZone)**

이벤트를 트리거한 패킷의 인그레스 보안 영역. 수동 배포에서는 이 보안 영역 필드만 입력됩니다.

인그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에 진입할 때 사용하는 가상 라우터의 이름입니다.

인라인 결과**(**시스템 로그**: InlineResult)**

워크플로 및 테이블 보기에서 이 필드는 다음 중 하나를 표시합니다.

표 ***323:*** 워크플로 및 테이블 보기에서 인라인 결과 필드 내용

아이콘	표시 내용
검은색 아래쪽 화살표	시스템이 규칙을 트리거한 패킷을 삭제했음을 나타냅니다.
회색 아래쪽 화살표	(인라인 구축에서) **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화하는 경우 또는 시스템 정리 중 Drop and Generate(삭제 및 생성) 규칙이 이벤트를 생성한 경우 IPS가 패킷을 삭제했음을 나타냅니다.
아이콘 없음(공란)	트리거된 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되지 않았음을 나타냅니다.

수동 구축에서 인라인 인터페이스가 탭 모드에 있는 경우를 포함하여 침입 정책의 규칙 상태 또는 인라인 삭제 작업에 상관없이 시스템은 패킷을 삭제하지 않습니다.

이 필드를 검색하는 경우 다음 중 하나를 입력합니다.

- **dropped** - 패킷이 인라인 구축에서 삭제되는지 여부를 지정
- **would have dropped** - 인라인 구축에서 패킷을 삭제하도록 침입 정책을 설정했다면 패킷이 삭제되었을 것인지를 지정

침입 정책 **(**시스템 로그**: IntrusionPolicy)**

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책. 액세스 제어 정책에 대한 기본 작업으로 침입 정책을 선택할 수 있습니다. 또는 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다.

IOC(시스템 로그**: NumIOC)**

침입 이벤트를 트리거한 트래픽이 연결과 관련된 호스트에 대해 IOC(indication of compromise)도 트리거했는지 여부.

이 필드를 검색하는 경우 **triggered(**트리거됨**)** 또는 **n/a(**해당 없음**)**를 지정합니다.

메시지**(**시스템 로그**: Message)**

이벤트에 대한 설명 텍스트 규칙 기반 침입 이벤트의 경우, 이벤트 메시지는 규칙에서 가져옵니다. 디코더 및 프리프로세서 기반 이벤트의 경우, 이벤트 메시지는 하드 코드됩니다.

Generator ID(GID), Snort ID(SID) 및 SID 버전(Revision)이 각 메시지 끝에 콜론으로 구분되는 숫자 형식으로 괄호안에 추가됩니다(GID:SID:version). 예: **(1:36330:2)**.

MPLS 레이블**(**시스템 로그**: MPLS_Label)**

이 침입 이벤트를 트리거한 패킷에 연결된 Multiprotocol Label Switching(다중 프로토콜 레이블 스위칭) 레이블.

네트워크 분석 정책(시스템 로그: **NAPPolicy**)

이벤드 생성과 관련된 네트워크 분석(해당되는 경우).

이 필드에는 추출된 URI의 첫 50자가 표시됩니다. 약식 URI의 표시된 부분 위로 마우스 포인터를 이동하여 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

원래 클라이언트 **IP**

XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더에서 추출된 원래 클라이언트 IP 주소.

이 필드의 값을 표시하려면 네트워크 분석 정책에서 HTTP 프리프로세서 **Extract Original Client IP Address**(원래 클라이언트 **IP** 주소 추출) 옵션을 활성화해야 합니다. 또한 네트워크 분석 정책에서 최대 6개의 맞춤형 클라이언트 IP 헤더를 지정할 수 있으며 시스템이 Original Client IP 이벤트 필드에 대한 값을 선택하는 우선순위 순서를 설정할 수 있습니다.

우선순위(시스템 로그: **Priority**)

Cisco Talos Intelligence Group(Talos)에 따라 결정된 이벤트 우선순위. 우선순위는 `priority` 키워드의 값 또는 `classtype`키워드의 값에 해당합니다. 기타 침입 이벤트의 경우, 우선순위는 디코더 또는 프리프로세서에 의해 결정됩니다. 유효한 값은 high(높음), medium(중간) 및 low(낮음)입니다.

프로토콜(시스템 로그: **Protocol**)

Firepower Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

http://www.iana.org/assignments/protocol-numbers에 열거된 대로 연결에 사용된 전송 프로토콜의 이름 또는 번호. 이것은 소스 및 대상 포트/ICMP 열과 관련된 프로토콜입니다.

검토자

이벤트를 검토한 사용자의 이름. 이 필드를 검색하는 경우, **`unreviewed`**(검토 안 함)를 입력하고 검토되지 않은 이벤트를 검색할 수 있습니다.

Revision(시스템 로그만 있음)

이벤트 생성에 사용된 서명의 버전.

다음에 나오는 침입 이벤트 필드인 Generator(생성기), GID, Message(메시지), SID 및 Snort ID에 대한 정보도 참조하십시오.

보안 상황(시스템 로그: **Context**)

트래픽이 통과된 가상 방화벽 그룹을 식별하는 메타데이터. 시스템은 다중 상황 모드의 ASA FirePOWER에 대해서만 이 필드에 내용을 입력합니다.

SID(시스템 로그만 있음)

이벤트를 생성하는 규칙의 서명 ID(Snort ID로도 알려짐).

다음에 나오는 침입 이벤트 필드인 Generator(생성기), GID, Message(메시지), Revision(개정) 및 Snort ID에 대한 정보도 참조하십시오.

Snort ID

이 필드는 검색 전용입니다.

(시스템 로그 필드에서 SID 참조).

검색을 수행하는 경우 이벤트를 생성한 규칙의 Snort ID(SID)를 지정합니다. 또는 선택적으로 규칙의 GID(Generator ID)와 SID 조합을 지정합니다. 여기서 GID와 SID는 GID:SID 형식으로 콜론(:)으로 구분됩니다. 다음 표에서 어떠한 값도 지정할 수 있습니다.

표 ***324: Snort ID*** 검색 값

값	예
단일 SID	10000
SID 범위	10000-11000
SID보다 큼	>10000
SID보다 크거나 같음	>=10000
SID보다 작음	<10000
SID보다 작거나 같음	<=10000
쉼표로 구분된 SID 목록	10000,11000,12000
단일 GID:SID 조합	1:10000
쉼표로 구분된 GID:SID 조합의 목록	1:10000,1:11000,1:12000
쉼표로 구분된 SID 및 GID:SID 조합의 목록	10000,1:11000,12000

보고 있는 이벤트의 SID가 Message(메시지) 열에 나열됩니다. 자세한 내용은 Message(메시지) 필드에 대한 이 섹션의 설명을 참조하십시오.

소스 대륙

침입 이벤트와 관련된 전송 호스트의 대륙.

소스 국가

침입 이벤트와 관련된 전송 호스트의 국가.

소스 **IP(**시스템 로그**: SrcIP)**

침입 이벤트와 관련된 전송 호스트가 사용하는 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

소스 포트/**ICMP** 유형(시스템 로그: **SrcPort, ICMPType**)

전송 호스트의 포트 번호. ICMP 트래픽에서 포트 번호가 없는 경우 이 필드에 ICMP 유형이 표시됩니다.

소스 사용자(시스템 로그: **User**)

연결을 시작한 호스트의 IP 주소와 연결된 사용자 이름으로, 익스플로잇의 소스 호스트일 수도 있고 아닐 수도 있습니다. 이 사용자 값은 일반적으로 네트워크의 사용자에게만 알려져 있습니다.

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

SSL 실제 작업(시스템 로그: **SSLActualAction**)

Firepower Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

시스템이 암호화된 트래픽에 적용하는 작업.

차단/차단 및 재설정

차단된 암호화된 연결을 나타냅니다.

암호 해독(재서명)

다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(대체 키)

대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(알려진 키)

알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.

기본 작업

연결이 기본 작업에 의해 처리되었음을 나타냅니다.

암호 해독 안 함

시스템이 암호 해독하지 않은 연결을 나타냅니다.

검색 워크플로 페이지의 **SSL Status**(**SSL** 상태) 필드에 필드값이 표시됩니다.

SSL 인증서 정보

이 필드는 검색 전용입니다.

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)

- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number(일련 번호)
- Certificate Fingerprint(인증서 지문)
- Public Key Fingerprint(공개 키 지문)

SSL Failure Reason(SSL 실패 이유)

이 필드는 검색 전용입니다.

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)

- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL Status

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)** (SSL 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)(암호 해독 하지 않음(알려지지 않은 암호화 그룹))`로 표시됩니다.

인증서 세부사항을 보려면 잠금 아이콘을 클릭합니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL Subject/Issuer Country(SSL 대상자/발급자 국가)

이 필드는 검색 전용입니다.

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

시간

이벤트의 날짜 및 시간. 이 필드는 검색할 수 없습니다.

VLAN ID (시스템 로그: VLAN_ID)

침입 이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID

웹 애플리케이션(시스템 로그: **WebApplication)**

침입 이벤트를 트리거한 트래픽에서 탐지된 HTTP 트래픽의 내용 또는 요청된 URL을 나타내는 웹 애플리케이션.

HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 그 대신 일반 웹 브라우징 지정을 제공합니다.

웹 애플리케이션 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

관련 항목

이벤트 검색, 2825 페이지

침입 이벤트 영향 레벨

이벤트가 네트워크에 미치는 영향을 평가할 수 있도록 Firepower Management Center는 침입 이벤트의 테이블 보기에 영향 레벨을 표시합니다. 각 이벤트에 대해 시스템은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관관계를 색으로 나타내는 영향 레벨 아이콘을 추가합니다.

참고 NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

다음 표에서는 영향 레벨의 가능한 값에 대해 설명합니다.

표 ***325:*** 영향 레벨

영향 레벨	취약성	색상	설명
알 수 없음(0)	알 수 없음	그레이	소스 호스트나 대상 호스트 모두 네트워크 검색에 의해 모니터링되는 네트워크에 없습니다.
취약(1)	취약함	빨간색	다음 중 하나에 해당합니다. • 소스 또는 대상 호스트가 네트워크 맵에 있으며, 취약성이 호스트에 매핑됨 • 소스 또는 대상 호스트가 바이러스, 트로이 목마 또는 기타 악성 소프트웨어에 감염되었을 가능성이 있음

영향 레벨	취약성	색상	설명
잠재적으로 취약(2)	잠재적으로 취약함	오렌지	소스 또는 대상 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우 포트가 서버 애플리케이션 프로토콜을 실행함 • 포트로 향하는 트래픽이 아닌 경우 호스트가 프로토콜을 사용함
현재 취약하지 않음(3)	현재 취약하지 않음	노란색	소스 또는 대상 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우(예: TCP 또는 UDP), 포트가 열려 있지 않음 • 포트로 향하는 트래픽이 아닌 경우(예: ICMP), 호스트가 프로토콜을 사용하지 않음
알 수 없는 대상(4)	알 수 없는 대상	블루	소스 호스트 또는 대상 호스트가 모니터링되는 호스트에 있지만 네트워크 맵에는 호스트에 대한 항목이 없음.

침입 이벤트 관련 연결 데이터 보기

시스템은 침입 이벤트가 탐지된 연결을 로깅할 수 있습니다. 이 로깅은 액세스 제어 규칙과 연결된 침입 정책에 대해 자동으로 수행되지만, 기본 작업에 대한 관련 연결 데이터를 보려면 연결 로깅을 수동으로 활성화해야 합니다.

이벤트의 테이블 보기 간에 탐색할 때에는 관련된 데이터를 보는 것이 가장 유용합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 테이블의 확인란을 사용하여 침입 이벤트를 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 **Connections(**연결**)**를 선택합니다.

팁 특정 연결에 연결된 침입 이벤트도 비슷한 방법으로 볼 수 있습니다. 자세한 내용은 워크플로 간 탐색, 2821 페이지를 참고하십시오.

관련 항목

허용된 연결에 대한 로깅, 2864 페이지
침입 이벤트 워크플로 사용, 2932 페이지
연결 및 보안 인텔리전스 이벤트 테이블 사용, 2900 페이지

검토된 침입 이벤트 표시

침입 이벤트가 악의적이지 않다고 확신하면 이벤트를 검토한 것으로 표시할 수 있습니다.

침입 이벤트를 검토한 결과 네트워크 보안에 위협이 되지 않을 것으로 확신하는 경우(예: 네트워크의 호스트 중 어떤 것도 탐지된 익스플로잇에 취약하지 않음을 알고 있음) 해당 이벤트를 검토한 것으로 표시할 수 있습니다. 검토된 이벤트는 이벤트 데이터베이스에 저장되며 이벤트 요약 통계에 포함되지만, 기본 침입 이벤트 페이지에는 더 이상 나타나지 않습니다. 사용자 이름이 검토자로 표시됩니다.

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

백업을 수행한 후 검토한 침입 이벤트를 삭제하면, 백업의 복원은 삭제된 침입 이벤트를 복원하지만 검토된 상태는 복원하지 않습니다. 복원된 침입 이벤트는 **Reviewed Events(**검토된 이벤트**)**가 아니라 **Intrusion Events(**침입 이벤트**)**에서 볼 수 있습니다.

프로시저

침입 이벤트를 보여주는 페이지에는 두 가지 옵션이 있습니다.

- 이벤트 목록에서 하나 이상의 침입 이벤트를 표시하려면, 이벤트 옆의 확인란을 선택하고 **Review(**검토**)**를 클릭합니다.
- 이벤트 목록에서 모든 침입 이벤트를 표시하려 **Review All(**모두 검토**)**을 클릭합니다.

관련 항목

침입 이벤트 워크플로 사용, 2932 페이지

이전에 검토된 침입 이벤트 보기

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Reviewed Events(**검토한 이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 타임 윈도우 변경, 2815 페이지에 설명된 대로 시간 범위를 조정합니다.
- 침입 이벤트 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(**워크플로 전환**)**를 클릭하여 시스템 제공 워크플로 중에서 선택합니다.
- 표시되는 이벤트에 대한 자세한 내용은 침입 이벤트 필드, 2912 페이지를 참조하십시오.

관련 항목

침입 이벤트 워크플로 사용, 2932 페이지

검토된 침입 이벤트를 검토되지 않은 것으로 표시

이벤트를 검토하지 않은 것으로 표시함으로써 검토된 이벤트를 기본 침입 이벤트 보기로 되돌릴 수 있습니다.

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

프로시저

검토된 이벤트를 표시하는 페이지에는 두 가지 옵션이 있습니다.

- 검토된 이벤트 목록에서 개별 침입 이벤트를 제거하려면 특정 이벤트 옆의 확인란을 선택하고 **Unreview(**검토 취소**)**를 클릭합니다.
- 검토된 이벤트의 목록에서 모든 침입 이벤트를 제거하려면 **Unreview All(**모두 검토 취소**)**을 클릭합니다.

전처리기 이벤트

전처리기는 다음 두 가지 기능을 제공합니다. 패킷에서 지정된 작업을 수행하고(예를 들어 HTTP 트래픽 디코딩 및 표준화) 패킷이 전처리기 옵션을 트리거하고 연결된 전처리기 규칙이 활성화될 때마다 이벤트를 생성하여 지정된 전처리기 옵션의 실행을 보고하는 것입니다. 예를 들어 `Double Encoding(이중 인코딩)` HTTP 검사 옵션과 HTTP 검사 생성기(GID)가 119이고 Snort ID(SID)가 2인 연

결된 전처리기 규칙을 활성화하여 전처리기에 IIS 이중 인코딩된 트래픽이 발생할 때 이벤트를 생성할 수 있습니다.

전처리기의 실행을 보고하는 이벤트를 생성하면 비정상적인 프로토콜 익스플로잇을 탐지하는 데 도움이 됩니다. 예를 들어 공격자는 중복 IP 프래그먼트를 조작하여 호스트에서 DoS 공격을 일으킬 수 있습니다. IP 조각 모음 전처리기는 이 유형의 공격을 탐지하고 이에 대한 침입 이벤트를 생성할 수 있습니다.

패킷 표시에 이벤트에 대한 자세한 규칙 설명이 포함되지 않는다는 점에서 전처리기 이벤트는 규칙 이벤트와 다릅니다. 대신 패킷 표시에는 이벤트 메시지, GID, SID, 패킷 헤더 데이터 및 패킷 페이로드가 나타납니다. 이를 통해 패킷의 헤더 정보를 분석하고, 헤더 옵션이 사용 중인지와 시스템을 악용할 수 있는지를 파악하고, 패킷 페이로드를 검사할 수 있습니다. 전처리기가 각 패킷을 분석한 후 규칙 엔진은 잠재적인 콘텐츠 수준 위협을 추가 분석하고 보고할 수 있도록 이에 대해 적절한 규칙을 실행합니다(전처리기가 이를 조각 모음하고 유효한 세션의 일부로 설정할 수 있는 경우).

전처리기 생성기 ID

각 전처리기에는 어떤 전처리기가 패킷에 의해 트리거되었는지를 나타내는 자체 GID(Generator ID)가 있습니다. 일부 전처리기에는 잠재적 공격을 분류하는 ID 번호인 관련 SID도 있습니다. 이를 통해 규칙의 Snort ID(SID)가 규칙을 트리거하는 패킷의 컨텍스트를 제공하는 것과 유사한 방식으로 이벤트의 유형을 카테고리화하여 이벤트를 더 효과적으로 분석할 수 있습니다. 침입 정책 Rules(규칙) 페이지의 Preprocessors(전처리기) 필터 그룹에서 전처리기별로 전처리기 규칙을 나열할 수 있습니다. 또한 Category(카테고리) 필터 그룹의 전처리기 및 패킷 디코더 하위 그룹에 전처리기 규칙을 나열할 수도 있습니다.

참고 표준 텍스트 규칙에 의해 생성된 이벤트는 생성기 ID 1(전역 도메인 또는 레거시 GID) 또는 1000 - 2000(하위 도메인)을 갖습니다. 공유 개체 규칙의 경우, 이벤트에 생성기 ID는 3입니다. 두 규칙 모두 이벤트의 SID는 트리거된 특정 규칙을 나타냅니다.

다음 표에서는 각 GID를 생성하는 이벤트 유형에 대해 설명합니다.

표 ***326:*** 생성기 ***ID***

ID	**Component(**구성 요소**)**	설명
1	표준 텍스트 규칙	패킷이 표준 텍스트 규칙(전역 도메인 또는 레거시 GID)을 트리거할 때 이벤트가 생성되었습니다.
2	태그가 지정된 패킷	태그 지정된 세션에서 패킷을 생성하는 Tag 생성기에 의해 이벤트가 생성되었습니다. 이는 `tag` 규칙 옵션이 사용될 때 발생합니다.
3	공유 개체 규칙	패킷이 공유 개체 규칙을 트리거할 때 이벤트가 생성되었습니다.

ID	Component(구성 요소)	설명
102	HTTP 디코더	디코더 엔진이 패킷 내에서 HTTP 데이터를 디코딩했습니다.
105	Back Orifice 탐지기	Back Orifice 탐지기가 패킷에 연결된 Back Orifice 공격을 식별했습니다.
106	RPC 디코더	RPC 디코더가 패킷을 디코딩했습니다.
116	패킷 디코더	패킷 디코더에 의해 이벤트가 생성되었습니다.
119, 120	HTTP 검사 전처리기	HTTP 검사 전처리기에 의해 이벤트가 생성되었습니다. GID 120 규칙은 서버별 HTTP 트래픽과 관련이 있습니다.
122	포트스캔 탐지기	포트스캔 플로우 디코더에 의해 이벤트가 생성되었습니다.
123	IP 조각 모음기	조각난 IP 데이터그램을 제대로 리어셈블할 수 없을 때 이벤트가 생성되었습니다.
124	SMTP 디코더	SMTP 전처리기가 SMTP 동사에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
125	FTP 디코더	FTP/텔넷 디코더가 FTP 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
126	텔넷 디코더	FTP/텔넷 디코더가 텔넷 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
128	SSH 전처리기	SSH 전처리기가 SSH 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
129	스트림 전처리기	스트림 전처리기에 의한 스트림 전처리 중에 이벤트가 생성되었습니다.
131	DNS 전처리기	DNS 전처리기에 의해 이벤트가 생성되었습니다.
133	DCE/RPC 전처리기	DCE/RPC 전처리기에 의해 이벤트가 생성되었습니다.

ID	Component(구성 요소)	설명
134	규칙 레이턴시 패킷 레이턴시	규칙 레이턴시가 침입 규칙의 그룹을 일시 중지(134:1) 또는 다시 활성화(134:2)하거나 패킷 레이턴시 임계값이 초과되었기 때문에 시스템이 패킷 검사를 중지하여(134:3) 이벤트가 생성되었습니다.
135	속도 기반 공격 탐지기	속도 기반 공격 탐지기가 네트워크의 호스트에 대한 과도한 연결을 식별하여 이벤트가 생성되었습니다.
137	SSL 전처리기	TLS/SSL 전처리기에 의해 이벤트가 생성되었습니다.
138, 139	민감한 데이터 전처리기	민감한 데이터 전처리기에 의해 이벤트가 생성되었습니다.
140	SIP 전처리기	SIP 전처리기에 의해 이벤트가 생성되었습니다.
141	IMAP 전처리기	IMAP 전처리기에 의해 이벤트가 생성되었습니다.
142	POP 전처리기	POP 전처리기에 의해 이벤트가 생성되었습니다.
143	GTP 전처리기	GTP 전처리기에 의해 이벤트가 생성되었습니다.
144	Modbus 전처리기	Modbus SCADA 전처리기에 의해 이벤트가 생성되었습니다.
145	DNP3 전처리기	DNP3 SCADA 전처리기에 의해 이벤트가 생성되었습니다.
148	CIP 전처리기	CIP SCADA 전처리기에 의해 이벤트가 생성되었습니다.
149	S7Commplus 전처리기	Modbus SCADA 전처리기에 의해 이벤트가 생성되었습니다.
1000 - 2000	표준 텍스트 규칙	패킷이 표준 텍스트 규칙(하위 도메인)을 트리거할 때 이벤트가 생성되었습니다.

침입 이벤트 워크플로 페이지

현재 침입 정책에서 활성화된 전처리기, 디코더 및 침입 규칙은 모니터링하는 트래픽이 정책을 위반할 때마다 침입 이벤트를 생성합니다.

Firepower System은 이벤트 데이터로 채워지고 침입 이벤트를 보고 분석할 수 있는 사전 정의된 워크플로 집합을 제공합니다. 이러한 각 워크플로는 평가할 침입 이벤트를 정확히 찾아낼 수 있도록 일련의 페이지를 통해 사용자를 안내합니다.

사전 정의된 침입 이벤트 워크플로에는 세 가지 페이지 유형 또는 이벤트 보기가 포함되어 있습니다.

- 하나 이상의 드릴다운 페이지
- 침입 이벤트의 테이블 보기
- 패킷 보기

*Drill-down(*드릴다운*)* 페이지에는 일반적으로 한 테이블(일부 드릴다운 보기의 경우 둘 이상의 테이블)에 하나의 특정 정보 유형을 볼 수 있는 둘 이상의 열이 포함되어 있습니다.

하나 이상의 대상 포트에 대한 추가 정보를 찾기 위해 "드릴다운"할 때 자동으로 이러한 이벤트를 선택하게 되며, 워크플로의 다음 페이지가 나타납니다. 이런 식으로 드릴다운 테이블은 한 번에 분석하는 이벤트 수를 줄입니다.

침입 이벤트의 초기 테이블 보기에서는 각 침입 이벤트가 고유한 행에 나열됩니다. 테이블의 열에는 시간, 소스 IP 주소와 포트, 대상 IP 주소와 포트, 이벤트 우선순위, 이벤트 메시지 등의 정보가 나열됩니다.

워크플로에서 이벤트를 선택하고 다음 페이지를 표시하는 대신, 테이블 보기에서 이벤트를 선택하면 제약 조건이라는 것이 추가됩니다. 제약 조건이란 분석할 이벤트 유형에 적용하는 제한입니다.

예를 들어 임의의 열에서 닫기( )을 클릭하고 드롭다운 목록에서 **Time(**시간**)**을 지우면 열 중 하나로 Time(시간)을 제거할 수 있습니다. 분석에서 이벤트 목록을 좁히려면 테이블 보기의 행 중 하나에서 값의 링크를 클릭할 수 있습니다. 예를 들어 소스 IP 주소 중 하나(잠재적인 공격자)에서 생성되는 이벤트로 분석을 제한하려면 **Source IP Address(**소스 **IP** 주소**)** 열에서 해당 IP 주소를 클릭합니다.

테이블 보기에서 하나 이상의 행을 선택한 다음 **View(**보기**)**를 클릭하면 패킷 보기가 나타납니다. 패킷 보기는 규칙을 트리거한 패킷 또는 이벤트를 생성한 전처리기에 대한 정보를 제공합니다. 패킷 보기의 각 섹션에는 패킷의 특정 레이어에 대한 정보가 포함되어 있습니다. 더 많은 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다.

미리 정의된 워크플로가 특정 요구 사항을 충족하지 않는 경우, 관심 있는 정보만 표시되는 맞춤형 워크플로를 만들 수 있습니다. 맞춤형 침입 이벤트 워크플로에는 드릴 다운 페이지나 이벤트의 테이블 보기 또는 둘 다가 포함될 수 있습니다. 시스템은 자동으로 패킷 페이지를 마지막 페이지로 포함

합니다. 이벤트를 조사하려는 방법에 따라 사전 정의 워크플로와 맞춤형 워크플로 간에 손쉽게 전환할 수 있습니다.

침입 이벤트 워크플로 사용

이벤트의 드릴다운 보기 및 테이블 보기에는 몇 가지 공통된 기능이 있습니다. 이러한 기능을 사용하면 이벤트 목록의 범위를 좁히고 관련 이벤트의 그룹으로 분석을 집중할 수 있습니다.

서로 다른 워크플로 페이지에 동일한 침입 이벤트가 표시되지 않도록, 시간 범위는 다른 이벤트 페이지를 표시하기 위해 페이지 아래쪽에서 링크를 클릭할 때 일시 중지되고, 후속 페이지에서 다른 작업을 수행하기 위해 클릭할 때 다시 시작됩니다.

팁 프로세스의 어떤 지점에서든 제약 조건을 검색 기준 집합으로 저장할 수 있습니다. 예를 들어 지난 며칠 동안 네트워크가 단일 IP 주소의 공격자에 의해 프로브된 것을 발견한 경우, 조사 중에 제약 조건을 저장한 다음 나중에 다시 사용할 수 있습니다. 그러나 복합 제약 조건을 검색 기준 집합으로 저장할 수는 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**를 사용하여 침입 이벤트 워크플로에 액세스합니다.

단계 **2** 원하는 경우, 침입 이벤트 드릴다운 페이지 제약 조건, 2934 페이지 또는 침입 이벤트 테이블 보기 제약 조건, 2934 페이지에 설명된 대로 이벤트 보기에 나타나는 침입 이벤트 수를 제한합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 표시되는 열에 대한 자세한 내용은 침입 이벤트 필드, 2912 페이지를 참조하십시오.
- 호스트의 프로파일을 보려면 호스트 IP 주소 옆에 표시되는 **Host Profile(**호스트 프로파일**)**을 클릭합니다.
- 지리위치 세부 사항을 보려면 Source Country(소스 국가) 또는 Destination Country(대상 국가) 열에 표시되는 플래그를 클릭합니다.
- Firepower 시스템 외부에서 이용할 수 있는 소스의 데이터를 보려면 이벤트 값에서 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지 섹션을 참조해 주십시오.
- 이벤트에 대한 일반 정보를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지를 참고하십시오.
- 표시된 이벤트의 시간 및 날짜 범위를 수정하려면 타임 윈도우 변경, 2815 페이지를 참조하십시오.

팁 이벤트 보기에 침입 이벤트가 나타나지 않는 경우 지정된 기간을 조정하면 결과가 반환될 수 있습니다. 더 오래된 시간 범위를 지정한 경우, 해당 시간 범위의 이벤트가 삭제되었을 수 있습니다. 규칙 임계값 지정 구성을 조정하면 이벤트가 생성될 수 있습니다.

참고 어플라이언스의 구성된 기간(전역 또는 이벤트 전용 모두 해당)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 현재 워크플로 페이지에서 이벤트를 정렬하거나 현재 워크플로 페이지 내에서 이동하려면 워크플로 사용, 2793 페이지을 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다.
- 나중에 인시던트에 전송할 수 있도록 이벤트를 클립보드에 추가하려면 **Copy(**복사**)** 또는 **Copy All(**모두 복사**)**을 클릭합니다.
- 이벤트 데이터베이스에서 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.
- 이벤트를 검토된 것으로 표시하여 침입 이벤트 페이지에서는 제거하되 이벤트 데이터베이스에서는 제거하지 않으려면 검토된 침입 이벤트 표시, 2926 페이지을 참조하십시오.
- 선택된 각 이벤트를 트리거한 패킷의 로컬 사본(libpcap 형식의 패킷 캡처 파일)을 다운로드하려면 다운로드하려는 패킷이 트리거한 이벤트 옆의 확인란을 선택한 다음 **Download Packets(**패킷 다운로드**)**를 클릭하거나 **Download All Packets(**모든 패킷 다운로드**)**를 클릭합니다. 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다.
- 다른 이벤트 보기로 이동해 연결된 이벤트를 보려면 워크플로 간 탐색, 2821 페이지을 참조하십시오.
- 다른 워크플로우를 임시로 사용하려면 **(**워크플로우 전환**)**를 클릭합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다.
- Summary Dashboard(요약 대시보드)의 Intrusion Events(침입 이벤트) 섹션을 보려면 **Dashboards(**대시보드**)**를 클릭합니다.
- 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.
- 현재 보기의 데이터를 기반으로 보고서를 생성하려면 이벤트 보기에서 보고서 템플릿 생성, 2657 페이지을 참조하십시오.

관련 항목

이벤트 검색, 2825 페이지
북마크, 2822 페이지

침입 이벤트 드릴다운 페이지 제약 조건

다음 표에서는 드릴다운 페이지를 사용하는 방법에 대해 설명합니다.

표 ***327:*** 드릴다운 페이지에서 이벤트 제한

목적	방법
다음 워크플로 페이지로 드릴다운하여 특정 값으로 제한	값을 클릭 합니다. 예를 들어 Destination Port(대상 포트) 워크플로에서 대상 포트 80으로 이벤트를 제한하려면 **DST Port/ICMP Code(DST** 포트**/ICMP** 코드**)** 열에서 **80/tcp**를 클릭합니다. 워크플로의 다음 페이지인 Events(이벤트)가 나타나고, 포트 80/tcp 이벤트만 포함됩니다.
다음 워크플로 페이지로 드릴다운하여 선택한 이벤트로 제한	다음 워크플로 페이지에서 보려는 이벤트 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다. 예를 들어 Destination Port(목적지 포트) 워크플로에서 목적지 포트 20/tcp 및 21/tcp로 이벤트를 제한하려면 해당 포트의 행 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다. 워크플로의 다음 페이지인 Events(이벤트)가 나타나고, 포트 20/tcp 및 21/tcp 이벤트만 포함됩니다. 여러 행으로 제한하려는 경우 테이블에 열이 두 개 이상이면(Count 열은 포함하지 않음) 복합 제약 조건을 구축해야 합니다. 복합 제약 조건은 의도한 것보다 더 많은 이벤트가 제약 조건에 포함되지 않도록 보장합니다. 예를 들어 Event and Destination(이벤트 및 목적지) 워크플로를 사용하는 경우 첫 번째 드릴다운 페이지에서 선택하는 각 행은 복합 제약 조건을 생성합니다. 목적지 IP 주소가 10.10.10.100인 이벤트 1:100을 선택하고 목적지 IP 주소가 192.168.10.100인 이벤트 1:200도 선택하는 경우, 복합 제약 조건은 1:100을 이벤트 유형으로, 192.168.10.100을 목적지 IP 주소로 포함하는 이벤트 또는 1:200을 이벤트 유형으로, 10.10.10.100을 목적지 IP 주소로 포함하는 이벤트도 선택되지 않도록 합니다.
현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운	**View All(**모두 보기**)**를 클릭합니다.

침입 이벤트 테이블 보기 제약 조건

다음 표에서는 테이블 보기를 사용하는 방법에 대해 설명합니다.

표 ***328:*** 이벤트의 테이블 보기에서 이벤트 제한

목적	방법
단일 속성이 있는 이벤트로 보기를 제한	속성을 클릭합니다. 예를 들어 목적지 포트가 80인 이벤트로 보기를 제한하려면 **DST Port/ICMP Code(DST** 포트**/ICMP** 코드**)** 열에서 **80/tcp**를 클릭합니다.
테이블에서 열 제거	숨기려는 열 머리글에서 닫기(✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다. 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, **Disabled Columns(**비활성화된 열**)** 아래에서 열 이름을 클릭합니다.
하나 이상의 이벤트에 연결된 패킷 보기	다음 중 하나: • 패킷을 보려는 이벤트 옆에 있는 아래쪽 화살표를 클릭합니다. • 패킷을 보려는 하나 이상의 이벤트를 선택하고 페이지 아래쪽에서 **View(**보기**)**를 클릭합니다. • 페이지 아래쪽에서, 현재 제약 조건과 일치하는 모든 이벤트에 대한 패킷을 보려면 **View All(**모두 보기**)**을 클릭합니다.

침입 이벤트 패킷 보기 사용

패킷 보기는 침입 이벤트를 생성한 규칙을 트리거한 패킷에 대한 정보를 제공합니다.

팁 이벤트를 탐지한 디바이스에 대해 **Transfer Packet(**패킷 전송**)** 옵션이 비활성화된 경우 Firepower Management Center의 패킷 보기에는 패킷 정보가 포함되지 않습니다.

패킷 보기는 패킷이 트리거한 침입 이벤트에 대한 정보를 제공함으로써 특정 패킷이 캡처된 이유를 나타냅니다. 그러한 정보에는 이벤트의 타임스탬프, 메시지, 분류, 우선순위가 포함되며, 이벤트가 표준 텍스트 규칙에 의해 생성된 경우 이벤트를 생성한 규칙도 포함됩니다. 패킷 보기는 또한 크기를 비롯한 패킷에 대한 일반 정보도 제공합니다.

패킷 보기에는 데이터 링크, 네트워크, 전송 등 패킷의 각 레이어에 대해 설명하는 섹션은 물론, 패킷을 구성하는 바이트에 대해 설명하는 섹션도 있습니다. 시스템이 패킷을 해독하면 해독된 바이트를 볼 수 있습니다. 자세한 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 침입 이벤트의 테이블 보기에서 침입 이벤트 테이블 보기 제약 조건, 2934 페이지에 설명된 대로 볼 패킷을 선택합니다.

단계 **2** 필요에 따라 하나 이상의 이벤트를 선택한 경우, 페이지 하단의 페이지 번호를 사용하여 패킷 보기에서 페이지를 전환할 수 있습니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- 조정 - 패킷 보기에서 날짜 및 시간 범위를 수정하려면 타임 윈도우 변경, 2815 페이지를 참조하십시오.
- 클립보드 - 나중에 인시던트에 전송할 수 있도록 이벤트를 클립보드에 이벤트를 추가하려면 **Copy(**복사**)**를 클릭해 패킷을 보고 잇는 이벤트를 복사하거나 **Copy All(**모두 복사**)**을 클릭하여 패킷을 이전에 선택한 모든 이벤트를 복사합니다.
- 구성 - 이벤트를 트리거한 침입 규칙을 구성하려면 Actions(작업) 옆의 화살표를 클릭하고 패킷 보기 내 침입 규칙 설정, 2940 페이지에 설명된 대로 계속합니다.
- 삭제 - 데이터베이스에서 이벤트를 삭제하려면 **Delete(**삭제**)**를 클릭하여 패킷을 보고 있는 이벤트를 삭제하거나 **Delete All(**모두 삭제**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 삭제합니다.
- 다운로드 - 이벤트를 트리거한 패킷의 로컬 사본(libpcap 형식의 패킷 캡처 파일)을 다운로드하려면 **Download Packet(**패킷 다운로드**)**을 클릭하여 보고 있는 이벤트의 캡처된 패킷 사본을 저장하거나 **Download All Packets(**모든 패킷 다운로드**)**를 클릭하여 패킷을 이전에 선택한 모든 이벤트의 캡처된 패킷 사본을 저장합니다. 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다.

  참고 단일 포트스캔 이벤트는 여러 패킷을 기반으로 하기 때문에 포트스캔 패킷을 다운로드할 수 없습니다. 그러나 포트스캔 보기는 사용할 만한 모든 패킷 정보를 제공합니다. 다운로드하려면 사용 가능한 디스크 공간이 15% 이상 남아 있어야 합니다.

- 검토 표시 - 이벤트를 검토된 것으로 표시하여 이벤트 보기에서는 제외하되 이벤트 데이터베이스에서는 제외하지 않으려면 **Review(**검토**)**를 클릭하여 패킷을 보고 있는 이벤트를 표시하거나 **Review All(**모두 검토**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 표시합니다. 자세한 내용은 검토된 침입 이벤트 표시, 2926 페이지를 참고하십시오.
- 추가 정보 보기 - 페이지 섹션을 확장하거나 축소하려면 섹션 옆에 있는 화살표를 클릭합니다. 자세한 내용은 이벤트 정보 필드, 2937 페이지, 프레임 정보 필드, 2943 페이지, 데이터 링크 레이어 정보 필드, 2944 페이지을 참조하십시오.
- 네트워크 레이어 정보 보기 - 네트워크 레이어 정보 보기, 2945 페이지를 참조하십시오.

- 패킷 바이트 정보 보기 - 패킷 바이트 정보 보기, 2950 페이지를 참조하십시오.
- 전송 레이어 정보 보기 - 다음 참조 Viewing Transport Layer Information, 2947 페이지

관련 항목

포트스캔 탐지, 2351 페이지
침입 이벤트 클립보드, 2951 페이지

이벤트 정보 필드

패킷 보기에서는 Event Information(이벤트 정보) 섹션에서 패킷에 대한 정보를 볼 수 있습니다.

Event(이벤트)

이벤트 메시지입니다. 규칙 기반 이벤트의 경우에는 규칙 메시지에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

이벤트의 ID는 (GID:SID:Rev) 형식으로 메시지에 추가됩니다. GID는 이벤트를 생성한 규칙 엔진, 디코더 또는 전처리기의 생성자 ID입니다. SID는 규칙, 디코더 메시지 또는 전처리기 메시지의 식별자입니다. Rev는 규칙의 개정 번호입니다.

타임스탬프

패킷이 캡처된 시간(UTC 시간대)입니다.

분류

이벤트 분류입니다. 규칙 기반 이벤트의 경우 규칙 분류에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

Priority(우선순위)

이벤트 우선순위입니다. 규칙 기반 이벤트의 경우 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

인그레스 보안 영역

이벤트를 트리거한 패킷의 인그레스 보안 영역입니다. 수동 배포에서는 이 보안 영역 필드만 입력됩니다.

이그레스 보안 영역

이벤트를 트리거한 패킷의 이그레스 보안 영역입니다. 패시브 구축에서는 이 필드가 채워지지 않습니다.

도메인

매니지드 디바이스가 속한 도메인입니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

디바이스

액세스 제어 정책이 구축된 매니지드 디바이스입니다.

스태킹된 구성의 기본 및 보조 디바이스는 마치 별도의 디바이스인 것처럼 침입 이벤트를 보고합니다.

보안 상황

트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터입니다. 시스템은 다중 상황 모드의 ASA FirePOWER에 대해서만 이 필드를 채웁니다.

인그레스 인터페이스

이벤트를 트리거한 패킷의 인그레스 인터페이스입니다. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다.

이그레스 인터페이스

인라인 집합의 경우 이벤트를 트리거한 패킷의 이그레스 인터페이스입니다.

Source/Destination IP

이벤트(소스)를 트리거한 패킷이 시작된 호스트 IP 주소 또는 도메인 이름 또는 이벤트를 트리거한 트래픽의 대상(목적지) 호스트입니다.

소스 포트**/ICMP** 유형

이벤트를 트리거한 패킷의 소스 포트입니다. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 유형을 표시합니다.

대상 포트**/ICMP** 코드

트래픽을 수신하는 호스트의 포트 번호입니다. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 코드를 표시합니다.

Email Headers(이메일 헤더**)**

이메일 헤더에서 추출된 데이터입니다. 이메일 헤더는 침입 이벤트의 테이블 보기에 나타나지 않지만 이메일 헤더를 검색 기준으로 사용할 수 있습니다.

이메일 헤더를 SMTP 트래픽의 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers(**헤더 로깅**)** 옵션을 활성화해야 합니다. 규칙 기반 이벤트의 경우 이메일 데이터가 추출될 때 이 행이 나타납니다.

HTTP Hostname(HTTP 호스트네임**)**

HTTP 요청 Host 헤더에서 추출된 호스트 이름(있는 경우). 이 행은 최대 256바이트까지 전체 호스트 이름을 표시합니다. 단일 행보다 길 경우 전체 호스트 이름을 확장할 수 있습니다.

호스트 이름을 표시하려면 HTTP Inspect 전처리기 **Log Hostname(**호스트 이름 로깅**)** 옵션을 활성화해야 합니다.

HTTP 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 이 행은 최대 2048바이트까지 전체 URI를 표시합니다. 단일 행보다 길 경우 전체 URI를 확장할 수 있습니다.

URI를 표시하려면 HTTP Inspect 전처리기 **Log URI(URI** 로깅**)** 옵션을 활성화해야 합니다.

HTTP 요청 패킷에 항상 URI가 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports(**양쪽 포트에서 스트림 리어셈블리 수행**)** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다.

침입 정책

침입 이벤트를 생성한 침입, 전처리기 또는 디코더 규칙이 활성화된 침입 정책(있는 경우). 액세스 제어 정책의 기본 작업으로 침입 정책을 선택하거나 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다.

액세스 제어 정책

이벤트를 생성한 침입, 전처리기 또는 디코더 규칙이 활성화된 침입 정책을 포함하는 액세스 제어 정책.

액세스 제어 규칙

이벤트를 생성한 침입 규칙에 연결된 액세스 제어 규칙입니다. Default Action(기본 작업)은 규칙이 활성화된 침입 정책이 액세스 제어 규칙과 연결되지 않은 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다.

규칙

표준 텍스트 규칙 이벤트의 경우, 이벤트를 생성한 규칙입니다.

이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

규칙 데이터에는 네트워크에 대한 민감한 정보가 포함될 수 있으므로 관리자는 사용자 역할 편집기의 View Local Rules(로컬 규칙 보기) 권한을 사용하여 패킷 보기에서 규칙 정보를 보는 사용자의 기능을 전환할 수 있습니다.

작업

표준 텍스트 및 맞춤형 규칙 이벤트의 경우, 이벤트를 트리거한 규칙에 대해 다음 작업을 수행하려면 **Actions(**작업**)**를 확장합니다.

- 규칙 수정
- 규칙의 개정 설명서를 봅니다. 표준 텍스트 규칙에 한해 Actions(작업)에서 **View Documentation(**설명서 보기**)**을 클릭한 후 설명서 팝업창에 있는 **Rule Documentation(**규칙 설명서**)**을 클릭하면 더 구체적인 규칙 세부 정보를 볼 수 있습니다.
- 규칙에 코멘트 추가
- 규칙의 상태 변경
- 규칙에 대한 임계값 설정
- 규칙 억제

이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

패킷 보기 내 침입 규칙 설정

침입 이벤트 패킷 보기 내에서 이벤트를 트리거한 규칙에 여러 작업을 수행할 수 있습니다. 이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 코멘트 - 표준 텍스트 규칙 이벤트의 경우, **Rule Comment(**규칙 코멘트**)**를 클릭하여 이벤트를 생성한 규칙에 텍스트 코멘트를 추가합니다. 그러면 식별된 정책 위반 또는 공격 및 규칙에 대한 자세한 컨텍스트 및 정보를 제공할 수 있습니다. 침입 규칙 편집기에서도 규칙 코멘트를 추가하고 볼 수 있습니다.
- 비활성화 - **Disable this rule...(**이 규칙 비활성화**...)**를 클릭하여 규칙을 비활성화합니다.

  이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우, 필요 시 규칙을 비활성화할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 규칙을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다.

  참고 패킷 보기에서 공유 개체 규칙을 비활성화할 수 없으며, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

- 패킷 삭제 - 규칙을 트리거하는 패킷을 삭제하도록 규칙을 설정하려면 **Set this rule to drop the triggering packet...(**트리거링하는 패킷을 삭제하도록 이 규칙 설정**...)**을 클릭합니다.

  매니지드 디바이스가 네트워크에서 인라인으로 구축된 경우, 이벤트를 트리거한 규칙이 로컬로 수정할 수 있는 모든 정책에서 규칙을 트리거하는 패킷을 삭제하도록 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다. 또한 이 옵션은 **Drop when Inline(**인라인 시 삭제**)**이 현재 정책에서 활성화된 경우에만 나타납니다.

- 편집 - 표준 텍스트 규칙 이벤트의 경우, 이벤트를 생성한 규칙을 수정하려면 **Edit(**수정**)**를 클릭합니다. 이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

  참고 (맞춤형 표준 텍스트 규칙과 달리) 시스템 제공 규칙을 수정하는 경우, 실제로는 새 로컬 규칙을 생성하는 것입니다. 이벤트를 생성하도록 로컬 규칙을 설정하고, 현재 침입 정책에서 원래 규칙을 비활성화해야 합니다. 그러나 기본 정책의 로컬 규칙은 활성화할 수 없습니다.

- 이벤트 생성 - 이벤트를 생성하도록 규칙을 설정하려면 **Set this rule to generate events...(**이벤트를 생성하도록 이 규칙 설정**...)**를 클릭합니다.

  이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우, 로컬에서 수정할 수 있는 모든 정책에서 이 이벤트를 생성하도록 규칙을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다.

  참고 패킷 보기에서 공유 개체 규칙을 비활성화할 수 없으며, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

- 억제 옵션 설정 - **Set Suppression Options(**억제 옵션 설정**)**를 확장하고 패킷 보기 내 삭제 옵션 설정, 2943 페이지에 설명된 대로 계속합니다.

  이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙을 억제할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 억제할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

- 임계값 옵션 설정 - **Set Thresholding Options(**임계값 옵션 설정**)**를 확장하고 패킷 보기 내 임계값 옵션 설정, 2942 페이지의 설명에 따라 계속합니다.

  이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙에 대해 임계값을 생성할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에 대해서만 임계값을 생성할 수 있습니다.

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 침입 정책은 수정할 수 없습니다.

- 설명서 보기 - 이벤트를 생성한 규칙에 대해 자세히 알아보려면 **View Documentation(**설명서 보기**)**을 클릭합니다.원하는 경우, 더 구체적인 규칙 세부 사항을 보려면 **Rule Documentation(**규칙 설명서**)**을 클릭합니다.

패킷 보기 내 임계값 옵션 설정

침입 이벤트의 패킷 보기에서 임계값 옵션을 설정하여 시간이 지남에 따라 규칙당 생성되는 이벤트의 수를 제어할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 임계값 옵션을 설정하거나 로컬로 수정할 수 있는 경우, 현재 정책(즉, 이벤트 생성을 트리거한 정책)에서만 임계값 옵션을 설정할 수 있습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** **Set Thresholding Options(**임계값 설정 옵션 설정**)**를 확장하고 가능한 다음 두 가지 옵션 중 하나를 선택합니다.

- 현재 정책에서
- 로컬에서 생성된 모든 정책에서

참고 현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다.

단계 **3** 설정하려는 임계값 유형을 선택합니다.

- **Limit(**제한**)**를 클릭하여 기간당 지정된 이벤트 인스턴스 수로 알림을 제한합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold(**임계값**)**를 클릭합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both(**모두**)**를 클릭합니다.

단계 **4** 이벤트 인스턴스를 소스 IP 주소로 추적할지 대상 IP 주소로 추적할지 나타내려면 해당 임계값을 클릭합니다.

단계 **5** 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(**카운트**)** 필드에 입력합니다.

단계 **6** 이벤트 인스턴스를 추적할 기간을 지정하는 1~86400의 숫자를 **Seconds(**초**)** 필드에 입력합니다.

단계 **7** 기존 침입 정책에서 이 규칙에 대한 현재 임계값을 재정의하려면 **Override any existing settings for this rule(**이 규칙의 모든 기본 설정 재정의**)** 확인란을 선택합니다.

단계 **8** **Save Thresholding(**임계값 설정 저장**)**을 클릭합니다.

패킷 보기 내 삭제 옵션 설정

억제 옵션을 사용하여 침입 이벤트를 완전히 억제하거나 소스 또는 목적지 IP 주소를 기반으로 억제할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 억제 옵션을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 억제 옵션을 설정할 수 있습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** **Set Suppression Options(**억제 옵션 설정**)**를 확장하고 가능한 다음 두 가지 옵션 중 하나를 선택합니다.

- 현재 정책에서
- 로컬에서 생성된 모든 정책에서

참고 현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

단계 **3** 다음 **Track By(**추적 기준**)** 옵션 중 하나를 선택합니다.

- 지정된 소스 IP 주소에서 시작되는 패킷에 의해 생성된 이벤트를 억제하려면 **Source(**소스**)**를 클릭합니다.
- 지정된 대상 IP 주소로 가는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination(**대상**)**을 클릭합니다.
- 이 이벤트를 트리거한 규칙의 이벤트를 완전히 억제하려면 **Rule(**규칙**)**을 클릭합니다.

단계 **4** 소스 또는 대상 IP 주소로 지정하려는 IP 주소 또는 CIDR 블록/접두사 길이를 **IP address or CIDR block(IP** 주소 또는 **CIDR** 블록**)** 필드에 입력합니다.

단계 **5** **Save Suppression(**억제 저장**)**을 클릭합니다.

관련 항목

Firepower System IP 주소 규칙, 19 페이지

프레임 정보 필드

패킷 보기에서 캡처된 프레임에 대한 정보를 볼 **Frame(**프레임**)** 옆에 있는 화살표를 클릭합니다. 패킷 보기에 단일 프레임 또는 다중 프레임이 표시될 수 있습니다. 각 프레임은 개별 네트워크 패킷에 대한 정보를 제공합니다. 예를 들면 태그가 지정된 패킷에서 또는 리어셈블된 TCP 스트림의 패킷에서 여러 프레임을 보게 될 수 있습니다.

Frame n

캡처된 프레임. 여기서 *n*은 단일 프레임 패킷의 경우 1이고 다중 프레임 패킷의 경우 증분 프레임 수입니다. 프레임에서 캡처된 바이트의 수가 프레임 수에 추가됩니다.

Arrival Time

프레임이 캡처된 날짜와 시간.

Time delta from previous captured frame

다중 프레임 패킷의 경우 이전 프레임이 캡처된 이후 경과한 시간.

Time delta from previous displayed frame

다중 프레임 패킷의 경우 이전 프레임이 표시된 이후 경과한 시간.

Time since reference or first frame

다중 프레임 패킷의 경우 첫 번째 프레임이 캡처된 이후 경과한 시간.

Frame Number

증분 프레임 수.

Frame Length

바이트 단위의 프레임 길이.

Capture Length

바이트 단위의 캡처된 프레임 길이.

Frame is marked

프레임이 표시되었는지 여부(true 또는 false).

Protocols in frame

프레임에 포함된 프로토콜.

관련 항목

tag 키워드, 2169 페이지
TCP 스트림 리어셈블리, 2335 페이지

데이터 링크 레이어 정보 필드

패킷 보기에서 데이터 링크 레이어 프로토콜(예: **Ethernet II**) 옆에 있는 화살표를 클릭하여 소스 및 대상 호스트의 48비트 MAC(media access control) 주소가 포함된 패킷에 대한 데이터 링크 레이어 정보를 봅니다. 하드웨어 프로토콜에 따라 패킷에 대한 기타 정보도 표시될 수 있습니다.

참고 이 예에서는 이더넷 링크 레이어 정보에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

패킷 보기는 데이터 링크 레이어에 사용된 프로토콜을 반영합니다. 다음 목록에서는 패킷 보기에 표시될 수 있는 Ethernet II 또는 IEEE 802.3 Ethernet 패킷 정보에 대해 설명합니다.

대상

대상 호스트의 MAC 주소.

참고 이더넷은 멀티캐스트 및 브로드캐스트 주소를 대상 주소로 사용할 수도 있습니다.

소스

소스 호스트의 MAC 주소.

유형

Ethernet II 패킷의 경우 이더넷 프레임으로 캡슐화된 패킷의 유형(예: IPv6 또는 ARP 데이터그램). 이 항목은 Ethernet II 패킷에 대해서만 나타납니다.

길이

IEEE 802.3 Ethernet 패킷의 경우 체크섬을 제외한 패킷의 전체 길이(바이트 단위). 이 항목은 IEEE 802.3 Ethernet 패킷에 대해서만 나타납니다.

네트워크 레이어 정보 보기

프로시저

패킷과 관련된 네트워크 레이어 정보에 대해 자세히 알아보려면 패킷 보기에서 네트워크 레이어 프로토콜(예: **Internet Protocol**) 옆에 있는 화살표를 클릭합니다.

참고 이 예에서는 IP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

IPv4 Network Layer Information(IPv4 네트워크 레이어 정보) 필드

다음 목록에서는 IPv4 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

버전

Internet Protocol version number(Internet Protocol 버전 번호).

Header Length(헤더 길이)

헤더의 바이트 수(IP 옵션 포함). 옵션이 없는 IP 헤더의 길이는 20바이트입니다.

Differentiated Services(차별화된 서비스) 필드

전송 호스트가 ECN(Explicit Congestion Notification)을 지원하는 방법을 나타내는 차별화된 서비스에 대한 값.

- `0x0` - ECT(ECN-Capable Transport)를 지원하지 않음
- `0x1` 및 `0x2` - ECT를 지원함
- `0x3` - CE(Congestion Experienced)

Total Length(총 길이)

IP 패킷에서 IP 헤더를 뺀 길이(바이트 단위).

식별

소스 호스트가 전송한 IP 데이터그램을 고유하게 식별하는 값. 이 값은 동일한 데이터그램의 프래그먼트를 추적하는 데 사용됩니다.

플래그

IP 프래그먼트화를 제어하는 값.

Last Fragment 플래그의 값은 데이터그램과 관련된 프래그먼트가 더 있는지 여부를 나타냅니다.

- `0` - 데이터그램에 연결된 프래그먼트가 더 이상 없음
- `1` - 데이터그램에 연결된 프래그먼트가 더 있음

Don't Fragment 플래그의 값은 데이터그램을 프래그먼트화할 수 있는지 여부를 나타냅니다.

- `0` - 데이터그램이 프래그먼트화될 수 있음
- `1` - 데이터그램이 프래그먼트화되어서는 안 됨

Fragment Offset(프래그먼트 오프셋)

데이터그램 시작에서부터 프래그먼트 오프셋의 값.

Time to Live(ttl)

데이터그램이 만료되기 전 데이터그램이 라우터 간에 만들 수 있는 나머지 홉(hop)의 수.

프로토콜

IP 데이터그램에서 캡슐화되는 전송 프로토콜(예: ICMP, IGMP, TCP 또는 UDP).

Header Checksum(헤더 체크섬)

IP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 침입 회피 시도에 사용 중일 수 있습니다.

소스/대상

소스(또는 대상) 호스트의 IP 주소나 도메인 이름.

도메인 이름을 표시하려면 IP 주소 확인을 활성화해야 합니다.

주소 또는 도메인 이름을 클릭하여 상황에 맞는 메뉴를 표시한 다음 호스트에서 whois 검색을 수행하려면 **Whois**를, 호스트 정보를 보려면 **View Host Profile(**호스트 프로파일 보기**)**을, 전역 차단 목록 또는 차단 안 함 목록에 주소를 추가하려면 옵션을 선택합니다.

IPv6 네트워크 레이어 정보 필드

다음 목록에서는 IPv6 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

Traffic Class(트래픽 클래스**)**

IPv4에 대해 제공되는 차별화된 서비스 기능과 유사한 IPv6 패킷 클래스 또는 우선순위를 식별하기 위한 IPv6 헤더의 실험적인 8비트 필드. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Flow Label

기본이 아닌 서비스 품질 또는 실시간 서비스 등의 특수 플로우를 식별하는 선택적인 20비트 IPv6 16진수 값 1~FFFFF. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Payload Length(페이로드 길이**)**

IPv6 페이로드에서 옥텟 수를 식별하는 16비트 필드로, IPv6 헤더 뒤에 나오는 모든 패킷(확장 헤더 포함)으로 구성됨.

Next Header(다음 헤더**)**

IPv6 헤더 바로 뒤에 나오는 헤더 유형을 식별하는 8비트 필드로, IPv4 Protocol 필드와 같은 값 사용.

Hop Limit(홉 제한**)**

패킷을 전달하는 각 노드가 1씩 감소하는 8비트 10진수 정수. 감소한 값이 0에 도달하면 패킷이 취소됩니다.

소스

소스 호스트의 128비트 IPv6 주소.

대상

대상 호스트의 128비트 IPv6 주소.

Viewing Transport Layer Information

프로시저

단계 **1** 패킷 보기에서 전송 레이어 프로토콜(예: **TCP**, **UDP** 또는 **ICMP**) 옆의 화살표를 클릭합니다.

단계 **2** 원하는 경우, 패킷 보기의 Packet Information(패킷 정보) 섹션에서 바로 위에 있는 프로토콜에 대한 페이로드의 처음 24바이트를 보려면 **Data**(있는 경우)를 클릭하십시오.

단계 **3** TCP Packet View(TCP 패킷 보기) 필드, 2948 페이지, UDP 패킷 보기 필드, 2949 페이지 또는 ICMP 패킷 보기 필드, 2949 페이지에 설명된 대로 TCP, UDP, ICMP 프로토콜 전송 계층의 콘텐츠를 확인합니다.

참고 이 예에서는 TCP, UDP 및 ICMP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

TCP Packet View(TCP 패킷 보기) 필드

이 절에서는 TCP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

소스 포트

시작 애플리케이션 프로토콜을 식별하는 번호.

대상 포트

수신 애플리케이션 프로토콜을 식별하는 번호.

sequence number(시퀀스 번호)

현재 TCP 세그먼트의 첫 번째 바이트에 대한 값으로, TCP 스트림에서 초기 시퀀스 번호로 키가 지정됨.

Next sequence number(다음 시퀀스 번호)

응답 패킷에서, 전송할 다음 패킷의 시퀀스 번호.

Acknowledgement number(승인 번호)

전에 허용된 데이터의 시퀀스 번호로 키가 지정되는 TCP 승인.

Header Length(헤더 길이)

헤더의 바이트 수.

플래그

TCP 세그먼트의 전송 상태를 나타내는 6개 비트.

- U - Urgent Pointer가 유효함
- A - 승인 번호가 유효함
- P - 수신자가 데이터를 푸시해야 함
- R - 연결 재설정
- S - 새 연결을 시작하도록 시퀀스 번호 동기화
- F — 보낸 사람이 데이터 전송을 완료 했습니다.

Window size(창 크기**)**

수신 호스트가 허용하는, 승인되지 않은 데이터의 양(바이트 단위)

체크섬

TCP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 회피 시도에 사용 중일 수 있습니다.

Urgent Pointer(긴급 포인터**)**

긴급 데이터가 종료되는 TCP 세그먼트의 위치(있는 경우). `U` 플래그와 함께 사용됨.

옵션

TCP 옵션의 값(있는 경우)

UDP 패킷 보기 필드

이 절에서는 UDP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

소스 포트

시작 애플리케이션 프로토콜을 식별하는 번호.

대상 포트

수신 애플리케이션 프로토콜을 식별하는 번호.

길이

UDP 헤더 및 데이터를 결합한 길이.

체크섬

UDP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

ICMP 패킷 보기 필드

이 절에서는 ICMP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

유형

ICMP 메시지의 유형:

- 0 - 에코 응답
- 3 - 목적지 도달 불가
- 4 - 소스 억제
- 5 - 리디렉션

- 8 - 에코 요청
- 9 - 라우터 알림
- 10 - 라우터 요청
- 11 - 시간 초과
- 12 - 파라미터 문제
- 13 - 타임스탬프 요청
- 14 - 타임스탬프 응답
- 15 - 정보 요청(사용되지 않음)
- 16 - 정보 응답(사용되지 않음)
- 17 - 주소 마스크 요청
- 18 - 주소 마스크 응답

코드

ICMP 메시지 유형에 대해 함께 제공 되는 코드입니다. ICMP 메시지 유형 3, 5, 11, 12에는 RFC 792에 설명된 대로 해당 코드가 있습니다.

체크섬

ICMP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

패킷 바이트 정보 보기

프로시저

패킷을 구성하는 바이트의 16진수 및 ASCII 버전을 보려면 패킷 보기에서 **Packet Bytes(**패킷 바이트**)** 옆에 있는 화살표를 클릭합니다. 시스템이 트래픽을 해독하면 해독된 패킷 바이트를 볼 수 있습니다.

내부 소스 침입 이벤트

내부 소스에서 들어오는 침입 이벤트는 네트워크의 호스트가 손상되었음을 나타냅니다. 소스 IP 주소가 네트워크에 있는 경우 이 호스트를 조사해야 한다는 신호입니다.

침입 이벤트 클립보드

클립보드는 침입 이벤트 보기에서 침입 이벤트를 복사할 수 있는 보관 영역입니다.

클립보드의 내용은 이벤트가 생성된 날짜 및 시간별로 정렬됩니다. 침입 이벤트를 클립보드에 추가한 후, 클립보드에서 삭제할 수도 있고 클립보드의 내용에 대해 보고서를 생성할 수도 있습니다.

보안 정책 위반과 관련이 있는 것으로 의심되는 이벤트의 모음인 인시던트에 클립보드의 침입 이벤트를 추가할 수도 있습니다.

관련 항목

침입 이벤트 워크플로 사용, 2932 페이지
침입 이벤트 패킷 보기 사용, 2935 페이지
인시던트 생성, 2744 페이지

클립보드 보고서 생성

다른 이벤트 보기에서 하는 것처럼 클립보드의 이벤트에 대한 보고서를 생성할 수 있습니다.

시작하기 전에

- 침입 이벤트 워크플로 사용, 2932 페이지 또는 침입 이벤트 패킷 보기 사용, 2935 페이지에 설명된 대로 하나 이상의 이벤트를 클립보드에 추가합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Clipboard(**클립보드**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 클립보드의 페이지에 있는 특정 이벤트를 포함하려면 해당 페이지로 이동하여 이벤트 옆의 확인란을 선택하고 **Generate Report(**보고서 생성**)**를 클릭합니다.
- 클립보드의 모든 이벤트를 포함하려면 **Generate Report All(**모든 보고서 생성**)**을 클릭합니다.

단계 **3** 보고서의 모양을 지정한 후 **Generate(**생성**)**를 클릭합니다.

단계 **4** 하나 이상의 출력 형식을 선택하고 필요한 경우, 그 밖의 설정을 수정합니다.

단계 **5** **Generate(**생성**)**를 클릭한 다음 **Yes(**예**)**를 클릭합니다.

단계 **6** 다음 옵션을 이용할 수 있습니다.

- 보고서 링크를 클릭해 보고서를 새 창에 표시합니다.
- **OK(**확인**)**를 클릭해 보고서 디자인을 수정할 수 있는 Report Templates(보고서 템플릿) 페이지로 돌아갑니다.

관련 항목

보고서 템플릿, 2653 페이지

클립보드에서 이벤트 삭제

클립보드의 이벤트 중 인시던트에 추가하지 않으려는 이벤트가 있으면 해당 이벤트를 삭제할 수 있습니다.

참고 이벤트를 클립보드에서 삭제해도 이벤트 데이터베이스에서 삭제되지는 않습니다. 그러나 이벤트 데이터베이스에서 이벤트를 삭제하면 클립보드에서도 해당 이벤트가 삭제됩니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Clipboard(**클립보드**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 특정 이벤트 삭제 - 클립보드의 페이지에서 특정 침입 이벤트를 삭제하려면 해당 페이지로 이동하여 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.
- 모든 이벤트 삭제 - 클립보드에서 모든 침입 이벤트를 삭제하려면 **Delete All(**모두 삭제**)**을 클릭합니다. Event Preferences(이벤트 환경설정)에서 **Confirm 'All' Actions('**모든**'** 작업 확인**)** 옵션을 선택하면 모든 이벤트를 삭제할 것인지 확인하는 메시지가 표시됩니다.

침입 이벤트 통계 보기

Intrusion Event Statistics(침입 이벤트 통계) 페이지에서는 어플라이언스의 현재 상태 및 네트워크에 대해 생성된 침입 이벤트에 대한 빠른 요약을 제공합니다.

페이지에 표시되는 각 IP 주소, 포트, 프로토콜, 이벤트 메시지 등은 링크입니다. 연결된 이벤트 정보를 보려면 링크를 클릭하십시오. 예를 들어 상위 10개 대상 포트 중 하나가 `80 (http)/tcp`인 경우 해당 링크를 클릭하면 기본 침입 이벤트 워크플로의 첫 번째 페이지가 표시되고, 해당 포트를 대상으로 하는 이벤트가 나열됩니다. 현재 시간 범위의 이벤트(및 이벤트를 생성하는 매니지드 디바이스)만 나타납니다. 또한 검토한 것으로 표시한 침입 이벤트는 통계에 계속 나타납니다. 예를 들어 현재의 시간 범위가 과거 시간이지만 첫 번째 이벤트가 5시간 전에 생성된 경우, **First Event(**첫 번째 이벤트**)** 링크를 클릭하면 시간 범위를 변경하기 전에는 결과 이벤트 페이지에 이벤트가 표시되지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Statistics(**침입 이벤트 통계**)**을(를) 선택합니다.

단계 **2** 페이지 상단에 있는 두 개의 선택 상자에서 통계를 보려는 영역 및 디바이스를 선택합니다. 침입 이벤트를 수집하는 모든 디바이스에 대한 통계를 보려면 **All Security Zones(**모든 보안 영역**)** 및 **All Devices(**모든 디바이스**)**를 선택합니다.

단계 **3** **Get Statistics(**통계 가져오기**)**를 클릭합니다.

팁 맞춤형 시간 범위의 데이터를 보려면 페이지 오른쪽 위 영역의 링크를 클릭하고 타임 윈도우 변경, 2815 페이지의 지침을 따르십시오.

호스트 통계 자료

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Host Statistics(호스트 통계) 절에서는 어플라이언스 자체에 대한 정보를 제공합니다. Firepower Management Center에서 이 섹션은 매니지드 디바이스에 대한 정보도 제공합니다.

이 정보에는 다음 항목이 포함됩니다.

시간

어플라이언스의 현재 시간.

Uptime(실행 시간**)**

어플라이언스 자체를 다시 시작한 이후의 일 수, 시간, 분. Firepower Management Center에서 업타임은 각 매니지드 디바이스가 마지막으로 재부팅된 시간, 로그인한 사용자 수 및 로드 평균도 보여줍니다.

디스크 사용

사용 중인 디스크의 백분율

메모리 사용

사용 중인 시스템 메모리의 백분율

로드 평균

지난 1분, 5분 15분 동안 CPU 큐 프로세스의 평균 수.

이벤트 개요

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Event Overview(이벤트 개요) 섹션에서는 침입 이벤트 데이터베이스의 정보 개요를 제공합니다.

이러한 통계에는 다음이 포함됩니다.

이벤트

침입 이벤트 데이터베이스의 이벤트 수.

시간 범위 내 이벤트

현재 선택된 시간 범위는 물론 시간 범위에 속하는 데이터베이스의 이벤트 수와 비율도 표시합니다.

첫 번째 이벤트

이벤트 데이터베이스에 있는 첫 번째 이벤트의 이벤트 메시지.

마지막 이벤트

이벤트 데이터베이스에 있는 마지막 이벤트의 이벤트 메시지.

참고 Firepower Management Center에서 침입 이벤트 데이터를 보는 동안 매니지드 디바이스를 선택하면 해당 디바이스에 대 한 Event Overview(이벤트 개요) 섹션이 대신 표시됩니다.

이벤트 통계

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Event Statistics(이벤트 통계) 섹션에서는 침입 이벤트 데이터베이스의 정보에 대한 좀 더 구체적인 정보를 제공합니다.

이 정보에는 다음에 대한 세부사항이 포함됩니다.

- 상위 10개 이벤트 유형
- 상위 10개 소스 IP 주소
- 상위 10개 대상 IP 주소
- 상위 10개 대상 포트
- 이벤트 수가 가장 많은 프로토콜, 수신 및 송신 보안 영역, 디바이스

참고 다중 도메인 구축에서 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 따라서 리프 도메인은 네트워크 내에서는 고유하지만 다른 리프 도메인과 동일한 IP 주소를 포함할 수 있습니다. 상위 도메인에서 이벤트 통계를 볼 때 반복되는 IP 주소의 여러 인스턴스가 표시될 수 있습니다. 처음에는 이것이 중복된 항목으로 보일 수 있습니다. 하지만 각 IP 주소의 호스트 프로파일 정보로 드릴다운하는 경우, 시스템은 이들이 서로 다른 리프 도메인에 속한다고 표시합니다.

침입 이벤트 성능 그래프 보기

침입 이벤트 성능 페이지에서 특정 기간 동안 Firepower Management Center 또는 매니지드 디바이스에 대한 침입 이벤트의 성능 통계를 보여주는 그래프를 생성할 수 있습니다. 초당 침입 이벤트의 수, 초당 메가비트의 수, 패킷당 평균 바이트 수, Snort에서 검사하지 않은 패킷의 비율, TCP 표준화로 인해 차단된 패킷의 수를 보여주는 그래프를 생성할 수 있습니다. 이러한 그래프는 운영의 마지막 시간, 마지막 날, 마지막 주 또는 마지막 달에 대한 통계를 보여줄 수 있습니다.

참고 새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생할 때까지 데이터가 변경되지 않을 수 있습니다. 각 그래프는 선택한 기간(마지막 달, 주, 날 또는 시간) 동안 표시된 간격(일, 시간 또는 5분) 내 평균 값을 표시합니다. 평균이 1보다 작으면 소수 값이 표시됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Performance(**침입 이벤트 성능**)**을(를) 선택합니다.

단계 **2** 데이터를 보려는 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다.

단계 **3** 침입 이벤트 성능 통계 그래프 유형, 2955 페이지에 설명된 대로 **Select Graph(s)(**그래프 선택**)** 목록에서 생성할 그래프 유형을 선택합니다.

단계 **4** **Select Time Range(**시간 범위 선택**)** 목록에서 그래프에 사용할 시간 범위를 선택합니다.

단계 **5** **Graph(**그래프**)**를 클릭합니다.

단계 **6** 그래프를 저장하려면 마우스 오른쪽 버튼으로 그래프를 클릭하고 브라우저의 지시에 따라 이미지를 저장합니다.

침입 이벤트 성능 통계 그래프 유형

다음 표에는 사용 가능한 그래프 유형이 나열되어 있습니다. 네트워크 분석 정책 **Inline Mode(**인라인 모드**)** 설정의 영향을 받는 데이터로 채워지는 경우 그래프 유형이 다르게 표시됩니다. **Inline Mode(**인라인 모드**)**가 비활성화되어 있으면 웹 인터페이스에서 별표(`*`)로 표시된 그래프 유형(아래 열에서 (`yes`로 표시된 행)은 **Inline Mode(**인라인 모드**)**가 활성화되었다면 시스템에서 수정 또는 삭제했을 트래픽에 대한 데이터로 채워집니다.

표 ***329:*** 침입 이벤트 성능 그래프 유형

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
평균 바이트/패킷	해당 없음	각 패킷에 포함된 평균 바이트 수입니다.	아니요
TCP 트래픽/패킷에서 표준화된 ECN 플래그	**Explicit Congestion Notification(**명시적 폭주 통지**)**를 활성화하고 **Packet(**패킷**)** 선택	협상 여부와 상관없이 패킷당 기준으로 ECN 플래그가 지워진 패킷의 수입니다.	예
TCP 트래픽/세션에서 표준화된 ECN 플래그	**Explicit Congestion Notification(**명시적 폭주 통지**)**을 활성화하고 **Stream(**스트림**)** 선택	ECN 사용이 협상되지 않은 경우 스트림 단위로 ECN 플래그가 지워진 횟수입니다.	예
이벤트/초	해당 없음	디바이스에서 생성되는 초당 이벤트 수입니다.	아니요
ICMPv4 에코 표준화	**Normalize ICMPv4** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv4 패킷의 수	예
ICMPv6 에코 정규화	**Normalize ICMPv6** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv4 패킷의 수입니다.	예
IPv4 DF 플래그 표준화	**Normalize IPv4** 및 **Normalize Don't Fragment Bit** 활성화	IPv4 Flags 헤더 필드의 단일 비트 Don't Fragment 하위 필드가 지워진 IPv4 패킷의 수입니다.	예
IPv4 옵션 표준화	**Normalize IPv4** 활성화	옵션 옥텟이 1(No Operation)로 설정된 IPv4 패킷의 수입니다.	예
IPv4 예약 플래그 표준화	**Normalize IPv4** 및 **Normalize Reserved Bit** 활성화	IPv4 Flags 헤더의 단일 비트 Reserved 하위 필드가 지워진 IPv4 패킷의 수입니다.	예
IPv4 크기 조정 표준화	**Normalize IPv4** 활성화	IP 헤더에 지정된 데이터그램 길이로 잘린, 과도한 길이의 페이로드가 있는 IPv4 패킷의 수입니다.	예

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
IPv4 TOS 표준화	**Normalize IPv4** 및 **Normalize TOS Bit** 활성화	1바이트 Differentiated Services(DS) 필드(이전의 Type of Service(TOS) 필드)가 지워진 IPv4 패킷의 수입니다.	예
IPv4 TTL 표준화	**Normalize IPv4**, **Maximum TTL** 및 **Reset TTL** 활성화	IPv4 Time to Live 표준화의 수입니다.	예
IPv6 옵션 정규화	**Normalize IPv6** 활성화	Hop-by-Hop Options(홉 바이 홉 옵션) 또는 Destination Options(대상 옵션) 확장 헤더의 Option Type(옵션 유형) 필드가 00(건너뛰고 계속 처리)으로 설정된 IPv6 패킷의 수입니다.	예
IPv6 TTL 정규화	**Normalize IPv6**, **Minimum TTL** 및 **Reset TTL** 활성화	IPv6 Hop Limit(TTL) 표준화의 수입니다.	예
메가비트/초	해당 없음	디바이스를 통해 전달되는 트래픽의 초당 메가비트 수입니다.	아니요
MSS 표준화에 맞게 크기 조정된 패킷	**Trim Data to MSS(MSS**로 데이터 절감**)** 활성화	페이로드가 TCP Data 필드보다 길어서 Maximum Segment Size로 잘리는 패킷의 수입니다.	예
TCP 창 표준화에 맞게 크기 조정된 패킷	**Trim Data to Window** 활성화	TCP Data 필드가 수신 호스트의 TCP 창에 맞게 잘리는 패킷의 수입니다.	예
삭제된 패킷 비율	해당 없음	선택한 모든 디바이스에서 검사하지 않은 패킷의 평균 비율입니다. 예를 들어 디바이스를 2개 선택하고 평균이 50%이면, 한 디바이스는 삭제율이 90%이고 나머지는 삭제율이 10%라는 뜻일 수 있습니다. 또는 두 디바이스 모두 삭제율이 50%임을 나타낼 수도 있습니다. 그래프는 단일 디바이스를 선택할 경우의 총 삭제 %만 나타냅니다.	아니요

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
데이터 스트립된 RST 패킷 표준화	**Remove Data on RST(RST** 데이터 제거**)** 활성화	TCP 재설정(RST) 패킷에서 데이터가 삭제된 패킷의 수입니다.	예
데이터 스트립된 SYN 패킷 표준화	**Remove Data on SYN(SYN** 데이터 제거**)** 활성화	TCP 운영체제가 Mac OS가 아닐 때 SYN 패킷에서 데이터가 제거된 패킷의 수입니다.	예
TCP 헤더 패딩 표준화	**Normalize/Clear Option Padding Bytes(**옵션 패딩 바이트 표준화/지우기**)** 활성화	옵션 패딩 바이트가 0으로 설정되었을 때 TCP 패킷의 수입니다.	예
TCP 옵션 없음 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Time Stamp 옵션이 제거된 패킷의 수입니다.	예
TCP NS 플래그 표준화	**Explicit Congestion Notification(**명시적 폭주 통지**)**을 활성화하고 **Packet(**패킷**)** 선택	ECN Nonce Sum(NS) 옵션 표준화의 수입니다.	예
TCP 옵션 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	옵션 필드가 No Operation(TCP Option 1)으로 설정된 옵션(MSS, Window Scale, Time Stamp 및 명시적으로 허용된 옵션 제외)의 수입니다.	예
표준화에 의해 차단된 TCP 패킷	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 실패함)	TCP 세그먼트를 제대로 리어셈블할 수 없기 때문에 삭제된 패킷의 수입니다.	예
TCP 예약 플래그 표준화	**Normalize/Clear Reserved Bits(**예약 비트 표준화/지우기**)** 활성화	Reserved 비트가 지워진 TCP 패킷의 수입니다.	예
TCP 세그먼트 리어셈블리 표준화	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 성공함)	재전송된 데이터의 일관성을 보장하기 위해 TCP Data 필드가 표준화된 패킷의 수(제대로 리어셈블할 수 없는 세그먼트는 삭제됨)입니다.	예

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
TCP SYN 옵션 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	SYN 제어 비트가 설정되지 않아 Maximum Segment Size or Window Scale 옵션이 No Operation(TCP Option 1)으로 설정된 옵션의 수입니다.	예
TCP 타임스탬프 ECR 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Acknowledgment(수신 확인, ACK) 제어 비트가 설정되지 않아 Time Stamp Echo Reply(타임 스탬프 에코 응답, TSecr) 옵션 필드가 지워진 패킷의 수입니다.	예
TCP 긴급 포인터 표준화	**Normalize Urgent Pointer(**긴급 포인터 표준화**)** 활성화	2바이트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드가 페이로드 길이보다 긴 패킷 및 페이로드 길이로 설정된 패킷의 수입니다.	예
총 차단된 패킷	**Inline Mode** 또는 **Drop when Inline** 설정	규칙, 디코더 및 전처리기 삭제를 비롯한 삭제된 패킷의 총 수입니다.	아니요
총 삽입된 패킷	**Inline Mode** 설정	재전송되기 전에 크기가 조정된 패킷의 수입니다.	아니요
총 TCP 필터링된 패킷	TCP 스트림 전처리 설정	TCP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수입니다.	아니요
총 UDP 필터링된 패킷	UDP 스트림 전처리 설정	UDP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수입니다.	아니요
긴급 플래그 지워진 표준화	**Clear URG if Urgent Pointer is Not Set(**긴급 포인터가 설정되지 않은 경우 **URG** 지우기**)** 활성화	긴급 포인터가 설정되지 않아서 TCP 헤더 URG 제어 비트가 지워진 패킷의 수입니다.	예
긴급 포인터 및 긴급 플래그 지워진 표준화	**Clear Urgent Pointer/URG on Empty Payload(**빈 페이로드의 긴급 포인터**/URG** 지우기**)** 활성화	페이로드가 없어 TCP 헤더 Urgent Pointer(긴급 포인터) 필드 및 URG 제어 비트가 지워진 패킷의 수입니다.	예

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode**(인라인 모드)의 영향 적용 여부
긴급 포인터 지워진 표준화	**Clear Urgent Pointer if URG=0**(URG=0인 경우 긴급 포인터 지우기) 활성화	Urgent(URG) 제어 비트가 설정되지 않아 16비트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드가 지워진 패킷의 수입니다.	예

관련 항목

인라인 정상화 전처리기, 2317 페이지
인라인 구축의 전처리기 트래픽 수정, 2224 페이지
인라인 구축의 삭제 작업, 2002 페이지

침입 이벤트 그래프 보기

Firepower System은 시간에 따른 침입 이벤트 추세를 보여주는 그래프를 제공합니다. 하나 또는 모든 매니지드 디바이스에 대해 지난 1시간부터 지난 달까지의 시간 동안의 침입 이벤트 그래프를 생성할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview**(개요) > **Summary**(요약) > **Intrusion Event Graphs**(침입 이벤트 그래프)을(를) 선택합니다.

단계 **2** **Select Device**(디바이스 선택) 아래에서 **all**을 선택하여 모든 디바이스를 포함하거나 그래프에 포함할 특정 디바이스를 선택합니다.

단계 **3** **Select Graph(s)**(그래프 선택)에서 생성할 그래프 유형을 선택합니다.

- 상위 10개 대상 포트
- 상위 10개 소스 IP 주소
- 상위 10개 이벤트 메시지

단계 **4** **Select Time Range**(시간 범위 선택)에서 그래프의 시간 범위를 선택합니다.

- 마지막 시간
- 지난 1일
- 지난주
- 지난달

단계 **5** **Graph**(그래프)를 클릭합니다.

침입 이벤트 기록

기능	버전	세부 사항
시스템 로그의 연결 이벤트 통합 식별자	6.4.0.4	다음 시스템 로그 필드는 함께 연결 이벤트를 개별적으로 식별하며, 침입 이벤트의 경우에는 시스템 로그에 디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터로 표시됩니다.
이제 IntrusionPolicy 필드가 시스템 로그에 포함됩니다.	6.4	침입 이벤트 시스템 로그는 이제 이벤트를 트리거한 침입 정책을 표시합니다.
새 침입 이벤트 검색 필드: CVE ID	6.4	이제 MITRE의 일반 취약성 및 노출 식별 번호로 검색할 수 있습니다. 수정된 화면: **Analysis(**분석**) > Intrusions(**침입**) > Events(**이벤트**) > Edit Search(**검색 편집**)** 지원되는 플랫폼: 전체.

123 장

파일/악성코드 이벤트 및 네트워크 파일 경로 분석

다음 주제에서는 파일 및 악성코드 이벤트, 로컬 악성코드 분석, 동적 분석, 캡처된 파일, 네트워크 파일 경로 분석의 개요를 제공합니다.

- 파일/악성코드 이벤트 및 네트워크 파일 경로 분석 정보, 2963 페이지
- 파일 및 악성코드 이벤트, 2964 페이지
- 분석된 파일에 대한 세부 정보 보기, 2984 페이지
- 캡처된 파일 워크플로 사용, 2985 페이지
- 분석을 위해 수동으로 파일 제출, 2991 페이지
- 네트워크 파일 전파 흔적 분석, 2992 페이지
- 파일, 악성코드 이벤트 및 네트워크 파일 경로 분석 기록, 2999 페이지

파일/악성코드 이벤트 및 네트워크 파일 경로 분석 정보

파일 정책은 일치된 트래픽에 대한 파일 및 악성코드 이벤트를 자동으로 생성하고 캡처된 파일 정보를 로깅합니다. 파일 정책이 파일 또는 악성코드 이벤트를 생성하거나 파일을 캡처하면 시스템도 연결된 연결 종료를 Firepower Management Center 데이터베이스에 자동으로 로깅합니다. 이 데이터를 분석하여 모든 부정적 영향을 해결하고 향후 공격을 차단할 수 있습니다.

파일 분석 결과를 바탕으로 Analysis(분석) > Files(파일) 메뉴에서 사용할 수 있는 페이지의 테이블을 사용하여 캡처된 파일과 생성된 악성코드 및 파일 이벤트를 검토할 수 있습니다. 사용 가능한 경우, 파일의 구성, 속성, 위협 점수, 동적 분석 요약 보고서를 검사하여 악성코드 분석에 대한 추가 통찰을 얻을 수 있습니다.

보다 집중적인 분석을 위해 악성코드 파일의 네트워크 파일 경로 분석(파일이 호스트를 통과하여 네트워크에서 이동한 방법과 다양한 파일 속성을 보여주는 맵)을 사용하여 시간이 지남에 따른 호스트에서의 개별 위협의 확산을 추적할 수 있으며, 이를 통해 가장 유용한 보안 침해 통제 및 방지에 집중할 수 있습니다.

파일 규칙에서 로컬 악성코드 분석 또는 동적 분석을 구성하는 경우, 시스템은 규칙과 일치 하는 파일을 사전 분류하고 파일 구성 보고서를 생성합니다.

조직에서 *AMP for Endpoints*를 구축하여 해당 구축을 Firepower Management Center에 통합한 경우, 해당 제품이 식별한 보안 침해 지표(IOC)뿐 아니라 스캔, 악성코드 탐지, 격리 레코드를 가져올 수 있습니다. 이 데이터는 네트워크에서 악성코드를 더 완벽하게 파악할 수 있도록 Firepower가 수집한 이벤트 데이터와 함께 표시됩니다.

Context Explorer, 대시보드, 보고 기능도 탐지, 캡처, 차단된 파일과 악성코드를 더욱 깊이 이해하는 데 도움이 됩니다. 이벤트를 사용하여 상관관계 정책 위반을 트리거하거나 이메일, SNMP 또는 syslog를 통해 알림을 받을 수도 있습니다.

참고 악성코드를 탐지하고 파일 및 악성코드 이벤트를 생성하도록 시스템을 구성하려면 파일 정책 및 악성코드 보호, 1861 페이지를 참조하십시오.

파일 및 악성코드 이벤트

Firepower Management Center는 다양한 유형의 파일 및 악성코드 이벤트를 로깅할 수 있습니다. 개별 이벤트에 사용 가능한 정보는 정보 생성 방법과 이유에 따라 달라질 수 있습니다.

- 파일 이벤트는 Firepower system이 탐지한 악성코드를 포함한 파일을 나타냅니다(AMP for Networks .) 파일 이벤트는 AMP for Endpoints 관련 필드를 포함하지 않습니다.
- 악성코드 이벤트는 AMP for Networks 또는 AMP for Endpoints에 의해 탐지된 악성코드를 나타냅니다. 악성코드 이벤트에는 스캔과 격리 등 AMP for Endpoints 구축이 제공하는 위협 외의 레코드 데이터도 포함될 수 있습니다.
- 회귀적 악성코드 이벤트는 AMP for Networks 에 의해 탐지된, 속성(파일이 악성코드인지 여부)이 변경된 파일을 나타냅니다.

참고

- AMP for Networks 에 의해 악성코드로 식별된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. AMP for Endpoints에 의해 생성된 악성코드 이벤트에는 상응하는 파일 이벤트가 없습니다.
- 클라이언트와 서버에 지속적인 연결이 설정되어 있기 때문에 NetBIOS-ssn (SMB) 트래픽 검사에 의해 생성된 파일 이벤트가 즉시 연결 이벤트를 생성하지는 않습니다. 시스템은 클라이언트 또는 서버가 세션을 종료한 후 연결 이벤트를 생성합니다.
- Firepower System은 유니코드(UTF-8) 문자를 사용하는 파일 이름의 표시와 입력을 지원합니다. 다만 유니코드 파일 이름은 문자 번역된 형식으로 PDF 보고서에 표시됩니다. 또한 SMB 프로토콜은 파일 이름에 있는 인쇄할 수 없는 문자를 마침표로 대체합니다.

파일 및 악성코드 이벤트 유형

파일 이벤트

시스템은 매니지드 디바이스가 네트워크 트래픽에서 파일을 탐지하거나 차단할 때 생성되는 파일 이벤트를 현재 구축된 파일 정책의 규칙에 따라 로깅합니다.

시스템은 파일 이벤트를 생성할 때 호출하는 액세스 제어 규칙의 로깅 구성과 관계없이 연결된 연결의 종료도 Firepower Management Center 데이터베이스에 로깅합니다.

악성코드 이벤트

Firepower System(특히 AMP for Networks 기능)은 전체 액세스 제어 구성의 일부로 네트워크 트래픽에서 악성코드를 탐지할 때 악성코드 이벤트를 생성합니다. 악성코드 이벤트에는 결과 이벤트의 속성과 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터가 포함됩니다.

표 ***330:*** 악성코드 이벤트 생성 시나리오

시스템이 파일을 탐지하고 다음을 수행하는 경우	속성
AMP 클라우드(악성코드 클라우드 조회 수행)에서 파일의 속성을 성공적으로 쿼리	Malware(악성코드), Clean(정상) 또는 Unknown(알 수 없음)
AMP 클라우드를 쿼리하지만 연결을 설정할 수 없거나 연결을 사용할 수 없음	사용 불가능 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.
파일에 연결된 위협 점수가 파일을 탐지한 파일 정책에서 정의한 악성코드 임계값 위협 점수를 초과하거나 로컬 악성코드 분석이 악성코드를 식별	악성코드
맞춤형 탐지 목록에 있음(수동으로 악성코드로 표시됨)	맞춤형 탐지
정상 목록에 있음(수동으로 정상으로 표시됨)	정상

회귀적 악성코드 이벤트

네트워크 트래픽에서 탐지된 악성코드의 경우, 속성이 변경될 수 있습니다. 예를 들어 AMP 클라우드는 이전에는 정상으로 간주되었던 파일이 지금은 악성코드로 식별되는 경우 또는 그 반대의 경우(악성코드로 식별된 파일이 실제로 정상임)를 결정할 수 있습니다. 지난주에 쿼리한 파일의 속성이 변경되면 AMP 클라우드가 시스템에 알립니다. 그러면 두 가지가 발생합니다.

- Firepower Management Center는 새로운 회귀적 악성코드 이벤트를 생성합니다.

  이 새로운 회귀적 악성코드 이벤트는 지난주에 탐지된 SHA-256 해시 값이 동일한 모든 파일의 속성 변경을 나타냅니다. 따라서 이러한 이벤트에는 Firepower Management Center에 속성 변경을 알린 날짜와 시간, 새로운 속성, 파일의 SHA-256 해시 값 및 위협 이름 등 제한된 정보가 포함됩니다. IP 주소나 기타 컨텍스트 정보는 포함되지 않습니다.

- Firepower Management Center은 이전에 탐지된 파일의 파일 속성을 회귀적 이벤트에 연결된 SHA-256 해시 값으로 변경합니다.

  파일의 속성이 Malware(악성코드)로 변경되면 Firepower Management Center은 새 악성코드 이벤트를 데이터베이스에 기록합니다. 새 속성 외에도 이 새 악성코드 이벤트의 정보는 파일이 처음 탐지됐을 때 생성된 파일 이벤트의 정보와 동일합니다.

  파일의 속성이 Clean(정상)으로 변경되는 경우, Firepower Management Center은 악성코드 이벤트를 삭제하지 않습니다. 대신 해당 이벤트는 속성의 변경을 반영합니다. 즉, 정상 속성의 파일이 악성코드 테이블에 나타날 수 있지만 원래 악성코드로 파악된 경우에 한합니다. 악성코드로 식별된 적이 없는 파일은 파일 테이블에만 나타납니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트

조직에서 AMP for Endpoints를 사용하는 경우, 개별 사용자가 엔드포인트(컴퓨터 및 모바일 디바이스)에 경량 커넥터를 설치합니다. 커넥터는 파일 업로드, 다운로드, 실행, 열기, 복사, 이동 등을 수행할 때 파일을 검사할 수 있습니다. 이러한 커넥터는 AMP 클라우드와 통신하여 검사된 파일에 악성코드가 포함되었는지 확인합니다.

파일이 악성코드로 식별되면 AMP 클라우드는 위협 식별 정보를 Firepower Management Center에 전송합니다. 또한 AMP 클라우드는 검사, 격리, 차단된 실행, 클라우드 회수에 대한 데이터를 비롯한 다른 종류의 정보도 Firepower Management Center에 전송할 수 있습니다. Firepower Management Center는 이러한 정보를 악성코드 이벤트로 로깅합니다.

참고 AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 보고된 IP 주소는 네트워크 맵에 없을 수 있으며, 모니터링되는 네트워크에도 없을 수 있습니다. 구축, 규정 준수 수준, 기타 요인에 따라 AMP for Endpoints가 모니터링하는 조직 내 엔드포인트가 AMP for Networks 에서 모니터링하는 것과 같은 호스트가 아닐 수 있습니다.

AMP for Endpoints를 사용한 악성코드 이벤트 분석

조직에서 Cisco AMP for Endpoints를 구축한 경우:

- Firepower Management Center 이벤트 페이지에 AMP for Networks가 탐지한 이벤트와 함께 AMP for Endpoints가 탐지한 악성코드 이벤트를 표시하도록 시스템을 구성할 수 있습니다.
-

위의 기능을 구성하려면 Firepower와 AMP for Endpoints 통합, 1898 페이지를 참조하십시오.

AMP for Endpoints의 이벤트 데이터

조직에서 악성코드 방지를 위해 AMP for Endpoints를 구축한 경우, AMP for Endpoints의 파일 및 악성코드 데이터를 사용하여 FMC에서 작업을 수행할 수 있도록 시스템을 구성할 수 있습니다.

다만 AMP for Endpoints의 파일 및 악성코드 데이터와 AMP for Networks (Firepower System을 사용한 악성코드 방지)의 파일 및 악성코드 데이터의 차이점에 유의해야 합니다.

AMP for Endpoints 악성코드 탐지는 다운로드 또는 실행 시 엔드포인트에서 수행되지만 매니지드 디바이스는 네트워크 트래픽에서 악성코드를 탐지하기 때문에 두 가지 유형의 악성코드 이벤트에 있는 정보는 서로 다릅니다. 예를 들어 AMP for Endpoints가 탐지하는 악성코드 이벤트("엔드포인트 기반 악성코드")에는 파일 경로, 클라이언트 애플리케이션 호출 등에 대한 정보가 포함됩니다. 반면 네트워크 트래픽에서의 악성코드 탐지에는 포트, 애플리케이션 프로토콜, 파일 전송에 사용되는 연결에 대한 원래 IP 주소 정보가 포함됩니다.

또 다른 예로 AMP for Networks가 탐지하는 악성코드 이벤트("네트워크 기반 악성코드 이벤트")의 경우, 사용자 정보에는 네트워크 검색에서 확인된 내용에 따라, 악성코드가 목표로 한 호스트에 가장 최근에 로그인한 사용자가 표시됩니다. 하지만 AMP for Endpoints에서 보고하는 사용자는 악성코드가 탐지된 엔드포인트에 현재 로그인한 사용자를 나타냅니다.

참고 구축에 따라 AMP for Endpoints에서 모니터링하는 엔드포인트는 AMP for Networks에서 모니터링하는 엔드포인트와 동일한 호스트가 아닐 수 있습니다. 따라서 AMP for Endpoints에서 생성한 악성코드 이벤트는 네트워크 맵에 호스트를 추가하지 않습니다. 그러나 시스템은 IP 및 MAC 주소 데이터를 사용하여 AMP for Endpoints 구축에서 가져온 보안 침해 지표로 모니터링되는 호스트에 태그를 지정합니다. 서로 다른 AMP 솔루션을 통해 모니터링되는 두 호스트의 IP 및 MAC 주소가 같은 경우에는 시스템이 AMP for Endpoints IOC로 모니터링되는 호스트에 태그를 잘못 지정할 수 있습니다.

다음 표에는 악성코드 라이선스 사용 시 Firepower에서 생성되는 이벤트 데이터와 AMP for Endpoints에서 생성되는 이벤트 데이터의 차이점이 요약되어 있습니다.

표 ***331: AMP*** 제품 간 데이터 차이점 요약

기능	**AMP for Networks**	**AMP for Endpoints**
생성되는 이벤트	파일 이벤트, 캡처된 파일, 악성코드 이벤트, 회귀적 악성코드 이벤트	악성코드 이벤트
악성코드 이벤트의 정보	기본적인 악성코드 이벤트 정보 및 연결 데이터(IP 주소, 포트, 애플리케이션 프로토콜)	심층적인 악성코드 이벤트 정보, 연결 데이터 없음
네트워크 파일 경로	FMC기반	FMC 및 AMP for Endpoints 관리 콘솔에는 각각 네트워크 파일 경로 분석이 있습니다. 두 가지 모두 유용합니다.

관련 주제

Firepower와 AMP for Endpoints 통합, 1898 페이지

파일 및 악성코드 이벤트 워크플로 사용

테이블에서 파일 및 악성코드 이벤트를 보고 분석에 관련된 정보에 따라 이벤트 보기를 조작하려면 이 절차를 사용하십시오. 이벤트에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보

기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

다음 중 하나를 선택합니다.

- **Analysis(**분석**)** > **Files(**파일**)** > **File Events(**파일 이벤트**)**
- **Analysis(**분석**)** > **Files(**파일**)** > **Malware Events(**악성코드 이벤트**)**

팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면 검색 제한 사항을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 필드 이름을 클릭합니다.

팁 특정 파일이 탐지된 연결을 신속하게 보려면 테이블의 확인란을 사용하여 파일을 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 **Connections Events(**연결 이벤트**)**를 선택합니다.

팁 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)

관련 항목

파일 및 악성코드 이벤트 필드, 2968 페이지
사전 정의 파일 워크플로, 2784 페이지
사전 정의 악성코드 워크플로, 2783 페이지
이벤트 보기 구성, 41 페이지

파일 및 악성코드 이벤트 필드

워크플로를 사용하여 확인 및 검색할 수 있는 파일 및 악성코드 이벤트는 이 섹션에서 열거하는 필드를 포함합니다. 개별 이벤트에 사용 가능한 정보는 정보 생성 방법과 이유에 따라 달라질 수 있습니다.

참고 AMP for Networks 이(가) 악성코드로 식별한 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. 엔드포인트용 AMP가 생성한 악성코드 이벤트에는 대응하는 파일 이벤트가 없으며, 파일 이벤트는 엔드포인트용 AMP 관련 필드를 포함하지 않습니다.

시스템 로그 메시지는 초기 값으로 채워지며, FMC 웹 인터페이스의 해당 필드가 회고 판정 등으로 업데이트되더라도 시스템 로그 메시지는 업데이트되지 않습니다.

작업 **(**시스템 로그**: FileAction)**

파일을 탐지한 파일 정책 규칙과 연결된 작업 및 관련된 모든 파일 규칙 작업 옵션

AMP 클라우드

AMP for Endpoints 이벤트 출처인 AMP 클라우드의 이름.

애플리케이션 파일 이름

AMP for Endpoints 탐지가 발생했을 때 악성코드 파일에 액세스하는 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 않습니다.

애플리케이션 파일 **SHA256**

탐지가 발생했을 때 AMP for Endpoints를 탐지 또는 격리하는 파일에 액세스한 상위 파일의 SHA-256 해시 값.

애플리케이션 프로토콜**(**시스템 로그**: ApplicationProtocol)**

매니지드 디바이스가 파일을 탐지한 트래픽에 의해 사용되는 애플리케이션 프로토콜.

애플리케이션 프로토콜 카테고리 또는 태그

애플리케이션의 기능을 파악하도록 애플리케이션의 특성을 분류하는 기준.

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

아카이브 깊이**(**시스템 로그**: ArchiveDepth)**

아카이브 파일에 중첩되는 파일의 레벨(해당되는 경우).

아카이브 이름**(**시스템 로그**: ArchiveFileName)**

악성코드 파일을 포함하는 아카이브 파일의 이름(해당되는 경우).

아카이브 파일의 내용을 보려면 **Analysis(**분석**) > Files(**파일**)**에 있는 아카이브 파일 목록 표로 이동하고 아카이브 파일의 테이블 행을 마우스 오른쪽 단추로 클릭한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 클릭합니다.

아카이브 **SHA256(**시스템 로그**: ArchiveSHA256)**

악성코드 파일을 포함하는 아카이브 파일(해당되는 경우)의 SHA-256 해시 값.

아카이브 파일의 내용을 보려면 Analysis(분석) > Files(파일)에 있는 아카이브 파일 목록 표로 이동하고 아카이브 파일의 테이블 행을 마우스 오른쪽 단추로 클릭한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 클릭합니다.

ArchiveFileStatus(시스템 로그만 있음**)**

검사 중인 아카이브의 상태. 다음과 같은 값을 사용할 수 있습니다.

- Pending(보류 중) - 아카이브를 검사하는 중
- Extracted(추출됨) - 문제없이 검사함
- Failed(장애 발생함) - 시스템 자원이 부족하여 검사하지 못함
- Depth Exceeded(수준 초과됨) - 검사는 성공했으나 아카이브에서 중첩 검사 수준이 초과됨
- Encrypted(암호화됨) - 검사가 일부분 성공함(아카이브가 암호화된 아카이브이거나 암호화된 아카이브를 포함함)
- Not Inspectable(검사 불가) - 검사가 일부분 성공함(파일이 손상되었거나 형식이 잘못되었을 수 있음)

사업 타당성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

카테고리/파일 유형 카테고리

파일 유형의 일반적인 카테고리(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)

클라이언트**(**시스템 로그**: Client)**

한 호스트에서 실행되며 서버에 의존하여 파일을 전송하는 클라이언트 애플리케이션.

클라이언트 카테고리 또는 태그

애플리케이션의 기능을 파악하도록 애플리케이션의 특성을 분류하는 기준.

Connection Counter (시스템 로그만 해당**)**

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

Connection Instance ID (시스템 로그만 해당**)**

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

개수

동일한 행을 둘 이상 생성하는 제약 조건을 적용하는 경우, 각 행의 정보와 일치하는 이벤트의 수.

탐지 이름

탐지된 악성코드의 이름.

탐지기

악성코드를 식별하는 AMP for Endpoints 탐지기(예: ClamAV, Spero 또는 SHA).

디바이스

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 파일을 탐지한 디바이스의 이름.

AMP for Endpoints에 의해 생성된 악성코드 이벤트 및 AMP 클라우드에 의해 생성된 회귀적 악성코드 이벤트에서 Firepower Management Center의 이름.

DeviceUUID (시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

속성**/**파일 속성**(**시스템 로그**: SHA_Disposition)**

파일 속성:

Malware(악성코드**)**

AMP 클라우드가 파일을 악성코드로 분류했거나, 로컬 악성코드 분석에서 악성코드가 식별되었거나, 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다.

정상

AMP 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. 정상 파일은 정상으로 변경된 경우에만 악성코드 테이블에 나타납니다.

알 수 없음

시스템이 AMP 클라우드를 쿼리했으나 파일에 상태가 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다.

맞춤형 탐지

사용자가 파일을 커스텀 탐지 목록에 추가했음을 나타냅니다.

사용 불가능

시스템이 AMP 클라우드를 쿼리하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.

해당 없음

파일 탐지 또는 파일 차단 규칙이 파일을 처리했으며 Firepower Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.

파일 속성은 시스템이 AMP 클라우드를 쿼리하지 않은 파일에 대해서만 표시됩니다.

시스템 로그는 초기 속성만 반영합니다. 회귀적 판정을 반영하도록 업데이트 되지 않습니다.

도메인

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 파일을 탐지한 디바이스의 도메인. AMP for Endpoints에 의해 생성된 악성코드 이벤트 및 AMP 클라우드에 의해 생성된 회귀적 악성코드 이벤트에서 해당 이벤트를 보고한 AMP 클라우드 연결과 관련된 도메인.

이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

DstIP(시스템 로그만 있음**)**

연결에 응답한 호스트의 IP 주소. FileDirection 필드 값에 따라 파일 발신자나 수신자의 IP 주소일 수 있습니다.

FileDirection이 **`Upload`(**업로드**)**인 경우 파일 수신자의 IP 주소입니다.

FileDirection이 **`Download`(**다운로드**)**인 경우 파일 발신자의 IP 주소입니다.

SrcIP도 참조하십시오.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

DstPort(시스템 로그만 있음**)**

DstIP아래 설명된 연결에 사용되는 포트.

이그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에서 벗어날 때 사용하는 가상 라우터의 이름입니다.

이벤트 하위 유형

악성코드 탐지로 이어진 AMP for Endpoints 작업(예: Create(생성), Execute(실행), Move(이동) 또는 Scan(스캔)).

이벤트 유형

악성코드 이벤트 하위 유형.

파일 이름**(**시스템 로그**: FileName)**

파일의 이름

File Path(파일 경로**)**

AMP for Endpoints에 의해 탐지된 악성코드 파일의 파일 경로(파일 이름 제외).

파일 정책**(**시스템 로그**: FilePolicy)**

파일을 탐지한 파일 정책.

파일 스토리지**/**저장됨 **(**시스템 로그**: FileStorageStatus)**

이벤트와 관련 된 파일의 저장 상태:

Stored(저장됨**)**

관련된 파일이 현재 저장되어 있는 모든 이벤트를 반환합니다.

Stored in connection(연결에 저장됨**)**

관련된 파일이 현재 저장되어 있는지와 상관없이, 시스템이 관련된 파일을 캡처 및 저장한 모든 이벤트를 반환합니다.

Failed(TLS 필수 실패**)**

시스템이 관련된 파일을 저장하지 못한 모든 이벤트를 반환합니다.

시스템 로그 필드는 초기 상태만 포함합니다. 변경된 상태를 반영하도록 업데이트되지 않습니다.

File Timestamp(파일 타임스탬프**)**

AMP for Endpoints가 악성코드 파일이 생성된 것으로 탐지한 시간 및 날짜.

FileDirection(시스템 로그만 있음**)**

연결 중 파일이 업로드되거나 다운로드되었는지 여부. 가능한 값은 다음과 같습니다.

- Download(다운로드) — DstIP에서 SrcIP로 파일이 전송되었습니다.
- Upload(업로드) — SrcIP에서 DstIP로 파일이 전송되었습니다.

FileSandboxStatus(시스템 로그만 있음**)**

동적 분석을 위해 파일이 전송되었는지 여부와 그러한 경우 해당 상태를 나타냅니다.

첫 번째 패킷 시간 **(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

FirstPacketSecond(시스템 로그만 있음**)**

파일 다운로드 또는 업로드 플로우가 시작된 시간으로, .

이벤트가 발생한 시간이 메시지 헤더 타임스탬프에 캡처됩니다.

HTTP 응답 코드

파일이 전송된 경우 클라이언트의 HTTP 요청에 대한 응답으로 제출된 HTTP 상태 코드.

인그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에 진입할 때 사용하는 가상 라우터의 이름입니다.

IOC

악성코드 이벤트가 연결과 관련된 호스트에 대해 IOC(indication of compromise)를 트리거했는지 여부. AMP for Endpoints 데이터 IOC 규칙을 트리거하는 경우, 전체 악성코드 이벤트가 AMP IOC 유형으로 생성됩니다.

Message

악성코드 이벤트와 연결된 추가 정보. 파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트의 경우, 이 필드는 속성이 변경되어 관련 회귀적 이벤트가 있는 파일에 대해서만 입력됩니다.

Protocol(시스템 로그만 있음)

연결에 사용된 프로토콜(예: TCP 또는 UDP).

Receiving Continent(수신 대륙)

파일을 수신하는 호스트의 대륙.

Receiving Country(수신 국가)

파일을 수신하는 호스트의 국가.

수신 **IP**

FMC 웹 인터페이스:

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 파일을 수신하는 호스트의 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 커넥터가 이벤트를 보고한 엔드포인트의 IP 주소.

시스템 로그에 해당하는 항목(Firepower 디바이스에서 생성된 이벤트만 해당)은 **DstIP** 및 **SrcIP**를 참조하십시오.

Receiving Port(수신 포트)

FMC 웹 인터페이스:

파일이 탐지된 트래픽에 의해 사용된 대상 포트.

시스템 로그 해당 정보는 **DstIP**, **SrcIP**, **DstPort**, **SrcPort**를 참조하십시오.

보안 상황(시스템 로그: **Context**)

트래픽이 통과된 가상 방화벽 그룹을 식별하는 메타데이터. 다중 상황 모드에서 실행되는 ASA FirePOWER디바이스를 최소한 한 개 관리하는 경우 시스템에 이 필드만 표시됩니다.

Sending Continent(송신 대륙)

파일을 전송하는 호스트의 대륙.

Sending Country(송신 국가)

파일을 전송하는 호스트의 국가.

송신 **IP**

FMC 웹 인터페이스: 파일을 전송하는 호스트의 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

시스템 로그 해당 정보는 **DstIP** 및 **SrcIP**를 참조하십시오.

Sending Port(송신 포트)

FMC 웹 인터페이스:

파일이 탐지된 트래픽에 의해 사용된 소스 포트.

시스템 로그 해당 정보는 **DstIP**, **SrcIP**, **DstPort**, **SrcPort**를 참조하십시오.

SHA256/ 파일 **SHA256** (시스템 로그: **FileSHA256**)

파일의 SHA-256 해시 값

SHA256 값을 생성하려면 다음 중 하나를 통해 파일을 처리해야 합니다.

- **Store files**(파일 저장)가 활성화된 Detect Files(파일 탐지) 파일 규칙
- **Store files**(파일 저장)가 활성화된 Block Files(파일 차단) 파일 규칙
- Malware Cloud Lookup file(악성코드 클라우드 검색) 파일 규칙
- Block Malware file(악성코드 차단) 파일 규칙
- AMP for Endpoints

이 열에는 가장 최근에 탐지된 파일 이벤트 및 파일 속성을 나타내고 네트워크 파일 경로로 링크되는 네트워크 파일 경로 아이콘도 표시됩니다.

크기(**KB**)/파일 크기(**KB**)(시스템 로그: **FileSize**)

FMC 웹 인터페이스에서 킬로바이트 단위의 파일 크기.

시스템 로그 메시지에서 바이트 단위의 파일 크기.

파일을 완전히 수신하기 전에 시스템에서 파일 유형을 결정하는 경우, 파일 크기가 계산되지 않을 수 있습니다. 그러한 경우 이 필드는 공란입니다.

SperoDisposition(시스템 로그만 있음)

파일 분석에 SPERO 서명이 사용되었는지를 나타냅니다. 가능한 값은 다음과 같습니다.

- 파일에서 수행되는 Spero 탐지
- 파일에서 수행되지 않는 Spero 탐지.

SrcIP(시스템 로그만 있음)

연결을 시작한 호스트의 IP 주소. FileDirection 필드 값에 따라 파일 발신자나 수신자의 IP 주소일 수 있습니다.

FileDirection이 **`Upload`**(업로드)인 경우 파일 발신자의 IP 주소입니다.

FileDirection이 **`Download`**(다운로드)인 경우 파일 수신자의 IP 주소입니다.

DstIP도 참조하십시오.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 2893 페이지도 참조하십시오.

SrcPort(시스템 로그만 있음)

SrcIP아래 설명된 연결에 사용되는 포트.

SSL 실제 작업 (시스템 로그: **SSLActualAction**)

시스템이 암호화된 트래픽에 적용하는 작업.

Block or Block with reset(차단 또는 차단 후 재설정)

차단된 암호화된 연결을 나타냅니다.

암호 해독(재서명)

다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(대체 키)

대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(알려진 키)

알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.

기본 작업

연결이 기본 작업에 의해 처리되었음을 나타냅니다.

암호 해독 안 함

시스템이 암호 해독하지 않은 연결을 나타냅니다.

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 인증서 정보

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)
- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number, Certificate Fingerprint(일련 번호, 인증서 지문)
- Public Key Fingerprint(공개 키 지문)

시스템 로그는 **SSLCertificate**를 참조하십시오.

SSL 실패 이유**(**시스템 로그**: SSLFlowStatus)**

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)

- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)
- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL Status

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)** (SSL 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업. 잠금 아이콘이 TLS/SSL 인증서 세부 사항으로 연결됩니다. 인증서를 사용할 수 없는 경우(예: TLS/SSL 핸드셰이크 오류로 연결 차단), 잠금 아이콘이 흐리게 표시됩니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`(암호 해독 하지 않음(알려지지 않은 암호화 그룹))로 표시됩니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL 대상자/발급자 국가

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

SSLCertificate(시스템 로그만 있음)

TLS/SSL 서버의 인증서 지문.

위협 이름 **(**시스템 로그**: ThreatName)**

탐지된 악성코드의 이름.

위협 점수 **(**시스템 로그**: ThreatScore)**

이 파일과 가장 최근에 연결된 위협 점수. 동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 값입니다.

위협 점수 아이콘이 Dynamic Analysis Summary(동적 분석 요약) 보고서로 링크됩니다.

시간

이벤트가 생성된 날짜 및 시간 이 필드는 검색할 수 없습니다.

시스템 로그 메시지에서 **FirstPacketSecond**를 참조하십시오.

유형**/**파일 유형**(**시스템 로그**: FileType)**

HTML 또는 MSEXE 등의 파일 형식

URI/파일 **URI(**시스템 로그**: URI)**

파일 트랜잭션과 관련된 연결의 URI(예: 사용자가 파일을 다운로드하는 URL).

사용자**(**시스템 로그**: User)**

연결을 시작한 IP 주소에 연결된 사용자 이름입니다. 이 IP 주소가 네트워크 외부에 있는 경우, 일반적으로 연결된 사용자 이름을 알 수 없습니다.

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 이 사용자는 네트워크 검색으로 결정됩니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 AMP for Endpoints가 사용자 이름을 결정합니다. 이러한 사용자는 사용자 검색 또는 제어에 연결할 수 없습니다. 이러한 사용자는 Users(사용자) 테이블에 나타나지 않으며 세부 사항도 확인할 수 없습니다.

웹 애플리케이션**(**시스템 로그**: WebApplication)**

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청된 URL을 나타내는 웹 애플리케이.

웹 애플리케이션 카테고리 또는 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

악성코드 이벤트 하위 유형

다음 표에는 악성코드 이벤트 하위 유형, AMP for Networks가 생성하는 악성코드 이벤트("네트워크 기반 악성코드 이벤트") 또는 AMP for Endpoints가 생성하는 악성코드 이벤트("엔드포인트 기반 악성

코드 이벤트")에 해당 하위 유형이 있을 수 있는지 여부, 시스템이 해당 하위 유형을 사용하여 네트워크 파일 경로 분석을 작성하는지 여부가 나열되어 있습니다.

표 ***332:*** 악성코드 이벤트 유형

악성코드 이벤트 하위 유형/검색 값	**AMP for Networks**	**AMP for Endpoints**	파일 경로 분석
네트워크 파일 전송에서 탐지된 위협	예	아니요	예
네트워크 파일 전송에서 탐지된 위협(회귀적)	예	아니요	예
위협 탐지됨	아니요	예	예
제외에서 위협 탐지	아니요	예	예
위협 격리됨	아니요	예	예
AMP IOC(보안 침해 지표)	아니요	예	아니요
차단된 실행	아니요	예	아니요
Cloud Recall 격리	아니요	예	아니요
Cloud Recall 격리 시도 실패	아니요	예	아니요
클라우드 리콜 격리 시작	아니요	예	아니요
격리에서 Cloud Recall 복원	아니요	예	아니요
격리에서 Cloud Recall 복원 실패	아니요	예	아니요
격리에서 클라우드 리콜 복원 시작	아니요	예	아니요
격리 실패	아니요	예	아니요
격리 항목 복원	아니요	예	아니요
격리 복원 실패	아니요	예	아니요
격리 복원 시작	아니요	예	아니요
스캔 완료, 탐지 항목 없음	아니요	예	아니요
스캔 완료, 탐지 항목 있음	아니요	예	아니요
스캔 실패	아니요	예	아니요

악성코드 이벤트 하위 유형/검색 값	**AMP for Networks**	**AMP for Endpoints**	파일 경로 분석
스캔 시작	아니요	예	아니요

파일 및 악성코드 이벤트 필드에서 사용할 수 있는 정보

다음 표에는 시스템이 각 파일 및 악성코드 이벤트 필드에 정보를 표시하는지 여부가 나열되어 있습니다.

조직이 AMP for Endpoints를 구축하고 해당 제품을 Firepower 구축에 통합한 경우:

- AMP for Endpoints 구축에서 가져온 악성코드 이벤트 및 보안 침해 지표 (IOC)에는 컨텍스트 연결 정보가 포함되지 않지만 파일 경로와 호출 클라이언트 애플리케이션 등 다운로드 또는 실행 시 얻는 정보는 포함됩니다.
- 파일 이벤트 테이블 보기에는 AMP for Endpoints 관련 필드가 표시되지 않습니다.

표 ***333:*** 파일 및 악성코드 이벤트 필드에서 사용할 수 있는 정보

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
작업	예	예	예	아니요
AMP 클라우드	아니요	아니요	아니요	예
애플리케이션 파일 이름	아니요	아니요	아니요	예
애플리케이션 파일 SHA256	아니요	아니요	아니요	예
Application Protocol(애플리케이션 프로토콜)	예	예	아니요	아니요
애플리케이션 프로토콜 카테고리 또는 태그	예	예	예	아니요
애플리케이션 위험성	예	예	예	아니요
아카이브 수준	예	예	아니요	예
아카이브 이름	예	예	아니요	예
아카이브 SHA256	예	예	아니요	예
Business Relevance	예	예	예	아니요

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
카테고리/파일 유형 카테고리	예	예	아니요	예
Client(클라이언트)	예	예	예	아니요
클라이언트 카테고리 또는 태그	예	예	예	아니요
개수	예	예	예	예
탐지 이름	아니요	예	아니요	아니요
탐지기	아니요	아니요	아니요	예
디바이스	예	예	예	예
속성/파일 속성	예	예	예	아니요
도메인	예	예	예	예
이벤트 하위 유형	아니요	아니요	아니요	예
이벤트 유형	아니요	예	예	예
파일 이름	예	예	아니요	예
File Path(파일 경로)	아니요	아니요	아니요	예
파일 정책	예	아니요	아니요	아니요
파일 타임스탬프	아니요	아니요	아니요	예
HTTP 응답 코드	예	예	아니요	아니요
IOC(보안 침해 지표)	아니요	예	예	예
Message	예	예	아니요	예
수신 대륙	예	예	예	아니요
수신 국가	예	예	아니요	아니요
수신 IP	예	예	아니요	예
수신 포트	예	예	아니요	아니요
보안 상황	예	예	예	예

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
송신 대륙	예	예	예	아니요
송신 국가	예	예	아니요	아니요
송신 IP	예	예	아니요	아니요
송신 포트	예	예	아니요	아니요
SHA256/파일 SHA256	예	예	예	예
크기(KB)/파일 크기(KB)	예	예	아니요	예
SSL 실제 작업(검색만 해당)	예	예	아니요	아니요
SSL 인증서 정보(검색만 해당)	예	예	아니요	아니요
SSL 실패 이유(검색만 해당)	예	예	아니요	아니요
SSL Status	예	예	아니요	아니요
SSL 주체/발급자 국가(검색만 해당)	예	예	아니요	아니요
파일 스토리지/저장됨(검색만 해당)	예	예	아니요	아니요
위협 이름	아니요	예	예	예
위협 점수	예	예	아니요	아니요
시간	예	예	예	예
파일/파일 형식	예	예	아니요	예
URI/파일 URI	예	예	아니요	아니요
User	예	예	아니요	예
웹 애플리케이션	예	예	예	아니요
웹 애플리케이션 카테고리 또는 태그	예	예	예	아니요

분석된 파일에 대한 세부 정보 보기

팁 추가 옵션을 보려면 이벤트 페이지의 테이블에서 파일 SHA를 마우스 오른쪽 버튼으로 클릭합니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지를 참고하십시오.

파일 구성 보고서

로컬 악성코드 분석 또는 동적 분석을 구성하는 경우, 시스템은 파일을 분석한 후 파일 구성 보고서를 생성합니다. 이 보고서를 사용하면 추가로 파일을 분석하여 포함된 악성 코드를 파일이 전달할 수 있는지 여부를 확인할 수 있습니다.

파일 구성 보고서에는 파일 속성, 파일에 포함된 개체, 탐지된 바이러스가 나열됩니다. 파일 구성 보고서에는 해당 파일 유형과 관련된 추가 정보도 나열될 수 있습니다. 시스템은 저장된 파일을 정리할 때 연결된 파일 구성 보고서도 정리합니다.

파일 구성 정보를 보려면 네트워크 파일 경로 분석 사용, 2996 페이지를 참조하십시오.

AMP 프라이빗 클라우드에서 파일 세부 정보 보기

AMP 프라이빗 클라우드를 구축한 경우, 프라이빗 클라우드에서 분석된 파일에 대한 추가 세부 정보를 볼 수 있습니다.

자세한 내용은 프라이빗 클라우드 설명서를 참조하십시오.

프로시저

AMP 프라이빗 클라우드 콘솔에 직접 로그인합니다.

위협 점수 및 동적 분석 요약 보고서

위협 점수

표 ***334:*** 위협 점수 평가

위협 점수	숫자 점수	아이콘
Low	0-24	**Low**
Medium	25-69	**Medium**
High	70-94	**High**

위협 점수	숫자 점수	아이콘
Very High	95-100	매우 높음

Firepower Management Center은 파일의 속성과 동일한 시간 동안 파일의 위협 점수를 캐시합니다. 이러한 파일이 나중에 탐지되는 경우, 시스템은 Cisco Threat Grid 클라우드 또는 Cisco Threat Grid 온프레미스 어플라이언스를 다시 쿼리하는 대신 캐시된 위협 점수를 표시합니다. 위협 점수가 정의된 악성코드 임계값 점수를 초과하는 파일에 자동으로 악성코드 파일 속성을 할당할 수 있습니다.

동적 분석 요약

동적 분석 요약을 사용할 수 있는 경우 위협 점수 아이콘을 클릭하여 위협 점수를 볼 수 있습니다. 여러 보고서가 존재하는 경우, 이 요약은 정확한 위협 점수와 일치하는 최근 보고서를 기반으로 합니다. 정확한 위협 점수와 일치하는 보고서가 없으면 위협 점수가 가장 높은 보고서가 표시됩니다. 보고서가 둘 이상이면 위협 점수를 선택하여 각각의 보고서를 볼 수 있습니다.

요약에는 위협 점수를 구성하는 각 구성 요소 위협이 나열되어 있습니다. 각 위협 요소를 확장하여 AMP 클라우드에서 발견한 내용 및 이 구성 요소 위협과 관련된 프로세스를 나열할 수 있습니다.

프로세스 트리에는 Cisco Threat Grid 클라우드가 파일 실행을 시도했을 때 시작된 프로세스가 표시됩니다. 이는 악성코드가 포함된 파일이 예상을 뛰어넘어 프로세스 및 시스템 리소스에 대한 액세스를 시도했는지(예: Word 문서를 실행하여 Microsoft Word를 열고, Explorer를 시작한 다음 Java Runtime Environment 시작) 여부를 파악하는 데 도움이 될 수 있습니다.

나열된 각 프로세스에는 실제 프로세스 확인에 사용할 수 있는 프로세스 식별자가 포함되어 있습니다. 프로세스 트리의 하위 노드는 상위 프로세스의 결과로 시작된 프로세스를 나타냅니다.

동적 분석 요약에서 **View Full Report(**전체 보고서 보기**)**를 클릭하여 AMP 클라우드의 전체 분석이 자세히 설명된 전체 분석 보고서를 볼 수 있습니다. 여기에는 일반 파일 정보, 탐지된 모든 프로세스에 대한 보다 심층적인 검토, 파일 분석의 분류 및 기타 관련 정보가 포함되어 있습니다.

캡처된 파일 워크플로 사용

매니지드 디바이스는 네트워크 트래픽에서 탐지된 파일을 캡처할 때 이벤트를 로깅합니다.

참고 악성코드가 포함된 파일을 디바이스가 캡처하는 경우, 디바이스는 2개의 이벤트를 생성합니다. 즉, 파일을 탐지하면 파일 이벤트를 생성하고 악성코드를 탐지하면 악성코드 이벤트를 생성합니다.

테이블에서 캡처된 파일 목록을 보고 분석과 관련된 정보에 따라 이벤트 보기를 조작하려면 이 절차를 사용하십시오. 캡처된 파일에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

파일 정책 업데이트 등 구성 변경 후 시스템이 파일을 다시 캡처하는 경우, 시스템은 해당 파일의 기존 정보를 업데이트합니다.

예를 들어 악성 코드 클라우드 조회 작업을 사용하여 파일을 캡처하도록 파일 정책을 구성하는 경우, 시스템은 파일과 함께 파일 속성 및 위협 점수를 저장합니다. 그런 다음 파일 정책을 업데이트하고 시스템이 새로운 **Detect Files(**파일 탐지**)** 작업으로 인해 동일한 파일을 다시 캡처하는 경우, 시스템은 파일의 **Last Changed(**마지막으로 변경된**)** 값을 업데이트합니다. 하지만 사용자가 다른 악성코드 클라우드 조회를 수행하지 않았더라도 시스템은 기존 속성과 위협 점수를 제거하지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

Analysis(분석**)** > **Files(**파일**)** > **Captured Files(**캡처된 파일**)**을(를) 선택합니다.

팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면 검색 제한 사항을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 필드 이름을 클릭합니다.

관련 항목

캡처된 파일 필드, 2986 페이지
사전 정의 캡처 파일 워크플로, 2784 페이지
이벤트 보기 구성, 41 페이지

캡처된 파일 필드

사전 정의된 캡처된 파일 워크플로의 마지막 페이지이며 맞춤형 워크플로에 추가할 수 있는 캡처된 파일의 테이블 보기에는 캡처된 파일 테이블의 각 필드에 대한 열이 포함됩니다.

이 테이블을 검색할 때는 검색하는 이벤트에서 사용할 수 있는 데이터에 따라 검색 결과가 달라짐에 유의하십시오. 사용 가능한 데이터에 따라 검색 제약 조건이 적용되지 않을 수도 있습니다. 예를 들어 동적 분석을 위해 제출된 적이 없는 파일에는 연결된 위협 점수가 없을 수 있습니다.

표 ***335:*** 캡처된 파일 필드

필드	설명
아카이브 검사 상태	아카이브 파일의 경우 아카이브 검사의 상태: • Pending(보류 중)은 시스템이 아카이브 파일 및 내용을 여전히 검사 중임을 나타냅니다. 파일이 시스템을 다시 통과하면 완전한 정보를 이용할 수 있게 됩니다. • Extracted(추출됨)는 시스템이 아카이브의 내용을 추출 및 검사할 수 있게 되었음을 나타냅니다. • 매우 드물지만 시스템이 추출을 처리할 수 없는 경우 Failed(실패함)가 발생할 수 있습니다. • Depth Exceeded(수준 초과)는 아카이브에 허용되는 최대 깊이를 초과하여 중첩된 아카이브 파일이 포함되어 있음을 나타냅니다. • Encrypted(암호화됨)는 아카이브 파일의 내용이 암호화되어 검사할 수 없음을 나타냅니다. • Not Inspectable(검사 불가능)은 시스템이 아카이브의 내용을 추출 및 검사할 수 없음을 나타냅니다. 이 상태의 세 가지 주요 원인은 정책 규칙 작업, 정책 구성 및 손상된 파일입니다. 아카이브 파일의 내용을 보려면 테이블에서 해당 행을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 표시한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 선택합니다.
카테고리	파일 유형의 일반적인 범주(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)
탐지 이름	탐지된 악성코드의 이름.

필드	설명
속성	파일의 AMP for Networks 속성: • Malware(악성코드)는 AMP 클라우드가 파일을 악성코드로 분류했거나 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. • Clean(정상)은 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • Unknown(알 수 없음)은 시스템이 AMP 클라우드를 쿼리했지만 파일에 속성이 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다. • Custom Detection(사용자 지정 탐지)은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • Unavailable(사용할 수 없음)은 시스템이 AMP 클라우드를 쿼리할 수 없음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. • N/A는 Detect Files(파일 탐지) 또는 Block Files(파일 차단) 규칙이 파일을 처리했고 Firepower Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.
도메인	캡처된 파일이 탐지된 도메인입니다. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

필드	설명
동적 분석 상태	파일이 동적 분석을 위해 제출되었는지 여부를 나타내는 다음 값 중 하나 이상: • Analysis Complete(분석 완료) - 위협 점수 및 동적 분석 요약 보고서를 받은, 동적 분석을 위해 제출된 파일 • Capacity Handled(처리된 용량) - 현재 제출할 수 없어서 저장된 파일 • Capacity Handled (Network Issue)(처리된 용량(네트워크 문제)) - 네트워크 연결 문제로 인해 제출할 수 없어서 저장된 파일 • Capacity Handled (Rate Limit)(처리된 용량(속도 제한)) - 최대 제출 수에 도달했기 때문에 제출할 수 없어 저장된 파일 • Device Not Activated(디바이스 활성화되지 않음) - 디바이스가 온프레미스 Cisco Threat Grid 어플라이언스에서 활성화되지 않아 제출되지 않은 파일 이 상태가 표시되면 지원 팀에 문의하십시오. • Failure (Analysis Timeout)(실패(분석 시간 초과)) - AMP 클라우드가 아직 결과를 반환하지 않은 제출된 파일 • Failure (Cannot Run File)(실패(파일 실행 불가)) - AMP 클라우드가 테스트 환경에서 실행할 수 없는 제출된 파일 • Failure (Network Issue)(실패(네트워크 문제)) - 네트워크 연결 오류로 인해 제출되지 않은 파일 • Not Sent for Analysis(분석을 위해 제출되지 않음) - 제출되지 않은 파일 • Not Suspicious (Not Sent For Analysis)(의심스럽지 않음(분석을 위해 제출되지 않음)) - 악성코드가 아닌 것으로 사전 분류된 파일 • 이전에 분석됨 - 캐시된 위협 점수가 있는 파일로, 이전에 전송되었음을 나타냅니다. • 분석이 거부됨 - 정적 분석을 기반으로 하는 파일은 예를 들어 동적 요소가 포함되어 있지 않으므로 위험할 가능성이 낮습니다. • Sent for Analysis(분석을 위해 전송) - 악성코드로 사전 분류되고 동적 분석을 위해 대기열에 넣은 파일

필드	설명
Dynamic Analysis Status Changed(동적 분석 상태 변경됨)	파일의 동적 분석 상태가 마지막으로 변경된 시간.
파일 이름	파일의 SHA-256 해시 값에 연결된, 가장 최근에 탐지된 파일 이름.
마지막 변경 날짜	이 파일에 연결된 정보가 마지막으로 업데이트된 시간.
마지막 전송	동적 분석을 위해 파일이 가장 최근에 클라우드에 제출된 시간.
로컬 악성코드 분석 상태	시스템이 파일에서 로컬 악성코드 분석을 수행했는지 여부를 나타내는 다음 값 중 하나: • Analysis Complete(분석 완료) - 시스템이 로컬 악성코드 분석을 사용하여 파일을 검사하고 사전 분류했습니다 • Analysis Failed(분석 실패) - 시스템이 로컬 악성코드 분석을 사용하여 파일 검사를 시도하고 실패했습니다 • Manual Request Submitted(수동 요청 제출됨) - 사용자가 로컬 악성코드 분석을 위해 파일을 제출했습니다 • Not Analyzed(분석되지 않음) - 시스템이 로컬 악성코드 분석을 사용하여 파일을 검사하지 않았습니다
SHA256	파일의 SHA-256 해시 값 및 가장 최근에 탐지된 파일 이벤트 및 파일 속성을 나타내는 네트워크 파일 경로 분석 아이콘. 네트워크 파일 경로 분석을 보려면 경로 분석 아이콘을 클릭합니다.
Storage Status	파일이 매니지드 디바이스에 저장되는지 여부를 나타냅니다. • File Stored • 저장되지 않음(속성 보류 중)
위협 점수	이 파일과 가장 최근에 연결된 위협 점수. 동적 분석 요약 보고서를 보려면 위협 점수 아이콘을 클릭합니다.
유형	파일 형식(예: HTML 또는 MSEXE).

저장된 파일 다운로드

디바이스가 파일을 저장하면 Firepower Management Center가 해당 디바이스와 통신할 수 있고 파일을 삭제하지 않은 한 사용자는 장기 스토리지 및 분석을 위해 파일을 로컬 호스트에 다운로드하고 수동으로 파일을 분석할 수 있습니다. 연결된 파일 이벤트, 악성코드 이벤트, 캡처된 파일 보기 또는 파일의 경로 분석에서 파일을 다운로드할 수 있습니다.

악성코드는 유해하므로 기본적으로 모든 파일 다운로드를 확인해야 합니다. 하지만 사용자 환경설정에서 확인을 비활성화할 수 있습니다.

Unknown(알 수 없음) 속성의 파일에는 악성코드가 포함되어 있을 수 있으므로 파일을 다운로드할 때 시스템은 먼저 해당 파일을 `.zip` 패키지에 아카이브합니다. `.zip` 파일 이름에는 파일 속성과 파일 형식 및 SHA-256 값(사용 가능한 경우)이 포함됩니다. 실수로 압축을 해제하지 못하도록 `.zip` 파일을 비밀번호로 보호할 수 있습니다. 사용자 환경설정에서 기본 `.zip` 파일 비밀번호를 수정하거나 제거할 수 있습니다.

주의 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

분석을 위해 수동으로 파일 제출

분석을 위해 파일을 수동으로 제출하면 시스템은 로컬 분석을 실행한 다음 동적 분석을 위해 클라우드에 이 파일을 제출합니다. 하지만 파일 정책에서 로컬 분석이 활성화되어 있지 않고 분석을 위해 수동으로 파일을 제출하는 경우, 파일은 동적 분석을 위해서만 전송됩니다.

실행 파일 외에 .swf, .jar 등과 같이 자동 제출에 적합하지 않은 파일 형식도 제출할 수 있습니다. 이렇게 하면 속성에 상관없이 광범위한 파일을 더욱 신속히 분석하고 인시던트의 정확한 원인을 파악할 수 있습니다.

참고 시스템은 AMP 클라우드에서 동적 분석 대상 파일 형식 목록(하루에 한 번)과 제출 가능한 최소 및 최대 파일 크기 업데이트를 확인합니다.

상황에 따라 분석을 위해 두 가지 방법으로 파일을 제출할 수 있습니다.

시작하기 전에

분석을 위해 캡처된 파일을 수동으로 제출하려면, 하나 이상의 파일 규칙을 파일을 저장하도록 구성해야 합니다. 자세한 내용은 파일 정책 및 악성코드 보호, 1861 페이지를 참조하십시오.

프로시저

단계 **1** 분석을 위해 단일 파일을 제출하려면:

a) 다음 중 하나를 선택합니다.

- **Analysis(**분석**) > Files(**파일**) > File Events(**파일 이벤트**)**
- **Analysis(**분석**) > Files(**파일**) > Malware Events(**악성코드 이벤트**)**
- **Analysis(**분석**) > Files(**파일**) > Captured Files(**캡처된 파일**)**

b) <이벤트 유형 또는 파일>의 테이블 보기를 클릭합니다.

c) 테이블에서 파일을 마우스 오른쪽 버튼으로 클릭하고 **Analyze File(**파일 분석**)**을 선택합니다.

단계 **2** 캡처된 여러 파일을 제출하려면(한 번에 최대 25개):

a) **Analysis(**분석**) > Files(**파일**) > Captured Files(**캡처된 파일**)**를 선택합니다.

b) 분석할 각 파일 옆의 확인란을 선택합니다.

c) **Analyze(**분석**)**를 클릭합니다.

네트워크 파일 전파 흔적 분석

네트워크 파일 경로 분석 기능은 호스트가 네트워크에서 악성코드 파일을 포함한 파일을 전송한 방법을 매핑합니다. 경로 분석은 파일 전송 데이터, 파일의 속성, 파일 전송의 차단 여부 또는 파일의 격리 여부를 차트로 표시합니다. 어떤 호스트와 가 악성코드를 전송했는지, 어떤 호스트가 위험한지를 확인하고 파일 전송 추세를 관찰할 수 있습니다.

AMP 클라우드가 속성을 할당한 모든 파일의 전송을 추적할 수 있습니다. 시스템은 AMP for Networks 및 AMP for Endpoints의 악성코드 탐지 및 차단 관련 정보를 사용하여 경로 분석을 작성할 수 있습니다.

최근 탐지된 악성코드 및 분석된 경로 분석

Network File Trajectory List(네트워크 파일 경로 분석 목록) 페이지에는 네트워크에서 가장 최근에 탐지된 악성코드는 물론 가장 최근에 경로 분석 맵을 살펴본 파일도 표시됩니다. 네트워크에서 각 파일을 가장 최근에 본 시간, 파일의 SHA-256 해시 값, 이름, 형식, 현재 파일 속성, 내용(아카이브 파일의 경우), 파일에 연결된 이벤트 수를 이러한 목록에서 확인할 수 있습니다.

이 페이지에는 SHA-256 해시 값이나 파일 이름을 기반으로, 또는 파일을 전송하거나 수신한 호스트의 IP 주소별로 파일을 찾을 수 있는 검색 상자도 포함되어 있습니다. 파일을 찾은 후 **File SHA256** 값을 클릭하여 자세한 경로 분석 맵을 볼 수 있습니다.

네트워크 파일 경로 분석 상세정보 보기

자세한 네트워크 파일 경로 분석을 살펴봄으로써 네트워크를 통해 파일을 추적할 수 있습니다. 파일의 세부 정보를 보려면 파일의 SHA 256 값을 검색하거나 Network File Trajectory(네트워크 파일 경로 분석) 목록에서 **File SHA 256** 링크를 클릭합니다.

네트워크 파일 경로 분석 세부 정보 페이지는 세 부분으로 구성됩니다.

- Summary Information(요약 정보) - 파일의 경로 분석 페이지에는 파일 식별 정보, 파일을 처음 본 시간과 네트워크에서 가장 최근에 본 시간, 파일에 연결된 관련 이벤트 및 호스트 수, 파일의 현재 속성을 비롯하여 파일에 대한 요약 정보가 표시됩니다. 매니지드 디바이스가 파일을 저장한 경우, 이 섹션에서 로컬로 파일을 다운로드하거나 동적 분석을 위해 파일을 제출하거나 파일 목록에 파일을 추가할 수 있습니다.
- Trajectory Map(경로 분석 맵) - 파일의 경로 분석 맵은 네트워크에서 처음 탐지될 때부터 가장 최근까지 파일을 시각적으로 추적합니다. 맵에는 호스트가 파일을 전송하거나 수신한 시간, 파일 전송 빈도, 파일이 차단되거나 격리된 시간이 표시됩니다. 데이터 포인트 사이의 세로 줄은 호스트 간 파일 전송을 나타냅니다. 데이터 포인트를 연결하는 가로 줄은 시간에 따른 호스트의 파일 활동을 보여줍니다.

  또한 파일의 파일 이벤트가 발생한 빈도와 시스템이 속성 또는 회귀적 속성을 할당한 시간도 표시됩니다. 맵에서 데이터 포인트를 선택하고 호스트가 해당 파일을 처음 전송한 인스턴스로 역추적하는 경로를 강조 표시할 수 있습니다. 이 경로는 또한 파일의 전송자 또는 수신자로서 호스트와 관련된 모든 시점과 교차하며.
- Related Events(관련 이벤트) - Events(이벤트) 테이블에는 맵의 각 데이터 포인트에 대한 이벤트 정보가 나열됩니다. 테이블과 맵을 사용하면 특정 파일 이벤트, 이 파일을 전송하거나 수신한 네트워크의 호스트, 맵의 관련 이벤트, 선택한 값으로 제한된 테이블의 기타 관련 이벤트를 정확히 파악할 수 있습니다.

네트워크 파일 경로 분석 요약 정보

Network File Trajectory(네트워크 파일 경로 분석) 목록에 표시되는 파일의 세부 정보 페이지 상단에는 다음 요약 정보가 표시됩니다.

팁 관련 파일 이벤트를 보려면 필드 값 링크를 클릭하십시오. File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지가 새 창에서 열리고, 선택한 값도 포함된 모든 파일 이벤트가 표시됩니다.

표 ***336: Network File Trajectory Summary Information(***네트워크 파일 경로 분석 요약 정보***)*** 필드

이름	설명
아카이브 콘텐츠	검사된 아카이브 파일의 경우, 아카이브에 포함된 파일 수입니다.

이름	설명
현재 폐기	다음 AMP for Networks 파일 속성 중 하나: • Malware(악성코드)는 AMP 클라우드가 파일을 악성코드로 분류했거나 로컬 악성코드 분석에서 악성코드로 식별했거나 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. • Clean(정상)은 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • Unknown(알 수 없음)은 시스템에서 AMP 클라우드를 쿼리했지만 파일에 속성이 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드가 파일을 분류하지 않았습니다. • Custom Detection(사용자 지정 탐지)은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • Unavaliable(사용할 수 없음)은 시스템이 AMP 클라우드를 쿼리할 수 없음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. • N/A는 Detect Files(파일 탐지) 또는 Block Files(파일 차단) 규칙이 파일을 처리했고 Firepower Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.
탐지 이름	로컬 악성코드 분석에서 탐지된 악성코드의 이름입니다.
이벤트 수	네트워크에 표시되는, 파일에 연결된 이벤트의 수, 그리고 탐지된 이벤트가 250개가 넘는 경우 맵에 표시되는 이벤트의 수.
파일 카테고리	파일 형식의 일반 카테고리(예: Office 문서 또는 시스템 파일).
파일 이름	네트워크에 표시되는, 이벤트와 연결된 파일의 이름. 여러 파일 이름이 하나의 SHA-256 해시 값에 연결되어 있으면 가장 최근에 탐지된 파일 이름이 나열됩니다. more(더 보기)를 클릭하여 이 항목을 확장하면 나머지 파일 이름을 볼 수 있습니다.
파일 SHA256	파일의 SHA-256 해시 값 해시는 기본적으로 압축된 형식으로 표시됩니다. 전체 해시 값을 보려면 포인터를 값 위로 이동합니다. 파일 이름 하나에 여러 SHA-256 해시 값이 연결되어 있는 경우 모든 해시 값을 보려면 포인터를 링크 위로 이동합니다.

이름	설명
파일 크기(KB)	킬로바이트 단위의 파일 크기.
File Type(파일 유형)	파일의 파일 형식(예: `HTML` 또는 `MSEXE`).
처음 표시	AMP for Networks 또는 AMP for Endpoints가 처음으로 파일을 탐지한 시간, 파일을 처음 업로드한 호스트의 IP 주소.
최종 확인	AMP for Networks 또는 AMP for Endpoints가 가장 최근에 파일을 탐지한 시간, 파일을 마지막으로 다운로드한 호스트의 IP 주소.
Parent Application(상위 애플리케이션)	AMP for Endpoints의 탐지가 발생했을 때 악성코드 파일에 액세스한 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 않습니다.
Seen On	파일을 전송했거나 수신한 호스트의 수. 한 호스트가 서로 다른 시간에 파일을 업로드 및 다운로드할 수 있으므로 총 호스트 수는 `Seen On Breakdown` 필드에 지정된 총 전송자 수와 총 수신자 수의 합과 일치하지 않을 수 있습니다.
Seen On Breakdown	파일을 보낸 호스트의 수와 파일을 받은 호스트의 수.
위협 이름	AMP for Endpoints가 탐지한 악성코드에 연결된 위협의 이름.
위협 점수	파일의 위협 점수.

네트워크 파일 경로 분석 맵 및 관련 이벤트 목록

파일 궤적 맵의 y 축은 파일과 상호 작용 한 모든 호스트 IP 주소의 목록을 포함 합니다. IP 주소는 시스템이 해당 호스트에서 파일을 처음 탐지한 시점을 기준으로 내림차순으로 나열됩니다. 각 행에는 단일 파일 이벤트, 파일 전송 또는 회귀적 이벤트 등 해당 IP 주소에 연결된 모든 이벤트가 포함됩니다. x축에는 시스템이 각 이벤트를 탐지한 날짜와 시간이 포함됩니다. 타임스탬프는 시간순으로 나열됩니다. 1분 내에 여러 이벤트가 발생한 경우 모두가 동일한 열에 나열됩니다. 맵을 가로와 세로로 스크롤하면 추가 이벤트 및 IP 주소를 볼 수 있습니다.

맵에는 파일 SHA-256 해시에 연결된 최대 250개의 이벤트가 표시됩니다. 이벤트가 250개가 넘으면 처음 10개가 표시되고 추가 이벤트는 **Arrow(**화살표**)**와 함께 생략됩니다. 그런 다음 나머지 이벤트 240개가 표시됩니다.

File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지는 파일 형식을 기반으로 제한된 모든 추가 이벤트와 함께 새 창에 나타납니다. AMP for Endpoints에 의해 생성된 악성코드 이벤트가 표시되지 않으면 Malware Events(악성코드 이벤트) 테이블로 전환하여 이러한 이벤트를 표시해야 합니다.

각 데이터 포인트는 맵 아래의 범례에 설명된 대로 이벤트 및 파일 속성을 나타냅니다. 예를 들어 Malware Block 이벤트 아이콘은 Malicious Disposition 아이콘과 Block Event 아이콘을 결합합니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")에는 하나의 아이콘이 포함됩니다. 회귀적이벤트는 파일이 탐지되는 각 호스트에 대한 열에 아이콘을 표시합니다. 파일 전송 이벤트에는 항상 두 개의 아이콘, 즉 파일 보내기 아이콘과 파일 받기 아이콘이 포함되며, 이 둘은 세로 선으로 연결됩니다. 화살표는 전송자에서 수신자로의 파일 전송 방향을 나타냅니다.

네트워크에서 파일의 진행 상황을 추적하려면 원하는 데이터 포인트를 클릭하여 선택한 데이터 포인트와 관련된 모든 데이터 포인트를 포함하는 경로를 강조 표시할 수 있습니다. 여기에는 다음 이벤트 유형에 연결된 데이터 포인트가 포함됩니다.

- 연결된 IP 주소 가 전송자 또는 수신자인 파일 전송
- 연결된 IP 주소와 관련하여 AMP for Endpoints가 생성한 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")
- 또 다른 IP 주소가 관련된 경우, 연결된 해당 IP 주소가 전송자 또는 수신자인 모든 파일 전송
- 다른 IP 주소가 관련된 경우, 다른 IP 주소와 관련하여 AMP for Endpoints가 생성한 안성코드 이벤트("엔드포인트 기반 악성코드 이벤트")

강조 표시된 데이터 포인트와 연결된 모든 IP 주소 및 타임스탬프도 강조 표시됩니다. Events(이벤트) 테이블의 해당 이벤트도 강조 표시됩니다. 경로에 생략된 이벤트가 포함된 경우 경로 자체는 점선으로 강조 표시됩니다. 생략된 이벤트는 경로와 교차할 수도 있지만 맵에는 표시되지 않습니다.

네트워크 파일 경로 분석 사용

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

AMP for Networks 을(를) 사용하는 경우 악성 코드 라이선스가 필요합니다.

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Files(**파일**)** > **Network File Trajectory(**네트워크 파일 경로**)**을(를) 선택합니다.

팁 Context Explorer, 대시보드 또는 파일 정보가 포함된 이벤트 보기에서도 파일의 분석 경로에 액세스할 수 있습니다.

단계 **2** 목록에서 **File SHA 256** 링크를 클릭합니다.

단계 **3** 원하는 경우, 전체 SHA-256 해시 값, 호스트 IP 주소 또는 추적할 파일의 파일 이름을 검색 필드에 입력하고 Enter 키를 누릅니다.

팁 일치하는 결과가 하나뿐이면 해당 파일의 Network File Trajectory(네트워크 파일 분석 경로) 페이지가 나타납니다.

단계 **4** Summary Information(요약 정보) 섹션에서 다음을 수행할 수 있습니다.

- 파일을 파일 목록에 추가 - 정상 목록 또는 맞춤형 탐지 목록에 파일을 추가 또는 제거하려면 수정( )을 클릭합니다.
- 파일 다운로드 - 파일을 다운로드하려면 다운로드( )을 클릭하고 메시지가 표시되면 파일을 다운로드하려 한다고 확인합니다. 파일을 다운로드할 수 없는 경우에는 이 다운로드 파일이 흐리게 표시됩니다.
- 보고 - 동적 분석 요약 보고서를 보려면 위협 점수를 클릭합니다.
- 동적 분석을 위해 제출 - 동적 분석을 위해 파일을 제출하려면 **AMP** 클라우드를 클릭합니다. 파일을 제출할 수 없거나 AMP 클라우드에 연결할 수 없는 경우 이 AMP 클라우드가 흐리게 표시됩니다.
- 아카이브 내용 보기 - 아카이브 파일의 내용에 대한 정보를 보려면 보기 ( )을 클릭합니다.
- 파일 구성 보기 - 파일의 구성을 보려면 파일 목록을 클릭합니다. 시스템이 파일 구성 보고서를 생성하지 않은 경우, 이 파일 목록이 흐리게 표시됩니다.
- 위협 점수가 동일한 캡처된 파일 보기 - 해당 위협 점수의 모든 캡처 파일을 보려면 위협 점수 링크를 클릭합니다.

참고 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

단계 **5** 경로 분석 맵에서 다음을 수행할 수 있습니다.

- 첫 번째 인스턴스 찾기 - IP 주소와 관련하여 파일 이벤트가 처음 발생한 때를 찾으려면 IP 주소를 클릭합니다. 그러면 해당 데이터 포인트 경로는 물론 첫 번째 파일 이벤트와 관련된 중간 파일 이벤트 및 IP 주소도 강조 표시됩니다. Events(이벤트) 테이블의 해당 이벤트도 강조 표시됩니다. 해당 데이터 포인트가 현재 보이지 않는 경우, 맵이 해당 데이터 포인트로 스크롤됩니다.
- 추적 - 데이터 포인트를 클릭하여 선택한 데이터 포인트와 관련된 모든 데이터 포인트를 포함하는 경로를 강조 표시하여 네트워크에서 파일의 진행 상황을 추적할 수 있습니다.
- 숨겨진 이벤트 보기 - File Summary(파일 요약) 이벤트 보기에 표시되지 않은 모든 이벤트를 보려면 화살표를 클릭합니다.
- 일치하는 파일 이벤트 보기 - 일치하는 파일 이벤트 위에 마우스 포인터를 올려놓으면 해당 이벤트의 요약 정보를 볼 수 있습니다. 이벤트 요약 정보 링크를 클릭할 경우, File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지가 파일 형식을 기반으로 제한된 모든 추가 이벤트와 함께 새 창에 나타납니다. File Summary(파일 요약) 이벤트 보기가 새 창에서 열리며, 클릭한 기준에 일치하는 모든 파일 이벤트가 표시됩니다.

단계 **6** Events(이벤트) 테이블에서 다음을 수행할 수 있습니다.

- 강조 표시 - 맵에서 데이터 포인트를 강조 표시하려면 테이블 행을 선택합니다. 선택한 파일 이벤트가 현재 보이지 않는 경우 해당 이벤트를 표시하도록 맵이 스크롤됩니다.

- 정렬 - 오름차순 또는 내림차순으로 이벤트를 정렬하려면 열 머리글을 클릭합니다.

AMP for Endpoints 콘솔의 이벤트 데이터 작업

조직이 AMP for Endpoints를 구축한 경우, AMP for Endpoints 콘솔에서 AMP for Endpoints 악성코드 이벤트 데이터를 볼 수 있으며, 해당 애플리케이션의 전역 네트워크 파일 분석 경로 도구를 사용하거나.

팁 AMP for Endpoints 및 콘솔 사용 방법은 콘솔의 온라인 도움말 또는 사용 가능한 기타 설명서를 참조하십시오. https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html

Firepower Management Center에서 AMP for Endpoints 콘솔에 액세스하려면 다음 중 하나를 수행하십시오.

시작하기 전에

- AMP for Endpoints에 대한 연결이 구성되어야 하며(Firepower와 AMP for Endpoints 통합, 1898 페이지 참조) Firepower Management Center이 AMP 클라우드에 연결할 수 있어야 합니다.
- AMP for Endpoints 자격 증명이 필요합니다.
- 이 작업을 수행하려면 관리자 사용자여야 합니다.
- FMC의 악성코드 이벤트에서 피벗하려는 경우, AMP for Endpoints 상황별 크로스 실행 옵션이 적절히 활성화되어 있어야 합니다. 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지의 항목을 참조하십시오.

프로시저

단계 **1** 방법 1:

a) **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.
b) 테이블에서 클라우드 이름을 클릭합니다.

단계 **2** 방법 2:

a) **Analysis(**분석**) > Files(**파일**)**아래 테이블에서 악성코드 이벤트로 이동합니다.
b) 파일 SHA를 마우스 오른쪽 버튼으로 클릭하고 AMP for Endpoints 옵션을 선택합니다.

파일, 악성코드 이벤트 및 네트워크 파일 경로 분석 기록

기능	버전	세부 사항
동적 분석을 위해 파일 사전 분류 개선	6.7	추가 평가를 통해 동적 분석을 위해 불필요한 파일 전송이 방지됩니다. 이 평가를 기반으로 클라우드로 전송되지 않은 파일에 대한 새로운 동적 분석이 **Rejected for Analysis(**분석을 위해 거부**)** 상태가 됩니다. 수정된 화면: Analysis(분석) > Captured Files(캡처된 파일) > Table View of Captured Files(캡처된 파일 테이블 보기) 지원되는 플랫폼: FMC
시스템 로그의 연결 이벤트 통합 식별자	6.4.0.4	다음 시스템 로그 필드는 연결 이벤트를 전체적으로 고유하게 식별하며, 파일 및 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)의 경우에는 시스템 로그에 표시됩니다.
시스템 로그를 통해 파일 및 악성코드 이벤트를 전송하는 기능	6.4	이 장의 필드 설명은 시스템 로그 메시지에 포함된 필드를 지정합니다. 구성 정보는 파일 및 악성코드 이벤트에 대한 시스템 로그 설정 위치, 2764 페이지의 내용을 참조하십시오.

124 장

호스트 프로파일 사용

다음 주제에서는 호스트 프로파일을 사용하는 방법에 설명합니다.

- 호스트 프로파일에 대한 요구 사항 및 사전 요건, 3001 페이지
- 호스트 프로파일, 3002 페이지
- 호스트 프로파일의 기본 호스트 정보, 3004 페이지
- 호스트 프로파일의 운영 체제, 3006 페이지
- 호스트 프로파일의 서버, 3010 페이지
- 호스트 프로파일의 웹 애플리케이션, 3015 페이지
- 호스트 프로파일의 호스트 프로토콜, 3017 페이지
- 호스트 프로파일의 보안 침해 지표, 3018 페이지
- 호스트 프로파일의 VLAN 태그, 3018 페이지
- 호스트 프로파일의 사용자 기록, 3019 페이지
- 호스트 프로파일의 호스트 속성, 3019 페이지
- 호스트 프로파일의 화이트 목록 위반, 3023 페이지
- 호스트 프로파일의 악성코드 탐지, 3024 페이지
- 호스트 프로파일의 취약성, 3025 페이지
- 호스트 프로파일의 스캔 결과, 3028 페이지
- 호스트 프로파일 기록, 3029 페이지

호스트 프로파일에 대한 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

- 보안 분석가

호스트 프로파일

호스트 프로파일은 시스템이 단일 호스트에 대해 수집한 모든 정보를 완벽하게 보여줍니다. 호스트 프로파일을 액세스하려면

- 아무 네트워크 맵 보기에서 해당 프로파일로 이동합니다.
- 모니터링되는 네트워크 상의 호스트 IP 주소를 포함하는 아무 이벤트 보기에서 해당 프로파일로 이동합니다.

호스트 프로파일은 탐지한 호스트 또는 디바이스에 대한 (호스트 이름 또는 MAC 주소 같은) 기본 정보를 제공합니다. 라이선스 및 시스템 설정에 따라, 호스트 프로파일은 다음 정보를 제공하기도 합니다.

- 호스트에서 실행 중인 운영체제
- 호스트에서 실행 중인 서버
- 호스트에서 실행 중인 클라이언트 및 웹 애플리케이션
- 호스트에서 실행 중인 프로토콜
- 호스트의 보안 침해 지표(IOC) 태그
- 호스트의 VLAN 태그
- 네트워크에서의 최근 24시간 동안의 사용자 활동
- 호스트와 관련된 규정준수 화이트리스트 위반
- 호스트에 대한 가장 최근의 악성코드 이벤트
- 호스트와 관련된 취약성
- 호스트에 대한 Nmap 스캔 결과

호스트 속성은 프로파일에도 나열됩니다. 호스트 속성을 사용하면 네트워크 환경에서 중요한 방법으로 호스트를 분류할 수 있습니다. 예를 들어, 다음이 가능합니다.

- 호스트가 위치한 건물을 나타내는 호스트 속성을 할당합니다.
- 호스트 중요도 특성을 사용하여 특정 호스트의 비즈니스 중요도를 할당하고 호스트 중요도를 기반으로 상관관계 정책 및 알림을 맞춤화합니다.

호스트 프로파일에서 해당 호스트에 적용된 기존 호스트 속성을 보고 호스트 속성 값을 수정합니다.

적응형 프로파일을(를) 수동 침입 방지 배포의 일부로 사용하는 경우, 시스템이 트래픽을 수정하는 방식을 호스트와 서버 및 호스트를 실행하는 클라이언트의 운영체제에 가장 적합하게 조정할 수 있습니다.

선택적으로, 호스트 프로파일에서 Nmap 스캔을 수행하여 호스트 프로파일의 서버 및 운영체제 정보를 보강할 수도 있습니다. Nmap 스캐너는 호스트를 적극적으로 조사하여 호스트에서 실행 중인 운영체제와 서버에 대한 정보를 가져옵니다. 스캔 결과는 호스트에 대한 운영체제 및 서버 ID의 목록에 추가됩니다.

관련 항목

호스트 프로파일 보기, 3003 페이지

호스트 프로파일 제한

사용할 수 없는 호스트

네트워크의 모든 호스트에 대해 호스트 프로파일을 이용할 수 있는 것은 아닙니다. 대표적인 가능한 원인:

- 시간 초과되어 호스트가 네트워크 맵에서 삭제됨
- 호스트 제한에 도달함
- 호스트가 네트워크 검색 정책에서 모니터링하지 않는 네트워크 세그먼트에 상주함

사용할 수 없는 정보

호스트 프로파일에 표시되는 정보는 호스트 유형 및 호스트에 대해 사용 가능한 정보에 따라 달라질 수 있습니다.

예를 들면 다음과 같습니다.

- 시스템에서 비 IP 기반 프로토콜(예: STP, SNAP, IPX)을 탐지한 경우, 호스트는 네트워크 맵에 MAC 호스트로 추가되는데 이 경우 IP 호스트에 비해 사용 가능한 정보가 훨씬 적습니다.
- 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지의 내용을 참조하십시오.

(VRF를 실행하는 구축**)** 단일 **IP** 주소가 여러 호스트를 나타낼 수 있습니다**.**

VRF를 실행하는 디바이스에서 호스트를 보고했다면, 단일 IP 주소가 실제로는 여러 호스트를 나타낼 수 있습니다. VRF는 중복 IP 주소가 있는 여러 네트워크를 모니터링할 수 있으므로, 동일한 IP 주소가 서로 다른 네트워크에 존재할 수 있습니다.

호스트 프로파일 보기

프로시저

다음 2가지 옵션을 사용할 수 있습니다.

- 네트워크 맵에서 프로파일을 보려는 호스트의 IP 주소로 드릴다운합니다.

- 이벤트 보기에서 프로필을 보려는 호스트의 IP 주소 옆에 있는 **Host Profile(**호스트 프로파일**)** 또는 **Compromised Host(**손상된 호스트**)**를 클릭합니다.

호스트 프로파일의 기본 호스트 정보

각 호스트 프로파일은 탐지된 호스트 또는 기타 디바이스에 대한 기본 정보를 제공합니다.

다음은 각각의 기본 호스트 프로파일 필드에 대한 설명입니다.

Domain(도메인**)**

호스트와 연결된 도메인.

IP 주소

호스트와 연결된 모든 IP 주소(IPv4 및 IPv6). 시스템은 호스트와 연결된 IP 주소를 탐지하며, 지원되는 경우 동일한 호스트에 의해 사용되는 여러 IP 주소를 그룹화합니다. IPv6 호스트에는 흔히 2개 이상의 IPv6 주소(로컬 전용 및 전역 라우팅 가능)가 있으며 IPv4 주소도 있을 수 있습니다. IPv4 전용 호스트에는 여러 개의 IPv4 주소가 있을 수 있습니다.

호스트 프로파일에는 해당 호스트와 연결된 모든 탐지된 IP 주소가 나열됩니다. 사용 가능한 경우, 라우팅 가능한 호스트 IP 주소에는 해당 주소에 연결된 지오로케이션 데이터를 나타내는 국가 코드 및 플래그 아이콘도 포함될 수 있습니다.

기본적으로 처음 3개 주소만 표시됩니다. 호스트의 모든 주소를 표시하려면 **show all(**모두 표시**)**을 클릭하십시오.

호스트 이름

알려진 경우 호스트의 정규화된 도메인 이름.

NetBIOS Name(NetBIOS 이름**)**

사용 가능한 경우 호스트의 NetBIOS 이름. Microsoft Windows 호스트는 물론 Macintosh, Linux 또는 NetBIOS를 사용하도록 구성된 기타 플랫폼은 NetBIOS 이름을 가질 수 있습니다. 예를 들어 Samba 서버로 구성된 Linux 호스트는 NetBIOS 이름을 가질 수 있습니다.

디바이스**(**홉**)**

다음 중 하나에 해당합니다.

- 네트워크 검색 정책에 정의된 대로 호스트가 상주하는 네트워크에 대한 보고 디바이스 또는
- 호스트를 네트워크 맵에 추가한 NetFlow 데이터를 처리한 디바이스

디바이스 이름 뒤에 호스트를 탐지한 디바이스와 호스트 자체 간 네트워크 홉의 수가 괄호로 표시됩니다. 여러 디바이스가 호스트를 볼 수 있는 경우 보고 디바이스는 굵은 글꼴로 표시됩니다.

이 필드가 비어 있는 경우는 다음 중 하나입니다.

- 네트워크 검색 정책에 정의된 대로, 호스트 상주 네트워크를 명시적으로 모니터링하지 않는 디바이스에 의해 호스트가 네트워크 맵에 추가되었습니다.
- 호스트가 호스트 입력 기능으로 추가되었으며 Firepower System에 의해 탐지되지 않았습니다.

MAC 주소(TTL)

호스트의 탐지된 MAC 주소 및 관련 NIC 공급업체, NIC의 하드웨어 공급업체와 현재 TTL(time-to-live) 값은 괄호로 표시됩니다.

여러 디바이스가 호스트를 탐지한 경우, 이를 보고한 디바이스와 상관없이 Firepower Management Center에서는 호스트에 연결된 모든 MAC 주소 및 TTL 값을 표시합니다.

MAC 주소가 굵은 글꼴로 표시된 경우, MAC 주소는 호스트의 실제/참/기본 MAC 주소이며, ARP 및 DHCP 트래픽을 통한 탐지에 의해 IP 주소에 확실히 연결됩니다.

굵은 글꼴로 표시되지 않은 MAC 주소는 호스트의 IP 주소에 확실히 연결될 수 없는 보조 주소입니다. 예를 들어 Firepower 디바이스는 자신의 네트워크 세그먼트에 있는 호스트의 MAC 주소만 획득할 수 있으므로 Firepower 디바이스가 직접 연결되지 않은 네트워크 세그먼트에서 트래픽이 시작되는 경우, 관찰된 MAC 주소(즉, 라우터 MAC 주소)는 호스트의 보조 MAC 주소로 표시됩니다.

Host Type(호스트 유형)

호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 또는 로드 밸런서 등 시스템이 탐지한 디바이스의 유형.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.
- 시스템이 모바일 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.
- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 User-Agent(사용자 에이전트) 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크 디바이스 또는 모바일 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

최종 확인

호스트의 IP 주소가 마지막으로 탐지된 날짜 및 시간.

Current User(현재 사용자**)**

가장 최근에 이 호스트에 로그인한 사용자.

기존의 현재 사용자가 권한 있는 사용자가 아닌 경우, 호스트에 로그인한 권한 없는 사용자는 호스트에서 현재 사용자로만 등록됩니다.

보기

연결, 검색, 악성코드 및 침입 이벤트 데이터의 보기에 대한 링크. 해당 이벤트 유형에 대해 기본 워크플로를 사용하며 호스트와 관련된 이벤트를 표시하도록 제한됩니다. 가능한 경우 이러한 이벤트에는 호스트와 연결된 모든 IP 주소가 포함됩니다.

호스트 프로파일의 운영 체제

시스템은 호스트에 의해 생성되는 트래픽에서 네트워크 및 애플리케이션 스택을 분석하거나 사용자 에이전트에 의해 보고된 호스트 데이터를 분석하여 호스트에서 실행되는 운영 체제의 ID를 수동적으로 탐지합니다. 시스템은 또한 Nmap 스캐너 또는 호스트 입력 기능을 통해 가져온 애플리케이션 데이터 등의 다른 소스에서 운영 체제 정보를 취합합니다. 사용할 ID를 결정할 때 시스템은 각 ID 소스에 할당된 우선순위를 고려합니다. 기본적으로 사용자 입력의 우선순위가 가장 높고, 그다음은 애플리케이션 또는 스캐너 소스, 그다음은 검색된 ID입니다.

트래픽 및 기타 ID 소스는 더 구체적인 ID에 대해 충분한 정보를 제공하지 않으므로 때때로 시스템은 특정한 운영 체제보다는 일반적인 운영 체제 정의를 제공합니다. 시스템은 가능한 한 가장 자세한 정의를 사용하기 위해 여러 소스의 정보를 취합합니다.

운영 체제는 호스트의 취약성 목록과 호스트를 대상으로 하는 이벤트에 대한 이벤트 영향 상관 관계에 영향을 미치기 때문에 더 구체적인 운영 체제 정보를 수동으로 제공하는 것이 좋습니다. 또한 운영 체제에 수정(예: 서비스 팩 및 업데이트)이 적용되었음을 나타낼 수 있고, 수정에 의해 해결된 취약성을 무효화할 수 있습니다.

예를 들어 시스템에서 호스트의 운영 체제를 Microsoft Windows 2003으로 식별했지만 실제로 호스트에서는 Microsoft Windows XP Professional 서비스 팩 2가 실행되고 있음을 알고 있는 경우, 운영 체제 ID를 올바르게 설정할 수 있습니다. 운영 체제 ID를 더 구체적으로 설정하면 호스트의 취약성 목록이 세부적으로 조정되므로, 해당 호스트에 대한 영향 상관 관계가 더 구체적이고 정확해집니다.

시스템이 호스트의 운영 체제 정보를 탐지하고 그 정보가 활성 소스에 의해 제공된 현재 운영 체제 ID와 충돌하는 경우, ID 충돌이 발생합니다. ID 충돌이 발생하면 시스템에서는 취약성과 영향 상관 관계에 두 ID를 모두 사용합니다.

NetFlow 엑스포터가 모니터링하는 호스트의 네트워크 맵에 검색 데이터를 추가하도록 네트워크 검색 정책을 구성할 수 있습니다. 하지만 호스트 입력 기능을 사용하여 운영 체제 ID를 설정하지 않는 한 사용할 수 있는 이러한 호스트의 운영 체제 데이터는 없습니다.

활성화된 네트워크 검색 정책의 규정준수 화이트리스트를 위반하는 운영체제가 호스트에서 실행되고 있는 경우, Firepower Management Center에서는 해당 운영체제 정보를 화이트리스트 **Violation(**위반**)**으로 표시합니다. 또한 탈옥 모바일 디바이스가 활성 화이트리스트를 위반하면 디바이스의 운영 체제 옆에 아이콘이 나타납니다.

호스트의 운영 체제 ID에 대해 맞춤형 표시 문자열을 설정할 수 있습니다. 그러면 해당 표시 문자열이 호스트 프로파일에 사용됩니다.

참고 호스트의 운영체제 정보를 변경하면 규정준수 화이트리스트 준수도 변경될 수 있습니다.

네트워크 디바이스의 호스트 프로파일에서 Operating Systems 섹션의 레이블이 Systems로 변경되며 추가 Hardware 열이 나타납니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

다음은 호스트 프로파일에 표시되는 운영 체제 정보 필드에 대한 설명입니다.

Hardware(하드웨어)

모바일 디바이스용 하드웨어 플랫폼.

OS Vendor/Vendor

운영 체제의 공급업체입니다.

OS Product/Product

다음 값 중 하나:

- 모든 소스에서 수집한 ID 데이터에 기반할 때 호스트에서 실행되고 있을 가능성이 가장 높다고 판단되는 운영 체제
- 시스템이 아직 운영 체제를 식별하지 못했고 사용 가능한 다른 ID 데이터가 없는 경우 `Pending`
- 시스템이 운영 체제를 식별할 수 없고 운영 체제에 대해 사용 가능한 다른 ID 데이터가 없는 경우 `unknown`

참고 호스트의 운영 체제를 시스템이 탐지할 수 없는 경우, 호스트 운영체제 식별, 2397 페이지를 참조하십시오.

OS Version/Version

운영 체제 버전. 호스트가 탈옥 모바일 디바이스인 경우, 버전 뒤에 괄호로 `Jailbroken`이 표시됩니다.

소스

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name

- 스캐너: scanner_type (Nmap 또는 기타 스캐너)
- Firepower

시스템에서는 운영 체제의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

운영 체제 ID 보기

호스트에 대해 추가되거나 검색된 특정 운영 체제 ID를 볼 수 있습니다. 시스템은 호스트에 대한 현재 ID를 확인하기 위해 소스 우선순위를 사용합니다. ID 목록에서 현재 ID는 굵은 글꼴로 강조 표시됩니다.

View(보기**)**는 호스트에 여러 운영체제 ID가 존재하는 경우에만 사용할 수 있습니다.

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 또는 **Operating System Conflicts(**운영 체제 충돌**)** 섹션에서 **View(**보기**)**를 클릭합니다.

단계 **2** 호스트 프로파일의 운영 체제, 3006 페이지에 설명된 정보를 봅니다.

단계 **3** 원하는 경우, 운영체제 ID 옆에 있는 삭제( )를 클릭합니다.

/firepower/fmc/fmc_config_guide/discovery-host-profiles/t_editing_server_identities.xml

참고 Cisco가 탐지한 운영 체제 ID는 삭제할 수 없습니다.

시스템은 Operating System Identity Information(운영 체제 ID 정보) 팝업 창에서 ID를 삭제하고, 해당되는 경우, 호스트 프로파일에서 운영 체제의 현재 ID를 업데이트합니다.

현재 운영 체제 ID 설정

Firepower System 웹 인터페이스를 사용하여 호스트의 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관 관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다. 그러나 사용자가 운영 체제를 수정한 후 시스템에서 호스트에 대해 충돌하는 운영 체제 ID를 탐지하면 운영 체제 충돌이 발생합니다. 이 경우 사용자가 충돌을 해결할 때까지 두 운영 체제 모두 현재 운영 체제로 간주됩니다.

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션에서 **Edit(**수정**)**를 클릭합니다.

단계 **2** 다음과 같은 몇 가지 옵션이 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition(OS** 정의**)** 드롭다운 목록에서 **Current Definition(**현재 정의**)**을 선택하고 6단계로 건너뜁니다.

- **OS Definition(OS** 정의**)** 드롭다운 목록에서 현재 운영 체제 ID에 대한 변형을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 **User-Defined(**사용자 정의**)**를 선택하고 3단계를 계속 진행합니다.

단계 **3** 원하는 경우, **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**, **Product String(**제품 문자열**)** 및 **Version String(**버전 문자열**)** 필드에 표시할 맞춤형 문자열을 수정합니다.

단계 **4** 원하는 경우, 다른 공급업체의 운영 체제로 변경하려면 **Product(**제품**)** 드롭다운 목록에서 **Vendor(**공급업체**)**를 선택합니다.

단계 **5** 원하는 경우, 운영 체제 제품 릴리스 수준을 구성하려면 **Major(**메이저**)**, **Minor(**마이너**)**, **Revision(**수정**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록에서 선택합니다.

단계 **6** 원하는 경우, 운영 체제의 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭합니다.

단계 **7** 드롭다운 목록에서 해당 수정을 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **8** 원하는 경우, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록을 사용하여 관련 패치와 확장을 추가합니다.

단계 **9** **Finish(**종료**)**를 클릭합니다.

관련 항목

운영 체제 ID 충돌, 3009 페이지

운영 체제 ID 충돌

현재 ID가 스캐너, 애플리케이션, 사용자 등의 활성 소스에 의해 제공된 경우, 시스템이 탐지한 새 ID가 현재 ID와 충돌하면 운영 체제 ID 충돌이 발생합니다.

충돌하는 운영 체제 ID 목록은 호스트 프로파일에서 굵은 글꼴로 표시됩니다.

시스템 웹 인터페이스를 통해 ID 충돌을 해결하고 호스트의 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관 관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다.

관련 항목

네트워크 검색 ID 충돌 확인 설정, 2553 페이지

충돌하는 운영 체제 ID를 현재 ID로 만들기

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션으로 이동합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트의 운영 체제로 설정하려는 운영 체제 ID 옆에 있는 **Make Current(**현재 **ID**로 만들기**)**를 클릭합니다.
- 현재 ID로 지정하지 않으려는 ID가 활성 소스에서 온 것이면 원하지 않는 ID를 삭제합니다.

운영 체제 **ID** 충돌 해결

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션에서 **Resolve(**해결**)**를 클릭합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition(OS** 정의**)** 드롭다운 목록에서 **Current Definition(**현재 정의**)**을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 충돌하는 운영 체제 ID 중 하나의 변형을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 **User-Defined(**사용자 정의**)**를 선택하고 3단계를 계속 진행합니다.

단계 **3** 원하는 경우, **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**, **Product String(**제품 문자열**)** 및 **Version String(**버전 문자열**)** 필드에 표시할 맞춤형 문자열을 입력합니다.

단계 **4** 원하는 경우, 다른 공급업체의 운영 체제로 변경하려면 **Product(**제품**)** 드롭다운 목록에서 **Vendor(**공급업체**)**를 선택합니다.

단계 **5** 원하는 경우, 운영 체제 제품 릴리스 수준을 구성하려면 **Major(**메이저**)**, **Minor(**마이너**)**, **Revision(**수정**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록에서 선택합니다.

단계 **6** 원하는 경우, 운영 체제의 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭합니다.

단계 **7** 적용한 수정을 수정 목록에 추가합니다.

단계 **8** **Finish(**종료**)**를 클릭합니다.

관련 항목

네트워크 검색 ID 충돌 확인 설정, 2553 페이지

호스트 프로파일의 서버

호스트 프로파일의 서버 섹션에는 모니터링되는 네트워크의 호스트에서 탐지되거나 내보낸 NetFlow 레코드에서 추가되거나 스캐너 또는 호스트 입력 기능 같은 활성 소스를 통해 추가된 서버가 나열됩니다.

목록은 호스트당 최대 100개의 서버를 포함할 수 있습니다. 이 제한에 도달하면 호스트에서 서버를 삭제하거나 서버가 시간 초과될 때까지 소스의 새 서버 정보(능동이든 수동이든)가 폐기됩니다.

Nmap을 사용하여 호스트를 스캔하면 Nmap은 열린 TCP 포트에서 실행되는, 전에 탐지되지 않은 서버의 결과를 Servers(서버) 목록에 추가합니다. Nmap 스캔을 수행하거나 Nmap 결과를 가져오는 경우, 호스트 프로파일에 Scan Results(스캔 결과) 섹션도 나타나며, 여기에 Nmap 스캔에 의해 호스트에서 탐지된 서버 정보가 나열됩니다. 또한 네트워크 맵에서 호스트가 삭제되면 호스트에 대한 해당 서버의 Nmap 스캔 결과가 삭제됩니다.

참고 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지의 내용을 참조하십시오.

호스트 프로파일의 서버 작업 프로세스는 프로파일에 액세스하는 방법에 따라 달라집니다.

- 네트워크 맵을 통해 드릴다운하여 호스트 프로파일에 액세스하는 경우, 굵은 글꼴로 강조 표시된 서버 이름과 함께 해당 서버에 대한 세부사항이 나타납니다. 호스트의 다른 서버에 대한 세부사항을 보려면 해당 서버 이름 옆에 있는 보기 ( )를 클릭합니다.
- 다른 방법으로 호스트 프로필에 액세스하는 경우, Servers(서버) 섹션을 확장하고 세부 사항을 보려는 서버 옆에 있는 보기 ( )를 클릭합니다.

참고 활성화된 상관관계 정책의 규정준수 화이트리스트를 위반하는 서버가 호스트에서 실행되고 있는 경우, Firepower Management Center에서는 규정을 준수하지 않는 서버를 화이트리스트 **Violation(위반)**으로 표시합니다.

다음은 Servers(서버) 목록의 열에 대한 설명입니다.

프로토콜

서버가 사용하는 프로토콜의 이름.

Port(포트)

서버가 실행하는 포트.

애플리케이션 프로토콜

다음 중 하나에 해당합니다.

- 애플리케이션 프로토콜의 이름
- 여러 이유 중 하나 때문에 시스템이 애플리케이션 프로토콜을 긍정적으로 또는 부정적으로 식별할 수 없는 경우 `pending`

- 알려진 애플리케이션 프로토콜 지문을 기반으로 시스템이 애플리케이션 프로토콜을 식별할 수 없거나 서버 추가 없이 포트 정보와 함께 취약성을 추가하여 호스트 입력을 통해 해당 서버가 추가된 경우 `unknown`

마우스를 애플리케이션 프로토콜 이름 위로 이동하면 태그가 표시됩니다.

Vendor and Version

Firepower System, Nmap 또는 다른 활성 소스에 의해 식별되었거나 호스트 입력 기능을 통해 수집된 공급업체 및 버전. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

관련 항목

호스트 제한 및 검색 이벤트 로깅, 2443 페이지
NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지
애플리케이션 탐지기 기초, 2440 페이지

호스트 프로파일의 서버 상세정보

Firepower Management Center는 서버당 최대 16개의 수동 탐지 ID를 나열합니다. 수동 탐지 소스에는 네트워크 검색 데이터 및 NetFlow 레코드가 포함됩니다. 시스템이 서버에 대해 여러 공급업체 또는 버전을 탐지하는 경우 해당 서버는 여러 수동 ID를 가질 수 있습니다. 예를 들어 웹 서버가 서버 소프트웨어와 동일한 버전을 실행하지 않는 경우, 매니지드 디바이스와 웹 서버 팜 간 로드 밸런서를 사용하면 시스템은 HTTP에 대해 여러 수동 ID를 식별하게 될 수 있습니다. Firepower Management Center는 사용자 입력, 스캐너 또는 기타 애플리케이션 등 활성 소스에서 오는 서버 ID의 수를 제한하지 않습니다.

현재 ID는 Firepower Management Center에서 굵은 글꼴로 표시됩니다. 시스템은 호스트에 취약성을 할당하고, 영향 평가를 수행하고, 호스트 프로파일 자격 및 규정준수 화이트리스트에 대해 작성된 상관관계 규칙을 평가하는 등 여러 용도로 서버의 현재 ID를 사용합니다.

서버 세부사항에는 선택한 서버에 대해 알려진 업데이트된 하위 서버 정보도 표시될 수 있습니다.

서버 세부사항에는 서버 배너도 표시될 수 있습니다. 이 배너는 호스트 프로파일에서 서버를 볼 때 서버 세부사항 아래에 표시됩니다. 서버 배너는 서버 식별에 도움이 될 수 있는, 서버에 대한 추가 정보를 제공합니다. 공격자가 고의로 서버 배너 문자열을 변경하면 시스템이 서버를 식별하지 못하거나 잘못된 서버를 탐지할 수 있습니다. 서버 배너에는 서버에 대해 탐지된 첫 번째 패킷의 처음 256바이트가 표시됩니다. 이러한 정보는 시스템에서 서버를 처음 탐지할 때 한 번만 수집됩니다. 배너 내용은 왼쪽에는 16진수로, 오른쪽에는 ASCII로 표시되어 두 열에 나타납니다.

참고 서버 배너를 보려면 네트워크 검색 정책에서 **Capture Banners(**배너 캡처**)** 확인란을 활성화해야 합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

호스트 프로파일의 서버 세부정보 섹션에는 다음 정보가 포함됩니다.

프로토콜

서버가 사용하는 프로토콜의 이름.

Port(포트)

서버가 실행하는 포트.

Hits(히트)

Firepower System 매니지드 디바이스 또는 Nmp 스캐너에 의해 서버가 탐지된 횟수. 호스트 입력을 통해 가져온 서버에 대한 트래픽을 시스템에서 탐지하지 못하면 해당 서버의 히트 수는 0입니다.

Last Used(최종 사용)

서버가 마지막으로 탐지된 시간 및 날짜. 시스템이 서버에 대해 새 트래픽을 탐지하지 못하면 호스트 입력 데이터의 마지막 사용 시간은 초기 데이터 가져오기 시간을 반영합니다. 호스트 입력 기능을 통해 가져온 스캐너 및 애플리케이션 데이터는 Firepower Management Center 구성에 따라 시간 초과되지만 FMC 웹 인터페이스를 통한 사용자 입력은 시간 초과되지 않습니다.

애플리케이션 프로토콜

알려진 경우, 서버에서 사용하는 애플리케이션 프로토콜의 이름.

Vendor(벤더)

서버 공급업체. 공급업체가 알려지지 않은 경우 이 필드는 나타나지 않습니다.

버전

서버 버전. 버전이 알려지지 않은 경우 이 필드는 나타나지 않습니다.

소스

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type (Nmap 또는 기타 스캐너)
- Firepower System에서 탐지된 어플라이언스의 `Firepower`, `Firepower Port Match` 또는 `Firepower Pattern Match`
- NetFlow 레코드에서 네트워크 맵에 추가된 서버의 `NetFlow`

시스템에서는 서버의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

관련 항목

애플리케이션 및 운영 체제에 대한 현재 ID, 2379 페이지

서버 상세정보 보기

프로시저

호스트 프로파일의 **Servers(**서버**)** 섹션 옆에 있는 보기 ( )을 클릭합니다.

서버 **ID** 수정

호스트의 서버에 대한 ID 설정을 수동으로 업데이트하고, 수정으로 해결된 취약성을 제거하도록 호스트에 적용한 수정을 구성할 수 있습니다. 서버 ID를 삭제할 수도 있습니다.

ID를 삭제해도 서버는 삭제되지 않습니다(유일한 ID를 삭제하는 경우에도). ID를 삭제하면 Server Detail(서버 세부정보) 팝업 창에서 ID가 제거되며, 해당되는 경우 호스트 프로파일에서 서버의 현재 ID가 업데이트됩니다.

Cisco가 관리하는 디바이스에 의해 추가된 서버 ID는 수정 또는 삭제할 수 없습니다.

프로시저

단계 **1** 호스트 프로파일의 **Servers(**서버**)** 섹션으로 이동합니다.

단계 **2** Server Details(서버 세부정보) 팝업 창을 열려면 **View(**보기**)**를 클릭합니다.

단계 **3** 서버 ID를 삭제하려면 제거할 서버 ID 옆에 있는 삭제( )을 클릭합니다.

단계 **4** 서버 ID를 수정하려면 서버 목록에서 서버 옆에 있는 수정( )을 클릭합니다.

단계 **5** 다음 2가지 옵션을 사용할 수 있습니다.

- **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 현재 정의를 선택합니다.
- **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 서버 유형을 선택합니다.

단계 **6** 원하는 경우, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type(**서버 유형으로 제한**)** 확인란을 선택합니다.

단계 **7** 원하는 경우, 서버 이름과 버전을 맞춤 설정하려면 **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**과 **Version String(**버전 문자열**)**을 입력합니다.

단계 **8** **Product Mappings(**제품 매핑**)** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예제**:**

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **9** 서버 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭하고 해당 서버에 적용하려는 패치를 수정 목록에 추가합니다.

단계 **10** **Finish(**종료**)**를 클릭합니다.

서버 ID 충돌 해결

애플리케이션이나 스캐너 같은 활성 소스가 서버의 ID 데이터를 호스트에 추가한 후 시스템이 해당 포트에서 서버 ID가 충돌함을 나타내는 트래픽을 탐지하면 서버 ID 충돌이 발생합니다.

프로시저

단계 **1** 호스트 프로파일에서 **Servers(**서버**)** 섹션으로 이동합니다.

단계 **2** 서버 옆에 있는 해결 아이콘을 클릭합니다.

단계 **3** **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 서버 유형을 선택합니다.

단계 **4** 원하는 경우, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type(**서버 유형으로 제한**)** 확인란을 선택합니다.

단계 **5** 원하는 경우, 서버 이름과 버전을 맞춤 설정하려면 **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**과 **Version String(**버전 문자열**)**을 입력합니다.

단계 **6** **Product Mappings(**제품 매핑**)** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예제**:**

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **7** 서버 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭하고 해당 서버에 적용하려는 패치를 수정 목록에 추가합니다.

단계 **8** **Finish(**종료**)**를 클릭합니다.

관련 항목

네트워크 검색 ID 충돌 확인 설정, 2553 페이지

호스트 프로파일의 웹 애플리케이션

호스트 프로파일의 Web Application(웹 애플리케이션) 섹션에는 네트워크의 호스트에서 실행 중이라고 시스템이 식별하는 클라이언트 및 웹 애플리케이션이 표시됩니다. 시스템은 수동 탐지 소스와 능동 탐지 소스의 클라이언트 및 웹 애플리케이션 정보를 식별할 수 있지만 NetFlow 레코드에서 추가된 호스트에 대한 정보는 제한됩니다.

이 섹션의 세부 정보는 호스트에서 탐지되는 애플리케이션의 제품 및 버전, 사용 가능한 클라이언트 또는 웹 애플리케이션 정보, 그리고 애플리케이션 사용이 마지막으로 탐지된 시간을 표시합니다.

이 섹션은 호스트에서 실행 중인 클라이언트를 최대 16개 나열합니다. 이 한계에 도달하면 사용자가 호스트에서 클라이언트 애플리케이션을 삭제하거나 비활성(클라이언트 시간 초과)으로 인해 시스템

이 호스트 프로파일에서 클라이언트를 삭제할 때까지 능동 및 수동 소스의 새 클라이언트 정보가 삭제됩니다.

또한 탐지된 각 웹 브라우저에 대해 시스템은 액세스된 처음 100개의 웹 애플리케이션을 표시합니다. 이 한계에 도달하면 다음과 같이 될 때까지 능동 및 수동 소스의 해당 브라우저에 연결된 새 웹 애플리케이션이 삭제됩니다.

- 웹 브라우저 클라이언트 애플리케이션이 시간 초과됨, 또는
- 호스트 프로파일에서 웹 애플리케이션과 관련된 애플리케이션 정보 삭제

활성화된 상관관계 정책의 규정 준수 화이트 목록을 위반하는 애플리케이션이 호스트에서 실행되고 있는 경우, Firepower Management Center에서는 규정을 준수하지 않는 애플리케이션을 화이트 목록 위반으로 표시합니다.

팁 호스트의 특정 애플리케이션에 연결된 연결 이벤트를 분석하려면 애플리케이션 옆에 있는 로깅( )을 클릭합니다. 연결 이벤트에 대한 기본 설정 워크플로의 첫 번째 페이지가 나타나고 애플리케이션의 유형, 제품 및 버전에 의해 제한되는 연결 이벤트 및 호스트의 IP 주소를 보여줍니다. 연결 이벤트에 대한 기본 설정 워크플로가 없다면 선택해야 합니다.

다음은 호스트 프로파일에 나타나는 애플리케이션 정보에 대한 설명입니다.

애플리케이션 프로토콜

애플리케이션(HTTP 브라우저, DNS 클라이언트 등)이 사용하는 애플리케이션 프로토콜을 표시합니다.

Client(클라이언트**)**

Firepower System에 의해 식별되거나 Nmap에 의해 캡처되거나 호스트 입력 기능을 통해 획득된 경우, 페이로드에서 추출되는 클라이언트 정보. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

버전

클라이언트의 버전을 표시합니다.

웹 애플리케이션

웹 브라우저의 경우 시스템이 http 트래픽에서 탐지한 콘텐츠. 웹 애플리케이션 정보는 Firepower System에 의해 식별되거나 Nmap에 의해 캡처되거나 호스트 입력 기능을 통해 수집된 특정 콘텐츠 유형(예: WMV 또는 QuickTime)을 나타냅니다. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

호스트 프로파일에서 웹 애플리케이션 삭제

호스트 프로파일에서 애플리케이션을 삭제하여 호스트에서 실행되고 있지 않은 애플리케이션을 제거할 수 있습니다. 호스트에서 애플리케이션을 삭제하면 해당 호스트는 화이트 목록 규정 준수 상태로 전환될 수 있습니다.

참고 해당 애플리케이션이 다시 탐지되면 네트워크 맵 및 호스트 프로파일에 다시 추가됩니다.

프로시저

단계 **1** 호스트 프로파일에서 **Applications(**애플리케이션**)** 섹션으로 이동합니다.

단계 **2** 삭제할 애플리케이션 옆에 있는 삭제( )을 클릭합니다.

호스트 프로파일의 호스트 프로토콜

각 호스트 프로파일에는 호스트와 연결된 네트워크 트래픽에서 탐지된 프로토콜에 대한 정보가 포함되어 있습니다. 이 정보에는 다음이 포함됩니다.

프로토콜

호스트가 사용하는 프로토콜의 이름.

레이어

프로토콜이 실행되는 네트워크 레이어(`Network` 또는 `Transport`).

호스트 프로파일에 표시되는 프로토콜이 활성화된 상관관계 정책의 규정준수 화이트리스트를 위반하는 경우, Firepower Management Center에서는 규정을 준수하지 않는 프로토콜을 화이트리스트 위반으로 표시합니다.

호스트에서 실행되고 있지 않음을 알고 있는 프로토콜이 호스트 프로파일에 나열되는 경우, 해당 프로토콜을 삭제할 수 있습니다. 호스트에서 프로토콜을 삭제하면 해당 호스트가 규정준수 화이트리스트를 준수하게 될 수 있습니다.

참고 시스템은 해당 프로토콜을 다시 탐지하면 네트워크 맵 및 호스트 프로파일에 다시 추가합니다.

호스트 프로파일에서 프로토콜 삭제

프로시저

단계 **1** 호스트 프로파일의 **Protocols(프로토콜)** 섹션으로 이동합니다.

단계 **2** 삭제할 프로토콜 옆에 있는 삭제( )를 클릭합니다.

호스트 프로파일의 보안 침해 지표

Firepower System은 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 상호 연결하여 모니터링되는 네트워크의 호스트가 악의적인 수단에 의해 보안이 침해될 가능성이 있는지를 확인합니다. 이벤트 데이터의 특정 조합 및 빈도는 영향받는 호스트에서 IOC(보안 침해 지표) 태그를 트리거합니다.

호스트 프로파일의 Indications of Compromise(보안 침해 지표) 섹션에는 호스트에 대한 모든 보안 침해 지표 태그가 표시됩니다.

보안 침해 지표 태그를 지정하도록 시스템을 구성하려면 보안 침해 지표 규칙 활성화, 2555 페이지를 참조하십시오.

보안 침해 지표를 사용하는 방법에 대한 자세한 내용은 보안 침해 지표 데이터, 3056 페이지 및 해당 항목의 하위 항목을 참조하십시오.

관련 항목

보안 침해 지표, 2554 페이지

호스트 프로파일의 **VLAN** 태그

호스트가 VLAN(Virtual LAN)의 멤버인 경우 호스트 프로파일의 VLAN Tag(VLAN 태그) 섹션이 나타납니다.

물리적 네트워크 장비는 종종 VLAN을 사용하여 서로 다른 네트워크 블록에서 논리적 네트워크 세그먼트를 생성합니다. 시스템은 802.1q VLAN 태그를 탐지하고 각각에 대해 다음과 같은 정보를 표시합니다.

- **VLAN ID**는 호스트가 멤버인 VLAN을 식별합니다. 802.1q VLAN의 경우 0~4095 사이의 정수일 수 있습니다.
- **Type**은 VLAN 태그를 포함하는 캡슐화된 패킷을 식별하며, 이더넷 또는 토큰 링일 수 있습니다.
- **Priority**는 VLAN 태그의 우선순위를 식별하며, 범위는 0~7의 정수이고 7이 가장 높은 우선순위입니다.

VLAN 태그가 패킷 내에 중첩된 경우 시스템은 가장 안쪽의 VLAN 태그를 처리하고 Firepower Management Center는 이를 표시합니다. 시스템은 ARP 및 DHCP 트래픽을 통해 식별하는 MAC 주소에 대해서만 VLAN 태그 정보를 수집하고 표시합니다.

예를 들면 VLAN이 프린터로만 구성되어 있고 시스템이 해당 VLAN에서 Microsoft Windows 2000 운영 체제를 탐지하는 경우에는 VLAN 태그 정보가 유용할 수 있습니다. VLAN 정보는 또한 시스템이 좀 더 정확한 네트워크 맵을 생성하는 데에도 도움이 됩니다.

호스트 프로파일의 사용자 기록

호스트 프로파일의 사용자 기록 부분은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 일반적인 사용자는 저녁에 로그오프하고 호스트 리소스를 다른 사용자와 공유할 것입니다. 이메일 확인을 위한 요청 등 정기적인 로그인 요청은 짧은 일반 막대로 표시됩니다. 사용자 ID의 목록에는 사용자 로그인이 탐지된 시점을 나타내는 막대 그래프가 제공됩니다. 권한 없는 로그인의 경우에는 막대 그래프가 회색입니다.

시스템은 권한 없는 사용자의 호스트 로그인을 해당 호스트의 IP 주소와 연결하여, 사용자가 호스트의 사용자 기록에 나타나도록 합니다. 그러나 동일한 호스트에서 권한 있는 사용자 로그인이 탐지되면 권한 있는 사용자 로그인과 연결된 사용자가 호스트 IP 주소의 연결 관계를 인수하며, 권한 없는 새 사용자 로그인은 호스트 IP 주소와 사용자의 연결 관계를 중단하지 않습니다. 네트워크 검색 정책에서 실패한 로그인의 캡처를 구성하는 경우 목록에는 호스트 로그인에 실패한 사용자가 포함됩니다.

호스트 프로파일의 호스트 속성

호스트 속성을 사용하면 네트워크 환경에서 중요한 방법으로 호스트를 분류할 수 있습니다. Firepower System에는 3가지 속성이 존재합니다.

- 사전 정의된 호스트 속성
- 컴플라이언스 화이트 리스트 호스트 속성
- 사용자 정의 호스트 속성

사전 정의된 속성을 설정하거나 사용자 정의 호스트 속성을 생성한 후에는, 호스트 속성 값을 할당해야 합니다.

참고 호스트 속성은 어떤 도메인 레벨에서도 정의할 수 있습니다. 현재 및 상위 도메인에서 생성된 호스트 속성을 할당할 수 있습니다.

사전 정의된 호스트 속성

Firepower Management Center은(는) 사전 정의된 호스트 속성 2개를 제공합니다.

Host Criticality(호스트 심각도**)**

이 속성을 사용하여 특정 호스트의 비즈니스 중요도를 지정하고 상관관계 응답을 호스트 중요도에 맞게 조정하십시오. 예를 들어 조직의 메일 서버가 일반적인 사용자 워크스테이션보다 비즈니스에 더 중요하다고 생각한다면 메일 서버에는 High, 다른 주요 비즈니스 디바이스에는 Medium, 기타 호스트에는 Low 값을 할당할 수 있습니다. 그런 다음 영향받는 호스트의 중요도를 기반으로 서로 다른 알림을 생성하는 상관관계 정책을 생성할 수 있습니다.

Notes(참고**)**

이 호스트 한정 속성을 사용하여 다른 분석가에게 보여줄 호스트에 대한 정보를 기록하십시오. 예를 들어 운영체제의 패치되지 않은 이전 버전이 있는 테스트용 컴퓨터가 네트워크에 있는 경우, Notes 기능을 사용하여 시스템을 의도적으로 패치하지 않았음을 표시할 수 있습니다.

화이트 목록 호스트 속성

자동으로 생성되는 각 규정 준수 화이트 목록은 화이트 목록과 동일한 이름으로 호스트 속성을 생성합니다. 가능한 화이트 목록 호스트 속성은 다음과 같습니다.

- Compliant - 화이트 목록을 준수하는 호스트를 식별합니다.
- Non-Compliant - 화이트 목록을 위반하는 호스트를 식별합니다.
- Not Evaluated - 화이트 목록의 유효한 대상이 아니거나 어떤 이유로든 평가되지 않은 호스트를 식별합니다.

화이트 목록 호스트 속성 값을 수정하거나 화이트 목록 호스트 속성을 삭제할 수 없습니다.

사용자 정의 호스트 속성

사전 정의된 호스트 속성 또는 컴플라이언스 화이트 목록 호스트 속성에서 사용하는 것과는 다른 기준을 이용해 호스트를 식별하고 싶다면, 사용자 정의 호스트 속성을 사용하면 됩니다. 예를 들어, 다음이 가능합니다.

- 호스트에 물리적 위치 식별자(예: 시설 코드, 도시 또는 방 번호)를 할당합니다.
- 특정 호스트의 담당 시스템 관리자가 누구인지를 나타내는 Responsible Party Identifier(담당자 식별자)를 할당합니다. 호스트와 관련된 문제가 탐지될 때 올바른 시스템 관리자에게 알림을 전송하도록 상관관계 규칙 및 정책을 구성할 수 있습니다.
- 호스트의 IP 주소를 기반으로 사전 정의된 목록에서 호스트로 값을 자동으로 할당합니다. 이 기능은 네트워크에 처음으로 표시되는 새 호스트에 값을 할당할 때 유용하게 활용할 수 있습니다.

사용자 정의 호스트 속성은 호스트 프로파일 페이지에 나타나며, 여기서 호스트 단위로 값을 할당할 수 있습니다. 다음 작업도 가능합니다.

- 상관관계 정책 및 검색에서 속성을 사용합니다.
- 호스트 속성 테이블 보기에서 속성을 보고 이를 기반으로 보고서를 생성합니다.

사용자 정의 호스트 속성의 유형은 다음과 같습니다.

텍스트

텍스트 문자열을 호스트에 수동으로 할당할 수 있습니다.

정수

양의 정수 범위의 첫 번째와 마지막 숫자를 지정한 다음 이러한 숫자 중 하나를 호스트에 수동으로 할당할 수 있습니다.

목록

문자열 값의 목록을 생성한 다음 이러한 값 중 하나를 호스트에 수동으로 할당할 수 있습니다. 호스트의 IP 주소를 기반으로 호스트에 값을 자동으로 할당할 수도 있습니다.

여러 IP 주소가 있는 호스트에서 한 IP 주소를 기반으로 값을 자동 할당하면, 그 호스트와 연결된 모든 주소에 해당 값이 적용됩니다. Host Attributes(호스트 속성) 테이블을 볼 때는 이러한 점에 유의해야 합니다.

목록 값을 자동으로 할당하는 경우에는 일반적인 IP 주소가 아닌 네트워크 개체 사용을 고려해 보십시오. 이 방법을 이용하면 관리 용이성을 개선할 수 있으며, 특히 재정의를 활성화한 개체가 하위 도메인 관리자가 자신의 로컬 환경에 맞게 상위 설정을 조정하도록 허용하는 다중 도메인 구축에서 더욱 효과적입니다. 다중 도메인 구축의 경우에는, 자동 할당된 목록을 상위 도메인 수준에서 정의하며 하위 도메인이 중복되는 IP 주소를 사용할 때 의도하지 않은 호스트가 매칭되지 않도록 주의하십시오.

URL

URL 값을 호스트에 수동으로 할당할 수 있습니다.

사용자 정의 호스트 속성을 삭제하면 이를 사용하는 모든 호스트 프로파일에서 해당 속성이 제거됩니다.

텍스트 또는 URL 기반 호스트 속성 생성

프로시저

단계 1 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Host Attributes(**호스트 속성**)**을(를) 선택합니다.

단계 2 **Host Attribute Management(**호스트 속성 관리**)**를 클릭합니다.

단계 3 **Create Attribute(**속성 생성**)**를 클릭합니다.

단계 4 **Name(**이름**)**을 입력합니다.

단계 5 사용자 정의 호스트 속성, 3020 페이지에 설명된 대로 생성하려는 속성의 **Type(**유형**)**을 선택합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

정수 기반 호스트 속성 생성

정수 기반 호스트 속성을 정의할 때는 호스트가 허용하는 숫자 범위를 지정해야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Hosts(**호스트**)** > **Host Attributes(**호스트 속성**)**을(를) 선택합니다.
단계 **2** **Host Attribute Management(**호스트 속성 관리**)**를 클릭합니다.
단계 **3** **Create Attribute(**속성 생성**)**를 클릭합니다.
단계 **4** **Name(**이름**)**을 입력합니다.
단계 **5** 사용자 정의 호스트 속성, 3020 페이지에 설명된 대로 생성하려는 속성의 **Type(**유형**)**을 선택합니다.
단계 **6** 호스트에 할당할 수 있는 최소 정수 값을 **Min(**최소**)** 필드에 입력합니다.
단계 **7** 호스트에 할당할 수 있는 최대 정수 값을 **Max(**최대**)** 필드에 입력합니다.
단계 **8** **Save(**저장**)**를 클릭합니다.

목록 기반 호스트 속성 생성

목록 기반 호스트 속성을 정의할 때에는 목록의 각 값을 제공해야 합니다. 이러한 값에는 영숫자 문자, 공백 및 기호가 포함될 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Hosts(**호스트**)** > **Host Attributes(**호스트 속성**)**을(를) 선택합니다.
단계 **2** **Host Attribute Management(**호스트 속성 관리**)**를 클릭합니다.
단계 **3** **Create Attribute(**속성 생성**)**를 클릭합니다.
단계 **4** **Name(**이름**)**을 입력합니다.
단계 **5** 사용자 정의 호스트 속성, 3020 페이지에 설명된 대로 생성하려는 속성의 **Type(**유형**)**을 선택합니다.
단계 **6** 목록에 값을 추가하려면 **Add Value(**값 추가**)**를 클릭합니다.
단계 **7** 추가하려는 첫 번째 값을 **Name(**이름**)** 필드에 입력합니다.
단계 **8** 원하는 경우, 방금 추가한 속성 값을 호스트에 자동 할당하려면 **Add Networks(**네트워크 추가**)**를 클릭합니다.
단계 **9** 추가한 값을 **Value(**값**)** 드롭다운 목록에서 선택합니다.
단계 **10** 이 값을 자동 할당할 IP 주소 블록을 나타내는 IP 주소와 네트워크 마스크(IPv4)를 **IP Address(IP** 주소**)** 및 **Netmask(**넷마스크**)** 필드에 입력합니다.
단계 **11** 목록에 값을 더 추가하여 IP 주소 블록에 속하는 새 호스트에 자동으로 할당하려면 6~10단계를 반복합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

호스트 속성값 설정

미리 정의된 호스트 속성 및 사용자 정의 호스트 속성의 값을 설정할 수 있습니다. 시스템에서 생성된 컴플라이언스 화이트 호스트 속성의 값은 설정할 수 없습니다.

프로시저

단계 **1** 수정하려는 호스트 프로파일을 엽니다.

단계 **2** **Attributes(**속성**)** 섹션에서 **Edit Attributes(**속성 수정**)**를 클릭합니다.

단계 **3** 원하는 대로 속성을 업데이트합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

호스트 프로파일의 화이트 목록 위반

규정 준수 화이트 목록(또는 화이트 목록)는 특정 서브넷에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정할 수 있는 기준 집합입니다.

활성 상관관계 정책에 화이트 목록을 추가한 경우 시스템이 호스트에서 화이트 목록 위반을 탐지하면, Firepower Management Center는 화이트 목록 이벤트(특정 상관관계 이벤트 유형)를 데이터베이스에 로깅합니다. 이러한 각 화이트 목록 이벤트는 특정 호스트가 어떻게, 왜 화이트 목록을 위반했는지를 나타내는 화이트목록 위반과 연결됩니다. 호스트가 하나 이상의 화이트 목록을 위반하면 호스트 프로필에서 두 가지 방법으로 이러한 위반을 볼 수 있습니다.

첫째, 호스트 프로필은 호스트에 연결된 모든 개별 화이트 목록 위반을 나열합니다.

다음은 호스트 프로필에 표시되는 화이트 목록 위반 정보에 대한 설명입니다.

유형

위반의 유형, 즉 위반이 발생한 원인(규정을 준수하지 않는 운영 체제, 애플리케이션, 서버 또는 프로토콜).

이유

위반의 특정 이유. 예를 들어 Microsoft Windows 호스트만 허용하는 화이트 목록이 있는 경우, 호스트 프로파일에는 호스트에서 실행 중인 현재 운영 체제(예: `Linux 2.4, 2.6`)가 표시됩니다.

화이트 목록

위반과 연결된 화이트 목록의 이름.

둘째, 운영 체제, 애플리케이션, 프로토콜 및 서버와 관련된 섹션에서 Firepower Management Center는 규정을 준수하지 않는 요소를 화이트 목록 위반 아이콘으로 표시합니다. 예를 들어 Microsoft Windows

호스트만 허용하는 화이트 목록의 경우, 호스트 프로필은 해당 호스트의 운영 체제 정보 옆에 화이트 목록 위반 아이콘을 표시합니다.

참고 호스트의 프로필을 사용하여 규정 준수 화이트 목록에 대한 공유 호스트 프로필을 생성할 수 있습니다.

공유 화이트 목록 호스트 프로파일 생성

규정 준수 화이트 목록 공유 호스트 프로필은 여러 화이트 목록에 걸쳐 대상 호스트에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정합니다. 여러 개의 화이트 목록을 생성하지만 동일한 호스트 프로파일을 사용하여 화이트 목록 전반에 걸쳐 특정 운영체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로파일을 사용합니다.

알려진 IP 주소가 있는 호스트의 호스트 프로필을 사용하여 규정 준수 화이트 목록이 사용할 수 있는 공유 호스트 프로필을 생성할 수 있습니다. 그러나 시스템이 호스트의 운영 체제를 아직 식별하지 못한 경우에는 개별 호스트의 호스트 프로파일을 기반으로 공유 호스트 프로파일을 생성할 수 없습니다.

프로시저

단계 **1** 호스트 프로파일에서 **Generate(**생성**)**화이트리스트 **Profile(**프로파일**)**을 클릭합니다.

단계 **2** 특정 요구에 맞게 공유 호스트 프로파일을 수정 및 저장합니다.

관련 항목

화이트 리스트 호스트 프로필 빌드, 2574 페이지

호스트 프로파일의 악성코드 탐지

Most Recent Malware Detections(가장 최근의 악성코드 탐지) 섹션에는 호스트가 악성코드 파일을 주고받은 가장 최근의 악성코드 이벤트가 최대 100개까지 나열됩니다. 호스트 프로파일에는 네트워크 기반 악성코드 이벤트(AMP for Networks 에 의해 생성)와 엔드포인트 기반 악성코드 이벤트(AMP for Endpoints에 의해 생성)가 모두 나열됩니다.

파일이 악성코드로 소급 식별된 파일 이벤트에 호스트가 관련된 경우, 악성코드 식별이 발생한 후 파일이 전송된 원래 이벤트가 악성코드 탐지 목록에 나타납니다. 악성코드로 식별된 파일이 악성코드가 아닌 것으로 소급 결정되면 해당 파일과 연결된 악성코드 이벤트가 더 이상 목록에 나타나지 않습니다. 예를 들어 파일에 `Malware(악성코드)` 속성이 있고 해당 속성이 `Clean(정상)`으로 변경되면 해당 파일의 이벤트는 호스트 프로파일의 악성코드 탐지 목록에서 제거됩니다.

호스트 프로필에서 악성코드 탐지를 볼 때 **Malware(**악성코드**)**를 클릭하여 해당 호스트의 악성코드 이벤트를 볼 수 있습니다.

다음은 호스트 프로파일의 Most Recent Malware Detections(가장 최근의 악성코드 탐지) 섹션에 있는 열에 대한 설명입니다.

시간

이벤트가 생성된 날짜 및 시간

파일이 악성코드로 소급 식별된 이벤트의 경우, 악성코드가 식별된 시간이 아니라 원래 이벤트의 시간을 나타냅니다.

호스트 역할

탐지된 악성코드 전송에서 호스트의 역할(발신자 또는 수신자). AMP for Endpoints에 의해 생성된 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")의 경우, 호스트는 항상 수신자입니다.

위협 이름

탐지된 악성코드의 이름.

파일 이름

악성코드 파일의 이름.

File Type(파일 유형)

`PDF` 또는 `MSEXE` 등의 파일 형식.

호스트 프로파일의 취약성

호스트 프로파일의 Vulnerabilities(취약성) 섹션에는 해당 호스트에 영향을 미치는 취약성이 나열됩니다. 이러한 취약성은 시스템이 호스트에서 탐지한 운영 체제, 서버, 애플리케이션에 기반합니다.

호스트의 운영 체제 ID 또는 호스트의 애플리케이션 프로토콜 중 하나에 ID 충돌이 있는 경우, 시스템은 충돌이 해결될 때까지 두 ID에 대한 취약성을 나열합니다.

NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

서버 공급업체 및 버전 정보는 대체로 트래픽에 포함되지 않습니다. 기본적으로 시스템은 트래픽을 보내고 받는 호스트에 대해 관련 취약성을 매핑하지 않습니다. 그러나 공급업체 또는 버전 정보가 없는 특정 애플리케이션 프로토콜에 대한 취약성을 매핑하도록 시스템을 구성할 수 있습니다.

호스트 입력 기능을 사용하여 네트워크의 호스트에 대한 서드파티 취약성 정보를 추가하는 경우 추가적인 Vulnerabilities(취약성) 섹션이 나타납니다. 예를 들어 QualysGuard Scanner에서 취약성을 가져오면 호스트 프로파일에 QualysGuard Vulnerabilities 섹션이 포함됩니다. 서드파티 취약성의 경우 호스트 프로파일의 해당 Vulnerabilities(취약성) 섹션에 표시되는 정보는 호스트 입력 기능을 사용하여 취약성 데이터를 가져올 때 제공한 정보로 제한됩니다.

서드파티 취약성을 운영 체제 및 애플리케이션 프로토콜과 연결할 수 있지만 클라이언트와는 연결할 수 없습니다. 서드파티 취약성 가져오기에 대한 자세한 내용은 *Firepower System Host Input API* 설명서를 참조하십시오.

다음은 호스트 프로파일의 Vulnerabilities(취약성) 섹션에 있는 열에 대한 설명입니다.

이름

취약성의 이름.

원격

취약성이 원격으로 악용될 수 있는지를 나타냅니다. 이 열이 비어 있으면 취약성 정의에 이 정보가 포함되지 않은 것입니다.

Component(구성 요소)

취약성과 관련된 운영 체제, 애플리케이션 프로토콜 또는 클라이언트의 이름.

Port(포트)

취약성이 지정된 포트에서 실행 중인 애플리케이션 프로토콜과 연결된 경우 포트 번호.

관련 항목

취약성 데이터 필드, 3069 페이지
취약성 비활성화, 3071 페이지

취약성 패치 다운로드

네트워크의 호스트에서 검색된 취약성을 완화하기 위한 패치를 다운로드할 수 있습니다.

프로시저

단계 **1** 패치를 다운로드할 호스트의 호스트 프로파일에 액세스합니다.
단계 **2** **Vulnerabilities(취약성)** 섹션을 확장합니다.
단계 **3** 패치를 적용할 취약성의 이름을 클릭합니다.
단계 **4** 취약성에 대한 패치의 목록을 표시하려면 **Fixes(수정)** 섹션을 확장합니다.
단계 **5** 다운로드할 패치 옆에 있는 **Download(다운로드)**를 클릭합니다.
단계 **6** 패치를 다운로드하고 영향받는 시스템에 적용합니다.

개별 호스트 취약성 비활성화

호스트 취약성 편집기를 사용하여 호스트별로 취약성을 비활성화할 수 있습니다. 호스트에 대한 취약성을 비활성화할 경우 해당 호스트에 대한 영향 상관관계에는 여전히 사용되지만 영향 레벨은 자동으로 한 단계 줄어듭니다.

프로시저

단계 **1** 호스트 프로파일의 **Vulnerabilities(**취약성**)** 섹션으로 이동합니다.

단계 **2** **Edit Vulnerabilities(**취약성 수정**)**를 클릭합니다.

단계 **3** **Valid Vulnerabilities(**유효한 취약성**)** 목록에서 취약성을 선택하고 아래쪽 화살표를 클릭하여 **Invalid Vulnerabilities(**유효하지 않은 취약성**)** 목록으로 이동시킵니다.

팁 클릭하고 끌어 여러 인접 취약성을 선택할 수 있습니다. 또한 취약성을 두 번 클릭하여 다른 목록으로 이동시킬 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 원하는 경우, **Invalid Vulnerabilities(**유효하지 않은 취약성**)** 목록에서 **Valid Vulnerabilities(**유효한 취약성**)** 목록으로 취약성을 이동시켜 호스트의 취약성을 활성화합니다.

관련 항목

개별 취약성 비활성화, 3027 페이지
다중 취약성 비활성화, 3073 페이지

개별 취약성 비활성화

호스트 프로파일에서 취약성을 비활성화하면 해당 취약성은 네트워크 맵의 모든 호스트에서 비활성화됩니다. 하지만 언제든 다시 활성화할 수 있습니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 **1** 취약성 세부 정보에 액세스:

- 영향을 받는 호스트 프로파일에서 **Vulnerabilities(**취약성**)** 섹션을 확장하고 활성화 또는 비활성화하려는 취약성의 이름을 클릭합니다.

- 미리 정의된 워크플로우에서 **Analysis(분석)** > **Hosts(호스트)** > **Vulnerabilities(취약성)**을 선택하고 클릭하고 활성화하거나 비활성화하려는 취약성 옆에 있는 보기 ( )를 클릭합니다.

단계 **2** **Impact Qualification** 드롭다운 목록에서 **Disabled(비활성화)**를 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **3** 네트워크 맵의 모든 호스트에 대해 **Impact Qualification** 값을 변경할 것인지 확인합니다.

단계 **4** **Done(완료)**을 클릭합니다.

다음에 수행할 작업

- 원하는 경우, 위의 단계를 수행하면서 **Impact Qualification** 드롭다운 목록에서 **Enabled(활성화)**를 선택하여 취약성을 활성화합니다.

관련 항목

개별 호스트 취약성 비활성화, 3027 페이지
다중 취약성 비활성화, 3073 페이지
운영 체제 ID 충돌, 3009 페이지

호스트 프로파일의 스캔 결과

Nmap을 사용하여 호스트를 스캔하거나 Nmap 스캔에서 결과를 가져오면 그러한 결과는 스캔에 포함된 호스트의 호스트 프로파일에 나타납니다.

필터링되지 않은 열린 포트에서 실행되는 호스트 운영 체제 및 서버에 대해 Nmap이 수집하는 정보는 각각 호스트 프로파일의 Operating System(운영 체제) 및 Servers(서버) 섹션에 직접 추가됩니다. 또한 Nmap은 해당 호스트에 대한 스캔 결과의 목록을 Scan Results(스캔 결과) 섹션에 추가합니다. Scan Results(스캔 결과) 섹션이 프로파일에 나타나려면 스캔은 호스트에서 열린 포트를 찾아야 합니다.

각 결과는 정보의 소스, 스캔된 포트의 번호와 유형, 포트에서 실행되는 서버의 이름, Nmap에서 탐지한 추가 정보(예: 포트의 상태 또는 서버의 공급업체 이름) 등을 나타냅니다. UDP 포트를 스캔하는 경우, 해당 포트에서 탐지된 서버는 Scan Results(스캔 결과) 섹션에만 나타납니다.

호스트 프로파일에서 Nmap 스캔을 수행할 수 있습니다.

호스트 프로파일에서 호스트 스캔

호스트 프로파일에서 호스트에 대해 Nmap 스캔을 수행할 수 있습니다. 스캔이 완료되면 해당 호스트의 서버 및 운영 체제 정보가 호스트 프로파일에서 업데이트됩니다. 호스트 프로파일의 Scan Results(스캔 결과) 섹션에 스캔 결과가 추가됩니다.

주의 또 다른 Nmap 스캔을 실행하거나 우선순위가 더 높은 호스트 입력으로 재정의할 때까지 Nmap 제공 서버 및 운영 체제 데이터는 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오.

시작하기 전에

- Nmap 스캔 인스턴스를 추가합니다(Nmap 스캔 인스턴스 추가, 2427 페이지 참조).

프로시저

단계 **1** 호스트 프로파일에서 **Scan Host(**호스트 스캔**)**를 클릭합니다.

단계 **2** 호스트 스캔에 사용할 스캔 교정 옆에 있는 **Scan(**스캔**)**을 클릭합니다.

시스템이 호스트를 스캔하고 결과를 호스트 프로파일에 추가합니다.

관련 항목

Nmap 스캔 자동화, 253 페이지

호스트 프로파일 기록

기능	버전	세부 사항
VRF 사용 시 제한 사항	6.6	사용자 환경에서 가상 라우팅 및 포워딩을 사용하는 경우 VRF가 중복 네트워크 공간을 포함할 수 있으므로 단일 IP 주소가 여러 호스트를 나타낼 수 있습니다. 지원되는 플랫폼: FMC

125 장

검색 이벤트 작업

다음 주제에서는 검색 이벤트를 사용하는 방법을 설명합니다.

- 검색 이벤트 요구 사항 및 사전 요건, 3031 페이지
- 검색 이벤트의 검색 및 ID 데이터, 3031 페이지
- 검색 이벤트 통계 보기, 3032 페이지
- 검색 성능 그래프 보기, 3035 페이지
- 검색 및 ID 워크플로 사용, 3037 페이지
- 검색 이벤트 작업 히스토리, 3091 페이지

검색 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 보안 분석가

검색 이벤트의 검색 및 ID 데이터

시스템은 모니터링되는 네트워크에서 탐지된 변경을 나타내는 이벤트의 테이블을 생성합니다. 이러한 테이블을 사용하여 네트워크에서의 사용자 활동을 검토하고 대응 방법을 결정할 수 있습니다. 네트워크 검색 및 *ID* 정책은 수집할 데이터 종류, 모니터링할 네트워크 세그먼트, 이를 위해 사용할 특정 하드웨어 인터페이스를 지정합니다.

검색 및 ID 이벤트 테이블을 사용하여 네트워크의 호스트, 애플리케이션, 사용자에 연결된 위협을 식별할 수 있습니다. 시스템은 시스템에서 생성되는 이벤트 분석에 사용할 수 있는 사전 정의 워크플로 집합을 제공합니다. 특정 요구와 일치하는 정보만 표시하는 맞춤형 워크플로를 생성할 수도 있습니다.

분석을 위해 네트워크 검색 및 ID 데이터를 수집하고 저장하려면 네트워크 검색 및 ID 정책을 구성해야 합니다. ID 정책을 구성한 후에는 액세스 제어 정책에서 ID 정책을 호출하여 트래픽 모니터링에 사용할 디바이스에 구축해야 합니다.

네트워크 검색 정책은 호스트, 애플리케이션, 권한 없는 사용자 데이터를 제공합니다. ID 정책은 권한 있는 사용자 데이터를 제공합니다.

다음 검색 이벤트 테이블은 Analysis(분석) > Hosts(호스트) 및 Analysis(분석) > Users(사용자) 메뉴 아래 위치합니다.

검색 이벤트 테이블	검색 데이터로 채워지는지 여부	**ID** 데이터로 채워지는지 여부
호스트	예	아니요
보안 침해 지표	예	아니요
애플리케이션	예	아니요
애플리케이션 세부사항	예	아니요
서버	예	아니요
호스트 속성	예	아니요
검색 이벤트	예	예
활성 세션	예	예
사용자의 활동	예	예
사용자	예	예
취약성	예	아니요
서드파티 취약성	예	아니요

검색 이벤트 통계 보기

Discovery Statistics(검색 통계) 페이지에는 시스템에서 탐지한 호스트, 이벤트, 프로토콜, 애플리케이션 프로토콜 및 운영 체제의 요약이 표시됩니다.

이 페이지에는 마지막 시간에 대한 통계 및 총 누적 통계가 나열됩니다. 특정 디바이스 또는 모든 디바이스에 대한 통계를 볼 수 있습니다. 요약 내에 나열된 이벤트, 서버, 운영 체제 또는 운영 체제 공급업체를 클릭하여 페이지의 항목과 일치하는 이벤트를 볼 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Discovery Statistics(**검색 통계**)**을(를) 선택합니다.

단계 **2** 통계를 보려는 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다. 선택적으로, 모든 관리하는 모든 디바이스에 대한 통계를 보려면 Firepower Management Center를 선택합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Statistics Summary(통계 요약)에서 통계 요약 섹션, 3033 페이지의 설명에 따라 일반 통계를 볼 수 있습니다.
- Event Breakdown(이벤트 분류)에서 보려고 하는 이벤트 유형을 클릭합니다. 이벤트가 표시되지 않는 경우, 타임 윈도우 변경, 2815 페이지에 설명된 대로 시간 범위를 조정해야 할 수 있습니다.
- Protocol Breakdown(프로토콜 분류)에서 탐지된 이벤트가 현재 사용 중인 프로토콜을 볼 수 있습니다.
- Application Protocol Breakdown(애플리케이션 프로토콜 분류)에서 보려는 애플리케이션 프로토콜의 이름을 클릭합니다.
- OS Breakdown(OS 분류)에서 **OS Name(OS** 이름**)** 또는 **OS Vendor(OS** 공급업체**)**를 클릭합니다.

관련 항목

이벤트 분류 섹션, 3034 페이지
프로토콜 분류 섹션, 3035 페이지
애플리케이션 프로토콜 분류 섹션, 3035 페이지
OS 분류 섹션, 3035 페이지

통계 요약 섹션

다음은 Statistics Summary(통계 요약) 섹션의 행에 대한 설명입니다.

Total events

Firepower Management Center에 저장된 총 검색 이벤트 수.

Total Events Last Hour

마지막 시간에 생성된 총 검색 이벤트 수.

Total Events Last Day

마지막 날에 생성된 총 검색 이벤트 수

Total Application Protocols

탐지된 호스트에서 실행 중인 서버의 총 애플리케이션 프로토콜 수.

Total IP Hosts

고유한 IP 주소로 식별된 총 탐지된 호스트 수.

Total MAC Hosts

IP 주소로 식별되지 않은 총 탐지된 호스트 수.

모든 디바이스에 대한 검색 통계를 보든 특정 디바이스에 대한 검색 통계를 보든, Total MAC Hosts 통계는 동일합니다. 매니지드 디바이스는 IP 주소를 기반으로 호스트를 검색하기 때문입니다. 이 통계는 다른 수단에 의해 식별되는 총 호스트 수를 제공하며 특정 매니지드 디바이스와는 독립적입니다.

Total Routers

라우터로서 식별된 총 탐지된 노드 수.

Total Bridges

브리지로서 식별된 총 탐지된 노드 수.

Host Limit Usage

현재 사용 중인 호스트 제한의 총 비율. 호스트 제한은 Firepower Management Center의 모델로 정의됩니다. 모든 매니지드 디바이스에 대한 통계를 보는 경우에만 Host Limit Usage가 나타납니다.

참고 호스트 제한에 도달하고 호스트가 삭제되는 경우, 검색 데이터를 비운 네트워크 맵에 호스트가 다시 나타나지 않습니다.

Last Event Received

가장 최근 검색 이벤트가 발생한 날짜 및 시간.

Last Connection Received

가장 최근 연결이 완료된 날짜 및 시간.

이벤트 분류 섹션

Event Breakdown(이벤트 분류) 섹션에는 마지막 시간 내에 발생한 검색 및 호스트 입력 이벤트의 각 유형별 카운트는 물론 데이터베이스에 저장된 각 이벤트 유형의 총 카운트도 나열됩니다.

검색 및 호스트 입력 이벤트에 대한 세부사항을 보는 데에도 Event Breakdown(이벤트 분류) 섹션을 사용할 수 있습니다.

관련 항목

검색 및 호스트 입력 이벤트, 3039 페이지

프로토콜 분류 섹션

Protocol Breakdown(프로토콜 분류) 섹션에는 탐지된 호스트에서 현재 사용 중인 프로토콜이 나열됩니다. 탐지된 각 프로토콜 이름, 프로토콜 스택에서의 "레이어", 프로토콜을 사용하여 통신하는 총 호스트 수가 표시됩니다.

애플리케이션 프로토콜 분류 섹션

Application Protocol Breakdown(애플리케이션 프로토콜 분류) 섹션에는 탐지된 호스트에서 현재 사용 중인 애플리케이션 프로토콜이 나열됩니다. 프로토콜 이름, 지난 시간 동안 애플리케이션 프로토콜을 실행하던 총 호스트 수, 특정 시점에 프로토콜을 실행하던 것으로 탐지된 총 호스트 수가 나열됩니다.

탐지된 프로토콜을 사용하는 서버에 대한 세부사항을 보는 데에도 Application Protocol Breakdown(애플리케이션 프로토콜 분류) 섹션을 사용할 수 있습니다.

관련 항목

서버 데이터, 3060 페이지

OS 분류 섹션

OS Breakdown(OS 분류) 섹션에는 모니터링되는 네트워크에서 현재 실행 중인 운영 체제와 더불어 해당 공급업체 및 각 운영 체제를 실행 중인 총 호스트 수가 나열됩니다.

운영 체제 이름 및 버전에 사용되는 `unknown` 값은 해당 운영 체제 및 버전이 시스템의 핑거프린트와 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제 및 버전을 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

탐지된 운영 체제에 대한 세부사항을 보는 데에도 OS Breakdown(OS 분류) 섹션을 사용할 수 있습니다.

관련 항목

호스트 데이터, 3047 페이지

검색 성능 그래프 보기

검색 이벤트와 함께 매니지드 디바이스에 대한 성능 통계를 표시하는 그래프를 생성할 수 있습니다.

새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생할 때까지 데이터가 변경되지 않을 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

애플리케이션 네트워크 검색 정책이 애플리케이션, 호스트, 사용자를 포함하도록 편집합니다. (이는 시스템 성능에 영향을 줄 수 있습니다.) 네트워크 검색 규칙 구성, 2540 페이지 및 작업 및 검색된 자산, 2541 페이지를 참조하십시오.

이 작업을 수행하려면 관리자 또는 유지보수 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Discovery Performance(**검색 성능**)**을(를) 선택합니다.

단계 **2** 포함할 Firepower Management Center 또는 매니지드 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다.

단계 **3** 검색 성능 그래프 유형, 3036 페이지에 설명된 대로 **Select Graph(s)(**그래프 선택**)** 목록에서 생성할 그래프 유형을 선택합니다.

단계 **4** **Select Time Range(**시간 범위 선택**)** 목록에서 그래프에 사용할 시간 범위를 선택합니다.

단계 **5** 선택한 통계를 그래프로 표시하려면 **Graph(**그래프**)**를 클릭합니다.

검색 성능 그래프 유형

다음은 사용 가능한 그래프 유형에 대한 설명입니다.

Processed Events/Sec

Data Correlator가 초당 처리하는 이벤트 수를 나타내는 그래프를 표시합니다.

Processed Connections/Sec

Data Correlator가 초당 처리하는 연결 수를 나타내는 그래프를 표시합니다.

Generated Events/Sec

시스템이 초당 생성하는 이벤트 수를 나타내는 그래프를 표시합니다.

Mbits/Sec

초당 검색 프로세스에 의해 분석되는 트래픽의 메가비트 수를 나타내는 그래프를 표시합니다.

Avg Bytes/Packet

검색 프로세스에 의해 분석되는 각 패킷에 포함된 평균 바이트 수를 나타내는 그래프를 표시합니다.

K Packets/Sec

초당 검색 프로세스에 의해 분석되는 패킷 수를 나타내는 그래프를 표시합니다(1,000 단위).

검색 및 ID 워크플로 사용

Firepower Management Center에서는 네트워크에 대해 생성되는 검색 및 ID 데이터 분석에 사용할 수 있는 이벤트 워크플로 집합을 제공합니다. 워크플로는 네트워크 맵과 더불어 네트워크 자산에 대한 핵심 정보 소스입니다.

Firepower Management Center에서는 검색 및 ID 데이터에 대한 사전 정의된 워크플로는 물론 탐지된 호스트와 호스트 속성, 서버, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 활동, 사용자 등에 대한 사전 정의된 워크플로도 제공합니다. 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 사전 정의된 워크플로에 액세스하려면 다음을 수행합니다.

- 검색 및 호스트 입력 데이터 — 검색 및 호스트 입력 이벤트 보기, 3045 페이지를 참조하십시오.
- 호스트 데이터 — 호스트 데이터 보기, 3047 페이지를 참조하십시오.
- 호스트 속성 데이터 — 호스트 속성 보기, 3054 페이지를 참조하십시오.
- 보안 침해 지표 데이터 — 보안 침해 지표 데이터 보기 및 작업, 3056 페이지를 참조하십시오.
- 서버 데이터 — 서버 데이터 보기, 3060 페이지를 참조하십시오.
- 애플리케이션 데이터 — 애플리케이션 데이터 보기, 3064 페이지를 참조하십시오.
- 애플리케이션 세부사항 데이터 — 애플리케이션 세부사항 데이터 보기, 3067 페이지를 참조하십시오.
- 활성 세션 데이터 — 활성 세션 데이터 보기, 3083 페이지를 참조하십시오.
- 사용자 데이터 — 사용자 데이터 보기, 3086 페이지를 참조하십시오.
- 사용자 활동 데이터 — 사용자 활동 데이터 보기, 3089 페이지를 참조하십시오.
- 네트워크 맵 — 네트워크 맵 보기, 2733 페이지를 참조하십시오.

단계 **2** 맞춤형 워크플로에 액세스하려면 **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**맞춤형 워크플로**)**를 선택합니다.

단계 **3** 맞춤형 테이블에 기반한 워크플로에 액세스하려면 **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**맞춤형 테이블**)**를 선택합니다.

단계 **4** 네트워크 검색 워크플로에서 액세스하는 모든 페이지에서 일반적으로 이루어지는 다음 작업을 수행합니다.

- 열 제한 — 표시되는 열을 제한하려면 숨기려는 열 머리글의 닫기(✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 삭제 — 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 후 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다. 이러한 항목은 시스템의 검색 기능이 다시 시작될 때까지(이 경우 다시 탐지될 수도 있음) 삭제된 상태로 유지됩니다.

  주의 Analysis > Users > Active Sessions(분석 > 사용자 > 활성 세션) 페이지에서 비 VPN 세션을 삭제하기 전에 해당 세션을 닫았는지 확인하십시오. 활성 세션을 삭제하면 해당 정책이 디바이스의 세션을 탐지할 수 없으므로, 이러한 작업을 수행하도록 정책을 구성한 경우에도 세션을 모니터링하거나 차단할 수 없습니다.

  참고 Analysis > Users > Active Sessions(분석 > 사용자 > 활성 세션) 페이지의 VPN 세션에 대한 자세한 내용은 원격 액세스 VPN 현재 사용자 보기를 참조하십시오.

  참고 Cisco(서드파티와 반대) 취약성은 삭제할 수 없습니다. 그러나 검토한 것으로 표시할 수는 있습니다.

- 드릴다운 — 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용, 2801 페이지을 참조하십시오.
- 현재 페이지 이동 — 현재 워크플로 페이지 내에서 이동하려면 워크플로 페이지 탐색 툴, 2798 페이지을 참조하십시오.
- 워크플로 내에서 이동 — 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 다른 워크플로로 이동 — 다른 이벤트 보기로 이동하여 관련 이벤트를 검토하려면 워크플로 간 탐색, 2821 페이지을 참조하십시오.
- 데이터 정렬 — 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
- 호스트 프로파일 보기 - IP 주소의 호스트 프로파일을 보려면 **Host Profile(**호스트 프로파일**)**을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 **Compromised Host(**보안 침해된 호스트**)**를 클릭합니다.
- 사용자 프로파일 - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘를 클릭합니다. 보기

관련 항목

워크플로 사용, 2793 페이지
FMC 데이터베이스에서 데이터 제거, 270 페이지

검색 및 호스트 입력 이벤트

시스템에서는 모니터링되는 네트워크 세그먼트의 변경 세부사항을 전달하는 검색 이벤트를 생성합니다. 새로 검색된 네트워크 기능에 대해서는 새 이벤트가 생성되고, 이전에 식별된 네트워크 자산의 변경 사항에 대해서는 변경 이벤트가 생성됩니다.

초기 네트워크 검색 단계에서 시스템은 각 호스트에 대해, 그리고 각 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버에 대해 새 이벤트를 생성합니다. 원하는 경우, 내보낸 NetFlow 레코드를 사용하여 이러한 새 호스트 및 서버 이벤트를 생성하도록 시스템을 구성할 수 있습니다.

또한 시스템은 검색된 각 호스트에서 실행 중인 각 애플리케이션 프로토콜, 네트워크 및 전송에 대해 새 이벤트를 생성합니다. NetFlow 엑스포터를 모니터링하도록 구성된 검색 규칙에서는 애플리케이션 프로토콜 탐지를 비활성화할 수 있지만 Firepower System 매니지드 디바이스를 모니터링하도록 구성된 검색 규칙에서는 비활성화할 수 없습니다. 비 NetFlow 검색 규칙에서 호스트 또는 사용자 검색을 비활성화하면 애플리케이션이 자동으로 검색됩니다.

초기 네트워크 매핑이 완료되면 시스템은 변경 이벤트를 생성하여 네트워크 변경 사항을 계속해서 기록합니다. 전에 검색된 자산의 구성이 변경될 때마다 변경 이벤트가 생성됩니다.

생성된 검색 이벤트는 데이터베이스에 로깅됩니다. Firepower Management Center 웹 인터페이스를 사용하여 검색 이벤트를 보고, 검색하고, 삭제할 수 있습니다. 상관관계 규칙에서도 검색 이벤트를 사용할 수 있습니다. 생성된 검색 이벤트 유형 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 기준을 충족하면 교정과 syslog, SNMP, 이메일 알림 응답을 실행합니다.

호스트 입력 기능을 사용하여 네트워크 맵에 데이터를 추가할 수 있습니다. 운영 체제 정보를 추가, 수정 또는 삭제할 수 있으며, 이 경우 시스템은 해당 호스트에 대한 해당 정보의 업데이트를 중지합니다. 또한 애플리케이션 프로토콜, 클라이언트, 서버 및 호스트 속성을 수동으로 추가, 수정 또는 삭제하거나 취약성 정보를 수정할 수도 있습니다. 이렇게 하면 시스템은 호스트 입력 이벤트를 생성합니다.

검색 이벤트 유형

네트워크 검색 정책에서 시스템이 기록하는 검색 이벤트의 유형을 설정할 수 있습니다. 검색 이벤트 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다. 다음은 검색 이벤트 유형에 대한 설명입니다.

호스트에 대해 추가 **MAC** 탐지됨

시스템이 전에 검색된 호스트에 대해 새 MAC 주소를 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 생성됩니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로파일 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다.

클라이언트 시간 초과

시스템이 비활성 상태를 이유로 클라이언트를 데이터베이스에서 삭제하면 이 이벤트가 생성됩니다.

클라이언트 업데이트

시스템이 HTTP 트래픽에서 페이로드(즉, 오디오, 비디오, 웹메일 등 특정 유형의 콘텐츠)를 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP 주소 변경됨

DHCP 주소 할당 때문에 호스트 IP 주소가 변경된 것을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP 주소 재할당

호스트가 IP 주소를 재사용할 경우, 즉 DHCP IP 주소 할당 때문에 호스트가 전에 다른 물리적 호스트에 사용되던 IP 주소를 얻는 경우 이 이벤트가 생성됩니다.

홉 변경

호스트 및 해당 호스트를 탐지하는 디바이스 간 다수의 네트워크 홉에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다. 발생 조건은 다음과 같습니다.

- 디바이스가 여러 라우터를 통과하는 호스트 트래픽을 확인하고 호스트 위치에 대한 더 나은 결정을 내릴 수 있는 경우
- 디바이스가 호스트로부터 ARP 전송을 탐지하고 로컬 세그먼트에 호스트가 있음을 나타내는 경우

호스트 삭제됨: 호스트 한도 도달함

Firepower Management Center에서 호스트 제한이 초과되어 네트워크 맵에서 모니터링되는 호스트가 삭제될 경우 이 이벤트가 생성됩니다.

호스트 삭제됨: 호스트 한도 도달함

Firepower Management Center에서 호스트 제한에 도달하여 새 호스트가 삭제될 경우 이 이벤트가 생성됩니다. 이 이벤트를 호스트 제한에 도달할 경우 오래된 호스트가 네트워크 맵에서 삭제되는 이전 이벤트와 비교해보십시오.

호스트 제한에 도달할 경우 새 호스트를 삭제하려면 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)** > **Advanced(**고급**)**로 이동하여 **When Host Limit Reached(**호스트 제한 도달 시**)**를 **Drop hosts(**호스트 삭제**)**로 설정합니다.

호스트 **IOC** 설정

호스트에 대해 IOC(indication of compromise)가 설정되고 알림이 생성될 경우 이 이벤트가 발생합니다.

호스트 시간 초과

호스트가 네트워크 검색 정책에 정의된 간격 내에 트래픽을 생성하지 못했기 때문에 네트워크 맵에서 삭제될 경우 이 이벤트가 생성됩니다. 개별 호스트 IP 주소 및 MAC 주소는 개별적으로 시간 초과됩니다. 관련된 모든 주소가 시간 초과되기 전에는 호스트가 네트워크 맵에서 사라지지 않습니다.

네트워크 검색 정책에서 모니터링할 네트워크를 변경하는 경우, 호스트 제한에서 계산되지 않도록 네트워크 맵에서 오래된 호스트를 수동으로 삭제하고자 할 수 있습니다.

네트워크 디바이스로 호스트 유형 변경됨

탐지된 호스트가 실제로 네트워크 디바이스임을 시스템에서 확인할 경우 이 이벤트가 생성됩니다.

ID 충돌

서버 또는 운영체제에 대한 현재의 능동 ID와 충돌하는 새 서버 또는 운영체제 ID를 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 충돌을 해결하려면 Nmap 교정을 트리거하는 Identity Conflict(ID 충돌) 이벤트를 사용할 수 있습니다.

ID 시간 초과

활성 소스의 서버 또는 운영체제 ID 데이터가 시간을 초과하면 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 데이터를 새로 고치려면 Nmap 교정을 트리거하는 Identity Conflict(ID 충돌) 이벤트를 사용할 수 있습니다.

MAC 정보 변경

특정 MAC 주소 또는 TTL 값과 연결된 정보에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 발생합니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로파일 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다. 트래픽이 여러 라우터를 통과할 수 있으므로 TTL이 변경될 수 있습니다. 또는 시스템이 호스트의 실제 MAC 주소를 탐지하는 경우에도 TTL이 변경될 수 있습니다.

NETBIOS 이름 변경

시스템이 호스트 NetBIOS 이름의 변경을 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 NetBIOS 프로토콜을 사용하는 호스트에 대해서만 생성됩니다.

새 클라이언트

시스템이 새 클라이언트를 탐지할 경우 이 이벤트가 생성됩니다.

참고 분석용 클라이언트 데이터를 수집 및 저장하려면 네트워크 검색 정책의 검색 규칙에서 애플리케이션 탐지를 활성화하십시오.

새 호스트

시스템이 네트워크에서 실행 중인 새 호스트를 탐지할 경우 이 이벤트가 생성됩니다.

이 이벤트는 디바이스가 새 호스트와 관련된 NetFlow 데이터를 처리하는 경우에도 생성될 수 있습니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 호스트를 검색하는 네트워크 검색 규칙을 설정해야 합니다.

새 네트워크 프로토콜

호스트가 새 네트워크 프로토콜(IP, ARP 등)과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새 **OS**

시스템이 호스트에 대한 새 운영체제를 탐지하거나 호스트 운영체제에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

새 **TCP** 포트

호스트에서 활성화된 새 TCP 서버 포트(예: SMTP 또는 웹 서비스에서 사용하는 포트)를 시스템이 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 애플리케이션 프로토콜 또는 이와 연결된 서버를 식별하는 데 사용되지 않습니다. 그러한 정보는 TCP Server Information Update(TCP 서버 정보 업데이트) 이벤트에서 전송됩니다.

또한 이 이벤트는 네트워크 맵에 존재하지 않는 모니터링되는 네트워크 상의 서버와 관련된 NetFlow 데이터를 디바이스가 처리할 때도 생성됩니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 애플리케이션을 검색하는 네트워크 검색 규칙을 설정해야 합니다.

새 전송 프로토콜

호스트가 TCP, UDP 등의 새 네트워크 프로토콜과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새 **UDP** 포트

시스템이 호스트에서 실행 중인 새 UDP 서버 포트를 탐지할 경우 이 이벤트가 생성됩니다.

또한 이 이벤트는 네트워크 맵에 존재하지 않는 모니터링되는 네트워크 상의 서버와 관련된 NetFlow 데이터를 디바이스가 처리할 때도 생성됩니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 애플리케이션을 검색하는 네트워크 검색 규칙을 설정해야 합니다.

TCP 포트 닫힘

시스템이 호스트에서 닫힌 TCP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

TCP 포트 시간 초과

시스템이 네트워크 검색 정책에 정의된 간격 내에 TCP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다.

TCP 서버 정보 업데이트

시스템이 호스트에서 실행 중인 검색된 TCP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

TCP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

UDP 포트 닫힘

시스템이 호스트에서 닫힌 UDP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

UDP 포트 시간 초과

시스템이 네트워크 검색 정책에 정의된 간격 내에 UDP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다.

UDP 서버 정보 업데이트

시스템이 호스트에서 실행 중인 검색된 UDP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

UDP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

VLAN 태그 정보 업데이트

시스템이 호스트에 속하는 VLAN 태그에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

관련 항목

호스트 입력 이벤트 유형, 3043 페이지
네트워크 검색 데이터 스토리지 설정, 2556 페이지
애플리케이션 및 운영 체제 ID 충돌, 2380 페이지
네트워크 검색 ID 충돌 설정, 2552 페이지

호스트 입력 이벤트 유형

검색 이벤트의 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다.

사용자가 특정 작업(예: 수동으로 호스트 추가)을 수행할 때 생성되는 호스트 입력 이벤트를 시스템이 모니터링되는 네트워크에서 직접 변경 사항을 탐지(예: 전에 탐지되지 않던 호스트에서 트래픽 탐지)할 때 생성되는 검색 이벤트와 비교해보십시오.

네트워크 검색 정책을 수정하여, 시스템이 기록하는 호스트 입력 이벤트의 유형을 설정할 수 있습니다.

서로 다른 유형의 호스트 입력 이벤트가 제공하는 정보를 이해하면 어떤 이벤트를 기록하고 알림을 전송할지, 상관관계 정책에서 이러한 알림을 어떻게 사용할지를 좀 더 효과적으로 결정할 수 있습니

다. 또한 이벤트 유형의 이름을 알면 좀 더 효과적으로 이벤트를 검색할 수 있습니다. 다음은 서로 다른 유형의 호스트 입력 이벤트에 대한 설명입니다.

클라이언트 추가

사용자가 클라이언트를 추가할 경우 이 이벤트가 생성됩니다.

호스트 추가

사용자가 호스트를 추가할 경우 이 이벤트가 생성됩니다.

프로토콜 추가

사용자가 프로토콜을 추가할 경우 이 이벤트가 생성됩니다.

스캔 결과 추가

시스템이 Nmap 스캔의 결과를 호스트에 추가할 경우 이 이벤트가 생성됩니다.

포트 추가

사용자가 서버 포트를 추가할 경우 이 이벤트가 생성됩니다.

클라이언트 삭제

사용자가 시스템에서 클라이언트를 삭제할 경우 이 이벤트가 생성됩니다.

호스트/네트워크 삭제

사용자가 시스템에서 IP 주소 또는 서브넷을 삭제할 경우 이 이벤트가 생성됩니다.

프로토콜 삭제

사용자가 시스템에서 프로토콜을 삭제할 경우 이 이벤트가 생성됩니다.

포트 삭제

사용자가 시스템에서 서버 포트 또는 서버 포트 그룹을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 추가

사용자가 새 호스트 속성을 생성할 경우 이 이벤트가 생성됩니다.

호스트 특성 삭제

사용자가 사용자 정의 호스트 속성을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 삭제 값

사용자가 호스트 속성에 할당된 값을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 설정 값

사용자가 호스트에 대한 호스트 속성 값을 설정할 경우 이 이벤트가 생성됩니다.

호스트 특성 업데이트

사용자가 사용자 정의 호스트 속성의 정의를 변경할 경우 이 이벤트가 생성됩니다.

호스트 중요도 설정

사용자가 호스트에 대한 호스트 중요도 값을 설정 또는 수정할 경우 이 이벤트가 생성됩니다.

운영 시스템 정의 설정

사용자가 호스트에 대한 운영체제를 설정할 경우 이 이벤트가 생성됩니다.

서버 정의 설정

사용자가 서버에 대한 벤더 및 버전 정의를 설정할 경우 이 이벤트가 생성됩니다.

취약성 영향 자격 설정

취약성 영향 자격이 설정될 경우 이 이벤트가 생성됩니다.

영향 자격에 대해 사용 중인 취약성이 전역 레벨에서 비활성화되거나 전역 레벨에서 취약성이 활성화될 경우 이 이벤트가 생성됩니다.

취약성 설정 유효하지 않음

사용자가 취약성을 무효화 또는 검토할 경우 이 이벤트가 생성됩니다.

취약성 설정 유효함

전에 잘못된 것으로 표시되었던 취약성을 사용자가 검증할 경우 이 이벤트가 생성됩니다.

관련 항목

검색 이벤트 유형, 3039 페이지

검색 및 호스트 입력 이벤트 보기

검색 이벤트 워크플로를 사용하면 검색 이벤트와 호스트 입력 이벤트에서 데이터를 볼 수 있습니다. 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 검색 이벤트의 테이블 보기 및 호스트 보기 종료 페이지를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Hosts(**호스트**)** > **Discovery Events(**검색 이벤트**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 타임 윈도우 변경, 2815 페이지에 설명된 대로 시간 범위를 조정합니다.

  참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(검색 이벤트 필드, 3046 페이지 참조).

관련 항목

검색 및 ID 워크플로 사용, 3037 페이지

검색 이벤트 필드

다음은 검색 이벤트 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

시간

시스템이 이벤트를 생성한 시간

이벤트

검색 이벤트 유형 또는 호스트 입력 이벤트 유형.

IP 주소

이벤트와 관련된 호스트와 연결된 IP 주소

User(사용자**)**

이벤트가 생성되기 전 이벤트와 관련된 호스트에 로그인한 마지막 사용자. 권한 있는 사용자 이후 권한 없는 사용자만 로그인한 경우, 권한 있는 사용자가 호스트에 대한 현재 사용자로 유지됩니다(또 다른 권한 있는 사용자가 로그인하지 않는 한).

MAC 주소

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 주소. 이 MAC 주소는 이벤트와 관련된 호스트의 실제 MAC 주소일 수도 있고, 트래픽이 통과한 네트워크 디바이스의 MAC 주소일 수도 있습니다.

MAC Vendor(MAC 벤더)

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 공급업체

이 필드를 검색할 경우 **virtual_mac_vendor**를 입력하여 가상 호스트와 관련된 이벤트와 일치시킵니다.

포트

이벤트를 트리거한 트래픽에서 사용하는 포트(해당되는 경우)

설명

이벤트의 텍스트 설명

Domain(도메인)

호스트를 검색한 디바이스의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

이벤트를 생성한 매니지드 디바이스의 이름입니다. NetFlow 데이터를 기반으로 하는 새 호스트 및 새 서버 이벤트의 경우 이것이 해당 데이터를 처리한 매니지드 디바이스입니다.

관련 항목

이벤트 검색, 2825 페이지

호스트 데이터

시스템은 호스트를 탐지하고 관련 정보를 수집하여 호스트 프로파일을 작성할 때 이벤트를 생성합니다. Firepower Management Center 웹 인터페이스를 사용하여 호스트를 보고, 검색하고, 삭제할 수 있습니다.

호스트를 보는 동안 선택한 호스트를 기반으로 트래픽 프로필 및 규정 준수 화이트 목록을 생성할 수 있습니다. 또한 호스트 중요도 값(비즈니스 중요도를 지정)을 비롯한 호스트 속성을 호스트 그룹에 할당할 수 있습니다. 그런 다음 상관관계 규칙 및 정책 내에서 이러한 중요도 값, 화이트 목록 및 트래픽 프로필을 사용할 수 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지의 내용을 참조하십시오.

관련 항목

NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지

호스트 데이터 보기

Firepower Management Center를 사용하면 시스템에서 탐지한 호스트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

호스트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 미리 정의된 두 워크플로는 사용자의 제한 사항을 충족하는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 호스트 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Hosts(호스트)**를 선택합니다.
- 호스트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Hosts(호스트)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(호스트 데이터 필드, 3048 페이지 참조).
- 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)
- 특정 호스트에 호스트 속성을 할당합니다(선택한 호스트에 대해 호스트 속성 설정, 3056 페이지 참조).
- 특정 호스트에 대한 트래픽 프로파일을 생성합니다(선택한 호스트에 대한 트래픽 프로파일 생성, 3053 페이지 참조).
- 특정 호스트를 기반으로 컴플라이언스 화이트 목록을 생성합니다(선택한 호스트를 기반으로 규정준수 화이트리스트 생성, 3053 페이지 참조).

호스트 데이터 필드

시스템은 호스트를 검색하면 해당 호스트에 대한 데이터를 수집합니다. 여기에는 호스트의 IP 주소, 실행 중인 운영 체제 등이 포함될 수 있습니다. 그러한 정보 중 일부는 호스트의 테이블 보기에서 볼 수 있습니다.

다음은 호스트 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Seen(최종 확인**)**

시스템에서 마지막으로 탐지한 호스트 IP 주소 중 하나의 날짜 및 시간. Last Seen(최종 확인) 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 호스트 IP 주소 중 하나에 대해 새 호스트 이벤트를 생성할 때 업데이트됩니다.

호스트 입력 기능을 사용하여 업데이트된 운영 체제 데이터가 있는 호스트의 경우 Last Seen(최종 확인) 값은 데이터가 원래 추가된 날짜 및 시간을 나타냅니다.

IP Address(IP 주소)

호스트와 연결된 IP 주소

MAC Address(MAC 주소)

호스트에서 탐지한 NIC의 MAC 주소.

MAC Address 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Address 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

MAC Vendor(MAC 벤더)

호스트에서 탐지한 NIC의 MAC 하드웨어 공급업체.

MAC Vendor 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Vendor 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

이 필드를 검색할 경우 `virtual_mac_vendor`를 입력하여 가상 호스트와 관련된 이벤트와 일치시킵니다.

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Host Criticality(호스트 심각도)

호스트에 할당된 사용자 지정 중요도 값.

NetBIOS Name(NetBIOS 이름)

호스트의 NetBIOS 이름. NetBIOS 프로토콜을 실행하는 호스트만이 NetBIOS 이름을 가질 수 있습니다.

VLAN ID

호스트에서 사용하는 VLAN ID.

Hops(홉)

호스트를 탐지한 디바이스에서 호스트로의 네트워크 홉 수

Host Type(호스트 유형)

호스트의 유형. 호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 및 로드 밸런서 중 어떤 것이든 가능합니다.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

이 필드를 검색할 경우 `!host`를 입력하여 모든 네트워크 디바이스를 검색합니다.

Hardware(하드웨어)

모바일 디바이스용 하드웨어 플랫폼.

OS

다음 중 하나에 해당합니다.

- 호스트에서 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제(이름, 벤더 및 버전)
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 ID를 탐지하면 쉼표로 구분된 목록으로 표시합니다.

대시보드의 Custom Analysis 위젯에서 호스트 이벤트 보기를 호출할 경우 이 필드가 나타납니다. 이것은 또한 호스트 테이블 기반의 사용자 지정 테이블에 있는 필드 옵션이기도 합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS Conflict(OS 컨플릭트)

이 필드는 검색 전용입니다.

OS Vendor(OS 벤더)

다음 중 하나에 해당합니다.

- 호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제의 벤더
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 벤더를 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS Name(OS 이름)

다음 중 하나에 해당합니다.

- 호스트에서 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 이름을 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS Version(OS 버전)

다음 중 하나에 해당합니다.

- 호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 버전을 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

Source Type(소스 유형)

호스트의 운영 체제 ID를 설정하는 데 사용되는 소스의 유형입니다.

- 사용자: user_name
- 애플리케이션: app_name

- 스캐너: scanner_type(네트워크 검색 구성을 통해 추가된 Nmap 또는 스캐너)
- 시스템에서 탐지한 운영 체제용 `Firepower`

시스템에서는 운영 체제의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

신뢰

다음 중 하나에 해당합니다.

- 호스트에서 실행 중인 운영 체제의 ID에 대한 시스템의 신뢰도 비율 - 시스템에서 탐지한 호스트
- 100% - 호스트 입력 기능 또는 Nmap 스캐너 등 활성 소스에 의해 식별된 운영 체제
- `unknown` - 시스템이 운영 체제 ID를 확인할 수 없는 호스트 및 NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트

이 필드를 검색할 경우 `n/a`를 입력하여 NetFlow 데이터에 기반한 네트워크 맵에 추가된 호스트를 포함합니다.

Notes(참고)

Notes 호스트 속성의 사용자 정의 내용.

Domain(도메인)

호스트와 연결된 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

트래픽을 탐지한 매니지드 디바이스를 입력하거나, NetFlow 또는 호스트 입력 데이터를 처리한 디바이스를 입력합니다.

이 필드가 비어 있는 경우, 다음 조건 중 하나가 사실에 해당합니다.

- 네트워크 검색 정책에 정의된 대로, 호스트 상주 네트워크를 명시적으로 모니터링하지 않는 디바이스에 의해 호스트가 네트워크 맵에 추가되었습니다.
- 호스트가 호스트 입력 기능으로 추가되었으며 시스템에 의해 탐지되지 않았습니다.

Count(개수)

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 이 필드가 나타납니다.

관련 항목

이벤트 검색, 2825 페이지
운영 체제 ID 충돌, 3009 페이지

선택한 호스트에 대한 트래픽 프로파일 생성

트래픽 프로파일은 네트워크의 트래픽 프로파일로, 지정한 기간에 수집된 연결 데이터를 기반으로 합니다. 트래픽 프로파일을 생성한 후에는 프로파일을 기준으로 새 트래픽을 평가하여, 정상적인 것처럼 보일 수 있는 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

지정한 호스트 그룹에 대한 트래픽 프로파일을 생성하려면 Hosts 페이지를 사용할 수 있습니다. 트래픽 프로파일은 지정한 호스트 중 하나가 호스트를 시작하는 것으로 탐지된 연결을 기반으로 합니다. 프로파일을 생성하고자 하는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 호스트 워크플로의 테이블 보기에서 트래픽 프로파일을 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

단계 **2** 페이지의 하단에서 **Create Traffic Profile(**트래픽 프로파일 생성**)**을 클릭합니다.

단계 **3** 특정 요구에 맞게 트래픽 프로파일을 수정 및 저장합니다.

관련 항목

트래픽 프로파일 소개, 2623 페이지

선택한 호스트를 기반으로 규정준수 화이트리스트 생성

규정준수 화이트리스트를 사용하면 네트워크에서 허용한 운영체제와 클라이언트, 네트워크, 전송 또는 애플리케이션 프로토콜을 지정할 수 있습니다.

지정한 호스트 그룹의 호스트 프로파일을 기반으로 규정준수 화이트리스트를 생성하려면 Hosts(호스트) 페이지를 사용하면 됩니다. 화이트리스트를 생성하고자 사용하려는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 호스트 워크플로우의 테이블 보기에서 화이트리스트를 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

단계 **2** 페이지의 하단에서 **Create(**생성**)**화이트리스트를 클릭합니다.

단계 **3** 특정 요구에 맞게 화이트리스트를 수정 및 저장합니다.

관련 항목

컴플라이언스 화이트 목록 소개, 2565 페이지

호스트 속성 데이터

Firepower System은 탐지한 호스트에 대한 정보를 수집하고 이 정보를 사용하여 호스트 프로파일을 작성합니다. 그러나 분석가에게 제공하고자 하는, 네트워크의 호스트에 대한 추가 정보가 있을 수 있습니다. 호스트 프로파일에 메모를 추가하거나, 호스트의 비즈니스 중요도를 설정하거나, 선택한 다른 정보를 제공할 수 있습니다. 이러한 각각의 정보를 호스트 속성이라고 합니다.

호스트 프로파일 자격에 호스트 속성을 사용할 수 있습니다. 이러한 속성은 트래픽 프로파일 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙에 대한 응답에 속성 값을 설정할 수도 있습니다.

관련 항목

호스트 속성 보기, 3054 페이지
세트 속성값 교정 구성, 2644 페이지

호스트 속성 보기

Firepower Management Center를 사용하면 시스템에서 탐지한 호스트의 테이블을 호스트 속성과 함께 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

호스트 속성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 호스트 및 해당 속성을 나열하는 호스트 속성의 테이블 보기를 포함하며, 제약 조건에 맞는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 호스트 속성 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Host Attributes(호스트 속성)**를 선택합니다.
- 호스트 속성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(워크플로 전환)**를 클릭한 다음 **Attributes(속성)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(워크플로 전환)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(호스트 속성 데이터 필드, 3055 페이지 참조).

- 특정 호스트에 호스트 속성을 할당합니다(선택한 호스트에 대해 호스트 속성 설정, 3056 페이지 참조).

호스트 속성 데이터 필드

MAC 주소에 의해서만 식별되는 호스트는 속성 테이블에 표시되지 않습니다.

다음은 호스트 속성 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

IP Address(IP 주소)

호스트와 연결된 IP 주소

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Host Criticality(호스트 심각도)

엔터프라이즈에 사용자가 할당하는 호스트의 중요도. 정책 위반 및 응답을 이벤트와 관련된 호스트의 중요도에 맞추려면 상관관계 규칙 및 정책에 호스트 중요도를 사용할 수 있습니다. Low, Medium, High 또는 None의 호스트 중요도를 할당할 수 있습니다.

Notes(참고)

다른 분석가에게 보여줄 호스트에 대한 정보.

임의의 사용자 정의 호스트 속성, 컴플라이언스 화이트 목록 대상 포함

사용자 정의 호스트 속성의 값. 호스트 속성 테이블에는 각 사용자 정의 호스트 속성에 대한 필드가 포함되어 있습니다.

Domain(도메인)

호스트와 연결된 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Count(개수)

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 2825 페이지

선택한 호스트에 대해 호스트 속성 설정

호스트 워크플로에서 사전 정의된 호스트 속성 및 사용자 정의 호스트 속성을 구성할 수 있습니다.

프로시저

단계 **1** 호스트 워크플로에서 호스트 속성을 추가하려는 호스트의 옆에 있는 확인란을 선택합니다.

팁 정렬 및 검색 기능을 사용하여, 특정 속성을 할당할 호스트를 격리합니다.

단계 **2** 페이지의 하단에서 **Set Attributes(**속성 설정**)**를 클릭합니다.

단계 **3** 선택적으로, 선택한 호스트의 호스트 중요도를 설정합니다. **None(**없음**)**, **Low(**낮음**)**, **Medium(**중간**)** 또는 **High(**높음**)**를 선택할 수 있습니다.

단계 **4** 필요한 경우, 텍스트 상자에서 선택한 호스트의 호스트 프로파일에 메모를 추가합니다.

단계 **5** 선택적으로, 이미 구성한 사용자 정의 호스트 속성을 설정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

보안 침해 지표 데이터

Firepower System은 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 상호 연결하여 모니터링되는 네트워크의 호스트가 악의적인 수단에 의해 보안이 침해될 가능성이 있는지를 확인합니다. 이벤트 데이터의 특정 조합 및 빈도는 영향받는 호스트에서 IOC(보안 침해 지표) 태그를 트리거합니다.이러한 호스트의 IP 주소는 이벤트 보기에서 빨간색의 보안 침해된 호스트 아이콘으로 표시됩니다.

악성코드가 포함된 파일이 IOC로 태그가 지정된 지 300초 내에 다시 발견되는 경우, 또 다른 IOC가 생성되지 않습니다. 동일한 파일이 300초 이상 지나 발견되는 경우에는 새 IOC가 생성됩니다.

보안 침해 지표로 이벤트에 태그를 지정하도록 시스템을 구성하려면 보안 침해 지표 규칙 활성화, 2555 페이지를 참조하십시오.

관련 항목

보안 침해 지표 규칙 활성화, 2555 페이지

보안 침해 지표 데이터 보기 및 작업

Firepower Management Center을 사용하여 IOC가 표시된 테이블을 볼 수 있습니다. 찾고 있는 정보에 따라 이벤트 보기를 조작합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용하는 워크플로에 따라 표시되는 페이지가 달라집니다. 제약 조건을 충족하는 모든 호스트 의 호스트 프로파일이 포함된 프로파일 보기에서 사전 정의된 IOC 워크플로가 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

- 시스템에서 보안 침해 지표(Indications of compromise, IOC)를 탐지하고 태깅하려면 네트워크 검색 정책에서 IOC 기능을 활성화하고 하나 이상의 IOC 규칙을 활성화해야 합니다. 보안 침해 지표 규칙 활성화, 2555 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 웹 인터페이스의 어느 위치가 요구 사항을 충족하는 정보를 제공하는지 확인합니다.

다음 위치를 사용하여 보안 침해 지표 데이터를 보거나 보안 침해 데이터 작업을 할 수 있습니다.

- 이벤트 뷰어(분석 메뉴 아래) - 연결, 보안 인텔리전스, 침입, 악성코드, IOC 검색 이벤트 보기는 이벤트가 IOC를 트리거했는지 여부를 나타냅니다. IOC 규칙을 트리거한 AMP for Endpoints에 의해 생성된 악성코드 이벤트는 이벤트 유형 `AMP IOC`를 가지며, 보안 침해를 지정하는 이벤트 하위 유형과 함께 표시됩니다.
- 대시보드 - 대시보드에서는 Summary Dashboard(요약 대시보드)의 Threats(위협)에 호스트 IOC 태그와 시간이 지나면서 트리거된 새 IOC 규칙이 기본적으로 표시됩니다. Custom Analysis 위젯은 IOC 데이터를 기반으로 하는 사전 설정을 제공합니다.
- Context Explorer - Context Explorer의 Indications of Compromise(보안 침해 지표) 섹션에는 IOC 카테고리별 호스트의 그래프 및 호스트별 IOC 카테고리의 그래프가 표시됩니다.
- 네트워크 맵 페이지 - Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) 아래의 Indications of Compromise(보안 침해 지표)는 보안 침해 유형과 IP 주소에 따라 보안 침해 가능성이 있는 네트워크의 호스트를 그룹화합니다.
- 네트워크 파일 분석 경로 세부 정보 페이지 - Analysis(분석) > Files(파일) > Network File Trajectory(네트워크 파일 분석 경로) 아래 나열된 파일 세부 정보 페이지를 사용하여 네트워크에서 보안 침해 지표를 추적할 수 있습니다.
- 보안 침해 지표 페이지 - Analysis(분석) > Hosts(호스트) 메뉴 아래의 Indications of Compromise(호스트 보안 침해 지표) 페이지에는 IOC 태그에 따라 그룹화된 모니터링되는 호스트가 나열됩니다. 이 페이지의 워크플로를 사용하여 데이터로 드릴다운합니다.
- 호스트 프로파일 페이지 - 보안 침해 가능성이 있는 호스트의 호스트 프로파일에는 해당 호스트에 연결된 모든 IOC 태그가 표시되며, 이를 사용하여 IOC 태그를 확인하고 IOC 규칙 상태를 구성할 수 있습니다.

단계 **2** 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**) > Hosts(**호스트**) > Indications of Compromise(**보안 침해 지표**(IoC))**를 선택합니다.

호스트 IOC 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Indications of Compromise(**보안 침해 지표**)**를 선택합니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(보안 침해 지표 데이터 필드, 3058 페이지 참조).
- **IP Address(IP** 주소**)** 열의 **Compromised Host(**보안 침해된 호스트**)**를 클릭하여 보안 침해된 호스트의 호스트 프로파일을 봅니다.
- 목록에 더 이상 나타나지 않도록 IOC 이벤트를 확인된 것으로 표시합니다. 이렇게 하려면 수정할 IOC 이벤트 옆에 있는 확인란을 선택한 다음 **Mark Resolved(**확인된 것으로 표시**)**를 클릭합니다.
- **First Seen(**처음 확인 날짜**)** 또는 **Last Seen(**마지막 확인 날짜**)** 열에서 보기 ( )을 클릭하여 IOC를 트리거한 이벤트의 세부사항을 봅니다.
- 더 많은 옵션 보기: 테이블의 값을 마우스 오른쪽 단추로 클릭합니다.

보안 침해 지표 데이터 필드

다음은 보안 침해 지표(Indications of compromise, IOC) 테이블의 필드입니다. 모든 IOC 관련 테이블에 전체 필드가 포함되어 있지는 않습니다.

IP Address(IP 주소**)**

IOC를 트리거한 호스트와 연결된 IP 주소.

Category(카테고리**)**

표시된 감염 유형에 대한 짧은 설명(예: `Malware Executed` 또는 `Impact 1 Attack`).

이벤트 유형

특정 IOC와 연결된 식별자로, 이를 트리거한 이벤트를 가리킴.

설명

침해 가능성이 있는 호스트에 미치는 영향에 대한 설명(예: `This host may be under remote control`(이 호스트가 원격 제어 상태일 수 있습니다) 또는 `Malware has been executed on this host`(이 호스트에서 악성코드가 실행되었습니다)).

First Seen/Last Seen(최초 확인**/**최종 확인**)**

IOC를 트리거하는 이벤트가 발생한 최초의/가장 최근의 날짜 및 시간.

Domain(도메인**)**

IOC를 트리거한 호스트의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

관련 항목

이벤트 검색, 2825 페이지

단일 호스트에 대한 보안 침해 지표 규칙 상태 수정

네트워크 검색 정책에서 활성화된 경우 보안 침해 지표 규칙은 모니터링되는 네트워크의 모든 호스트에게 적용됩니다. 개별 호스트에 대한 규칙을 비활성화하여 유용하지 않은 IOC 태그를 방지할 수 있습니다(예: DNS 서버에 IOC 태그를 표시하지 않으려는 경우). 적용 가능한 네트워크 검색 정책에서 규칙이 비활성화된 경우, 특정 호스트에 대해 해당 규칙을 활성화할 수 없습니다.

프로시저

단계 **1** 호스트 프로파일의 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** **Edit Rule States(**규칙 상태 수정**)**를 클릭합니다.

단계 **3** 규칙의 **Enabled** 열에서 슬라이더를 클릭하여 규칙을 활성화 또는 비활성화합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

보안 침해 지표 태그의 소스 이벤트 보기

호스트 프로 파일 보안 침해 지표 섹션을 사용 하 여 IOC 태그를 트리거한 이벤트를 빠르게 이동할 수 있습니다. 이러한 이벤트를 분석하면 보안 침해 위협을 해결하기 위해 조치가 필요한지 및 필요한 조치를 결정하는 데 필요한 정보를 얻을 수 있습니다.

IOC 태그의 타임스탬프 옆에 있는 보기 ( )을 클릭하면 IOC 태그를 트리거한 이벤트만 표시하도록 제한된, 관련 이벤트 유형에 대한 이벤트의 테이블 보기로 이동합니다.

프로시저

단계 **1** 호스트 프로파일에서 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** 조사하려는 IOC 태그의 **First Seen** 또는 **Last Seen** 열에서 보기 ( )을 클릭합니다.

보안 침해 지표 태그 해결

보안 침해 지표(IOC) 태그에 의해 표시된 위협을 분석 및 해결했거나 IOC 태그가 오탐인 것으로 확인되는 경우, 이벤트를 해결된 것으로 표시할 수 있습니다. 해결된 것으로 표시된 이벤트는 호스트 프로파일에서 제거됩니다. 프로파일의 활성 IOC 태그가 모두 해결되면 보안 침해된 호스트 이 더 이상 나타나지 않습니다. 해결된 IOC에 대해 여전히 IOC 트리거링 이벤트가 표시될 수 있습니다.

IOC 태그를 트리거한 이벤트가 반복되는 경우, 호스트에 대해 IOC 규칙을 비활성화하지 않았다면 태그가 다시 설정됩니다.

프로시저

단계 **1** 호스트 프로파일에서 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 개별 IOC 태그를 해결된 것으로 표시하려면 해결하려는 태그의 오른쪽에 있는 삭제( )을 클릭합니다.
- 프로파일의 모든 IOC 태그를 해결된 것으로 표시하려면 **Mark All Resolved(**모두 해결된 것으로 표시**)**를 클릭합니다.

서버 데이터

Firepower System은 모니터링되는 네트워크 세그먼트의 호스트에서 실행 중인 모든 서버에 대한 정보를 수집합니다. 이 정보에는 다음이 포함됩니다.

- 서버 이름
- 서버가 사용하는 애플리케이션 및 네트워크 프로토콜
- 서버 공급업체 및 버전
- 서버를 실행하는 호스트와 연결된 IP 주소.
- 서버 통신 포트

시스템은 서버를 탐지하면 연결된 호스트가 이미 최대 서버 수에 도달하지 않은 경우 검색 이벤트를 생성합니다. Firepower Management Center 웹 인터페이스를 사용하여 서버 이벤트를 보고, 검색하고, 삭제할 수 있습니다.

상관관계 규칙의 기반을 서버 이벤트에 둘 수도 있습니다. 예를 들어, 시스템이 호스트 중 하나에서 실행 중인 채팅 서버(예: ircd)를 검색할 경우 상관관계 규칙을 트리거할 수 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지의 내용을 참조하십시오.

관련 항목

호스트 제한 및 검색 이벤트 로깅, 2443 페이지
NetFlow와 매니지드 디바이스 데이터의 차이점, 2382 페이지

서버 데이터 보기

Firepower Management Center를 사용하면 탐지한 서버의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

서버에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 모든 사전 정의 워크플로는 제약 조건을 충족하는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 서버 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Servers(서버)**를 선택합니다.
- 서버의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Servers(서버)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(서버 데이터 필드, 3061 페이지 참조).
- 수정할 서버에 대한 이벤트 옆에 있는 확인란을 선택한 다음 **Set Server Identity(**서버 **ID** 설정**)**를 클릭합니다.
- 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)

관련 항목

서버 ID 수정, 3014 페이지

서버 데이터 필드

다음은 서버에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Used(최종 사용**)**

네트워크에서 서버가 마지막으로 사용된 날짜 및 시간, 또는 호스트 입력 기능을 사용하여 서버가 원래 업데이트된 날짜 및 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 서버 정보 업데이트를 탐지할 때 업데이트됩니다.

IP Address(IP 주소**)**

서버를 실행하는 호스트와 연결된 IP 주소.

Port(포트**)**

서버가 실행 중인 포트.

Protocol(프로토콜**)**

서버에서 사용하는 네트워크 또는 전송 프로토콜.

Application Protocol(애플리케이션 프로토콜**)**

다음 중 하나에 해당합니다.

- 서버에 대한 애플리케이션 프로토콜의 이름
- `pending` - 여러 이유 중 하나 때문에 시스템이 서버를 긍정적으로 또는 부정적으로 식별할 수 없는 경우
- `unknown` - 시스템이 알려진 서버 핑거프린트를 기반으로 서버를 식별할 수 없는 경우 또는 서버가 호스트 입력을 통해 추가되었고 애플리케이션 프로토콜을 포함하지 않은 경우

Category, Tags, Risk, or Business Relevance for Application Protocols(애플리케이션 프로토콜의 카테고리**,** 태그**,** 위험 또는 사업 타당성**)**

애플리케이션 프로토콜에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Vendor(벤더**)**

다음 중 하나에 해당합니다.

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 공급업체
- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 공급업체를 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

Version(버전**)**

다음 중 하나에 해당합니다.

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 버전
- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 버전을 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

Web Application(웹 애플리케이션**)**

HTTP 트래픽에서 시스템에 의해 탐지된 페이로드 내용을 기반으로 하는 웹 애플리케이션. `HTTP`의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 일반 웹 브라우징 지정을 제공합니다.

Category, Tags, Risk, or Business Relevance for Web Applications(웹 애플리케이션의 카테고리, 태그, 위험 또는 사업 타당성**)**

웹 애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Hits(히트**)**

서버에 액세스한 횟수. 호스트 입력 기능을 사용하여 추가된 서버의 경우 이 값은 항상 0입니다.

Source Type(소스 유형**)**

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type(네트워크 검색 구성을 통해 추가된 Nmap 또는 스캐너)
- Firepower System에서 탐지된 서버의 `Firepower`, `Firepower Port Match` 또는 `Firepower Pattern Match`
- NetFlow 데이터를 사용하여 추가된 서버의 `NetFlow`

Domain(도메인**)**

서버를 실행하는 호스트의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스**)**

트래픽을 탐지한 매니지드 디바이스를 입력하거나, NetFlow 또는 호스트 입력 데이터를 처리한 디바이스를 입력합니다.

Current User(현재 사용자**)**

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Count(개수**)**

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 이 필드가 나타납니다.

관련 항목

이벤트 검색, 2825 페이지

네트워크 검색 데이터 스토리지 설정, 2556 페이지

애플리케이션 및 애플리케이션 상세정보 데이터

모니터링되는 호스트가 다른 호스트에 연결되면, 시스템은 많은 경우 어떤 애플리케이션이 사용되었는지를 확인할 수 있습니다. Firepower System에서는 이메일, 인스턴트 메시징, 피어 투 피어, 웹 애플리케이션 및 기타 유형의 애플리케이션 사용을 탐지합니다.

탐지된 각 애플리케이션에 대해 시스템은 애플리케이션을 사용한 IP 주소, 제품, 버전, 탐지된 사용 횟수 등을 로깅합니다. 웹 인터페이스를 사용하여 애플리케이션 이벤트를 보고, 검색하고, 삭제할 수 있습니다. 또한 호스트 입력 기능을 사용하여 호스트의 애플리케이션 데이터를 업데이트할 수 있습니다.

어떤 애플리케이션이 어떤 호스트에서 실행 중인지 안다면, 이를 통해 호스트 프로파일 자격을 생성할 수 있습니다. 이 자격은 트래픽 프로파일 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙의 기반을 애플리케이션 탐지에 둘 수도 있습니다. 예를 들어 직원이 특정 메일 클라이언트를 사용하도록 하려면, 호스트 중 하나에서 다른 메일 클라이언트가 실행 중임을 시스템에서 탐지할 때 상관관계 규칙을 트리거할 수 있습니다.

각 Firepower System 업데이트의 릴리스 노트와 각 VDB 업데이트의 권고를 꼼꼼히 읽으면 Firepower의 애플리케이션 탐지기에 대한 최신 정보를 얻을 수 있습니다.

분석을 위해 애플리케이션 데이터를 수집 및 저장하려면 네트워크 검색 정책에서 애플리케이션 탐지를 활성화하십시오.

애플리케이션 데이터 보기

Firepower Management Center를 사용하면 탐지한 애플리케이션의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

애플리케이션에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 애플리케이션 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Application Details(**애플리케이션 세부 정보**)**를 선택합니다.
- 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Clients(**클라이언트**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.

- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(애플리케이션 데이터 필드, 3065 페이지 참조).
- 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션 옆에 있는 **Application Detail View(**애플리케이션 세부 사항 보기**)**를 클릭하여 특정 애플리케이션의 Application Detail View(애플리케이션 세부 사항 보기)를 엽니다.
- 이벤트 값에서 마우스 오른쪽 버튼으로 클릭하여 Firepower 시스템 외부에서 소스의 데이터를 봅니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지 섹션을 참조해 주십시오.
- 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택하여 이벤트에 대한 인텔리전스를 수집합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지를 참고하십시오.

애플리케이션 데이터 필드

알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다.

다음은 애플리케이션 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Application(애플리케이션**)**

탐지된 애플리케이션의 이름

IP Address(IP 주소**)**

애플리케이션을 사용하는 호스트와 연결된 IP 주소

Type(유형**)**

애플리케이션 유형:

애플리케이션 프로토콜

호스트 간의 통신을 나타냅니다.

클라이언트 애플리케이션

호스트에서 실행 중인 소프트웨어를 나타냅니다.

Web Applications

HTTP 트래픽에 대한 콘텐츠 또는 요청 URL을 나타냅니다.

카테고리

가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.

태그

애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.

위험

조직의 보안 정책을 거스를 수 있는 용도로 애플리케이션이 사용될 가능성. 애플리케이션 위험의 범위는 Very Low(매우 낮음)에서 Very High(매우 높음)까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Risk, Client Risk, Web Application Risk의 세 가지 중 최고(사용 가능한 경우).

Business Relevance(사업 타당성**)**

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성. 애플리케이션 비즈니스 연관성의 범위는 Very Low(매우 낮음)에서 Very High(매우 높음)까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Business Relevance, Client Business Relevance, Web Application Business Relevance의 세 가지 중 최저(사용 가능한 경우).

Current User(현재 사용자**)**

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Domain(도메인**)**

애플리케이션을 사용하는 호스트의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Count(개수**)**

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 2825 페이지

애플리케이션 세부사항 데이터 보기

Firepower Management Center를 사용하면 탐지한 애플리케이션 세부사항의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

애플리케이션 세부사항에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 애플리케이션 세부사항 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Application Details(**애플리케이션 세부 정보**)**를 선택합니다.
- 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Clients(**클라이언트**)**를 선택하십시오.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(애플리케이션 세부사항 데이터 필드, 3067 페이지 참조).
- 클라이언트 옆에 있는 **Application Detail View(**애플리케이션 세부사항 보기**)** 를 클릭하여 특정 애플리케이션의 애플리케이션 세부사항 보기를 엽니다.
- 이벤트 값에서 마우스 오른쪽 버튼으로 클릭하여 Firepower 시스템 외부에서 이용할 수 있는 소스의 데이터를 봅니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지 섹션을 참조해 주십시오.
- 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택하여 이벤트에 대한 인텔리전스를 수집합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지를 참고하십시오.

애플리케이션 세부사항 데이터 필드

알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다.

다음은 애플리케이션 세부사항 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Used(최종 사용**)**

애플리케이션이 마지막으로 사용된 시간 또는 호스트 입력 기능을 사용하여 애플리케이션 데이터가 업데이트된 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 애플리케이션 정보 업데이트를 탐지할 때 업데이트됩니다.

IP Address(IP 주소**)**

애플리케이션을 사용하는 호스트와 연결된 IP 주소

Client(클라이언트**)**

애플리케이션의 이름. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

Version(버전**)**

애플리케이션의 버전

Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications(클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션의 카테고리, 태그, 위험 또는 사업 타당성**)**

애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Application Protocol(애플리케이션 프로토콜**)**

애플리케이션에서 사용하는 애플리케이션 프로토콜. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

Web Application(웹 애플리케이션**)**

HTTP 트래픽에서 시스템에 의해 탐지된 페이로드 내용 또는 URL을 기반으로 하는 웹 애플리케이션. HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 여기에서 일반 웹 브라우징 지정을 제공합니다.

Hits(히트**)**

시스템이 사용 중인 애플리케이션을 탐지한 횟수. 호스트 입력 기능을 사용하여 추가된 애플리케이션의 경우 이 값은 항상 `0`입니다.

Domain(도메인**)**

애플리케이션을 사용하는 호스트의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Domain(디바이스**)**

애플리케이션 세부사항을 포함하는 검색 이벤트를 생성한 디바이스.

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Count(개수)

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 2825 페이지
네트워크 검색 데이터 스토리지 설정, 2556 페이지

취약성 데이터

Firepower System에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트에 연결된 취약성을 식별할 수 있습니다. 호스트에서 실행 중인 운영 체제, 서버 및 클라이언트는 연결된 취약성 집합이 서로 다릅니다.

Firepower Management Center를 사용하여 다음을 수행할 수 있습니다.

- 각 호스트의 취약성을 추적하고 검토합니다.
- 호스트를 패치하거나 그 밖의 방법으로 호스트가 취약성에 대해 면역력이 있다고 판단한 후 취약성을 비활성화합니다.

서버가 사용하는 애플리케이션 프로토콜이 Firepower Management Center 구성에서 매핑되어 있지 않으면 공급업체가 없는 서버 및 버전이 없는 서버의 취약성은 매핑되지 않습니다. 공급업체가 없는 클라이언트 및 버전이 없는 클라이언트의 취약성은 매핑할 수 없습니다.

관련 항목

서버의 취약성 매핑, 1389 페이지

취약성 데이터 필드

언급된 경우를 제외하고 이러한 필드는 **Analysis(분석) > Hosts(호스트) > Vulnerabilities(취약점)** 아래의 모든 페이지에 표시됩니다.

Count(개수)

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)의 취약성에 연결된 식별 번호.

NVD(National Vulnerability Database)에서 이 취약점에 대한 세부 정보를 보려면 CVE ID를 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명 보기**)**를 선택합니다.

게시 날짜

취약성이 게시된 날짜입니다.

설명

NVD(National Vulnerability Database)의 취약점에 대한 간략한 설명입니다.

전체 설명을 보려면 CVE ID를 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명 보기**)**를 선택하여 NVD(National Vulnerability Database)에서 세부 정보를 봅니다.

영향

"취약점 영향"(아래)을 참조하십시오.

영향 자격

이 필드는 Vulnerability Details(취약점 세부 사항) 페이지에서만 사용할 수 있습니다.

드롭다운 목록을 사용하여 취약성을 활성화 또는 비활성화합니다. Firepower Management Center는 영향 상관관계에서 비활성화된 취약성을 무시합니다.

여기서 지정하는 설정은 시스템 전체에서 취약성의 취급 방법을 결정하며, 값을 선택한 호스트 프로파일로 제한되지 않습니다.

원격

취약성이 원격으로 악용될 수 있는지 여부(`TRUE`/`FALSE`)를 나타냅니다.

심각도

NVD(National Vulnerability Database)의 기본 점수 및 CVSS(Common Vulnerability Scoring System) 점수입니다.

Snort ID

Snort ID(SID) 데이터베이스의 취약성에 연결된 ID 번호입니다. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성은 둘 이상의 SID와 연결될 수 있습니다(SID와 연결되지 않을 수도 있음). 취약성이 둘 이상의 SID에 연결된 경우, 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

SVID

시스템에서 취약성 추적에 사용하는 취약성 ID 번호.

이 취약점에 대한 세부 정보를 보려면 보기 ( )을(를) 클릭합니다.

취약점 영향/영향

0에서 10까지의 범위에서 취약성의 심각도를 나타내며, 10이 가장 심각합니다.

관련 항목

이벤트 검색, 2825 페이지

취약성 비활성화

취약성을 비활성화하면 시스템은 해당 취약성을 사용하여 침입 영향 상관관계를 평가할 수 없습니다. 네트워크의 호스트에 패치를 적용하거나 그 밖의 방법으로 호스트가 취약성의 영향을 받지 않는다고 판단한 후 취약성을 비활성화할 수 있습니다. 시스템이 해당 취약성의 영향을 받는 새 호스트를 검색하면, 이 취약성은 해당 호스트에 대해 유효한 것으로 간주됩니다(따라서 자동으로 비활성화되지 않음).

IP 주소로 제한되지 않은 취약성 워크플로 내에서 취약성을 비활성화하면 네트워크에서 탐지된 모든 호스트에 대해 취약성이 비활성화됩니다. 취약성 워크플로 내의 취약성은 다음에서만 비활성화할 수 있습니다.

- 기본 취약성 워크플로의 두 번째 페이지인 **Vulnerabilities on the Network(**네트워크의 취약성**)**. 여기에는 네트워크의 호스트에 해당되는 취약성만 표시됩니다.
- 검색을 사용하여 IP 주소를 기반으로 제한한 맞춤형 또는 사전 정의된 취약성 워크플로의 페이지.

네트워크 맵을 사용하거나 호스트의 호스트 프로파일을 사용하거나 취약성을 비활성화하려는 호스트의 IP 주소를 기반으로 취약성 워크플로를 제한하여 단일 호스트의 취약성을 비활성화할 수 있습니다. 연결된 IP 주소가 여러 개인 호스트의 경우, 이 기능은 해당 호스트의 선택된 단일 IP에만 적용됩니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

관련 항목

개별 호스트 취약성 비활성화, 3027 페이지
개별 취약성 비활성화, 3027 페이지
다중 취약성 비활성화, 3073 페이지

취약성 데이터 보기

Firepower Management Center를 사용하여 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 취약성의 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 탐지된 호스트가 취약성을 보이는지 여부와 상관없이 테이블 보기에는 데이터베이스의 각 취약성에 대한 행이 포함되어 있습니다. 사전 정의 워크플로의 두 번째 페이지에는 네트워크에서 탐지된 호스트에 적용되는 각 취약성의 행(비활성

화하지 않은)이 포함되어 있습니다. 사전 정의 워크플로는 제약 조건을 충족하는 모든 취약성에 대한 자세한 설명이 포함된 취약성 세부사항 보기에서 종료됩니다.

팁 단일 호스트 또는 호스트 집합에 적용되는 취약성을 보려면 호스트의 IP 주소 또는 IP 주소 범위를 지정하여 취약성 검색을 수행하십시오.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

취약성 테이블은 다중 도메인 구축에서 도메인에 의해 제한되지 않습니다.

프로시저

단계 **1** 취약성 테이블에 액세스합니다.

- 사전 정의된 취약성 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택합니다.
- 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities(**취약성**)**를 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 현재 취약한 호스트의 침입 영향 상관관계에 더 이상 사용되지 않도록 취약성을 비활성화합니다(다중 취약성 비활성화, 3073 페이지 참조).
- SVID 열에서 보기 ( )을 클릭하여 취약성의 세부사항을 봅니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다. 취약성 세부사항 보기, 3072 페이지에서 추가 세부 정보를 보는 옵션을 참조하십시오.
- 제목을 마우스 오른쪽 버튼으로 클릭하고 **Show Full Text(**전체 텍스트 표시**)**를 선택하여 취약성 제목의 전체 텍스트를 확인합니다.

취약성 세부사항 보기

프로시저

다음 방법 중 하나로 취약성 세부사항을 볼 수 있습니다.

- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택하고 SVID 옆에 있는 보기 ( )를 클릭합니다.
- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Third-Party Vulnerabilities(**서드파티 취약성**)**를 선택하고 SVID 옆에 있는 보기 ( )를 클릭합니다.
- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**를 선택하고 **Vulnerabilities(**취약성**)**을 클릭합니다.

- 취약성의 영향을 받는 호스트의 프로필을 보고(**Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**, **Hosts(**호스트**)**를 클릭하고, 드릴다운해서 조사하는 호스트를 클릭합니다), 프로필의 **Vulnerabilities(**취약성**)** 섹션을 확장합니다.
- **Analysis(**분석**)> Hosts(**호스트**)> Vulnerabilities(**취약성**)** 아래의 테이블에서 **CVE ID** 열의 값을 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명보기**)**를 선택하여 NVD(National Vulnerabilities Database) 웹 사이트에서 해당 CVE를 봅니다.

다중 취약성 비활성화

IP 주소로 제한되지 않은 취약성 워크플로 내에서 취약성을 비활성화하면 네트워크에서 탐지된 모든 호스트에 대해 취약성이 비활성화됩니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 **1** 취약성 테이블에 액세스합니다.

- 사전 정의된 취약성 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택합니다.
- 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities(**취약성**)**를 선택합니다.

단계 **2** **Vulnerabilities on the Network(**네트워크의 취약성**)**를 클릭합니다.

단계 **3** 비활성화하려는 취약성 옆의 확인란을 선택합니다.

단계 **4** 페이지 하단의 **Review(**검토**)**를 클릭합니다.

관련 항목

개별 호스트 취약성 비활성화, 3027 페이지
개별 취약성 비활성화, 3027 페이지

서드파티 취약성 데이터

Firepower System에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트에 연결된 취약성을 식별할 수 있습니다.

서드파티 애플리케이션에서 가져온 네트워크 맵 데이터로 시스템의 취약성 데이터를 보강할 수 있습니다. 그러려면 조직이 스크립트를 작성하거나 명령줄 파일 가져오기를 만들어 데이터를 가져올 수 있어야 합니다. 자세한 내용은 *Firepower System Host Input API* 설명서을 참조하십시오.

가져온 데이터를 영향 상관관계에 포함하려면 서드파티 취약성 정보를 데이터베이스의 운영 체제 및 애플리케이션 정의에 매핑해야 합니다. 서드파티 취약성 정보를 클라이언트 정의에 매핑할 수는 없습니다.

서드파티 취약성 데이터 보기

호스트 입력 기능을 사용하여 서드파티 취약성 데이터를 가져왔으면 Firepower Management Center를 사용하여 서드파티 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

서드파티 취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 서드파티 취약성 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Third-Party Vulnerabilities(서드파티 취약성)**를 선택합니다.
- 서드파티 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, **(switch workflow)(워크플로 전환)**를 클릭한 다음 **Vulnerabilities by Source(소스별 취약성)** 또는 **Vulnerabilities by IP Address(IP 주소별 취약성)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(워크플로 전환)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(서드파티 취약성 데이터 필드, 3074 페이지 참조).
- SVID 열에서 보기 ( )를 클릭하여 서드파티 취약성의 취약성 세부 사항을 봅니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다.

서드파티 취약성 데이터 필드

다음은 서드파티 취약성 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Vulnerability Source

서드파티 취약성의 소스(예: QualysGuard 또는 NeXpose).

취약성 **ID**

소스의 취약성과 연결된 ID 번호.

IP 주소

취약성의 영향을 받는 호스트와 연결된 IP 주소.

Port(포트**)**

취약성이 특정 포트에서 실행 중인 서버와 연결된 경우 포트 번호.

Bugtraq ID

Bugtraq 데이터베이스의 취약성과 관련된 ID 번호입니다. (http://www.securityfocus.com/bid/)

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)의 취약성에 연결된 식별 번호.

SVID

시스템이 취약성 추적에 사용하는 레거시 취약성 식별 번호.

SVID에 대한 취약성 세부사항에 액세스하려면 보기 ( )을 클릭합니다.

Snort ID

Snort ID(SID) 데이터베이스의 취약성에 연결된 ID 번호입니다. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성은 둘 이상의 SID와 연결될 수 있습니다(SID와 연결되지 않을 수도 있음). 취약성이 둘 이상의 SID에 연결된 경우, 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

직함

취약성의 제목입니다.

설명

취약성에 대한 간단한 설명.

도메인

취약성이 있는 호스트의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Count(개수**)**

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 2825 페이지

활성 세션, 사용자 및 사용자 활동 데이터

ID 소스는 활성 세션 데이터, 사용자 데이터, 사용자 활동 데이터를 수집합니다. 데이터는 개별 사용자 관련 워크플로에 표시됩니다.

- 활성 세션 - 이 워크플로는 네트워크의 모든 현재 사용자 세션을 표시합니다. 여러 활성 세션을 동시에 실행하는 단일 사용자는이 테이블에서 여러 행을 차지합니다. 이 워크플로에 표시되는 사용자 데이터 유형에 대한 자세한 내용은 활성 세션 데이터, 3083 페이지를 참조하십시오.
- 사용자 - 이 워크플로는 네트워크에서 보이는 모든 사용자를 표시합니다. 단일 사용자는 이 테이블에서 단일 행을 차지합니다. 이 워크플로에 표시되는 사용자 데이터 유형에 대한 자세한 내용은 사용자 데이터, 3084 페이지를 참조하십시오.
- 사용자 활동 - 이 워크플로는 네트워크에서 보이는 모든 사용자 활동을 표시합니다. 사용자 활동의 인스턴스가 여러 개 있는 단일 사용자는 이 테이블에서 여러 행을 차지합니다. 이 워크플로에 표시되는 사용자 활동 유형에 대한 자세한 내용은 사용자 활동 데이터, 3087 페이지를 참조하십시오.

이러한 워크플로를 채우는 ID 소스에 대한 자세한 내용은 사용자 ID 소스 정보를 참조하십시오.

사용자 관련 필드

사용자 관련 데이터는 활성 세션, 사용자, 사용자 활동 테이블에 표시됩니다.

표 ***337:*** 활성 세션, 사용자, 사용자 활동 필드 설명

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
활성 세션 수	사용자와 연결된 활성 세션의 수.	아니요	예	아니요
인증 유형	인증 유형: `No Authentication`(인증 없음), `Passive Authentication`(패시브 인증), `Active Authentication`(액티브 인증), `Guest Authentication`(게스트 인증), `Failed Authentication`(실패한 인증) 또는 `VPN Authentication`(VPN 인증) 각 인증 유형에 지원되는 ID 소스에 대한 자세한 내용은 사용자 ID 소스 정보를 참조하십시오.	예	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
개수	참고 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count(**개수**)** 필드가 표시됩니다. 테이블에 따라 특정 행에 표시되는 정보와 일치하는 세션, 사용자 또는 활동 이벤트의 수입니다.	예	예	예
현재 **IP**	사용자가 로그인하는 호스트와 연결된 IP 주소. 사용자의 활성 세션이 없는 경우 사용자 테이블에서 이 필드는 비어 있습니다.	예	예	아니요
Department(부서**)**	영역에서 가져온 사용자의 부서. 서버의 사용자와 명시적으로 연결된 부서가 없는 경우, 부서는 서버가 할당하는 기본 그룹으로 나열됩니다. 예를 들면 Active Directory에서는 `Users (ad)` 입니다. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • Firepower Management Center에서는 FMC 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우).	예	예	아니요
설명	세션, 사용자 또는 사용자 활동에 대한 추가 정보(제공되는 경우).	아니요	아니요	예
디바이스	트래픽 기반 탐지 또는 액티브 인증 ID 소스에서 탐지된 사용자 활동의 경우, 사용자를 식별한 디바이스의 이름입니다. 다른 사용자 활동 유형의 경우, 관리하는 Firepower Management Center. 참고 고가용성 구축에서 VPN을 구성한 경우 활성 VPN 세션에 대해 표시되는 디바이스 이름은 사용자 세션을 식별한 기본 또는 보조 디바이스일 수 있습니다.	예	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
검색 애플리케이션	사용자를 탐지하는 데 사용된 애플리케이션 또는 프로토콜. • 트래픽 기반 탐지에서 탐지된 사용자 활동의 경우 다음 중 하나에 해당: ldap, pop3, imap, oracle, sip, ftp, http, mdns, aim. 참고 사용자는 SMTP 로그인에 기반한 데이터베이스에 추가되지 않습니다. • 모든 기타 사용자 활동의 경우: ldap	예	예	예
Current IP Domain(현재 **IP** 도메인**)/Domain(**도메인**)**	활성 세션 테이블에서 사용자 활동이 탐지된 멀티테넌시 도메인. 사용자 테이블에서 사용자의 영역과 연결된 멀티테넌시 도메인. 사용자 활동 테이블에서 사용자 활동이 탐지된 멀티테넌시 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.	예	예	예
E-Mail(이메일**)**	사용자의 이메일 주소. 다음과 같은 경우 이 필드는 비어 있습니다. • AIM 로그인을 통해 사용자가 데이터베이스에 추가된 경우. • LDAP 로그인을 통해 사용자가 데이터베이스에 추가되었으며 LDAP 서버의 사용자와 연결된 이메일 주소가 없는 경우.	예	예	아니요
종료 포트	TS 에이전트에서 사용자를 보고하고 세션이 현재 활성화된 경우, 이 필드는 사용자에게 할당된 포트 범위의 종료 값을 식별합니다. 사용자의 TS 에이전트 세션이 비활성화되어 있거나 다른 ID 소스에서 사용자를 보고한 경우 이 필드는 비어 있습니다.	예	아니요	예
Endpoint Location(엔드포인트 위치**)**	ISE에서 식별된 사용자를 인증하기 위해 ISE가 사용되는 네트워크 디바이스의 IP 주소. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
엔드포인트 프로파일	Cisco ISE에서 식별된 사용자의 엔드포인트 디바이스 유형. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
Event(이벤트**)**	사용자 활동 이벤트 유형.	아니요	아니요	예
이름	영역에서 가져온 사용자의 이름. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • Firepower Management Center에서는 FMC 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 이름이 없는 경우.	예	예	아니요
IP 주소	**User Login(**사용자 로그인**)** 사용자 활동의 경우, 로그인과 관련된 IP 주소 또는 내부 IP 주소: • LDAP, POP3, IMAP, FTP, HTTP, MDNS, AIM 로그인 — 사용자 호스트의 주소 • SMTP 및 Oracle 로그인 — 서버의 주소 • SIP 로그인 — 세션 시작 주체의 주소 IP 주소가 연결되어 있다고 해서 사용자가 해당 IP 주소의 현재 사용자라는 의미는 아닙니다. 권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
성	영역에서 가져온 사용자의 성. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • Firepower Management Center에서는 FMC 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 성이 없는 경우.	예	예	아니요
최종 확인	사용자의 세션이 마지막으로 시작된(또는 사용자 데이터가 업데이트된) 날짜 및 시간.	예	예	아니요
로그인 시간	사용자의 세션이 시작된 날짜 및 시간.	예	아니요	아니요
전화	영역에서 가져온 사용자의 전화 번호. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • Firepower Management Center에서는 FMC 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 전화 번호가 없는 경우.	예	예	아니요
영역	사용자와 연결된 ID 영역.	예	예	예
Security Group Tag(보안 그룹 태그**)**	패킷이 신뢰할 수 있는 TrustSec 네트워크에 들어갔을 때 Cisco TrustSec에서 적용한 SGT(Security Group Tag) 속성. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
Session Duration(세션 기간**)**	**Login Time(**로그인 시간**)**과 현재 시간에서 계산된 사용자 세션의 기간.	예	아니요	아니요

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
시작 포트	TS 에이전트에서 사용자를 보고하고 세션이 현재 활성화된 경우, 이 필드는 사용자에게 할당된 포트 범위의 시작 값을 식별합니다. 사용자의 TS 에이전트 세션이 비활성화되어 있거나 다른 ID 소스에서 사용자를 보고한 경우 이 필드는 비어 있습니다.	예	아니요	예
시간	시스템이 사용자 활동을 탐지한 시간.	아니요	아니요	예
사용자	이 필드에는 최소한 사용자의 영역 및 사용자 이름이 표시됩니다. 예를 들어 `Lobby\jsmith`의 경우 Lobby는 영역이고 jsmith는 사용자 이름입니다. 영역이 LDAP 서버에서 사용자 추가 데이터를 다운로드하고 시스템이 이를 사용자와 연결할 경우, 이 필드에는 또한 사용자의 이름, 성, 유형이 표시됩니다. 예를 들어 `John Smith (Lobby\jsmith, LDAP)`의 경우 John Smith는 사용자의 이름이고 LDAP는 유형입니다. 참고 트래픽 기반 탐지는 실패한 AIM 로그인을 기록할 수 있으므로, Firepower Management Center에서는 잘못된 AIM 사용자(예: 사용자가 사용자 이름의 철자를 잘못 쓴 경우)를 저장할 수 있습니다.	예	예	아니요
Username	사용자와 연결된 사용자 이름.	예	예	예
VPN Bytes In(VPN 바이트 인**)**	원격 액세스 VPN에서 보고된 사용자 활동의 경우, Firepower Threat Defense에서 원격 피어 또는 클라이언트로부터 수신된 총 바이트 수입니다. 참고 사용자의 VPN 세션이 종료되면 수신된 총 바이트 수를 볼 수 있습니다. 진행 중인 VPN 세션의 경우, 이는 동적 카운터가 아닙니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
VPN Bytes Out(VPN 바이트 아웃**)**	원격 액세스 VPN에서 보고된 사용자 활동의 경우, Firepower Threat Defense에서 원격 피어 또는 클라이언트로 전송한 총 바이트 수입니다. 참고 사용자의 VPN 세션이 종료되면 전송한 총 바이트 수를 볼 수 있습니다. 진행 중인 VPN 세션의 경우, 이는 동적 카운터가 아닙니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN Client Application(VPN 클라이언트 애플리케이션**)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 원격 사용자의 AnyConnect VPN 클라이언트 애플리케이션입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN Client Country(VPN 클라이언트 국가**)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, AnyConnect VPN 클라이언트에서 보고된 국가 이름입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN Client OS(VPN 클라이언트 **OS)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, AnyConnect VPN 클라이언트에서 보고된 원격 사용자의 엔드포인트 운영 체제입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN Client Public IP(VPN 클라이언트 공개 **IP)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 공개적으로 라우팅 가능한 AnyConnect VPN 클라이언트 디바이스의 IP 주소입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN Connection Duration(VPN 연결 지속 시간**)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 세션이 활성화된 총 시간(HH:MM:SS)입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN Connection Profile(VPN 연결 프로파일**)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, VPN 세션에서 사용된 연결 프로파일(터널 그룹)의 이름입니다. 연결 프로파일은 원격 액세스 VPN 정책의 일부입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
VPN Group Policy(VPN 그룹 정책**)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, VPN 세션을 설정했을 때 클라이언트에 할당된 그룹 정책의 이름입니다. 이러한 정책은 VPN 연결 프로파일과 연결된 정적으로 할당된 그룹 정책이거나, RADIUS가 인증에 사용된 경우 동적으로 할당된 그룹 정책입니다. RADIUS 서버에서 할당한 경우, 이 그룹 정책은 VPN 연결 프로파일에 구성된 고정 정책을 재정의합니다. 그룹 정책은 원격 액세스 VPN 정책의 사용자 그룹에 대한 일반 속성을 구성합니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN Session Type(VPN 세션 유형**)**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 세션의 유형(LAN 대 LAN 또는 원격)입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예

활성 세션 데이터

Analysis(분석**)** > **Users(**사용자**)** > **Active Sessions(**활성 세션**)** 워크플로에는 현재 사용자 세션에 대한 선택 정보가 표시됩니다. 네트워크의 한 사용자가 여러 세션을 동시에 실행 중인 경우, Firepower System은 세션이 다음과 같은 상태인지 여부를 고유하게 식별할 수 있습니다.

- 세션에 고유한 **IP Address(IP** 주소**)** 값이 있는지 식별합니다.
- 세션에 고유한 **Current IP Domain(**현재 **IP** 도메인**)** 값이 있는지 식별합니다.
- 다른 ID 소스에서 인증되었는지 식별합니다.
- 다른 ID 영역과 연결되었는지 식별합니다.

시스템에 저장된 사용자 및 사용자 활동 데이터에 대한 자세한 내용은 사용자 데이터, 3084 페이지 및 사용자 활동 데이터, 3087 페이지를 참조하십시오.

일반적인 사용자 관련 이벤트 문제 해결에 대한 자세한 내용은 영역 및 사용자 다운로드 문제 해결, 2480 페이지을 참조하십시오. Remote Access VPN 문제 해결에 대한 자세한 내용은 을 참조하십시오.Firepower Threat Defense VPN 문제 해결, 1235 페이지

활성 세션 데이터 보기

활성 세션의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용자에게 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 사용자를 나열하는 사용자의 테이블 보기를 포함하며 사용자 세부사항 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 사용자 세부사항 페이지는 제약 조건을 충족하는 모든 사용자에 대한 정보를 제공합니다.

프로시저

단계 **1** 사용자 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Users(**사용자**)** > **Active Sessions(**활성 세션**)**를 선택합니다.
- 활성 세션의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음, **Active Sessions(**활성 세션**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(활성 세션 데이터, 3083 페이지 및 사용자 관련 필드, 3076 페이지 참조).

사용자 데이터

ID 소스가 아직 데이터베이스에 없는 사용자의 사용자 로그인을 보고하면, 이러한 로그인 유형을 특별히 제한하지 않은 경우 해당 사용자는 데이터베이스에 추가됩니다.

시스템은 다음 중 한 가지 상황이 발생할 경우 사용자 데이터베이스를 업데이트합니다.

- Firepower Management Center의 사용자가 사용자 테이블에서 권한 없는 사용자를 수동으로 삭제합니다.
- ID 소스가 해당 사용자의 로그오프를 보고합니다.
- 영역은 영역의 **User Session Timeout: Authenticated Users(**사용자 세션 시간 초과**:** 인증된 사용자**)**, **User Session Timeout: Failed Authentication Users(**사용자 세션 시간 초과**:** 실패한 인증 사용자**)** 또는 **User Session Timeout: Guest Users(**사용자 세션 시간 초과**:** 게스트 사용자**)** 설정에서 지정된 대로 사용자 세션을 종료합니다.

참고 ISE/ISE-PIC를 구성한 경우, 사용자 테이블에 호스트 데이터가 표시될 수 있습니다. ISE/ISE-PIC에서는 호스트 탐지를 일부만 지원하므로, ISE에서 보고한 호스트 데이터를 사용하여 사용자 제어를 수행할 수 없습니다.

시스템에서 탐지한 사용자 로그인의 유형은 새로운 사용자에 대해 어떤 정보를 저장할지 결정합니다.

Identity Source(ID 소스)	로그인 유형	저장되는 사용자 데이터
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	• 사용자 이름 • 현재 IP 주소 • SGT(Security Group Tag) — ISE-PIC에서 지원되지 않음 • 엔드포인트 프로파일/디바이스 유형 — ISE-PIC에서 지원되지 않음 • 엔드포인트 위치/위치 IP — ISE-PIC에서 지원되지 않음 • 유형(LDAP)
캡티브 포털(captive portal)	Active Directory LDAP	• 사용자 이름 • 현재 IP 주소 • 유형(LDAP)
트래픽 기반 탐지	LDAP AIM Oracle SIP HTTP FTP MDNS	• 사용자 이름 • 현재 IP 주소 • 유형(AD)
	POP3 IMAP	• 사용자 이름 • 현재 IP 주소 • 이메일 주소 • 유형(`pop3` 또는 `imap`)

사용자를 자동으로 다운로드하도록 영역을 구성할 경우, Firepower Management Center에서는 지정된 간격을 기준으로 서버를 쿼리합니다. 시스템에서 새 사용자 로그인을 탐지한 후 Firepower Management Center 데이터베이스에서 사용자 메타데이터를 업데이트하는 데 5~10분 정도 걸릴 수 있습니다. Firepower Management Center에서는 각 사용자에 대한 다음과 같은 정보 및 메타데이터를 얻습니다.

- 사용자 이름
- 이름 및 성
- 이메일 주소

- department
- 전화번호
- 현재 IP 주소
- SGT(Security Group Tag) - 제공되는 경우
- 엔드포인트 프로파일 - 제공되는 경우
- 엔드포인트 위치 - 제공되는 경우

Firepower Management Center에서 데이터베이스에 저장할 수 있는 사용자 수는 Firepower Management Center 모델에 따라 다릅니다. 권한 없는 사용자가 호스트에 로그인한 것이 탐지되면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 해당 호스트에서 권한 있는 사용자 로그인이 탐지되면, 또 다른 권한 있는 사용자 로그인만이 현재 사용자를 변경합니다.

AIM, Oracle, SIP 로그인의 트래픽 기반 탐지는 시스템이 LDAP 서버에서 가져오는 사용자 메타데이터와 연결되지 않으므로 중복 사용자 레코드를 생성합니다. 이러한 프로토콜의 중복 사용자 레코드로 인한 사용자 수 남용을 방지하려면, 해당 프로토콜을 무시하도록 트래픽 기반 탐지를 구성합니다.

데이터베이스에서 사용자를 검색하고 보고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자를 삭제할 수도 있습니다.

일반적인 사용자 관련 이벤트 문제 해결에 대한 자세한 내용은 영역 및 사용자 다운로드 문제 해결, 2480 페이지을 참조하십시오.

사용자 데이터 보기

사용자의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용자에게 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 사용자를 나열하는 사용자의 테이블 보기를 포함하며 사용자 세부사항 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 사용자 세부사항 페이지는 제약 조건을 충족하는 모든 사용자에 대한 정보를 제공합니다.

프로시저

단계 **1** 사용자 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석) > Users(사용자) > Users(사용자)**를 선택합니다.
- 사용자의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(워크플로 전환)**를 클릭한 다음 **Users(사용자)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(사용자 관련 필드, 3076 페이지 참조).

사용자 활동 데이터

Firepower System은 네트워크에서 사용자 활동의 세부사항을 전달하는 이벤트를 생성합니다. 시스템이 사용자 활동을 탐지하면 사용자 활동 데이터가 데이터베이스에 로깅됩니다. 사용자 활동을 보고 검색하고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자 활동을 삭제할 수도 있습니다.

사용자가 네트워크에 최초로 나타나면 시스템은 사용자 활동 이벤트를 로깅합니다. 해당 사용자가 다음번에 나타날 경우에는 새로운 사용자 활동 이벤트를 로깅하지 않습니다. 그러나 사용자의 IP 주소가 변경되면 시스템은 새로운 사용자 활동 이벤트를 로깅합니다.

또한, Firepower System은 사용자 활동을 다른 이벤트 유형과 서로 연관시킵니다. 예를 들어, 침입 이벤트는 이벤트 발생 시점에 소스 및 대상 호스트에 로그인한 사용자를 알려줄 수 있습니다. 이러한 상관관계를 통해 공격 대상인 호스트에 로그인한 사용자, 또는 내부 공격이나 포트스캔을 시작한 사용자를 알 수 있습니다.

상관관계 규칙에서 사용자 활동을 사용할 수도 있습니다. 사용자 활동 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 조건을 충족하면 교정과 알림 응답을 실행합니다.

참고 ISE/ISE-PIC를 구성한 경우, 사용자 테이블에 호스트 데이터가 표시될 수 있습니다. ISE/ISE-PIC에서는 호스트 탐지를 일부만 지원하므로, ISE에서 보고한 호스트 데이터를 사용하여 사용자 제어를 수행할 수 없습니다.

다음은 네 가지 유형의 사용자 활동 데이터에 대한 설명입니다.

새로운 사용자 **ID**

시스템이 데이터베이스에 없는 알 수 없는 사용자의 로그인을 탐지할 경우 이 유형의 이벤트가 생성됩니다.

사용자가 네트워크에 최초로 나타나면 시스템은 사용자 활동 이벤트를 로깅합니다. 해당 사용자가 다음번에 나타날 경우에는 새로운 사용자 활동 이벤트를 로깅하지 않습니다. 그러나 사용자의 IP 주소가 변경되면 시스템은 새로운 사용자 활동 이벤트를 로깅합니다.

사용자 로그인

다음 중 하나가 발생할 경우 이 유형의 이벤트가 생성됩니다.

- ISE가 사용자 로그인 성공을 보고한 경우
- 캡티브 포털(captive portal)은 성공 또는 실패한 사용자 인증을 수행합니다.

- 트래픽 기반 탐지는 성공 또는 실패한 사용자 로그인을 탐지합니다.

참고 트래픽 기반 탐지에서 탐지된 SMTP 로그인은 데이터베이스에 이미 일치하는 이메일 주소의 사용자가 있지 않은 한 기록되지 않습니다.

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다.

캡티브 포털(captive portal) 또는 트래픽 기반 탐지를 사용할 경우, 실패한 사용자 로그인 및 실패한 사용자 인증 데이터에 대한 다음 사항에 유의하십시오.

- 트래픽 기반 탐지(LDAP, IMAP, FTP 및 POP3 트래픽)에서 보고한 실패한 로그인은 사용자의 테이블 보기가 아닌 사용자 활동의 테이블 보기에 표시됩니다. 알려진 사용자가 로그인에 실패한 경우, 시스템은 사용자 이름으로 해당 사용자를 식별합니다. 알 수 없는 사용자가 로그인에 실패한 경우, 시스템은 **Failed Authentication(**실패한 인증**)**을 사용자 이름으로 사용합니다.
- 캡티브 포털(captive portal)에서 보고한 실패한 인증은 사용자 활동의 테이블 보기 및 사용자의 테이블 보기에 모두 표시됩니다. 알려진 사용자가 인증에 실패한 경우, 시스템은 사용자 이름으로 해당 사용자를 식별합니다. 알 수 없는 사용자가 인증에 실패한 경우, 시스템은 사용자가 입력한 사용자 이름으로 해당 사용자를 식별합니다.

사용자 **ID** 삭제

데이터베이스에서 사용자를 수동으로 삭제할 경우 이 유형의 이벤트가 생성됩니다.

User Identity Dropped: User Limit Reached(사용자 **ID** 차단**:** 사용자 한계 도달**)**

시스템이 데이터베이스에 없는 사용자를 탐지했지만, Firepower Management Center 모델에서 확인된 데이터베이스의 사용자 최대 수에 도달했기 때문에 해당 사용자를 추가할 수 없는 경우 이 유형의 이벤트가 생성됩니다.

사용자 제한에 도달하면 대부분의 경우 시스템에서는 데이터베이스에 새 사용자를 추가하지 않습니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

그러나 시스템은 권한 있는 사용자를 선호합니다. 제한에 도달한 상태에서 시스템이 전에 탐지하지 못한 권한 있는 사용자의 로그인을 탐지하면, 오랫동안 비활성 상태를 유지한 권한 없는 사용자를 삭제하고 새로운 권한 있는 사용자를 대신 추가합니다.

일반적인 사용자 관련 이벤트 문제 해결에 대한 자세한 내용은 영역 및 사용자 다운로드 문제 해결, 2480 페이지을 참조하십시오.

관련 항목

사용자 활동 데이터베이스, 2389 페이지

사용자 활동 데이터 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용자 활동의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다. 사용자 활동에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 사용자 활동의 테이블 보기를 포함하며 사용자 세부사항 페이지(제약 조건을 충족하는 모든 사용자에 대한 사용자 세부사항 포함)에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 사용자 활동 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Users(**사용자**)** > **User Activity(**사용자 활동**)**를 선택합니다.
- 사용자 활동의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **User Activity(**사용자 활동**)**를 선택합니다.

팁 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 타임 윈도우 변경, 2815 페이지을 참조하십시오.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 3037 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(사용자 관련 필드, 3076 페이지 참조).

사용자 프로파일 및 호스트 기록

User(사용자) 팝업 창을 통해 특정 사용자에 대해 자세히 알아볼 수 있습니다. 이 문서에서 "User Profile"이라고 하는 표시되는 페이지의 웹 인터페이스에서의 제목은 "User Identity"입니다.

다음에서 창을 표시할 수 있습니다.

- 사용자 데이터를 다른 종류의 이벤트와 연결하는 이벤트 보기
- 활성 세션의 테이블 보기
- 사용자의 테이블 보기

사용자 정보는 사용자 워크플로의 종료 페이지에도 나타납니다.

표시되는 사용자 데이터는 사용자의 테이블 보기에 표시되는 것과 동일합니다.

보안 침해 지표 섹션

이 섹션에 대한 정보는 다음을 참조하십시오.

- 보안 침해 지표, 2554 페이지
- 보안 침해 지표 데이터 필드, 3058 페이지
- 단일 호스트에 대한 보안 침해 지표 규칙 상태 수정, 3059 페이지
- 보안 침해 지표 태그 해결, 3059 페이지
- 보안 침해 지표 태그의 소스 이벤트 보기, 3059 페이지

호스트 기록 섹션

호스트 기록은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 사용자가 로그인하고 로그오프한 호스트의 IP 주소 목록은 막대 그래프로 로그인 시간과 로그아웃 시간의 근사치를 계산합니다. 일반 사용자는 하루에 수차례 호스트에 로그인 및 로그오프할 수 있습니다. 예를 들어, 메일 서버에 대한 정기적인 자동 로그인은 여러 개의 짧은 세션으로 표시되고, 좀 더 긴 로그인(예: 근무 시간 중)은 더 긴 세션으로 표시될 수 있습니다.

트래픽 기반 탐지 또는 캡티브 포털을 사용하여 실패한 로그인을 캡처하는 경우, 호스트 기록에는 사용자가 로그인에 실패한 호스트도 포함됩니다.

호스트 기록을 생성하는 데 사용된 데이터는 사용자 기록 데이터베이스에 저장됩니다. 이 데이터베이스에는 기본적으로 1,000만 개의 사용자 로그인 이벤트가 저장됩니다. 특정 사용자에 대한 호스트 기록에 데이터가 없는 경우, 사용자가 비활성 상태이거나 데이터베이스 한도를 늘려야 할 수 있습니다.

관련 항목

사용자 데이터 필드

사용자 상세정보 및 호스트 기록 보기

프로시저

다음 2가지 옵션을 사용할 수 있습니다.

- 사용자를 나열하는 이벤트 보기에서 사용자 ID 옆에 표시되는 사용자 아이콘을 클릭합니다.
- 사용자 워크플로에서 Users 종료 페이지를 클릭합니다.

검색 이벤트 작업 히스토리

표 ***338:***

기능	버전	세부 사항
취약점 페이지 변경	6.7	Bugtraq 및 취약점 데이터는 더 이상 사용할 수 없습니다. 다음과 같이 변경되었습니다. • 현재 대부분의 취약점 데이터는 NVD(National Vulnerability Database)에서 제공됩니다. • 사용되지 않는 필드와 중복된 필드가 제거되었습니다. • 새 CVE ID 열이 테이블 보기에 추가되었으며 새 심각도 필드가 테이블 및 세부 사항 페이지에 추가되었습니다. • 이제 테이블에서 CVE ID를 마우스 오른쪽 버튼으로 클릭하여 NVD의 취약점에 대한 세부 정보를 볼 수 있습니다. • 테이블의 취약점 영향 열의 이름이 Impact로 변경되었습니다. (세부 사항 보기의 필드 이름은 변경되지 않습니다.) • Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) > Hosts(호스트)에서 호스트 프로파일의 취약점을 볼 때 취약점에 대한 세부 정보(타사 취약점 제외)는 새로운 필드 집합을 사용합니다. • Bugtraq 옵션이 Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) > Vulnerabilities(취약점) 페이지의 취약점 옵션에서 제거되었습니다. 수정된 화면: • Analysis(분석)> Hosts(호스트)> Vulnerabilities(취약점) 아래의 모든 페이지 • Hosts and Vulnerabilities(호스트 및 취약점) 탭의 Analysis(분석)> Hosts(호스트)> Network Map(네트워크 맵) 페이지 지원되는 플랫폼: FMC

126 장

상관관계 및 규정 준수 이벤트

다음 주제에서는 상관관계 및 규정 준수 이벤트를 보는 방법을 설명합니다.

- 상관관계 이벤트 보기, 3093 페이지
- 컴플라이언스 화이트 목록 워크플로우 사용, 3097 페이지
- 교정 상태 이벤트, 3103 페이지

상관관계 이벤트 보기

활성 상관관계 정책 내 상관관계 규칙이 트리거되면 시스템은 상관관계 이벤트를 생성하고 이를 데이터베이스에 로깅합니다.

참고 활성 상관관계 정책 내 규정준수 화이트 목록이 트리거되면 시스템은 화이트 목록 이벤트를 생성합니다.

상관관계 이벤트의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

상관관계 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 상관관계 이벤트의 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Correlation Events(**상관관계 이벤트**)** 을(를) 선택합니다.

원하는 경우, 맞춤형 워크플로 등 다른 워크플로를 사용하려면 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.

팁 상관관계 이벤트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.

단계 **2** 원하는 경우, 타임 윈도우 변경, 2815 페이지에 설명된 대로 시간 범위를 조정합니다.

단계 **3** 다음 작업 중 하나를 수행합니다.

- 표시되는 열에 대한 자세한 내용은 상관관계 이벤트 필드, 3095 페이지를 참조하십시오.
- IP 주소의 호스트 프로파일을 보려면 IP 주소 옆에 표시되는 호스트 프로파일을 클릭합니다.
- 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘를 클릭합니다.
- 이벤트를 정렬 및 제한하거나 현재 워크플로 페이지 내에서 이동하려면 워크플로 사용, 2793 페이지를 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다.
- 워크플로의 다음 페이지로 드릴다운하여 특정 값으로 제한하려면 드릴다운 페이지 사용, 2801 페이지를 참조하십시오.
- 일부 또는 모든 상관관계 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제하려 한다고 확인합니다.
- 다른 이벤트 보기로 이동해 연결된 이벤트를 보려면 워크플로 간 탐색, 2821 페이지을 참조하십시오.
- Firepower 시스템 외부에서 이용할 수 있는 소스의 데이터를 보려면 이벤트 값에서 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지 섹션을 참조해 주십시오.
- 이벤트에 대한 인텔리전스를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 2750 페이지를 참고하십시오.

관련 항목

데이터베이스 이벤트 제한 수, 1351 페이지
워크플로 페이지, 2797 페이지

상관관계 이벤트 필드

상관관계 규칙이 트리거되면 시스템은 상관관계 이벤트를 생성합니다. 다음 표는 상관관계 테이블에서 보고 검색할 수 있는 필드를 설명합니다.

표 ***339:*** 상관관계 이벤트 필드

필드	설명
설명	상관관계 이벤트의 설명. 설명의 정보는 규칙이 트리거된 방식에 따라 달라집니다. 예를 들어 규칙이 운영 체제 정보 업데이트 이벤트에 의해 트리거된 경우 새 운영 체제 이름 및 신뢰도 레벨이 나타납니다.
디바이스	정책 위반을 트리거한 이벤트를 생성한 디바이스의 이름.
도메인	모니터링되는 트래픽이 정책 위반을 트리거한 디바이스의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
영향	침입 데이터, 검색 데이터, 취약성 정보 간 상관관계를 기반으로 상관관계 이벤트에 할당되는 영향 레벨. 이 필드를 검색할 때 대소문자를 구분하지 않는 유효한 값은 `Impact 0`, `Impact Level 0`, `Impact 1`, `Impact Level 1`, `Impact 2`, `Impact Level 2`, `Impact 3`, `Impact Level 3`, `Impact 4`, `Impact Level 4`입니다. 영향 아이콘 색 이나 부분 문자열을 사용하지 마십시오(예를 들어 `blue`, `level 1` 또는`0`을 사용하지 마십시오).
Ingress Interface 또는 Egress Interface	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 인터페이스.
Ingress Security Zone 또는 Egress Security Zone	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 보안 영역.

필드	설명
인라인 결과	다음 중 하나에 해당합니다. • 검은색 아래쪽 화살표 - 시스템이 침입 규칙을 트리거한 패킷을 삭제했음을 나타냄 • 회색 아래쪽 화살표 - **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화했다면 시스템이 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제했을 것임을 나타냄 • 공백 - 트리거된 침입 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)으로 설정되지 않았음을 나타냄 이 필드를 사용하여 침입 이벤트에 의해 트리거되는 정책 위반을 검색할 때는 다음 중 하나를 입력합니다. • `dropped` - 패킷이 인라인, 스위치드 또는 라우티드 구축에서 삭제되었는지 여부를 지정 • `would have dropped` - 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제하도록 침입 정책을 구성했다면 패킷이 삭제되었을 것인지를 지정 침입 정책의 규칙 상태 또는 삭제 동작과 상관없이, 인라인 집합이 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.
정책	위반된 정책의 이름.
Priority(우선순위)	트리거된 규칙 또는 위반된 상관관계 정책의 우선순위에 의해 결정되는 상관관계 이벤트의 우선순위. 이 필드를 검색할 때 우선순위가 없는 경우, `none`을 입력합니다.
규칙	정책 위반을 트리거한 규칙의 이름.
보안 인텔리전스 카테고리	정책 위반을 트리거한 이벤트에서 차단된 IP 주소를 나타내거나 포함하는 개체의 이름. 이 필드를 검색할 때 정책 위반을 트리거한 상관 관계 이벤트에 연결된 보안 인텔리전스 카테고리를 지정합니다. 보안 인텔리전스 카테고리는 보안 인텔리전스 개체의 이름, 전역 차단 목록, 맞춤형 보안 인텔리전스 목록이나 피드 또는 인텔리전스 피드의 카테고리 중 하나일 수 있습니다.
Source Continent 또는 Destination Continent	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트 IP 주소에 연결된 대륙.

필드	설명
Source Country 또는 Destination Country	정책 위반을 트리거한 이벤트에서 소스 또는 대상 IP 주소에 연결된 국가.
Source Host Criticality 또는 Destination Host Criticality	상관관계 이벤트와 관련된 소스 또는 대상 호스트에 사용자가 할당하는 호스트 중요도: `None`, `Low`, `Medium`, `High`. 검색 이벤트, 호스트 입력 이벤트 또는 연결 이벤트 기반의 규칙에 의해 생성된 상관관계 이벤트에만 소스 호스트 중요도가 포함됩니다.
Source IP 또는Destination IP	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트의 IP 주소.
Source Port/ICMP Type 또는 Destination Port/ICMP Code	정책 위반을 트리거한 이벤트에 연결된 소스 트래픽의 소스 포트 또는 ICMP 유형 또는 대상 트래픽의 대상 포트 또는 ICMP 코드.
Source User 또는 Destination User	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트에 로그인한 사용자의 이름.
시간	상관관계 이벤트가 생성된 날짜 및 시간. 이 필드는 검색할 수 없습니다.
Count(개수)	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약조건을 적용한 경우에만 **Count(개수)** 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색, 2825 페이지

컴플라이언스 화이트 목록 워크플로우 사용

Firepower Management Center에서는 네트워크에 대해 생성되는 화이트 목록 이벤트 및 위반의 분석에 사용할 수 있는 워크플로우 집합을 제공합니다. 워크플로는 네트워크 맵 및 대시보드와 더불어 네트워크 자산의 규정 준수에 대한 핵심 정보 소스입니다.

시스템은 화이트 목록 이벤트 및 위반에 대한 사전 정의된 워크플로우를 제공합니다. 사용자 지정 워크플로를 생성할 수도 있습니다. 규정 준수 화이트 목록 워크플로우를 사용하면 여러 일반적인 작업을 수행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 보안 분석가 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관 관계**)** 메뉴를 사용하여 화이트 목록 워크플로우에 액세스합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 워크플로 전환 - 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 시간 범위 - 시간 범위를 조정합니다. 이벤트가 표시되지 않는 경우에 유용합니다(타임 윈도우 변경, 2815 페이지 참조).
- 호스트 프로파일 - IP 주소의 호스트 프로파일을 보려면 호스트 프로파일()을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 보안 침해된 호스트를 클릭합니다.
- 사용자 프로파일(이벤트만 해당) - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘를 클릭합니다.
- 제한 - 표시되는 열을 제한하려면 숨기려는 열 머리글의 닫기( )을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 검색 제약 조건을 확장한 다음 Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 드릴다운 - 드릴다운 페이지 사용, 2801 페이지 참조.
- 정렬 - 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
- 이 페이지 탐색 - 워크플로 페이지 이동 툴, 2798 페이지 참조.
- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.
- 이벤트 삭제(이벤트만 해당) - 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.

관련 항목

워크플로 페이지, 2797 페이지
이벤트 보기 구성, 41 페이지

화이트리스트 이벤트 보기

최초 평가 후 시스템은 모니터링되는 호스트가 활성 화이트리스트 규정준수에서 벗어날 때마다 화이트리스트 이벤트를 생성합니다. 화이트리스트는 특수한 종류의 상관관계 이벤트이며, FMC 상관관계 이벤트 데이터베이스에 로깅됩니다.

Firepower Management Center를 사용하여 규정준수 화이트리스트 이벤트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

화이트리스트 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로우에 따라 달라집니다. 이벤트의 테이블 보기에서 종료되는 미리 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 보안 분석가 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > 화이트리스트**Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행하려면 컴플라이언스 화이트 목록 워크플로우 사용, 3097 페이지를 참조하십시오.
- 테이블의 열 내용을 자세히 알아보려면 화이트 목록 이벤트 필드, 3099 페이지를 참조하십시오.
- 더 많은 옵션을 보려면 테이블의 값을 마우스 오른쪽 버튼으로 클릭합니다.

화이트 목록 이벤트 필드

워크플로를 사용하여 보고 검색할 수 있는 화이트 목록 이벤트에는 다음 필드가 포함됩니다.

디바이스

화이트 목록 위반을 탐지한 매니지드 디바이스의 이름입니다.

설명

화이트 목록을 어떤 식으로 위반했는지 설명합니다. 예를 들면 다음과 같습니다.

클라이언트 “AOL Instant Messenger”는 허용되지 않습니다.

애플리케이션 프로토콜과 관련된 위반은 애플리케이션 프로토콜 이름과 버전은 물론 애플리케이션 프로토콜이 사용 중인 포트와 프로토콜(TCP 또는 UDP)을 나타냅니다. 금지를 특정 운영 체제로 제한할 경우, 설명에는 해당 운영 체제 이름이 포함됩니다. 예를 들면 다음과 같습니다.

서버 "ssh / 22 TCP (OpenSSH 3.6.1p2)"는 운영 체제 “Linux Linux 2.4 또는 2.6”에서 허용되지 않습니다.

도메인

화이트 목록을 준수하지 않게 된 호스트의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Host Criticality(호스트 심각도**)**

화이트 목록을 준수하지 않는 소스 호스트에 대해 사용자가 할당하는 호스트 중요도(None, Low, Medium, High)입니다.

IP 주소

화이트 목록을 준수하지 않게 된 호스트의 IP 주소.

정책

위반된 상관관계 정책의 이름입니다. 즉, 화이트 목록이 포함된 상관관계 정책입니다.

포트

애플리케이션 프로토콜 화이트 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 검색 이벤트에 연결된 포트. 다른 유형의 화이트 목록 위반의 경우, 이 필드는 비어 있습니다.

Priority(우선순위**)**

정책 또는 정책 위반을 트리거한 화이트 목록에 의해 지정된 우선순위. 상관관계 정책의 화이트 목록 우선 순위 또는 상관관계 정책 자체의 우선 순위에 의해 결정됩니다. 화이트 목록 우선 순위는 해당 정책의 우선 순위를 재정의합니다. 이 필드를 검색할 때 우선 순위가 없는 경우, `none`을 입력합니다.

시간

화이트 목록 이벤트가 생성된 시간 및 날짜입니다. 이 필드는 검색할 수 없습니다.

User

화이트 목록을 준수하지 않게 된 호스트에 로그인한 알려진 사용자의 ID.

화이트 목록

화이트 목록의 이름입니다.

Count(개수**)**

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

화이트리스트 위반 보기

시스템은 네트워크에서 현재 화이트리스트 위반의 레코드를 유지합니다. 각 위반은 호스트 중 하나에서 허용되지 않는 것이 실행 중임을 나타냅니다. 호스트가 규정을 준수하게 되면 시스템은 이제 수정된 위반을 데이터베이스에서 제거합니다.

Firepower Management Center를 사용하여 모든 활성 화이트리스트에 대한 화이트리스트 위반 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

화이트리스트 위반에 액세스할 때 표시되는 페이지는 사용하는 워크플로우에 따라 달라집니다. 사전 정의 워크플로는 제약 조건을 충족하는 모든 호스트의 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > 화이트리스트**Violations(**위반**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행하려면 컴플라이언스 화이트 목록 워크플로우 사용, 3097 페이지를 참조하십시오.
- 테이블의 열 내용을 자세히 알아보려면 화이트 목록 위반 필드, 3101 페이지를 참조하십시오.
- 더 많은 옵션을 보려면 테이블의 값을 마우스 오른쪽 버튼으로 클릭합니다.

화이트 목록 위반 필드

워크플로를 사용하여 보고 검색할 수 있는 화이트 목록 위반에는 다음 필드가 포함됩니다.

도메인

규정을 준수하지 않는 호스트가 있는 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.

정보

화이트 목록 위반과 관련하여 제공되는 모든 공급업체, 제품 또는 버전 정보입니다. 화이트 목록을 위반하는 프로토콜의 경우, 이 필드에는 위반이 네트워크 프로토콜로 인한 것인지 전송 프로토콜로 인한 것이지도 표시됩니다.

IP 주소

규정 준수 위반 호스트의 IP 주소입니다.

Port(포트**)**

애플리케이션 프로토콜 화이트 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트에 연결된 포트입니다. 다른 유형의 화이트 목록 위반의 경우, 이 필드는 비어 있습니다.

프로토콜

애플리케이션 프로토콜 화이트 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트에 연결된 프로토콜. 다른 유형의 화이트 목록 위반의 경우, 이 필드는 비어 있습니다.

시간

화이트 목록 위반이 탐지된 시간 및 날짜입니다.

유형

화이트 목록 위반의 유형입니다. 즉, 규정을 준수하지 않아 발생한 위반인지 나타냅니다.

- 운영체체(os) (이 필드를 검색할 때는 **os** 또는 **operating system**을 입력합니다.)
- 애플리케이션 프로토콜(서버)
- 클라이언트
- protocol
- 웹 애플리케이션(웹) (이 필드를 검색할 때는 **web application**을 입력합니다.)

화이트 목록

위반된 화이트 목록의 이름입니다.

Count(개수**)**

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

교정 상태 이벤트

교정이 트리거되면 시스템은 교정 상태 이벤트를 데이터베이스에 로깅합니다. 이러한 이벤트는 Remediation Status(교정 상태) 페이지에서 볼 수 있습니다. 교정 상태 이벤트를 검색하고 보고 삭제할 수 있습니다.

관련 항목

교정 상태 테이블 필드, 3104 페이지

교정 상태 이벤트 보기

교정 상태 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 교정 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 테이블 보기에는 각 교정 상태 이벤트의 행이 포함됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Status(**상태**)**을(를) 선택합니다.

단계 **2** 원하는 경우, 타임 윈도우 변경, 2815 페이지에 설명된 대로 시간 범위를 조정합니다.

단계 **3** 원하는 경우, 맞춤형 워크플로 등 다른 워크플로를 사용하려면 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.

팁 교정의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)** 메뉴를 클릭한 다음 **Remediation Status(**교정 상태**)**를 선택하십시오.

단계 **4** 다음 옵션을 이용할 수 있습니다.

- 표시되는 열에 대한 자세한 내용은 교정 상태 테이블 필드, 3104 페이지를 참조하십시오.
- 이벤트를 정렬하고 제한하려면 워크플로 사용, 2793 페이지를 참조하십시오.
- 상관관계 이벤트 보기로 이동해 연결된 이벤트를 보려면 **Correlation Events(**상관관계 이벤트**)**를 클릭합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다. 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.

- 테이블 보기의 데이터를 기반으로 보고서를 생성하려면 이벤트 보기에서 보고서 템플릿 생성, 2657 페이지의 설명에 따라 **Report Designer(**리포트 디자이너**)**를 클릭합니다.
- 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용, 2801 페이지 섹션을 참조하십시오.
- 시스템에서 교정 상태 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제하려 한다고 확인합니다.
- 교정 상태 이벤트를 검색하려면 **Search(**검색**)**를 클릭합니다.

관련 항목

워크플로 사용, 2793 페이지

교정 상태 테이블 필드

다음 표는 교정 상태 테이블에서 보고 검색할 수 있는 필드를 설명합니다.

표 ***340:*** 교정 상태 필드

필드	설명
도메인	모니터링되는 트래픽이 정책 위반을 트리거한 다음 교정을 트리거한 디바이스의 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
정책	위반되어 교정을 트리거한 상관관계 정책의 이름.
Remediation Name(리미디에이션 이름)	실행된 교정의 이름.

필드	설명
결과 메시지	교정이 실행되었을 때 발생한 상황을 설명하는 메시지. 상태 메시지는 다음을 포함합니다. • 성공적으로 교정 완료 • 교정 모듈에 제공된 입력에 오류가 있음 • 교정 모듈 구성에 오류가 있음 • 원격 디바이스 또는 서버에 로그인할 때 오류 발생 • 원격 디바이스 또는 서버에 대한 필요한 권한을 얻을 수 없음 • 원격 디바이스 또는 서버에 로그인할 때 시간 초과 • 원격 명령 또는 서버를 실행할 때 시간 초과 • 원격 디바이스 또는 서버에 연결하지 못했음 • 교정을 시도했으나 실패했음 • 리미디에이션 프로그램을 실행하지 못함 • 알 수 없는/예기치 않은 오류 맞춤형 교정 모듈이 설치된 경우 맞춤형 모듈에 의해 구현되는 추가 상태 메시지를 볼 수 있습니다.
규칙	교정을 트리거한 상관관계 규칙의 이름입니다.
시간	Firepower Management Center가 교정을 트리거한 날짜 및 시간
Count(개수)	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색, 2825 페이지

교정 상태 이벤트 테이블 사용

이벤트 보기의 레이아웃을 변경하거나 보기의 이벤트를 필드 값으로 제한할 수 있습니다.

비활성화한 열은 나중에 다시 추가하지 않는 한 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화하면 Count(카운트) 열이 추가됩니다.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Status(**상태**)**을(를) 선택합니다.

팁 교정의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)** 메뉴를 클릭한 다음 **Remediation Status(**교정 상태**)**를 선택하십시오.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 표시되는 열에 대한 자세한 내용은 교정 상태 테이블 필드, 3104 페이지를 참조하십시오.
- 이벤트를 정렬하고 제한하려면 워크플로 사용, 2793 페이지를 참조하십시오.

부록 A

보안, 인터넷 액세스 및 통신 포트

다음 항목에서는 시스템 보안, 인터넷 액세스 및 통신 포트에 대한 정보를 제공합니다.

- 보안 요건, 3107 페이지
- Cisco Cloud, 3107 페이지
- 인터넷 액세스 요구 사항, 3108 페이지
- 통신 포트 요구 사항, 3110 페이지

보안 요건

Firepower Management Center를 보호하려면 보호된 내부 네트워크에 설치해야 합니다. 필요한 서비스와 사용 가능한 포트만 사용하도록 FMC를 구성한 경우에도 방화벽 외부의 공격이 방어 센터(또는 매니지드 디바이스)에 도달할 수 없는지 확인해야 합니다.

FMC 및 관리되는 디바이스가 동일한 네트워크에 상주하는 경우 디바이스의 관리 인터페이스를 FMC와 동일한 보호된 내부 네트워크에 연결할 수 있습니다. 이렇게 하면 FMC에서 디바이스를 안전하게 제어할 수 있습니다. 또한 FMC에서 다른 네트워크에 있는 디바이스의 트래픽을 관리 및 격리할 수도 있도록 복수 관리 인터페이스를 구성할 수도 있습니다.

어플라이언스를 구축하는 방식과 상관없이 어플라이언스 간 통신은 암호화됩니다. 하지만 DDoS(Distributed Denial of Service) 또는 중간자 공격(man-in-the-middle attack)등으로 어플라이언스 간 통신이 중단, 차단 또는 변조될 수 없도록 방지하는 단계를 수행해야 합니다.

Cisco Cloud

FMC는 다음 기능을 위해 Cisco Cloud의 리소스와 통신합니다.

- **AMP(Advanced Malware Protection)**

  퍼블릭 클라우드는 기본적으로 구성되어 있습니다. 변경하는 방법은 AMP 옵션 변경, 1876 페이지의 내용을 참조하십시오.

- **URL** 필터링

  자세한 내용은 다음을 참조해 주십시오.

  - URL 필터링 옵션, 1674 페이지
  - 범주 및 평판을 사용한 URL 필터링 활성화, 1674 페이지

- **SecureX** 및 **Cisco SecureX Threat Response**의 통합

  자세한 내용은 다음에서 연결된 통합 문서를 참조하십시오.

  - Cisco SecureX와의 통합, 2749 페이지
  - 다음을 이용한 이벤트 분석 Cisco SecureX Threat Response, 2749 페이지

- 사전 지원 기능

  자세한 내용은 Cisco 지원 진단, 176 페이지를 참조하십시오.

- **Cisco Success Network**

  자세한 내용은 Cisco Success Network를 참고하십시오.

인터넷 액세스 요구 사항

기본적으로 Firepower 어플라이언스는 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 직접 연결하도록 구성됩니다. 어플라이언스가 인터넷에 직접 액세스하지 않도록 하려면 프록시 서버를 구성할 수 있습니다.

대부분의 경우, 인터넷에 액세스하는 것은 Firepower Management Center입니다. 하지만 때로는 매니지드 디바이스도 인터넷에 액세스합니다. 예를 들어 악성코드 방지 구성이 동적 분석을 사용하는 경우, 매니지드 디바이스는 파일을 직접 Cisco Threat Grid 클라우드에 전송합니다. 또는 디바이스를 외부 NTP 서버와 동기화할 수 있습니다.

팁 AMP for Networks 또는 AMP for Endpoints를 사용하는 경우, FMC가 액세스하는 AMP 클라우드 리소스는 위치에 따라 결정될 수 있습니다. Required Server Addresses for Proper AMP Operations Troubleshooting TechNote에는 Firepower 어플라이언스뿐 아니라 커넥터와 프라이빗 클라우드 어플라이언스 같은 Cisco AMP 구성 요소에 필요한 인터넷 리소스(고정 IP 주소 포함)가 나열되어 있습니다.

보안, 인터넷 액세스 및 통신 포트

표 ***341: Firepower*** 인터넷 액세스 요구 사항

기능	이유	리소스
AMP for Networks	악성코드 클라우드 조회.	cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.sourcefire.com cloud-sa.apjc.amp.sourcefire.com cloud-sa-589592150.us-east-1.elb.amazonaws.com
	파일 사전 분류 및 로컬 악성코드 분석을 위한 서명 업데이트를 다운로드합니다.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	동적 분석을 위해 파일을 제출합니다(매니지드 디바이스). 동적 분석 결과를 쿼리합니다(FMC).	panacea.threatgrid.com
AMP for Endpoints 통합	AMP for Endpoints가 탐지한 악성코드 이벤트를 AMP 클라우드에서 수신합니다.	api.amp.sourcefire.com api.eu.amp.sourcefire.com api.apjc.amp.sourcefire.com export.amp.sourcefire.com export.eu.amp.sourcefire.com export.apjc.amp.sourcefire.com
보안 인텔리전스	보안 인텔리전스 피드를 다운로드합니다.	intelligence.sourcefire.com
URL 필터링	URL 카테고리 및 평판 데이터를 다운로드합니다. 수동으로 URL 카테고리 및 평판 데이터를 쿼리합니다. 미분류 URL을 쿼리합니다.	database.brightcloud.com service.brightcloud.com
Cisco Smart Licensing	Cisco Smart Software Manager와 통신합니다.	tools.cisco.com
시스템 업데이트	Cisco에서 어플라이언스로 직접 업데이트를 다운로드합니다. • 시스템 소프트웨어 • 침입 규칙 • VDB(Vulnerability Database) • GeoDB(지리위치 데이터베이스)	cisco.com sourcefire.com

기능	이유	리소스
시간 동기화	구축에서 시간을 동기화합니다. 프록시 서버에서는 지원되지 않습니다.	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
RSS 피드	대시보드에 Cisco Threat Research 블로그를 표시합니다.	blogs.cisco.com/talos cloud.google.com
Whois	외부 호스트의 whois 정보 요청 프록시 서버에서는 지원되지 않습니다.	whois 클라이언트는 쿼리할 적절한 서버를 추측하려 시도합니다. 추측할 수 없는 경우, 다음을 사용합니다. • NIC 핸들: whois.networksolutions.com • IPv4 주소 및 네트워크 이름: whois.arin.net

통신 포트 요구 사항

Firepower 어플라이언스는 포트 8305/tcp를 사용하는 양방향 SSL-암호화 통신을 사용하여 통신합니다. 이 포트는 플랫폼 내 기본 통신을 위해 반드시 열려 있어야 합니다.

다른 포트는 특정 기능에 필요한 외부 리소스에 대한 액세스뿐만 아니라 보안 관리도 허용합니다. 일반적으로 기능과 관련된 포트는 관련 기능을 활성화 또는 구성할 때까지 닫은 상태를 유지해야 합니다. 개방된 포트를 닫음으로써 구축에 어떤 영향을 미칠지 이해하기 전까지 개방된 포트를 변경하거나 닫지 마십시오.

표 ***342: Firepower*** 통신 포트 요구 사항

Port(포트)	프로토콜/기능	플랫폼	방향	세부 사항
7/UDP	UDP/감사 로깅	FMC, 클래식	아웃바운드	감사 로깅을 구성할 때 시스템 로그 서버와의 연결을 확인합니다.
22/tcp	SSH	FMC 모든 디바이스	인바운드	어플라이언스에 대한 보안 원격 연결
25/tcp	SMTP	FMC	아웃바운드	이메일 알림 및 경고 전송
53/tcp 53/udp	DNS	FMC 모든 디바이스	아웃바운드	DNS
67/udp 68/udp	DHCP	FMC 모든 디바이스	아웃바운드	DHCP

Port(포트)	프로토콜/기능	플랫폼	방향	세부 사항
80/tcp	HTTP	FMC 7000/8000 시리즈	아웃바운드	대시보드에 RSS 피드 표시
80/tcp	HTTP	FMC	아웃바운드	URL 카테고리 및 평판 데이터 다운로드 또는 쿼리(포트 443도 필요)
80/tcp	HTTP	FMC	아웃바운드	HTTP를 통해 사용자 정의 보안 인텔리전스 다운로드
123/udp	NTP	FMC 모든 디바이스	아웃바운드	시간 동기화
161/udp	SNMP	FMC 모든 디바이스	인바운드	SNMP 폴링을 통해 MIB에 대한 액세스 허용
162/udp	SNMP	FMC 모든 디바이스	아웃바운드	SNMP 경고를 원격 트랩 서버로 전송
389/tcp 636/tcp	LDAP	FMC 7000/8000 시리즈	아웃바운드	외부 인증을 위해 LDAP 서버와 통신 감지된 LDAP 사용자의 메타데이터 가져오기(FMC 전용) 구성 가능합니다.
443/tcp	HTTPS	FMC 7000/8000 시리즈	인바운드	웹 인터페이스 액세스
443/tcp	Remote Access VPN(SSL/IPSec)	FTD	인바운드	원격 사용자로부터 네트워크에 보안 VPN 연결 허용
500/udp 4500/udp	Remote Access VPN(IKEv2)	FTD	인바운드	원격 사용자로부터 네트워크에 보안 VPN 연결 허용
443/tcp	HTTPS	FMC 모든 디바이스	아웃바운드	인터넷에서 데이터 송수신 자세한 내용은 인터넷 액세스 요구 사항, 3108 페이지을 참조해 주십시오.
443	HTTPS	FMC	아웃바운드	AMP 클라우드와 통신(퍼블릭 또는 프라이빗) 포트 32137에 대한 정보를 참조하십시오.
443	HTTPS	FMC	인바운드 및 아웃바운드	AMP for Networks와의 통합

보안, 인터넷 액세스 및 통신 포트

Port(포트)	프로토콜/기능	플랫폼	방향	세부 사항
514/udp	시스템 로그(알림)	FMC 모든 디바이스	아웃바운드	원격 syslog 서버에 대한 경고 전송
623/udp	SOL/LOM	FMC 7000/8000 시리즈	인바운드	SOL(Serial Over LAN) 연결을 사용하여 Lights-Out Management(LOM) 수행
885/tcp	캡티브 포털	모든 디바이스	인바운드	캡티브 포털 ID 소스와 통신
1500/tcp 2000/tcp	데이터베이스 액세스	FMC	인바운드	서드파티 클라이언트의 이벤트 데이터베이스에 대한 읽기 전용 액세스 허용
1812/udp 1813/udp	RADIUS	FMC 7000/8000 시리즈	아웃바운드	외부 인증 및 어카운트 관리를 위해 RADIUS 서버와 통신 구성 가능합니다.
5222/tcp	ISE	FMC	아웃바운드	ISE ID 소스와 통신
8302/tcp	eStreamer	FMC 7000/8000 시리즈	인바운드	eStreamer 클라이언트와 통신
8305/tcp	어플라이언스 통신	FMC 모든 디바이스	Both(모두)	구축 어플라이언스 간 보안 통신. 구성 가능합니다. 이 포트를 변경하는 경우 구축의 모든 어플라이언스에 대해 이 포트를 변경해야 합니다. 기본값을 유지하는 것이 좋습니다.
8307/tcp	호스트 입력 클라이언트	FMC	인바운드	호스트 입력 클라이언트와 통신
8989/tcp	Cisco 지원 진단	FMC FTD	Both(모두)	인증된 요청을 수락하고 사용량 정보 및 통계를 전송합니다.
32137/tcp	AMP for Networks	FMC	아웃바운드	Cisco AMP 클라우드와 통신 이 구성은 레거시 구성입니다. 기본값(443)을 사용하는 것이 좋습니다.

관련 항목

LDAP 인증 서버 식별
FMC에 대한 LDAP 외부 인증 개체 추가, 59 페이지
RADIUS 연결 설정 구성
FMC에 대한 RADIUS 외부 인증 개체 추가, 66 페이지

B 부록

명령줄 참조

CLI 참조는 다음에 적용됩니다.

- 7000 및 8000 Series
- ASA FirePOWER
- NGIPSv

Firepower Management Center에 대한 CLI 액세스는 사용할 수 없습니다. 대신 FMC는 Cisco TAC(Technical Assistance Center) 감독 하의 Linux 셸 액세스를 지원합니다.

- 클래식 디바이스 CLI 정보, 3113 페이지
- 클래식 디바이스 CLI 관리 명령, 3114 페이지
- 클래식 디바이스 CLI 명령 표시, 3117 페이지
- 클래식 디바이스 CLI 구성 명령, 3146 페이지
- 클래식 디바이스 CLI 시스템 명령, 3165 페이지
- 클래식 디바이스 CLI 기록, 3172 페이지

클래식 디바이스 CLI 정보

CLI를 통해 클래식 디바이스(7000 및 8000 Series, ASA FirePOWER, NGIPSv)에 로그인(7000/8000 시리즈, ASA FirePOWER, NGIPSv 디바이스에서 CLI에 로그인, 36 페이지 참조)한 다음 이 부록에 설명된 명령을 사용하여 디바이스를 보고, 구성하고, 문제를 해결할 수 있습니다.

참고 7000 또는 8000 Series 디바이스를 재부팅하고 가능한 한 빨리 CLI에 로그인하는 경우, 웹 인터페이스를 사용할 수 있을 때까지는 실행하는 명령이 감사 로그에 기록되지 않습니다.

CLI 명령은 대소문자를 구분하지 않습니다. 단, 텍스트가 CLI 프레임워크의 일부가 아닌 매개 변수(예: 사용자 이름 및 검색 필터)는 예외입니다.

관련 항목

Firepower System 유저 인터페이스, 27 페이지

클래식 디바이스 **CLI** 모드

CLI는 4가지 모드를 포함합니다. 기본 모드인 CLI Management에는 CLI 자체 내에서 탐색하기 위한 명령이 포함됩니다. 나머지 모드에는 클래식 디바이스 기능의 세 가지 영역을 처리하는 명령이 포함됩니다. 이러한 모드 내의 명령은 모드 이름(`system`, `show` 또는 `configure`)으로 시작합니다.

모드에 진입하면 CLI 프롬프트는 현재 모드를 반영하도록 변경됩니다. 예를 들어 시스템 구성 요소에 대한 버전 정보를 표시하려면 표준 CLI 프롬프트에서 전체 명령을 입력할 수 있습니다.

```
> show version
```

`show` 모드에 진입한 경우, show 모드 CLI 프롬프트에서 `show` 키워드 없이 명령을 입력할 수 있습니다.

```
show> version
```

클래식 디바이스 **CLI** 액세스 레벨

각 모드 내에서 사용자가 이용할 수 있는 명령은 사용자의 CLI 액세스에 따라 다릅니다. 사용자 계정을 만들 때 다음 CLI 액세스 레벨 중 하나를 할당할 수 있습니다.

- Basic(기본) - 사용자는 읽기 전용 액세스 권한을 가지고 있으며 시스템 성능에 영향을 주는 명령을 실행할 수 없습니다.
- Configuration(구성) - 사용자는 읽기-쓰기 액세스 권한을 가지고 있으며 시스템 성능에 영향을 미치는 명령을 실행할 수 있습니다.
- None(없음) - 사용자는 CLI에 로그인할 수 없습니다.

7000 및 8000 Series 디바이스에서 로컬 웹 인터페이스의 User Management(사용자 관리) 페이지에서 명령줄 권한을 할당할 수 있습니다. NGIPSv 및 ASA FirePOWER에서 CLI를 사용하여 명령줄 권한을 할당합니다.

클래식 디바이스 **CLI** 관리 명령

CLI 관리 명령은 CLI와 상호 작용하는 기능을 제공하며, 디바이스의 작동에는 영향을 미치지 않습니다.

configure password

현재 사용자가 자신의 비밀번호를 변경하도록 허용합니다. 이 명령을 실행하면 현재(또는 이전) 비밀번호를 입력하라는 CLI 프롬프트가 표시된 다음 새 비밀번호를 두 번 입력하라는 프롬프트가 표시됩니다.

액세스

기본

Syntax

```
configure password
```

예

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

exit

CLI 컨텍스트를 다음으로 가장 높은 CLI 컨텍스트 레벨로 이동합니다. 기본 모드에서 이 명령을 실행하면 사용자가 현재 CLI 세션에서 로그아웃되며, `logout` CLI 명령 실행과 동일한 결과가 나타납니다.

액세스

기본

Syntax

```
exit
```

예

```
configure network ipv4> exit
configure network>
```

expert

Linux 셸을 호출합니다.

⚠

주의 Cisco TAC가 지시하거나 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다. 자세한 내용은 Firepower System 사용자 어카운트, 25 페이지의 내용을 참고하십시오.

액세스

구성

Syntax

```
expert
```

예

```
> expert
```

history

현재 세션의 명령줄 기록을 표시합니다.

액세스

기본

Syntax

```
history limit
```

여기서 `limit`는 기록 목록의 크기를 설정합니다. 크기를 무제한으로 설정하려면 0을 입력합니다.

예

```
history 25
```

logout

현재 사용자를 현재 CLI 콘솔 세션에서 로그아웃합니다.

액세스

기본

Syntax

```
logout
```

예

```
> logout
```

? (물음표)

CLI 명령 및 매개 변수에 대한 상황별 도움말을 표시합니다. 물음표(?) 명령은 다음과 같이 사용하십시오.

- 현재 CLI 컨텍스트 내에서 사용 가능한 명령의 도움말을 표시하려면 명령 프롬프트에서 물음표(?)를 입력합니다.
- 특별한 문자 집합으로 시작되는 사용 가능한 명령 목록을 표시하려면 약식 명령 바로 뒤에 물음표(?)를 입력합니다.
- 명령의 공식적인 인수에 대한 도움말을 표시하려면 명령 프롬프트에서 인수 자리에 물음표(?)를 입력합니다.

물음표(?)는 콘솔로 다시 에코되지 않습니다.

액세스

기본

Syntax

```
?
abbreviated_command ?
command [arguments] ?
```

예

```
> ?
```

클래식 디바이스 **CLI** 명령 표시

show 명령은 디바이스의 상태에 대한 정보를 제공합니다. 이러한 명령은 디바이스의 작동 모드를 변경하지 않으며, 명령 실행 시 시스템 작동에 미치는 영향이 최소 수준입니다. 대부분의 show 명령은 모든 CLI 사용자가 이용할 수 있지만 `show user` 명령은 구성 CLI 액세스 권한이 있는 사용자만 실행할 수 있습니다.

access-control-config

다음을 포함하여 현재 구축된 액세스 제어 구성을 표시합니다.

- 보안 인텔리전스 설정
- 액세스 컨트롤 정책이 호출하는 하위 정책의 이름
- 침입 변수 집합 데이터
- 로깅 설정
- 정책 수준 성능, 전처리, 일반 설정을 포함한 그 밖의 고급 설정

소스 및 대상 포트 데이터(ICMP 항목의 유형 및 코드 포함)와 같은 정책 관련 연결 정보와 각 액세스 제어 규칙과 일치하는 연결 수(히트 수)도 표시합니다.

액세스

기본

Syntax

```
show access-control-config
```

예

```
> show access-control-config
```

경보

디바이스에서 현재 활성 상태인(failed/down) 하드웨어 알람을 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER 디바이스에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show alarms
```

예

```
> show alarms
```

arp-tables

네트워크에 해당되는 Address Resolution Protocol(주소 확인 프로토콜) 테이블을 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show arp-tables
```

예

```
> show arp-tables
```

audit-log

감사 로그를 역시간순으로 표시합니다. 최근 감사 로그가 가장 먼저 나열됩니다.

액세스

기본

Syntax

```
show audit-log
```

예

```
> show audit-log
```

우회

7000 또는 8000 Series 디바이스에서는 사용 중인 인라인 집합을 나열하고 이러한 집합의 우회 모드 상태를 다음 중 하나로 표시합니다.

- `armed` - 인터페이스 쌍이 실패하거나(**Bypass Mode: Bypass**) **`configure bypass close`** 명령으로 강제로 fail-close된 경우, 하드웨어 우회로 들어가도록 구성됨
- `engaged` - 인터페이스 쌍이 열기 실패했거나 **`configure bypass open`** 명령으로 강제로 하드웨어 우회됨
- `off` - 인터페이스 쌍이 fail-close로 설정되고(**Bypass Mode: Non-Bypass**), 인터페이스 쌍이 실패하면 패킷이 차단됨

액세스

기본

Syntax

```
show bypass
```

예

```
> show bypass
s1p1 ↔ s1p2: status 'armed'
s1p1 ↔ s1p2: status 'engaged'
```

high-availability 명령

고가용성 구성, 상태 및 멤버 디바이스 또는 스택에 대한 정보를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER 디바이스에서는 사용할 수 없습니다.

액세스

기본

config

디바이스에서 고가용성 구성을 표시합니다.

Syntax

```
show high-availability config
```

예

```
> show high-availability config
```

high-availability ha-statistics

고가용성 쌍의 디바이스에 대한 상태 공유 통계를 표시합니다.

Syntax

```
show high-availability ha-statistics
```

예

```
> show high-availability ha-statistics
```

cpu

디바이스의 모든 CPU의 플랫폼에 해당하는 현재 CPU 사용량을 표시합니다.

7000 및 8000 Series 디바이스의 경우, 다음 값이 표시됩니다.

- CPU - 프로세서 수.
- Load - 0~100의 숫자로 표시되는 CPU 사용률. 0은 로드되지 않은 것이고 100은 완전히 로드된 것입니다.

NGIPSv 및 ASA FirePOWER 디바이스의 경우, 다음 값이 표시됩니다.

- CPU - 프로세서 수.
- %user - 사용자 레벨(애플리케이션)에서 실행되는 동안 발생한 CPU 사용률.
- %nice - 사용자 레벨(nice 우선순위)에서 실행되는 동안 발생한 CPU 사용률.
- %sys - 시스템 레벨(커널)에서 실행되는 동안 발생한 CPU 사용률. interrupt 또는 softirq의 서비스에 사용된 시간은 포함되지 않습니다. softirq(software interrupt)는 여러 CPU에서 동시에 실행할 수 있는 32개의 열거된 software interrupt 중 하나입니다.
- %iowait - 시스템에 해결되지 않은 디스크 I/O 요청이 있을 때 CPU가 유휴 상태였던 시간의 백분율.
- %irq - interrupt 서비스에 CPU가 사용된 시간의 백분율.
- %soft - softirq 서비스에 CPU가 사용된 시간의 백분율.
- %steal - 하이퍼바이저가 다른 가상 프로세서를 서비스하는 동안 가상 CPU가 비자발적으로 대기하는 데 사용된 시간의 백분율.
- %guest - 가상 프로세서 실행에 CPU가 사용된 시간의 백분율.
- %idle - CPU가 유휴 상태이고 시스템에 해결되지 않은 디스크 I/O 요청이 없는 시간의 백분율.

액세스

기본

Syntax

```
show cpu [procnum]
```

여기서 `procnum`은 사용률 정보를 표시할 프로세서의 수입니다. 유효한 값의 범위는 0부터 시스템의 총 프로세서 수에서 1을 뺀 값까지입니다. 7000 또는 8000 Series 디바이스에 대해 `procnum`을 사용하면 무시됩니다. 해당 플랫폼에서는 사용률 정보를 모든 프로세서에 대해서만 표시할 수 있기 때문입니다.

```
> show cpu
```

database 명령

`show database` 명령은 디바이스의 관리 인터페이스를 구성합니다.

액세스

기본

processes

실행 중인 데이터베이스 쿼리의 목록을 표시합니다.

액세스

기본

Syntax

```
show database processes
```

예

```
> show database processes
```

slow-query-log

데이터베이스의 느린 쿼리 로그를 표시합니다.

액세스

기본

Syntax

```
show database slow-query-log
```

예

```
> show database slow-query-log
```

device-settings

현재 디바이스에 해당하는 애플리케이션 우회 설정에 대한 정보를 표시합니다.

액세스

기본

Syntax

```
show device-settings
```

예

```
> show device-settings
```

disk

현재 디스크 사용량을 표시합니다.

액세스

기본

Syntax

```
show disk
```

예

```
> show disk
```

disk-manager

시스템의 각 부분(silos, low watermarks, high watermarks 등)에 대한 자세한 디스크 사용량 정보를 표시합니다.

액세스

기본

Syntax

```
show disk-manager
```

예

```
> show disk-manager
```

dns

현재 DNS 서버 주소 및 검색 도메인을 표시합니다.

액세스

기본

Syntax

```
show dns
```

예

```
> show dns
```

fan-status

하드웨어 팬의 현재 상태를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER 디바이스에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show fan-status
```

예

```
> show fan-status
```

fastpath-rules

현재 구성된 8000 Series fastpath 규칙을 표시합니다. 이 명령은 8000 Series 디바이스에서만 사용할 수 있습니다.

액세스

기본

Syntax

```
show fastpath-rules
```

예

```
> show fastpath-rules
```

gui

웹 인터페이스의 현재 상태를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show gui
```

예

```
> show gui
```

hostname

디바이스의 호스트 이름 및 어플라이언스 UUID를 표시합니다. CLI를 사용하여 디바이스의 호스트 이름을 수정하려면 관리하는 Firepower Management Center에 변경 사항이 반영되는지 확인하십시오. 경우에 따라 디바이스 관리 설정을 수동으로 편집해야 할 수도 있습니다.

액세스

기본

Syntax

```
show hostname
```

예

```
> show hostname
```

호스트

ASA FirePOWER 모듈의 /etc/hosts 파일 내용을 표시합니다.

액세스

기본

Syntax

```
show hosts
```

예

```
> show hosts
```

hyperthreading

하이퍼스레딩의 활성화 여부를 표시합니다. 이 명령은 ASA FirePOWER에서 사용할 수 없습니다.

액세스

기본

Syntax

```
show hyperthreading
```

예

```
> show hyperthreading
```

inline-sets

모든 인라인 보안 영역 및 관련 인터페이스의 구성 데이터를 표시합니다. 이 명령은 ASA FirePOWER에서 사용할 수 없습니다.

액세스

기본

Syntax

```
show inline-sets
```

예

```
> show inline-sets
```

인터페이스

매개 변수를 지정하지 않으면 구성된 모든 인터페이스의 목록이 표시됩니다. 매개 변수를 지정하면 지정된 인터페이스에 대한 자세한 정보가 표시됩니다.

액세스

기본

Syntax

```
show interfaces interface
```

여기서 *interface*는 자세한 정보를 원하는 특정 인터페이스입니다.

예

```
> show interfaces
```

ifconfig

ASA FirePOWER 모듈에 대한 인터페이스 구성을 표시합니다.

액세스

기본

Syntax

```
show ifconfig
```

예

```
> show ifconfig
```

lcd

LCD 하드웨어 디스플레이의 활성화 여부를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show lcd
```

예

```
> show lcd
```

link-aggregation 명령

`show link-aggregation` 명령은 LAG(link aggregation group)에 대한 디스플레이 구성 및 통계 정보를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER 디바이스에서는 사용할 수 없습니다.

액세스

기본

구성

LAG ID, 인터페이스 수, 구성모드, 로드 밸런싱 모드, LACP 정보, 물리적 인터페이스 유형 등 구성된 각 LAG에 대한 구성 세부사항을 표시합니다.

액세스

기본

Syntax

```
show link-aggregation configuration
```

예

```
> show link-aggregation configuration
```

statistics

상태, 링크 상태와 속도, 구성모드, 수신/송신된 패킷의 카운터, 수신/송신된 바이트의 카운터를 비롯한 구성된 각 LAG에 대한 통계를 인터페이스별로 표시합니다.

액세스

기본

Syntax

```
show link-aggregation statistics
```

예

```
> show link-aggregation statistics
```

link-state

디바이스 포트의 유형, 링크, 속도, 이중 상태, 우회 모드를 표시합니다. 이 명령은 ASA FirePOWER 디바이스에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show link-state
```

예

```
> show link-state
```

log-ips-connection

로깅된 침입 이벤트와 관련된 연결 이벤트 로깅의 활성화 여부를 표시합니다.

액세스

기본

Syntax

```
show log-ips-connection
```

예

```
> show log-ips-connection
```

관리자

Firepower Management Center의 구성 및 통신 상태를 표시합니다. 등록이 보류 중이면 등록 키와 NAT ID만 표시됩니다.

디바이스가 스태킹된 구성에서 보조 디바이스로 구성된 경우, 관리하는 FMC 및 기본 디바이스 모두에 대한 정보가 표시됩니다.

액세스

기본

Syntax

```
show managers
```

예

```
> show managers
```

memory

디바이스에 대한 총 메모리, 사용 중인 메모리 및 사용 가능한 메모리를 표시합니다.

액세스

기본

Syntax

```
show memory
```

예

```
> show memory
```

모델

디바이스의 모델 정보를 표시합니다.

액세스

기본

Syntax

```
show model
```

예

```
> show model
```

mpls-depth

관리 인터페이스에 구성된 MPLS 레이어의 수(0~6)를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show mpls-depth
```

예

```
> show mpls-depth
```

NAT 명령

`show nat` 명령은 관리 인터페이스에 대한 NAT 데이터 및 구성 정보를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER 디바이스에서는 사용할 수 없습니다.

액세스

기본

active-dynamic

동적 규칙에 따라 변환된 NAT 플로우를 표시합니다. 이러한 항목은 플로우가 규칙과 일치할 때 표시되며, 규칙이 시간 초과될 때까지 지속됩니다. 따라서 목록이 부정확할 수 있습니다. 시간 초과는 프로토콜에 따라 다릅니다. ICMP는 5초, UDP는 120초, TCP는 3600초, 나머지 모든 프로토콜은 60초입니다.

Syntax

```
show nat active-dynamic
```

예

```
> show nat active-dynamic
```

active-static

고정 규칙에 따라 변환된 NAT 플로우를 표시합니다. 이러한 항목은 디바이스에 규칙을 구축하자마자 표시되며, 목록은 고정 NAT 규칙과 일치하는 활성 플로우를 나타내지 않습니다.

Syntax

```
show nat active-static
```

예

```
> show nat active-static
```

allocators

동적 규칙에 사용되는 변환된 주소의 풀인 모든 NAT allocator에 대한 정보를 표시합니다.

Syntax

```
show nat allocators
```

예

```
> show nat allocators
```

config

관리 인터페이스에 대한 현재 NAT 정책 구성을 표시합니다.

Syntax

```
show nat config
```

예

```
> show nat config
```

dynamic-rules

지정된 allocator ID를 사용하는 동적 NAT 규칙을 표시합니다.

Syntax

```
show nat dynamic-rules allocator_id
```

여기서 `allocator_id`는 유효한 allocator ID 번호입니다.

예

```
> show nat dynamic-rules 9
```

플로우

지정된 allocator ID를 사용하는 규칙에 대한 플로우의 수를 표시합니다.

Syntax

```
show nat flows allocator-id
```

여기서 *allocator_id*는 유효한 allocator ID 번호입니다.

예

```
> show nat flows 81
```

static-rules

모든 고정 NAT 규칙을 표시합니다.

Syntax

```
show nat static-rules
```

예

```
> show nat static-rules
```

netstat

ASA FirePOWER 모듈에 대한 활성 네트워크 연결을 표시합니다.

액세스
기본

Syntax

```
show netstat
```

예

```
> show netstat
```

network

관리 인터페이스의 IPv4 및 IPv6 구성, MAC 주소, HTTP 프록시 주소, 포트 및 사용자 이름을 표시합니다(구성된 경우).

액세스

기본

Syntax

```
show network
```

예

```
> show network
```

network-modules

설치된 모든 모듈 및 해당 정보를 일련 번호와 함께 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show network-modules
```

예

```
> show network-modules
```

network-static-routes

구성된 모든 네트워크 고정 경로와 해당 정보(인터페이스, 대상 주소, 네트워크 마스크, 게이트웨이 주소 포함)를 표시합니다.

액세스

기본

Syntax

```
show network-static-routes
```

예

```
> show network-static-routes
```

ntp

ntp 구성을 표시합니다.

액세스

기본

Syntax

```
show ntp
```

예

```
> show ntp
```

perfstats

디바이스에 대한 성능 통계를 표시합니다.

액세스

기본

Syntax

```
show perfstats
```

예

```
> show perfstats
```

portstats

디바이스에 설치된 모든 포트에 대한 포트 통계를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show portstats [copper | fiber | internal | external | all]
```

여기서 copper는 모든 copper 포트를, fiber는 모든 fiber 포트를, internal은 모든 internal 포트를, external은 모든 external 포트를, all은 모든 포트(external 및 internal)를 지정합니다.

예

```
> show portstats fiber
```

power-supply-status

하드웨어 전력 공급 장치의 현재 상태를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show power-supply-status
```

예

```
> show power-supply-status
```

process-tree

디바이스에서 현재 실행 중인 프로세스를 유형별 트리 형식으로 정렬하여 표시합니다.

액세스

기본

Syntax

```
show process-tree
```

예

```
> show process-tree
```

processes

디바이스에서 현재 실행 중인 프로세스를 내림차순 CPU 사용량으로 정렬하여 표시합니다.

액세스

기본

Syntax

```
show processes sort-flag filter
```

여기서 *sort-flag*에는 `-m`(메모리 기준 내림차순 정렬), `-u`(프로세스 이름보다는 사용자 이름 기준 정렬) 또는 `verbose`(명령의 전체 이름 및 경로 표시)를 사용할 수 있습니다. *filter* 매개 변수는 명령 또는 사용자 이름에서 결과가 필터링되는 검색어를 지정합니다. 헤더 행은 여전히 표시됩니다.

예

```
> show processes -u user1
```

route

ASA FirePOWER 모듈의 라우팅 정보를 표시합니다.

액세스

기본

Syntax

```
show route
```

예

```
> show route
```

routing-table

매개 변수를 지정하지 않으면 모든 가상 라우터에 대한 라우팅 정보가 표시됩니다. 매개 변수를 지정하면 지정한 라우터 및 지정한 라우팅 프로토콜 유형(해당되는 경우)이 표시됩니다. 모든 매개 변수는 선택 사항입니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show routing-table name [ ospf | rip | static ]
```

여기서 *name*은 정보를 원하는 특정 라우터의 이름이고 `ospf`, `rip` 및 `static`은 라우팅 프로토콜 유형을 지정합니다.

예

```
> show routing-table Vrouter1 static
```

serial-number

새시 일련 번호를 표시합니다. 이 명령은 NGIPSv에서 사용할 수 없습니다.

액세스

기본

Syntax

```
show serial-number
```

예

```
> show serial-number
```

ssl-policy-config

정책 설명, 기본 로깅 설정, 활성화된 모든 SSL 규칙 및 규칙 구성, 신뢰할 수 있는 CA 인증서, 해독 불가 트래픽 작업을 포함하여 현재 구축된 SSL 정책 구성을 표시합니다.

액세스

기본

Syntax

```
show ssl-policy-config
```

예

```
> show ssl-policy-config
```

스태킹

매니지드 디바이스에서 스태킹 구성 및 위치를 표시하고, 기본 디바이스로 구성된 디바이스에서는 모든 보조 디바이스에 대한 데이터도 나열합니다. 고가용성 쌍의 스택인 경우, 이 명령은 스택이 고가용성 쌍의 멤버라는 것도 나타냅니다. 사용자는 웹 인터페이스를 사용하여 스태킹을 활성화(대부분의 경우)하거나 비활성화해야 합니다. 스태킹이 활성화되어 있지 않으면 `Stacking not currently configured`가 반환됩니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show stacking
```

예

```
> show stacking
```

summary

가장 흔히 사용되는 디바이스 정보(버전, 유형 UUID 등)의 요약을 표시합니다. 자세한 내용은 `show` 명령(`version`, `interfaces`, `device-settings`, `access-control-config`)을 참조하십시오.

액세스

기본

Syntax

```
show summary
```

예

```
> show summary
```

시간

현재 날짜와 시간을 UTC 및 현재 사용자에 대해 구성된 현지 표준 시간대로 표시합니다.

액세스

기본

Syntax

```
show time
```

예

```
> show time
```

traffic-statistics

매개 변수를 지정하지 않으면 모든 포트에서 전송 및 수신된 바이트에 대한 세부사항이 표시됩니다. 포트를 지정하면 지정한 포트에 대한 정보만 표시됩니다. ASA FirePOWER 모듈에 대해서는 포트를 지정할 수 없으며, 시스템은 데이터 평면 인터페이스만 표시합니다.

참고 일부 상황에서 실제로 디바이스가 트래픽을 삭제하지 않을 때 이 명령의 출력이 패킷 삭제를 표시할 수 있습니다. 잘못된 형식의 패킷이 수신되면 삭제 카운터가 증가합니다. 잘못된 형식의 패킷은 헤더에서 특정 정보가 누락되거나 CRC(Cyclical Redundancy Check)에 실패했을 수 있습니다. 일반적으로 형식이 잘못된 패킷의 근본 원인은 잘못된 케이블이나 잘못된 인터페이스 같은 데이터 링크 레이어 문제입니다. 삭제된 패킷은 로깅되지 않습니다. 하지만 소스가 TCP와 같은 신뢰할 수 있는 전송 프로토콜인 경우, 패킷이 재전송됩니다.

액세스

기본

Syntax

```
show traffic-statistics port
```

여기서 *port*는 정보를 원하는 특정 포트입니다.

예

```
> show traffic-statistics s1p1
```

user

NGIPSv에만 해당합니다. 지정된 사용자에 대한 자세한 구성 정보를 표시합니다. 다음 값이 표시됩니다.

- Login - 로그인 이름
- UID - 숫자 사용자 ID.
- Auth(`Local` 또는 `Remote`) - 사용자를 인증하는 방법
- Access(`Basic` 또는 `Config`) - 사용자의 권한 레벨
- Enabled (`Enabled` 또는 `Disabled`) - 사용자가 활성 상태인지 여부
- Reset(`Yes` 또는 `No`) - 다음 로그인 때 사용자가 비밀번호를 변경해야 하는지 여부
- Exp(`Never` 또는 숫자) - 사용자 비밀번호를 변경해야 할 때까지의 일수
- Warn(`N/A` 또는 숫자) - 비밀번호가 만료되기 전 사용자에게 변경을 알리는 일수
- Str(`Yes` 또는 `No`) - 사용자 비밀번호가 강도 검사 기준을 충족해야 하는지 여부
- Lock(`Yes` 또는 `No`) - 로그인 실패가 너무 많아 사용자 계정이 잠겼는지 여부
- Max(`N/A` 또는 숫자) - 사용자 계정이 잠길 때까지 최대 로그인 실패 수

액세스

구성

Syntax

```
show user username username username ...
```

여기서 *username*은 사용자의 이름을 지정하며, 사용자 이름은 공백으로 분리합니다.

예

```
> show user jdoe
```

사용자

NGIPSv 및 ASA FirePOWER에만 해당합니다. 모든 로컬 사용자에 대한 자세한 구성 정보를 표시합니다. 다음 값이 표시됩니다.

- Login - 로그인 이름
- UID - 숫자 사용자 ID.
- Auth(`Local` 또는 `Remote`) - 사용자를 인증하는 방법

- Access(`Basic` 또는 `Config`) - 사용자의 권한 레벨
- Enabled (`Enabled` 또는 `Disabled`) - 사용자가 활성 상태인지 여부
- Reset(`Yes` 또는 `No`) - 다음 로그인 때 사용자가 비밀번호를 변경해야 하는지 여부
- Exp(`Never` 또는 숫자) - 사용자 비밀번호를 변경해야 할 때까지의 일수
- Warn(`N/A` 또는 숫자) - 비밀번호가 만료되기 전 사용자에게 변경을 알리는 일수
- Str(`Yes` 또는 `No`) - 사용자 비밀번호가 강도 검사 기준을 충족해야 하는지 여부
- Lock (`Yes` or `No`) - 로그인 실패가 너무 많아 사용자 계정이 잠겨 있는지 여부
- Max(`N/A` 또는 숫자) - 사용자 계정이 잠길 때까지 최대 로그인 실패 수

액세스

구성

Syntax

```
show users
```

예

```
> show users
```

버전

제품 버전 및 빌드를 표시합니다. `detail` 매개 변수를 지정하면 추가 구성 요소의 버전이 표시됩니다.

참고 `detail` 매개 변수는 ASA with FirePOWER Services에서 사용할 수 없습니다.

액세스

기본

Syntax

```
show version [detail]
```

예

```
> show version
```

virtual-routers

매개 변수를 지정하지 않으면 DHCP 릴레이, OSPF 및 RIP 정보와 함께 현재 구성된 모든 가상 라우터 목록이 표시됩니다. 매개 변수를 지정하면 지정된 경로 유형으로 제한된, 지정된 라우터에 대한 정보가 표시됩니다. 모든 매개 변수는 선택 사항입니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show virtual-routers [ dhcprelay | ospf | rip ] name
```

여기서 `dhcprelay`, `ospf` 및 `rip`는 경로 유형을 지정하고 *name*은 정보를 원하는 특정 라우터의 이름입니다. `ospf`를 지정하면 경로 유형과 라우터 이름(있는 경우) 간 `neighbors`, `topology` 또는 `lsadb`를 추가로 지정할 수 있습니다.

예

```
> show virtual-routers ospf VRouter2
```

virtual-switches

매개 변수를 지정하지 않으면 현재 구성된 모든 가상 스위치의 목록이 표시됩니다. 매개 변수를 지정하면 지정한 스위치에 대한 정보가 표시됩니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

기본

Syntax

```
show virtual-switches name
```

예

```
> show virtual-switches Vswitch1
```

vmware-tools

가상 디바이스에서 VMware Tools가 현재 활성화되었는지를 나타냅니다. 이 명령은 NGIPSv에서만 사용할 수 있습니다.

VMware Tools는 가상 머신의 성능 향상을 위한 유틸리티 제품군입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. 다음 플러그인은 모든 가상 어플라이언스에서 지원됩니다.

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware Tools 및 지원되는 플러그인에 대한 자세한 내용은 VMware 웹사이트(http://www.vmware.com)를 참조하십시오.

액세스

기본

Syntax

```
show vmware-tools
```

예

```
> show vmware-tools
```

VPN 명령

`show VPN` 명령은 VPN 연결에 대한 VPN 상태 및 구성 정보를 표시합니다. 이 명령은 NGIPSv 및 ASA FirePOWER 디바이스에서는 사용할 수 없습니다.

액세스

기본

config

모든 VPN 연결의 구성을 표시합니다.

Syntax

```
show vpn config
```

예

```
> show vpn config
```

config by virtual router

가상 라우터에 대한 모든 VPN 연결의 구성을 표시합니다.

Syntax

```
show vpn config virtual router
```

예

```
> show vpn config VRouter1
```

status

모든 VPN 연결의 상태를 표시합니다.

Syntax

```
show vpn status
```

예

```
> show vpn status
```

status by virtual router

가상 라우터에 대한 모든 VPN 연결의 상태를 표시합니다.

Syntax

```
show vpn status virtual router
```

예

```
> show vpn status VRouter1
```

카운터

모든 VPN 연결의 카운터를 표시합니다.

Syntax

```
show vpn counters
```

예

```
> show vpn counters
```

counters by virtual router

가상 라우터에 대한 모든 VPN 연결의 카운터를 표시합니다.

Syntax

```
show vpn counters virtual router
```

예

```
> show vpn counters VRouter1
```

클래식 디바이스 CLI 구성 명령

configuration 명령을 통해 사용자는 시스템을 구성 및 관리할 수 있습니다. 이러한 명령은 시스템 운영에 영향을 미칩니다. 따라서 기본 레벨 `configure password`를 제외하고 구성 CLI 액세스 권한이 있는 사용자만 이러한 명령을 실행할 수 있습니다.

우회

7000 또는 8000 Series 디바이스에서는 인라인 쌍을 fail-open(하드웨어 우회) 또는 fail-close 모드에 배치합니다. 이 명령은 인라인 집합 **Bypass Mode** 옵션이 **Bypass**로 설정된 경우에만 사용할 수 있습니다.

디바이스를 재부팅하면 인라인 집합이 fail-open 모드에서 빠져나옵니다.

액세스

구성

Syntax

```
configure bypass {open | close} {interface}
```

여기서 `interface`는 인라인 쌍에 있는 두 하드웨어 포트 중 하나의 이름입니다.

예

```
> configure bypass open s1p1
```

high-availability

디바이스에서 고가용성을 위한 우회를 비활성화하거나 구성합니다. 이 명령은 NGIPSv, ASA FirePOWER 또는 보조 스택 멤버로 구성된 디바이스에서 사용할 수 없습니다.

액세스

구성

Syntax

```
configure high-availability {disable | bypass}
```

예

```
> configure high-availability disable
```

gui

시스템에 대한 주요 업데이트 중 나타나는 간소화된 업그레이드 웹 인터페이스를 비롯한 디바이스 웹 인터페이스를 활성화 또는 비활성화합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

구성

Syntax

```
configure gui [enable | disable]
```

예

```
> configure gui disable
```

lcd

디바이스 앞쪽에 있는 LCD 디스플레이를 활성화 또는 비활성화합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

구성

Syntax

```
configure lcd {enable | disable}
```

예

```
> configure lcd disable
```

log-ips-connections

로깅된 침입 이벤트와 관련이 있는 연결 이벤트의 로깅을 활성화 또는 비활성화합니다.

액세스

구성

Syntax

```
configure log-ips-connections {enable | disable}
```

예

```
> configure log-ips-connections disable
```

manager 명령

`configure manager` 명령은 관리하는 Firepower Management Center에 대한 디바이스의 연결을 구성합니다.

액세스

구성

add

관리하는 Firepower Management Center로부터의 연결을 허용하도록 디바이스를 구성합니다. 이 명령은 디바이스가 적극적으로 관리되지 않는 경우에만 실행됩니다.

디바이스를 Firepower Management Center에 등록하려면 고유한 영숫자 등록 키가 항상 필요합니다. 대부분의 경우 등록 키와 함께 호스트 이름 또는 IP 주소를 제공해야 합니다. 그러나 디바이스와 Firepower Management Center가 NAT 디바이스에 의해 분리된 경우, 등록 키와 함께 고유한 NAT ID를 입력하고 호스트 이름 대신 `DONTRESOLVE`를 지정해야 합니다.

Syntax

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]
```

여기서 {hostname | IPv4_address | IPv6_address | DONTRESOLVE}는 이 디바이스를 관리하는 Firepower Management Center의 DNS 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다. Firepower Management Center의 주소를 직접 지정할 수 없는 경우 DONTRESOLVE를 사용합니다. DONTRESOLVE를 사용하는 경우, nat_id가 필요합니다. regkey는 디바이스를 Firepower Management Center에 등록하는 데 필요한 고유한 영숫자 등록 키입니다. nat_id는 등록 프로세스 중에 Firepower Management Center과 디바이스 사이에서 사용되는 선택 사항인 영숫자 문자열입니다. 호스트 이름이 DONTRESOLVE로 설정된 경우 반드시 필요합니다.

예

```
> configure manager add DONTRESOLVE abc123 efg456
```

delete

디바이스에서 Firepower Management Center의 연결 정보를 제거합니다. 이 명령은 디바이스가 적극적으로 관리되지 않는 경우에만 작동합니다.

Syntax

```
configure manager delete
```

예

```
> configure manager delete
```

mpls-depth

관리 인터페이스에서 MPLS 레이어의 수를 구성합니다. 이 명령은 NGIPSv 및 ASA FirePOWER에서는 사용할 수 없습니다.

액세스

구성

Syntax

```
configure mpls-depth depth
```

여기서 *depth*는 0~6의 숫자입니다.

예

```
> configure mpls-depth 3
```

network 명령

configure network 명령은 디바이스의 관리 인터페이스를 구성합니다.

액세스

구성

dns searchdomains

DNS 검색 도메인의 현재 목록을 명령에 지정된 목록으로 교체합니다.

Syntax

```
configure network dns searchdomains {searchlist}
```

여기서 searchlist는 쉼표로 구분된 도메인 목록입니다.

예

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

DNS 서버의 현재 목록을 명령에 지정된 목록으로 교체합니다.

Syntax

```
configure nework dns servers {dnslist}
```

여기서 dnslist는 쉼표로 구분된 DNS 서버 목록입니다.

예

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

디바이스의 호스트 이름을 설정합니다.

Syntax

```
configure network hostname {name}
```

여기서 name은 새 호스트 이름입니다.

예

```
> configure network hostname sfrocks
```

http-proxy

7000 및 8000 Series 및 NGIPSv 디바이스에서 HTTP 프록시를 구성합니다. 명령을 실행하면 CLI는 사용자에게 HTTP 프록시 주소와 포트, 프록시 인증이 필요한지 여부를 묻는 프롬프트를 표시하며, 해당 인증이 필요한 경우 프록시 사용자 이름, 프록시 비밀번호, 프록시 비밀번호 확인 프롬프트를 표시합니다.

가상 디바이스가 동적 분석을 위해 AMP 클라우드에 파일을 제출할 수 있도록 HTTP 프록시 서버를 구성하려면 NGIPSv에서 이 명령을 사용하십시오.

Syntax

프록시 비밀번호는 영숫자 문자만 사용할 수 있습니다.

```
configure network http-proxy
```

예

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

7000 시리즈, 8000 Series 또는 NGIPSv 디바이스에서 모든 HTTP 프록시 구성을 삭제합니다.

Syntax

```
configure network http-proxy-disable
```

예

```
> configure network http-proxy-disable
```

```
Are you sure that you wish to delete the current
http-proxy configuration? (y/n):
```

ipv4 delete

디바이스 관리 인터페이스의 IPv4 구성을 비활성화합니다.

Syntax

```
configure network ipv4 delete
```

예

```
> configure network ipv4 delete eth1
```

ipv4 dhcp

디바이스 관리 인터페이스의 IPv4 구성을 DHCP로 설정합니다. 관리 인터페이스는 DHCP 서버와 통신하여 구성 정보를 가져옵니다.

Syntax

```
configure network ipv4 dhcp [management_interface]
```

여기서 *management_interface*는 관리 인터페이스 ID입니다. DHCP는 기본 관리 인터페이스에서만 지원되므로 이 인수를 사용할 필요가 없습니다.

예

```
> configure network ipv4 dhcp
```

ipv4 manual

디바이스 관리 인터페이스의 IPv4 구성을 수동으로 구성합니다.

Syntax

```
configure network ipv4 manual ipaddr netmask [gw]
```

여기서 *ipaddr*은 IP 주소, *netmask*는 서브넷 마스크, *gw*는 기본 게이트웨이의 IPv4 주소입니다.

예

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

디바이스 관리 인터페이스의 IPv6 구성을 비활성화합니다.

Syntax

```
configure network ipv6 delete
```

예

```
> configure network ipv6 delete
```

ipv6 dhcp

디바이스 관리 인터페이스의 IPv6 구성을 DHCP로 설정합니다. 관리 인터페이스는 DHCP 서버와 통신하여 구성 정보를 가져옵니다.

Syntax

```
configure network ipv6 dhcp [management_interface]
```

여기서 *management_interface*는 관리 인터페이스 ID입니다. DHCP는 기본 관리 인터페이스에서만 지원되므로 이 인수를 사용할 필요가 없습니다.

예

```
> configure network ipv6 dhcp
```

ipv6 manual

디바이스 관리 인터페이스의 IPv6 구성을 수동으로 구성합니다.

Syntax

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw]
```

여기서 *ip6addr*/*ip6prefix*는 IP 주소 및 접두사 길이이고, *ip6gw*는 기본 게이트웨이의 IPv6 주소입니다.

예

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

ipv6 router

디바이스 관리 인터페이스의 IPv6 구성을 Router로 설정합니다. 관리 인터페이스는 IPv6 라우터와 통신하여 구성 정보를 가져옵니다.

Syntax

```
configure network ipv6 router
```

예

```
> configure network ipv6 router
```

management-interface disable

관리 인터페이스를 비활성화합니다. 여러 관리 인터페이스는 8000 Series 디바이스와 FirePOWER 서비스가 포함된 ASA 5585-X에서만 지원됩니다.

Syntax

```
configure network management-interface disable ethn
```

여기서 *n* 은 구성하려는 관리 인터페이스의 수입니다. **eth0**는 기본 관리 인터페이스이고 **eth1**은 선택 사항인 이벤트 인터페이스입니다. 관리 채널과 이벤트 채널이 모두 활성화된 상태로 eth0 기본 관리 인터페이스를 활성화된 상태로 두는 것이 좋습니다. Firepower Management Center 및 매니지드 디바이스에서 별도의 이벤트 인터페이스를 사용하는 자세한 방법은 Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지의 내용을 참조하십시오.

예

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

지정된 관리 인터페이스에서 이벤트 트래픽 채널을 비활성화합니다. 여러 관리 인터페이스는 8000 Series 디바이스와 FirePOWER 서비스가 포함된 ASA 5585-X에서만 지원됩니다.

Syntax

```
configure network management-interface disable-event-channel ethn
```

여기서 *n* 은 구성하려는 관리 인터페이스의 수입니다. **eth0**는 기본 관리 인터페이스이고 **eth1**은 선택 사항인 이벤트 인터페이스입니다. 관리 채널과 이벤트 채널이 모두 활성화된 상태로 eth0 기본 관리 인터페이스를 활성화된 상태로 두는 것이 좋습니다. Firepower Management Center 및 매니지드 디바이스에서 별도의 이벤트 인터페이스를 사용하는 자세한 방법은 Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지의 내용을 참조하십시오.

예

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

지정된 인터페이스에서 관리 채널을 비활성화합니다. 여러 관리 인터페이스는 8000 Series 디바이스와 FirePOWER 서비스가 포함된 ASA 5585-X에서만 지원됩니다.

Syntax

```
configure network management-interface disable-management-channel ethn
```

여기서 *n* 은 구성하려는 관리 인터페이스의 수입니다. **eth0**는 기본 관리 인터페이스이고 **eth1**은 선택 사항인 이벤트 인터페이스입니다. 관리 채널과 이벤트 채널이 모두 활성화된 상태로 eth0 기본 관리 인터페이스를 활성화된 상태로 두는 것이 좋습니다. Firepower Management Center 및 매니지드 디바이스에서 별도의 이벤트 인터페이스를 사용하는 자세한 방법은 Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지의 내용을 참조하십시오.

예

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

지정된 관리 인터페이스를 활성화합니다. 여러 관리 인터페이스는 8000 Series 디바이스와 FirePOWER 서비스가 포함된 ASA 5585-X에서만 지원됩니다.

Syntax

```
configure network management-interface enable ethn
```

여기서 *n* 은 활성화 하려는 관리 인터페이스의 수입니다. **eth0** 는 기본 관리 인터페이스 및 **eth1** 선택적 이벤트 인터페이스입니다.

디바이스 관리의 경우, Firepower Management Center 관리 인터페이스에는 두 개의 별도 트래픽 채널이 있습니다. 즉, 관리 트래픽 채널은 모든 내부 트래픽(예: 디바이스 관리와 관련된 디바이스 간 트래픽)을 전달하고, 이벤트 트래픽 채널은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다. 원하는 경우, Management Center에 별도의 이벤트 전용 인터페이스를 구성하여 이벤트 트래픽을 처리할 수도 있습니다(이 구성을 수행하려면 Firepower Management Center 참조). 하나의 이벤트 전용 인터페이스만 구성할 수 있습니다. 이벤트 트래픽은 많은 양의 대역폭을 사용할 수 있으므로 관리 트래픽에서 이벤트 트래픽을 분리하면 Management Center의 성능이 향상될 수 있습니다.

기본 eth0 인터페이스는 기본적으로 관리 채널과 이벤트 채널을 모두 포함합니다. 원하는 경우, eth0 인터페이스를 이벤트 전용 인터페이스로 활성화할 수 있습니다. 이벤트 트래픽은 가능한 경우, 디바이스 이벤트 인터페이스와 Firepower Management Center 이벤트 인터페이스 간에 전송됩니다. 이벤트 네트워크가 다운되면 이벤트 트래픽은 기본 관리 인터페이스로 되돌아갑니다. 가능하다면 별도의 이벤트 인터페이스가 사용되지만 관리 인터페이스는 항상 백업입니다.

관리 인터페이스를 활성화하면 관리 채널과 이벤트 채널이 기본적으로 모두 활성화됩니다. 관리 채널과 이벤트 채널 모두에 기본 관리 인터페이스를 사용한 다음 이벤트 전용 인터페이스를 활성화하

는 것이 좋습니다. Firepower Management Center 이벤트 전용 인터페이스는 관리 채널 트래픽을 허용할 수 없으므로 디바이스 이벤트 인터페이스에서 관리 채널을 비활성화해야 합니다.

configure network {**ipv4** | **ipv6**} **manual** 명령을 사용하여 관리 인터페이스의 주소를 구성합니다.

예

```
> configure network management-interface enable eth1
> configure network management-interface disable-management-channel eth1
```

management-interface enable-event-channel

지정된 관리 인터페이스에서 이벤트 트래픽 채널을 활성화합니다. 여러 관리 인터페이스는 8000 Series 디바이스와 FirePOWER 서비스가 포함된 ASA 5585-X에서만 지원됩니다.

Syntax

```
configure network management-interface enable-event-channel ethn
```

여기서 *n* 은 구성하려는 관리 인터페이스의 수입니다. **eth0**는 기본 관리 인터페이스이고 **eth1**은 선택 사항인 이벤트 인터페이스입니다. 관리 채널과 이벤트 채널이 모두 활성화된 상태로 eth0 기본 관리 인터페이스를 활성화된 상태로 두는 것이 좋습니다. Firepower Management Center 및 매니지드 디바이스에서 별도의 이벤트 인터페이스를 사용하는 자세한 방법은 Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지의 내용을 참조하십시오.

예

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

지정된 관리 인터페이스에서 관리 트래픽 채널을 활성화합니다. 여러 관리 인터페이스는 8000 Series 디바이스와 FirePOWER 서비스가 포함된 ASA 5585-X에서만 지원됩니다.

Syntax

```
configure network management-interface enable-management-channel ethn
```

여기서 *n* 은 구성하려는 관리 인터페이스의 수입니다. **eth0**는 기본 관리 인터페이스이고 **eth1**은 선택 사항인 이벤트 인터페이스입니다. 관리 채널과 이벤트 채널이 모두 활성화된 상태로 eth0 기본 관리 인터페이스를 활성화된 상태로 두는 것이 좋습니다. Firepower Management Center 및 매니지드 디바이스에서 별도의 이벤트 인터페이스를 사용하는 자세한 방법은 Management Interfaces(관리 인터페이스)관리 인터페이스, 1353 페이지의 내용을 참조하십시오.

예

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

관리용 TCP 포트의 값을 변경합니다.

Syntax

```
configure network management-interface tcpport port
```

여기서 *port*는 구성하려는 관리 포트 값입니다.

예

```
> configure network management-interface tcpport 8500
```

management-port

디바이스의 TCP 관리 포트 값을 설정합니다.

Syntax

```
configure network management-port number
```

여기서 *number*는 구성하려는 관리 포트 값입니다.

예

```
> configure network management-port 8500
```

static-routes ipv4 add

지정된 관리 인터페이스에 대한 IPv4 고정 경로를 추가합니다.

Syntax

```
configure network static-routes ipv4
add interface destination netmask gateway
```

여기서 interface는 관리 인터페이스, destination은 목적지 IP 주소, netmask는 네트워크 마스크 주소, gateway는 추가하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv4
add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

지정된 관리 인터페이스에 대한 IPv4 고정 경로를 삭제합니다.

Syntax

```
configure network static-routes ipv4
delete interface destination netmask gateway
```

여기서 interface는 관리 인터페이스, destination은 목적지 IP 주소, netmask는 네트워크 마스크 주소, gateway는 삭제하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv4
delete eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv6 add

지정된 관리 인터페이스에 대한 IPv6 고정 경로를 추가합니다.

Syntax

```
configure network static-routes ipv6
add interface destination prefix gateway
```

여기서 interface는 관리 인터페이스, destination은 목적지 IP 주소, prefix는 IPv6 접두사 길이, gateway는 추가하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv6
add eth1 2001:DB8:3ffe:1900:4545:3:200: f8ff:fe21:67cf 64
```

static-routes ipv6 delete

지정된 관리 인터페이스에 대한 IPv6 고정 경로를 삭제합니다.

Syntax

```
configure network static-routes ipv6
delete interface destination prefix gateway
```

여기서 interface는 관리 인터페이스, destination은 목적지 IP 주소, prefix는 IPv6 접두사 길이, gateway는 삭제하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv6
delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff: fe21:67cf 64
```

password

현재 사용자가 자신의 비밀번호를 변경하도록 허용합니다. 이 명령을 실행하면 현재(또는 이전) 비밀번호를 입력하라는 CLI 프롬프트가 표시된 다음 새 비밀번호를 두 번 입력하라는 프롬프트가 표시됩니다.

액세스

기본

Syntax

```
configure password
```

예

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

stacking disable

7000 및 8000 Series 디바이스에서 해당 디바이스에 있는 모든 스태킹 구성을 제거합니다.

- 기본 디바이스로 구성된 디바이스에서는 스택이 완전히 제거됩니다.
- 보조 디바이스로 구성된 디바이스에서는 해당 디바이스가 스택에서 제거됩니다.

이 명령은 NGIPSv 또는 ASA FirePOWER 모듈에서 사용할 수 없으며, 디바이스 고가용성 쌍을 분리하는 데 사용할 수 없습니다.

스태킹 계층 구조에서 더 위에 있는 어플라이언스와 통신을 설정할 수 없는 경우 이 명령을 사용하십시오. Firepower Management Center를 통신에 이용할 수 있는 경우 대신 Firepower Management Center 웹 인터페이스를 사용하라는 메시지가 표시됩니다. 마찬가지로, 기본 디바이스를 이용할 수 있는 경우 보조로 구성된 디바이스에서 `stacking disable`을 입력하면 기본 디바이스에서 명령을 입력하라는 메시지가 나타납니다.

액세스

구성

Syntax

```
configure stacking disable
```

예

```
> configure stacking disable
```

user 명령

NGIPSv에만 적용 가능한 `configure user` 명령은 디바이스의 로컬 사용자 데이터베이스를 관리합니다.

액세스

구성

access

지정된 사용자의 액세스 레벨을 수정합니다. 이 명령은 지정된 사용자가 다음에 로그인할 때 적용됩니다.

Syntax

```
configure user access username [basic | config]
```

여기서 *username*은 액세스를 수정할 사용자의 이름을 지정하고, `basic`은 기본 액세스를 나타내며, `config`는 구성 액세스를 나타냅니다.

예

```
> configure user access jdoe basic
```

add

지정된 이름 및 액세스 레벨로 새 사용자를 생성합니다. 사용자의 비밀번호를 입력하라는 프롬프트가 표시됩니다.

Syntax

```
configure user add username [basic | config]
```

여기서 username은 새 사용자의 이름을 지정하고, basic은 기본 액세스를 나타내며, config는 구성 액세스를 나타냅니다.

예

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

사용자 비밀번호의 만료를 강제로 적용합니다.

Syntax

```
configure user aging username max_days warn_days
```

여기서 username은 사용자의 이름을 지정하고, max_days는 비밀번호가 유효한 최대 일수를 나타내며, warn_days는 비밀번호 만료 전 사용자에게 변경을 알리는 일수를 나타냅니다.

예

```
> configure user aging jdoe 100 3
```

delete

사용자 및 사용자 홈 디렉토리를 삭제합니다.

Syntax

```
configure user delete username
```

여기서 username은 사용자의 이름을 지정합니다.

예

```
> configure user delete jdoe
```

비활성화

사용자를 비활성화합니다. 비활성화된 사용자는 로그인할 수 없습니다.

Syntax

```
configure user disable username
```

여기서 username은 사용자의 이름을 지정합니다.

예

```
> configure user disable jdoe
```

enable

사용자를 활성화합니다.

Syntax

```
configure user enable username
```

여기서 username은 사용자의 이름을 지정합니다.

예

```
> configure user enable jdoe
```

forcereset

사용자가 다음에 로그인할 때 비밀번호를 변경하도록 합니다. 사용자가 로그인하여 비밀번호를 변경하면 강도 확인이 자동으로 활성화됩니다.

Syntax

```
configure user forcereset username
```

여기서 *username*은 사용자의 이름을 지정합니다.

예

```
> configure user forcereset jdoe
```

maxfailedlogins

지정된 사용자에 대한 최대 실패 로그인 수를 설정합니다.

Syntax

```
configure user maxfailedlogins username number
```

여기서 *username*은 사용자의 이름을, *number*는 최대 실패 로그인 수를 지정합니다.

예

```
> configure user maxfailedlogins jdoe 3
```

minpasswdlen

사용자 비밀번호에 포함되어야 할 최소 문자 수를 설정합니다.

Syntax

```
configure user minpasswdlen username number
```

여기서 *username*은 사용자 계정의 이름을 지정하고, *number*는 해당 계정에 포함되어야 할 최소 문자 수(1~127자)를 지정합니다.

예

```
> configure user minpasswdlen jdoe 13
```

password

사용자의 비밀번호를 설정합니다. 사용자의 비밀번호를 입력하라는 프롬프트가 표시됩니다.

Syntax

```
configure user password username
```

여기서 *username*은 사용자의 이름을 지정합니다.

예

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

사용자 비밀번호의 강도 요구 사항을 활성화 또는 비활성화합니다. 사용자 비밀번호가 만료되거나 configure user forcereset 명령이 사용되면, 사용자가 다음에 로그인할 때 이 요건이 자동으로 활성화됩니다.

Syntax

```
configure user strengthcheck username {enable | disable}
```

여기서 *username*은 사용자의 이름을 지정하고, `enable`은 지정된 사용자 비밀번호의 요구 사항을 설정하고, `disable`은 지정된 사용자 비밀번호의 요구 사항을 제거합니다.

예

```
> configure user strengthcheck jdoe enable
```

잠금 해제

실패한 로그인의 최대 수를 초과한 사용자의 잠금을 해제합니다.

Syntax

```
configure user unlock username
```

여기서 *username*은 사용자의 이름을 지정합니다.

예

```
> configure user unlock jdoe
```

vmware-tools

NGIPSv에서 VMware Tools 기능을 활성화하거나 비활성화합니다. 이 명령은 NGIPSv에서만 사용할 수 있습니다.

VMware Tools는 가상 머신의 성능 향상을 위한 유틸리티 제품군입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. 다음 플러그인은 모든 가상 어플라이언스에서 지원됩니다.

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware Tools 및 지원되는 플러그인에 대한 자세한 내용은 VMware 웹사이트(http://www.vmware.com)를 참조하십시오.

액세스

기본

Syntax

```
configure vmware-tools [enable | disable]
```

예

```
> configure vmware-tools enable
```

클래식 디바이스 CLI 시스템 명령

system 명령을 사용하면 시스템 전반의 파일 및 액세스 제어 설정을 관리할 수 있습니다. 구성 CLI 액세스 권한이 있는 사용자만 시스템 모드에서 명령을 실행할 수 있습니다.

access-control 명령

`system access-control` 명령을 사용하면 디바이스에서 액세스 제어 구성을 관리할 수 있습니다.

액세스

구성

archive

현재 구축된 액세스 제어 정책을 `/var/common`에 텍스트 파일로 저장합니다.

Syntax

```
system access-control archive
```

예

```
> system access-control archive
```

clear-rule-counts

액세스 제어 규칙 히트 수를 0으로 재설정합니다.

Syntax

```
system access-control clear-rule-counts
```

예

```
> system access-control clear-rule-counts
```

롤백

전에 구축된 액세스 제어 구성으로 시스템을 되돌립니다. 이 명령은 스택 또는 고가용성 쌍의 디바이스에 사용할 수 없습니다.

Syntax

```
system access-control rollback
```

예

```
> system access-control rollback
```

disable-http-user-cert

브라우저가 유효한 클라이언트 인증서를 제시해야 한다는 요구 사항을 비활성화합니다.

액세스

구성

Syntax

```
system disable-http-user-cert
```

예

```
> system disable-http-user-cert
```

file 명령

`system file` 명령을 사용하면 디바이스의 공통 디렉터리에서 파일을 관리할 수 있습니다.

액세스

구성

copy

로그인 사용자 이름을 사용하여 호스트에서 원격 위치로 파일을 전송하려면 FTP를 사용합니다. 로컬 파일은 공통 디렉터리에 두어야 합니다.

Syntax

```
system file copy hostname username path filenames filenames ...
```

여기서 `hostname`은 대상 원격 호스트의 이름 또는 IP 주소, `username`은 원격 호스트에 있는 사용자의 이름, `path`는 원격 호스트에 있는 대상 경로, `filenames`는 전송할 로컬 파일을 지정합니다. 파일 이름은 공백으로 구분합니다.

예

```
> system file copy sfrocks jdoe /pub *
```

delete

공통 디렉터리에서 지정된 파일을 제거합니다.

Syntax

```
system file delete filenames filenames ...
```

여기서 `filenames`는 삭제할 파일을 지정합니다. 파일 이름은 공백으로 구분됩니다.

예

```
> system file delete *
```

list

파일 이름을 지정하지 않으면 공통 디렉터리의 모든 파일에 대한 수정 시간, 크기 및 파일 이름이 표시됩니다. 파일 이름을 지정하면 지정된 파일 이름과 일치하는 파일에 대한 수정 시간, 크기 및 파일 이름이 표시됩니다.

Syntax

```
system file list filenames
```

여기서 *filenames*는 삭제할 파일을 지정합니다. 파일 이름은 공백으로 구분됩니다.

예

```
> system file list
```

secure-copy

로그인 사용자 이름을 사용하여 호스트에서 원격 위치로 파일을 전송하려면 SCP를 사용합니다. 로컬 파일은 `/var/common` 디렉터리에 두어야 합니다.

Syntax

```
system file secure-copy hostname username path filenames filenames ...
```

여기서 *hostname*은 대상 원격 호스트의 이름 또는 IP 주소, *username*은 원격 호스트에 있는 사용자의 이름, *path*는 원격 호스트에 있는 대상 경로, *filenames*는 전송할 로컬 파일을 지정합니다. 파일 이름은 공백으로 구분합니다.

예

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

Cisco에서 분석할 문제 해결 데이터를 생성합니다.

⚠

주의 메모리가 적은 디바이스에서 문제 해결 파일을 생성하는 경우 자동 애플리케이션 우회(AAB)가 활성화되어 있는 경우 AAB가 발생할 수 있습니다. 적어도 AAB가 작동하면 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 507 페이지을 참고하십시오. 일부 경우에는 AAB가 작동하여 디바이스가 일시적으로 동작하지 않을 수 있습니다. 만약 동작 정지 상태가 지속되면 Cisco TAC(Technical Assistance Center)에 문의할 경우 구축 시 적절한 솔루션을 제시할 것입니다. 영향을 받기 쉬운 디바이스에는 Firepower 7010, 7020 및 7030, 5508-X, 5516-X NGIPSv가 있습니다.

액세스

구성

Syntax

```
system generate-troubleshoot option1 optionN
```

여기서 옵션은 다음 중 하나 이상이며 공백으로 구분됩니다.

- `All`: 다음 옵션을 모두 실행.
- `SNT`: Snort 성능 및 구성
- `PER`: 하드웨어 성능 및 로그
- `SYS`: 시스템 구성, 정책, 로그

- DES: 탐지 구성, 정책, 로그
- NET: 인터페이스 및 네트워크 관련 데이터
- VDB: 검색, 인식, VDB 데이터, 로그
- UPG: 업그레이드 데이터 및 로그
- DBO: 모든 데이터베이스 데이터
- LOG: 모든 로그 데이터
- NMP: 네트워크 맵 정보

예

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

ldapsearch

사용자가 지정된 LDAP 서버의 쿼리를 수행할 수 있도록 합니다. 모든 매개 변수는 필수입니다.

액세스

구성

Syntax

```
system ldapsearch host port baseDN userDN basefilter
```

여기서 host는 LDAP 서버 도메인, port는 LDAP 서버 포트, baseDN은 검색을 위한 DN(고유 이름), userDN은 LDAP 디렉토리에 바인딩되는 사용자의 DN, basefilter는 검색하려는 레코드를 지정합니다.

예

```
> system ldapsearch ldap.example.com 389 cn=users,

dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown

`expert` 명령과 디바이스의 Linux 셸에 대한 액세스를 제거합니다.

⚠

주의 이 명령은 고객 지원의 핫픽스 없이는 취소할 수 없습니다. 주의해서 사용해야 합니다.

액세스

구성

Syntax

```
system lockdown
```

예

```
> system lockdown
```

nat rollback

전에 적용된 NAT 구성으로 시스템을 되돌립니다. 이 명령은 NGIPSv 또는 ASA FirePOWER에서 사용할 수 없습니다. 이 명령은 스택 또는 고가용성 쌍의 디바이스에 사용할 수 없습니다.

액세스

구성

Syntax

```
system nat rollback
```

예

```
> system nat rollback
```

reboot

디바이스를 재부팅합니다.

액세스

구성

Syntax

```
system reboot
```

예

```
> system reboot
```

restart

디바이스 애플리케이션을 다시 시작합니다.

액세스

구성

Syntax

```
system restart
```

예

```
> system restart
```

shutdown

디바이스를 종료합니다. 이 명령은 ASA FirePOWER 모듈에서 사용할 수 없습니다.

액세스

구성

Syntax

```
system shutdown
```

예

```
> system shutdown
```

클래식 디바이스 **CLI** 기록

기능	버전	세부 사항
사용되지 않는 CLI 명령	6.5	

기능	버전	세부 사항
		다음 CLI 명령은 버전 6.5에서 지원하지 않는 디바이스에서만 유용합니다. • **show alarms** • **show arp-tables** • **show bypass** 및 **config bypass** • **show high-availability** 및 **configure high-availability**(모든 명령) • **show fan-status** • **show fastpath-rules** • **show gui** 및 **configure gui** • **show http-cert-expire-date** • **show lcd** 및 **configure lcd** • **show link-aggregation** (모든 명령) • **show mpls-depth** 및 **configure mpls-depth** • **show nat** 및 **system nat**(모든 명령) • **show network-modules** • **show portstats** • **show power-supply-status** • **show routing-table** • **show stacking** 및 **configure stacking** • **show virtual-routers** • **show virtual-switches** • **show vpn** (모든 명령) • **configure network management-interface** (관리 및 이벤트 채널을 활성화 및 비활성화하는 모든 명령) • **system renew-http-cert** CLI에서 ?(물음표) 명령을 사용하면 이러한 사용하지 않는 명령에 대한 도움말이 표시되지만, 이 가이드나 온라인 도움말에서는 설명하지 않습니다. 이러한 명령에 대한 자세한 내용은 디바이스 버전에 해당하는 Firepower Management Center 구성 가이드의 CLI 부록을 참조하십시오.

기능	버전	세부 사항
HTTPS 인증서	6.3	시스템과 함께 제공되는 기본 HTTPS 서버 인증서는 이제 3년 후에 자동으로 만료됩니다. 어플라이언스가 버전 6.3으로 업그레이드하기 전에 생성된 기본 인증서를 사용하는 경우 해당 인증서는 처음 생성된 시점에서 20년 후에 만료됩니다. 기본 HTTPS 서버 인증서를 사용하는 경우 시스템은 이제 이 인증서를 갱신할 수 있는 기능을 제공합니다. 새로운 기존 CLI 명령: **show http-cert-expire date**, **system renew-http-cert** 지원되는 플랫폼: 물리적 FMC, 7000 및 8000 Series 디바이스
클래식 CLI 명령 `system lockdown-sensor` 구문.	6.3	이제 클래식 CLI의 **system lockown-sensor** 명령이 **system lockdown**(으)로 변경되었습니다.

C 부록

Firepower Management Center 명령줄 참조

이 참조에서는 Firepower Management Center의 명령줄 인터페이스(CLI)에 대해 설명합니다.

참고 클래식 디바이스(7000 및 8000 Series, ASA FirePOWER, NGIPSv)의 경우에는 명령줄 참조, 3113 페이지의 내용을 참조하십시오.

참고 Firepower Threat Defense의 경우에는 Cisco Firepower Threat Defense 명령 참조의 내용을 참조하십시오.

- Firepower Management Center CLI 정보, 3175 페이지
- Firepower Management Center CLI 관리 명령, 3176 페이지
- Firepower Management Center CLI show 명령, 3177 페이지
- Firepower Management Center CLI 구성 명령, 3178 페이지
- Firepower Management Center CLI 시스템 명령, 3179 페이지
- Firepower Management Center CLI의 기록, 3181 페이지

Firepower Management Center CLI 정보

SSH를 이용해 Firepower Management Center에 로그인하면, CLI에 액세스하게 됩니다. 권장하지는 않지만, `expert` 명령을 사용하여 Linux 셸에 액세스할 수도 있습니다.

주의 Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸에 액세스하지 않는 것이 좋습니다.

⚠

주의 Linux 셸 액세스 권한이 있는 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- 외부 인증을 설정하는 경우 Linux 셸 액세스 권한이 있는 사용자 목록을 적절하게 제한해야 합니다.
- 사전 정의된 관리자 사용자 외에 Linux 셸 사용자를 설정하지 마십시오.

이 부록에 설명된 명령을 사용하여 Firepower Management Center을(를) 보고 문제를 해결할 수 있을 뿐 아니라 제한된 구성 작업도 수행할 수 있습니다.

Firepower Management Center CLI 모드

CLI는 4가지 모드를 포함합니다. 기본 모드인 CLI Management에는 CLI 자체 내에서 탐색하기 위한 명령이 포함됩니다. 나머지 모드에는 Firepower Management Center 기능의 세 가지 영역을 처리하는 명령이 포함됩니다. 이러한 모드 내의 명령은 모드 이름(`system`, `show` 또는 `configure`)으로 시작합니다.

모드에 진입하면 CLI 프롬프트는 현재 모드를 반영하도록 변경됩니다. 예를 들어 시스템 구성 요소에 대한 버전 정보를 표시하려면 표준 CLI 프롬프트에서 전체 명령을 입력할 수 있습니다.

```
> show version
```

`show` 모드에 진입한 경우, show 모드 CLI 프롬프트에서 `show` 키워드 없이 명령을 입력할 수 있습니다.

```
show> version
```

Firepower Management Center CLI 관리 명령

CLI 관리 명령은 CLI와 상호 작용하는 기능을 제공하며, 디바이스의 작동에는 영향을 미치지 않습니다.

exit

CLI 컨텍스트를 다음으로 가장 높은 CLI 컨텍스트 레벨로 이동합니다. 기본 모드에서 이 명령을 실행하면 현재 CLI 세션에서 사용자가 로그아웃됩니다.

Syntax

```
exit
```

예

```
system> exit
>
```

expert

Linux 셸을 호출합니다.

Syntax

```
expert
```

예

```
> expert
```

? (물음표)

CLI 명령 및 매개 변수에 대한 상황별 도움말을 표시합니다. 물음표(?) 명령은 다음과 같이 사용하십시오.

- 현재 CLI 컨텍스트 내에서 사용 가능한 명령의 도움말을 표시하려면 명령 프롬프트에서 물음표(?)를 입력합니다.
- 특별한 문자 집합으로 시작되는 사용 가능한 명령 목록을 표시하려면 약식 명령 바로 뒤에 물음표(?)를 입력합니다.
- 명령의 공식적인 인수에 대한 도움말을 표시하려면 명령 프롬프트에서 인수 자리에 물음표(?)를 입력합니다.

물음표(?)는 콘솔로 다시 에코되지 않습니다.

Syntax

```
?
abbreviated_command ?
command [arguments] ?
```

예

```
> ?
```

Firepower Management Center CLI show 명령

show 명령은 어플라이언스의 상태에 대한 정보를 제공합니다. 이러한 명령은 어플라이언스의 작동 모드를 변경하지 않으며, 명령 실행 시 시스템 작동에 미치는 영향이 최소 수준입니다.

버전

제품 버전 및 빌드를 표시합니다.

Syntax

```
show version
```

예

```
> show version
```

Firepower Management Center CLI 구성 명령

configuration 명령을 통해 사용자는 시스템을 구성 및 관리할 수 있습니다. 이러한 명령은 시스템 작동에 영향을 줍니다.

password

현재 CLI 사용자가 자신의 비밀번호를 변경하도록 허용합니다.

⚠

주의 시스템 보안상의 이유로 모든 어플라이언스에서 사전 정의된 관리자 외에 셸 사용자를 설정하지 않는 것이 좋습니다.

이 명령을 실행하면 현재(또는 이전) 비밀번호를 입력하라는 CLI 프롬프트가 표시된 다음 새 비밀번호를 두 번 입력하라는 프롬프트가 표시됩니다.

Syntax

```
configure password
```

예

```
> configure password
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Firepower Management Center CLI 시스템 명령

system 명령을 사용하면 시스템 전반의 파일 및 액세스 제어 설정을 관리할 수 있습니다.

generate-troubleshoot

Cisco에서 분석할 문제 해결 데이터를 생성합니다.

Syntax

```
system generate-troubleshoot option1 optionN
```

여기서 옵션은 다음 중 하나 이상이며 공백으로 구분됩니다.

- `All`: 다음 옵션을 모두 실행.
- `SNT`: Snort 성능 및 구성
- `PER`: 하드웨어 성능 및 로그
- `SYS`: 시스템 구성, 정책, 로그
- `DES`: 탐지 구성, 정책, 로그
- `NET`: 인터페이스 및 네트워크 관련 데이터
- `VDB`: 검색, 인식, VDB 데이터, 로그
- `UPG`: 업그레이드 데이터 및 로그
- `DBO`: 모든 데이터베이스 데이터
- `LOG`: 모든 로그 데이터
- `NMP`: 네트워크 맵 정보

예

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

`expert` 명령과 디바이스의 Linux 셸에 대한 액세스를 제거합니다.

주의 이 명령은 고객 지원의 핫픽스 없이는 취소할 수 없습니다. 주의해서 사용해야 합니다.

Syntax

```
system lockdown
```

예

```
> system lockdown
```

reboot

어플라이언스를 재부팅합니다.

Syntax

```
system reboot
```

예

```
> system reboot
```

restart

어플라이언스 애플리케이션을 다시 시작합니다.

Syntax

```
system restart
```

예

```
> system restart
```

shutdown

어플라이언스를 종료합니다.

Syntax

```
system shutdown
```

예

```
> system shutdown
```

Firepower Management Center CLI의 기록

기능	버전	세부 사항
다음에 대한 자동 CLI 액세스 FMC	6.5	SSH를 이용해 FMC에 로그인하면, CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI `expert` 명령을 사용하면 Linux 셸에 액세스할 수 있습니다. 참고 이 기능을 이용하면 버전 6.3 기능인 FMC에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 FMC에서는 **System(**시스템**)** > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)** 페이지가 표시되지 않습니다. 물리적 FMC에서는 계속 표시됩니다.
CLI 액세스를 활성화 및 비활성화 하는 기능 FMC	6.3	신규/수정된 화면: FMC 웹 인터페이스 관리자가 사용할 수 있는 새 체크박스: **Enable CLI Access(CLI** 액세스 활성화**)(System(**시스템**)** > **Configuration(**구성**)**에 위치) > (**Console Configuration(**콘솔 구성**))** 페이지 • 선택: SSH를 사용하여 FMC에 로그인하면 CLI에 액세스할 수 있습니다. • 선택 취소: SSH를 사용하여 FMC에 로그인하면 Linux 셸에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다. 지원되는 플랫폼: FMC

Firepower Management Center 명령줄 참조

기능	버전	세부 사항
FMC CLI	6.3	도입된 기능. 처음에는 다음 명령을 지원합니다. • `exit` • `expert` • `?` • `show version` • `configure password` • `system generate-troubleshoot` • `system lockdown` • `system reboot` • `system restart` • `system shutdown` 지원되는 플랫폼: FMC