



ASA 디바이스 구성

이 장에는 다음 섹션이 포함되어 있습니다.

- ASA 연결 자격 증명 업데이트, 2 페이지
- ASA 인터페이스 구성, 3 페이지
- ASA 시스템 설정 정책, 15 페이지
- 개체, on page 26
- ASA 라우팅, 62 페이지
- 보안 정책 관리, 65 페이지
- 레거시 ASA 액세스 정책 관리, 65 페이지
- ASA 정책(확장 액세스 목록), on page 76
- ASA 글로벌 액세스 정책 구성, 78 페이지
- 적중률, on page 79
- 네트워크 정책 규칙 내보내기, on page 80
- 디바이스에 ASA 정책 변경 사항 적용, 80 페이지
- ASA 정책의 보안 그룹 태그, 81 페이지
- 새도우 규칙, 81 페이지
- 네트워크 주소 변환, 83 페이지
- NAT 규칙 처리 순서, on page 84
- 네트워크 주소 변환 마법사, on page 86
- NAT의 일반적인 사용 사례, 87 페이지
- CDO에서 가상 프라이빗 네트워크 관리, 98 페이지
- ASA 템플릿, on page 172
- API 토큰, 175 페이지
- FDM-관리 디바이스 템플릿으로 ASA 구성 마이그레이션, on page 175
- ASA 인증서 관리, 176 페이지
- ASA 파일 관리, on page 184
- ASA 고가용성 관리, 188 페이지
- ASA에서 DNS 구성, on page 189
- CDO 명령줄 인터페이스, on page 190
- 대량 명령줄 인터페이스, on page 192

- 명령줄 인터페이스 매크로, on page 196
- CDO CLI를 사용하여 ASA 구성, 200 페이지
- CDO를 사용하여 ASA 구성 비교, on page 200
- ASA 대량 CLI 사용 사례, on page 201
- ASA 명령줄 인터페이스 설명서, on page 202
- CDO CLI 명령 결과 내보내기, on page 203
- ASA 구성 복원, on page 206
- ASA 및 Cisco IOS 디바이스 구성 파일 관리, on page 208
- 변경 사항 읽기, 삭제, 확인 및 구축, 209 페이지
- 모든 디바이스 구성 읽기, on page 210
- ASA에서 CDO로 구성 변경 사항 읽기, 212 페이지
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 212 페이지
- CDO에서 ASA로 구성 변경 사항 구축, 213 페이지
- 디바이스 구성 대량 구축, on page 217
- 예약된 자동 배포, on page 218
- 구성 변경 사항 확인, on page 220
- 변경 사항 취소, on page 221
- 디바이스의 대역 외 변경 사항, on page 222
- Defense Orchestrator와 디바이스 간 구성 동기화, 222 페이지
- 충돌 탐지, on page 223
- 디바이스에서 대역 외 변경 사항 자동 수락, on page 224
- 구성 충돌 해결, on page 225
- 디바이스 변경 사항에 대한 폴링 예약, on page 227

ASA 연결 자격 증명 업데이트

ASA를 온보딩하는 과정에서 CDO가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호를 입력했습니다. 디바이스에서 해당 자격 증명이 변경된 경우 **Update Credentials**(자격 증명 업데이트) 디바이스 작업을 사용하여 CDO에서도 해당 자격 증명을 업데이트하십시오. 이 기능을 사용하면 디바이스를 다시 등록하지 않고도 CDO에서 자격 증명을 업데이트할 수 있습니다. 전환할 사용자 이름과 암호 조합은 해당 사용자의 ASA 또는 AAA(Authentication, Authorization, and Accounting) 서버에 이미 존재해야 합니다. 이 프로세스는 Cisco Defense Orchestrator 데이터베이스에만 영향을 미칩니다. 자격 증명 업데이트 기능을 사용할 때 ASA 구성이 변경되지 않습니다.

단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(장치) 탭을 클릭한 다음 **ASA**를 클릭합니다.

단계 3 업데이트할 연결 자격 증명에 있는 ASA를 선택합니다. 한 번에 하나 이상의 ASA에서 자격 증명을 업데이트할 수 있습니다.

단계 4 **Device Actions**(장치 작업) 창에서 **Update Credentials**(자격 증명 업데이트)를 클릭합니다.

단계 5 ASA를 CDO에 연결하는 데 사용하는 Cloud Connector 또는 SDC(보안 디바이스 커넥터)를 선택합니다.

단계 6 ASA에 연결하는 데 사용할 새 사용자 이름 및 비밀번호를 입력합니다.

단계 7 자격 증명이 변경된 후 CDO는 디바이스를 동기화합니다.

참고 CDO가 디바이스를 동기화하지 못하면 CDO의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 경우 유효하지 않은 사용자 이름과 비밀번호 조합을 사용하려고 시도했을 수 있습니다. 사용하려는 자격 증명이 ASA 또는 AAA 서버에 저장되어 있는지 확인하고 다시 시도하십시오.

SDC 간에 ASA 이동

CDO는 **테넌트당 둘 이상의 SDC 사용을 지원**합니다. 다음 절차를 사용하여 한 SDC에서 다른 SDC로 관리형 ASA를 이동할 수 있습니다.

단계 1 CDO 메뉴 모음에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 다른 SDC로 이동하려는 ASA를 선택합니다.

단계 3 Device Actions(디바이스 작업) 창에서 **Update Credentials(자격 증명 업데이트)**를 클릭합니다.

단계 4 보안 디바이스 커넥터 버튼을 클릭하고 디바이스를 이동하려는 SDC를 선택합니다.

단계 5 ASA를 온보딩하는 데 사용한 관리자 사용자 이름 및 비밀번호를 입력하고 Update(업데이트)를 클릭합니다. 이러한 변경 사항을 디바이스에 구축할 필요는 없습니다.

ASA 인터페이스 구성

CDO(Cisco Defense Orchestrator)는 명령줄 인터페이스를 사용할 필요가 없는 사용자 친화적 인터페이스를 제공하여 ASA 인터페이스 구성을 간소화합니다. 사용자는 ASA의 물리적 인터페이스, 하위 인터페이스 및 EtherChannel의 구성을 완벽하게 제어할 수 있습니다. 또한 경로 기반 사이트 간 VPN 중에 생성된 Virtual Tunnel Interface도 볼 수 있지만 읽기 전용입니다. CDO를 사용하여 ASA 디바이스에서 데이터 인터페이스 또는 관리/진단 인터페이스를 구성하고 편집할 수 있습니다.

물리적 또는 가상 인터페이스 연결에 케이블을 연결하려면 인터페이스를 구성해야 합니다. 최소한 인터페이스 이름을 지정하고 트래픽을 전달하도록 인터페이스를 활성화해야 합니다. 인터페이스가 브리지 그룹의 멤버인 경우에는 인터페이스의 이름을 지정하는 작업만 수행하면 됩니다. 인터페이스가 BVI(브리지 가상 인터페이스)인 경우 BVI에 IP 주소를 할당해야 합니다. 지정된 포트의 단일 실제 인터페이스가 아닌 VLAN 하위 인터페이스를 생성하려는 경우에는 일반적으로 실제 인터페이스가 아닌 하위 인터페이스에 IP 주소를 구성합니다. VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다.

인터페이스 목록에는 사용 가능한 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다. 인터페이스 행을 선택하고 Actions(작업) 창에서 **Edit(편집)**를 클릭하여 인터페이스의 상태를 on 또는 off로 변경하거나 인터페이스를 편집할 수 있습니다. 목록에는 컨피그레이션을 기준으로 인터페이스 특성이 표시됩니다. 인터페이스 행을 확장하여 하위 인터페이스 또는 브리지 그룹 멤버를 확인합니다.

관리 인터페이스

다음에 연결하여 ASA를 관리할 수 있습니다.

- 통과 트래픽 인터페이스
- 전용 관리 슬롯/포트 인터페이스(모델에 제공되는 경우)

MTU 설정 사용

MTU는 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.

Virtual Tunnel Interface(VTI)에 대한 읽기 전용 지원

두 ASA 디바이스 간에 경로 기반 사이트 간 VPN 터널을 구성하면 디바이스 간에 VTI(Virtual Tunnel Interface)가 생성됩니다. VTI 터널이 구성된 디바이스는 CDO에 온보딩할 수 있습니다. CDO에서 검색하고 ASA 인터페이스 페이지에 나열하지만 관리를 지원하지 않습니다.

ASA 물리적 인터페이스 구성

단계 1 CDO 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 수정하려는 디바이스를 선택하고 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.

단계 4 구성할 물리적 인터페이스를 클릭하고 **Edit**(편집)을 클릭합니다.

Editing Physical Interface(물리적 인터페이스 편집) 대화 상자가 나타납니다.

단계 5 **Logical Name**(논리적 이름) 필드에 인터페이스 이름을 입력합니다.

단계 6 다음 절차 중 하나를 계속합니다.

- 이 인터페이스에 IPv4 주소를 할당하려면 [ASA 물리적 인터페이스에 대한 IPv4 주소 지정 구성](#)합니다.
- 이 인터페이스에 IPv6 주소를 할당해야 하는 경우 [ASA 물리적 인터페이스에 대한 IPv6 주소 지정 구성](#), 5 페이지.
- **고급 ASA 물리적 인터페이스 옵션 구성** 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 인터페이스를 저장한 경우 고급 인터페이스 옵션을 계속 진행하지 않으려면 [ASA 물리적 인터페이스 활성화](#)를 계속 진행합니다.

ASA 물리적 인터페이스에 대한 IPv4 주소 지정 구성

단계 1 **Edit Physical Interface**(물리적 인터페이스 편집) 대화 상자의 **IPv4 Address(IPv4 주소)** 탭에서 다음을 구성합니다.

- 유형: 인터페이스에 대해 고정 IP 주소 지정 또는 DHCP를 사용할 수 있습니다.

Static(고정) - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다.

- **IP Address and Subnet Mask(IP 주소 및 서브넷 마스크)**: 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다.
- **Standby IP Address(스탠바이 IP 주소)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다.

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.

DHCP: 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다.

Obtain Default Route(기본 경로 얻기) 확인란을 선택하여 DHCP 서버에서 기본 경로를 가져올 수 있습니다. 일반적으로 이 옵션을 선택합니다.

단계 2 완료한 경우 **Save(저장)**를 클릭하거나 다음 절차 중 하나를 계속합니다.

- 이 인터페이스에 IPv6 주소를 할당해야 하는 경우 [ASA 물리적 인터페이스에 대한 IPv6 주소 지정 구성, 5 페이지](#).
- [고급 ASA 물리적 인터페이스 옵션 구성](#) 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 인터페이스를 저장한 경우 고급 인터페이스 옵션을 계속 진행하지 않으려면 [ASA 물리적 인터페이스 활성화](#)를 계속 진행합니다.

ASA 물리적 인터페이스에 대한 IPv6 주소 지정 구성

단계 1 **Editing Physical Interface**(물리적 인터페이스 편집) 대화 상자에서 **IPv6 Address(IPv6 주소)** 탭을 클릭합니다.

단계 2 다음을 구성합니다.

- **State(상태)**: IPv6 처리를 활성화하고 전역 주소를 구성하지 않을 때 링크 로컬 주소를 자동으로 구성하려면 **State(상태)** 슬라이더를 클릭하여 사용하도록 설정합니다. 링크-로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 구성용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration**(주소 자동 구성):

주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성된 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Suppress RA**(**RA** 표시 안 함): 라우터 알림을 표시하지 않으려면 이 상자를 선택합니다. 디바이스는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

- **DAD Attempts**(**DAD** 시도): 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 구성 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.

- **Link-Local Address**(링크-로컬 주소): 주소를 링크 로컬로만 사용하려면 Link-Local Address(링크-로컬 주소) 필드에 주소를 입력합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). 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.

- **Standby Link-Local Address**(스탠바이 링크-로컬 주소): 인터페이스가 고가용성 디바이스 쌍을 연결하는 경우 이 주소를 구성합니다. 이 인터페이스가 연결된 다른 디바이스에 있는 인터페이스의 링크-로컬 주소를 입력합니다.

- **Static Address/Prefix**(고정 주소/접두사): 스테이트리스 자동 구성을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. 다른 고정 주소를 추가할 수 있습니다.

- **Standby IP Address**(스탠바이 IP 주소): 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이

주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

단계 3 완료한 경우 **Save(저장)**를 클릭하거나 다음 절차 중 하나를 계속합니다.

- **고급 ASA 물리적 인터페이스 옵션 구성** 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 인터페이스를 저장한 경우 고급 인터페이스 옵션을 계속 진행하지 않으려면 **ASA 물리적 인터페이스 활성화**를 계속 진행합니다.

고급 ASA 물리적 인터페이스 옵션 구성

고급 인터페이스 옵션에는 대부분의 네트워크에 적합한 기본 설정이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 설정을 구성하십시오.

다음 절차에서는 인터페이스가 이미 정의되어 있다고 가정합니다. 인터페이스를 처음 수정하거나 생성할 때 이러한 설정을 수정할 수도 있습니다.

이 절차 및 모든 단계는 선택 사항입니다.

단계 1 **Editing Physical Interface(물리적 인터페이스 편집)** 대화 상자에서 **Advanced(고급)** 탭을 클릭합니다.

단계 2 다음 고급 설정을 구성합니다.

- **HA Monitoring(HA 모니터링)**: 디바이스가 HA 쌍이 고가용성 구성에서 피어 디바이스로 페일오버할지 여부를 결정할 때 인터페이스의 상태를 요소로 포함하려면 활성화합니다. 이 옵션은 고가용성을 구성하지 않는 경우 무시되며 인터페이스의 이름을 구성하지 않는 경우에도 무시됩니다.
- **Management Only(관리만)**: 데이터 인터페이스 관리만 수행하려면 활성화합니다.
관리 전용 인터페이스에서는 통과 트래픽을 허용하지 않으므로 데이터 인터페이스를 관리 전용 인터페이스로 설정할 때 사용할 수 있는 값은 거의 없습니다. 관리/진단 인터페이스(항상 관리 전용)의 경우에는 이 설정을 변경할 수 없습니다.
- **MTU**: 기본 MTU는 1500바이트입니다. 64~9198 사이의 값을 지정할 수 있습니다. 네트워크에서 대개 점보 프레임이 표시되면 높은 값을 설정합니다.
- **Duplex and Speed (Mbps)(듀플렉스 및 속도(Mbps))**: 기본적으로 인터페이스는 연결 반대쪽의 인터페이스와 최적의 이중 및 속도를 협상하지만, 필요한 경우 특정 이중이나 속도를 강제 적용할 수 있습니다. 나열된 옵션은 인터페이스에서 지원하는 유일한 옵션입니다. 네트워크 모듈의 인터페이스에 이러한 옵션을 설정하기 전에 인터페이스 구성에 대한 제한 사항을 읽어보십시오.
 - **Duplex(듀플렉스)**: Auto(자동), Half(하프) 또는 Full(풀)을 선택합니다. 인터페이스가 지원하는 경우가 이 기본값입니다.
 - **Speed(속도)**: Auto(자동)를 선택하여 인터페이스가 속도를 협상하도록 하거나(이 옵션이 기본값임), 10, 100, 1000, 10000Mbps 중에서 특정 속도를 선택합니다. 다음과 같은 특수 옵션을 선택할 수도 있습니다.

- **DAD Attempts(DAD 시도)**: 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 구성 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.
- **MAC Address(MAC 주소)**: H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 00C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).
- **Standby MAC Address(스탠바이 MAC 주소)**: 고가용성에 사용할 주소입니다. 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 3 인터페이스를 저장한 경우 고급 인터페이스 옵션을 계속 진행하지 않으려면 **ASA 물리적 인터페이스 활성화**를 계속 진행합니다.

단계 4 **Save(저장)**를 클릭합니다.

ASA 물리적 인터페이스 활성화

단계 1 활성화할 물리적 인터페이스를 선택합니다.

단계 2 인터페이스의 논리적 이름과 연결된 창의 오른쪽 상단에 있는 **State(상태)** 슬라이더를 이동합니다.

단계 3 변경한 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**합니다.

ASA VLAN 하위 인터페이스 추가

VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 실제 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 실제 인터페이스 또는 디바이스를 더 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

스위치의 트렁크 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성합니다. 스위치 트렁크 포트에 표시될 수 있는 각 VLAN에 대해 하위 인터페이스를 생성합니다. 스위치의 액세스 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성할 필요가 없습니다.

- [ASA VLAN 하위 인터페이스 구성](#)
ASA 하위 인터페이스에 대한 IPv4 주소 지정 구성, 9 페이지
- [ASA 하위 인터페이스에 대한 IPv6 주소 지정 구성, 10 페이지](#)
- [고급 ASA VLAN 하위 인터페이스 옵션 구성, 12 페이지](#)

- 하위 인터페이스 활성화, 13 페이지


ASA VLAN 하위 인터페이스 구성

단계 1 CDO 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 수정하려는 디바이스를 선택하고 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.

단계 4 다음 방법 중 하나를 사용하여 하위 인터페이스를 추가할 수 있습니다.

-  -> **Subinterface**(하위 인터페이스)를 선택합니다.
- 구성할 물리적 인터페이스를 선택하고 오른쪽의 **Actions**(작업) 창에서 **New Subinterface**(새로운 하위 인터페이스)를 클릭합니다.

단계 5 **VLAN ID** 필드에 1~4094 범위의 VLAN ID를 입력합니다.

일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로 스위치 설명서에서 자세한 내용을 확인하십시오. 다중 상황 모드의 경우 시스템 컨피그레이션에서 VLAN만 설정할 수 있습니다.

단계 6 **Subinterface ID**(하위 인터페이스 ID) 필드에 하위 인터페이스 ID를 1~4294967293 범위의 정수로 입력합니다.

허용되는 하위 인터페이스의 개수는 플랫폼에 따라 다릅니다. 다음을 설정한 후에는 ID를 변경할 수 없습니다.

단계 7 다음 절차 중 하나를 계속합니다.

- 이 인터페이스에 IPv4 주소를 할당하려면 **ASA 하위 인터페이스에 대한 IPv4 주소 지정 구성**합니다.
- 이 인터페이스에 IPv6 주소를 할당하려면 **ASA 하위 인터페이스에 대한 IPv6 주소 지정 구성**합니다.
- **고급 ASA VLAN 하위 인터페이스 옵션 구성**. 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 하위 인터페이스를 저장한 경우 고급 하위 인터페이스 옵션을 계속 진행하지 않으려면 **하위 인터페이스 활성화**를 계속 진행합니다.

ASA 하위 인터페이스에 대한 IPv4 주소 지정 구성

단계 1 **Create Subinterface**(하위 인터페이스 생성) 대화 상자의 **IPv4 Address(IPv4 주소)** 탭에서 다음을 구성합니다.

- 유형: 인터페이스에 대해 고정 IP 주소 지정 또는 DHCP를 사용할 수 있습니다.

Static(고정) - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다.

- **IP Address and Subnet Mask(IP 주소 및 서브넷 마스크)**: 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다.

- **Standby IP Address(스탠바이 IP 주소)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다.

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.

DHCP: 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다.

Obtain Default Route(기본 경로 얻기) 확인란을 선택하여 DHCP 서버에서 기본 경로를 가져올 수 있습니다. 일반적으로 이 옵션을 선택합니다.

단계 2 완료한 경우 **Save(저장)**를 클릭하거나 다음 절차 중 하나를 계속합니다.

- 이 인터페이스에 IPv6 주소를 할당하려면 [ASA 하위 인터페이스에 대한 IPv6 주소 지정 구성](#)합니다.
- **고급 ASA VLAN 하위 인터페이스 옵션 구성.** 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 하위 인터페이스를 저장한 경우 고급 하위 인터페이스 옵션을 계속 진행하지 않으려면 [ASA 물리적 인터페이스 활성화](#)를 계속 진행합니다.

ASA 하위 인터페이스에 대한 IPv6 주소 지정 구성

단계 1 **Creating Subinterface(하위 인터페이스 생성)** 대화 상자에서 **IPv6 Address(IPv6 주소)** 탭을 클릭합니다.

단계 2 다음을 구성합니다.

- **State(상태):** IPv6 처리를 활성화하고 전역 주소를 구성하지 않을 때 링크 로컬 주소를 자동으로 구성하려면 **State(상태)** 슬라이더를 클릭하여 사용하도록 설정합니다. 링크-로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 구성용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(주소 자동 구성):**

주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성된 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Suppress RA(RA 표시 안 함):** 라우터 알림을 표시하지 않으려면 이 상자를 선택합니다. 디바이스는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

- **DAD 시도 - 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다.** 기본값은 1입니다. 스테이트리스 자동 구성 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.
- **Link-Local Address(링크-로컬 주소):** 주소를 링크 로컬로만 사용하려면 Link-Local Address(링크-로컬 주소) 필드에 주소를 입력합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:fee:6a82). 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.
- **Standby Link-Local Address(스탠바이 링크-로컬 주소):** 인터페이스가 고가용성 디바이스 쌍을 연결하는 경우 이 주소를 구성합니다. 이 인터페이스가 연결된 다른 디바이스에 있는 인터페이스의 링크-로컬 주소를 입력합니다.
- **Static Address/Prefix(고정 주소/접두사):** 스테이트리스 자동 구성을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. 다른 고정 주소를 추가할 수 있습니다.
- **Standby IP Address(스탠바이 IP 주소):** 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

단계 3 완료한 경우 **Save(저장)**를 클릭하거나 다음 절차 중 하나를 계속합니다.

- **고급 ASA VLAN 하위 인터페이스 옵션 구성.** 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 하위 인터페이스를 저장한 경우 고급 하위 인터페이스 옵션을 계속 진행하지 않으려면 **하위 인터페이스 활성화**를 계속 진행합니다.

고급 ASA VLAN 하위 인터페이스 옵션 구성

고급 인터페이스 옵션에는 대부분의 네트워크에 적합한 기본 설정이 있습니다. 네트워킹 문제를 해결하는 경우에만 이러한 설정을 구성하십시오.

다음 절차에서는 인터페이스가 이미 정의되어 있다고 가정합니다. 인터페이스를 처음 수정하거나 생성할 때 이러한 설정을 수정할 수도 있습니다.

이 절차 및 모든 단계는 선택 사항입니다.

단계 1 Creating Subinterface(하위 인터페이스 생성) 대화 상자에서 **Advanced**(고급) 탭을 클릭합니다.

단계 2 다음 고급 설정을 구성합니다.

- **HA Monitoring**(HA 모니터링): 디바이스가 HA 쌍이 고가용성 구성에서 피어 디바이스로 페일오버할지 여부를 결정할 때 인터페이스의 상태를 요소로 포함하려면 활성화합니다. 이 옵션은 고가용성을 구성하지 않는 경우 무시되며 인터페이스의 이름을 구성하지 않는 경우에도 무시됩니다.
- **Management Only**(관리만): 데이터 인터페이스 관리만 수행하려면 활성화합니다.
관리 전용 인터페이스에서는 통과 트래픽을 허용하지 않으므로 데이터 인터페이스를 관리 전용 인터페이스로 설정할 때 사용할 수 있는 값은 거의 없습니다. 관리/진단 인터페이스(항상 관리 전용)의 경우에는 이 설정을 변경할 수 없습니다.
- **MTU**: 기본 MTU는 1500바이트입니다. 64~9198 사이의 값을 지정할 수 있습니다. 네트워크에서 대개 점보 프레임이 표시되면 높은 값을 설정합니다.
- **DAD Attempts**(DAD 시도): 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 구성 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.
- **MAC Address**(MAC 주소): H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 00C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).
- **Standby MAC Address**(스탠바이 MAC 주소): 고가용성에 사용할 주소입니다. 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 3 인터페이스를 저장한 경우 고급 인터페이스 옵션을 계속 진행하지 않으려면 **하위 인터페이스 활성화**를 계속 진행합니다.

단계 4 Save(저장)를 클릭합니다.

하위 인터페이스 활성화

단계 1 활성화할 하위 인터페이스를 선택합니다.

단계 2 인터페이스의 논리적 이름과 연결된 창의 오른쪽 상단에 있는 **State(상태)** 슬라이더를 이동합니다.

단계 3 변경한 사항을 검토하고 구축합니다.

ASA 하위 인터페이스 제거

ASA에서 하위 인터페이스를 제거하려면 다음 절차를 수행합니다.

단계 1 CDO 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 수정하려는 디바이스를 선택하고 오른쪽의 **Management(관리)** 창에서 **Interfaces(인터페이스)**를 클릭합니다.

단계 4 **Interfaces(인터페이스)** 페이지에서 삭제할 하위 인터페이스와 연결된 물리적 인터페이스를 확장한 다음 해당 하위 인터페이스를 선택합니다.

단계 5 오른쪽의 **Actions(작업)** 창에서 **Remove(제거)**를 클릭합니다.

단계 6 EtherChannel 인터페이스 삭제를 확인하고 **Delete(삭제)**를 클릭합니다.

단계 7 변경한 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**합니다.

ASA EtherChannel 인터페이스 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.

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.

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 컨피그레이션이 확인되지 않습니다.

ASA EtherChannel 인터페이스에 대한 자세한 내용은 [ASDM 설명서 1: Cisco ASA 시리즈 일반 작업 ASDM 구성 가이드, X, Y의 EtherChannel](#) 및 이중 인터페이스 장을 참조하십시오.

ASA EtherChannel 구성

ASA에 새 EtherChannel 인터페이스를 추가하려면 이 절차를 사용합니다.

시작하기 전에

ASA 인터페이스에서 EtherChannel을 구성하려면 다음 사전 요건을 충족해야 합니다.

- 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. 속도가 Detect SFP(SFP 탐지)로 설정되어 있는 한 다른 인터페이스 용량을 지원하는 Secure Firewall 3100의 경우를 제외하고, 대용량 인터페이스에서는 속도를 더 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합할 수 없습니다. 이 경우 최저 공통 속도가 사용됩니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 채널 그룹에 추가할 수 없습니다. 먼저 이름을 제거해야 합니다.
- 다른 EtherChannel 인터페이스 그룹, Switchport 인터페이스 및 하위 인터페이스가 있는 인터페이스의 일부는 추가할 수 없습니다.

단계 1 CDO 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 수정하려는 디바이스를 선택하고 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.

단계 4  > **EtherChannel Interface**(EtherChannel 인터페이스)를 선택합니다.

단계 5 **Logical Name**(논리적 이름) 필드에 EtherChannel 인터페이스의 이름을 제공합니다.

단계 6 **EtherChannel ID**에 1~8 사이의 정수를 입력합니다.

단계 7 **Link Aggregation Control Protocol**(링크 어그리게이션 제어 프로토콜)의 드롭다운 버튼을 클릭하고 두 가지 옵션 중 하나를 선택합니다.

- **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**(켜짐)인 EtherChannel은 **On**(켜짐)으로 구성된 다른 EtherChannel과만 연결할 수 있습니다.

단계 8 EtherChannel에 멤버로 포함할 인터페이스를 검색하여 선택합니다. 하나 이상의 인터페이스를 포함해야 합니다.

경고! EtherChannel 인터페이스를 멤버로 추가하고 이미 IP 주소가 구성된 경우 CDO는 멤버의 IP 주소를 제거합니다.

단계 9 **IPv4, IPv6, Advanced**(고급) 탭 중에서 선택하여 하위 인터페이스의 IP 주소를 구성합니다.

- 이 인터페이스에 IPv4 주소를 할당하려면 [ASA 물리적 인터페이스에 대한 IPv4 주소 지정 구성](#)합니다.
- 이 인터페이스에 IPv6 주소를 할당하려면 [ASA 물리적 인터페이스에 대한 IPv6 주소 지정 구성](#)합니다.

- **고급 ASA 물리적 인터페이스 옵션 구성** 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 10 창의 오른쪽 상단에 있는 **State(상태)** 슬라이더를 이동하여 EtherChannel 인터페이스를 활성화합니다.

단계 11 **Save(저장)**를 클릭합니다.

단계 12 변경한 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**합니다.

ASA EtherChannel 편집

ASA에서 기존 EtherChannel을 편집하려면 이 절차를 수행합니다.

단계 1 CDO 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 수정하려는 디바이스를 선택하고 오른쪽의 **Management(관리)** 창에서 **Interfaces(인터페이스)**를 클릭합니다.

단계 4 **Interfaces(인터페이스)** 페이지에서 편집할 EtherChannel 인터페이스를 선택합니다.

단계 5 오른쪽의 **Actions(작업)** 창에서 **Edit(편집)**를 클릭합니다.

단계 6 원하는 값을 수정하고 **Save(저장)**를 클릭합니다.

단계 7 변경한 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**합니다.

ASA EtherChannel 인터페이스 제거

ASA에서 EtherChannel 인터페이스를 제거하려면 다음 절차를 수행합니다.

단계 1 CDO 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 수정하려는 디바이스를 선택하고 오른쪽의 **Management(관리)** 창에서 **Interfaces(인터페이스)**를 클릭합니다.

단계 4 **Interfaces(인터페이스)** 페이지에서 삭제할 EtherChannel 인터페이스를 선택합니다.

단계 5 오른쪽의 **Actions(작업)** 창에서 **Remove(제거)**를 클릭합니다.

단계 6 EtherChannel 인터페이스 삭제를 확인하고 **Delete(삭제)**를 클릭합니다.

단계 7 변경한 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**합니다.

ASA 시스템 설정 정책

ASA 시스템 설정 정책 소개

시스템 설정 정책을 사용하여 ASA 디바이스의 작동 및 기능을 관리합니다. 이 정책은 도메인 이름 서비스, 보안 복사 서버 활성화, 메시지 로깅, ACL 확인 없이 VPN 트래픽 허용 등의 필수 구성을 포

합합니다. 정책을 설정하면 디바이스가 보안 네트워크 환경을 유지하도록 올바르게 구성되도록 할 수 있습니다.

ASA 디바이스를 구성할 때는 공유 시스템 설정 정책으로 여러 디바이스의 설정을 관리하는 옵션을 사용할 수도 있고 단일 디바이스의 설정을 개별적으로 수정할 수도 있다는 점을 기억해야 합니다.

공유 시스템 설정 정책

공유 시스템 설정 정책은 네트워크의 여러 ASA 디바이스에 적용됩니다. 이를 사용하면 여러 매니지드 디바이스를 한 번에 구성할 수 있으므로 구축 일관성을 유지하고 관리 작업을 간소화할 수 있습니다. 공유 정책의 매개변수에 적용되는 변경 사항은 해당 정책을 사용하는 다른 ASA 디바이스에 영향을 미칩니다.


Policies(정책) -> **ASA System Settings(ASA 시스템 설정)**를 선택합니다. [새 공유 시스템 설정 정책 생성, 16 페이지](#)의 내용을 참조하십시오.

또한 단일 ASA 디바이스에 해당하는 디바이스별 시스템 설정을 수정하여 공유 시스템 설정 정책을 재정의할 수 있습니다. **Inventory(재고 목록)** > **ASA device(ASA 디바이스)** > **Management(관리)** > **Settings(설정)**를 선택합니다. [디바이스별 시스템 설정 구성 또는 수정, 23 페이지](#)의 내용을 참조하십시오.

새 공유 시스템 설정 정책 생성

이 섹션을 사용하여 ASA 디바이스에 대한 새로운 공유 시스템 설정 정책을 생성합니다.

단계 1 Policies(정책) -> **ASA System Settings(ASA 시스템 설정)**를 선택합니다.

단계 2  버튼을 클릭합니다.

단계 3 Name(이름) 필드에 정책 이름을 입력하고 **Save(저장)**를 클릭합니다.

단계 4 ASA 공유 시스템 설정 편집 페이지에서 원하는 매개변수를 구성합니다.

- 기본 DNS 설정 구성, 17 페이지
- HTTP 설정 구성, 18 페이지
- NTP 서버를 사용하여 날짜 및 시간 설정, 18 페이지
- SSH 액세스 구성, 19 페이지
- 시스템 로깅 구성, 20 페이지
- Sysopt 설정 활성화, 22 페이지

참고

- 해당 매개변수의 주황색 점(●)은 저장되지 않은 변경 사항을 강조 표시합니다.
- 거부된 기호(⊘)는 디바이스의 기존 로컬 값을 사용하는 매개변수를 강조 표시합니다.


기본 DNS 설정 구성

ASA에서 호스트 이름의 IP 주소를 확인할 수 있도록 DNS 서버를 구성해야 합니다. 또한 액세스 규칙에서 FQDN(Fully Qualified Domain Name) 네트워크 개체를 사용하려면 DNS 서버를 구성해야 합니다.

단계 1 ASA 시스템 설정 편집 페이지의 왼쪽 창에서 **DNS**를 클릭합니다.

단계 2 공유 ASA 시스템 설정 정책의 값을 구성하려면 **Retain existing values**(기존 값 유지) 확인란의 선택을 취소합니다.

중요 **Retain existing values**(기존 값 유지) 확인란이 선택되어 있으면 필드가 표시되지 않으므로 값을 구성할 수 없습니다. CDO는 이 설정에 ASA 디바이스의 기존 로컬 값을 사용하며 공유 정책에서 상속되지 않습니다.

단계 3 DNS 섹션에서  을 클릭하여 서버를 구성합니다.

- **IP Version(IP 버전)**: 사용할 IP 주소 버전을 선택합니다.
- **IP Address(IP 주소)**: DNS 서버의 IP 주소를 지정합니다.
- **Interface Name(인터페이스 이름)**: DNS 조회를 활성화할 인터페이스를 지정합니다.

참고 여기에 지정된 인터페이스 이름이 이 공유 시스템 설정 정책과 연결된 ASA 디바이스에서 동일한지 확인하십시오.

단계 4 **Save**(저장)를 클릭합니다.

단계 5 **Domain name**(도메인 이름) 필드에서 ASA의 도메인 이름을 지정합니다.

ASA는 도메인 이름을 정규화되지 않은 이름에 접미사로 추가합니다. 예를 들어, 도메인 이름을 “example.com”으로 설정하고 “jupiter”라는 정규화되지 않은 이름으로 syslog 서버를 지정한 경우 ASA는 해당 이름을 “jupiter.example.com”으로 정규화합니다.

단계 6 **DNS Lookup**(DNS 조회) 섹션에서  을 클릭하고 인터페이스 이름을 지정합니다.

인터페이스에서 DNS 조회를 활성화하지 않으면 ASA에서는 해당 인터페이스의 DNS 서버와 통신하지 않습니다. DNS 서버에 액세스하는 데 사용할 모든 인터페이스에서 DNS 조회를 활성화해야 합니다.

참고 구성된 인터페이스를 제거하려면 **Actions**(작업) 아래에서 삭제 아이콘을 클릭합니다.

단계 7 **Save**(저장)를 클릭합니다.

HTTP 설정 구성

관리 액세스를 위해 ASA 인터페이스에 액세스하려면 HTTP를 사용하여 ASA에 액세스할 수 있는 모든 호스트/네트워크의 주소를 지정해야 합니다. HTTPS에 HTTP 연결을 리디렉션하도록 지정하기 위해 HTTP 리디렉션을 구성하는 경우, HTTP를 허용하도록 액세스 규칙을 활성화해야 합니다. 액세스 규칙을 활성화하지 않으면 인터페이스가 HTTP 포트를 수신 대기할 수 없습니다.

단계 1 ASA 시스템 설정 편집 페이지의 왼쪽 창에서 **HTTP**를 클릭합니다.


단계 2 공유 ASA 시스템 설정 정책의 값을 구성하려면 **Retain existing values**(기존 값 유지) 확인란의 선택을 취소합니다.

중요 **Retain existing values**(기존 값 유지) 확인란이 선택되어 있으면 필드가 표시되지 않으므로 값을 구성할 수 없습니다. CDO는 이 설정에 ASA 디바이스의 기존 로컬 값을 사용하며 공유 정책에서 상속되지 않습니다.

단계 3 HTTP 서버를 활성화하려면 **Enable HTTP Server**(HTTP 서버 활성화) 확인란을 선택합니다.

단계 4 **Port Number**(포트 번호) 필드에서 포트 번호를 설정합니다. port는 인터페이스가 HTTP 연결을 리디렉션하는 포트를 식별합니다.

경고! 디바이스의 HTTP 포트를 변경하면 CDO에 대한 연결에 문제가 발생할 수 있습니다. 디바이스의 네트워크 연결과 관련된 설정을 변경하려는 경우 이 점을 기억하는 것이 중요합니다.

단계 5 HTTP 정보를 추가하려면  을 클릭합니다.

- **Interface**(인터페이스): 여기에 지정된 인터페이스 이름이 이 공유 시스템 설정 정책과 연결된 ASA 디바이스에서 동일한지 확인하십시오.
- **IP Version**(IP 버전): 사용할 IP 주소 버전을 선택합니다.
- **IP Address**(IP 주소): HTTP를 사용하여 ASA에 액세스할 수 있는 모든 호스트/네트워크의 주소를 지정합니다.
- **Netmask**(넷마스크): 네트워크의 서브넷 마스크를 지정합니다.

참고 호스트를 제거하려면 **Actions**(작업) 아래에서 삭제 아이콘을 클릭합니다.

단계 6 **Save**(저장)를 클릭합니다.

NTP 서버를 사용하여 날짜 및 시간 설정

NTP는 네트워크 시스템 간에 정확하게 동기화된 시간을 제공하는 계층적 서버 시스템을 구현하는 데 사용됩니다. 정밀한 타임 스탬프가 포함된 CRL 검증과 같이 시간에 민감한 작업에는 이러한 정확성이 필요합니다. 여러 NTP 서버를 구성할 수 있습니다. ASA는 데이터의 신뢰도 지표인 **stratum**이 가장 낮은 서버를 선택합니다.


NTP 서버에서 가져온 시간은 직접 설정한 어떤 시간도 재정의합니다.

ASA는 NTPv4를 지원합니다.

단계 1 ASA 시스템 설정 편집 페이지의 왼쪽 창에서 **NTP**를 클릭합니다.

단계 2 공유 ASA 시스템 설정 정책의 값을 구성하려면 **Retain existing values**(기존 값 유지) 확인란의 선택을 취소합니다.

중요 **Retain existing values**(기존 값 유지) 확인란이 선택되어 있으면 필드가 표시되지 않으므로 값을 구성할 수 없습니다. CDO는 이 설정에 ASA 디바이스의 기존 로컬 값을 사용하며 공유 정책에서 상속되지 않습니다.

단계 3 NTP 서버 세부 정보를 추가하려면  를 클릭합니다.

- **IP Version(IP 버전)**: 사용할 IP 주소 버전을 선택합니다.

- **IP Address(IP 주소)**: NTP 서버의 IP 주소를 지정합니다.

서버의 호스트 이름은 입력할 수 없습니다. ASA에서는 NTP 서버에 대한 DNS 조회를 지원하지 않습니다.

- **Key Id(키 ID)**: 1~4294967295 사이의 숫자를 입력합니다.

이 설정은 이 인증 키의 키 ID를 지정합니다. 그러면 인증을 사용하여 NTP 서버와 통신할 수 있습니다. NTP 서버 패킷에서도 이 키 ID를 사용해야 합니다.

- **Interface Name(인터페이스 이름)**: 인터페이스 이름을 지정합니다. 여기에 지정된 인터페이스 이름이 이 공유 시스템 설정 정책과 연결된 ASA 디바이스에서 동일한지 확인하십시오.

NTP는 알고리즘을 사용하여 어떤 서버가 가장 정확한지 알아내고 그 서버와 동기화합니다. 서버의 정확도가 비슷하면 기본 서버를 사용합니다. 그러나 어떤 서버가 기본 서버보다 훨씬 더 정확할 경우 ASA는 더 정확한 쪽을 사용합니다.

- **Prefer(기본)**: (선택 사항) : 이 서버를 기본 서버로 설정하려면 **Preferred(기본)** 확인란을 선택합니다.

참고 NTP 서버를 제거하려면 **Actions**(작업) 아래에서 삭제 아이콘을 클릭합니다.

단계 4 **Save**(저장)를 클릭합니다.

SSH 액세스 구성

ASA에서 SCP(Secure Copy) 서버를 활성화할 수 있습니다. SSH를 사용하여 ASA에 액세스하는 것이 허용된 클라이언트만 SCP 연결을 설정할 수 있습니다.


단계 1 ASA 시스템 설정 편집 페이지의 왼쪽 창에서 **SSH**를 클릭합니다.

단계 2 공유 ASA 시스템 설정 정책의 값을 구성하려면 **Retain existing values**(기존 값 유지) 확인란의 선택을 취소합니다.

중요 **Retain existing values**(기존 값 유지) 확인란이 선택되어 있으면 필드가 표시되지 않으므로 값을 구성할 수 없습니다. CDO는 이 설정에 ASA 디바이스의 기존 로컬 값을 사용하며 공유 정책에서 상속되지 않습니다.

단계 3 **Enable Scopy SSH(Scopy SSH 활성화)**(보안 복사 SSH)를 활성화합니다.

단계 4 **Timeout in Minutes**(시간 초과(분)) 필드에서 1분~60분 범위에서 시간 제한을 설정합니다. 기본값은 5분입니다. 이 기본값은 대개 너무 짧으므로 모든 프로덕션 전 단계 테스트 및 문제 해결을 완료할 수 있도록 늘려야 합니다.

단계 5  을 클릭하고 다음을 구성합니다.

- **Interface**(인터페이스): 인터페이스 이름을 지정합니다. 여기에 지정된 인터페이스 이름이 이 공유 시스템 설정 정책과 연결된 ASA 디바이스에서 동일한지 확인하십시오.
- **IP Version**(IP 버전): 사용할 IP 주소 버전을 선택합니다.
- **IP Address**(IP 주소): SSH를 사용하여 ASA에 액세스할 수 있는 모든 호스트/네트워크의 주소를 지정합니다.
- **Netmask**(넷마스크): 네트워크의 서브넷 마스크를 지정합니다.

참고 SSH 세부 정보를 제거하려면 **Actions**(작업) 아래에서 삭제 아이콘을 클릭합니다.

단계 6 **Save**(저장)를 클릭합니다.

시스템 로깅 구성

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 인시던트 처리에 모두 유용합니다.

보안 수준

다음 표는 syslog 메시지 심각도 수준을 나열합니다.

표 1: Syslog 메시지 심각도 레벨

레벨 번호	Security Level(보안 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.

레벨 번호	Security Level(보안 레벨)	설명
5	notification(알림)	일반적이지만 중요한 상태입니다.
6	informational(정보)	정보 메시지만 해당됩니다.
7	debugging(디버깅)	디버깅 메시지만 해당됩니다. 문제를 디버깅할 때 이 레벨에서 일시적으로만 기록합니다. 이 로그 레벨은 시스템 성능에 영향을 미칠 수 있는 메시지를 너무 많이 생성할 수 있습니다.



참고 ASA는 심각도 레벨이 0(응급)인 Syslog 메시지를 생성하지 않습니다.


단계 1 ASA 시스템 설정 편집 페이지의 왼쪽 창에서 **Syslog**(시스템 로그)를 클릭합니다.

단계 2 공유 ASA 시스템 설정 정책의 값을 구성하려면 **Retain existing values**(기존 값 유지) 확인란의 선택을 취소합니다.

중요 **Retain existing values**(기존 값 유지) 확인란이 선택되어 있으면 필드가 표시되지 않으므로 값을 구성할 수 없습니다. CDO는 이 설정에 ASA 디바이스의 기존 로컬 값을 사용하며 공유 정책에서 상속되지 않습니다.

단계 3 다음을 구성합니다.

- **Logging Enabled**(로깅 활성화): 보안 로깅을 활성화합니다.
- **Timestamp Enabled**(타임스탬프 활성화): 시스템 로그 메시지에 날짜와 시간을 포함하려면 활성화합니다.
- **Permit host down**(호스트 다운 허용): (선택 사항)TCP 연결 syslog 서버가 다운되었을 때 새로운 연결을 차단하려면 이 기능을 비활성화합니다.
- **Buffer Size**(버퍼 크기): 내부 로그 버퍼의 크기를 지정합니다. 허용되는 범위는 4096 ~ 1048576바이트입니다.
- **Buffered Logging Level**(버퍼링된 로깅 수준): 임시 저장 위치 역할을 하는 내부 로그 버퍼로 어떤 시스템 로그 메시지를 전송할지 지정합니다.
- **Console Logging Level**(콘솔 로깅 수준): 콘솔 포트에 어떤 syslog 메시지를 보낼지 지정합니다.
- **Trap Logging Level**(트랩 로깅 수준): 어떤 시스템 로그 메시지를 시스템 로그 서버에 전송할지 지정합니다.

단계 4 시스템 로그 서버 세부 정보를 추가하려면  를 클릭합니다.

- **Interface Name**(인터페이스 이름): 시스템 로그 서버가 위치하는 인터페이스 이름을 지정합니다. 여기에 지정된 인터페이스 이름이 이 공유 시스템 설정 정책과 연결된 ASA 디바이스에서 동일한지 확인하십시오.
- **IP Version**(IP 버전): 사용할 IP 주소 버전을 선택합니다.

- **IP Address(IP 주소):** 시스템 로그 서버의 IP 주소를 지정합니다.
- **Protocol(프로토콜):** 시스템 로그 메시지를 시스템 로그 서버로 보낼 때 ASA가 사용해야 하는 프로토콜(TCP 또는 UDP)을 선택합니다.
 - **Port(포트):** 시스템 로그 서버가 시스템 로그 메시지에 대해 수신 대기하는 포트를 지정합니다. 허용되는 TCP 포트 범위는 1~65535이고, UDP 포트 범위는 1025~65535입니다.
 - **Log messages in Cisco EMBLEM format(Cisco EMBLEM 형식으로 메시지 기록)(UDP만 해당):** UDP만 사용하는 시스템 로그 서버에 대해 EMBLEM 형식 로깅을 사용하도록 활성화합니다.
 - **Enable secure syslog using SSL?(SSL을 사용하여 보안 시스템 로그 활성화?):** 원격 로깅 호스트로의 연결이 TCP에 한해 SSL/TLS를 사용하도록 지정합니다.
- **Reference Identity(참조 ID):** 이전에 구성된 참조 ID 개체를 기반으로 인증서에 대해 RFC 6125 참조 ID 확인을 활성화하려면 참조 ID 유형을 지정합니다. 참조 ID 개체에 대한 자세한 내용은 [Configure Reference Identities\(참조 ID 구성\)](#)을 참조하십시오.

참고 시스템 로그 서버를 제거하려면 **Actions(작업)** 아래에서 삭제 아이콘을 클릭합니다.

단계 5 **Save(저장)**를 클릭합니다.

Sysopt 설정 활성화

발신 인터페이스에 바인딩된 암호화 맵 ACL은 VPN 터널을 통한 IPsec 패킷을 허용 또는 거부합니다. IPsec는 IPsec 터널에서 도착하는 패킷을 인증하고 암호를 해독하며 터널에 연계된 ACL에 대한 평가를 받게 합니다.

ACL이 보호할 IP 트래픽을 정의합니다. 예를 들어 2개의 서브넷 또는 2개의 호스트 간에 모든 IP 트래픽을 보호하도록 ACL을 생성할 수 있습니다.

단계 1 ASA 시스템 설정 편집 페이지의 왼쪽 창에서 **Sysopt**를 클릭합니다.

단계 2 공유 ASA 시스템 설정 정책의 값을 구성하려면 **Retain existing values(기존 값 유지)** 확인란의 선택을 취소합니다.

중요 **Retain existing values(기존 값 유지)** 확인란이 선택되어 있으면 필드가 표시되지 않으므로 값을 구성할 수 없습니다. CDO는 이 설정에 ASA 디바이스의 기존 로컬 값을 사용하며 공유 정책에서 상속되지 않습니다.

단계 3 **Allow VPN traffic to bypass interface access lists(VPN 트래픽이 인터페이스 액세스 목록을 우회하도록 허용)**를 활성화하면 ACL 검사를 우회합니다.

단계 4 **Save(저장)**를 클릭합니다.

Shared System Settings(공유 시스템 설정) 페이지에서 정책 할당

공유 시스템 설정 정책을 구성한 후 온보딩된 ASA 디바이스를 할당하고 변경 사항이 적용되도록 디바이스에 설정을 구축합니다. 정책에 대한 변경 사항은 정책과 연결된 디바이스에 영향을 줍니다.

[Device-Specific Settings\(디바이스별 설정\) 페이지에서 정책 할당](#)할 수도 있습니다.



참고 ASA 디바이스를 하나의 공유 시스템 설정 정책에만 연결할 수 있습니다.


단계 1 **Policies(정책)** -> **ASA System Settings(ASA 시스템 설정)**를 선택합니다.

단계 2 공유 정책을 선택하고 **Edit(편집)**를 클릭합니다.

단계 3 정책 이름 옆에 나타나는 필터를 클릭하여 디바이스를 할당합니다.

단계 4 선택한 정책과 연결할 ASA 디바이스를 선택하고 **OK(확인)**를 클릭합니다.

참고 선택한 정책과 이미 연결된 디바이스에 대한 확인란이 선택됩니다.

빨간색 아이콘  이 표시되는 경우, 공유 시스템 설정 정책을 디바이스에 적용하는 중에 오류가 발생했음을 의미합니다. 문제를 해결하려면 **ASA System Settings(ASA 시스템 설정)** 페이지에서 정책을 클릭하고 **Error Detected(오류 탐지)** 창에서 **Device Workflows(디바이스 워크플로우)**를 클릭하여 추가 정보를 가져옵니다.

단계 5 변경한 사항을 **CDO GUI를 사용하여 구성 변경 사항 구축**합니다.

디바이스별 시스템 설정 구성 또는 수정

디바이스별 시스템 설정은 CDO를 사용하여 수정할 수 있는 ASA 디바이스에 해당하는 기존 값입니다. 공유 시스템 설정 정책 값을 원하는 매개변수의 기존의 디바이스 특정 값으로 재정의할 수 있습니다.

이 주제에서는 온보딩된 ASA 디바이스의 시스템 설정을 구성하는 방법에 대해 설명합니다.

단계 1 왼쪽 창에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 원하는 ASA 디바이스를 선택하고 오른쪽의 **Management(관리)** 창에서 **Settings(설정)**를 클릭합니다.

선택한 ASA 디바이스의 디바이스별 시스템 설정이 표시됩니다.

참고 선택한 디바이스에 공유 시스템 설정 정책이 할당된 경우 **Parent Policy(상위 정책)**에서 정책을 열 수 있는 링크를 제공합니다. 디바이스 관련 설정 페이지에서 정책을 할당할 수도 있습니다. 선택한 정책과 연결할 ASA 디바이스를 선택하고 **OK(확인)**를 클릭합니다.


단계 4 원하는 시스템 설정의 값을 구성하거나 수정하고 **Save(저장)**를 클릭합니다.

참고 공유 및 디바이스별 시스템 설정에 대한 필드 설명은 동일하게 유지됩니다. 아래의 해당 링크를 클릭하면 자세한 내용을 확인할 수 있습니다.

- 기본 DNS 설정 구성, 17 페이지
- HTTP 설정 구성, 18 페이지
- NTP 서버를 사용하여 날짜 및 시간 설정, 18 페이지
- SSH 액세스 구성, 19 페이지
- 시스템 로깅 구성, 20 페이지
- Sysopt 설정 활성화, 22 페이지

Return to Inventory(재고 목록으로 돌아가기)를 클릭하여 재고 목록 페이지로 이동할 수 있습니다.

단계 5 변경한 후 **Save**(저장)를 클릭합니다.

참고 해당 매개변수의 주황색 점()은 저장되지 않은 변경 사항을 강조 표시합니다.

Device-Specific Settings(디바이스별 설정) 페이지에서 정책 할당

온보딩된 ASA 디바이스의 디바이스별 설정 페이지에서 정책을 할당할 수도 있습니다.

단계 1 왼쪽 창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **ASA** 탭을 클릭합니다.

단계 3 원하는 ASA 디바이스를 선택하고 오른쪽의 **Management**(관리) 창에서 **Settings**(설정)를 클릭합니다.

선택한 ASA 디바이스의 디바이스별 설정이 표시됩니다.

참고 선택한 디바이스에 공유 시스템 설정 정책이 할당된 경우 **Parent Policy**(상위 정책)에서 정책을 열 수 있는 링크를 제공합니다. 선택한 정책과 연결할 ASA 디바이스를 선택하고 **OK**(확인)를 클릭합니다.

단계 4 공유 시스템 설정 정책을 할당하려면 **Parent Policy**(상위 정책) 버튼을 클릭합니다.

단계 5 정책을 선택하고 **Apply**(적용)를 클릭합니다.

단계 6 변경한 사항을 **CDO GUI**를 사용하여 구성 변경 사항 구축합니다.

공유 시스템 설정 정책에 ASA 디바이스 자동 할당

새 ASA 디바이스를 온보딩하거나 변경 사항을 확인하거나 기존 디바이스에 대한 대역 외 변경 사항을 전달할 때 CDO는 다음을 확인합니다.

- 디바이스별 설정이 기존 공유 시스템 설정 정책과 일치합니다. 일치하는 항목이 있으면 디바이스는 공유 시스템 설정 정책에 할당됩니다.
- 온보딩된 디바이스의 디바이스별 설정은 서로 일치합니다. 그러면 새 공유 시스템 설정 정책이 자동으로 생성되고, 동일한 로컬 설정의 디바이스가 이 공유 정책에 할당됩니다.



참고 사용자가 생성했는지 또는 시스템이 생성했는지에 상관없이 공유 설정 정책의 이름을 변경할 수 있습니다.

ASA 공유 시스템 설정 정책 필터링

ASA System Setting(ASA 시스템 설정) 페이지에서 특정 공유 시스템 설정 정책을 검색하는 경우 문제 및 사용량을 기준으로 필터를 사용하여 검색을 좁히고 더 쉽게 원하는 항목을 찾을 수 있습니다.

Policies(정책) > ASA System Settings(ASA 시스템 설정) > ▼를 선택합니다.

- **Issues(문제):**

- **Issue Detected(문제 탐지됨):** 디바이스를 적용할 때 문제가 있는 정책만 표시됩니다.
- **No issue(문제 없음):** 디바이스에 성공적으로 적용된 정책만 표시됩니다.

- **Usage(사용):**

- **In Use(사용 중):** 디바이스에 할당된 정책을 표시합니다.
- **Unused(사용되지 않음):** 디바이스에 아직 할당되지 않은 정책을 표시합니다.

공유 시스템 설정 정책에서 디바이스 연결 해제

ASA 디바이스가 공유 시스템 설정 정책에 더 이상 필요하지 않은 경우에는 쉽게 분리를 해제할 수 있습니다. 다음과 같은 경우 디바이스가 정책에서 분리됩니다.

- 디바이스 관련 설정이 변경되며, 이 경우 공유 정책의 해당 설정이 디바이스의 기존 값을 유지하도록 구성되지 않습니다.
- 디바이스는 공유 시스템 설정 정책에서 수동으로 분리됩니다.
- 공유 시스템 설정 정책이 CDO에서 삭제되었습니다. 이 경우 디바이스가 삭제되지는 않습니다. [공유 설정 정책 삭제, 26 페이지](#)의 내용을 참조하십시오.

단계 1 **Policies(정책) -> ASA System Settings(ASA 시스템 설정)**를 선택합니다.

단계 2 공유 정책을 선택하고 **Edit(편집)**를 클릭합니다.

단계 3 정책 이름 옆에 나타나는 필터를 클릭하여 디바이스를 분리합니다.

단계 4 선택한 공유 시스템 설정 정책에서 분리하려는 디바이스의 선택을 취소하고 **OK(확인)**를 클릭합니다.

참고 변경 사항은 자동으로 저장되며 수동 구축이 필요하지 않습니다.

공유 설정 정책 삭제

일부 공유 설정 정책을 제거하려는 경우 하나 이상의 정책을 선택하고 삭제할 수 있습니다. 하지만 아직 디바이스에 적용되거나 커밋되지 않은 경우에만 삭제할 수 있습니다.

시작하기 전에

삭제하려는 공유 설정 정책에서 디바이스가 분리되어 있는지 확인합니다. 자세한 내용은 [공유 시스템 설정 정책에서 디바이스 연결 해제](#)를 참조하십시오.

단계 1 **Policies(정책)** -> **ASA System Settings(ASA 시스템 설정)**를 선택합니다.

단계 2 공유 정책을 선택하고 **Delete(삭제)**를 클릭합니다.


단계 3 **OK(확인)**를 클릭하여 작업을 확인합니다.

참고 CDO에서 ASA를 삭제하면 디바이스 관련 설정 및 구성도 삭제되며 공유 설정 정책에서 디바이스 참조가 제거됩니다.


개체



개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 합니다.

디바이스를 온보딩하면, CDO는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects(개체)** 페이지에 나열합니다. **Objects(개체)** 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

CDO는 여러 디바이스에서 사용되는 개체를 **shared object(공유 개체)**라고 부르고 **Objects(개체)** 페이지에서 이 배지 로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects(중복 개체)**는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘 로 식별됩니다.

- **Inconsistent objects**(일관성 없는 개체) 는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘 로 식별됩니다.
- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘 로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다.

Objects(개체) 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 CDO에 의해 관리되는 개체를 볼 수 있습니다.

CDO은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. CDO에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.

- 다양한 기준에 따라 모든 개체를 검색하고 **모든 개체를 필터링**합니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.
- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- CDO에 은보당된 후 디바이스에서 사용 중인 개체를 캡처합니다.

은보당된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 [문제 해결 Cisco Defense Orchestrator](#)를 참조하십시오.

개체 유형

다음 표에서는 CDO를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

Table 2: ASA(Adaptive Security Appliance) 개체 유형

개체	설명
IP 주소 풀 생성	개별 IPv4 또는 IPv6 주소 또는 IP 주소 범위와 일치하도록 주소 풀 개체를 구성할 수 있습니다.

개체	설명
RA VPN AnyConnect 클라이언트 프로파일 업로드	AnyConnect 클라이언트 프로파일 개체는 파일 개체이며 구성(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect 클라이언트 프로파일 및 AnyConnect 클라이언트 이미지 파일을 포함할 수 있습니다.
네트워크	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다.
서비스	서비스 개체, 서비스 그룹 및 포트 그룹은 TCP/IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.
시간 범위	시간 범위 개체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. 네트워크 정책에서 이 개체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다.
신뢰 지점	신뢰 지점을 사용하여 ASA에서 디지털 인증서를 관리하고 추적할 수 있습니다.

공유 개체

CDO(Cisco Defense Orchestrator)는 이름과 콘텐츠가 동일한 여러 디바이스의 개체인 공유 개체를 호출합니다. 공유 개체는 이 아이콘으로 식별됩니다.



Objects(개체) 페이지에서 공유 개체를 사용하면 한 곳에서 개체를 수정할 수 있으며 변경 사항은 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 정책을 쉽게 유지 관리할 수 있습니다. 공유 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

공유 개체를 볼 때 CDO는 개체 테이블에 있는 개체의 내용을 표시합니다. 공유 개체는 정확히 동일한 내용을 갖습니다. CDO는 세부 정보 창에서 개체 요소의 결합된 보기 또는 "평평한" 보기를 보여줍니다. 세부 정보 창에서 네트워크 요소는 간단한 목록으로 병합되며 명명된 개체와 직접 연결되지 않습니다.

The screenshot shows the ASA configuration interface. On the left, a list of objects is displayed, with 'ATL-TMG-INT' selected. Below the list is a table with columns 'OBJECT REFERENCE' and 'TYPE'.

OBJECT REFERENCE	TYPE
ATLFTMGP01	Network Object
ATLFTMGP02	Network Object

On the right, the details for 'ATL-TMG-INT' are shown. It is a 'Network Group' of type 'Network Group'. Under the 'SHARED' section, a 'Network' dropdown is expanded, showing two IP addresses: '130.131.230.149' and '130.131.230.150'. Below this, the 'Relationships' section lists 'locksco1', 'locksco3', and 'locksco_1_1'.

개체 재정의

개체 오버라이드를 사용하면 특정 디바이스에서 공유 네트워크 개체의 값을 오버라이드할 수 있습니다. CDO는 오버라이드를 구성할 때 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 CDO는 이러한 값이 오버라이드 되기 때문에 **Inconsistent objects**(일관성 없는 개체)로 식별하지 않습니다.

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 각 사무실에 .프린터 서버가 있고, 프린터 서버 개체인 `print-server`를 만든 시나리오를 생각해 보십시오. ACL에는 프린터 서버가 인터넷에 액세스하는 것을 거부하는 규칙이 있습니다. 프린터 서버 개체에는 한 사무실에서 다른 사무실로 변경하려는 기본값이 있습니다. 값이 다를 수 있지만 개체 오버라이드를 사용하고 규칙과 "프린터-서버" 개체를 모든 위치에서 일관되게 유지함으로써 이 작업을 수행할 수 있습니다.

Editing Shared Network Object
✕

Object Name * Devices 2 Devices Usage 0 Rule Sets

print-server

Description

printer server object

Default Value ▾

eq ▲ 126.0.1.0 ASAv-99-18

Override Values ▾

Enter a value to add it

Value	Devices	
126.0.2.4	Pasadena-ftd-730-516-...	✎ ⬆ 🗑
126.0.1.6	BGL_FTD_7.3	✎ ⬆ 🗑
126.0.1.9	connected_fmc	✎ ⬆ 🗑

Cancel Save



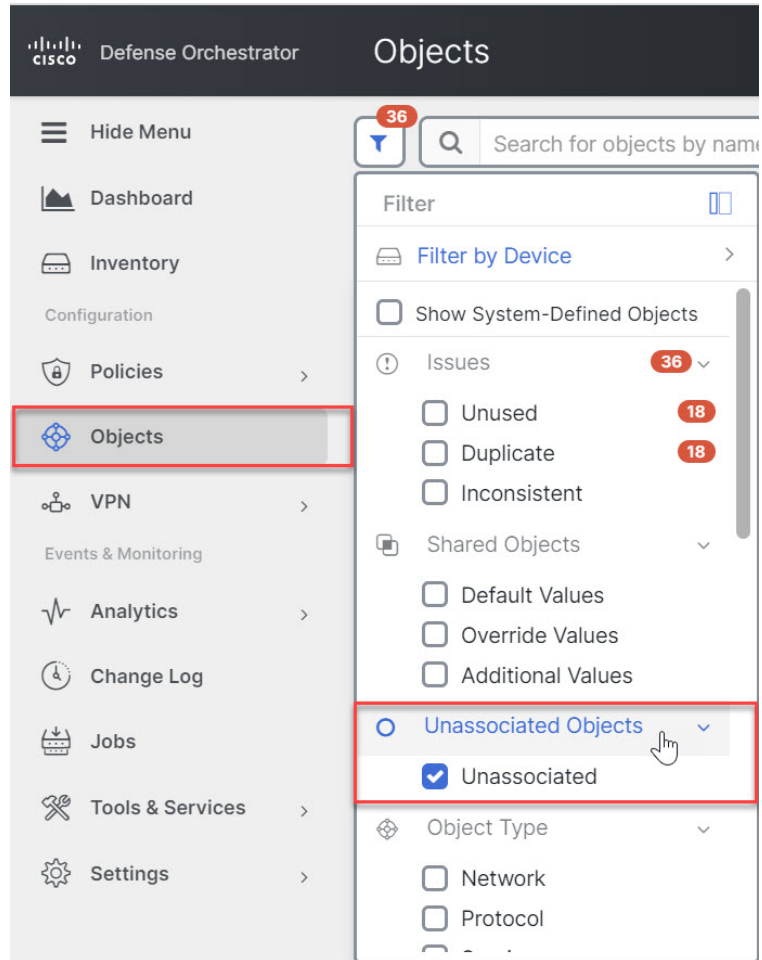
Note 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 [불일치 개체 문제 해결](#)을 참조하십시오.

연결 해제된 개체

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수 있습니다. 규칙이나 정책과 연결되지 않은 개체를 생성할 수도 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용할 때, CDO는 해당 개체의 사본을 생성하고 해당 사본을 사용합니다. 연결되지 않은 원래 개체는 야간 유지 관리 작업에 의해 삭제되거나 사용자가 삭제할 때까지 사용 가능한 개체 목록에 남아 있습니다.

개체와 연결된 규칙 또는 정책이 실수로 삭제된 경우 모든 구성이 손실되지 않도록 연결되지 않은 개체는 사본으로 CDO에 남아 있습니다.

연결되지 않은 개체를 보려면 개체 탭의 왼쪽 창에서 를 클릭하고 **Unassociated** (연결되지 않음) 확인란을 선택합니다.



개체 비교

단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 3 **Compare**(비교) 버튼  **Compare** 를 클릭합니다.

단계 4 비교할 개체를 최대 3개까지 선택합니다.


단계 5 화면 하단에서 개체를 나란히 봅니다.

- 개체 세부 정보 제목 표시줄에서 위쪽 및 아래쪽 화살표를 클릭하면 개체 세부 정보를 더 많이 또는 더 적게 볼 수 있습니다.
- 세부 정보 및 관계 상자를 확장하거나 축소하여 더 많거나 적은 정보를 확인합니다.

단계 6 (선택 사항) 관계 상자는 개체가 사용되는 방식을 보여줍니다. 디바이스 또는 정책과 연결될 수 있습니다. 개체가 디바이스와 연결된 경우 디바이스 이름을 클릭한 다음 **View Configuration**(구성 보기)을 클릭하여 디바이스 구성을 볼 수 있습니다. CDO는 디바이스의 구성 파일을 표시하고 해당 개체에 대한 항목을 강조 표시합니다.

필터

Inventory(재고 목록) 및 **Objects**(개체) 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

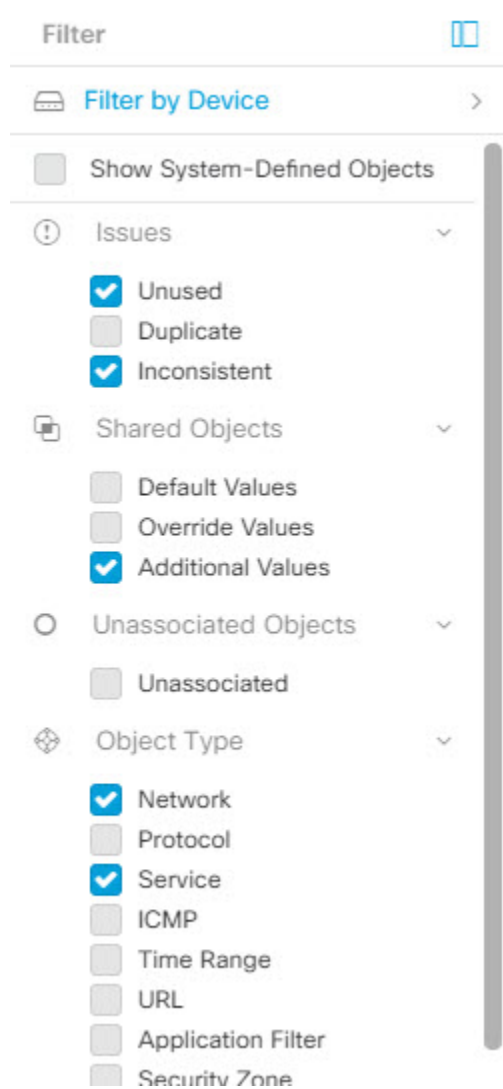
필터링하려면 **Inventory**(재고 목록), **Policies**(정책) 및 **Objects**(개체) 탭의 왼쪽 창에서 을 클릭합니다.

Inventory(재고 목록) 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.



개체 필터

필터링하려면 Objects(개체) 탭의 왼쪽 창에서 ▼을(를) 클릭합니다.

- **All Objects(모든 개체)** - 이 필터는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 개체를 제공합니다. 이 필터는 모든 개체를 찾아보거나 하위 필터를 검색하거나 추가로 적용하기 위한 시작점으로 유용합니다.
- **Shared Objects(공유 개체)** - 이 빠른 필터는 CDO가 두 개 이상의 디바이스에서 공유하는 것으로 확인한 모든 개체를 표시합니다.
- **Objects By Device(디바이스별 개체)** - 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 수 있습니다.

하위 필터 - 각 기본 필터에는 선택 범위를 좁히기 위해 적용할 수 있는 하위 필터가 있습니다. 이러한 하위 필터는 네트워크, 서비스, 프로토콜 등의 개체 유형을 기반으로 합니다.

이 필터 표시줄에서 선택한 필터는 다음 기준과 일치하는 개체를 반환합니다.

* 두 디바이스 중 하나에 있는 개체. (디바이스를 지정하려면 **Filter by Device**(디바이스별 필터링)를 클릭합니다.) 및

* 일치하지 않는 개체 및

* 네트워크 개체 또는 서비스 개체 및

* 개체 명명 규칙에 "group"이라는 단어가 있습니다.

Show System Objects(시스템 개체 표시)를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

시스템 개체 필터 표시

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.


Show System Objects(시스템 개체 표시)는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System Objects**(시스템 개체 표시)를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 **Show System Objects**(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

시스템 개체를 숨기면 검색 및 필터링 결과에 포함되지 않습니다. 시스템 개체를 표시하면 개체 검색 및 필터링 결과에 포함됩니다.

개체 필터 구성

원하는 만큼 기준을 필터링할 수 있습니다. 더 많은 범주를 필터링할수록 예상되는 결과는 줄어듭니다.

단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 페이지 상단의 필터 아이콘  을 클릭하여 필터 패널을 엽니다. 선택한 필터를 선택 취소하여 실수로 필터링된 개체가 없는지 확인합니다. 또한 검색 필드를 살펴보고 검색 필드에 입력되었을 수 있는 텍스트를 삭제합니다.

단계 3 특정 디바이스에 있는 것으로 결과를 제한하려면 다음을 수행합니다.

- a. **Filter By Device**(디바이스별 필터링)를 클릭합니다.
- b. 모든 디바이스를 검색하거나 디바이스 탭을 클릭하여 특정 종류의 디바이스만 검색합니다.
- c. 필터 기준에 포함할 디바이스를 선택합니다.
- d. **OK**(확인)를 클릭합니다.

단계 4 검색 결과에 시스템 개체를 포함하려면 **Show System Objects**(시스템 개체 표시)를 선택합니다. 검색 결과에서 시스템 개체를 제외하려면 **Show System Objects**(시스템 개체 표시)의 선택을 취소합니다.

단계 5 필터링할 개체 **Issues**(문제)를 선택합니다. 두 개 이상의 문제를 선택하면 선택한 범주의 개체가 필터 결과에 포함됩니다.

- 단계 6 문제가 있었지만 관리자가 무시한 개체를 확인하려면 **Ignored**(무시됨) 문제를 선택합니다.
- 단계 7 두 개 이상의 디바이스 간에 공유되는 개체를 필터링하는 경우 **Shared Objects**(공유 개체)에서 필수 필터를 선택합니다.
- **Default Values**(기본값): 기본값만 있는 개체를 필터링합니다.
 - **Override Values**(값 재정의): 오버라이드된 값이 있는 개체를 필터링합니다.
 - **Additional Values**(추가 값): 추가 값이 있는 개체를 필터링합니다.
- 단계 8 규칙 또는 정책의 일부가 아닌 개체를 필터링하는 경우 **Unassociated**(연결되지 않음)를 선택합니다.
- 단계 9 필터링할 개체 유형을 선택합니다.
- 단계 10 Objects(개체) 검색 필드에 개체 이름, IP 주소 또는 포트 번호를 추가하여 필터링된 결과 중에서 검색 기준으로 개체를 찾을 수도 있습니다.

필터 기준에서 디바이스를 제외해야 하는 경우

필터링 기준에 디바이스를 추가하면 결과에 디바이스의 개체가 표시되지만 해당 개체와 다른 디바이스의 관계는 표시되지 않습니다. 예를 들어 **ObjectA**가 ASA1과 ASA2 간에 공유된다고 가정합니다. ASA1에서 공유 개체를 찾기 위해 개체를 필터링하는 경우 **ObjectA**를 찾을 수 있지만 **Relationships**(관계) 창에는 해당 개체가 ASA1에 있다는 것만 표시됩니다.

개체와 관련된 모든 디바이스를 보려면 검색 기준에 디바이스를 지정하지 마십시오. 다른 기준으로 필터링하고 원하는 경우 검색 기준을 추가하십시오. CDO가 식별하는 개체를 선택한 다음 관계 창을 살펴봅니다. 개체와 관련된 모든 디바이스 및 정책이 표시됩니다.

개체 무시

사용되지 않거나 중복되거나 일관성이 없는 개체를 해결하는 한 가지 방법은 해당 개체를 무시하는 것입니다. 개체가 사용되지 않거나 중복되거나 일관성이 없더라도 해당 상태에 대한 타당한 이유가 있다고 판단하고 개체 문제를 해결되지 않은 상태로 두도록 선택할 수 있습니다. 나중에 무시된 개체를 해결해야 할 수도 있습니다. CDO는 개체 문제를 검색할 때 무시된 개체를 표시하지 않으므로 무시된 개체에 대한 개체 목록을 필터링한 다음 결과에 따라 조치를 취해야 합니다.

- 단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 무시된 개체를 필터링하고 검색합니다.
- 단계 3 **Object**(개체) 테이블에서 무시할 개체를 선택합니다. 한 번에 하나의 개체를 무시 취소할 수 있습니다.
- 단계 4 세부 정보 창에서 **Unignore**(무시)를 클릭합니다.
- 단계 5 요청을 확인합니다. 이제 문제별로 개체를 필터링하면 이전에 무시되었던 개체를 찾아야 합니다.

개체 삭제

단일 개체 또는 여러 개체를 삭제할 수 있습니다.

단일 개체 삭제



Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects(개체) > ASA Objects(ASA 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 1 왼쪽의 CDO 탐색 모음에서 **Objects(개체)**를 선택하고 옵션을 선택합니다.

단계 2 개체 필터와 검색 필드를 사용하여 삭제하려는 개체를 찾아 선택합니다.

단계 3 **Relationships(관계)** 창을 검토합니다. 개체가 정책 또는 개체 그룹에서 사용되는 경우 해당 정책 또는 그룹에서 개체를 제거할 때까지 개체를 삭제할 수 없습니다.

단계 4 작업 창에서 **Remove(제거)** 아이콘 를 클릭합니다.

단계 5 **OK(확인)**을 클릭하여 개체 삭제를 확인합니다.


단계 6 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

사용되지 않는 개체 그룹 삭제

디바이스를 온보딩하고 개체 문제를 해결하기 시작하면 사용하지 않는 개체를 많이 찾습니다. 한 번에 최대 50개의 사용하지 않는 개체를 삭제할 수 있습니다.

단계 1 **Issues(문제)** 필터를 사용하여 미사용 개체를 찾습니다. 디바이스 필터를 사용하여 디바이스 없음을 선택하여 디바이스와 연결되지 않은 개체를 찾을 수도 있습니다. 개체 목록을 필터링하면 개체 확인란이 나타납니다.

단계 2 개체 테이블 머리글에서 **Select all(모두 선택)** 확인란을 선택하여 개체 테이블에 나타나는 필터에 의해 발견된 모든 개체를 선택합니다. 또는 삭제할 개별 개체에 대한 개별 확인란을 선택합니다.

단계 3 작업 창에서 **Remove(제거)** 아이콘 를 클릭합니다.

단계 4 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

네트워크 개체

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 그룹은 그룹에 추가하는 네트워크 개체 및 기타 개별 주소 또는 서브 네트워크의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

Table 3: 네트워크 개체의 허용되는 값

디바이스 유형	IPv4 / IPv6	단일 주소	주소 범위	전체(Fully Qualified) 도메인 이름	CIDR 표기법의 서브넷
ASA	IPv4 및 IPv6	예	예	예	예

Table 4: 네트워크 그룹의 허용되는 콘텐츠

디바이스 유형	IP 값	네트워크 개체	네트워크 그룹
ASA	예	예	예

제품 간 네트워크 개체 재사용

Cisco Defense Orchestrator 테넌트가 하나 있고 클라우드 사용 Firewall Management Center 및 하나 이상의 온프레미스 Management Center가 테넌트에 온보딩된 경우:

- Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 사용 Firewall Management Center를 구성할 때 사용되는 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.
- Secure Firewall Threat Defense, FDM 관리 위협 방어 또는 ASA 네트워크 개체나 그룹을 생성하면 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Firewall Management Center에 대해 항목이 생성됩니다. 이 목록에서 개체를 사용하려는 온프레미스 Management Center에 개체를 선택하여 구축하고 원하지 않는 개체를 폐기할 수 있습니다. **Tools & Services(도구 및 서비스) > Firewall Management Center**로 이동하고, 온프레미스 Management Center를 선택한 후 **Objects(개체)**를 클릭하여 온프레미스 Firewall Management Center 사용자 인터페이스에서 개체를 확인하고 정책에 할당합니다.

한 페이지에서 네트워크 개체 또는 그룹에 대한 변경 사항은 두 페이지의 개체 또는 그룹 인스턴스에 적용됩니다. 한 페이지에서 개체를 삭제하면 다른 페이지에서도 개체의 해당 복사본이 삭제됩니다.

예외:

- 클라우드 사용 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우 Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체는 Cisco

Defense Orchestrator의 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지에서 복제되지 않습니다.

- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 위협 방어 디바이스의 네트워크 개체 및 그룹은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지에 복제되지 않으며, 클라우드 사용 Firewall Management Center에서 사용할 수 없습니다.

클라우드 사용 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall Management Center 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 구축된 정책에서 사용되었다면 네트워크 개체 및 그룹이 CDO 개체 페이지에 복제됩니다.

- CDO와 클라우드 사용 Firewall Management Center 간에 네트워크 개체 공유는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 사용 Firewall Management Center와 공유하지 않는 경우 **TAC에 문의**하여 테넌트에서 기능을 활성화하십시오.
- CDO와 온프레미스 Management Center 간의 네트워크 개체 공유는 CDO에 온보딩된 새 온프레미스 Management Center에 대해 CDO에서 자동으로 활성화되지 않습니다. 네트워크 개체가 온프레미스 Management Center와 공유되지 않는 경우 **Settings**(설정)에서 온프레미스 Management Center에 대해 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리) 토글 버튼이 활성화되어 있는지 확인하거나 **TAC에 문의**하여 테넌트에서 기능을 활성화하십시오.

네트워크 개체 보기

CDO를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 인식되는 CDO가 **Objects**(개체) 페이지에 표시됩니다. 개체 유형으로 레이블이 지정됩니다. 이렇게 하면 개체 유형으로 필터링하여 원하는 개체를 빠르게 찾을 수 있습니다.

Objects(개체) 페이지에서 네트워크 개체를 선택하면 **Details**(세부 정보) 창에 개체의 값이 표시됩니다. **Relationships**(관계) 창에는 개체가 정책에서 사용되는지 여부와 개체가 저장된 디바이스가 표시됩니다.

네트워크 그룹을 클릭하면 해당 그룹의 콘텐츠가 표시됩니다. 네트워크 그룹은 네트워크 개체에 의해 제공되는 모든 값의 복합물입니다.

ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집

ASA 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체, 네트워크 그룹 및 IP 주소의 복합 그룹입니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

Table 5: ASA 네트워크 개체 및 그룹의 허용 값

디바이스 유형	IPv4 / IPv6	단일 주소	주소 범위	PQDN(Partially Qualified Domain Name)	CIDR 표기법의 서브넷
ASA	IPv4 / IPv6	예	예	예	예



Note 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > ASA Objects(ASA 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.



Caution 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > ASA Objects(ASA 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

새 네트워크 개체 생성

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 개체는 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.



Note 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > ASA Objects(ASA 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**를 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **ASA > Network(ASA 네트워크)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 **Create a network object**(네트워크 개체 생성)를 선택합니다.

단계 6 (선택 사항) 개체 설명을 입력합니다.

단계 7 **Value**(값) 섹션에서 다음 방법 중 하나로 IP 주소 정보를 추가합니다.

- **eq**를 선택한 다음 단일 IP 주소, CIDR 표기법을 사용한 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택한 다음 IP 주소의 범위를 입력합니다. 시작 주소와 끝 주소를 공백으로 구분하여 범위를 입력합니다. 예: 10.1.1.1 10.1.1.255 또는 2001:DB8:1::1 2001:DB8:1::3

단계 8 **Add**(추가)를 클릭합니다.

Important 새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 ASA 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated**(연결되지 않음) 개체 범주를 선택합니다. 자세한 내용은 **개체 필터**를 참고하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

ASA 네트워크 그룹 생성

네트워크 그룹은 IP 주소 값, 네트워크 개체 및 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다. 네트워크 그룹은 IPv4 및 IPv6 주소를 모두 포함할 수 있습니다.



Note 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **ASA Objects**(ASA 개체) 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **ASA Objects**(ASA 개체)을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **ASA > Network**(ASA 네트워크)를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 **Create a network group**(네트워크 그룹 생성)을 선택합니다.

단계 6 (선택 사항) 개체 설명을 입력합니다.

- 단계 7 **Values(값)** 필드에 값 또는 개체 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.
- 단계 8 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
- 단계 9 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
- 단계 10 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(값 추가)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

Note 편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 11 필요한 개체를 추가한 후 **Add(추가)**를 클릭하여 새 네트워크 그룹을 생성합니다.

단계 12 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 212.](#)

ASA 네트워크 개체 편집



Caution


클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > ASA Objects(ASA 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 네트워크 개체를 선택하고 **Actions(작업)** 창에서 편집 아이콘  을 클릭합니다.

단계 4 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 편집합니다.

Note 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

ASA 네트워크 그룹 편집



Caution


클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **ASA Objects**(ASA 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.


한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **ASA Objects**(ASA 개체)를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.

단계 3 SGT 그룹을 선택하고 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 4 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

- a. 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘  을 클릭하여 편집합니다.
- b. 확인 표시를 클릭하여 변경 사항을 저장합니다.

Note 네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.

단계 5 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

- a. **Values**(값) 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
- b. CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add**(추가)를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
- c. 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.
 - 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name**(이 이름의 새 개체로 추가)을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

- 새 개체를 생성하려면 **Add as New Object**(새 개체로 추가)를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value**(값 추가)를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 6 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 정책이 표시됩니다.

단계 7 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 8 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 212.**

공유 네트워크 그룹에 값 추가

연결된 모든 디바이스에 있는 공유 네트워크 그룹의 값을 "기본값"이라고 합니다. CDO를 사용하면 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바이스에 해당 값을 할당할 수 있습니다. CDO는 변경 사항을 디바이스에 구축할 때 콘텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 푸시하고 지정된 디바이스에만 "추가 값"을 푸시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.



Note

일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 [일관되지 않은 개체 문제 해결](#)을 참조하십시오.




Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **ASA Objects**(ASA 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

-
- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.
- 단계 3 **Actions(작업)** 창에서 편집 아이콘  을 클릭합니다.
- **Devices(디바이스)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
 - **Usage(사용)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
 - **Default Values(기본값)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.
- 단계 4 추가 값 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.
- 단계 5 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
- 단계 6 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
- 단계 7 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.
- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
 - 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
 - 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(값 추가)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.
- 단계 8 **Devices(디바이스)** 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices(디바이스 추가)**를 클릭합니다.
- 단계 9 원하는 디바이스를 선택하고 **OK(확인)**를 클릭합니다.
- 단계 10 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.
- 단계 11 **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.
- 단계 12 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 212.](#)
-

공유 네트워크 그룹의 추가 값 편집

**Caution**


클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > ASA Objects(ASA 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Management Center에 대한 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Management Center에 구축할 수 있습니다.



한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > ASA Objects(ASA 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.

단계 3 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 오버라이드 값을 편집합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Devices(디바이스)** 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides(오버라이드 제거)**를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
- **Default Values(기본값)**의  화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
- **Override Values(값 재정의)**에서  화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
- 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 7 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 212.

네트워크 개체 및 그룹 삭제

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > ASA Objects(ASA 개체)** 페이지에서 네트워크 개체나 그룹을 삭제하면 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

트러스트 포인트 개체

CDO를 사용하면 디지털 인증서를 트러스트 포인트 개체로 추가한 다음 하나 이상의 관리 ASA 디바이스에 설치할 수 있습니다. 단일 트러스트 포인트 개체는 ID 쌍(ID 인증서 및 발급자의 CA 인증서), ID 인증서만 또는 CA 인증서만 포함하는 컨테이너입니다.

ASA 디바이스에서 여러 트러스트 포인트를 구성할 수 있습니다. 지원되는 인증서 형식은 PKCS12, PEM 및 DER입니다.

PKCS12를 사용하여 ID 인증서 개체 추가

이 절차에서는 인증서 파일을 업로드하거나 기존 인증서 텍스트를 텍스트 상자에 붙여넣어 내부 인증서 ID 또는 내부 ID 인증서를 생성합니다. ID 인증서는 원하는 만큼 생성할 수 있습니다.

PKCS12 형식으로 인코딩된 파일을 업로드할 수 있습니다. PKCS12는 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관하는 단일 파일입니다. PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다. 암호 해독을 위해 **Passphrase**(암호 문구) 값을 입력합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **ASA Objects**(ASA 개체)을 클릭합니다.

단계 2  아이콘을 클릭하고 **ASA > Trustpoints**(트러스트 포인트)를 선택합니다.

단계 3 인증서의 **Object Name**(개체 이름)을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지 않습니다.

단계 4 **Certificate Type**(인증서 유형) 단계에서 **Identity Certificate**(ID 인증서)를 선택합니다.

단계 5 **Import Type**(가져오기 유형) 단계에서 **Upload**(업로드)를 선택하여 인증서 파일을 업로드합니다.

Enrollment(등록) 단계가 **Terminal**(터미널)로 설정되어 있습니다.

단계 6 **Certificate Contents**(인증서 콘텐츠) 단계에서 PKCS12 형식 세부 정보를 입력합니다.

PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다. 암호 해독을 위해 **Passphrase**(암호 문구) 값을 입력합니다.

단계 7 **Continue**(계속)를 클릭합니다.

단계 8 **Advanced Options**(고급 옵션) 단계에서 다음을 구성할 수 있습니다.

Revocation(해지) 탭에서 다음을 구성할 수 있습니다.

- **CRL**(Certificate Revocation List) 활성화 - CRL 확인 활성화 여부를 확인합니다.

기본적으로 **Use CRL distribution point from the certificate**(인증서에서 CRL 배포 지점 사용) 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

Cache Refresh Time (in minutes)(캐시 새로 고침 시간(분)) - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **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.

Disable Nonce Extension(Nonce 확장 비활성화) - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce 확장 비활성화)** 확인란을 선택 취소합니다.

Evaluation Priority(평가 우선순위) - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

해지 확인에 대한 자세한 내용은 [Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책](#), XY 문서에서 "디지털 인증서" 장을 참조하십시오.

Others(기타) 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(다음을 위한 CA 인증서 사용)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.

- **IPSec Client(IPSec 클라이언트)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
- **SSL Client(SSL 클라이언트)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
- **SSL Server(SSL 서버)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.

- **Use Identity Certificate for(ID 인증서 사용)** - 등록된 ID 인증서의 사용 방법을 지정합니다.

- **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.
- **Code Signer(코드 서명자)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.

- 기타 옵션:

- **Enable CA flag in basic constraints extension(기본 제약 조건 확장에서 CA 플래그 활성화)** - 이 인증서에서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
- **Accept certificates issued by this CA(CA에서 발급된 인증서 허용)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
- **Ignore IPsec Key Usage(IPsec 키 사용 무시)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 9 **Add(추가)**를 클릭합니다.

자체 서명 인증서 개체 생성

이 절차에서는 마법사에서 적절한 인증서 필드 값을 입력하여 ASA에 대한 자체 서명 인증서를 생성하는 단계를 설명합니다. 자체 서명 인증서는 원하는 만큼 생성할 수 있습니다.

자체 서명 ID 인증서 개체를 생성하려면 다음 단계를 수행합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 2  아이콘을 클릭하고 **ASA > Trustpoints(트러스트 포인트)**를 선택합니다.

단계 3 인증서의 **Object Name(개체 이름)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 4 **Identity Certificate(ID 인증서)** 단계에서 **Identity Certificate(ID 인증서)**를 선택합니다.

단계 5 **Import Type(가져오기 유형)** 단계에서 **New(새로 만들기)**를 선택하여 인증서 파일을 업로드하고 **Continue(계속)**를 클릭합니다.

단계 6 **Enrollment(등록)** 단계에서 **Self-Signed(자체 서명)**를 선택하고 **Continue(계속)**를 클릭합니다.

Certificates Content(인증서 콘텐츠) 단계가 나타납니다. 생성 중인 자체 서명 인증서의 CN 및 SANS 콘텐츠를 이해하려면 [인증서 콘텐츠를 기반으로 하는 자체 서명 및 CSR 인증서 생성](#)을 읽어보십시오.

단계 7 **Certificate Contents(인증서 콘텐츠)** 단계에서 다음을 구성합니다.

- **국가(C)**— 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(주/도) (ST)** — 인증서에 포함할 주/도입니다.
- **Locality or City(구/군/시) (L)** — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- **조직(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(조직 단위(부서)) (OU)** — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- **일반 이름(CN)** - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Email Address(이메일 주소) (EA)**— ID 인증서와 연결된 이메일 주소입니다.
- **IP Address(IP 주소)**— 점으로 구분된 4개의 십진수로 표기되는 네트워크상의 ASA IP 주소입니다.
- **Device's FQDN(디바이스의 FQDN)**— DNS 트리 계층 구조에서 노드의 위치를 나타내는 명확한 도메인 이름입니다.
- **Include Device's Serial Number(디바이스의 일련 번호 포함)**— 인증서 매개 변수에 ASA 일련 번호를 추가하려면 확인란을 선택합니다.

a) **Key(키)** 탭을 클릭합니다.

- **RSA** 또는 **ECDSA** 키 유형을 선택합니다.
- **Key Size(키 크기)** - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. RSA의 권장 키 크기는 1024이고 ECDSA의 경우 348입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)
- **Continue(계속)**를 클릭합니다.

단계 8 **Advanced Options(고급 옵션)** 단계에서 다음을 구성할 수 있습니다.

Revocation(해지) 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List) 활성화** - CRL 확인 활성화 여부를 확인합니다.

기본적으로 **Use CRL distribution point from the certificate(인증서에서 CRL 배포 지점 사용)** 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

Cache Refresh Time (in minutes)(캐시 새로 고침 시간(분)) - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **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.

Disable Nonce Extension(Nonce 확장 비활성화) - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce 확장 비활성화)** 확인란을 선택 취소합니다.

Evaluation Priority(평가 우선순위) - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OCSP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached(해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주)** - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

해지 확인에 대한 자세한 내용은 **Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책**, XY 문서에서 "디지털 인증서" 장을 참조하십시오.

Others(기타) 탭을 클릭합니다.

- **Use CA Certificate for the Validation of(다음을 위한 CA 인증서 사용)** - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
 - **IPSec Client(IPSec 클라이언트)** - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.

- **SSL Client(SSL 클라이언트)** - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
- **SSL Server(SSL 서버)** - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- **Use Identity Certificate for(ID 인증서 사용)** - 등록된 ID 인증서의 사용 방법을 지정합니다.
 - **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.
 - **Code Signer(코드 서명자)** — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.
- 기타 옵션:
 - **Enable CA flag in basic constraints extension(기본 제약 조건 확장에서 CA 플래그 활성화)** - 이 인증서에 서 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
 - **Accept certificates issued by this CA(CA에서 발급된 인증서 허용)** - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
 - **Ignore IPsec Key Usage(IPsec 키 사용 무시)** - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 9 **Add(추가)**를 클릭합니다.

CSR(Certificate Signing Request)을 위한 ID 인증서 개체 추가

CSR(Certificate Signing Requests)을 생성하고 지정된 CA에서 ID 인증서를 얻으려면 CA(Certification Authority) 서버 정보 및 등록 매개변수가 필요합니다. 요청을 생성하려면 RSA(Rivest-Shamir-Adleman) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 키 유형을 선택해야 합니다.

식별 정보를 제공하고 선택적으로 CA에서 얻은 CA 인증서를 업로드하여 트러스트 포인트 개체를 생성합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 2  아이콘을 클릭하고 **ASA > Trustpoints(트러스트 포인트)**를 선택합니다.

단계 3 인증서의 **Object Name(개체 이름)**을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 4 **Identity Certificate(ID 인증서)** 단계에서 **Identity Certificate(ID 인증서)**를 선택합니다.

단계 5 **Import Type(가져오기 유형)** 단계에서 **New(새로 만들기)**를 선택하여 인증서 파일을 업로드하고 **Continue(계속)**를 클릭합니다.

단계 6 **Enrollment(등록)** 단계에서 **Manual(수동)**을 선택합니다.

단계 7 (선택 사항) CA에서 가져온 CA 인증서를 붙여넣거나 업로드할 수 있습니다. 필드를 비워둘 수 있습니다.

단계 8 Continue(계속)를 클릭합니다.

Certificates Content(인증서 콘텐츠) 단계가 나타납니다. 생성 중인 서명 인증서의 CN 및 SANS 콘텐츠를 이해하려면 **인증서 콘텐츠를 기반으로 하는 자체 서명 및 CSR 인증서 생성**을 읽어보십시오.

단계 9 **Certificate Contents**(인증서 콘텐츠) 단계에서 다음을 구성합니다.

- **국가(C)**— 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(주/도) (ST)** — 인증서에 포함할 주/도입니다.
- **Locality or City(구/군/시) (L)** — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- **조직(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(조직 단위(부서)) (OU)** — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- **일반 이름(CN)** - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Email Address(이메일 주소) (EA)**— ID 인증서와 연결된 이메일 주소입니다.
- **IP Address(IP 주소)**— 점으로 구분된 4개의 십진수로 표기되는 네트워크상의 ASA IP 주소입니다.
- **SAN(Subject Alternative Name)** - 이 필드는 'unstructuredName'으로도 인증서 주체 DN의 일부가 됩니다. 인증서가 여러 도메인 또는 IP 주소에 사용되는 경우, 이 필드를 활용하는 것이 좋습니다.
 - **Use Device Host Name**(디바이스 호스트 이름 사용): 디바이스의 호스트 이름이 사용됩니다.
 - **Custom: Device's FQDN**(사용자 지정 디바이스의 FQDN)— DNS 트리 계층 구조에서 노드의 위치를 나타내는 명확한 도메인 이름입니다.

참고 CN 및 사용자 지정 FQDN에 지정된 값은 동일한 것이 좋습니다.
- **Include Device's Serial Number**(디바이스의 일련 번호 포함)— 인증서에 ASA의 일련 번호를 추가하려면 확인란을 선택합니다. CA는 인증서 인증 또는 추후 특정 디바이스와 인증서를 연결하기 위해 일련 번호를 사용합니다. 확실하지 않은 경우 일련 번호를 포함하면 디버깅 시 유용합니다.

a) **Key**(키) 탭을 클릭합니다.

- **RSA** 또는 **ECDSA** 키 유형을 선택합니다.
- **Key Size**(키 크기) - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. RSA의 권장 키 크기는 1024이고 ECDSA의 경우 384입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)
- **Continue**(계속)를 클릭합니다.

단계 10 **Advanced Options**(고급 옵션) 단계에서 다음을 구성할 수 있습니다.

Revocation(해지) 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

기본적으로 **Use CRL distribution point from the certificate**(인증서에서 CRL 배포 지점 사용) 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

Cache Refresh Time (in minutes)(캐시 새로 고침 시간(분)) - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **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.

Disable Nonce Extension(Nonce 확장 비활성화) - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장으로 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce 확장 비활성화)** 확인란을 선택 취소합니다.

Evaluation Priority(평가 우선순위) - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OCSP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached**(해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주) - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

해지 확인에 대한 자세한 내용은 [Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책](#), XY 문서에서 "디지털 인증서" 장을 참조하십시오.

Others(기타) 탭을 클릭합니다.

- **Use CA Certificate for the Validation of**(다음에 대한 CA 인증서 사용) - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.

- **IPSec Client**(IPSec 클라이언트) - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
- **SSL Client**(SSL 클라이언트) - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
- **SSL Server**(SSL 서버) - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.

- **Use Identity Certificate for**(ID 인증서 사용) - 등록된 ID 인증서의 사용 방법을 지정합니다.

- **SSL & IPSec** - SSL 및 IPSec 연결 인증에 사용합니다.
- **Code Signer**(코드 서명자) — 코드 서명자 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA에서 가져온 것으로, 서명된 코드 자체가 인증서 원본을 나타냅니다.

• 기타 옵션:

- **Enable CA flag in basic constraints extension**(기본 제약 조건 확장에서 CA 플래그 활성화) - 이 인증서에 다른 인증서에 서명할 수 있어야 하는 경우 이 옵션을 선택합니다. 기본 제약 조건 확장은 인증서의 주체가 CA(Certificate Authority)인지 여부를 식별하며 이 경우 인증서를 사용하여 다른 인증서에 서명할 수 있습니다. CA 플래그는 이 확장의 일부입니다. 인증서에 이러한 항목이 있는지 여부
- **Accept certificates issued by this CA**(CA에서 발급된 인증서 허용) - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
- **Ignore IPsec Key Usage**(IPsec 키 사용 무시) - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 11 **Add**(추가)를 클릭합니다.

이렇게 하면 트러스트 포인트 인증서 개체가 생성됩니다.

신뢰할 수 있는 CA 인증서 개체 추가

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성하십시오. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **ASA Objects**(ASA 개체)을 클릭합니다.

단계 2  아이콘을 클릭하고 **ASA > Trustpoints**(트러스트 포인트)를 선택합니다.

단계 3 인증서의 **Object Name**(개체 이름)을 입력합니다. 이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 4 **Certificate Type**(인증서 유형) 단계에서 **Trusted CA Certificate**(신뢰할 수 있는 CA 인증서)를 선택합니다.

단계 5 **Certificate Contents**(인증서 콘텐츠) 단계에서 텍스트 상자에 인증서 콘텐츠를 붙여넣거나 마법사의 설명에 따라 CA 인증서 파일을 업로드합니다.

단계 6 **Continue**(계속)를 클릭합니다. 마법사가 4단계로 진행합니다.

인증서는 다음 지침을 따라야 합니다.

- 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.
- 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.

- 붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxZzAJBgNV
BAYTA1VTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAxh
OTIuMTY4LjEuMTEUMTBIGAlUEAwLMTkyLjE2OC4xLjEwHhcNMjYxMjMjIzNDE3
WhcNMjYxMjMjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAKGA1UECAwCVFgxDzAN
BgNVBACMBmFlc3RpbjEUMTBIGAlUECgwLMTkyLjE2OC4xLjEwExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIIICiJANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgK1OwXbRvOdkstzTezVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZx9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMfEXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

단계 7 **Advanced Options**(고급 옵션) 단계에서 다음을 구성할 수 있습니다.

Revocation(해지) 탭에서 다음을 구성할 수 있습니다.

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.

기본적으로 **Use CRL distribution point from the certificate**(인증서에서 CRL 배포 지점 사용) 확인란이 선택되어 인증서에서 해지 목록 배포 URL을 가져옵니다.

Cache Refresh Time (in minutes)(캐시 새로 고침 시간(분)) - 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 범위는 1분 ~ 1440분입니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐시이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 상황을 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

- **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.

Disable Nonce Extension(Nonce 확장 비활성화) - 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 확인란을 활성화합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable Nonce Extension(Nonce 확장 비활성화)** 확인란을 선택 취소합니다.

Evaluation Priority(평가 우선순위) - 인증서의 해지 상태를 CRL에서 먼저 평가할지 OSCP에서 먼저 평가할지를 지정합니다.

- **Consider the certificate valid if revocation information cannot be reached**(해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주) - 해지 정보에 연결할 수 없는 경우 인증서를 유효한 인증서로 간주하려면 이 확인란을 선택합니다.

해지 확인에 대한 자세한 내용은 [Cisco ASA Series 일반 운영 ASDM 설정의 "기본 설정" 책](#), XY 문서에서 "디지털 인증서" 장을 참조하십시오.

Others(기타) 탭을 클릭합니다.

- **Use CA Certificate for the Validation of**(다음을 위한 CA 인증서 사용) - 이 CA가 검증할 수 있는 연결 유형을 지정합니다.
 - **IPSec Client**(IPSec 클라이언트) - 원격 SSL 서버에서 제공하는 인증서를 검증합니다.
 - **SSL Client**(SSL 클라이언트) - 수신 SSL 연결에서 제공하는 인증서를 검증합니다.
 - **SSL Server**(SSL 서버) - 수신 IPSec 연결에서 제공하는 인증서를 검증합니다.
- 기타 옵션:
 - **Enable CA flag in basic constraints extension**(기본 제약 확장에서 CA 플래그 활성화) - 기본 제약 확장을 사용하는 인증서의 주체가 CA인지 검증하려면 이 옵션을 선택합니다.
 - **Accept certificates issued by this CA**(CA에서 발급된 인증서 허용) - ASA에서 지정된 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
 - **Accept certificates issued by the subordinates CAs of this CA**(이 CA의 하위 CA에서 발급한 인증서 수락) - ASA에서 하위 CA의 인증서를 허용해야 하는 경우 이 옵션을 선택합니다.
 - **Ignore IPsec Key Usage**(IPsec 키 사용 무시) - IPsec 원격 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않으려는 경우 이 옵션을 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

단계 8 **Add**(추가)를 클릭합니다.

이렇게 하면 트러스트 포인트 인증서 개체가 생성됩니다.

인증서 내용을 기반으로 하는 자체 서명 및 CSR 인증서 생성

자체 서명 및 CSR 인증서의 CN 및 SANS 콘텐츠에 대한 아이디어가 필요합니다. 콘텐츠는 생성 과정에서 지정한 매개변수를 기반으로 합니다. AnyConnect 클라이언트가 조직의 원하는 VPN 헤드엔드에 연결하려면 매개변수를 정확하게 구성해야 합니다.

이 섹션에서는 지정된 매개변수를 기반으로 자체 서명 및 CSR 인증서의 내용에 대한 아이디어를 제공하는 다양한 사용 사례를 예시와 함께 제공합니다.

사용 사례 1: 다른 CN 및 FQDN 값

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: mysan.com

표 6: 예: 다른 CN 및 FQDN 값

	공용 이름(CN)	unstructuredName	SANS
자체 서명	mywebsite.com	mysan.com	mysan.com
CSR	mywebsite.com	mysan.com	-

사용 사례 2: 없음으로 설정된 FQDN 필드

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: 없음

표 7: 예: 없음으로 설정된 FQDN 필드

	공용 이름(CN)	SANS
자체 서명	호스트 이름	-
CSR	mywebsite.com	-

사용 사례 3: FQDN 없음(기본 FQDN)

예:

- Common Name(공용 이름)(CN): mywebsite.com

표 8: 예: FQDN 없음(기본 FQDN)

	공용 이름(CN)	unstructuredName	SANS
자체 서명	mywebsite.com	호스트 이름	-
CSR	mywebsite.com	호스트 이름	호스트 이름

사용 사례 4: FQDN에 IP 주소가 지정됨

예:

- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: 4.5.6.7

표 9: 예: FQDN에 IP 주소가 지정됨

	공용 이름(CN)	unstructuredName	SANS
자체 서명	mywebsite.com	4.5.6.7	-

	공용 이름(CN)	unstructuredName	SANS
CSR	mywebsite.com	4.5.6.7	4.5.6.7

사용 사례 5: IP 주소가 지정됨

예:

- IP 주소: 4.5.6.7
- Common Name(공용 이름)(CN): mywebsite.com
- FQDN: fqdn.com

표 10: 예: IP 주소가 지정됨

	공용 이름(CN)	unstructuredAddress	unstructuredName	SANS
자체 서명	mywebsite.com	4.5.6.7	fqdn.com	-
CSR	mywebsite.com	4.5.6.7	fqdn.com	fqdn.com

사용 사례 6: 일련 번호 확인란이 선택됨

예:

- 일련 번호: 9AQXMWOKDT9

표 11: 예: IP 일련 번호 확인란이 선택됨

	serialNumber	SANS
자체 서명	9AQXMWOKDT9	-
CSR	9AQXMWOKDT9	fqdn.com

활용 사례 7: 이메일 주소가 지정됨

예:

- EA: abc@xyz.com

표 12: 예: 이메일 주소가 지정됨

	unstructuredName	emailAddress	SANS
자체 서명	호스트 이름	abc@xyz.com	호스트 이름
CSR	호스트 이름	abc@xyz.com	-

RA VPN 개체

서비스 개체

ASA 서비스 개체

ASA 서비스 개체, 서비스 그룹 및 포트 그룹은 IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다. 서비스 개체에서 단일 프로토콜을 지정하고 이를 소스 포트, 목적지 포트 또는 소스 및 목적지 포트 모두에 할당할 수 있습니다. 서비스 그룹은 여러 서비스 개체를 포함하며 여러 프로토콜을 포함할 수 있습니다.

포트 그룹은 일종의 ASA 서비스 개체입니다. 포트 그룹은 서비스 유형(예: TCP 또는 UDP)과 포트 번호 또는 포트 번호 범위를 페어링하는 포트 개체를 포함합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 보안 정책의 개체를 사용할 수 있습니다. 예를 들어 액세스 제어 규칙에서 이를 사용하여 특정 TCP 포트 범위에 대한 트래픽을 허용할 수 있습니다.

자세한 내용은 [ASA 서비스 개체 생성 및 편집](#)을 참조하십시오.

프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름 및 [프로토콜 번호](#)로 식별됩니다. CDO는 ASA 및 Firepower(FDM 관리) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

ICMP 개체

ICMP(Internet Control Message Protocol) 개체는 ICMP 및 IPv6-ICMP 메시지를 위한 서비스 개체입니다. CDO는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되고 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공할 때 이러한 개체를 인식합니다.

CDO를 사용하면 ASA 구성에서 ICMP 개체를 제거하거나 이름을 바꿀 수 있습니다. CDO를 사용하여 Firepower 구성에서 ICMP 및 ICMPv6 개체를 생성, 업데이트 및 삭제할 수 있습니다.



Note ICMPv6 프로토콜의 경우 AWS는 특정 인수 선택을 지원하지 않습니다. 모든 ICMPv6 메시지를 허용하는 규칙만 지원됩니다.

관련 정보:

- [개체 삭제](#)

ASA 서비스 개체 생성 및 편집

서비스 개체에서 단일 프로토콜을 지정하고 이를 소스 포트, 목적지 포트 또는 소스 및 목적지 포트 모두에 할당할 수 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 2 **Create Object(개체 생성) > ASA > Service(서비스)**를 클릭합니다.

단계 3 개체 이름을 입력합니다.

단계 4 서비스 개체 생성을 선택합니다.

단계 5 **Service Type(서비스 유형)** 버튼을 클릭하고 개체를 만들 프로토콜을 선택합니다.

- **TCP, UDP 및 TCP-UDP** 서비스 유형의 경우 소스 포트, 목적지 포트 또는 둘 다를 입력합니다.
 - 소스 포트 식별자를 사용하면 번호가 지정된 특정 포트에서 시작되는 트래픽을 일치시킬 수 있습니다. 소스 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
 - 목적지 포트 식별자를 사용하면 번호가 지정된 특정 포트에 도착하는 트래픽을 일치시킬 수 있습니다. 목적지 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
- 프로토콜 서비스 유형에 대해, 0-255 사이의 **프로토콜 번호** 또는 ip, tcp, udp, gre 등과 같이 잘 알려진 이름을 입력합니다.

단계 6 **Add(추가)**를 클릭합니다.

예

- 수신 FTP 트래픽을 식별하는 서비스 개체는 TCP 서비스 유형 및 대상 포트 범위가 21인 개체입니다.
- 발신 DNS 및 TCP 트래픽을 통한 DNS를 식별하는 서비스 개체는 tcp-udp 서비스 유형 및 소스 포트가 53인 개체입니다.

ASA 서비스 그룹 생성

서비스 그룹은 하나 이상의 프로토콜을 나타내는 하나 이상의 서비스 개체로 구성될 수 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 2 **Create Object(개체 생성) > ASA > Service(서비스)**를 클릭합니다.

단계 3 개체 이름을 입력합니다.

단계 4 **Create a service group(서비스 그룹 생성)**를 선택합니다.

단계 5 **Add Object(개체 추가)**를 클릭하고, 개체를 선택하고, **Select(선택)**을 클릭하여 기존 개체를 추가합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 6 필요한 경우 서비스 그룹에 별도의 개별 서비스 유형 값을 추가합니다.

- **TCP, UDP 및 TCP-UDP** 서비스 유형의 경우 소스 포트, 목적지 포트 또는 둘 다를 입력합니다.

- 소스 포트 식별자를 사용하면 번호가 지정된 특정 포트에서 시작되는 트래픽을 일치시킬 수 있습니다. 소스 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
- 목적지 포트 식별자를 사용하면 번호가 지정된 특정 포트에 도착하는 트래픽을 일치시킬 수 있습니다. 목적지 포트 식별자에서 같음, 범위, 보다 작음, 보다 큼 또는 같지 않음 연산자를 선택하고 적절한 포트 번호 또는 범위를 제공합니다.
- 프로토콜 서비스 유형에 대해, 0-255 사이의 **프로토콜 번호** 또는 ip, tcp, udp, gre 등과 같이 잘 알려진 이름을 입력합니다.

단계 7 개별 포트 값을 더 추가하려면 **Add Another Value**(다른 값 추가)를 클릭하고 단계 6을 반복합니다.

단계 8 서비스 그룹에 서비스 개체 및 서비스 값 추가를 완료하면 **Add**(추가)를 클릭합니다.

ASA 서비스 개체 또는 서비스 그룹 편집

단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **ASA Objects**(ASA 개체)를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 세부 정보 창에서 **Edit**(편집)  를 클릭합니다.

단계 4 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

ASA 시간 범위 개체

시간 범위 개체란 무엇입니까?

시간 범위 개체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. 네트워크 정책에서 이 개체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다. 예를 들어, 업무 시간에만 특정 서버에 대한 액세스를 허용하는 액세스 규칙을 만들 수 있습니다. 시간 범위 생성은 디바이스에 대한 액세스를 제한하지 않습니다. 이러한 개체에 대해 구성된 시간은 디바이스에 대해 로컬입니다.

이 개체에 절대 또는 반복 시간 범위를 추가할 수 있습니다. 반복 범위는 주기적인 시간 범위로 간주됩니다.



Note 시간 범위에 절대값과 기간 값이 모두 지정된 경우, 절대 시작 시간에 도달해야 기간 값의 평가가 이루어지며 절대 종료 시간에 도달하면 더 이상 평가되지 않습니다.

ASA 시간 범위 개체 생성

다음 절차에 따라 ASA 디바이스에 대한 시간 범위 개체를 생성합니다.


단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **ASA > 시간범위(Time Range)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 시간 범위를 정의합니다.

- 절대 시간 범위 - 원하는 시간 범위에 대한 시작 시각과 종료 시각을 입력합니다. 몇 분, 몇 시간, 며칠 또는 몇 주에 걸쳐 이 개체를 실행하도록 선택할 수 있습니다. 시간 범위 개체는 하나의 절대 시간 범위만 가질 수 있습니다.
- 반복 시간 범위 -  를 클릭하여 일주일 내내 반복되는 주기적 시간 범위를 추가합니다. 드롭다운 메뉴에서 **Frequency(빈도)**, 시간 범위가 적용될 **Days(요일)** 및 **Start(시작)** 및 **End(종료)** 시각을 선택합니다. 시간 범위 개체는 여러 주기 범위를 가질 수 있습니다.

Note 시간 범위 개체에 대한 시작 및 종료 시각은 옵션입니다. 개체에 설정된 시작 시각이 없는 경우 시간 범위가 즉시 적용됩니다. 개체에 설정된 종료 시각이 없는 경우 시간 범위는 무기한 지속됩니다.

단계 6 **Add(추가)**를 클릭하여 개체를 생성합니다.

ASA 시간 범위 개체 편집

다음 절차를 사용하여 ASA 디바이스에 대한 시간 범위 개체를 편집합니다.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > ASA Objects(ASA 개체)**를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 세부 정보 창에서 **Edit(편집)**  를 클릭합니다.

단계 4 필요에 따라 값을 편집하고 **Save(저장)**를 클릭합니다.

단계 5 개체가 현재 정책에서 사용 중인 경우 CDO는 변경의 영향을 받는 정책을 표시합니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 6 개체가 디바이스의 정책에서 사용되는 경우 변경 사항을 지금 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 여러 변경 사항을 여러 변경 사항을 한 번에 배포합니다.

관련 정보:

- [개체 삭제](#)
- [레거시 ASA 액세스 정책 관리](#)

ASA 라우팅

라우팅 프로토콜은 메트릭을 사용하여 패킷이 이동할 최적의 경로를 평가합니다. 메트릭은 경로 대역폭과 같은 측정 기준이며, 대상에 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 데 사용됩니다.

ASA 고정 경로 정보

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.

ASA 라우팅 개념 및 CLI 명령에 대한 일반적인 정보는 다음 문서를 참조하십시오.

- [ASDM 책 1: Cisco ASA 시리즈 일반 작업 ASDM 구성 가이드, X,Y](#)의 정적 및 기본 경로 장.
- [CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드, X,Y](#)의 정적 및 기본 경로 장.

기본 라우터

가장 간단한 옵션은 트래픽을 라우팅해주는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 정적 경로를 컨피그레이션하는 것입니다. 기본 고정 경로는 ASA가 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 ASA에 직접 연결되지 않은 내부 네트워크로 트래픽을 안 내할 수 없습니다.
- 동적 라우팅 프로토콜을 지원하지 않는 기능을 사용 중입니다.

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 ASA의 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.

ASA에서는 ASA에서 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 ASA가 통신해야 하는 대상 네트워크에 있는 서버.
- 목적지 네트워크에 있는 지속적인 네트워크 객체.

ASA 고정 경로 구성

고정 경로는 특정 목적지 네트워크로 향하는 트래픽을 어디로 보낼지 정의합니다.

이 섹션에서는 ASA 디바이스에 고정 경로를 추가하는 단계를 설명합니다.

- 단계 1 왼쪽 창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **ASA** 탭을 클릭합니다.
- 단계 3 고정 경로를 구성할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Routing**(라우팅)을 클릭합니다.

단계 5  를 클릭하여 고정 경로를 추가합니다.

단계 6 경로에 대한 **Description**(설명)을 입력할 수 있습니다.

단계 7 경로가 **IPv4** 주소인지 아니면 **IPv6** 주소인지를 선택합니다.

단계 8 경로 속성을 구성합니다.

- **Interface**(인터페이스): 트래픽을 전송하는 데 사용할 인터페이스를 선택합니다. 이 인터페이스를 통해 게이트웨이 주소에 액세스할 수 있어야 합니다.

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.

ASA CLI에서는 Null0 또는 null0 문자열을 모두 사용이 가능합니다.

- **Gateway**(게이트웨이): (**Null0** 경로에는 적용되지 않음) 대상 네트워크에 대해 게이트웨이의 IP 주소를 식별하는 네트워크 개체를 선택합니다. 트래픽은 이 주소로 전송됩니다.
- **Metric**(메트릭): 경로의 관리 거리(1~254)입니다. 정적 경로의 경우 기본값은 1입니다. 인터페이스와 게이트웨이 간에 추가 라우터가 있으면 홉 수를 관리 거리로 입력합니다.

관리 거리는 경로를 비교하는 데 사용되는 파라미터입니다. 값이 작을수록 경로에는 더 높은 우선 순위가 지정됩니다. 연결된 경로(디바이스의 인터페이스에 직접 연결되는 네트워크)가 항상 고정 경로보다 우선적으로 사용됩니다.

- **Destination IP**(대상 IP): 대상 네트워크를 식별하고 이 경로에서 게이트웨이를 사용하는 호스트를 포함하는 네트워크 개체를 선택합니다.
- **Destination Mask**(대상 마스크)(IPv4 주소 지정에만 해당): 대상 IP의 서브넷 마스크를 입력합니다.
- **Tracking**(추적)(IPv4 주소 지정에만 해당): 필드에 경로 추적 프로세스를 위한 고유한 식별자를 입력합니다.

단계 9 **Save**(저장)를 클릭합니다.

단계 10 변경 사항을 **CDO GUI**를 사용하여 구성 변경 사항 구축하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

ASA 고정 경로 편집

ASA 디바이스와 연결된 고정 경로 매개변수를 편집할 수 있습니다.



참고 그러나 고정 경로를 수정하는 동안 다른 IP 버전을 선택할 수는 없습니다. 또는 요구 사항에 따라 새 고정 경로를 생성할 수 있습니다.

단계 1 고정 경로를 수정할 ASA 디바이스를 선택합니다.

단계 2 오른쪽의 **Management**(관리) 창에서 **Routing**(라우팅)을 클릭합니다.

단계 3 라우팅 목록 페이지에서 수정할 경로를 선택하고 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

- 단계 4 원하는 값을 수정하고 **Save**(저장)를 클릭합니다. 라우팅 매개변수에 대한 자세한 내용은 [ASA 고정 경로 구성, 63 페이지](#)의 내용을 참조하십시오.
- 단계 5 변경 사항을 [CDO GUI를 사용하여 구성 변경 사항 구축](#)하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

고정 경로 삭제

시작하기 전에

고정 경로를 삭제하면 디바이스의 로컬 SDC 또는 CDO에 대한 연결에 영향을 줄 수 있습니다. 연결 손실에 대비하여 적절한 재해 복구 절차를 적용해야 합니다.

- 단계 1 삭제할 ASA 디바이스를 선택합니다.
- 단계 2 오른쪽의 **Management**(관리) 창에서 **Routing**(라우팅)을 클릭합니다.
- 단계 3 라우팅 목록 페이지에서 수정할 경로를 선택하고 오른쪽의 **Actions**(작업) 창에서 **Delete**(삭제)를 클릭합니다.
- 단계 4 OK(확인)를 클릭하여 변경 사항을 확인합니다.
- 단계 5 변경 사항을 [CDO GUI를 사용하여 구성 변경 사항 구축](#)하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

보안 정책 관리

보안 정책에서 네트워크 트래픽을 검사하는 궁극적인 목표는 트래픽을 의도한 대상으로 허용하거나 보안 위협이 식별된 경우 트래픽을 삭제하는 것입니다. CDO를 사용하여 다양한 유형의 디바이스에서 보안 정책을 구성할 수 있습니다.

- [ASA 정책\(확장 액세스 목록\), 76 페이지](#)
- [네트워크 주소 변환, 83 페이지](#)

레거시 ASA 액세스 정책 관리

이 섹션에서는 Cisco CDO(Defense Orchestrator)에서 관리하는 모든 디바이스에서 사용 중인 모든 네트워크 정책 목록을 표시하는 레거시 네트워크 정책 페이지에 대한 정보를 제공합니다. **Policies**(정책) > **ASA Policies**(ASA 정책)을 탐색하여 네트워크 정책 페이지로 이동합니다.

네트워크 정책은 네트워크 규칙의 모음입니다. 각 네트워크 규칙은 원본 및 대상 IP 주소, IP 프로토콜, 포트 번호, EtherType 등과 같은 특성을 기반으로 네트워크 트래픽이 네트워크 대상에 도달하는 것을 허용하거나 방지합니다.

CDO는 네트워크 정책을 생성할 때 이를 ASA 인터페이스와 연결하고 정책에 하나의 기본 규칙을 생성합니다. 네트워크 정책은 인터페이스와 연결될 때 ASA에서 "액세스 그룹"이라고 합니다. 정책이

름은 ASA의 ACL(액세스 제어 목록) 이름과 동일합니다. CDO가 만든 기본 규칙과 이 네트워크 정책에 추가하는 후속 규칙을 ASA에서는 ACE(액세스 제어 항목)이라고 합니다.

관련 정보:

- 레거시 보기에서 ASA 네트워크 정책 생성
- ASA 네트워크 정책 편집
- ASA 네트워크 정책 복사
- ASA 네트워크 정책 비교
- ASA 네트워크 정책 삭제
- ASA 네트워크 정책 및 규칙 검색 및 필터링
- 공유 ASA 네트워크 정책
- ACE(액세스 제어 항목)

레거시 보기에서 ASA 네트워크 정책 생성

이 절차를 사용하여 ASA 네트워크 정책을 생성합니다.

단계 1 **Policies**(정책) > **ASA Policies**(ASA 정책)를 선택합니다.

단계 2 **Create Policy**(정책 생성)를 클릭합니다.

단계 3 디바이스 필터를 클릭하여 정책을 저장할 디바이스를 검색하십시오.

단계 4 정책의 이름을 입력합니다. 참고로 디바이스에 이름이 같은 두 개의 네트워크 정책이 있을 수 없습니다.

단계 5 이 정책을 적용하려는 인터페이스를 선택합니다.

단계 6 정책이 아웃바운드 또는 인바운드 트래픽용인지 지정합니다. 참고로 동일한 디바이스에서 동일한 방향으로 동일한 인터페이스에 대해 두 개의 정책을 가질 수 없습니다.

단계 7 **Save**(저장)를 클릭합니다. CDO는 네트워크 정책 및 해당 정책에 대한 단일 "permit IP any any" 규칙을 생성합니다.

단계 8 필요에 따라 **ASA 네트워크 정책 편집**합니다.

단계 9 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한번에 구축합니다.

ASA 네트워크 정책 편집

Defense Orchestrator를 사용하면 정책 세부 정보 페이지에서 네트워크 정책 및 정책 규칙을 편집할 수 있습니다. 다음과 같은 방법으로 ASA 정책을 편집할 수 있습니다.


- 정책 이름 변경
- 정책에 규칙 추가

- 정책 내에서 규칙 이동
- 정책 간 규칙 이동
- 정책에서 규칙 비활성화
- 로그 규칙 활동
- 정책의 시간 범위 정의

정책 이름 변경

단계 1 **Policies(정책) > ASA Policies(ASA 정책)**를 선택합니다.

단계 2 이름을 바꾸려는 네트워크 정책을 선택합니다.

단계 3 세부 정보 창에서 이름 변경 아이콘  를 클릭합니다.


단계 4 정책 이름을 편집한 다음 파란색 확인란을 클릭하여 변경 사항을 저장합니다.

정책에 규칙 추가

단계 1 **Policies(정책) > ASA Policies(ASA 정책)**을 선택합니다.

단계 2 편집하려는 네트워크 정책을 선택합니다.

단계 3 **Edit Policy(정책 편집)**를 클릭합니다.

단계 4 세부 정보 창에서 도구 편집 도구 모음의  을 클릭하여 네트워크 정책에 규칙을 추가합니다. 정책에서 강조 표시된 규칙 위에 새 규칙이 추가됩니다. 규칙은 규칙 목록의 위치에 따라 1부터 "마지막"까지 우선 순위가 지정됩니다.

Note 새 규칙에는 기본적으로 **Permit(허용)** 작업이 할당됩니다.

단계 5 **Save(저장)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 6 정책 세부 정보 창에서 디바이스 필드를 검토합니다. 최적의 항목 수를 초과한 경우 ASA가 설치된 ASA 하드웨어 모델에 따라 "ACE 수 초과, 최대 항목 500개, 1000개 발견"과 같은 경고가 표시됩니다.


단계 7 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.


정책 내에서 규칙 이동

단계 1 **Policies(정책) > ASA Policies(ASA 정책)**을 선택합니다.

단계 2 네트워크 정책을 선택합니다.



단계 3 세부 정보 창에서 **Edit Policy(정책 편집)**를 클릭합니다.

단계 4 규칙 테이블에서 규칙을 선택하고 편집 도구 모음에서 **cut(잘라내기)**  를 클릭합니다.

- 단계 5 방금 잘라낸 규칙이 앞에 오도록 할 규칙을 선택합니다. 규칙은 규칙 목록에서 위치별로 우선 순위가 지정됩니다. 규칙이 높을수록 우선 순위가 높아집니다.
- 단계 6 Paste(붙여넣기) 를 클릭합니다.
- 단계 7 Save(저장)를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.
- 단계 8 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.


정책 간 규칙 이동

한 정책에서 규칙을 복사하여 다른 정책에 붙여넣을 수 있습니다.

- 단계 1 **Policies(정책) > ASA Policies(ASA 정책)**를 선택합니다.
- 단계 2 복사할 규칙이 있는 네트워크 정책을 선택합니다.
- 단계 3 세부 정보 창에서 **Edit Policy(정책 편집)**를 클릭합니다.
- 단계 4 규칙 테이블에서 규칙을 선택하고 편집 도구 모음에서 **copy(복사)** 를 클릭합니다.
- 단계 5 **Policies(정책) > ASA Policies(ASA 정책)**을 선택합니다.
- 단계 6 규칙을 복사할 네트워크 정책을 선택합니다.
- 단계 7 세부 정보 창에서 **Edit Policy(정책 편집)**를 클릭합니다.
- 단계 8 방금 복사한 규칙 뒤에 올 규칙을 선택합니다. 규칙은 규칙 목록에서 위치별로 우선 순위가 지정됩니다. 규칙이 높을수록 우선 순위가 높아집니다.
- 단계 9 Paste(붙여넣기) 를 클릭합니다.
- 단계 10 **Save(저장)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.
- 단계 11 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

정책에서 규칙 비활성화

규칙은 기본적으로 활성화되어 있습니다. 정책 내에서 개별 규칙을 비활성화할 수 있습니다.

- 단계 1 **Policies(정책) > ASA Policies(ASA 정책)**을 선택합니다.
- 단계 2 비활성화하려는 규칙이 있는 네트워크 정책을 선택합니다.
- 단계 3 세부 정보 창에서 **Edit Policy(정책 편집)**를 클릭합니다.
- 단계 4 비활성화하려는 규칙을 선택합니다.
- 단계 5  활성 설정을 끕니다.
- 단계 6 **Save(저장)**를 클릭합니다.
- 단계 7 **Save(저장)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 8 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

로그 규칙 활동


네트워크 정책 규칙으로 인한 활동은 기본적으로 로깅되지 않습니다. 개별 규칙에 대한 로깅을 활성화할 수 있습니다.

단계 1 **Policies(정책) > ASA Policies(ASA 정책)**를 선택합니다.

단계 2 활성화하려는 규칙이 있는 네트워크 정책을 선택합니다.

단계 3 세부 정보 창에서 **Edit Policy(정책 편집)**를 클릭합니다.

단계 4 활동을 로깅하려는 규칙을 선택합니다.

단계 5 로깅을 활성화하려면 슬라이더를 클릭합니다. 

단계 6 **Edit(편집)**를 클릭합니다.

단계 7 해당 규칙의 활동이 수집되는 로깅 수준과 빈도를 선택합니다. 다음 표는 Syslog 메시지 심각도 수준을 나열합니다.

심각도 레벨	설명
emergencies(비상)	시스템을 사용할 수 없습니다.
Alert(긴급 경고)	즉각적인 행동이 필요합니다.
critical(심각)	심각한 상태입니다.
error(오류)	오류 상태입니다.
warning(경고)	경고 상태입니다.
notification(알림)	일반적이지만 중요한 상태입니다.
informational(정보)	정보 메시지만 해당됩니다.
debugging(디버깅)	디버깅 메시지만 해당됩니다.
Note	ASA는 심각도 레벨이 0(응급)인 Syslog 메시지를 생성하지 않습니다.

단계 8 로깅 간격을 변경할 수도 있습니다. 로깅 간격은 해당 간격 동안 로그에 도달한 횟수를 보여줍니다. 로깅 간격은 1~600초 범위에서 정의됩니다. 기본값은 300입니다. 이 값은 삭제 통계 수집에 쓰이는 캐시에서 비활성 플로우를 삭제하기 위한 시간 초과 값으로도 사용됩니다.

단계 9 **Save(저장)**를 클릭합니다. Defense Orchestrator는 변경의 영향을 받는 디바이스를 식별합니다.

단계 10 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

정책의 시간 범위 정의

시간 기반 ASA 네트워크 정책은 시간을 기준으로 네트워크 및 리소스에 대한 액세스를 허용합니다. 시간은 시간 범위 개체로 정의됩니다. 시간 범위 개체에는 시작 시간과 종료 시각이 있으며 반복 이벤트로 정의할 수도 있습니다.


시간 범위 개체가 ASA에 이미 정의되어 있는 경우 이를 네트워크 정책과 연결할 수 있습니다. 시간 범위 개체가 ASA에 아직 존재하지 않는 경우 Defense Orchestrator의 CLI 도구를 사용하여 생성하거나 ASA에서 직접 생성해야 합니다.

네트워크 정책에 대한 시간 범위를 추가하려면 다음 절차를 따르십시오.

- 단계 1 **Policies(정책) > ASA Policies(ASA 정책)**를 선택합니다.
- 단계 2 편집하려는 네트워크 정책을 선택합니다.
- 단계 3 **Edit Policy(정책 편집)**를 클릭합니다.
- 단계 4 네트워크 정책 상자에서 슬라이더를 클릭하여 시간 범위를 활성화합니다.
- 단계 5 시간 범위 개체를 생성하거나 드롭다운 목록에서 기존 시간 범위 개체를 **Choose(선택)**합니다.
- 단계 6 **Save(저장)**를 클릭합니다.
- 단계 7 **Devices & Services(디바이스 및 서비스)** 페이지로 돌아가 방금 정책을 편집한 디바이스를 선택합니다. 디바이스가 동기화되지 않았는지 확인해야 합니다.
- 단계 8 미리보기 및 배포...를 클릭합니다.
- 단계 9 디바이스 동기화 상자에서 정책을 생성할 명령과 정책의 규칙을 검토합니다.
- 단계 10 제안된 변경 사항에 만족하면 **Apply Changes to Device(디바이스에 변경 사항 적용)**를 클릭합니다.
- 단계 11 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA 네트워크 정책 복사

이 절차를 사용하여 한 ASA에서 다른 ASA로 네트워크 정책을 복사합니다.

- 단계 1 **Policies(정책) > ASA Policies(ASA 정책)**를 선택합니다.
- 단계 2 복사하려는 정책을 검색하고 필터링합니다.
- 단계 3 복사할 네트워크 정책 행에서 **copy icon(복사 아이콘)**를 클릭합니다. 
- 단계 4 디바이스에 정책을 추가합니다.

- 단일 인터페이스에 할당된 네트워크 정책의 경우: **Add Policy to Device**(디바이스에 정책 추가) 대화 상자에서 정책을 복사할 디바이스, 인터페이스 및 트래픽 방향을 선택합니다. 전역 액세스 정책을 다른 디바이스에 복사하는 경우
- 전역 정책의 경우: **Add Policy to Device**(디바이스에 정책 추가) 대화 상자에서 정책을 복사할 디바이스를 선택하고 전역 정책으로 만들기를 선택합니다. 정책에 대한 인터페이스나 방향을 선택할 수 없음을 알 수 있습니다. 전역 정책은 항상 디바이스의 모든 인터페이스에 할당되며 항상 인바운드 트래픽을 평가합니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA 네트워크 정책 비교

단계 1 탐색 창에서 **Policies**(정책) > **ASA Policies**(ASA 정책)을 선택합니다.

단계 2 뷰어의 오른쪽 상단에서 **Compare**(비교)를 클릭합니다.

단계 3 비교할 최대 2개의 정책을 선택합니다.

단계 4 뷰어 하단에서 **View Comparison**(비교 보기)를 클릭합니다. 그러면 비교 뷰어가 나타납니다. 마치면 **Done**(완료)를 클릭한 다음 **Done Comparing**(비교 완료)를 클릭합니다.

ASA 네트워크 정책 삭제

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭하고 정책을 삭제할 ASA를 검색하여 선택합니다.

단계 4 관리 창에서 **Configuration**(구성)를 클릭합니다.

단계 5 **Edit**(편집)를 클릭합니다.

단계 6 디바이스 구성에서 네트워크 정책 및 규칙을 찾습니다.

네트워크 정책은 ASA 구성 파일에서 액세스 그룹이라고 하며 형식은 다음과 같습니다.

```
access-group <policy name> <direction of traffic> interface <interface name>
```

다음은 액세스 그룹 항목의 예입니다.

```
access-group abc-75-1-out out interface interface-1
```

네트워크 규칙은 ASA 구성 파일에서 액세스 목록이라고 하며 형식은 다음과 같습니다.

```
access-list <policy name> extended permit ip any any
```

다음은 액세스 목록 항목의 예입니다.

```
access-list abc-75-1-out extended permit ip any any
```

단계 7 네트워크 정책이 포함된 행과 네트워크 규칙이 포함된 행을 강조 표시하고 삭제합니다.

단계 8 변경 사항을 **Save**(저장)합니다.

단계 9 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA 네트워크 정책 및 규칙 검색 및 필터링

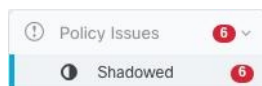
검색 표시줄을 사용하여 네트워크 정책의 이름과 정책 내의 규칙에서 이름, 키워드 또는 구를 검색합니다. 검색은 대/소문자를 구분하지 않습니다.

필터

필터 사이드바를 사용하여 네트워크 정책 문제, 공유 정책 및 특정 디바이스에 대한 정책을 찾으십시오. 필터링은 추가되지 않으며 각 필터 설정은 서로 독립적으로 작동합니다.

정책 문제

CDO는 새도우 규칙이 포함된 네트워크 정책을 식별합니다. 새도우 규칙을 포함하는 정책의 수는 정책 문제 필터에 표시됩니다.



CDO는 네트워크 정책 페이지에서 새도우 배지 **●**로 새도우 규칙과 이를 포함하는 네트워크 정책을 표시합니다. 새도우 규칙을 포함하는 모든 정책을 보려면 **Shadowed**(숨겨짐)를 클릭합니다. 자세한 내용은 **새도우 규칙**을 참조하십시오.

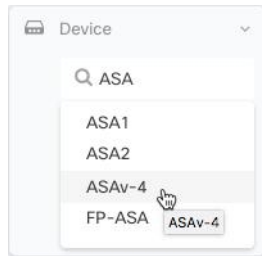
공유 정책

공유 정책은 두 개 이상의 디바이스에서 발견되는 정책입니다. 공유 정책에 대한 변경 사항은 해당 정책이 있는 모든 디바이스에 영향을 미칩니다. 아래 예에서 **inside-acl-in** 정책은 두 디바이스에서 공유됩니다. 자세한 내용은 **공유 ASA 네트워크 정책**을 참조하십시오.

Network Policies		
Q Search for policies by name, components or objects used		
NAME	DEVICES	INTERFACES
▶ ● inside-acl-in	2	

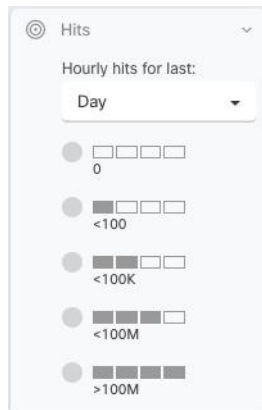
디바이스

Device(디바이스) 필터를 확장하고 **Search devices**(디바이스 검색) 필드에 이름 또는 IP 주소를 입력한 다음 결과에서 찾은 디바이스를 선택하여 디바이스별로 네트워크 정책 목록을 필터링합니다.



Hits(히트)

이 필터를 사용하여 지정된 기간 동안 여러 번 트리거된 디바이스 전체의 정책을 찾으십시오.



적중 횟수가 0인 모든 네트워크 정책 찾기

적중되지 않은 네트워크 정책이 있는 경우 정책을 수정하여 더 효과적으로 만들거나 간단히 삭제할 수 있습니다.

-
- 단계 1 **Policies**(정책) > **ASA Policies**(정책)을 탐색합니다.
 - 단계 2 필터 창에서 **Show All**(모두 표시)을 클릭하여 기존 필터를 지웁니다.
 - 단계 3 **Hits**(적중) 필터를 확장합니다.
 - 단계 4 기간을 선택합니다.
 - 단계 5 0의 적중 횟수를 선택합니다.
-

적중 횟수가 0인 디바이스의 모든 네트워크 정책 찾기

-
- 단계 1 **Policies**(정책) > **ASA Policies**(정책)을 탐색합니다.
 - 단계 2 필터 창에서 **Show All**(모두 표시)을 클릭하여 기존 필터를 지웁니다.
 - 단계 3 디바이스 필터를 확장하고 필터링할 디바이스를 선택합니다.
 - 단계 4 **Hits**(적중) 필터를 확장합니다.

단계 5 기간을 선택합니다.

단계 6 0의 적용 횟수를 선택합니다.

네트워크 정책의 규칙이 적용되는 빈도 찾기

단계 1 **Policies**(정책) > **ASA Policies**(정책)을 탐색합니다.

단계 2 필터 창에서 **Show All**(모두 표시)을 클릭하여 기존 필터를 지웁니다.

단계 3 하나의 디바이스에서 사용되는 네트워크 정책을 선택합니다.

단계 4 네트워크 정책의 각 규칙이 적용되는 빈도를 알아보려면 규칙 테이블의 **Hits**(적중) 열을 살펴보십시오.

단계 5 네트워크 정책에 규칙이 너무 많아 결과를 한 눈에 볼 수 없는 경우 적용 필터를 확장합니다.

단계 6 기간을 선택합니다.

단계 7 다른 적용 필터를 선택하여 다른 규칙이 어떤 범주에 속하는지 확인합니다.

공유 네트워크 정책이 적용되는 빈도 찾기

네트워크 정책에 대한 적용은 개별 디바이스에 대해 계산됩니다. 필터에서 디바이스를 지정하지 않으면 두 개 이상의 디바이스에서 공유되는 단일 네트워크 정책에 대한 적용률을 확인할 수 없습니다.

단계 1 **Policies**(정책) > **ASA Access Policies**(ASA 액세스 정책)를 탐색합니다.

단계 2 기존 정책을 지우려면 정책 테이블 위에서 **Clear**(지우기)를 클릭합니다.

단계 3 **Shared Policies**(공유 정책) 필터를 확장하고 **Shared**(공유)를 클릭합니다.

단계 4 공유 네트워크 정책을 선택합니다.

단계 5 해당 정책의 세부 정보 창에서 해당 네트워크 정책을 사용하는 디바이스를 기록한 다음 네트워크 정책 테이블로 돌아갑니다.

단계 6 검색 필드에 공유 정책의 이름을 입력합니다.

단계 7 **Devices**(디바이스) 필터를 확장하고 공유 정책을 사용하는 디바이스 중 하나로 필터링합니다.

단계 8 **Hits**(적중) 필터를 확장합니다.

단계 9 기간을 선택합니다.

단계 10 다른 적용 필터를 선택하여 어떤 범주에 속하는지 결정합니다.

적용률을 기준으로 네트워크 정책 필터링

단계 1 **Policies**(정책) > **ASA Access Policies**(ASA 액세스 정책)를 탐색합니다.

단계 2 기존 필터를 지우려면 정책 테이블 위에서 **Clear**(지우기)를 클릭합니다.

단계 3 **Hits**(적중) 필터를 확장합니다.

단계 4 기간을 선택합니다.

단계 5 다른 적중률 범주를 선택합니다. CDO는 지정한 적중률만큼 적중되는 정책을 표시합니다. 적중률 기준과 일치하는 공유 네트워크 정책이 있는 경우 CDO는 공유 정책을 사용하는 모든 디바이스에 대한 행을 표시합니다.

공유 ASA 네트워크 정책

CDO(Cisco Defense Orchestrator)는 여러 ASA에서 사용하는 동일한 네트워크 정책을 찾아 네트워크 정책 페이지에서 식별합니다. 공유 네트워크 정책이 있는 경우 정책을 한 번 변경하고 공유되는 다른 디바이스에 변경 사항을 배포할 수 있습니다. 이렇게 하면 디바이스 간에 네트워크 정책이 일관되게 유지됩니다.

공유 네트워크 정책 속성

네트워크 정책 테이블은 네트워크 정책을 사용하는 디바이스 수를 식별합니다. 둘 이상의 디바이스에서 사용 중임을 나타내는 모든 네트워크 정책은 공유 정책입니다. 공유 네트워크 정책 찾기:

단계 1 **Policies**(정책) > **ASA Policies**(정책)을 탐색합니다.

단계 2 페이지에서 이전 필터링 또는 검색 기준을 지우려면 필터 창에서 **Show All**(모두 표시)을 클릭합니다.

단계 3 필터 표시줄에서 **Shared Policies**(공유 정책)를 확장하고 **Shared**(공유)를 선택합니다.

단계 4 검색을 더욱 구체화하려면 검색 창에 키워드를 입력합니다.

단계 5 네트워크 정책 테이블에서 공유 네트워크 정책을 선택합니다.



Note

필터 및 검색 기준은 조합하여 사용되지 않으며 한번에 하나만 사용할 수 있습니다. 예를 들어 "Shared Policies(공유 정책)"로 필터링하면 모든 공유 정책이 표시됩니다. 디바이스 이름을 검색에 추가하면 정책 공유 여부와 상관없이 해당 디바이스 이름에서 사용하는 모든 네트워크 정책이 표시됩니다.

공유 네트워크 정책 편집

단계 1 편집할 **공유 ASA 네트워크 정책**.

단계 2 공유 정책을 선택합니다. CDO는 CDO에서 관리하는 디바이스가 해당 네트워크 정책을 사용하는지 식별합니다.

단계 3 세부 정보 창에서 **Edit Policy**(정책 편집)을 클릭합니다.

단계 4 정책에서 규칙을 수정합니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 변경의 영향을 받을 디바이스를 확인합니다.

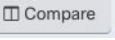
단계 7 **Devices & Service**(디바이스 및 서비스) 페이지를 열고 디바이스가 더 이상 동기화되지 않는지 확인합니다.

단계 8 **Deploy Changes Manually**(수동으로 변경 사항 구축)...를 클릭하고 표시되는 지침에 따라 ASA에 저장된 구성을 변경 사항으로 업데이트합니다.

공유 네트워크 정책 비교

공유 네트워크 정책을 비교하는 목적은 약간 분기된 정책을 찾아 재정렬하는 것입니다. 거의 동일한 정책이 여러 개 있는 경우, 해당 정책이 분기되어 실제로는 동일해야 합니다. 네트워크 정책을 재정렬하면 CDO가 정책을 공유된 것으로 인식하며, 정책을 변경하면 해당 정책을 사용하여 다른 디바이스에 변경 사항을 배포할 수 있습니다.

단계 1 비교할 공유 ASA 네트워크 정책.

단계 2 비교  를 클릭합니다.

단계 3 비교할 두 네트워크 정책을 선택하고 **View Comparison**(비교 보기)을 클릭합니다.

단계 4 차이점을 확인하고 **Done Comparing**(비교 완료)을 클릭합니다.

단계 5 정책 중 하나를 변경하여 다른 정책과 일치시키려면 네트워크 정책 테이블에서 해당 정책을 선택하고 세부 정보 창에서 **Edit Policy**(정책 편집)를 클릭하여 수정합니다.

ASA 정책(확장 액세스 목록)

CDO(Cisco Defense Orchestrator)는 사용자에게 모든 디바이스에서 네트워크 및 애플리케이션 보안 정책을 일관되게 유지할 수 있는 기능을 제공합니다. 이 고유한 기능을 사용하면 여러 디바이스에서 동시에 정책을 간단하고 쉽게 변경할 수 있습니다.

ACE(액세스 제어 항목)

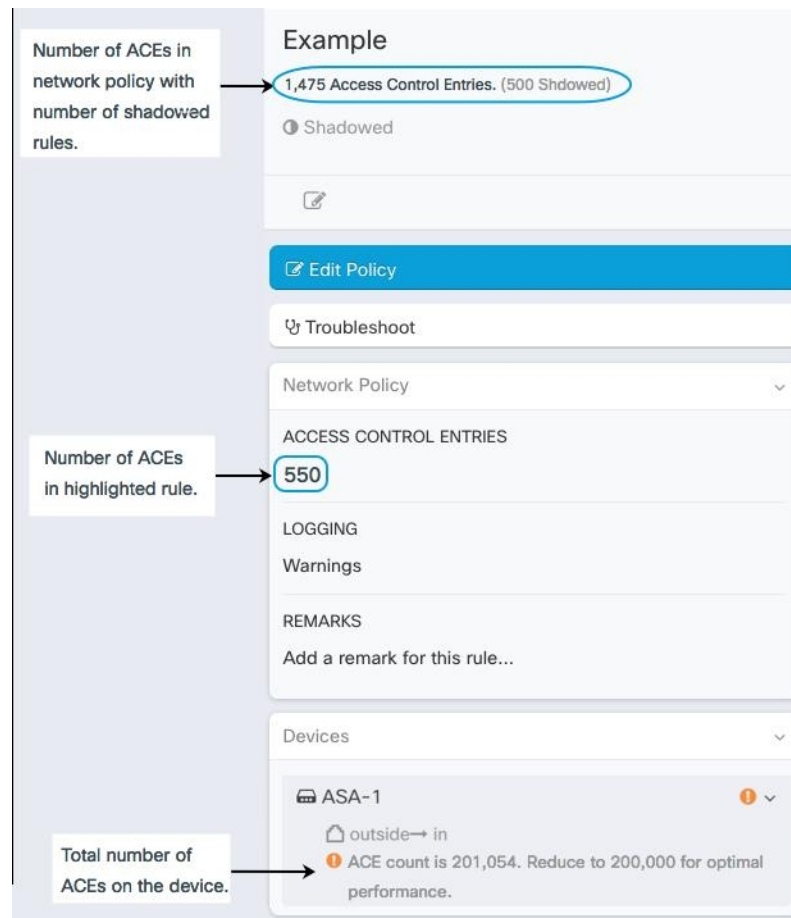
볼 수 있는 항목과 볼 수 없는 항목의 관점에서 액세스 제어 항목에 대해 생각해 보십시오.

여러분은 다음과 같은 것을 볼 수 있습니다. CDO의 사용자 인터페이스 측면에서 네트워크 정책에 추가하는 규칙은 ASA의 액세스 제어 항목입니다. 이 규칙은 소스와 대상 주소 또는 한 주소 그룹과 다른 주소 그룹 간에 허용되는 네트워크 트래픽을 정의합니다.

여러분은 다음과 같은 것을 볼 수 없습니다. ASA는 네트워크 규칙이 암시하는 소스 IP 주소와 대상 IP 주소의 가능한 모든 조합을 설명하기 위해 생성한 네트워크 규칙을 확장합니다. 예를 들어 한 네트워크 개체에 있는 3개의 IP 주소가 다른 개체에 있는 3개의 IP 주소에 액세스하는 것이 거부되는 규칙이 있는 경우 ASA가 메모리에 저장하는 가능한 액세스 제어 항목은 9개입니다.

ASA에서 처리할 수 있는 ACE 수에는 하드 코딩된 제한이 없지만 ACE 수가 너무 많으면 ASA 성능이 저하됩니다. 표 4를 참조하십시오. 특정 ASA 디바이스에 대해 예상되는 최대 ACE 항목 수에 대한 [적응형 보안 어플라이언스 FAQ](#)에서 "Cisco ASA 모델에 대한 최대 액세스 제어 항목".

CDO는 모든 네트워크 정책에서 파생된 총 ACE 수를 유지하고 해당 ACE 수가 어플라이언스에서 예상되는 최대 ACE 제한을 초과할 때 알려줍니다. CDO가 제공하는 정보는 다음과 같습니다.



디바이스의 ACE 수 줄이기

다음은 예상되는 최대 ACE 수를 초과한 디바이스에서 ACE 수를 줄이는 몇 가지 방법입니다.

- 부분적으로 그리고 완전히 **새도우 규칙** 규칙이 있는 정책을 찾습니다. 적절한 경우 이러한 규칙을 삭제하십시오.
- **적중 횟수가 0인 디바이스의 모든 네트워크 정책 찾기** 적중률이 0인 **네트워크 정책의 규칙이 적중되는 빈도 찾기** 적절한 경우 히트가 0인 정책 또는 규칙을 삭제합니다.
- 액세스 제어 항목의 예상 수를 초과한 **ASA 네트워크 정책 및 규칙 검색 및 필터링** 해당 정책을 검토합니다. 해당 정책의 소스 및 대상 주소가 원래 계획한 만큼 광범위해야 하는지 고려하십시오.

ASA 글로벌 액세스 정책 구성

전역 액세스 정책은 ASA의 모든 인터페이스에 적용되는 네트워크 정책입니다. 이러한 정책은 인바운드 네트워크 트래픽에만 적용됩니다. 규칙 집합을 모든 ASA 인터페이스에 균일하게 적용하려면 전역 액세스 정책을 생성합니다.

ASA에는 하나의 전역 액세스 정책만 구성할 수 있습니다. 다른 정책과 마찬가지로 전역 액세스 정책에 둘 이상의 규칙이 할당될 수 있습니다.

ASA 전역 액세스 정책은 특정 인터페이스에 대한 네트워크 정책 이후, 그리고 모든 트래픽에 대한 암시적 거부 규칙 이전에 처리됩니다. ASA에서 규칙을 처리하는 순서는 다음과 같습니다.

1. 인터페이스 액세스 규칙.
2. 브리지 그룹 멤버 인터페이스의 경우, BVI(Bridge Virtual Interface) 액세스 규칙입니다.
3. 전역 액세스 규칙
4. 암시적 거부

ASA 글로벌 액세스 정책 구성에 대한 제한 사항

CDO를 사용하면 ASA에 대한 전역 액세스 정책을 생성하고 수정할 수 있습니다. 그러나 CDO에 온보딩할 때 ASA에 전역 액세스 정책이 있었다면 다음과 같은 제한 사항이 적용됩니다.

- 정책을 수정할 수는 있지만 디바이스당 하나의 전역 액세스 정책만 허용되므로 새 정책을 생성할 수는 없습니다.
- ASA의 전역 액세스 정책에 CDO가 지원하지 않는 규칙이 포함된 경우 정책을 수정할 수 없습니다.
- CLI 인터페이스를 사용하거나 디바이스 구성 파일을 수정하는 방법으로만 정책을 삭제할 수 있습니다.

글로벌 액세스 정책 생성

단계 1 **Policies(정책) > ASA Policies(ASA 정책)**를 클릭합니다.

단계 2 필터 패널에서 정책 목록을 필터링하여 전역 정책을 추가할 디바이스를 찾습니다.

단계 3 **Network Policies(네트워크 정책)** 테이블의 **Interfaces(인터페이스)** 열에 "global(전역)"이라는 레이블이 붙은 정책이 없는지 확인합니다.

단계 4 **Create Policy(정책 생성)**를 클릭합니다.

단계 5 **Device(디바이스)** 버튼을 클릭하고 전역 정책을 추가할 ASA를 선택합니다. **Select(선택)**를 클릭합니다.

단계 6 정책에 이름을 지정하고 **Create as global policy(전역 정책으로 생성)**를 선택합니다. 정책에 대한 인터페이스나 방향을 선택할 수 없음을 알 수 있습니다. 전역 정책은 항상 디바이스의 모든 인터페이스에 할당되며 항상 인바운드 트래픽을 평가합니다.

단계 7 **Save**(저장)를 클릭합니다.

단계 8 새 정책에 규칙을 추가하려면 [ASA 네트워크 정책 편집](#)을 사용합니다.

글로벌 액세스 정책 편집

위에서 설명한 구성 제한 사항을 염두에 두고 [ASA 네트워크 정책 편집](#)를 사용하여 전역 액세스 정책을 편집합니다.



Note Edit Policy(정책 편집) 버튼이 비활성화되어 글로벌 정책을 편집할 수 없다면, 정책이 ASA에서 생성되었고 CDO에서 지원하지 않는 개체가 포함된 규칙이 포함되어 있기 때문일 수 있습니다. 이러한 규칙은 전역 액세스 정책 테이블에서 볼 수 없습니다. 이 경우 CDO의 CLI 툴을 사용하여 구성 파일을 편집하거나 CDO를 사용하여 ASA의 구성 파일을 편집하거나 ASA에서 직접 전역 정책을 편집해야 합니다.

다른 디바이스에 전역 액세스 정책 복사

[ASA 네트워크 정책 복사](#)를 사용하여 한 디바이스에서 다른 디바이스로 전역 액세스 정책을 복사하거나 한 디바이스에서 다른 디바이스의 단일 인터페이스로 전역 액세스 정책을 복사합니다.

전역 액세스 정책 삭제

CDO의 사용자 인터페이스를 사용하여 전역 액세스 정책을 삭제할 수 없습니다. 전역 액세스 정책을 삭제하려면 CDO의 CLI 툴을 사용하거나 CDO를 사용하여 ASA의 구성 파일을 편집하거나 ASA에서 직접 전역 액세스 정책을 편집하여 명령줄에서 전역 액세스 정책을 삭제해야 합니다.

적중률

CDO를 사용하면 클라우드의 단일 창에서 보다 정확한 정책 분석 및 근본 원인에 대한 즉각적인 조치 가능한 피벗을 위한 간단한 시각화를 제공하여 정책 규칙의 결과를 평가할 수 있습니다. 적중률 기능을 사용하면 다음을 수행할 수 있습니다.

- 보안 상태를 증가하는 사용되지 않는 정책 규칙을 제거합니다.
- 병목 현상을 즉시 식별하여 방화벽 성능을 최적화하고 정확하고 효율적인 우선순위를 적용합니다(예: 가장 많이 트리거되는 정책 규칙이 우선순위가 높음).
- 구성된 데이터 보존 기간(1년)에 대한 디바이스 또는 정책 규칙 재설정 시에도 적중률 기록 정보 유지
- 실행 가능한 정보를 기반으로 의심스러운 새도우 및 사용되지 않는 규칙에 대한 검증을 강화합니다. 업데이트 또는 삭제에 대한 의심 제거

- 사전 정의된 시간 간격(일, 주, 월, 연도) 및 실제 적용 횟수(0, >100, >100k 등)를 활용하여 전체 정책에 대한 컨텍스트에서 정책 규칙 사용을 시각화하여 네트워크를 통과하는 패킷에 대한 영향을 평가합니다.

ASA 정책의 적용률 보기

단계 1 CDO 메뉴 모음에서 **Policies(정책)** > **ASA Access Policies(ASA 액세스 정책)**를 선택합니다.

단계 2 필터 아이콘을 클릭하고 필터를 열린 상태로 고정합니다.

단계 3 Hits(적중) 영역에서 다양한 적용 횟수 필터를 클릭하여 다른 정책보다 적용 빈도가 높거나 낮은 정책을 표시합니다.


네트워크 정책 규칙 내보내기

각 Access-Group 또는 Crypto-Map의 콘텐츠를 .csv 파일로 내보낼 수 있습니다. 이 .csv는 각 ACL(Access Control List) 및 CDO가 각 ACL에 대해 보유한 데이터를 표시합니다.

단계 1 탐색 창에서 **Policies(정책)** > **ASA Policies(ASA 정책)**를 클릭합니다.

단계 2 (선택 사항) **ASA 네트워크 정책 및 규칙 검색 및 필터링**를 사용하여 결과를 필터링합니다.

단계 3 결과에서 네트워크 정책을 선택합니다.

단계 4 **Export to CSV(CSV로 내보내기)**  를 클릭합니다.

단계 5 CDO는 화면에 표시되는 규칙을 .csv 파일로 내보냅니다.

디바이스에 ASA 정책 변경 사항 적용

CDO(Cisco Defense Orchestrator)에서 보안 정책을 수정하면 영향을 받는 디바이스 또는 서비스에 변경 사항이 적용됩니다. 그 결과 구성이 동기화되지 않습니다. 현재 동기화되지 않은 모든 디바이스 또는 서비스에서 **Deploy to Device...(디바이스에 구축...)**를 클릭하여 정책 변경 사항을 검토하고 적용할 수 있습니다.

스크립트로 디바이스에 구축

ASA 디바이스 정책 구성 변경이 완료되면 변경 사항을 검토하고 디바이스에 적용해야 합니다.

단계 1 **Devices(디바이스)** 탭으로 이동하여 **Devices(디바이스)** 탭을 클릭합니다.

- 단계 2 적절한 디바이스 유형 탭을 클릭하고 테이블에서 수정된 디바이스를 선택합니다. 구성 상태가 **Not Synced**(동기화되지 않음)로 표시되어야 하며, 이는 디바이스에 아직 적용되지 않은 변경 사항이 있음을 나타냅니다.
- 단계 3 오른쪽 사이드바에서 **Sync**(동기화)를 클릭하여 디바이스에 적용할 명령을 생성하여 CDO 구성과 동기화된 상태로 전환합니다.
- 단계 4 메시지가 표시되면 **Download Commands**(명령 다운로드)를 클릭하여 명령의 복사본을 로컬로 다운로드합니다. 이러한 명령은 텍스트 파일에 포함되며 적용하기 전에 검토할 수 있습니다. 원하는 경우 변경 사항을 되돌리는 명령도 생성됩니다.
- 단계 5 CDO 외부에서 표준 프로토콜을 사용하여 디바이스에 로그인하고 다운로드한 명령을 적용합니다.
- 단계 6 모든 명령을 입력한 후 CDO로 돌아가서 **Devices**(디바이스) 탭에서 수정된 디바이스를 다시 선택합니다.
- 단계 7 **Refresh**(새로 고침)를 클릭하여 CDO와의 동기화를 확인합니다.

명령의 하위 집합이 실행되었거나 추가 명령이 대역 외에서 실행된 경우 CDO는 차이점을 표시하는 창을 열고 사용자에게 *Conflict Detected*(충돌 감지됨)라는 업데이트된 상태를 제공하여 차이점을 나타냅니다.

ASA 정책의 보안 그룹 태그

액세스 제어 규칙에서 보안 그룹 개체 그룹(이후 "SGT 그룹"이라고 함)의 보안 그룹 태그를 사용하는 ASA를 온보딩하는 경우 Cisco Defense Orchestrator를 사용하여 SGT 그룹을 사용하는 규칙을 편집하고 해당 규칙이 있는 정책을 관리할 수 있습니다. 그러나 CDO GUI를 사용하여 SGT 그룹을 생성하거나 편집할 수는 없습니다. SGT 그룹을 생성하거나 수정하려면 ASA의 ASDM(Adaptive Security Device Manager) 또는 CDO에서 사용 가능한 명령줄 인터페이스를 사용해야 합니다.

CDO의 개체 페이지에서 SGT 그룹의 세부 정보를 읽을 때 해당 개체가 편집 불가능한 시스템 제공 개체로 식별되는 것을 확인할 수 있습니다.

CDO 관리자는 SGT 그룹을 포함하는 ACL 및 ASA 정책에서 다음 작업을 수행할 수 있습니다.

- CDO 관리자는 소스 및 대상 보안 그룹을 제외한 ACL의 모든 측면을 편집할 수 있습니다.
- 한 ASA에서 다른 ASA로 SGT 그룹을 포함하는 정책을 복사합니다.

명령줄 인터페이스를 사용하여 Cisco TrustSec을 구성하는 방법에 대한 자세한 지침은 해당 ASA 릴리스의 [ASA CLI 제2권: Cisco ASA Series 방화벽 CLI 구성 가이드](#)의 "ASA 및 Cisco TrustSec" 장을 참조하십시오.

새도우 규칙

새도우 규칙이 있는 네트워크 정책은 정책에 있는 하나 이상의 규칙이 선행하는 규칙이 새도우 규칙에 의해 패킷이 평가되는 것을 방지하기 때문에 절대 트리거되지 않는 정책입니다.

예를 들어 "예제" 네트워크 정책에서 다음과 같은 네트워크 개체 및 네트워크 규칙을 고려하십시오.

```
object network 02-50
range 10.10.10.2 10.10.10.50
```

```
object network 02-100
range 10.10.10.2 10.10.10.100

access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

이 규칙에 의해 트래픽이 평가되지 않습니다.

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

이전 규칙 때문에,

```
access-list example extended deny ip any4 object 02-50
```

ipv4 주소가 **10.10.10.2 - 10.10.10.50** 범위의 주소에 도달하는 것을 거부합니다.

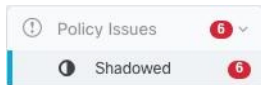
새도우 규칙이 있는 네트워크 정책 찾기

새도우 규칙이 있는 네트워크 정책을 찾으려면 네트워크 정책 필터를 사용합니다.

단계 1 탐색 창에서 **Policies(정책) > ASA Policies(ASA 정책)**를 클릭합니다.

단계 2 ASA Access Policies(ASA 액세스 정책) 테이블 상단에 있는 필터 아이콘을 클릭합니다.

단계 3 정책 문제 필터에서 **Shadowed(새도우)**를 선택하여 새도우 규칙이 있는 모든 정책을 확인합니다.



새도우 규칙 문제 해결

위의 "예제" 네트워크 정책에 설명된 규칙은 다음과 같이 표시됩니다.

LINE	ACTION	PROTOCOL	SOURCE	PORT	DESTINATION	PORT	HITS (DAY)
1	Deny	ip	any4	any	02-50	any	0000
2	Permit	ip	10.10.10.35	any	02-50	any	0000
3	Permit	ip	any4	any	02-100	any	0000

1행의 규칙은 정책의 다른 규칙을 새도우하므로 새도우 경고 배지 ▲로 표시됩니다. 2행의 규칙은 정책의 다른 규칙에 의해 새도우된 ●로 표시됩니다. 2행의 규칙에 대한 작업은 정책의 다른 규칙에 의해 새도우되어 있으므로 회색으로 표시됩니다. CDO는 정책의 어떤 규칙이 2행의 규칙을 새도우하는지 알려줄 수 있습니다.

라인 3의 규칙은 일부 시간에만 트리거될 수 있습니다. 이것은 부분적으로 새도우 규칙입니다.

10.10.10.2-10.10.10.50 범위의 IP 주소에 도달하려는 모든 IPv4 주소의 네트워크 트래픽은 첫 번째 규

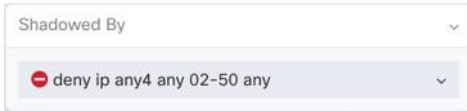
칙에 의해 이미 거부되었기 때문에 평가되지 않습니다. 그러나 10.10.10.51-10.10.10.100 범위의 주소에 도달하려는 모든 IPv4 주소는 마지막 규칙에 의해 평가되고 허용됩니다.



Caution CDO는 부분적으로 음영 처리된 규칙에 새도우 경고 배지 ▲를 적용하지 않습니다.

단계 1 정책에서 새도우 규칙을 선택합니다. 위의 예에서는 줄 2를 클릭하는 것을 의미합니다.

단계 2 규칙 세부 정보 창에서 **Shadowed By** 영역을 찾습니다. 이 예에서 2행의 규칙에 대한 **Shadowed By** 영역은 1행의 규칙에 의해 새도우 처리되고 있음을 보여줍니다.



단계 3 새도우 처리 중인 규칙을 검토합니다. 너무 광범위합니까? 새도우 처리된 규칙을 검토합니다. 정말로 필요하십니까? 새도우 처리 중인 규칙을 수정하거나 새도우 처리된 규칙을 삭제합니다.

Note 새도우 규칙을 삭제하면 ASA의 ACE(Access Control Entry) 수가 줄어듭니다. 이렇게 하면 다른 ACE를 사용하여 다른 규칙을 생성할 수 있는 공간이 확보됩니다. CDO는 네트워크 정책의 모든 규칙에서 파생된 ACE 수를 계산하고 네트워크 정책 세부 정보 창 상단에 총계를 표시합니다. 네트워크 정책의 규칙 중 새도우 규칙이 있으면 해당 번호도 나열됩니다.

Example

22 Access Control Entries (7 Shadowed)

● Shadowed

또한 CDO는 네트워크 정책의 단일 규칙에서 파생된 ACE의 수를 표시하고 네트워크 정책 세부 정보 창에 해당 정보를 표시합니다. 다음은 해당 목록의 예입니다.



단계 4 네트워크 정책 세부 정보 창의 **Devices**(디바이스) 영역에서 정책을 사용하는 디바이스를 확인합니다.

단계 5 **Devices & Service**(디바이스 및 서비스) 페이지를 열고 정책 변경의 영향을 받는 디바이스에 다시 변경사항을 배포합니다.

네트워크 주소 변환

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.

Cisco Defense Orchestrator를 사용하여 다양한 활용 사례에 대한 NAT 규칙을 생성할 수 있습니다. NAT 규칙 마법사 또는 다음 항목을 사용하여 다른 NAT 규칙을 생성합니다.

NAT 규칙 처리 순서

네트워크 개체 NAT 규칙과 2회 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 일치 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

Table 13: NAT 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	2회 NAT(ASA) 수동 NAT(FTD)	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 2회 NAT 규칙은 섹션 1에 추가됩니다.

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 2	네트워크 개체 NAT(ASA) 자동 NAT(FTD)	<p>섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다.</p> <ol style="list-style-type: none"> 고정 규칙 동적 규칙 <p>각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다.</p> <ol style="list-style-type: none"> 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다. 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다. IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들어 "Arlington" 개체는 "Detroit" 개체보다 먼저 평가됩니다.
섹션 3	2회 NAT(ASA) 수동 NAT(FTD)	<p>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.</p>

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 Detroit)
- 172.16.1.0/24(동적)(개체 Arlington)

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 Arlington)
- 172.16.1.0/24(동적) (개체 Detroit)
- 192.168.1.0/24(동적)

네트워크 주소 변환 마법사

NAT(Network Address Translation) 마법사는 다음 유형의 액세스에 대해 디바이스에서 NAT 규칙을 만드는 데 도움이 됩니다.

- 내부 사용자의 인터넷 액세스를 활성화합니다. 이 NAT 규칙을 사용하여 내부 네트워크의 사용자가 인터넷에 연결할 수 있습니다.
- 내부 서버를 인터넷에 노출합니다. 이 NAT 규칙을 사용하여 네트워크 외부의 사람들이 내부 웹 또는 이메일 서버에 도달하도록 허용할 수 있습니다.

"내부 사용자를 위한 인터넷 액세스 활성화"의 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 특정 사용자만 인터넷에 연결할 수 있도록 하려면 해당 사용자의 서브넷 주소가 필요합니다.

"내부 서버를 인터넷에 노출"하기 위한 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 인터넷 연결 IP 주소로 변환하려는 네트워크 내부 서버의 IP 주소입니다.
- 서버에서 사용할 공용 IP 주소입니다.

다음 작업

NAT 마법사를 사용하여 NAT 규칙 생성, on page 87의 내용을 참조하십시오.

NAT 마법사를 사용하여 NAT 규칙 생성

Before you begin

NAT 마법사를 사용하여 NAT 규칙을 만드는 데 필요한 사전 요구 사항은 [네트워크 주소 변환 마법사](#), on page 86를 참조하십시오.

단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 **filter**(필터) 및 **search**(검색) 필드를 사용하여 NAT 규칙을 생성하려는 디바이스를 찾으십시오.

단계 5 상세정보 패널의 **Management**(관리) 영역에서 **NAT** > **NAT**를 클릭합니다.

단계 6  > **NAT Wizard**(NAT 마법사)를 클릭합니다.

단계 7 NAT 마법사 질문에 응답하고 화면의 지시를 따르십시오.

- NAT 마법사는 **네트워크 개체**를 사용하여 규칙을 생성합니다. 드롭다운 메뉴에서 기존 개체를 선택하거나 만지기 버튼 **+ Create...**를 사용하여 새 개체를 생성합니다.
- NAT 규칙을 저장하려면 먼저 모든 IP 주소를 네트워크 개체로 정의해야 합니다.

단계 8 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

NAT의 일반적인 사용 사례

2회 NAT 및 수동 NAT

다음은 "자동 NAT"라고도 하는 "네트워크 개체 NAT"를 사용하여 수행할 수 있는 몇 가지 일반적인 작업입니다.

- **공용 IP** 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화, 88 페이지
- 내부 네트워크의 사용자가 외부 인터페이스의 **공용 IP** 주소를 사용하여 인터넷에 액세스하도록 활성화, 89 페이지
- **공용 IP** 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정, 90 페이지
- **사설 IP** 주소 범위를 **공용 IP** 주소 범위로 변환, 94 페이지

네트워크 개체 및 NAT자동 NAT

다음은 "수동 NAT"라고도 하는 "Twice NAT"를 사용하여 수행할 수 있는 일반적인 작업입니다.

- 외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지, 96 페이지

공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화

활용 사례


인터넷에서 액세스해야 하는 사설 IP 주소가 있는 서버가 있고 사설 IP 주소에 대해 하나의 공용 IP 주소를 NAT하기에 충분한 공용 IP 주소가 있는 경우 이 NAT 전략을 사용합니다. 공용 IP 주소가 제한된 경우 **공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정**를 참조하세요 (해당 솔루션이 더 적합할 수 있음).

전략

서버에는 정적 사설 IP 주소가 있으며 네트워크 외부의 사용자는 서버에 연결할 수 있어야 합니다. 고정 사설 IP 주소를 고정 공용 IP 주소로 변환하는 네트워크 개체 NAT 규칙을 생성합니다. 그런 다음 해당 공용 IP 주소에서 사설 IP 주소에 도달하는 트래픽을 허용하는 액세스 정책을 생성합니다. 마지막으로 이러한 변경 사항을 디바이스에 배포합니다.

Before you begin

시작하기 전에 두 개의 네트워크 개체를 생성합니다. 하나의 개체는 *servername_inside*로 이름을 지정하고 다른 개체는 *servername_outside*로 이름을 지정합니다. *servername_inside* 네트워크 개체는 서버의 사설 IP 주소를 포함해야 합니다. *servername_outside* 네트워크 개체에는 서버의 공용 IP 주소가 포함되어야 합니다. 지침은 **네트워크 개체 생성**을 참조하십시오.

-
- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
- 원본 주소 메뉴를 확장하고 **Choose**(선택)을 클릭한 다음 **servername_inside** 개체를 선택합니다.
 - 변환된 주소 메뉴를 확장하고 **Choose**(선택)을 클릭한 다음 **servername_outside** 개체를 선택합니다.
- 단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.

- 단계 11 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다.
- 단계 13 ASA의 경우 네트워크 정책 규칙을 배포하거나 기다렸다가, FDM 관리 디바이스의 경우 액세스 제어 정책 규칙을 배포하여 트래픽이 *servername_inside*에서 *servername_outside*로 흐를 수 있도록 합니다.
- 단계 14 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.



Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

이 절차에 의해 생성된 **NAT** 규칙

```
object network servername_inside
nat (inside,outside) static servername_outside
```

내부 네트워크의 사용자가 외부 인터페이스의 공용 IP 주소를 사용하여 인터넷에 액세스하도록 활성화

활용 사례

외부 인터페이스의 공용 주소를 공유하여 개인 네트워크의 사용자와 컴퓨터가 인터넷에 연결할 수 있도록 합니다.

전략

사실 네트워크의 모든 사용자가 디바이스의 외부 인터페이스 공용 IP 주소를 공유할 수 있도록 허용하는 포트 주소 변환(PAT) 규칙을 생성합니다.

사실 주소가 공용 주소 및 포트 번호에 매핑된 후 디바이스는 해당 매핑을 기록합니다. 해당 공용 IP 주소 및 포트에 향하는 들어오는 트래픽이 수신되면 디바이스는 이를 요청한 사실 IP 주소로 다시 보냅니다.

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 5 오른쪽의 **Management(관리)** 창에서 **NAT**를 클릭합니다.

단계 6  > **Network Object NAT**를 클릭합니다.

단계 7 섹션 1, 유형 에서 **Dynamic(동적)**을 선택합니다. **Continue(계속)**를 클릭합니다.

단계 8 섹션 2, 인터페이스에서, 소스 인터페이스로 **any(아무거나)**를 선택하고 대상 인터페이스로 **outside(외부)**를 선택합니다. **Continue(계속)**를 클릭합니다.

단계 9 섹션 3, **Packets(패킷)**에서, 다음 작업을 수행합니다.

- a. 원래 주소 메뉴를 확장하고, **Choose(선택)**을 클릭한 다음 네트워크 구성에 따라 **any-ipv4** 또는 **any-ipv6** 개체를 선택합니다.
- b. 변환된 주소 메뉴를 확장하고 사용 가능한 목록에서 인터페이스를 선택합니다. 인터페이스는 외부 인터페이스의 공용 주소를 사용하도록 나타냅니다.

단계 10 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙의 이름을 입력합니다.

단계 11 **Save(저장)**를 클릭합니다.

단계 12 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한번에 구축합니다.

ASA의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.



Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

이 절차에 의해 생성된 **NAT** 규칙

```
object network any_network
nat (any,outside) dynamic interface
```

공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정


활용 사례

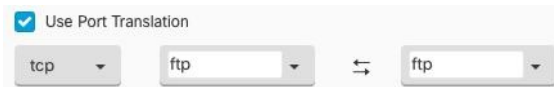
공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

사전 요구 사항

시작하기 전에 FTP, HTTP 및 SMTP 서버에 각각 하나씩 세 개의 개별 네트워크 개체를 생성합니다. 다음 절차를 위해 이러한 개체를 **ftp-server-object**, **http-server-object** 및 **smtp-server-object**라고 합니다. 지침은 [네트워크 개체 생성](#)을 참조하십시오.

FTP 서버에 대한 NAT 수신 FTP 트래픽

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
 - 원본 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **ftp-server-object**를 선택합니다.
 - 변환된 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **Interface**(인터페이스)를 선택합니다.
 - **Use Port Translation**(포트 변환 사용)을 선택합니다.
 - **tcp, ftp, ftp**를 선택합니다.



- 단계 10 섹션 4, **Advanced**(고급)을 건너뛵니다.
- 단계 11 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다. NAT 테이블의 **NAT 규칙 처리 순서**에 새 규칙이 생성됩니다.
- 단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한번에 배포합니다.

ASA의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.



Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network ftp-object
host 10.1.2.27
```

이 절차에 의해 생성된 **NAT** 규칙


```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

HTTP 서버에 대한 NAT 수신 HTTP 트래픽

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

Before you begin

시작하기 전에 http 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는 개체를 **http-object**라고 합니다. 지침은 [네트워크 개체 생성](#)을 참조하십시오.

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
 - 원본 주소 메뉴를 확장하고 **Choose**(선택)을 클릭한 다음 **http-object**를 선택합니다.
 - 변환된 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **Interface**(인터페이스)를 선택합니다.
 - **Use Port Translation**(포트 변환 사용)을 선택합니다.
 - **tcp**, **http**, **http**를 선택합니다.



- 단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.
- 단계 11 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다. NAT 테이블의 **NAT 규칙 처리 순서**에 새 규칙이 생성됩니다.
- 단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

ASA의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.



Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network http-object
host 10.1.2.28
```

이 절차에 의해 생성된 **NAT** 규칙


```
object network http-object
nat (inside,outside) static interface service tcp www www
```

SMTP 서버에 대한 NAT 수신 SMTP 트래픽

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

Before you begin

시작하기 전에 smtp 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는 개체를 **smtp-개체**라고 합니다. 지침은 [네트워크 개체 생성](#)을 참조하십시오.

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.

단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.

- 원본 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 smtp-server-object를 선택합니다.
- 변환된 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **Interface**(인터페이스)를 선택합니다.
- **Use Port Translation**(포트 변환 사용)을 선택합니다.
- **tcp, smtp, smtp**를 선택합니다.



단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.

단계 11 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 12 **Save**(저장)를 클릭합니다. NAT 테이블의 **NAT 규칙 처리 순서**에 새 규칙이 생성됩니다.

단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

ASA의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.



Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network smtp-object
host 10.1.2.29
```

이 절차에 의해 생성된 **NAT** 규칙

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

사설 IP 주소 범위를 공용 IP 주소 범위로 변환

활용 사례

수신 디바이스(트랜잭션의 다른 끝에 있는 디바이스)가 트래픽을 허용하도록 IP 주소를 특정 범위로 변환해야 하는 특정 디바이스 유형 또는 사용자 유형 그룹이 있는 경우 이 접근 방식을 사용합니다.

내부 주소 풀을 외부 주소 풀로 변환

Before you begin

변환하려는 사설 IP 주소 풀에 대한 네트워크 개체를 생성하고 해당 사설 IP 주소를 변환하려는 공용 주소 풀에 대한 네트워크 개체를 생성합니다.


ASA의 경우 "원래 주소" 풀(변환하려는 개인 IP 주소 풀)은 주소 범위가 있는 네트워크 개체, 서브넷을 정의하는 네트워크 개체 또는 풀의 모든 주소를 포함하는 네트워크 그룹일 수 있습니다. FTD의 경우 "원래 주소" 풀은 풀의 모든 주소를 포함하는 네트워크 그룹 또는 서브넷을 정의하는 네트워크 개체일 수 있습니다.



Note ASA의 경우 "변환된 주소" 풀을 정의하는 네트워크 그룹은 서브넷을 정의하는 네트워크 개체일 수 없습니다.

이러한 주소 풀을 생성할 때 지침을 보려면 [ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집](#)을 사용하고 하십시오.

다음 절차를 위해 개인 주소 풀의 이름을 **inside_pool**로 지정하고 공용 주소 풀의 이름을 **outside_pool**로 지정했습니다.

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1 **Type**(유형)에서 **Dynamic**(동적)을 선택하고 **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, 인터페이스에서 소스 인터페이스를 내부로, 대상 인터페이스를 외부로 설정합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
 - 원본 주소의 경우 **Choose**(선택)을 클릭한 다음 위의 전제 조건 섹션에서 만든 **inside_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.
 - 변환된 주소의 경우 **Choose**(선택)을 클릭한 다음 위의 전제 조건 섹션에서 만든 **outside_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.
- 단계 10 섹션 4, **Advanced**(고급)을 건너뛸니다.
- 단계 11 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다.

단계 13 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA의 저장된 구성 파일 항목

이러한 절차의 결과로 ASA의 저장된 구성 파일에 나타나는 항목입니다.



Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network outside_pool
  range 209.165.1.1 209.165.1.255
object network inside_pool
  range 10.1.1.1 10.1.1.255
```

이 절차에 의해 생성된 NAT 규칙

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지

활용 사례

이 Twice NAT 사용 사례를 사용하여 사이트 투 사이트 VPN을 활성화합니다.

전략

네트워크의 한 위치에 있는 IP 주소가 다른 위치에 변경되지 않고 도착하도록 IP 주소 풀을 자체적으로 변환하고 있습니다.

2회 NAT 규칙 생성


Before you begin

변환할 IP 주소 풀을 정의하는 네트워크 개체 또는 네트워크 그룹을 생성합니다. ASA의 경우 주소 범위는 IP 주소 범위를 사용하는 네트워크 개체, 서브넷을 정의하는 네트워크 개체 또는 범위의 모든 주소를 포함하는 네트워크 그룹 개체로 정의할 수 있습니다.

네트워크 개체 또는 네트워크 그룹을 생성할 때 지침을 보려면 [ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집](#) 을 사용합니다.

다음 절차를 위해 네트워크 개체 또는 네트워크 그룹인 Site-to-Site-PC-Pool을 호출합니다.

단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Twice NAT**(2회 NAT)를 클릭합니다..
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, 패킷에서 다음과 같이 변경합니다.
- 원래 주소 메뉴를 확장하고 **Choose**(선택)를 클릭한 다음 전제 조건 섹션에서 생성한 사이트 투 사이트 PC 풀 개체를 선택합니다.
 - 변환된 주소 메뉴를 펼치고 **Choose**(선택)를 클릭한 후 전제 조건 섹션에서 생성한 Site-to-Site-PC-Pool 개체를 선택합니다.
- 단계 10 섹션 4, **Advanced**(고급)을 건너뛵니다.
- 단계 11 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다.
- 단계 13 ASA의 경우 암호화 맵을 생성합니다. 암호화 맵 생성에 대한 자세한 내용은 [CLI 책 3: Cisco ASA Series VPN CLI 구성 가이드](#)를 참조하고 LAN-to-LAN IPsec VPN에 대한 장을 검토하십시오.
- 단계 14 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한번에 배포합니다.

ASA의 저장된 구성 파일 항목

이러한 절차의 결과로 ASA의 저장된 구성 파일에 나타나는 항목입니다.



Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

이 절차에 의해 생성된 **NAT** 규칙

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

CDO에서 가상 프라이빗 네트워크 관리

VPN(Virtual Private Network)은 인터넷과 같은 공용 네트워크를 통해 엔드포인트 간에 보안 터널을 설정합니다.

이 섹션은 ASA(Adaptive Security Appliance) 디바이스의 원격 액세스 및 사이트 투 사이트 VPN에 적용됩니다. 또한 ASA에서 VPN 연결을 배포하고 원격 액세스하는 데 사용되는 SSL 표준에 대해서도 설명합니다.

CDO에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

- [사이트 간 가상 프라이빗 네트워크, 98 페이지](#)
- [원격 액세스 가상 프라이빗 네트워크](#)

사이트 간 가상 프라이빗 네트워크

사이트간 VPN 터널은 다양한 위치에 있는 네트워크를 연결합니다. 관리형 디바이스 및 관리형 디바이스와 모든 관련 표준을 준수하는 다른 Cisco 또는 타사 피어 간에 Site-to-Site IPsec 연결을 만들 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다. Site-to-Site 터널은 IPsec(Internet Protocol Security) 프로토콜 제품군 및 인터넷 키 교환 버전 2(IKEv2)를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

VPN 토폴로지

새로운 Site-to-Site VPN 토폴로지를 생성하려면 고유한 이름을 부여하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다 및 인증 방법을 선택해야 합니다. 구성된 후 토폴로지를 ASA에 구축합니다.

IPsec 및 IKE

CDO에서 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

VPN 연결을 인증하려면 각 디바이스의 토폴로지에서 사전 공유 키를 구성합니다. 사전 공유 키를 사용하면 IKE 인증 단계에서 사용되는 보안 키를 두 피어 간에 공유할 수 있습니다.

VPN 암호화 도메인

VPN의 암호화 도메인은 경로 기반 또는 정책 기반 트래픽 선택기라는 두 가지 방법으로 정의할 수 있습니다.

- 정책 기반: 암호화 도메인은 IPSec 터널에 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPSec 로컬 및 원격 트래픽 선택기는 0.0.0.0으로 설정됩니다. 즉, IPSec 터널로 라우팅되는 모든 트래픽은 소스/대상 서브넷에 관계없이 암호화됩니다. ASA는 암호화 맵을 사용하는 정책 기반 VPN을 지원합니다.
- 경로 기반: 암호화 도메인은 소스와 대상 모두에 대해 특정 IP 범위만 암호화하도록 설정됩니다. 이는 가상 IPsec 인터페이스를 생성하며, 해당 인터페이스에 들어오는 모든 트래픽은 암호화 및 암호 해독됩니다. ASA는 VTI(Virtual Tunnel Interface)를 사용하여 경로 기반 VPN을 지원합니다.

관련 정보:

- [ASA에 대한 사이트 간 VPN 구성, on page 99](#)
- [ASA 사이트 간 가상 사설망 모니터링](#)

ASA에 대한 사이트 간 VPN 구성

CDO(Cisco Defense Orchestrator)는 ASA(Adaptive Security Appliance) 디바이스에서 사이트 간 VPN 기능의 다음 측면을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 사이트 간 VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.
- 엔드포인트로 작동하는 엑스트라넷 디바이스의 정적 또는 동적 IP 주소 지원.

엑스트라넷 디바이스

각 토폴로지 유형에는 CDO에서 관리되지 않는 엑스트라넷 디바이스가 포함될 수 있습니다. 예를 들면 다음과 같습니다.

- CDO에서 지원하지만 조직에는 책임이 부여되지 않는 Cisco 디바이스. 회사 내의 다른 조직에서 관리하는 네트워크의 스포크 또는 서비스 제공자나 파트너의 네트워크에 대한 연결 등이 포함됩니다.
- 관리되지 않는 디바이스. CDO를 사용하여 관리되지 않는 디바이스에 구성을 생성하거나 구축할 수 없습니다. 관리되지 않는 디바이스를 VPN 토폴로지에 "엑스트라넷" 디바이스로 추가합니다.

동적 주소 지정 피어로 사이트 간 VPN 연결 구성

CDO를 사용하면 피어의 VPN 인터페이스 IP 주소 중 하나를 알 수 없거나 인터페이스가 DHCP 서버에서 주소를 가져올 때 피어 간에 사이트 간 VPN 연결을 생성할 수 있습니다. 사전 공유 키, IKE 설정 및 IPsec 구성이 다른 피어와 일치하는 모든 동적 피어는 사이트 간 VPN 연결을 설정할 수 있습니다.

피어 A와 B를 고려하십시오. 고정 피어는 VPN 인터페이스의 IP 주소가 고정되어 있는 디바이스이고 동적 피어는 VPN 인터페이스의 IP 주소를 알 수 없거나 임시 IP 주소가 있는 디바이스입니다.

다음 사용 사례에서는 동적으로 주소가 지정된 피어를 사용하여 안전한 사이트 간 VPN 연결을 설정하는 다양한 시나리오를 설명합니다.

- A는 정적 피어이고 B는 동적 피어이거나 그 반대입니다.
- A는 고정 피어이고 B는 DHCP 서버에서 확인된 IP 주소를 사용하거나 그 반대로 하는 동적 피어입니다.
- A는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.
- A는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.



참고 ASDM(Adaptive Security Device Manager)과 같은 로컬 관리자를 사용하여 인터페이스의 IP 주소를 변경하면 CDO에서 해당 피어의 **Configuration Status**(구성 상태)에 "Conflict Detected(충돌 탐지됨)"가 표시됩니다. "충돌 탐지됨" 상태 해결하면 다른 피어의 **Configuration Status**(구성 상태)가 "Not Synced(동기화되지 않음)" 상태로 변경됩니다. "Not Synced(동기화되지 않음)" 상태인 디바이스에 CDO 구성을 구축해야 합니다.

일반적으로 동적 피어는 연결을 시작하는 피어여야 합니다. 다른 피어는 동적 피어의 IP 주소를 알지 못하기 때문입니다. 원격 피어가 연결을 설정하려고 시도하면 다른 피어가 사전 공유 키, IKE 설정 및 IPsec 구성을 사용하여 연결을 검증합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.



참고 다음 시나리오에서는 사이트 간 VPN 연결을 구성할 수 없습니다.

디바이스에 둘 이상의 동적 피어 연결이 있는 경우

- 3개의 디바이스 A, B 및 C를 고려하십시오.
- A(고정 피어)와 B(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다.
- 엑스트라넷 디바이스를 생성하여 A와 C(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다. A의 고정 VPN 인터페이스 IP 주소를 엑스트라넷 디바이스에 할당하고 C와의 연결을 설정합니다.

ASA 사이트 간 VPN 지침 및 제한 사항

- CDO는 S2S VPN에 대한 흥미로운 트래픽을 설계하기 위해 `crypto-acl`을 지원하지 않습니다. 이는 보호된 네트워크만 지원됩니다.

- IKE 포트 500/4500이 사용 중이거나 활성화된 일부 PAT 변환이 있을 때마다 사이트 간 VPN을 동일한 포트에서 구성할 수 없으므로 해당 포트에서 서비스를 시작하는 데 실패합니다.
- 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.
- 이 릴리스에서는 하나 이상의 VPN 터널을 포함하는 PTP 토폴로지만 지원됩니다. Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.

Virtual Tunnel Interface에 대한 지침

- VTI는 IPsec 모드에서만 구성할 수 있습니다. ASA에서의 GRE 터널 종료는 지원되지 않습니다.
- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다. 그러나 VTI가 활성화된 후 물리적 인터페이스 MTU를 변경하는 경우, 새 MTU 설정을 사용하려면 VTI를 비활성화했다가 다시 활성화해야 합니다.
- 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 통과하는 모든 트래픽이 암호화됩니다.
- 기본적으로 VTI 인터페이스의 보안 레벨은 0입니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.
- VTI에서는 BGP만 지원됩니다.
- ASA가 IOS IKEv2 VTI 클라이언트를 종료하는 경우, IOS에서 config-exchange 요청을 비활성화합니다. ASA는 IOS VTI 클라이언트에서 시작한 이 L2L 세션에 대한 mode-CFG 속성을 검색할 수 없기 때문입니다.
- IPv6은 지원되지 않습니다.

관련 정보:


- [사이트 간 VPN 터널 생성, 102 페이지](#)

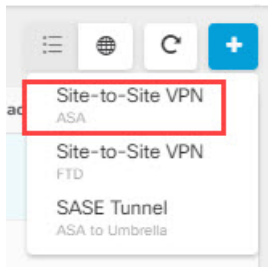
- VPN에서 사용되는 암호화 및 해시 알고리즘
- NAT에서 원격 액세스 트래픽 제외, 166 페이지

사이트 간 VPN 터널 생성

두 ASA 또는 엑스트라넷 디바이스를 사용하는 ASA 간에 사이트 간 VPN 터널을 생성하려면 다음 절차를 수행합니다.

단계 1 탐색 창에서 **VPN > Site-to-Site ASA/FDM** (사이트 간 ASA/FDM)을 선택합니다.

단계 2 오른쪽 상단 모서리에 있는 파란색 더하기  를 클릭하고 ASA 레이블이 있는 **Site-to-Site VPN**(사이트 간 VPN)을 클릭합니다.



단계 3 **Configuration Name**(구성 이름) 필드에 생성한 사이트 간 VPN 구성의 이름을 입력합니다.

단계 4 새 정책 기반 또는 경로 기반 사이트 간 VPN을 생성하는 옵션 중 하나를 선택합니다.

단계 5 **Peer Devices**(피어 디바이스) 섹션에서 다음을 수행합니다.

- 피어 1: ASA 디바이스를 선택하고 **Select**(선택)를 클릭합니다.
- 피어 2: 다른 ASA 디바이스를 선택한 다음 **Select**(선택)를 클릭합니다.

엑스트라넷: 피어 2에서 엑스트라넷 디바이스를 선택하려면 엑스트라넷 슬라이더를 클릭하여 활성화합니다.

Static(고정)을 선택하고 IP 주소를 지정하거나, DHCP 할당 IP가 있는 엑스트라넷 디바이스의 경우 **Dynamic**(동적)을 선택합니다. **IP Address**(IP 주소)는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned**(DHCP 할당됨)를 표시합니다.

- 엔드포인트 디바이스에 대한 **VPN 액세스 인터페이스**를 선택합니다.
- (경로 기반 VPN에 적용 가능) LAN 서브넷을 제어하는 **LAN 인터페이스**를 선택합니다. 여러 인터페이스를 선택할 수 있습니다.

선택한 LAN 인터페이스에 연결된 네트워크가 라우팅 정책 액세스 목록에 추가됩니다. 라우팅 정책 액세스 목록과 일치하는 트래픽은 VPN 터널에 의해 암호화/암호 해독됩니다.

- 참여하는 디바이스에 대해 **Protected Networks**(보호된 네트워크)를 추가하려면 **Add Network**(네트워크 추가)를 클릭합니다. 보호된 네트워크는 이 VPN 엔드포인트로 보호되는 네트워크를 정의합니다.
- (선택 사항이며 정책 기반에 적용 가능) 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외하려면 **NAT Exempt**(NAT 면제)를 선택합니다. 개별 피어에 대해 수동으로 구성해야 합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘

이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 ASA 사이트 간 VPN 트래픽 제외를 참조하십시오.

g) **Next**(다음)를 클릭합니다.

단계 6 (라우트 기반에 적용 가능) 이전 단계에서 피어 디바이스가 구성되면 터널 세부 정보에서 **VTI** 주소 필드가 자동으로 채워집니다. 필요한 경우 새 VTI로 사용할 IP 주소를 수동으로 입력할 수 있습니다.

단계 7 IKE Settings(IKE 설정) 섹션에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 [글로벌 IKE 정책 구성](#)을 참조하십시오.

CDO는 사용자가 수행한 구성에 따라 IKE 설정을 제안합니다. 권장 IKE 구성 설정을 계속 사용하거나 새로 정의할 수 있습니다.

참고 IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.

a) 적절하게 IKE 버전 중 하나 또는 둘 다를 선택합니다.

기본적으로 **IKEV** 버전 **2**가 활성화되어 있습니다.

참고 경로 기반 VPN에는 두 IKE 버전을 모두 활성화할 수 없습니다.

b) **Add IKEv2 Policy(IKEv2 정책 추가)**를 클릭하고 IKEv2 정책을 선택합니다.

참고 **Create New IKEv2 Policy(새 IKEv2 정책 생성)**를 클릭하여 새 IKEv2 정책을 생성합니다. 새 IKEv2 정책 생성에 대한 자세한 내용은 [IKEv2 정책 관리](#)을 참조하십시오. 기존 IKEv2 정책을 삭제하려면 선택한 정책 위에 마우스를 놓고 x 아이콘을 클릭합니다.

c) 참여 디바이스에 대한 사전 공유 키를 입력합니다. 사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. IKE는 인증 단계 중에 이러한 키를 사용합니다.

(IKEv2) 피어 **1** 사전 공유 키, 피어 **2** 사전 공유 키: IKEv2의 경우 각 피어에서 고유한 키를 구성할 수 있습니다. 사전 공유 키를 입력합니다. show(표시) 버튼을 클릭하고 피어에 대해 적절한 사전 공유를 입력할 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다. 다음 표에서는 두 피어에 대한 사전 공유 키의 용도에 대해 설명합니다.

	로컬 사전 공유 키	원격 피어 사전 공유 키
피어 1	피어 1 사전 공유 키	피어 2 사전 공유 키
피어 2	피어 2 사전 공유 키	피어 1 사전 공유 키

d) **IKE Version 1(IKE 버전 1)**을 클릭하여 활성화합니다.

e) **Add IKEv1 Policy(IKEv1 정책 추가)**를 클릭하고 IKEv1 정책을 선택합니다. **Create New IKEv1 Policy(새 IKEv1 정책 생성)**를 클릭하여 새 IKEv1 정책을 생성합니다. 새 IKEv1 정책 생성에 대한 자세한 내용은 [IKEv1 정책 관리](#)을 참조하십시오. 기존 IKEv1 정책을 삭제하려면 선택한 정책 위에 마우스 커서를 올리고 x 아이콘을 클릭합니다.

f) (IKEv1) 사전 공유 키: IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. 키는 영숫자 1~127자가 될 수 있습니다. 이 시나리오에서 피어 1과 피어 2는 동일한 사전 공유 키를 사용하여 데이터를 암호화하고 해독합니다.

g) **Next**(다음)를 클릭합니다.

단계 8 **IPSec Settings(IPSec 설정)** 섹션에서 CDO는 사용자가 수행한 구성을 기반으로 IKEv2 제안을 제안합니다. 권장 IKE 구성 설정을 계속 사용하거나 새로 정의할 수 있습니다. IPSec 설정에 대한 자세한 내용은 IPsec 제안 구성을 참고하십시오.

- a) **+ IKEv2 Proposals(+ IKEv2 제안)**를 클릭하여 IPSec 구성을 선택합니다. **IKE Settings(IKE 설정)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다. 기존 IKEv2 제안을 삭제하려면 선택한 제안 위에 마우스를 올려 놓고 x 아이콘을 클릭합니다.

참고 **Create New IKEv2 Proposals(새 IKEv2 제안 생성)**를 클릭하여 새 IKEv2 제안을 생성합니다. 새 IKEv2 정책 생성에 대한 자세한 내용은 **IPsec 제안 구성**을 참고하십시오.

- b) **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 **VPN에서 사용되는 암호화 및 해시 알고리즘, 104 페이지**를 참조하십시오.
- c) **Next(다음)**를 클릭합니다.

단계 9 **Finish(완료)** 섹션에서 구성을 읽고 구성에 만족하는 경우에만 계속 진행하고 **Submit(제출)**을 클릭하십시오.

새로 구성된 사이트 간 VPN 터널을 표시하는 VPN Tunnels(VPN 터널) 페이지로 이동합니다. 변경 사항이 준비되며 수동으로 구축해야 합니다. VTI 터널을 통해 디바이스 간에 VTI 트래픽을 자동으로 라우팅하도록 라우팅 정책이 생성됩니다. 이 정책을 보려면 **Inventory(인벤토리)** 페이지에서 디바이스를 선택하고 **Configuration(구성) > Diff(차이)**를 선택하십시오.

새 터널과 연결된 디바이스에 사이트 간 VPN 구성을 구축하려면 **CDO GUI를 사용하여 구성 변경 사항 구축** 섹션을 참조하십시오.

기존 CDO 사이트 투 사이트 VPN 삭제

단계 1 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 선택합니다.

단계 2 삭제할 원하는 사이트 투 사이트 VPN 터널을 선택합니다.

단계 3 **Actions(작업)** 창에서 **Delete(삭제)**를 클릭합니다.

선택한 사이트 투 사이트 VPN 터널이 삭제됩니다.

VPN에서 사용되는 암호화 및 해시 알고리즘

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.

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.

- AES-GCM - (IKEv2만 해당) 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-GMAC - (IKEv2 IPsec 제안만 해당) AES-GMAC(Advanced Encryption Standard Galois Message Authentication Code)는 데이터 원본 인증 기능만 제공하는 블록 암호화 작동 모드입니다. 이 모드는 데이터를 암호화하지 않고 데이터 인증을 허용하는 AES-GCM의 변형입니다. AES-GMAC는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다.
- 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. 3DES보다 속도가 빠르며 시스템 리소스를 더 적게 사용하지만 보안성은 더 낮습니다. 강력한 데이터 기밀 유지 기능이 필요하지 않으며 시스템 리소스나 속도가 중요한 경우에는 DES를 선택하십시오.
- 3DES - 56비트 키를 사용하여 암호화를 3회 수행하는 3DES(Triple DES)는 서로 다른 키를 사용하여 각 데이터 블록을 3회 처리하므로 DES보다 안전합니다. 그러나 시스템 리소스를 더 많이 사용하며 DES보다 속도가 느립니다.
- 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(SHA-1)에서는 160비트 다이제스트를 생성합니다. SHA는 MD5보다 무차별 암호 대입 공격에 대한 방어력이 뛰어납니다. 그러나 MD5보다 리소스를 더 많이 사용합니다. 최고 보안 레벨이 필요한 구현의 경우 SHA 해시 알고리즘을 사용합니다.
- IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.
 - SHA-256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
 - SHA-384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
 - SHA-512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
- MD5(Message Digest 5) - 128비트 다이제스트를 생성합니다. MD5는 SHA보다 전반적으로 성능이 우수하여 처리 시간이 짧지만 SHA보다 취약한 것으로 간주됩니다.
- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 암호화 알고리즘으로 AES-GCM/GMAC 옵션 중 하나를 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.

- 2 - Diffie-Hellman 그룹 2: 1024비트 MODP(모듈식 지수) 그룹. 이 옵션은 더 이상 좋은 보호 방법으로 간주되지 않습니다.

- 5 - Diffie-Hellman 그룹 5: 1536비트 MODP 그룹. 전에는 이 옵션이 128비트 키에 대해 좋은 보호 방법으로 간주되었지만 이제는 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 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
- 24 - Diffie-Hellman 그룹 24: 2048비트 MODP 그룹 및 256비트 소수 위수 하위 그룹. 이 옵션은 더 이상 권장되지 않습니다.

사용할 인증 방법 결정

다음과 같은 방법을 사용하여 사이트 간 VPN 연결에서 피어를 인증할 수 있습니다.

사전 공유 키

사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용됩니다. IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. IKEv2의 경우, 각 피어에 고유 키를 컨피그레이션할 수 있습니다.

사전 공유 키는 인증서에 비해 확장성이 떨어집니다. 다수의 Site-to-Site VPN 연결을 컨피그레이션해야 하는 경우, 사전 공유 키 방법 대신 인증서 방법을 사용하십시오.

NAT에서 사이트 간 VPN 트래픽 제외

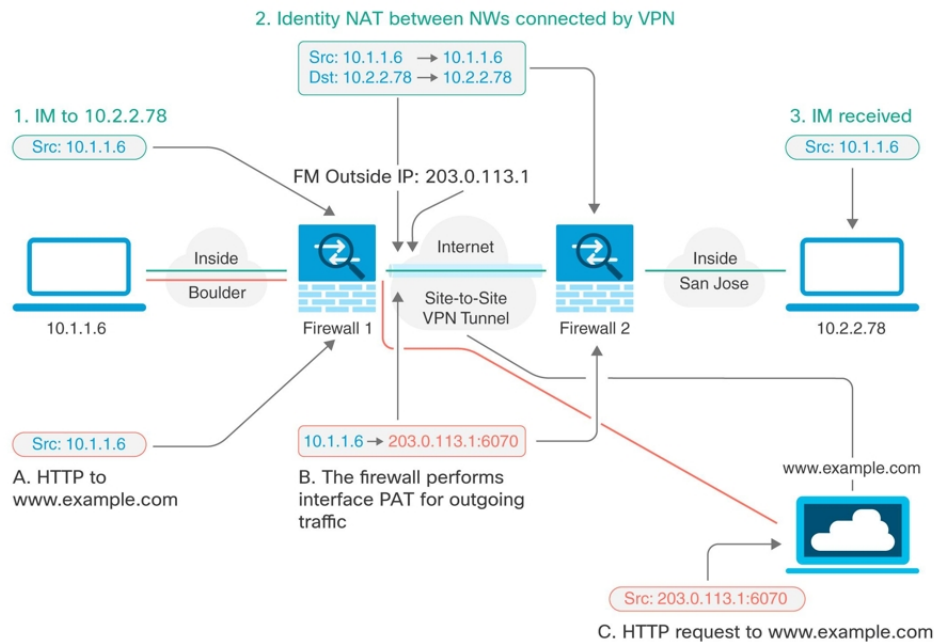
인터페이스에 사이트 대 사이트 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

VPN 연결을 생성할 때 **NAT Exempt(NAT 제외)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 대 사이트 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래 예에서는 인터페이스 PAT(Port Address Translation) 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 주소를 동일한 주소로 변환합니다.




다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 멤버 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.



Note 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.


단계 1 여러 네트워크를 정의하기 위한 개체를 생성합니다.

- 좌측의 CDO 내비게이션 바에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- ASA > Network(ASA 네트워크)**를 클릭합니다.
- 볼더 내부 네트워크를 확인합니다.

- e. 개체 이름을 입력합니다(예: boulder-network).
- f. **Create a network object**(네트워크 개체 생성)를 선택합니다.
- g. Value(값) 섹션에서 다음을 수행합니다.
 - eq를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
 - 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.

The screenshot shows a configuration window titled "Adding ASA Network Object". It has several sections:

- Object Name ***: A text input field containing "boulder-network".
- Description**: A text input field containing "Object description".
- Value**: A section with two radio buttons: "Create a network group" (unselected) and "Create a network object" (selected). Below the radio buttons is a dropdown menu set to "eq" and a text input field containing "10.1.1.0/24".

- h. **Add**(추가)를 클릭합니다.
- i. 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- j. 내부 산호세 네트워크를 정의합니다.
- k. 개체 이름(예: san-jose)을 입력합니다.
- l. **Create a network object**(네트워크 개체 생성)를 선택합니다.
- m. Value(값) 섹션에서 다음을 수행합니다.
 - eq를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
 - 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력합니다.

Adding ASA Network Object

Object Name *
sanjose-network

Description
Object description

Create a network group Create a network object

Value

eq ▲ 10.2.2.0/24

n. **Add**(추가)를 클릭합니다.

단계 2 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

- a. CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- b. 필터를 사용하여 NAT 규칙을 생성할 디바이스를 찾습니다.
- c. 상세정보 패널의 **Management**(관리) 영역에서 **NAT** > **NAT** 를 클릭합니다.
- d. **+** > **2회 NAT**를 클릭합니다.
 - 섹션 1에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
 - 섹션 2에서 **Source Interface**(소스 인터페이스) = **inside**(내부) 및 **Destination Interface**(대상 인터페이스) = **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
 - 섹션 3에서 **Source Original Address**(소스 원본 주소) = 'boulder-network' 및 **Source Translated Address**(소스 변환 주소) = 'boulder-network'를 선택합니다.
 - **Use Destination**(대상 사용)을 선택합니다.
 - **Destination Original Address**(대상 원본 주소) = 'sanjose-network' 및 **Source Translated Address**(소스 변환 주소) = 'sanjose-network'를 선택합니다. 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.

ASA: ASA_BGL_972 / NAT Rules Cancel

1	Type	Static	
2	Interfaces	inside	outside
3	Packets	<p>Source</p> <p>Original Address: boulder-network</p> <p>Translated Address: boulder-network</p> <p><input checked="" type="checkbox"/> Use Destination</p> <p>Destination</p> <p>Original Address: sanjose-network</p> <p>Translated Address: sanjose-network</p> <p><input type="checkbox"/> Use Service Objects</p>	<p>i Select the original address and the translated address packets going through this NAT rule.</p>
4	Advanced	<p><input type="checkbox"/> Include after-auto (place in Section 3)</p> <p><input checked="" type="checkbox"/> Disable proxy ARP for incoming packets</p> <p><input type="checkbox"/> Use net-to-net translation (for NAT 46)</p> <p><input type="checkbox"/> Use route lookup to determine the egress interface</p>	


- **Disable proxy ARP for Incoming packet**(수신 패킷에 대해 프록시 ARP 비활성화)을 선택합니다.
- **Save**(저장)를 클릭합니다.
- 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 3 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다. 참고: 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 구성 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 컨피그레이션을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뛸 수 있습니다.

- > 2회 NAT를 클릭합니다.
- 섹션 1에서 **Dynamic**(동적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 섹션 2에서 **Source Interface**(소스 인터페이스) = **inside**(내부) 및 **Destination Interface**(대상 인터페이스) = **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 섹션 3에서 **Source Original Address**(소스 원본 주소) = 'boulder-network' 및 **Source Translated Address**(소스 변환 주소) = 'interface'를 선택합니다.

ASA: ASA_BGL_972 / NAT Rules

Cancel Save



The diagram shows a NAT rule configuration. It features two boxes: 'GigabitEthernet inside' on the left and 'GigabitEthernet outside' on the right. Between them are two interface icons labeled '0/0' and '0/1' with a double-headed arrow indicating bidirectional traffic.

1 Type ↔ Dynamic

2 Interfaces 🏠 inside 🏠 outside Edit

3 Packets

Source

Original Address boulder-network Translated Address interface

Use Destination

Use Service Objects

i Select the original address and the translated address for packets going through this NAT rule.

e. **Save**(저장)를 클릭합니다.

f. 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 4 CDO에 구성 변경 사항을 구축합니다. 자세한 내용은 [CDO GUI를 사용하여 구성 변경 사항 구축, on page 215](#)를 참고하십시오.

단계 5 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 `boulder-network`일 때는 `sanjose-network`용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 `sanjose-network`용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

글로벌 IKE 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계를)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.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높

습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 Edit(수정)을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- [IKEv1 정책 관리](#)

- [IKEv2 정책 관리](#)

IKEv1 정책 관리

IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics


[IKEv1 정책 생성 또는 편집](#), 113 페이지

IKEv1 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy**(새 IKE 정책 생성) 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- **과란색 더하기 ** 버튼을 클릭하고 **FDM > IKEv1 Policy**(IKEv1 정책)를 선택하여 새 IKEv1 정책을 생성합니다.
- 개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv1 속성을 구성합니다.

- **Priority(우선순위)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에서 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 발생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime(라이프타임)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 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. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.
- **Authentication(인증)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 [사용할 인증 방법 결정](#)을 참조하십시오.
 - **Preshared Key(사전 공유 키)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
 - **Certificate(인증서)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 [사용할 Diffie-Hellman 모듈러스 그룹 결정](#)을 참조하십시오.

단계 5 Add(추가)를 클릭합니다.

IKEv2 정책 관리

IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics


[IKEv2 정책 생성 또는 편집](#), 115 페이지

IKEv2 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy**(새 IKEv2 정책 생성) 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 더하기  버튼을 클릭하고 **FTD > IKEv2 Policy**(IKEv2 정책)를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 수정할 IKEv2 정책을 선택하고 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv2 속성을 구성합니다.

- **Priority**(우선순위)—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그다음 우선 순위에서 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **State**(상태) - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption**(암호화) - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)을 참조하십시오.
- **Diffie-Hellman Group**(Diffie-Hellman 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. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 Diffie-Hellman 모듈러스 그룹 결정](#)을 참조하십시오.
- **Integrity Hash**(무결성 해시) - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)을 참조하십시오.
- **PRF**(Pseudo-Random Function) 해시 - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및

PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)을 참조하십시오.

- **Lifetime(라이프타임)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 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 연결을 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 5 **Add(추가)**를 클릭합니다.

IPsec 제안 구성

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 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연결(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 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 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

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.



Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- [IKEv1 IPsec 제안 개체 관리](#)
- [IKEv2 IPsec 제안 개체 관리](#)

IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO(Cisco Defense Orchestrator)는 IKEv1 IPsec 제안 개체를 지원합니다.

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.



Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

Related Topics

[IKEv1 IPsec 제안 개체 생성 또는 편집](#), 117 페이지


IKEv1 IPsec 제안 개체 생성 또는 편집

여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal**(새 IKEv1 제안 생성) 링크를 클릭하여 사이트 투 사이트 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM > IKEv1 IPsec Proposal**(IKEv1 IPsec 제안)을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit**(편집)를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPsec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 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.
- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPsec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

단계 5 이 제안에 대한 **ESP Encryption**(ESP 암호화)(Encapsulating Security Protocol) 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)을 참조하십시오.

단계 6 인증에 사용할 **ESP Hash(ESP 해시)** 또는 무결성 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)을 참조하십시오.

단계 7 **Add(추가)**를 클릭합니다.

IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

Related Topics

[IKEv2 IPsec 제안 개체 생성 또는 편집](#), 118 페이지


IKEv2 IPsec 제안 개체 생성 또는 편집

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(새 IPsec 제안 생성)** 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM > IKEv2 IPsec Proposal(IKEv2 IPsec 제안)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(편집)**를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKE2 IPsec 제안 개체 구성:

- **Encryption(암호화)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)을 참조하십시오.
- **Integrity Hash(무결성 해시)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)을 참조하십시오.

단계 5 **Add**(추가)를 클릭합니다.

ASA 사이트 간 가상 사설망 모니터링

CDO를 사용하면 온보딩된 ASA 디바이스에서 이미 존재하는 사이트 간 VPN 구성을 모니터링할 수 있습니다. 사이트 간 구성을 수정하거나 삭제할 수 없습니다.

사이트 투 사이트 VPN 터널 연결 확인

Check Connectivity(연결 확인) 버튼을 사용하여 터널에 대한 실시간 연결 확인을 트리거하여 터널이 현재 **사이트 간 VPN 터널 검색 및 필터링** 인지를 식별합니다. 온디맨드 연결 확인 버튼을 클릭하지 않으면 온보딩된 모든 디바이스에서 사용 가능한 모든 터널의 확인이 1시간에 한 번 수행됩니다.



Note

- CDO는 ASA에서 이 연결성 검사 명령을 실행하여 터널이 활성 상태인지 유틸리티 상태인지를 확인합니다.

```
show vpn-sessiondb 121 sort ipaddress
```

- 모델 ASA 디바이스 터널은 항상 유틸리티로 표시됩니다.

VPN 페이지에서 터널 연결을 확인하려면 다음을 수행합니다.

단계 1 기본 탐색 모음에서 VPN > ASA/FDM Site-to-Site VPN를 클릭합니다.

단계 2 사이트 투 사이트 VPN 터널에 대한 터널 목록을 **사이트 간 VPN 터널 검색 및 필터링** 하고 선택합니다.

단계 3 오른쪽의 작업 창에서 **Check Connectivity**(연결 확인)를 클릭합니다.

VPN 문제 식별



CDO는 ASA에서 VPN 문제를 식별할 수 있습니다. (이 기능은 아직 AWS VPC 사이트 투 사이트 VPN 터널에 사용할 수 없습니다.) 이 문서에서는 다음을 설명합니다.

- [누락된 피어가 있는 VPN 터널 찾기](#)
- [암호화 키 문제가 있는 VPN 피어 찾기](#)
- [터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기](#)
- [터널 구성에서 문제 찾기](#)

[터널 구성 문제 해결, on page 121](#)

누락된 피어가 있는 VPN 터널 찾기



"Missing IP Peer" 상태는 FDM 관리 디바이스보다 ASA 디바이스에서 발생할 가능성이 높습니다.

-
- 단계 1 CDO 탐색 창에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.
- 단계 4 감지된 문제를 확인합니다.
- 단계 5 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 **Peers(피어)** 창을 확인합니다. 하나의 피어 이름이 나열됩니다. CDO는 다른 피어 이름을 "[Missing peer IP.]"로 보고합니다.
-

암호화 키 문제가 있는 VPN 피어 찾기



이 접근 방식을 사용하여 다음과 같은 암호화 키 문제가 있는 VPN 피어를 찾습니다.

- IKEv1 또는 IKEv2 키가 잘못되었거나 누락되었거나 일치하지 않습니다.
- 사용되지 않거나 낮은 암호화 터널

-
- 단계 1 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.
- 단계 4 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 **Peers(피어)** 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.
- 단계 5 디바이스 중 하나에 대해 **View Peers(피어 보기)**를 클릭합니다.
- 단계 6 **Diagram View(다이아그램 보기)**에서 문제를 보고하는 디바이스를 두 번 클릭합니다.
- 단계 7 하단의 **Tunnel Details(터널 세부 정보)** 창에서 **Key Exchange(키 교환)**를 클릭합니다. 두 디바이스를 모두 보고 해당 지점에서 주요 문제를 진단할 수 있습니다.
-

터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기

"불완전하거나 잘못 구성된 액세스 목록" 상태는 ASA 디바이스에서만 발생할 수 있습니다.

-
- 단계 1 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.
- 단계 4 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 **Peers(피어)** 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.
- 단계 5 디바이스 중 하나에 대해 **View Peers(피어 보기)**를 클릭합니다.

단계 6 Diagram View(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.

단계 7 하단의 Tunnel Details(터널 세부 정보) 패널에서 **Tunnel Details**(터널 세부 정보)를 클릭합니다. "Network Policy: Incomplete(네트워크 정책: 완료되지 않음)" 메시지가 표시됩니다.


터널 구성에서 문제 찾기


터널 구성 오류는 다음 시나리오에서 발생할 수 있습니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.



단계 1 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.

단계 2 **Table View**(테이블 보기)를 선택합니다.

단계 3 필터 아이콘  을 클릭하여 필터 패널을 엽니다.

단계 4 터널 문제에서 탐지된 문제를 클릭하여 오류를 보고하는 VPN 구성을 봅니다. 구성 보고 문제  를 볼 수 있습니다.

단계 5 VPN 구성 보고 문제를 선택합니다.

단계 6 오른쪽의 피어 창에 문제가 있는 피어에 대한  아이콘이 나타납니다.  아이콘 위로 마우스를 가져가면 문제와 해결 방법을 볼 수 있습니다.

다음 단계: [터널 구성 문제 해결](#).

터널 구성 문제 해결

이 절차는 다음과 같은 터널 구성 문제를 해결하려고 시도합니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

자세한 내용은 [터널 구성에서 문제 찾기](#)를 참조하십시오.

단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 문제를 보고하는 VPN 구성과 연결된 디바이스를 선택합니다.

단계 4 **"충돌 탐지됨" 상태 해결**

단계 5 CDO 탐색 창에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.

단계 6 이 문제를 보고하는 VPN 구성을 선택합니다.

단계 7 **Actions**(작업)창에서 **Edit**(편집) 아이콘을 클릭합니다.


단계 8 4단계에서 **Finish**(마침) 버튼을 클릭할 때까지 각 단계에서 **Next**(다음)를 클릭합니다.

단계 9 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 212 페이지.

사이트 간 VPN 터널 검색 및 필터링

필터 사이드바 를 검색 필드와 함께 사용하여 VPN 터널 다이어그램에 표시된 VPN 터널 검색에 집중할 수 있습니다.

단계 1 기본 내비게이션 바에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**으로 이동합니다.

단계 2 필터 아이콘 을 클릭하여 필터 창을 엽니다.

단계 3 다음 필터를 사용하여 검색을 구체화합니다.

- **Filter by Device**(디바이스별 필터링) - **Filter by Device**(디바이스별 필터링)를 클릭하고 디바이스 유형 탭을 선택한 후 필터링을 통해 찾으려는 디바이스를 선택합니다.
- **Tunnel Issues**(터널 문제) - 터널의 양쪽에 문제가 있음을 탐지했는지 여부입니다. 디바이스에 문제가 있는 몇 가지 예로는 연결된 인터페이스 또는 피어 IP 주소 또는 액세스 목록 누락, IKEv1 제안 불일치 등이 있습니다 (AWS VPC VPN 터널에서는 터널 문제 탐지를 아직 사용할 수 없음).
- **Devices/Services**(디바이스/서비스) - 디바이스 유형을 기준으로 필터링합니다.
- **Status**(상태) - 터널 상태는 활성 또는 유휴 상태일 수 있습니다.
 - **Active**(활성) - 네트워크 패킷이 VPN 터널을 통과하는 열린 세션이 있거나 성공적인 세션이 설정되었고 아직 시간 초과되지 않았습니다. **Active**(활성)는 터널이 활성 상태이고 관련성이 있음을 나타내는 데 도움이 될 수 있습니다.
 - **Idle**(유휴) - CDO가 이 터널에 대한 열린 세션을 검색할 수 없습니다. 터널이 사용 중이 아니거나 이 터널에 문제가 있을 수 있습니다.
- **Onboarded**(온보딩됨) - CDO에서 디바이스를 관리하거나 CDO에서 관리하지 않을 수 있습니다(관리되지 않음).
 - 관리됨 - CDO가 관리하는 디바이스별로 필터링합니다.
 - 관리되지 않음 - CDO가 관리하지 않는 디바이스로 필터링합니다.
- **Device Types**(디바이스 유형) - 터널의 한쪽이 라이브(연결된 디바이스) 디바이스인지 아니면 모델 디바이스인지 여부입니다.


단계 4 검색 창에 디바이스 이름 또는 IP 주소를 입력하여 필터링된 결과를 검색할 수도 있습니다. 검색은 대/소문자를 구분하지 않습니다.

관리되지 않는 디바이스 온보딩

CDO는 피어 중 하나가 온보딩될 때 사이트 간 VPN 터널을 검색 합니다. 두 번째 피어가 CDO에서 관리되지 않는 경우 VPN 터널 목록을 필터링하여 관리되지 않는 디바이스를 찾아 온보딩할 수 있습니다.

단계 1 기본 내비게이션 바에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 선택하여 VPN 페이지를 엽니다.

단계 2 **Table View(테이블 보기)**를 선택합니다.

단계 3 를 클릭하여 필터 패널을 엽니다.

단계 4 **Unmanaged(관리되지 않음)**를 선택합니다.

단계 5 결과의 테이블에서 터널을 선택합니다.

단계 6 오른쪽의 **Peers(피어)** 창에서 **Onboard Device(온보드 디바이스)**를 클릭하고 화면의 지침을 따릅니다.

관련 정보:

- [디바이스 및 서비스 온보딩](#)
- [ASA 디바이스 온보딩](#)

사이트 투 사이트 VPN 터널의 IKE 개체 세부 정보 보기

선택한 터널의 피어/디바이스에 구성된 IKE 개체의 세부 정보를 볼 수 있습니다. 이러한 세부 정보는 IKE 정책 개체의 우선 순위에 따라 계층 구조의 트리 구조로 나타납니다.



Note 엑스트라넷 디바이스는 IKE 개체 세부 정보를 표시하지 않습니다.

단계 1 왼쪽의 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**를 클릭합니다.

단계 2 **VPN Tunnels(VPN 터널)** 페이지에서 피어를 연결하는 VPN 터널의 이름을 클릭합니다.

단계 3 오른쪽의 **Relationships(관계)** 아래에 세부 정보를 보려는 개체를 확장합니다.

마지막으로 성공한 사이트 투 사이트 VPN 터널 설정 날짜 보기

단계 1 **사이트 간 VPN 터널 정보 보기.**

단계 2 **Tunnel Details(터널 세부 정보)** 창을 클릭합니다.

단계 3 **Last Seen Active(마지막 확인한 활성)** 필드를 확인합니다.

사이트 간 VPN 터널 정보 보기

사이트 간 VPN 테이블 보기는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 사이트 간 VPN 터널의 전체 목록입니다. 터널은 이 목록에 한 번만 존재합니다. 테이블에 나열된 터널을 클릭하면 추가 조사를 위해 터널의 피어로 직접 이동할 수 있는 옵션이 오른쪽 사이드바에 제공됩니다.

CDO가 터널의 양쪽을 모두 관리하지 않는 경우 **관리되지 않는 디바이스 온보딩**를 클릭하여 언매니지드 피어의 온보드 기본 온보딩 페이지를 열 수 있습니다. CDO가 터널의 양쪽을 모두 관리하는 경우 Peer 2(피어 2) 옆에 매니지드 디바이스의 이름이 포함됩니다. 그러나 AWS VPC의 경우 Peer 2 옆에 VPN 게이트웨이의 IP 주소가 포함됩니다.

테이블 보기에서 사이트 간 VPN 연결을 보려면 다음을 수행합니다.

단계 1 기본 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN**를 클릭합니다.

단계 2 **Table view**(테이블 보기) 버튼을 클릭합니다.

단계 3 **사이트 간 VPN 터널 검색 및 필터링**를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

사이트 투 사이트 VPN 전역 보기

단계 1 기본 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN**를 클릭합니다.

단계 2 **Global view**(전역 보기) 버튼을 클릭합니다.

단계 3 **사이트 간 VPN 터널 검색 및 필터링**를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

단계 4 전역 보기에 표시된 피어 중 하나를 선택합니다.

단계 5 **View Details**(세부사항 보기)를 클릭합니다.

단계 6 VPN 터널의 다른 쪽 끝을 클릭하면 CDO에 해당 연결에 대한 Tunnel Details(터널 세부 정보), NAT Information(NAT 정보) 및 Key Exchange(키 교환) 정보가 표시됩니다.

- **Tunnel Details**(터널 세부 정보) - 터널에 대한 이름 및 연결 정보를 표시합니다. Refresh(새로 고침) 아이콘을 클릭하면 터널에 대한 연결 정보가 업데이트됩니다.
- **Tunnel Details specific to AWS connections**(AWS 연결 관련 터널 세부 정보) - AWS 사이트 투 사이트 연결에 대한 터널 세부 정보는 다른 연결과 약간 다릅니다. AWS VPC에서 VPN 게이트웨이로 연결된 각 연결에 대해 AWS는 2개의 VPN 터널을 생성합니다. 이는 고가용성을 위한 것입니다.
 - 터널의 이름은 VPN 게이트웨이가 연결된 VPC의 이름을 나타냅니다. 터널에 이름이 지정된 IP 주소는 VPN 게이트웨이가 VPC로 인식하는 IP 주소입니다.
 - CDO 연결 상태가 "active(활성)"로 표시되면 AWS 터널 상태가 "Up(가동 중)"입니다. CDO 연결 상태가 "inactive(비활성)"인 경우 AWS 터널 상태는 "Down(중단)"입니다.
- **NAT Information**(NAT 정보) - 사용 중인 NAT 규칙의 유형, 원래 및 변환된 패킷 정보를 표시하고, 해당 터널에 대한 NAT 규칙을 볼 수 있는 NAT 테이블에 대한 링크를 제공합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)

- **Key Exchange**(키 교환) - 터널 및 키 교환 문제에서 사용 중인 암호화 키를 표시합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)

터널 창

Tunnels(터널) 창에는 특정 VPN 게이트웨이와 연결된 모든 터널의 목록이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 사이트 간 VPN 연결의 경우, tunnels(터널) 창에는 VPN 게이트웨이에서 VPC로의 모든 터널이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 각 사이트 간 VPN 연결에는 2개의 터널이 있으므로 다른 디바이스에 대해 일반적으로 표시되는 터널 수가 두 배입니다.

VPN 게이트웨이 세부 정보

VPN 게이트웨이에 연결된 피어의 수 및 VPN 게이트웨이의 IP 주소를 표시합니다. 이는 VPN Tunnels(VPN 터널) 페이지에만 표시됩니다.

피어 창

사이트 간 VPN 피어 쌍을 선택하면 Peers(피어) 창에 쌍의 두 디바이스가 나열되며 디바이스 중 하나에 대해 **View Peers**(피어 보기)를 클릭할 수 있습니다. **View Peers**(피어 보기)를 클릭하면 디바이스가 연결된 다른 사이트 간 피어가 표시됩니다. 이는 Table(테이블) 보기 및 Global(전역) 보기에 표시됩니다.

원격 액세스 가상 프라이빗 네트워크

RA VPN(원격 액세스 VPN)을 사용하면 개별 사용자가 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 따라서 모바일 근무자가 홈 네트워크 또는 공개 Wi-Fi 네트워크 등에서 연결할 수 있습니다.

RA VPN 구성은 다음 구성 요소로 구성됩니다.

- 연결 프로파일: 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있도록 원격 액세스 VPN 연결 프로파일을 생성할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다. 연결 프로파일은 ID 소스와 그룹 정책으로 구성됩니다.

관련 정보:

- [ASA에 대한 원격 액세스 VPN 구성, on page 131](#)

원격 액세스 가상 프라이빗 네트워크 세션

RA VPN(Remote Access Virtual Private Network)은 모바일 사용자 또는 재택 근무자와 같은 원격 사용자에게 보안 연결을 제공합니다. 이러한 연결을 모니터링하면 연결 및 사용자 세션 성능에 대한 중요한 지표를 얻을 수 있습니다. Cisco Defense Orchestrator (CDO) RA VPN 모니터링 기능을 통해 원격 액세스 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. 필요에 따라 원격 액세스 VPN 세션의 연결을 끊을 수도 있습니다.


Remote Access Virtual Private Monitoring(원격 액세스 가상 프라이빗 모니터링) 페이지는 다음 정보를 제공합니다.

- 최대 1년 동안의 활성 및 기록 세션 목록입니다.
- CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 직관적인 그래픽 시각적 개체를 표시합니다.
- 라이브 세션 화면에는 CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 VPN 연결 프로파일이 표시됩니다. 또한 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- 디바이스 유형, 디바이스 이름, 세션 길이, 전송 및 수신된 데이터의 양과 같은 기준을 기반으로 검색 범위를 좁힐 수 있는 필터링 기능입니다.

관련 정보:

- [라이브 AnyConnect 원격 액세스 VPN 세션 모니터링, on page 126](#)
- [기록 AnyConnect RA VPN 세션 모니터링, on page 128](#)
- [RA VPN 세션 검색 및 필터링](#)
- [RA VPN 모니터링 보기 사용자 지정](#)
- [RA VPN 세션을 CSV 파일로 내보내기](#)
- [사용자의 모든 활성 RA VPN 세션 연결 끊기](#)


라이브 AnyConnect 원격 액세스 VPN 세션 모니터링

디바이스의 활성 AnyConnect RA VPN 세션에서 실시간 데이터를 모니터링할 수 있습니다. 이 데이터는 10분마다 자동으로 새로 고쳐집니다. 언제든지 최신 세션 목록을 검색하려면 화면 오른쪽 모서리에 나타나는 다시 로드 아이콘  을 클릭하십시오.

시작하기 전에

- RA VPN 헤드 엔드를 CDO에 온보딩합니다.
- 라이브 데이터를 모니터링하려는 디바이스의 연결 상태는 **Inventory**(인벤토리) 페이지에서 "Online(온라인)"인지 확인합니다.

단계 1 CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring**(VPN 원격 액세스 VPN 모니터링)을 클릭합니다.

또는 CDO 홈 페이지에서 **View Active Remote Access VPN Sessions**(활성 원격 액세스 VPN 세션 보기)를 클릭하거나 **VPN > Remote Access VPN**(원격 액세스 VPN)으로 이동하여 화면 오른쪽 상단 모서리에 있는  아이콘을 클릭할 수 있습니다.

단계 2 **RA VPN**을 클릭합니다.

단계 3 **Live**(라이브)를 클릭합니다.

RA VPN 세션 검색 및 필터링하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

참고 데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

라이브 데이터 보기

라이브 데이터는 대시보드 및 테이블 형식으로 표시됩니다.

Dashboard(대시보드) 보기

대시보드를 보려면 화면의 오른쪽 상단 모서리에 나타나는 **Show Charts View**(차트 보기 표시) 아이콘을 클릭해야 합니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 확인할 수 있도록 제공합니다.

- **Breakdown (All Devices)**(애널리틱스 데이터(모든 디바이스)): 총 라이브 세션 수를 표시합니다. 4개의 호 길이로 구분된 원도표도 표시됩니다. 세션 수가 가장 많은 상위 3개 디바이스의 VPN 세션 비율을 보여줍니다. 나머지 호 길이는 다른 디바이스의 어그리게이션을 나타냅니다.
- CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 연결 프로파일이 표시됩니다.
- 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- **Active Sessions by Country**(국가별 활성 세션): RA VPN 헤드엔드에 연결된 사용자 위치의 인터랙티브 히트맵을 표시합니다.
 - 사용자가 연결한 국가는 해당 국가에서 설정된 세션의 상대적 비율에 따라 점점 더 짙은 파란색 음영으로 표시됩니다. 파란색이 어두울수록 해당 국가에서 더 많은 세션이 설정되었음을 의미합니다.
 - 맵의 맨 아래에 있는 범례는 국가의 세션 수와 국가를 표시하는 데 사용되는 파란색 음영 간의 상관관계를 나타내는 척도를 제공합니다.
 - 맵에 마우스 포인터를 올려놓으면 해당 국가의 이름 및 해당 국가에서 설정된 총 활성 사용자 세션 수를 확인할 수 있습니다.
 - 테이블 위에 마우스 포인터를 올려놓으면 해당 국가의 위치와 맵의 총 활성 사용자 세션 수를 확인할 수 있습니다.

테이블 형식 보기

데이터를 테이블 형식으로 보려면 화면의 오른쪽 상단 모서리에 있는 **Show Tabular View**(테이블 형식 보기 표시) 아이콘을 클릭합니다.

테이블 형식은 현재 연결된 VPN 사용자의 전체 목록을 제공합니다.

- **Location(위치)** 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.



중요 CDO는 라이브 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 사용자 지정 필터는 시각적 대시보드 보기에서 지원되지 않으므로, 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 적용한 모든 필터를 제거하려면 **Clear(지우기)**를 클릭합니다. 표준 필터는 제거할 수 없습니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active(활성)** 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.


기록 AnyConnect RA VPN 세션 모니터링

지난 3개월 동안 기록된 AnyConnect RA VPN 세션의 기록 데이터를 모니터링할 수 있습니다.

시작하기 전에

- RA VPN 헤드 엔드를 CDO에 온보딩합니다.

단계 1 CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring(VPN 원격 액세스 VPN 모니터링)**을 클릭합니다.

또는 CDO 홈 페이지에서 **View Active Remote Access VPN Sessions(활성 원격 액세스 VPN 세션 보기)**를 클릭하거나 **VPN > Remote Access VPN(VPN 원격 액세스 VPN)**으로 이동하여 오른쪽 상단 모서리에 있는 아이콘 을 클릭할 수 있습니다.

단계 2 **RA VPN**을 클릭합니다.

단계 3 **Historical(기록)**을 클릭합니다.

CDO는 지난 3개월 동안 기록된 RA VPN 세션의 기록 데이터를 표시합니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

이력 데이터 보기

이력 데이터는 대시보드 및 표 형식으로 표시됩니다.

Dashboard(대시보드) 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Charts View**(차트 보기 표시) 아이콘을 클릭해야 합니다. 테이블 보기와 함께 대시보드 보기가 표시됩니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 제공합니다. 지난 24시간, 7일 및 30일 동안 모든 디바이스에 대해 기록된 VPN 세션을 보여주는 막대 그래프를 제공합니다. 드롭다운에서 기간을 선택할 수 있습니다. 개별 막대에 마우스 커서를 대면 해당 날짜의 총 세션 수와 날짜를 확인할 수 있습니다.

테이블 형식 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Tabular View**(테이블 형식 보기 표시) 아이콘을 클릭하여 테이블 형식 보기만 표시해야 합니다. 테이블 형식은 지난 3개월 동안 연결된 VPN 사용자의 전체 목록을 제공합니다.

Location(위치) 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.



중요 CDO는 기록 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 대시보드는 맞춤형 필터를 지원하지 않으므로 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 새로 적용된 필터를 지우면 대시보드가 다시 실행됩니다. 화면에서 **Clear**(지우기)를 클릭하여 수동으로 적용된 필터를 제거합니다. 표준 필터는 제거할 수 없습니다.

RA VPN 세션 검색 및 필터링 기능을 사용하여 세션 날짜와 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

Status(상태) 열에 **Active**(활성) 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

RA VPN 세션 검색 및 필터링

검색

검색 창 기능을 사용하여 RA VPN 세션을 찾습니다. 검색 창에 디바이스 이름, IP 주소 또는 일련 번호를 입력하기 시작합니다. 그러면 검색 기준에 맞는 RA VPN 세션이 표시됩니다. 검색은 대/소문자를 구분하지 않습니다.


필터

필터 사이드바를 사용하여 세션 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위 등의 기준에 따라 RA VPN 세션을 찾습니다. 필터 기능은 라이브 보기와 기록 보기 모두에서 사용할 수 있습니다.

- **Filter by Devices**(디바이스별 필터링): **All Types**(모든 유형) 탭에서 하나 또는 모든 디바이스를 선택하여 선택한 디바이스의 세션을 봅니다. 창은 또한 유형에 따라 디바이스를 분류하고 해당 탭 아래에 표시합니다.

- **Sessions Time Range**(세션 시간 범위)(기록 데이터에만 적용 가능): 지정된 날짜 및 시간 범위의 기록 세션을 표시합니다. 지난 3개월 동안 기록된 데이터를 볼 수 있습니다.
- **Sessions Length**(세션 길이): 지정된 세션의 기간 길이를 기준으로 세션을 표시합니다. 시간 단위(시간, 분 또는 초)를 설정하고 슬라이더를 이동하여 최소 및 최대 기간 길이를 지정합니다. 제공된 필드에 길이를 지정할 수도 있습니다.
- **Upload (TX)**(업로드(TX)): 보안 네트워크에 업로드되거나 전송된 데이터의 지정된 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.
- **Download (RX)**(다운로드(RX)): 보안 네트워크에서 다운로드하거나 수신한 지정된 데이터 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.

RA VPN 모니터링 보기 사용자 지정

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 모드에서 RA VPN 모니터링 보기를 편집할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘  을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.

CDO는 다음에 CDO에 로그인할 때 선택 항목을 기억합니다.

RA VPN 세션을 CSV 파일로 내보내기


하나 이상의 디바이스의 RA VPN 세션을 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. Microsoft Excel과 같은 스프레드시트 애플리케이션에서 .csv 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다. 이 정보는 RA VPN 세션을 분석하는 데 도움이 됩니다. 세션을 내보낼 때마다 CDO는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.

CDO는 최대 100,000개의 활성 세션을 CSV 파일로 내보낼 수 있습니다. 모든 디바이스의 총 세션 수가 최대 제한을 초과하는 경우 **View By Device**(디바이스별 보기) 필터를 사용하여 개별 디바이스에 대한 보고서를 생성할 수 있습니다.

단계 1 CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring**(VPN 원격 액세스 VPN 모니터링)을 클릭합니다.

단계 2 **View By Devices**(디바이스별 보기) 영역에서 다음 중 하나를 선택합니다.

- **All Devices**(모든 디바이스) - 그 아래에 나열된 모든 디바이스에서 활성 세션을 내보냅니다.
- 해당 디바이스의 세션을 내보낼 디바이스를 클릭합니다.

단계 3 오른쪽 상단 모서리에 있는  아이콘을 클릭합니다. CDO는 화면에 표시되는 규칙을 .csv 파일로 내보냅니다.

단계 4 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

ASA 사용자의 모든 활성 RA VPN 세션 연결 끊기

ASA 디바이스에서 모든 사용자의 모든 활성 RA VPN 세션을 종료할 수 있습니다. 라이브 모드와 기록 모드 모두에서 이 작업을 수행할 수 있습니다.

CDO는 사용자가 VPN 세션을 보고 종료할 수 있도록 VPN 세션 관리자 사용자 역할을 제공합니다. 자세한 내용은 [사용자 역할](#)을 참조하십시오.

단계 1 CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring(VPN 원격 액세스 VPN 모니터링)**을 클릭합니다.

단계 2 디바이스별 보기 영역에서 해당 디바이스의 모든 활성 세션을 종료하려는 ASA 디바이스를 클릭합니다.

단계 3 오른쪽 상단에 나타나는 **Terminate All Sessions(모든 세션 종료)**를 클릭합니다.

단계 4 **Yes, Terminate All Sessions(예, 모든 세션을 종료합니다)**를 클릭하여 선택을 확인합니다.

사용자의 모든 활성 RA VPN 세션 연결 끊기

사용자의 연결을 끊으면 CDO는 해당 ASA 디바이스에서 사용자의 모든 활성 RA VPN 세션을 종료합니다. 라이브 모드와 기록 모드 모두에서 이 작업을 수행할 수 있습니다.

단계 1 CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring(VPN 원격 액세스 VPN 모니터링)**을 클릭합니다.

단계 2 세션의 연결을 끊을 사용자를 검색합니다. **Search(검색)** 막대에 검색 기준을 입력할 수 있습니다.

단계 3 활성 세션을 클릭하고 오른쪽의 **Actions(작업)** 창에서 **Terminate all RA VPN sessions for this user(이 사용자에 대한 모든 RA VPN 세션 종료)** 링크를 클릭합니다.

ASA에 대한 원격 액세스 VPN 구성

ASA에서는 사용자에게 비공개 연결로 표시되는 TCP/IP 네트워크(예를 들어 인터넷)를 통해 보안 연결을 생성하여 VPN(Virtual Private Network)을 생성합니다. 단일 사용자-LAN(single-user-to-LAN) 연결 및 LAN-to-LAN 연결을 만들 수 있습니다.

보안 연결을 터널이라고 하며, ASA에서는 터널링 프로토콜을 사용하여 보안 파라미터를 협상하고, 터널을 생성하고 관리하며, 패킷을 캡슐화하고, 터널을 통해 패킷을 전송하거나 수신하고, 패킷의 캡슐화를 해제합니다. ASA에서는 양방향 터널 엔드포인트로서의 기능을 수행합니다. 플레인 패킷을 수신하고, 이를 캡슐화한 다음, 해당 패킷의 캡슐화가 해제되고 최종 대상으로 전송되는 터널의 다른 쪽 끝에 패킷을 전송합니다. ASA에서는 캡슐화된 패킷을 수신하고 해당 패킷의 캡슐화를 해제한 후 이를 최종 대상으로 전송할 수도 있습니다.

CDO는 새로운 RA VPN(Remote Access Virtual Private Network)을 구성하기 위한 직관적인 사용자 인터페이스를 제공합니다. 또한 CDO에 온보딩된 여러 ASA(Adaptive Security Appliance) 디바이스에 대한 RA VPN 연결을 쉽고 빠르게 구성할 수 있습니다.

CDO를 사용하면 ASA 디바이스에서 RA VPN 구성을 처음부터 구성할 수 있습니다. 또한 ASDM(Adaptive Security Defense Manager) 또는 CSM(Cisco Security Manager)과 같은 다른 ASA 관리 도구를 사용하여 이미 구성된 RA VPN 설정을 관리할 수 있습니다. 이미 RA VPN 설정이 있는 ASA 디바이스를 온보딩하는 경우 CDO는 자동으로 "기본 RA VPN 구성"을 생성하고 ASA 디바이스를 이

구성과 연결합니다. 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다. CDO로 읽히는 RAVPN 속성을 이해하려면 [온보딩된 ASA 디바이스의 RA VPN 구성 읽기](#) 섹션을 참조하십시오. 그렇지 않으면 "ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스" 섹션에 설명된 단계를 수행할 수 있습니다.

관련 정보:

- [ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스](#)
 - [ASA에 대한 ID 소스 구성](#)
 - [ASA Active Directory 영역 개체 생성 또는 편집](#)
 - [ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)
 - [새 ASA RA VPN 그룹 정책 생성, on page 138](#)
 - [ASA RA VPN 구성 생성, on page 146](#)
 - [ASA RA VPN 연결 프로파일 구성, on page 150](#)
- [온보딩된 ASA 디바이스의 RA VPN 구성 읽기](#)
- [IP 주소 풀 생성](#)
- [NAT에서 원격 액세스 트래픽 제외, on page 166](#)
- [ASA의 원격 액세스 VPN 구성 확인](#)
- [ASA의 원격 액세스 VPN 구성 세부 정보 보기](#)

ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스

이 섹션에서는 CDO에 온보딩된 ASA 디바이스에서 RA VPN(Remote Access Virtual Private Network)을 구성하는 엔드 투 엔드 절차를 제공합니다.

클라이언트에 대한 원격 액세스 VPN을 활성화하려면 여러 개의 개별 항목을 구성해야 합니다. 다음 절차에서는 이러한 엔드 투 엔드 프로세스를 제공합니다.

단계 1 원격 사용자 인증에 사용되는 ID 소스를 구성합니다. 자세한 내용은 [ASA에 대한 ID 소스 구성](#)을 참조하십시오.

다음 소스를 사용하여 RA VPN을 사용하여 네트워크에 연결을 시도하는 사용자를 인증할 수 있습니다. 또한 인증을 위해 클라이언트 인증서를 단독으로 또는 ID 소스와 함께 사용할 수 있습니다.

- **AD(Active Directory) ID 영역:** 기본 인증 소스로 사용됩니다. AD(Active Directory) 서버에서 사용자 어카운트가 정의됩니다. AD ID 영역 구성을 참조하십시오. [ASA Active Directory 영역 개체 생성 또는 편집](#)을 참조하십시오.
- **RADIUS 서버 그룹:** 기본 또는 보조 인증 소스로서, 권한 부여 및 계정 관리를 위한 것입니다. [ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)을 참조하십시오.
- **Local Identity Source(로컬 사용자 데이터베이스):** 기본 또는 대체 소스로 사용됩니다. 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부서

버에 설명한 것과 같은 사용자 이름/비밀번호를 정의해야 합니다. 참고: ASDM(Adaptive Security Device Manager)에서만 ASA 디바이스에서 직접 사용자 계정을 생성할 수 있습니다. [Cisco ASA Series Firewall ASDM 구성 가이드, XY의 개체 액세스 제어](#) 장에서 "로컬 사용자 그룹 구성" 섹션을 참조하십시오.

단계 2 (선택 사항) 새 ASA RA VPN 그룹 정책 생성, on page 138. 그룹 정책에서는 사용자와 관련된 속성을 정의합니다. 그룹 멤버십에 근거하여 리소스에 차등 액세스를 제공하도록 그룹 정책을 구성할 수 있습니다. 또는 모든 연결에 기본 정책을 사용합니다.

단계 3 ASA RA VPN 구성 생성, on page 146.

단계 4 ASA RA VPN 연결 프로파일 구성, on page 150.

단계 5 (선택 사항) NAT에서 원격 액세스 트래픽 제외, on page 166.

단계 6 CDO에서 ASA로 구성 변경 사항 구축.

Important ASDM(Adaptive Security Device Manager)과 같은 로컬 관리자를 사용하여 원격 액세스 VPN 구성을 변경하면 CDO에서 해당 디바이스의 구성 상태가 "Conflict Detected(충돌 탐지됨)"로 표시됩니다. [디바이스의 대역 외 변경 사항](#)을 참조하십시오. 이 ASA에서 [구성 충돌 해결](#)할 수 있습니다.


What to do next

다음 단계

RA VPN 구성이 ASA 디바이스에 다운로드되면 사용자는 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 테넌트의 모든 온보딩된 ASA RA VPN 헤드엔드에서 라이브 AnyConnect RA VPN(Remote Access RA VPN) 세션을 모니터링할 수 있습니다. [원격 액세스 가상 프라이빗 네트워크 세션](#)을 참조하십시오.

ASA에 대한 ID 소스 구성

Microsoft Active Directory(AD) 영역 및 RADIUS 서버와 같은 ID 소스는 조직 내 사용자의 사용자 계정을 정의하는 AAA 서버 및 데이터베이스입니다. IP 주소와 연결된 사용자 ID를 제공하거나 원격 액세스 VPN 연결 또는 CDO에 대한 액세스를 인증하는 등 다양한 방법으로 이 정보를 사용할 수 있습니다.

Objects(개체) > FTD Network Objects(FTD 네트워크 개체)를 클릭한 다음  **> Identity Source(ID 소스)**를 클릭하여 소스를 생성합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다. 적절한 필터를 적용하여 기존 소스를 검색하고 관리할 수 있습니다.

디렉터리 기본 DN 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.



Note 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우 도메인 관리자로 Active Directory 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 부분 이름 "John*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 그룹 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

ADSI 편집 프로그램을 사용하여 Active Directory 구조를 찾을 수도 있습니다(**Start(시작) > Run(실행) > adsiedit.msc**). ADSI 편집에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로 클릭하고 **Properties(속성)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

단계 1 디렉터리 속성의 Test Connection(연결 테스트) 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.

단계 2 디바이스에 변경 사항을 커밋합니다.

단계 3 액세스 규칙을 생성하고 **Users(사용자)** 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 편집해야 합니다.

What to do next

자세한 내용은 [ASA Active Directory 영역 개체 생성 또는 편집](#)을 참조하십시오.

RADIUS 서버 및 그룹

RADIUS 서버를 사용하여 관리 사용자를 인증하고 권한을 부여할 수 있습니다. RADIUS 서버를 사용하도록 기능을 구성할 때는 개별 서버 대신 RADIUS 그룹을 선택합니다. RADIUS 그룹은 서로의 복사본인 RADIUS 서버가 모인 컬렉션입니다. 그룹에 서버가 여러 개 포함된 경우 이러한 서버는 백업 서버 체인을 형성하여 한 서버를 사용할 수 없는 경우 이중화를 제공합니다. 하지만 서버가 하나뿐이더라도 멤버가 하나인 그룹을 생성하여 기능에 대한 RADIUS 지원을 구성해야 합니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 인증용 ID 소스이자 권한 부여 및 과금 용도의 원격 액세스 VPN. AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

자세한 내용은 [ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)을 참조하십시오.

ASA Active Directory 영역 개체 생성 또는 편집

AD 영역 개체와 같은 ID 소스 개체를 생성하거나 편집할 때 CDO는 SDC를 통해 ASA 디바이스에 구성 요청을 보냅니다. 그런 다음 ASA는 구성된 AD 영역과 통신합니다.

개체를 생성하려면 다음 절차를 따르십시오.

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > ASA Objects(ASA 개체)**를 클릭합니다.
- 단계 2 **Create Object(개체 생성)** (+) **RA VPN Objects(개체) (ASA & FDM) > Identity Source(ID 소스)**를 클릭합니다.
- 단계 3 개체의 **Object name(개체 이름)**을 입력합니다.
- 단계 4 **Device Type(장치 유형)**을 **ASA**로 선택합니다.
- 단계 5 마법사의 첫 번째 부분에서 **ID 소스 유형**으로 **Active Directory** 영역을 선택합니다. **Continue(계속)**를 클릭합니다.
- 단계 6 기본 영역 속성을 구성합니다.

- 디렉터리 사용자 이름, 디렉터리 암호- 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유한 사용자 이름과 암호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 정규화되어야 합니다. 예를 들어 [Administrator@example.com](#)(단순히 Administrator가 아님)입니다.

참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 [Administrator@example.com](#)은 cn=adminstrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환의 일부이므로 여기에서 일반 이름 "users" 폴더 아래에 지정하는 사용자를 구성해야 합니다.

- **Base Distinguished Name(기본 고유 이름)** - 사용자 및 그룹 정보를 검색하거나 조회하기 위한 디렉토리 트리, 즉 사용자 및 그룹의 공통 상위. cn=users,dc=example,dc=com을 예로 들 수 있습니다.

- 단계 7 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(호스트 이름/IP 주소)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.

- **Port(포트)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
 - 암호화- 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려면 **LDAPS**를 선택하여 SSL을 사용하여 ASA와 LDAP 서버 간의 통신을 보호합니다. SSL을 통한 LDAP가 필요합니다. 이 옵션은 포트 636을 사용합니다.
- 기본값은 **None(없음)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.

단계 8 (선택 사항) **Test(테스트)** 버튼을 사용하여 구성을 확인합니다.

단계 9 (선택 사항) AD(Active Directory) 영역에 여러 AD 서버를 추가하려면 **Add another configuration(다른 구성 추가)**를 클릭합니다. 이 AD 서버들은 서로의 중복이어야 하고 동일한 AD 도메인을 지원해야 합니다. 따라서 디렉터리 이름, 디렉터리 암호 및 기본 고유 이름과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다.

단계 10 **Add(추가)**를 클릭합니다.


ASA Active Directory 영역 개체 편집

ID 소스 개체를 편집할 때는 ID 소스 유형을 변경할 수 없습니다. 올바른 유형으로 새 개체를 생성해야 합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > ASA Objects(ASA 개체)**을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 편집할 개체를 선택합니다.

단계 4 세부정보 패널의 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 5 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 편집합니다. 아래 나열된 구성 표시줄을 확장하여 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트합니다.

단계 6 **Save(저장)**를 클릭합니다.

단계 7 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 8 지금 변경 사항을 **CDO에서 ASA로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집


RADIUS 서버 개체 또는 RADIUS 서버 개체 그룹과 같은 ID 소스 개체를 생성하거나 편집할 때 CDO는 SDC를 통해 구성 요청을 ASA 디바이스로 보냅니다.

RADIUS 서버 개체 생성

RADIUS 서버는 AAA(인증, 권한 부여 및 계정 관리) 서비스를 제공합니다.

개체를 생성하려면 다음 절차를 따르십시오.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > ASA Objects(ASA 개체)**를 클릭합니다.

단계 2 **Create Object(개체 생성)** () > **RA VPN Objects(개체) (ASA & FDM) > Identity Source(ID 소스)**를 클릭합니다.

단계 3 개체의 **Object name(개체 이름)**을 입력합니다.

단계 4 **Device Type(장치 유형)**을 **ASA**로 선택합니다.

단계 5 ID 소스 유형으로 **RADIUS Server Group(RADIUS 서버 그룹)**을 선택합니다. **Continue(계속)**를 클릭합니다.

단계 6 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- **Server Name or IP Address(서버 이름 또는 IP 주소)** - 서버의 정규화된 호스트 이름(FQDN) 또는 IP 주소입니다.
- **Authentication Port(인증 포트)(선택 사항)** - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- **Timeout(시간 제한)** - 시스템이 다음 서버로 요청을 보내기 전까지 서버의 응답을 기다리는 시간(1~300초)입니다. 기본값은 10초입니다.
- **Server Secret Key(서버 비밀 키)입력(선택 사항)** - ASA 디바이스와 RADIUS 서버 간에 데이터를 암호화하는데 사용되는 공유 비밀입니다. 이 키는 대/소문자를 구분하며 공백은 포함하지 않는 영숫자 문자열(최대 64자)입니다. 또한 영숫자 문자 또는 밑줄로 시작해야 하며 특수 문자 \$ & - _ . + @는 포함할 수 없습니다. 문자열은 RADIUS 서버에 구성된 것과 일치해야 합니다. 비밀 키를 구성하지 않으면 연결이 암호화되지 않습니다.

단계 7 **Add(추가)**를 클릭합니다.


단계 8 지금 변경 사항을 **CDO에서 ASA로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

RADIUS 서버 그룹 생성

RADIUS 서버 그룹은 하나 이상의 RADIUS 서버 개체를 포함합니다. 그룹 내의 서버는 서로의 복사본이어야 합니다. 이러한 서버는 백업 서버 체인을 형성하므로 첫 번째 서버를 사용할 수 없는 경우 시스템이 목록의 다음 서버 사용을 시도할 수 있습니다.

개체 그룹을 생성하려면 다음 절차를 따르십시오.

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > ASA Objects(ASA 개체)**를 클릭합니다.

단계 2 **Create Object(개체 생성)** () **RA VPN Objects(개체) (ASA & FDM)Identity Source(ID 소스)**를 클릭합니다.

단계 3 개체의 **Object name(개체 이름)**을 입력합니다.

단계 4 **Device Type(장치 유형)**을 **ASA**로 선택합니다.

단계 5 ID 소스 유형으로 **RADIUS Server (RADIUS 서버) Group(그룹)**을 선택합니다. **Continue(계속)**를 클릭합니다.

단계 6 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- **데드 타임** - 실패한 서버는 모든 서버가 실패한 후에만 재활성화됩니다. 데드 시간은 모든 서버를 다시 활성화하기 전에 마지막 서버가 실패한 후 대기하는 시간입니다.

- **Maximum Failed Attempts**(최대 실패 시도 횟수) - 다음 서버 사용을 시도하기 전에 그룹의 RADIUS 서버로 전송되었으나 실패한 요청(즉, 응답을 받지 못한 요청)의 수입니다. 최대 실패 시도 횟수가 초과되면 시스템에서 해당 서버를 Failed(장애 발생)로 표시합니다. 특정 기능에 대해 로컬 데이터베이스를 사용하여 대체 방법을 구성했는데 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 방법을 시도합니다. 서버 그룹은 데드 타임 동안 응답하지 않는 것으로 표시된 상태를 유지하므로 해당 기간 내의 추가 AAA 요청은 서버 그룹에 연결을 시도하지 않으며 폴백 방법이 즉시 사용됩니다.
- **Dynamic Authorization/Port**(동적 인증/포트) (선택사항) - RADIUS 동적 인증 또는 이 RADIUS 서버 그룹에 대한 CoA(Change of Authorization) 서비스를 활성화할 경우, 해당 그룹은 CoA 알림이 등록되며 Cisco ISE(Identity Services Engine)의 CoA 정책 업데이트를 위해 지정된 포트를 수신합니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

단계 7 드롭다운 메뉴에서 RADIUS 서버를 지원하는 AD 영역을 선택합니다. AD 영역을 아직 생성하지 않은 경우 드롭다운 메뉴에서 **Create**(생성)를 클릭합니다.

단계 8 기존 RADIUS 서버 개체를 추가하려면 **RADIUS SERVER Add**(RADIUS 서버 추가)  버튼을 클릭합니다. 선택 사항으로 이 창에서 새 RADIUS 서버 개체를 만들 수 있습니다.

Note 목록의 첫 번째 서버가 응답하지 않을 때까지 사용되므로 이러한 개체를 우선 순위에 추가하십시오. 그런 다음 ASA는 목록의 다음 서버로 기본 설정됩니다.

단계 9 지금 변경 사항을 **CDO에서 ASA로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.


RADIUS 서버 개체 또는 그룹 편집

Radius 서버 개체 또는 Radius 서버 그룹을 편집하려면 다음 절차를 따르십시오.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **ASA Objects**(ASA 개체)을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 편집할 개체를 선택합니다.

단계 4 세부정보 패널의 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 5 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다. 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트하려면 구성 표시줄을 확장합니다.

단계 6 **Save**(저장)를 클릭합니다.

단계 7 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 8 지금 변경 사항을 **CDO에서 ASA로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

새 ASA RA VPN 그룹 정책 생성

그룹 정책은 원격 액세스 VPN 연결을 위한 사용자 중심 속성/값 쌍의 집합입니다. 연결 프로파일은 터널이 설정된 이후에 사용자 연결을 위한 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사

용하면 각 사용자에게 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

시스템에는 "DfltGrpPolicy"라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.



참고 일치하지 않는 그룹 정책 개체를 RA VPN 구성에 추가할 수 없습니다. RA VPN 구성 그룹 정책을 추가하기 전에 모든 불일치를 해결하십시오.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FTD Network Objects(FTD 네트워크 개체)**을 클릭합니다.

단계 2 파란색 더하기  버튼을 클릭합니다.

단계 3 **RA VPN Objects (ASA & FTD)(RA VPN 개체 (ASA 및 FDM)) > RA VPN Group Policy(RA VPN 그룹 정책)**를 클릭합니다.

단계 4 그룹 정책의 이름을 입력합니다. 이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다.

단계 5 **Device Type(디바이스 유형)** 드롭다운에서 **ASA**를 선택합니다.

단계 6 다음 중 하나를 수행합니다.

- 필요한 탭을 클릭하고 페이지에서 속성을 구성합니다.

- [ASA RA VPN 그룹 정책 속성](#)
- [AnyConnect 클라이언트 프로파일, 140 페이지](#)
- [세션 설정 속성, 141 페이지](#)
- [주소 할당 속성, 141 페이지](#)
- [스플릿 터널링 속성, 142 페이지](#)
- [AnyConnect 속성, 143 페이지](#)
- [트래픽 필터 속성, 145 페이지](#)
- [Windows 브라우저 프록시 속성, 145 페이지](#)

단계 7 **Save(저장)**를 클릭하여 그룹 정책을 생성합니다.

ASA RA VPN 그룹 정책 속성

이 섹션에서는 ASA RA VPN 그룹 정책과 관련된 속성에 대해 설명합니다.

일반 속성

그룹 정책의 일반 속성에서는 그룹의 이름 및 기타 기본 설정을 정의합니다.

- **DNS Server(DNS 서버)**: VPN에 연결된 경우 도메인 이름 확인을 위한 DNS 서버의 IP 주소를 입력합니다. 쉼표를 사용하여 주소를 구분할 수 있습니다.
- **Banner(배너)**: 로그인 시 사용자에게 표시할 배너 텍스트 또는 환영 메시지입니다. 기본값은 배너 없음입니다. 길이는 최대 496자까지 가능합니다. AnyConnect 클라이언트에서는 부분 HTML을 지원합니다. 원격 사용자에게 배너가 적절히 표시되게 하려면
 태그를 사용하여 줄 바꿈을 나타냅니다.
- **Default Domain(기본 도메인)**: RA VPN의 사용자에게 대한 기본 도메인 이름입니다. example.com 등을 예로 들 수 있습니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com)이 아닌 serverA)에 추가됩니다.

AnyConnect 클라이언트 프로파일

이 기능은 소프트웨어 버전 6.7 이상을 실행하는 FTD에서 지원됩니다.

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.

VPN 사용자가 VPN AnyConnect 클라이언트 소프트웨어를 다운로드할 때 클라이언트에 다운로드할 AnyConnect VPN 프로파일 개체 및 AnyConnect 모듈을 선택할 수 있습니다.

1. AnyConnect VPN 프로파일 개체를 선택하거나 생성합니다. [RA VPN AnyConnect 클라이언트 프로파일 업로드](#), on page 169의 내용을 참조하십시오. DART 및 Start Before Login(로그인 전 시작) 모듈을 제외하고 AnyConnect VPN 프로파일 개체를 선택해야 합니다.
2. **Add Any Connect Client Module**(모든 연결 클라이언트 모듈 추가)을 클릭합니다.

다음 AnyConnect 모듈은 선택 사항이며 이러한 모듈을 VPN AnyConnect 클라이언트 소프트웨어와 함께 다운로드하도록 구성할 수 있습니다.

- **AMP Enabler** — 엔드포인트용 AMP(Advanced Malware Protection)를 구축합니다.
- **DART** — 시스템 로그 및 기타 진단 정보를 캡처하여 데스크톱에 .zip 파일을 만듭니다. 따라서 편리하게 Cisco TAC로 문제 해결 정보를 보낼 수 있습니다.
- **Feedback**(피드백) - 고객이 활성화하고 사용한 기능 및 모듈에 대한 정보를 제공합니다.
- **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 로그인하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.

- **Umbrella** 로밍 보안 — 활성화 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.

3. 클라이언트 모듈 목록에서 **AnyConnect** 모듈을 선택합니다.
4. **Profile**(프로파일) 목록에서 AnyConnect 클라이언트 프로파일을 포함하는 프로파일 개체를 선택하거나 생성합니다.
5. 프로파일과 함께 클라이언트 모듈을 다운로드하려면 **Enable Module Download**(모듈 다운로드 활성화)를 선택하여 엔드포인트를 활성화합니다. 선택하지 않으면 엔드포인트는 클라이언트 프로파일만 다운로드할 수 있습니다.

세션 설정 속성

그룹 정책의 세션 설정에서는 사용자가 VPN을 통해 연결할 수 있는 시간과 설정할 수 있는 별도 연결의 개수를 제어합니다.

- **Maximum Connection Time**(최대 연결 시간): 사용자가 로그아웃했다가 다시 연결하지 않고 VPN에 연결된 상태를 유지할 수 있는 최대 시간을 1~4473924(분)로 입력하거나 비워 둡니다. 기본값은 무제한(비워 둠)이지만 유희 시간 제한은 계속 적용됩니다.
- **Connection Time Alert Interval**(연결 시간 알림 간격): 최대 연결 시간을 지정하는 경우, 알림 간격에서는 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 최대 시간을 정의합니다. 사용자는 연결 종료를 선택하고 다시 접속해 타이머를 다시 시작할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Idle Time**(유희 시간): VPN 연결이 자동으로 종료될 때까지 유희 상태일 수 있는 시간을 1~35791394(분) 범위 내로 입력합니다. 이 연속되는 분 단위 시간 동안 연결에서 통신 활동이 없는 경우, 시스템에서는 연결을 중지합니다. 기본값은 30분입니다.
- **Idle Time Alert Interval**(유희 시간 알림 간격): 유희 세션으로 인해 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 유희 시간입니다. 어떤 활동에서도 타이머를 재설정할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Simultaneous Login Per User**(사용자당 동시 로그인 수): 한 사용자에게 허용되는 동시 연결의 최대 개수입니다. 기본값은 3입니다. 1~2147483647개의 연결을 지정할 수 있습니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

주소 할당 속성

그룹 정책의 주소 할당 속성에서는 그룹에 대해 IP 주소 풀을 정의합니다. 여기에 정의된 풀은 이 그룹을 사용하는 모든 연결 프로파일에 정의된 풀을 재정의합니다. 연결 프로파일에 정의된 풀을 사용하려면 이러한 설정을 비워둡니다.

- **IPv4 Address Pool**(IPv4 주소 풀), **IPv6 Address Pool**(IPv6 주소 풀): 이 옵션에서는 원격 엔드포인트의 주소 풀을 정의합니다. 클라이언트가 VPN 연결을 설정하는 데 사용하는 IP 버전에 따라 이러한 풀의 주소가 클라이언트에 할당됩니다. 지원하려는 각 IP 유형에 대한 서브넷을 정의하

는 IP 주소 풀을 선택합니다. 해당 IP 버전을 지원하고 싶지 않은 경우, 목록을 비워두십시오. 예를 들어 IPv4 풀을 10.100.10.0/24로 정의할 수 있습니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다. 새 **IP 주소 풀 생성**을 생성합니다. 로컬 주소 할당에 사용할 최대 6개의 주소 풀로 구성된 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 시스템에서는 풀이 표시되는 순서에 따라 이 풀에서 주소를 할당합니다. 참고: 동일한 그룹 정책에 대해 IPv4 주소 풀과 IPv6 주소 풀을 둘 다 구성할 수 있습니다. 동일한 그룹 정책에 두 버전의 IP 주소가 모두 구성된 경우 IPv4에 대해 구성된 클라이언트는 IPv4 주소를 가져오고 IPv6에 대해 구성된 클라이언트는 IPv6 주소를 가져오며 IPv4 주소와 IPv6 주소 둘 다에 대해 구성된 클라이언트는 IPv4 주소와 IPv6 주소를 둘 다 가져옵니다.

- **DHCP Scope(DHCP 범위):** 연결 프로파일에서 주소 풀에 대한 DHCP 서버를 컨피그레이션하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 풀에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다. 네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순서로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다. 범위를 지정하려면 네트워크 번호 호스트 주소를 포함하는 네트워크 개체를 입력합니다. 예를 들어 192.168.5.0/24 서브넷 풀에서 주소를 사용하도록 DHCP 서버에 지시하려면 192.168.5.0을 호스트 주소로 지정하는 네트워크 개체를 입력하십시오. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다.

스플릿 터널링 속성

그룹 정책의 스플릿 터널링 속성에서는 내부 네트워크로 가는 트래픽과 외부로 가는 트래픽을 시스템에서 각각 분별하여 처리하는 방식을 정의합니다. 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.

일반적으로 원격 액세스 VPN에서는 VPN 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 VPN 사용자가 RA VPN에 연결되어 있는 동안 외부 네트워크에 액세스하도록 허용할 수 있습니다. 이 기술을 스플릿 터널링 또는 헤어피닝이라고도 합니다. 스플릿 터널을 이용하면 보안 터널을 통한 원격 네트워크 VPN 연결이 가능하며, VPN 터널 외부의 네트워크에도 연결할 수 있습니다. 스플릿 터널링은 FTD 디바이스의 네트워크 부하를 줄이고 외부 인터페이스의 대역폭을 늘립니다.

시작하기 전에

IPv4 네트워크에 대해 스플릿 터널 정책을 생성하고 IPv6 네트워크에 대해 다른 스플릿 터널 정책을 생성하는 경우, 지정한 액세스 목록이 두 가지 프로토콜 모두에 사용됩니다. 따라서 액세스 목록은 IPv4 및 IPv6 트래픽에 대한 ACE(Access Control Entries: 액세스 제어 항목)를 포함해야 합니다.

ASA 디바이스가 CDO에 온보딩되면 디바이스와 연결된 확장 ACL을 읽습니다. 자세한 내용은 [그룹 정책](#) 을 참조하십시오. 새 ACL을 생성하려면 [ASA 정책\(확장 액세스 목록\)](#) 을 참조하십시오.



Note 생성 중인 ACL에서 스플릿 터널링을 위한 네트워크를 소스 네트워크로 지정해야 합니다.

- **IPv4 Split Tunneling(IPv4 스플릿 터널링), IPv6 Split Tunneling(IPv6 스플릿 터널링):** 트래픽에서 IPv4와 IPv6 중 어떤 주소 지정을 사용하는지에 따라 다른 옵션을 지정할 수 있지만, 각각의 경우 옵션은 동일합니다. 스플릿 터널링을 활성화하려는 경우, 네트워크 개체를 선택해야 하는 옵션 중 하나를 지정합니다.
 - **Allow all traffic over tunnel(터널을 지나는 모든 트래픽 허용):** 스플릿 터널링은 실행하지 마십시오. 사용자가 RA VPN 연결을 하면 사용자의 모든 트래픽은 보호된 터널을 통과합니다. 이는 기본값입니다. 또한 이 기본값은 가장 안전한 옵션으로 간주됩니다.
 - **Allow specified traffic over the tunnel(터널을 통해 지정된 트래픽 허용):** 소스 네트워크를 정의하는 확장 액세스 목록을 선택합니다. 이러한 소스의 모든 트래픽은 보호된 터널을 통과합니다. 클라이언트는 다른 소스의 트래픽을 터널 외부의 연결(예: 로컬 Wi-Fi 또는 네트워크 연결)로 라우팅합니다.
 - **Exclude networks specified below(아래에 지정된 네트워크 제외):** 소스 네트워크를 정의하는 네트워크 개체를 선택합니다. 클라이언트는 이러한 소스의 모든 트래픽을 터널 외부의 연결로 라우팅합니다. 다른 소스의 트래픽은 터널을 통과합니다.
 - **Network List(네트워크 목록):** IPv4 및 IPv6 네트워크를 모두 포함할 수 있는 확장 ACL 네트워크를 선택합니다.
- **Split DNS(스플릿 DNS):** 보안 연결을 통해 일부 DNS 요청을 전송하도록 시스템을 구성함과 동시에 클라이언트가 클라이언트에 구성된 DNS 서버로 다른 DNS 요청을 전송하도록 허용할 수 있습니다. 다음 DNS 동작을 컨피그레이션할 수 있습니다.
 - **Send DNS Request as per split tunnel policy(스플릿 터널 정책에 따라 DNS 요청 전송):** 이 옵션을 사용하면 스플릿 터널 옵션을 정의하는 것과 동일한 방식으로 DNS 요청이 처리됩니다. 스플릿 터널링을 활성화하는 경우, DNS 요청은 대상 주소에 근거하여 전송됩니다. 스플릿 터널링을 활성화하지 않는 경우, 모든 DNS 요청은 보호된 연결을 경유해 전송됩니다.
 - **Always send DNS requests over tunnel(항상 터널을 통해 DNS 요청 전송):** 스플릿 터널링을 활성화하되 모든 DNS 요청을 보호된 연결을 경유해 그룹에 정의된 DNS 서버로 전송하려는 경우, 이 옵션을 선택합니다.
 - **Send only specified domains over tunnel(지정된 도메인만 터널을 통해 전송):** 보호된 DNS 서버에서 특정 도메인에 대해서만 주소를 확인하게 하고 싶은 경우, 이 옵션을 선택합니다. 그런 다음, 도메인 이름을 쉼표로 구분하여 해당 도메인을 지정합니다. example.com, example1.com을 예로 들 수 있습니다. 내부 DNS 서버에서는 내부 도메인의 이름을 확인하고 외부 DNS 서버에서는 다른 모든 인터넷 트래픽을 처리하게 하려는 경우, 이 옵션을 사용합니다.

AnyConnect 속성

그룹 정책의 AnyConnect 속성에서는 원격 액세스 VPN 연결에 대해 AnyConnect 클라이언트에서 사용하는 일부 SSL 및 연결 설정을 정의합니다.

- **SSL 설정**

- **Enable Datagram Transport Layer Security (DTLS)(DTLS(Datagram Transport Layer Security) 활성화):** AnyConnect 클라이언트에서 2개의 터널(SSL 터널 및 DTLS 터널)을 동시에 사용하도록 허용할지 여부를 선택합니다. DTLS를 사용하면 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다. DTLS를 활성화하지 않은 경우에는 SSL VPN 연결을 설정하는 AnyConnect 클라이언트 사용자가 SSL 터널만 사용하여 연결합니다.
- **DTLS Compression(DTLS 압축):** LZS를 사용하여 이 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.
- **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. 따라서 SSL 압축으로 인해 디바이스의 전체 처리량은 줄어듭니다.
- **SSL Rekey Method(SSL 키 재입력 방법), SSL Rekey Interval(SSL 키 재입력 간격):** 클라이언트는 VPN 연결에 키를 재입력하여 암호화 키 및 초기화 벡터를 재협상할 수 있어 연결 보안이 강화됩니다. **None(없음)**을 선택하여 키 재입력을 비활성화합니다. 키 재입력을 활성화하려면 **New Tunnel(새 터널)**을 선택하여 매번 새 터널을 생성합니다. (**Existing Tunnel(기존 터널)** 옵션을 선택하면 **New Tunnel(새 터널)**과 동일한 조치가 수행됩니다.) 키 재입력을 활성화하는 경우, 키 재입력 간격도 설정하십시오. 기본값은 4분입니다. 4~10080분(일주일) 범위 내에서 간격을 설정할 수 있습니다.

• 연결 설정

- **Ignore the DF (Don't Fragment) bit(DF(Don't Fragment) 비트 무시):** 단편화해야 하는 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. 이 옵션을 선택하면 DF 비트가 설정된 패킷의 강제 단편화가 허용되므로 이 패킷이 터널을 통과할 수 있습니다.
- **Client Bypass Protocol(클라이언트 우회 프로토콜):** 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 가정합니다. 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.

- **MTU:** Cisco AnyConnect VPN 클라이언트에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트입니다. 범위는 576~1462바이트입니다.

- **Keepalive Messages Between AnyConnect and VPN Gateway**(AnyConnect와 VPN 게이트웨이 간의 연결 유지 메시지): 피어 간에 연결 유지 메시지를 교환하여 터널에서 데이터를 송수신하는 데 사용할 수 있다는 것을 시연할지 여부를 선택합니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.
- **DPD on Gateway Side Interval**(게이트웨이 측 간격의 DPD), **DPD on Client Side Interval**(클라이언트 측 간격의 DPD): DPD(Dead Peer Detection)를 활성화하면 피어가 더 이상 응답하지 않을 경우 VPN 게이트웨이 또는 VPN 클라이언트를 신속하게 탐지할 수 있습니다. 게이트웨이 또는 클라이언트 DPD를 별도로 활성화할 수 있습니다. DPD 메시지 전송의 기본 간격은 30초입니다. 간격은 5-3600초 사이일 수 있습니다.

트래픽 필터 속성

그룹 정책의 트래픽 필터 속성에서는 그룹에 할당된 사용자에게 부과하고 싶은 제한 사항을 정의합니다. 액세스 제어 정책 규칙을 생성하는 대신 이 속성을 사용해 RA VPN 사용자를 호스트 또는 서브넷 주소 및 프로토콜, VLAN에 따라 특정 리소스로 제한할 수 있습니다. 기본적으로 그룹 정책에 따라 RA VPN 사용자는 보호된 네트워크의 어떤 대상에 액세스하는 것도 제한되지 않습니다.

- **Access List Filter**(액세스 목록 필터): 확장된 ACL(액세스 제어 목록)을 사용하여 액세스를 제한합니다. Smart CLI 확장 ACL 개체를 선택합니다. 확장 ACL을 통해 소스 주소, 대상 주소 및 프로토콜(예: IP 또는 TCP)을 기준으로 필터링할 수 있습니다. ACL은 하향식, 최초 일치 방식에 따라 평가되므로 특정 규칙이 다수의 일반 규칙보다 먼저 배치되도록 보장합니다. ACL의 끝에는 암목적 "deny any(모두 거부)"가 있으므로 서브넷 몇 개에 대한 액세스만 거부하고 다른 모든 액세스는 허용하려면 ACL의 끝에 "permit any(모두 허용)" 규칙을 포함하십시오. 확장 ACL 스마트 CLI 개체를 수정하는 중에는 네트워크 개체를 생성할 수 없으므로 그룹 정책을 수정하기 전에 ACL을 생성해야 합니다. 그러지 않는 경우, 개체만 생성할 수 있습니다. 그런 다음 다시 돌아가 네트워크 개체를 생성한 후 필요한 모든 액세스 제어 항목을 생성하면 됩니다. ACL을 생성하려면 FDM에 로그인하고 **Device**(디바이스) > **Advanced Configuration**(고급 구성) > **Smart CLI**(스마트 CLI) > **Objects**(개체)로 이동하여 개체를 생성하고 **Extended Access List**(확장 액세스 목록)를 개체 유형으로 선택합니다.
- **Restrict VPN to VLAN**(VPN을 VLAN으로 제한): “VLAN 매핑”이라고도 하는 이 속성에서는 이 그룹 정책이 적용되는 세션에 이그레스(egress) VLAN 인터페이스를 지정합니다. 시스템에서는 이 그룹에서 나오는 모든 트래픽을 선택한 VLAN으로 전달합니다. 이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 속성에 값을 할당하는 방법도 가능합니다. 디바이스에서 하위 인터페이스에 정의된 VLAN 번호를 반드시 지정하십시오. 값의 범위는 1에서 4094까지입니다.

Windows 브라우저 프록시 속성

그룹 정책의 Windows 브라우저 프록시 속성에서는 사용자의 브라우저에 정의된 프록시의 작동 방식과 작동 여부를 결정합니다.

Browser Proxy During VPN Session(VPN 세션 중 브라우저 프록시)에 대해 다음 값 중 하나를 선택할 수 있습니다.

- **No change in endpoint settings**(엔드포인트 설정에 변경 사항 없음): 이 옵션을 통해 사용자는 HTTP에 대해 브라우저 프록시를 컨피그레이션하거나 컨피그레이션하지 않을 수 있으며 컨피그레이션되어 있는 경우 프록시를 사용할 수 있습니다.
- **Disable browser proxy**(브라우저 프록시 비활성화): 브라우저에 대해 정의된 프록시(있는 경우)를 사용하지 않습니다. 이 경우 프록시를 통해 브라우저 연결이 설정되지 않습니다.
- **Auto detect settings**(설정 자동 탐지): 클라이언트 디바이스에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **Use custom settings**(사용자 정의 설정 사용): HTTP 트래픽에 대해 모든 클라이언트 디바이스에서 사용해야 하는 프록시를 정의합니다. 다음 설정을 구성합니다.
 - **Proxy Server IP or Hostname**(프록시 서버 IP 또는 호스트네임), **Port**(포트): 프록시 서버의 IP 주소 또는 호스트네임, 프록시 서버에서 프록시 연결에 사용하는 포트입니다. 호스트와 포트를 합해 100자를 초과할 수 없습니다.
 - **Browser Exemption List**(브라우저 면제 목록): 면제 목록의 호스트/포트에 대한 연결은 프록시를 통과하지 않습니다. 프록시를 사용해서는 안 되는 대상에 대해 모든 호스트/포트 값을 추가합니다. www.example.com port 80을 예로 들 수 있습니다. 목록에 항목을 추가하려면 **Add Proxy Exemption**(프록시 예외 추가)을 클릭합니다. 항목을 삭제하려면 휴지통 아이콘을 클릭합니다. 모든 주소와 포트를 합한 전체 프록시 예외 목록은 255자를 초과할 수 없습니다.

ASA RA VPN 구성 생성

CDO를 사용하면 하나 이상의 ASA(Adaptive Security Appliance) 디바이스를 RA VPN 구성 마법사에 추가하고 디바이스와 연결된 VPN 인터페이스, 액세스 제어 및 NAT 면제 설정을 구성할 수 있습니다. 따라서 각 RA VPN 구성에는 RA VPN 구성과 연결된 여러 ASA 디바이스에서 공유되는 연결 프로파일 및 그룹 정책이 있을 수 있습니다. 또한 연결 프로파일 및 그룹 정책을 생성하여 구성을 개선할 수 있습니다.

RA VPN 설정으로 이미 구성된 ASA 디바이스 또는 RA VPN 설정이 없는 새 디바이스를 온보딩할 수 있습니다. [ASA 디바이스 온보딩](#)를 참고하십시오. 이미 RA VPN 설정이 있는 ASA 디바이스를 온보딩하는 경우 CDO는 자동으로 "기본 RA VPN 구성"을 생성하고 ASA 디바이스를 이 구성과 연결합니다. 또한 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다. [온보딩된 ASA 디바이스의 RA VPN 구성 읽기](#)를 참조하십시오. CDO를 사용하면 기본 구성을 삭제할 수 있습니다.



중요

- 동일한 원격 액세스 VPN 구성에서 ASA 및 FTD 를 추가할 수 없습니다.
- ASA 디바이스는 두 개 이상의 RA VPN 구성을 가질 수 없습니다.

시작하기 전에

RA VPN 구성에 ASA 디바이스를 추가하려면 먼저 다음 사전 요구 사항을 충족해야 합니다.

- 라이선스 요구 사항

수출 통제 기능을 사용하려면 디바이스를 활성화해야 합니다.

ASA 디바이스의 라이선스 요약을 보려면 ASA 명령줄 인터페이스에서 `show license summary` 명령을 실행합니다. CDO ASA CLI 인터페이스를 사용하려면 [CDO 인터페이스에서 ASA CLI 사용](#)을 참조하십시오.

- 라이선스 요약에서 활성화된 수출 통제 기능의 예:

등록: 상태: REGISTERED 스마트 어카운트: Cisco SVS temp-request access licensing@cisco.com
내보내기 제어 기능: ALLOWED

마지막 갱신 시도: 없음

다음 갱신 시도: 2021년 6월 8일 09:46:22 UTC

VPN 구성을 생성하거나 편집하려면 '내보내기 제어 기능' 속성이 '허용됨' 상태여야 합니다.

이 속성이 '허용되지 않음' 상태인 경우 CDO는 VPN 구성을 생성하거나 편집하고 디바이스에서 RA VPN 구성을 허용하지 않을 때 오류 메시지('RA VPN은 수출 규격이 아닌 디바이스에 대해 구성할 수 없습니다.')를 표시합니다.

- 디바이스 ID 인증서

클라이언트와 ASA 디바이스 간의 SSL 연결을 인증하려면 인증서가 필요합니다. VPN 구성을 시작하려면 먼저 ASA 디바이스에 ID 인증서가 이미 있는지 확인합니다.

디바이스에 인증서가 있는지 여부를 확인하려면 ASA 명령줄 인터페이스에서 `show crypto CA Certificates` 명령을 실행합니다. CDO ASA CLI 인터페이스를 사용하려면 [CDO 인터페이스에서 ASA CLI 사용](#)을 참조하십시오.

ID 인증서가 없거나 새 인증서를 등록하려는 경우 CDO를 사용하여 ASA에 설치합니다. ASA 인증서 관리를 참조하십시오.

원격 액세스 VPN 컨텍스트에서 디지털 인증서의 사용은 [원격 액세스 VPN 인증서 기반 인증, 165 페이지](#)에 설명되어 있습니다.

- 외부 인터페이스.

외부 인터페이스는 ASA 디바이스에 이미 구성되어 있어야 합니다. 인터페이스를 구성하려면 ASDM 또는 ASA CLI를 사용해야 합니다. ASDM을 사용한 인터페이스 구성에 대해 알아보려면 [Cisco ASA Series General Operations CLI Configuration Guide, X.Y](#)의 "Interfaces" 책을 참조하십시오.

- AnyConnect 패키지를 다운로드하고 원격 서버에 업로드하십시오. 나중에 RA VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 서버에서 ASA로 AnyConnect 소프트웨어 패키지를 업로드하십시오. [ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리](#)를 참조하십시오.
- 보류 중인 구성 배포가 없습니다.
- 인증에 로컬 데이터베이스를 사용하는 경우 ASDM 또는 ASA CLI를 사용하여 로컬 데이터베이스에 사용자 계정을 추가합니다.


ASDM을 사용하여 사용자 계정을 추가하려면 [Cisco ASA Series VPN CLI 구성 가이드, X.Y](#)의 "AAA 서버 및 로컬 데이터베이스" 책에서 "로컬 데이터베이스에 사용자 계정 추가" 섹션을 참조하십시오.

ASA CLI를 사용하여 사용자 계정을 추가하려면, **username[username] password [password] privilege [priv_level] command.usernamepasswordpriv_level** 명령을 실행합니다.


- ASA 변경 사항은 CDO에 동기화됩니다.
 1. 왼쪽의 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭하고 동기화할 하나 이상의 ASA 디바이스를 검색합니다.
 2. 하나 이상의 디바이스를 선택한 다음 **Check for changes**(변경 사항 확인)를 클릭합니다. CDO는 하나 이상의 FTD 디바이스와 통신하여 변경 사항을 동기화합니다.
- RA VPN 구성 그룹 정책 개체가 일치합니다.
 - 일치하지 않는 모든 그룹 정책 개체는 RA VPN 구성에 추가할 수 없으므로 확인해야 합니다. 문제를 해결하거나 **Objects**(개체) 페이지에서 일치하지 않는 그룹 정책 개체를 제거합니다. 자세한 내용은 [중복 개체 문제 해결](#) 및 [불일치 개체 문제 해결](#)을 참조하십시오.

단계 1 [ASA 디바이스 온보딩](#).

단계 2 왼쪽의 CDO 탐색 모음에서 **VPN > ASA/FDM** 원격 액세스 VPN 구성을 클릭합니다.

단계 3 파란색 더하기  버튼을 클릭하여 새 RA VPN 구성을 생성합니다.

단계 4 원격 액세스 VPN 구성의 이름을 입력합니다.

단계 5 파란색 더하기  버튼을 클릭하여 ASA 디바이스를 구성에 추가합니다.

디바이스 세부 정보를 추가하고 디바이스와 연결된 네트워크 트래픽 관련 권한을 구성할 수 있습니다.

1. 다음 디바이스 세부 사항을 입력합니다.

- 디바이스: 추가할 ASA 디바이스를 선택하고 **Select**(선택)를 클릭합니다. 중효동일한 원격 액세스 VPN 구성에서 ASA 및 FTD를 추가할 수 없습니다.
- **Certificate of Device Identity**(디바이스 ID의 인증서): 디바이스의 ID를 설정하는 데 사용되는 내부 인증서를 선택합니다. 그러면 AnyConnect 클라이언트가 디바이스에 연결할 때 디바이스 ID를 설정합니다. 보안 VPN 연결을 완료하려면 클라이언트가 이 인증서를 허용해야 합니다.
- **Outside Interface**(외부 인터페이스): 원격 액세스 VPN 연결 시 사용자가 연결할 인터페이스를 선택합니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 이 연결 프로파일을 사용하여 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.

주의 수출 규격이 아닌 디바이스에 대한 RA VPN 구성을 생성하거나 편집할 수 없습니다. 수출 통제 기능이 활성화된 ASA 디바이스에 라이선스를 부여하고 다시 시도해야 합니다.

2. **Continue**(계속)를 클릭하여 트래픽 권한을 구성합니다.

- **Bypass Access Control policy for decrypted traffic**(암호 해독된 트래픽에 대해 액세스 제어 정책 우회)(**sysopt permit-vpn**): 암호 해독된 트래픽은 기본적으로 액세스 제어 정책 검사를 받습니다. 이 옵션을 활성화하면 암호 해독된 트래픽 옵션이 액세스 제어 정책 검사를 무시하지만, VPN 필터 ACL과 AAA 서버에서 다운로드한 인증 ACL이 VPN 트래픽에 계속 적용됩니다.

이 옵션을 선택하는 경우, 시스템에서는 전역 설정인 `sysopt connection permit-vpn` 명령을 구성한다는 점에 유의하십시오. 이로 인해 Site-to-Site VPN 연결의 동작도 영향을 받습니다.

이 옵션을 선택하지 않는 경우, 외부 사용자가 원격 액세스 VPN 주소 풀의 IP 주소를 스누핑할 수 있고, 따라서 네트워크에 액세스할 수 있습니다. 이것이 가능한 이유는 주소 풀에서 내부 리소스에 액세스할 수 있게 허용하는 액세스 제어 규칙을 생성해야 하기 때문입니다. 액세스 제어 규칙을 사용하는 경우, 소스 IP 주소만 사용하기보다 사용자 사양을 이용해 액세스를 제어하는 것이 좋습니다.

이 옵션을 선택할 경우의 단점은 VPN 트래픽이 검사되지 않는다는 것입니다. 즉 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

- **NAT 제외(Exempt)**: NAT 제외는 주소 변환을 제외하고 변환된 호스트와 원격 호스트가 모두 보호되는 호스트와의 연결을 시작할 수 있도록 허용합니다. NAT 제외를 구성하여 NAT 변환에서 원격 액세스 VPN 엔드포인트로 오가는 트래픽을 제외합니다. [NAT에서 원격 액세스 트래픽 제외, 166 페이지](#)의 내용을 참조하십시오.

3. 확인을 클릭합니다.

AnyConnect Packages Detected(감지된 **AnyConnect** 패키지)는 디바이스에서 이미 사용 가능한 AnyConnect 패키지를 표시합니다.

RA VPN 마법사에서 AnyConnect 패키지를 ASA에 업로드하는 두 가지 옵션이 있습니다.

- (방법 1): CDO 저장소에서 패키지를 선택합니다. ASA는 인터넷에 액세스할 수 있어야 합니다.
- (방법 2): AnyConnect 패키지가 사전 로드된 ftp/http/https/scp/smb/tftp URL 위치를 지정합니다.

지침은 [ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리](#)를 참조하십시오.

참고 참고: 기존 패키지를 교체하려면 [ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리](#)를 참조하십시오.

단계 6 OK(확인)를 클릭합니다.



ASA VPN 구성이 생성됩니다.

ASA RA VPN 구성 수정

기존 RA VPN 구성의 이름 및 디바이스 세부 정보를 수정할 수 있습니다.

단계 1 수정할 구성을 선택하고 **Actions**(작업) 아래에서 **Edit**(편집)를 클릭합니다.

- 필요한 경우 이름을 수정합니다.

- 디바이스를 추가하려면 파란색 더하기 버튼  을 클릭합니다.
 -  을 클릭하여 ASA 디바이스에서 다음을 수행합니다.
 - **Edit(편집)**를 클릭하여 기존 RA VPN 구성을 수정합니다.
 - **Remove(제거)**를 클릭하여 RA VPN 구성에서 ASA 디바이스를 제거합니다. 그룹 정책을 제외하고 해당 디바이스와 연결된 모든 연결 프로파일 및 RA VPN 설정이 삭제됩니다. 개체 페이지에서 그룹 정책을 명시적으로 제거할 수 있습니다.
- Note** ASA가 구성을 사용하는 유일한 디바이스인 경우 ASA를 제거할 수 없습니다. 또는 RA VPN 구성을 제거할 수 있습니다.

단계 2 CDO에서 ASA로 구성 변경 사항 구축.

What to do next

구성 또는 디바이스의 이름을 입력하여 Remote Access VPN 구성을 검색할 수도 있습니다.

관련 정보:

- [ASA RA VPN 연결 프로파일 구성, on page 150.](#)

ASA RA VPN 연결 프로파일 구성

원격 액세스 VPN 연결 프로파일에서는 외부 사용자가 AnyConnect 클라이언트를 사용하여 시스템에 VPN 연결을 할 수 있게 허용하는 특성을 정의합니다. 각 프로파일에서 정의하는 것은 사용자를 인증하는 데 사용되는 AAA 서버 및 인증서, 사용자에게 IP 주소를 할당하기 위한 주소 풀, 다양한 사용자 중심 속성을 정의하는 그룹 정책입니다.

여러 사용자 그룹에 가변적인 서비스를 제공해야 하는 경우 또는 다양한 인증 소스가 있는 경우, RA VPN 구성 내에 프로파일을 여러 개 생성합니다. 예를 들어 조직이 다른 인증 서버를 사용하는 다른 조직과 병합하는 경우, 해당 인증 서버를 사용하는 새 그룹에 대해 프로파일을 만들 수 있습니다.


RA VPN 연결 프로파일을 사용하면 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다.

시작하기 전에

[ASA RA VPN 구성 생성, 146 페이지.](#)

단계 1 CDO 탐색 창에서 **VPN > ASA/FDM Remote Access VPN Configuration(ASA/FDM 원격 액세스 VPN 구성)**를 클릭합니다. VPN 구성을 클릭하여 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지에 대한 요약 정보를 볼 수 있습니다.

참고 디바이스에 할당된 그룹 정책을 확인하려면 **Actions(작업)**에서 **Group Policies(그룹 정책)**를 클릭합니다. 연결 프로파일에 할당된 그룹 정책은 목록에 자동으로 추가되며 제거할 수 없습니다.

필요한 그룹 정책이 아직 없는 경우  을 클릭하고 목록에서 선택합니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다. 새 [ASA RA VPN 그룹 정책 생성, 138 페이지](#)을 참조하십시오.

단계 2 연결 프로파일을 클릭하고 오른쪽 사이드바의 **Actions(작업)** 아래에서 **Add Connection Profile(연결 프로파일 추가)**를 클릭합니다.

단계 3 기본 연결 속성을 구성합니다.

- **Connection Profile Name(연결 프로파일 이름):** 이 연결의 이름을 공백 없이 50자까지 입력합니다. 예를 들면 MainOffice를 입력합니다.

참고 여기서 입력하는 이름이 AnyConnect 클라이언트에서 사용자에게 표시되는 연결 목록에 나타납니다. 따라서 사용자가 쉽게 이해할 수 있는 이름을 선택해야 합니다.

- **Group Alias(그룹 별칭), Group URL(그룹 URL):** 별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. ASA 디바이스에 연결하는 경우, VPN 사용자는 연결 목록의 AnyConnect 클라이언트에서 별칭 이름을 선택할 수 있습니다. 연결 프로파일 이름이 그룹 별칭으로 자동 추가됩니다. 또한 원격 액세스 VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 그룹 URL의 목록을 구성할 수 있습니다. 사용자가 그룹 URL을 사용하여 연결하는 경우, 시스템에서는 URL과 일치하는 연결 프로파일을 자동으로 사용합니다. 이 URL은 설치된 AnyConnect 클라이언트가 아직 없는 클라이언트에서 사용됩니다. 그룹 별칭 및 URL을 필요한 만큼 추가하십시오. 이러한 별칭 및 URL은 디바이스에 정의된 모든 연결 프로파일 전반에 걸쳐 고유한 것이어야 합니다. 그룹 URL은 **https://**로 시작해야 합니다.

- 예를 들어 별칭 계약자 및 그룹 URL <https://ravpn.example.com/contractor>가 있을 수 있습니다. AnyConnect 클라이언트가 설치된 후 사용자는 연결의 AnyConnect VPN 드롭다운 목록에서 그룹 별칭을 선택하기만 하면 됩니다.

단계 4 기본 ID 소스를 구성하고, 선택적으로 보조 ID 소스를 구성합니다. 이 옵션을 통해 원격 사용자가 원격 액세스 VPN 연결을 활성화하기 위해 디바이스에 인증하는 방식을 결정합니다. 가장 간단한 방식은 AAA만 사용하여 AD 영역을 선택하거나 LocalIdentitySource를 사용하는 것입니다. **Authentication Type(인증 유형)**에는 다음과 같은 방식을 사용할 수 있습니다.

- **AAA Only(AAA만):** 사용자 이름 및 암호에 근거하여 사용자를 인증하고 사용자에게 권한을 부여합니다. 자세한 내용은 [연결 프로파일에 대해 AAA 구성, 152 페이지](#) 섹션을 참조하십시오.
- **Client Certificate Only(클라이언트 인증서만):** 클라이언트 디바이스 ID 인증서에 근거하여 사용자를 인증합니다. 자세한 내용은 [연결 프로파일에 대한 인증서 인증 구성](#)을 참조하십시오.
- **AAA and ClientCertificate(AAA 및 ClientCertificate):** 사용자 이름/암호와 클라이언트 디바이스 ID 인증서를 모두 사용합니다.


단계 5 클라이언트에 대해 주소 풀을 구성합니다. 주소 풀에서는 원격 클라이언트가 VPN 연결을 설정할 때 시스템에서 원격 클라이언트에 할당할 수 있는 IP 주소를 정의합니다. 자세한 내용은 [클라이언트 주소 풀 할당 구성](#)을 참조하십시오.

단계 6 **Continue(계속)**를 클릭합니다.

단계 7 목록에서 이 프로파일에 사용할 **Group Policy(그룹 정책)**를 선택하고 **Select(선택)**를 클릭합니다.

그룹 정책에서는 터널이 설정된 후에 사용자 연결에 대한 조건을 설정합니다. 시스템에는 'DfltGrpPolicy'라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다. [새 ASA RA VPN 그룹 정책 생성, 138 페이지](#)를 참조하십시오.

단계 8 Continue(계속)를 클릭합니다.

단계 9 요약을 검토합니다. 먼저 요약이 정확한지 확인합니다. AnyConnect 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악할 수 있습니다.  를 클릭하여 지침을 클립보드에 복사한 다음 사용자에게 배포합니다.

단계 10 Done(완료)를 클릭합니다.

단계 11 ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스의 5단계를 수행합니다.

연결 프로파일에 대해 AAA 구성

인증, 권한 부여, 계정 관리 (AAA) 서버에서는 사용자 이름과 암호를 사용하여 사용자에게 원격 액세스 VPN에 대한 액세스가 허용되어 있는지 확인합니다. RADIUS 서버를 사용하는 경우, 인증된 사용자들 사이에서 권한 부여 수준을 구별하여 보호받는 리소스에 대한 차등 액세스를 제공할 수 있습니다. 또한 RADIUS 계정 관리 서비스를 사용하여 사용량을 추적할 수 있습니다.

AAA를 구성하는 경우, 기본 ID 소스를 구성해야 합니다. 보조 및 대체 소스는 선택 사항입니다. 2단계 인증을 구현하려면 RSA 토큰 또는 듀오와 같은 보조 소스를 사용합니다.

기본 ID 소스 옵션

- 사용자 인증을 위한 기본 ID 소스: 인증은 일반적으로 액세스 권한이 부여되기 전에 사용자가 유효한 사용자 이름과 유효한 암호를 입력하도록 하여 사용자를 식별하는 방법을 제공합니다. 원격 사용자를 인증하는 데 사용되는 기본 ID 소스입니다. VPN 연결을 완료하려면 이 소스 또는 대체 소스(선택 사항)에서 최종 사용자를 정의해야 합니다. 다음 중 하나를 선택합니다.

- AD(Active Directory) ID 영역.
- Radius 서버 그룹.
- LocalIdentitySource(로컬 사용자 데이터베이스): 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다.

[ASA에 대한 ID 소스 구성](#)를 클릭하여 새 ID 소스를 생성할 수 있습니다.

- **Fallback Local Identity Source**(대체 로컬 ID 소스): 기본 소스가 외부 서버인데 기본 서버를 사용할 수 없는 경우, 대체 소스로 LocalIdentitySource를 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 로컬 사용자 이름/비밀번호를 정의해야 합니다.
- **Strip options**(제거 옵션): 영역은 관리 도메인입니다. 다음 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구분 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.
 - **Strip Identity Source Server from Username**(사용자 이름에서 ID 소스 서버 제거): AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 ID 소스 이름을 제거할지 여부. 예를 들

이 옵션을 선택하고 사용자가 사용자 이름으로 `domain\username`을 입력하면 도메인이 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 제거할지 여부. 이 옵션은 `username@domain` 형식에서 지정된 이름에 적용되며, 도메인 및 @ 기호를 제거합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

보조 ID 소스

- **Secondary Identity Source for User Authorization**(사용자 권한 부여를 위한 보조 ID 소스): 두 번째 ID 소스로서 선택 사항입니다. 사용자가 기본 소스로 인증에 성공하는 경우, 사용자에게 보조 소스를 사용해 인증하라는 메시지가 표시됩니다. AD 영역, RADIUS 서버 그룹 또는 로컬 ID 소스를 선택할 수 있습니다.
- **Advanced options**(고급 옵션): **Advanced**(고급) 링크를 클릭하고 다음 옵션을 구성합니다.
 - **Fallback Local Identity Source for Secondary**(보조용 대체 시스템 로컬 ID 소스): 보조 소스가 외부 서버인데 보조 서버를 사용할 수 없는 경우, `LocalIdentitySource`를 대체 소스로 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우, 보조 외부 서버에 정의한 것과 같은 로컬 사용자 이름/암호를 정의해야 합니다.
 - **Use Primary Username for Secondary Login**(보조 로그인에 기본 사용자 이름 사용): 보조 ID 소스를 사용하는 경우, 시스템에서는 기본적으로 보조 소스에 대한 사용자 이름 및 암호를 모두 입력하라는 메시지를 표시합니다. 이 옵션을 선택하는 경우, 시스템에서는 보조 암호만 입력하라는 메시지를 표시하고 기본 ID 소스에 대해 인증된 보조 소스에 동일한 사용자 이름을 사용합니다. 기본 및 보조 ID 소스 모두에서 동일한 사용자 이름을 구성하는 경우, 이 옵션을 선택합니다.
 - **Username for Session Server**(세션 서버의 사용자 이름): 인증에 성공하면 사용자 이름이 이벤트 및 통계 대시보드에 표시되고, 이 이름은 사용자 또는 그룹 기반 SSL 암호 해독 및 액세스 제어 규칙에 대한 일치 여부를 확인하고 계정을 관리하는 데 사용됩니다. 두 가지 인증 소스를 사용하고 있기 때문에 기본 또는 보조 사용자 이름을 사용자 ID로 사용할지 여부를 시스템에 알려주어야 합니다. 기본적으로 기본 이름을 사용합니다.
 - **Password Type**(암호 유형): 보조 서버의 암호를 가져오는 방법. 기본값은 **Prompt**(프롬프트)입니다. 이는 사용자에게 암호를 입력하라는 메시지가 표시됨을 뜻합니다. 사용자가 기본 서버에 인증할 때 입력한 암호를 자동으로 사용하려면 **Primary Identity Source Password**(기본 ID 소스 암호)를 선택합니다. 모든 사용자에게 대해 동일한 암호를 사용하려면 **Common Password**(공통 암호)를 선택한 다음, **Common Password**(공통 암호) 필드에 해당 암호를 입력합니다.
 - **Authorization Server**(권한 부여 서버): 원격 액세스 VPN 사용자를 인증하도록 구성된 RADIUS 서버 그룹. 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 작

동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게 동일한 액세스 권한을 제공합니다.

시스템이 그룹 정책에 정의된 것과 중복되는 권한 부여 속성을 RADIUS 서버에서 가져오는 경우, RADIUS 속성은 그룹 정책 속성을 오버라이드한다는 점에 유의하십시오.

[ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)을 클릭하여 새 서버 그룹을 생성할 수 있습니다.

- **Accounting Server**(과금 서버): (선택 사항) 원격 액세스 VPN 세션에 대한 계정 관리에 사용할 RADIUS 서버 그룹입니다. 계정 관리 기능에서는 사용자가 액세스 중인 서비스뿐 아니라 사용 중인 네트워크 리소스의 수까지도 추적합니다. ASA 디바이스에서는 RADIUS 서버에 사용자 활동을 보고합니다. 계정 관리 정보에는 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 대한 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

[ASA RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)을 클릭하여 새 서버 그룹을 생성할 수 있습니다.

연결 프로파일에 대한 인증서 인증 구성



Note 이 섹션은 **Authentication Type**(인증 유형)이 **AAA Only**(AAA만)인 경우에는 적용되지 않습니다.

클라이언트 디바이스에 설치된 인증서를 사용해 원격 액세스 VPN 연결을 인증할 수 있습니다.

클라이언트 인증서를 사용하는 경우에도 보조 ID 소스, 대체 소스, 권한 부여 및 과금 서버를 구성할 수 있습니다. 이 옵션은 AAA 옵션입니다. 자세한 내용은 [ASA RA VPN 연결 프로파일 구성, on page 150](#)을 참조하십시오.

다음은 인증서별 속성입니다. 기본 및 보조 ID 소스에 대해 개별적으로 이러한 속성을 구성할 수 있습니다. 보조 소스 구성은 선택 사항입니다.

- **Username from Certificate**(인증서의 사용자 이름): 다음 중 하나를 선택합니다.
 - **Map Specific Field**(특정 필드 매핑): **Primary Field**(기본 필드) 및 **Secondary Field**(보조 필드)의 순서대로 인증서 요소를 사용합니다. 기본값은 CN(Common Name) 및 OU(Organizational Unit)입니다. 조직에 대해 작동하는 옵션을 선택합니다. 필드는 서로 결합하여 사용자 이름을 제공하고, 이 이름은 이벤트, 대시보드에서 사용되며 SSL 암호 해독 및 액세스 제어 규칙에서 일치 목적으로 사용됩니다.
 - **Use entire DN (distinguished name) as username**(전체 DN(고유 이름)을 사용자 이름으로 사용): 시스템은 DN 필드에서 사용자 이름을 자동으로 파생합니다.
- 고급 옵션(**Authentication Type**(인증 유형)이 **Client Certificate Only**(클라이언트 인증서 전용))인 경우에는 해당되지 않음): **Advanced**(고급) 링크를 클릭하고 다음 옵션을 구성합니다.

- **Prefill username from certificate on user login window**(인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기): 사용자에게 인증하라는 메시지를 표시할 때 사용자 이름 필드에 검색된 사용자 이름을 입력할지 여부.
- **Hide username in login window**(로그인 창에서 사용자 이름 숨기기): **Prefill**(미리 채우기) 옵션을 선택하면 사용자 이름을 숨길 수 있습니다. 따라서 사용자는 암호 프롬프트에서 사용자 이름을 편집할 수 없습니다.

클라이언트 주소 풀 할당 구성

원격 액세스 VPN에 연결하는 엔드포인트에 대한 IP 주소를 시스템에서 제공할 방법이 있어야 합니다. AAA 서버는 이러한 주소, DHCP 서버, 그룹 정책에 구성된 IP 주소 풀 또는 연결 프로파일에 구성된 IP 주소 풀을 제공할 수 있습니다. 시스템은 순서대로 이 리소스를 시도하고 사용 가능한 주소를 가져올 때 중지했다가 이 주소를 클라이언트에 할당합니다. 따라서 동시 연결 수가 비정상적인 경우에 파일세이프를 생성할 수 있는 여러 가지 옵션을 구성할 수 있습니다.

연결 프로파일에 대한 주소 풀을 구성하려면 다음 방법 중 한 가지 이상을 사용합니다.

- **IPv4 Address Pool(IPv4 주소 풀)** 및 **IPv6 Address Pool(IPv6 주소 풀)**: 먼저 서브넷을 지정하는 최대 6개의 네트워크 개체를 생성합니다. IPv4 및 IPv6에 대해 별도 풀을 구성할 수 있습니다. 그런 다음, 그룹 정책 또는 연결 프로파일의 **IPv4 Address Pool(IPv4 주소 풀)** 및 **IPv6 Address Pool(IPv6 주소 풀)** 옵션에서 이러한 개체를 선택합니다. IPv4 및 IPv6 모두 구성할 필요는 없고 지원하려는 주소 체계를 구성하면 됩니다. 또한 그룹 정책 및 연결 프로파일 모두에서 풀을 구성할 필요는 없습니다. 그룹 정책에서는 연결 프로파일 설정을 오버라이드하므로 그룹 정책에서 풀을 구성하는 경우, 연결 프로파일에서 옵션을 비워두십시오. 풀은 나열한 순서대로 사용된다는 점에 유의하십시오. 새 IPv4 또는 IPv6 주소 풀을 생성하려면, **IP 주소 풀 생성**을 참조하십시오.
- **DHCP Servers(DHCP 서버)**: 먼저 RA VPN에 대한 IPv4 주소 범위를 하나 이상 사용하여 DHCP 서버를 구성합니다(DHCP를 사용하여 IPv6 풀을 구성할 수는 없음). 그런 다음, DHCP 서버의 IP 주소로 호스트 네트워크 개체를 생성합니다. 그러면 연결 프로파일의 **DHCP Servers(DHCP 서버)** 속성에서 이 개체를 선택할 수 있습니다. 두 개 이상의 DHCP 서버를 구성할 수 있습니다. DHCP 서버에 주소 풀이 여러 개인 경우, 연결 프로파일에 연결하는 **새 ASA RA VPN 그룹 정책 생성**에서 **DHCP Scope(DHCP 범위)** 속성을 사용해 어떤 풀을 사용할지 선택할 수 있습니다. 풀의 네트워크 주소로 호스트 네트워크 개체를 생성합니다. 예를 들어 DHCP 풀에 192.168.15.0/24 및 192.168.16.0/24가 포함된 경우, DHCP 범위를 192.168.16.0으로 설정하면 192.168.16.0/24 서브넷에서 주소가 선택됩니다.

관련 정보:

[ASA에 대한 엔드 투 엔드 원격 액세스 VPN 구성 프로세스](#)

ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리

원격 액세스 VPN 마법사를 사용하여 AnyConnect 패키지를 업로드하려면 다음 단계 중 하나를 수행할 수 있습니다.

- CDO 저장소에서 패키지를 업로드합니다.

- HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜을 사용하여 서버에서 패키지를 업로드합니다.


CDO 저장소에서 AnyConnect 패키지 업로드

원격 액세스 VPN 구성 마법사는 CDO 저장소에서 운영 체제별로 AnyConnect 패키지를 제공하며, 이러한 패키지를 선택하여 디바이스에 업로드할 수 있습니다. 디바이스가 인터넷 및 적절한 DNS 구성에 액세스할 수 있는지 확인합니다.



참고 표시된 목록에서 원하는 패키지를 사용할 수 없거나 디바이스에서 인터넷에 액세스할 수 없는 경우 AnyConnect 패키지가 미리 로드된 서버를 사용하여 패키지를 업로드할 수 있습니다.

단계 1 운영 체제에 해당하는 필드를 클릭하고 AnyConnect 패키지를 선택합니다.

단계 2  를 클릭하여 패키지를 업로드합니다. 체크섬이 일치하지 않으면 AnyConnect 패키지 업로드가 실패합니다. 장애에 대한 자세한 내용은 디바이스의 워크플로우 탭을 참조하십시오.

서버에서 ASA로 AnyConnect 패키지 업로드

AnyConnect 클라이언트 소프트웨어 패키지를 컴퓨터에 다운로드하고 ASA에서 액세스할 수 있는 원격 서버에 업로드합니다. 나중에 RA VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 서버에서 ASA로 AnyConnect 소프트웨어 패키지를 업로드하십시오. 도메인 이름을 사용하는 URL의 경우 디바이스에서 DNS를 올바르게 구성해야 합니다.

ASA RA VPN 마법사는 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜을 사용한 패키지 업로드를 지원합니다.

파일 업로드에 지원되는 프로토콜의 syntax(명령문):

프로토콜	Syntax	예
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazon-tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	ftp://10.10.16.6/ftd/components.html
SMB	smb://[[path/]filename]	smb://10.10.32.145/sambashare/hello.txt
SCP	scp://[[user[:password]@]server[:port]/[path/]filename]	scp://root@10.10.166/10.10.166/ftd/events_sendpy

Before you begin

원하는 운영 체제에 대한 "AnyConnect 헤드엔드 배포 패키지"를 다운로드했는지 확인하십시오. 항상 최신 AnyConnect 버전을 다운로드하여 최신 기능, 버그 수정 및 보안 패치가 있는지 확인하십시오. 디바이스에서 패키지를 정기적으로 업데이트합니다.



Important ASA 파일 관리 마법사를 사용하여 패키지를 업로드하려는 경우, 다운로드한 후 패키지의 이름을 수정하지 마십시오.



Note 운영 체제(Windows, Mac, Linux)별로 AnyConnect 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

단계 1 <https://software.cisco.com/download/home/283000185>에서 AnyConnect 패키지를 다운로드합니다.

- EULA에 동의하고 K9(암호화된 이미지) 권한이 있는지 확인합니다.
- 운영 체제에 맞는 "AnyConnect Headend Deployment Package" 패키지를 선택합니다. 패키지 이름은 "anyconnect-win-4.7.04056-webdeploy-k9.pkg"와 유사합니다. Windows, macOS 및 Linux용 별도의 헤드엔드 패키지가 있습니다.

단계 2 AnyConnect 패키지를 원격 서버에 업로드합니다. ASA 디바이스 및 서버에서 네트워크 경로가 있는지 확인합니다. ASA RA VPN 마법사는 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 프로토콜로 패키지 업로드를 지원합니다.

Important AnyConnect 패키지를 HTTPS 서버에 업로드하는 경우 다음 단계를 수행해야 합니다.

- ASA 디바이스에서 해당 서버의 신뢰할 수 있는 CA 인증서를 업로드합니다.
- HTTPS 서버에 신뢰할 수 있는 CA 인증서를 설치합니다.


단계 3 원격 서버의 URL은 인증 프롬프트가 표시되지 않는 직접 링크여야 합니다. URL이 사전 인증된 경우 RA VPN 마법사의 URL을 지정하여 파일을 다운로드할 수 있습니다.

단계 4 원격 서버 IP 주소가 NAT된 경우 원격 서버 위치의 NAT된 공용 IP 주소를 제공해야 합니다.

ASA에 새 AnyConnect 패키지 업로드

RA VPN 마법사 또는 ASA 파일 관리 마법사를 사용하여 AnyConnect 소프트웨어 패키지를 ASA에 업로드할 수 있습니다.

다음 절차를 사용하여 HTTP 또는 HTTPS 서버에서 ASA 디바이스에 새 AnyConnect 패키지를 업로드합니다.

- 단계 1 **AnyConnect Package Detected**(AnyConnect 패키지 감지됨)에서 Windows, Mac 및 Linux 엔드포인트용 개별 패키지를 업로드할 수 있습니다.
- 단계 2 해당하는 Platform(플랫폼) 필드에서 Windows, Mac 및 Linux와 호환되는 AnyConnect 패키지가 사전 업로드되는 서버의 경로를 지정합니다. 서버 경로의 예:
 'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
 'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.
- 단계 3 를 클릭하여 패키지를 업로드합니다. CDO는 경로에 연결할 수 있고 지정된 파일 이름이 유효한 패키지인지 확인합니다. 검증에 성공하면 AnyConnect 패키지의 이름이 나타납니다. RA VPN 구성에 ASA 디바이스를 추가하면 AnyConnect 패키지를 여기에 업로드할 수 있습니다.
- 단계 4 **OK**(확인)를 클릭합니다. AnyConnect 패키지가 RA VPN 구성에 추가됩니다.
- 단계 5 5단계부터 [ASA RA VPN 구성 생성](#)을 계속 진행합니다.

What to do next

VPN 연결을 완료하려면 사용자가 해당 워크스테이션에 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 자세한 내용은 [ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법](#)을 참조하십시오.

파일 관리 마법사를 사용하여 AnyConnect 패키지 업로드

HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP 서버에서 단일 또는 여러 ASA 디바이스로 AnyConnect 패키지를 업로드하려면 파일 관리 마법사를 사용합니다. AnyConnect 패키지를 여러 ASA 디바이스에 동시에 푸시하려는 경우 대량 업로드가 유용합니다. 자세한 내용은 [ASA 파일 관리](#)를 참조하십시오.



Important ASA 파일 관리 마법사를 사용하여 패키지를 업로드하려는 경우, 다운로드한 후 패키지의 이름을 수정하지 마십시오.



업로드가 완료되면 ASA RA VPN 구성 마법사를 열고 패키지가 자동으로 탐지되는지 확인합니다. OS 버전에 대해 여러 패키지를 업로드하는 경우 마법사의 드롭다운 목록에 해당 패키지가 나열되어 그중 하나를 선택할 수 있습니다. 그런 다음 RA VPN 구성을 생성하여 디바이스에 구축할 수 있습니다.

기존 AnyConnect 패키지 교체


AnyConnect 패키지가 디바이스에 이미 있는 경우 RA VPN 마법사에서 확인할 수 있습니다. 드롭다운 목록에서 운영 체제에 대해 사용 가능한 모든 AnyConnect 패키지를 볼 수 있습니다. 목록에서 기존 패키지를 선택하고 새 패키지로 교체할 수 있지만 새 패키지를 목록에 추가할 수는 없습니다.



Note 기존 패키지를 새 패키지로 교체하려면 ASA 디바이스가 연결할 수 있는 네트워크의 서버에 AnyConnect 패키지가 이미 업로드되어 있는지 확인합니다.

- 단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN > ASA/FDM** 원격 액세스 **VPN**을 클릭합니다.
- 단계 2 수정할 RA VPN 구성을 선택하고 **Actions(작업)** 아래에서 **Edit(편집)**를 클릭합니다.
- 단계 3 **AnyConnect Packages Detected(AnyConnect 패키지 탐지됨)**에서 기존 AnyConnect 패키지 옆에 나타나는  아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 교체할 패키지를 선택하고 **Edit(편집)**를 클릭합니다. 해당 필드에서 기존 패키지가 사라집니다.
- 단계 4 새 AnyConnect 패키지가 사전 로드되는 서버의 경로를 지정하고  을 클릭하여 패키지를 업로드합니다.
- 단계 5 **OK(확인)**를 클릭합니다. 새 AnyConnect 패키지가 RA VPN 구성에 추가됩니다.
- 단계 6 6단계부터 [ASA RA VPN 구성 생성, on page 146](#)로 계속 진행합니다.

AnyConnect 패키지 삭제

- 단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN > ASA/FDM** 원격 액세스 **VPN**을 클릭합니다.
- 단계 2 수정할 RA VPN 구성을 선택하고 **Actions(작업)** 아래에서 **Edit(편집)**를 클릭합니다.
- 단계 3 **AnyConnect Packages Detected(탐지된 AnyConnect 패키지)**에서 삭제할 AnyConnect 패키지 옆에 표시되는  아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 삭제할 패키지를 선택합니다. 해당 필드에서 기존 패키지가 사라집니다.

Note 삭제 작업을 중지하고 기존 패키지를 유지하려면 **Cancel(취소)**을 클릭합니다.

- 단계 4 **OK(확인)**를 클릭합니다. 디바이스의 구성 상태가 '동기화되지 않음' 상태입니다.

Note 이 단계에서 삭제 작업을 실행 취소하려면 **Inventory(인벤토리)** 페이지로 이동하여 **Discard Changes(변경 사항 취소)**를 클릭하여 기존 AnyConnect 패키지를 유지합니다.

- 단계 5 CDO에서 [ASA로 구성 변경 사항 구축](#).

온보딩된 ASA 디바이스의 RA VPN 구성 읽기

이미 RA VPN 설정이 있는 ASDM 관리형 ASA 디바이스를 온보딩하면 기존 원격 액세스 VPN 구성을 검색하고 표시합니다. CDO는 "기본 RA VPN 구성"을 자동으로 생성하고 ASA 디바이스를 이 구성과 연결합니다. CDO에서 읽히지 않거나 지원되지 않지만 CDO 명령줄 인터페이스에서 구성할 수 있는 일부 RA VPN 구성이 있습니다.



Note 이 섹션에서는 CDO에서 지원되거나 지원되지 않는 모든 구성을 다루지는 않습니다. 대신 가장 일반적으로 사용되는 항목만 설명합니다.

온보딩된 ASA에서 RA VPN 구성을 보려면, 다음 단계를 수행합니다.

단계 1 CDO 인터페이스에서 **VPN > ASA/FDM Remote Access VPN Configuration**(ASA/FDM 원격 액세스 VPN 구성)으로 이동합니다.

단계 2 온보딩된 ASA 디바이스에 해당하는 RA VPN 구성을 클릭합니다. CDO는 "기본 RA VPN 구성"을 자동으로 생성하고 ASA 디바이스를 이 구성과 연결합니다. 기본 구성을 삭제할 수 있습니다. CDO에서 읽는 ASA RA VPN 구성은 다음과 같이 분류됩니다.

- 디바이스 설정
- 연결 프로파일
- 그룹 정책

디바이스 설정

온보딩된 ASA 디바이스와 연결된 RA VPN 구성이 **Default_RA_VPN_Configuration**에 나타납니다. 해당 구성과 연결된 ASA 디바이스(오른쪽의 **Devices**(디바이스) 창에서)의 이름을 보려면 이 구성을 클릭해야 합니다. 편집 버튼을 클릭하여 ASA 디바이스에 있는 AnyConnect 패키지를 확인할 수도 있습니다.

연결 프로파일

CDO는 ASA 디바이스의 "AnyConnect 클라이언트 VPN 액세스"에 정의된 연결 프로파일을 지원하고 읽습니다. "클라이언트리스 SSL VPN 액세스" 구성은 지원되지 않습니다.

연결 프로파일 속성을 보려면 다음을 수행합니다.

단계 1 **Default_RA_VPN_Configuration**을 확장합니다.

단계 2 원하는 연결 프로파일 중 하나를 클릭하고 **Edit**(편집)를 클릭합니다.

모든 기본 및 고급 ASA RA VPN 속성은 CDO RA VPN 구성 페이지의 연결 프로파일 이름 및 세부 정보에서 확인할 수 있습니다.



Note 기본 구성을 삭제할 수 있습니다(기본 RA VPN 구성을 선택하고 오른쪽의 **Actions**(작업) 창에서 **Remove**(제거) 클릭).

기본 ID 소스

- CDO는 **Connection Aliases**(연결 별칭) 및 **Group URLs**(그룹 URL) 속성을 **Group Alias**(그룹 별칭) 및 **Group URL**(그룹 URL)로 읽습니다.

**Note**

- SAML, 다중 인증서 및 AAA, 다중 인증서로 구성된 연결 프로파일은 읽을 수 없습니다.
- 인터페이스 및 서버 그룹이 있는 인증 서버 그룹은 지원되지 않습니다.

- CDO는 기본 ID 소스에서 "AAA", "AAA 및 인증서" 및 "인증서 전용" 인증 방법으로 구성된 AnyConnect 연결 프로파일을 지원합니다.
 - AAA 서버 그룹은 CDO에서 기본 ID 소스의 사용자 인증을 위한 기본 ID 소스로 읽힙니다(인증 유형으로 AAA 또는 AAA 및 클라이언트 인증서를 선택하여 이 속성을 확인할 수 있음).
 - AAA 서버 그룹이 로컬이 아닌 다른 항목으로 구성된 경우 CDO는 이 특성을 읽고 **Primary Identity Source**(기본 ID 소스) 아래의 **Fallback Local Identity Source**(대체 로컬 ID 소스) 필드에 이 속성을 표시합니다. (인증 유형으로 AAA를 선택하여 이 속성을 확인할 수 있습니다.)
- CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 [AAA 서버 그룹](#)을 참조하십시오.

보조 ID 소스

Secondary Identity Source(보조 ID 소스)에는 ASA 디바이스의 보조 인증 속성이 표시됩니다. 이러한 속성을 보려면 인증 유형으로 AAA 또는 **AAA and Client Certificate**(클라이언트 인증서)를 선택하고 **View Secondary Identity Source**(보조 ID 소스 보기)를 클릭합니다.

- **Secondary Identity Source for User Authentication**(사용자 인증을 위한 보조 ID 소스)에 보조 인증 **Server Group**(서버 그룹) 속성이 표시됩니다.
 - 서버 그룹이 LOCAL(로컬) 이외의 항목으로 구성된 경우 CDO는 이 특성을 읽고 **Secondary Identity Source**(보조 ID 소스) 아래의 **Fallback Local Identity Source for Secondary**(보조 ID 소스에 대한 대체 로컬 ID 소스) 필드에 이 속성을 표시합니다.
- CDO는 **Attribute Server**(속성 서버) 및 **Interface-Specific Authorization Server Groups**(인터페이스별 권한 부여 서버 그룹) 속성을 지원하지 않습니다.

CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 [AAA 서버 그룹](#)을 참조하십시오.

권한 부여 서버

- **Authorization Server**(권한 부여 서버)에 권한 부여 **Server Group**(서버 그룹) 속성이 표시됩니다.
- CDO는 인터페이스 및 서버 그룹이 있는 권한 부여 서버 그룹을 지원하지 않습니다.

CDO에서 읽은 RADIUS 서버 그룹 특성에 대한 자세한 내용은 [RADIUS 서버 그룹](#)을 참조하십시오.

계정 관리 서버

Accounting Server(과금 서버)에 과금 서버 그룹 속성이 표시됩니다. CDO에서 읽은 서버 그룹 특성에 대한 자세한 내용은 [RADIUS 서버 그룹](#)을 참조하십시오.

클라이언트 주소 풀 할당

CDO는 **Client Address Assignment**(클라이언트 주소 할당) 속성(DHCP 서버, 클라이언트 주소 풀 및 클라이언트 IPv6 주소 풀)을 개체로 읽습니다. (이러한 속성은 **Client Address Pool Assignment**(클라이언트 주소 풀 할당)에서 확인할 수 있습니다.) DHCP 서버 세부 정보는 리터럴로 읽힙니다.



Note CDO는 특정 인터페이스에 할당된 IP 주소 풀을 지원하지 않습니다. 그러나 이러한 속성은 ASA CLI(명령줄 인터페이스)에서 확인할 수 있습니다.

AAA 서버 그룹

CDO는 LDAP 서버 그룹 및 연결된 LDAP 서버를 **Active Directory** 영역 개체로 나타냅니다. AD(Active Directory)의 경우 영역은 Active Directory 도메인과 동일합니다. CDO는 이미 존재하는 AD 영역 개체의 AD 비밀번호를 읽습니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **ASA Objects**(ASA 개체)을 클릭합니다.

단계 2 이 개체를 보려면 **Active Directory Realms**(Active Directory 영역) 필터를 적용합니다.

단계 3 원하는 Active Directory 영역 개체를 선택하고 **Edit**(편집)를 클릭하여 세부 정보를 확인합니다.

What to do next

AD 영역에 연결된 AD 서버 및 해당 구성이 포함되어 있음을 확인할 수 있습니다. AD 영역에 대해 여러 AD(Active Directory) 서버가 있는 경우 AD 서버는 서로 중복되어야 하며 동일한 AD 도메인을 지원해야 합니다. 따라서 **Directory Name**(디렉터리 이름), **Directory Password**(디렉터리 비밀번호), **Base Distinguished Name**(기본 고유 이름)과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다. 이러한 속성이 동일하지 않은 경우 CDO는 Active Directory 영역 개체에 경고 메시지를 표시합니다. AD 서버 전체에서 일관성을 유지하려면 이러한 속성을 수정해야 합니다. 이 경고를 해결하지 않고 계속 진행하면 CDO는 AD 서버 속성 중 하나를 사용하여 해당 영역 개체의 다른 서버에 적용합니다.

RADIUS 서버 그룹

ASA 디바이스의 AAA RADIUS 서버 그룹 속성은 CDO에서 RADIUS 서버 그룹 개체로 읽힙니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **ASA Objects**(ASA 개체)을 클릭합니다.

단계 2 이 개체를 보려면 **RADIUS** 서버 그룹 필터를 적용합니다.

단계 3 원하는 개체를 선택한 다음 **Edit**(편집)를 클릭하여 세부 정보를 확인합니다.

- ASA에서 **Enable dynamic authorization**(동적 권한 부여 활성화)는 CDO에서 **Dynamic Authorization**(동적 권한 부여)(RA VPN에만 해당)으로 읽힙니다.
- **Reactivation Mode**(재활성화 모드)의 **Depletion**(감소) 옵션은 CDO에서 읽히므로, 감소 시간과 관련된 **Dead Time**(데드 타임) 값은 CDO에서 읽힙니다. 그러나 **Timed**(시간 제한) 속성은 CDO에서 읽히지 않습니다.
- CDO **Accounting Mode**(계정 관리 모드), **Timed**(시간 제한), **Enable interim accounting update**(임시 계정 업데이트 활성화), **Enable interim accounting update**(임시 계정 업데이트 활성화) 및 **Use authorization only mode**(권한 부여 전용 모드 사용)을 지원하지 않습니다.

RADIUS 서버

CDO는 ASA에서 Radius 서버를 읽을 때 이름을 "Radius 서버 group_server 이름 또는 IP 주소의 이름"으로 지정하는 Radius 서버 개체를 생성합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **ASA Objects**(ASA 개체)을 클릭합니다.

단계 2 이 개체를 보려면 **RADIUS Server**(RADIUS 서버) 필터를 적용합니다.

단계 3 원하는 개체를 선택한 다음 **Edit**(편집)를 클릭하여 세부 정보를 확인합니다.

그룹 정책

Group Policy(그룹 정책) 섹션에서 드롭다운을 클릭하여 디바이스와 연결된 그룹 정책을 확인합니다.



Attention CDO는 터널링 프로토콜로 구성된 그룹 정책을 **SSL VPN** 클라이언트로 읽습니다.

CDO는 ASA에 구성된 대부분의 그룹 정책 속성을 읽습니다. 이 정보는 RA VPN 그룹 정책 마법사의 여러 탭에 표시됩니다. ASA 디바이스에서 읽은 그룹 정책의 세부 정보를 보려면 다음을 수행해야 합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FTD Network Objects**(FTD 네트워크 개체)을 클릭합니다.

단계 2 **RA VPN Group Policy**(RA VPN 그룹 정책)를 기준으로 필터링합니다.

단계 3 해당 디바이스와 연결된 그룹 정책을 선택하고 **Edit**(편집)를 클릭합니다.

What to do next



Note CDO는 ASA 디바이스의 스플릿 터널링에 정의된 표준 ACL(Access Control List)을 지원하지 않습니다. ACL(Extended Access Control List)을 지원하며 ASA 정책에서 ACL로 읽습니다. 자세한 내용은 [ASA RA VPN 그룹 정책 속성](#)을 참조하십시오. 정책을 보려면 내비게이션 바에서 **Policies(정책)** > **ASA Access Policies(ASA 액세스 정책)**를 클릭합니다.

확장 ACL을 선택하려면 다음을 수행합니다.

- **Split Tunneling(스플릿 터널링)** 탭을 클릭합니다.
- ASA의 트래픽이 IPv4 주소를 사용하는지 IPv6 주소를 사용하는지에 따라 해당 드롭다운 목록에서 "Allow specified traffic over tunnel(터널을 통한 지정된 트래픽 허용)" 또는 "Exclude networks specified below(아래에 지정된 네트워크 제외)"를 선택합니다. ASA에서 가져온 확장 ACL을 선택합니다.

IP 주소 풀 생성

VPN 연결을 사용하여 네트워크에 원격으로 연결하는 클라이언트에 할당하도록 ASA에 대한 IPv4 및 IPv6 IP 주소 풀을 구성할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 연결 프로파일 또는 그룹 정책에 대해 둘 이상의 주소 풀을 구성한 경우 ASA에서는 ASA에 추가된 순서대로 주소 풀을 사용합니다.

IPv4 주소 풀을 정의하려면 IP 주소 범위를 제공합니다. IPv4 주소 풀의 예는 10.10.147.100 - 10.10.147.177입니다.

IPv6 주소 풀을 정의하려면 시작 IP 주소 범위, 주소 접두사 및 풀에 구성할 수 있는 주소 수를 지정합니다. IPv6 주소 풀의 예는 2001:DB8:1::1입니다.

로컬이 아닌 서브넷에서 주소를 할당할 경우 이러한 네트워크에 대한 경로를 보다 쉽게 추가할 수 있도록 서브넷 경계에 속하는 풀을 추가하는 것이 좋습니다.

IP 주소 풀을 생성하려면 다음을 수행합니다.

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체)** > **ASA Objects(ASA 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하고 **ASA > Address Pool(ASA 주소 풀)**을 선택합니다.

단계 3 **Create IP Address Pool(IP 주소 풀 생성)** 대화 상자에서 다음 정보를 입력합니다.

- **Object Name(개체 이름)** - 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
- **IPv4 address pool(IPv4 주소 풀)**: IPv4 주소 풀을 구성하려면 이 라디오 버튼을 선택합니다.
 - **IPv4 Address Range(IPv4 주소 범위)**: 구성된 각 풀에서 사용 가능한 첫 번째 IP 주소와 마지막 IP 주소를 입력합니다. 예: 10.10.147.100 - 10.10.147.177.
 - **Mask(마스크)** - 이 IP 주소 풀이 있는 서브넷을 식별합니다.

- **IPv6 address pool(IPv6 주소 풀):** IPv6 주소 풀을 구성하려면 이 라디오 버튼을 선택합니다.
- **IPv6 주소:** 구성된 풀에서 사용한 첫 번째 IP 주소 및 접두어 길이를 비트로 입력합니다. <address>/<prefix> 형식. 예: 2001:DB8:1::1/3.
- **Number of Addresses(주소 수) - 풀에 있는 IP 주소부터 시작하여 IPv6 주소의 수를 식별합니다.**

단계 4 **Save(저장)**를 클릭합니다.

원격 액세스 VPN 인증서 기반 인증

원격 액세스 VPN은 다음 시나리오에서 보안 게이트웨이 및 AnyConnect 클라이언트(종단)를 인증하기 위해 디지털 인증서를 사용합니다.



중요 CDO는 VPN 헤드엔드(ASA)에서 디지털 인증서 설치를 처리합니다. AnyConnect 클라이언트 디바이스에 대한 인증서 설치는 처리하지 않습니다. 조직의 관리자가 이를 처리해야 합니다.

• VPN 헤드엔드 디바이스(ASA) 식별 및 인증:

VPN 헤드엔드는 AnyConnect 클라이언트가 VPN 연결을 요청할 때 자신을 식별하고 인증하기 위해 ID 인증서가 필요합니다. CDO를 사용하여 디바이스에 ID 인증서를 설치해야 합니다. PKCS12 또는 인증서 및 키를 사용하여 ID 인증서 설치를 참조하십시오. AnyConnect 클라이언트에 발급자의 CA 인증서를 반드시 설치해야 하는 것은 아닙니다.

CDO에서 원격 액세스 VPN 구성을 생성하는 동안 등록된 ID 인증서를 디바이스의 외부 인터페이스에 할당하고 구성을 디바이스로 다운로드합니다. ID 인증서는 디바이스의 외부 인터페이스에서 완전히 작동합니다.

AnyConnect 클라이언트가 VPN에 연결을 시도하면 디바이스는 AnyConnect 클라이언트에 ID 인증서를 제공하여 자체적으로 인증합니다. AnyConnect 클라이언트는 신뢰할 수 있는 CA 인증서로 이 ID 인증서를 확인하고 인증서와 디바이스를 신뢰합니다. CA 인증서가 AnyConnect 클라이언트에 설치되어 있지 않은 경우 메시지가 표시되면 사용자는 디바이스를 수동으로 신뢰해야 합니다.

• AnyConnect 클라이언트 식별 및 인증:



참고 이는 RA VPN 구성의 연결 프로파일에서 인증 방법으로 "클라이언트 인증서 전용" 또는 "AAA 및 클라이언트 인증서"를 사용하는 경우에 적용됩니다. "AAA 전용"에는 적용되지 않습니다.

디바이스가 신뢰되면 AnyConnect 클라이언트는 VPN 연결을 완료하기 위해 스스로를 인증해야 합니다. AnyConnect 클라이언트에 ID 인증서를 설치하고 CDO를 사용하여 디바이스에 신뢰할 수 있는 CA 인증서를 설치해야 합니다. 동일한 인증 기관이 이러한 인증서를 발급해야 합니다. ASA에서 신뢰할 수 있는 CA 인증서 설치를 참조하십시오.

AnyConnect 클라이언트는 ID 인증서를 제시하고 디바이스는 신뢰할 수 있는 CA 인증서로 이 인증서를 확인하고 VPN 연결을 설정합니다.

NAT에서 원격 액세스 트래픽 제외

NAT 제외를 구성하여 NAT 변환에서 원격 액세스 VPN 엔드포인트로 오가는 트래픽을 제외합니다. NAT에서 VPN 트래픽을 제외하지 않는 경우 내부 인터페이스와 외부 인터페이스에 대한 기존 NAT 규칙이 주소의 RA VPN 풀에 적용되지 않는지 확인합니다. NAT 제외 규칙은 지정된 소스/대상 인터페이스 및 네트워크 조합에 대한 수동 고정 ID NAT 규칙이며 NAT 정책에서는 반영되지 않고 숨겨집니다. NAT 제외를 활성화하는 경우에는 다음 항목도 구성해야 합니다.

- 내부 인터페이스: 원격 사용자가 액세스할 내부 네트워크의 인터페이스를 선택합니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
- 내부 네트워크: 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체를 선택합니다. 네트워크 목록에는 지원할 주소 풀과 동일한 IP 유형이 포함되어 있어야 합니다.

시작하기 전에

해당 디바이스의 연결 프로파일 및 그룹 정책에서 사용되는 로컬 IP 주소 풀의 구성과 일치하는 ASA 네트워크 개체를 생성합니다. 이러한 네트워크 개체는 NAT 규칙을 구성할 때 대상 주소 및 변환된 주소로 할당되어야 합니다. [새 네트워크 개체 생성](#)의 내용을 참조하십시오.

단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

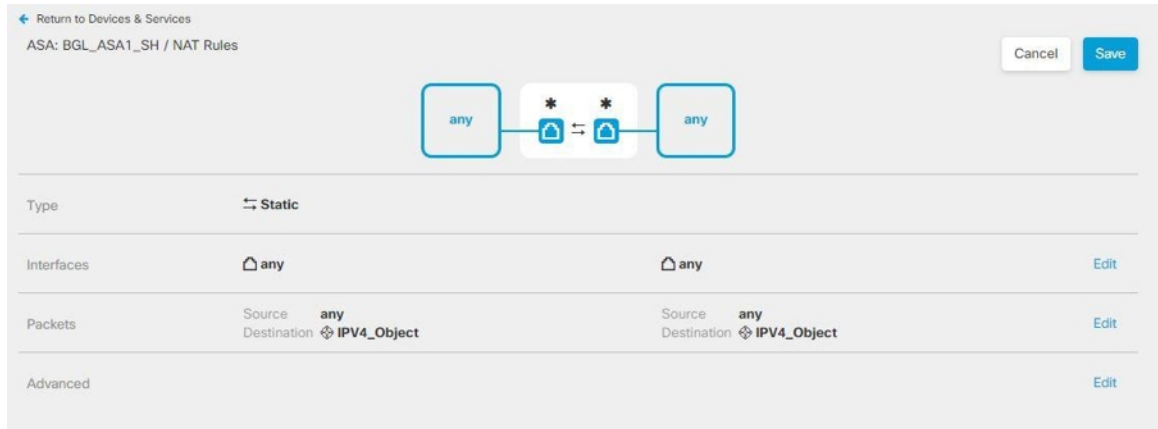
단계 2 **Inventory**(재고 목록) 필터 및 검색 필드를 사용하여 NAT 규칙을 생성하려는 ASA 디바이스를 찾습니다.

단계 3 상세정보 패널의 **Management**(관리) 영역에서 **NAT** > **NAT**를 클릭합니다.

단계 4  > **Twice NAT**(2회 NAT)를 클릭합니다.

1. 섹션 1에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
2. 섹션 2에서 **Source Interface**(소스 인터페이스) = 'any' 및 **Destination Interface**(대상 인터페이스) = 'any'를 선택합니다. **Continue**(계속)를 클릭합니다.
3. 섹션 3에서 **Source Original Address**(소스 원본 주소) = 'any' 및 **Source Translated Address**(소스 변환 주소) = 'any'를 선택합니다.
4. **Use Destination**(대상 사용)을 선택합니다.
 1. **Destination Original Address**(대상 원본 주소) 및 **Source Translated Address**(소스 변환 주소): 드롭다운에서 **Choose**(선택)를 클릭하고 로컬 IP 주소 풀의 구성과 일치하는 네트워크 개체를 선택합니다. 아래 예에서 'IPV4_Object'는 ASA(BGL_ASA1_SH) 디바이스의 연결 프로파일 및 그룹 정책 설정에서 사용되는 IPv4 주

소 폴 개체와 동일한 구성을 가진 네트워크 개체입니다.



2. **Disable proxy ARP for Incoming packet**(수신 패킷에 대해 프록시 ARP 비활성화)을 선택합니다.
3. **Save**(저장)를 클릭합니다.
4. 4단계부터 프로세스를 반복하여 IP 주소 풀에 해당하는 다른 각 네트워크 개체에 대해 동일한 규칙을 생성합니다.

단계 5 CDO에서 ASA로 구성 변경 사항 구축.

ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법

VPN 연결을 완료하려면 사용자가 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 기존 소프트웨어 배포 방법을 사용하여 소프트웨어를 직접 설치할 수 있습니다. 또는 사용자가 ASA 디바이스에서 AnyConnect 클라이언트를 직접 설치하게 할 수도 있습니다.



Note 소프트웨어를 설치하려면 사용자에게 워크스테이션에 대한 관리자 권한이 있어야 합니다.

사용자가 ASA 디바이스에서 소프트웨어를 처음 설치하도록 하려면 사용자에게 다음 단계를 수행하도록 하십시오.



Note Android 및 iOS 사용자는 해당 앱 스토어에서 AnyConnect를 다운로드해야 합니다.

단계 1 웹 브라우저를 사용하여 **https://ravpn-address**를 엽니다. 여기서 **ravpn-address**는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 원격 액세스 VPN을 구성할 때 이 인터페이스를 식별합니다. 시스템에서 사용자에게 로그인하라는 메시지를 표시합니다.

단계 2 사이트에 로그인합니다. 사용자는 원격 액세스 VPN용으로 구성된 디렉터리 서버를 사용하여 인증을 합니다. 로그인에 성공해야 설치를 계속할 수 있습니다. 로그인이 성공하면 시스템은 사용자에게 필요한 AnyConnect 클라이언

트 버전이 이미 있는지를 확인합니다. 사용자 컴퓨터에 AnyConnect 클라이언트가 없거나 클라이언트가 하위 레벨인 경우에는 시스템에서 AnyConnect 소프트웨어 설치를 자동으로 시작합니다. 설치가 완료되면, AnyConnect에서 원격 액세스 VPN 연결을 완료합니다.

온보딩된 ASA의 원격 액세스 VPN 구성 수정

ASA 디바이스가 CDO에 온보딩되면 온보딩된 ASA 디바이스에서 기존 원격 액세스 VPN 구성을 검색하고 표시합니다. 자세한 내용은 [온보딩된 ASA 디바이스의 RA VPN 구성 읽기, 159 페이지](#)를 참조하십시오.

이러한 구성을 수정하고 새 구성을 디바이스에 다운로드할 수 있습니다.

- [ASA RA VPN 구성 수정](#)
- [ASA 연결 프로파일 수정](#)

원격 액세스 VPN 구성 수정

단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN > Remote Access VPN Configuration**(원격 액세스 VPN 구성)을 클릭합니다.

단계 2 VPN 구성에 그룹 정책을 추가하거나 제거하려면 온보딩된 ASA 디바이스와 연결된 VPN 구성을 클릭합니다. 왼쪽의 **Actions**(작업) 창에서 **Group Policies**(그룹 정책)를 클릭합니다.

- a) 파란색 + 아이콘을 클릭하고 선택 항목을 구성한 다음 **Select**(선택)를 클릭합니다.
- b) **Save**(저장)를 클릭합니다. 새 **ASA RA VPN 그룹 정책** 생성할 수도 있습니다.

단계 3 VPN 구성을 클릭하고 왼쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

마법사는 구성과 연결된 ASA 디바이스를 나열합니다.

- a) 생성된 것과 동일한 방식으로 다음 세부 정보를 수정할 수 있습니다.
 - RA VPN 구성의 이름을 변경합니다.
 - 디바이스 세부 정보를 표시하는 행에 나타나는 점 3개를 클릭하고 **Edit**(편집)를 클릭합니다.

자세한 내용은 [ASA RA VPN 구성 생성, 146 페이지](#) 항목을 참조하십시오.

단계 4 **OK**(확인)를 클릭합니다.

단계 5 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 212 페이지](#)

ASA 연결 프로파일 수정

단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN > Remote Access VPN Configuration**(원격 액세스 VPN 구성)을 클릭합니다.

단계 2 온보딩된 ASA 디바이스와 연결된 VPN 구성을 확장하고 연결 프로파일을 선택합니다.

단계 3 왼쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 4 생성된 것과 동일한 방식으로 값을 편집하고 **Done**(완료)을 클릭합니다.

자세한 내용은 [ASA RA VPN 연결 프로파일 구성, 150 페이지](#)을 참조해 주십시오.

단계 5 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 212 페이지

RA VPN AnyConnect 클라이언트 프로파일 업로드

원격 액세스 VPN AnyConnect 클라이언트 프로파일은 파일에 저장된 구성 매개변수의 그룹입니다. 핵심 클라이언트 VPN 기능과 선택적 클라이언트 모듈인 Network Access Manager, AMP Enabler, ISE Posture, 네트워크 가시성, 고객 피드백 경험 프로파일, Umbrella 로밍 보안 및 웹 보안에 대한 구성 설정을 포함하는 다양한 AnyConnect 클라이언트 프로파일이 있습니다.

CDO는 이러한 프로파일을 나중에 그룹 정책에서 사용할 수 있는 개체로 업로드할 수 있습니다.

- **AnyConnect VPN** 프로파일 — AnyConnect 클라이언트 프로파일은 AnyConnect 클라이언트 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 AnyConnect 클라이언트 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. CDO는 XML 파일 형식을 지원합니다.
- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 AMP Enabler 및 이 프로파일이 FDM 관리 디바이스에서 엔드 포인트로 푸시됩니다. CDO는 XML 및 ASP 파일 형식을 지원합니다.
- **피드백 프로파일** - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다. CDO는 FSP 파일 형식을 지원합니다.
- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다. CDO는 XML 및 ISP 파일 형식을 지원합니다.
- **Network Access Manager** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다. CDO는 XML 및 NSP 파일 형식을 지원합니다.
- **네트워크 가시성** 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다. CDO는 XML 및 NVMSPP 파일 형식을 지원합니다.
- **Umbrella** 로밍 보안 프로파일 - Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다. CDO는 XML 및 JSON 파일 형식을 지원합니다.
- **웹 보안** 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다. CDO는 XML, WSO 및 WSP 파일 형식을 지원합니다.

Before you begin

적합한 GUI 기반 AnyConnect 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. AnyConnect Secure Mobility Client 범주의 [Cisco 소프트웨어 다운로드 센터](#)에서 프로파일 편집기를 다운로드하고 AnyConnect "프로파일 편집기 - Windows/독립형 설치 프로그램(MSI)"을 설치할 수 있습니다. 프로파일 편집기 설치 프로그램에는 독립형 버전의 프로파일 편집기가 포함되어 있습니다. 설치 파일은

Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 AnyConnect 버전입니다. 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다.

Umbrella 로밍 보안 프로파일 편집기를 제외하고 이 패키지에는 모듈을 생성하는 데 필요한 모든 프로파일 편집기가 포함되어 있습니다. 자세한 내용은 [Cisco AnyConnect Secure Mobility Client 관리자 가이드](#)에서 해당 릴리스의 AnyConnect 프로파일 편집기 장을 참조하십시오. Umbrella 대시보드와 별도로 Umbrella 로밍 보안 프로파일을 다운로드합니다. 자세한 내용은 [Cisco Umbrella 사용 설명서](#)의 "Umbrella 로밍 보안" 장에서 "Umbrella 대시보드에서 AnyConnect 로밍 보안 프로필 다운로드" 섹션을 참조하십시오.

단계 1 좌측의 CDO 내비게이션 바에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 파란색 더하기  버튼을 클릭합니다.

단계 3 **RA VPN Objects (ASA & FDM)(RA VPN 개체(ASA 및 FDM)) > AnyConnect Client Profile(AnyConnect 클라이언트 프로파일)**를 클릭합니다.

단계 4 **Object Name(개체 이름)** 필드에 AnyConnect 클라이언트 프로파일의 이름을 입력합니다.

단계 5 **Browse(찾아보기)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 6 **Open(열기)**를 클릭하여 프로파일을 업로드합니다.

단계 7 **Add(추가)**를 클릭하여 개체를 추가합니다.

관련 정보:

- RA VPN 그룹 정책 창에서 클라이언트 모듈을 AnyConnect VPN 프로파일과 연결합니다. [새 ASA RA VPN 그룹 정책 생성](#) 을 참조하십시오.



Note 클라이언트 모듈 연결은 소프트웨어 버전 6.7 이상을 실행하는 모든 ASA 버전 및 FDM에서 지원됩니다.

ASA의 원격 액세스 VPN 구성 확인

원격 액세스 VPN을 구성하고 디바이스에 구성을 배포한 후에는 원격 연결을 수행할 수 있는지 확인합니다.

단계 1 외부 네트워크에서 AnyConnect 클라이언트를 사용하여 VPN 연결을 설정합니다. 웹 브라우저를 사용하여 **https://ravpn-address**를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 필요한 경우, 클라이언트 소프트웨어를 설치하여 연결을 완료합니다. [ASA에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법](#) 을 참조하십시오. 그룹 URL을 구성한 경우, 그룹 URL도 시도해 보십시오.

단계 2 **Devices & Services(디바이스 및 서비스)** 페이지에서, 확인하려는 디바이스(FTD 또는 ASA)를 선택하고 디바이스 작업(**Device Actions**) 아래의 **Command Line Interface(명령줄 인터페이스)**를 클릭합니다.

단계 3 **show vpn-sessiondb** 명령을 사용하여 현재 VPN 세션에 대한 요약 정보를 봅니다.

단계 4 통계에는 활성 AnyConnect 클라이언트 세션, 누적 세션에 대한 정보, 최대 동시 세션 수, 비활성 세션이 표시되어야

```
> show vpn-sessiondb
-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
AnyConnect Client      :      1 :      49 :      3 :      0
  SSL/TLS/DTLS         :      1 :      49 :      3 :      0
  Clientless VPN       :      0 :      1 :      1 :      0
  Browser               :      0 :      1 :      1 :      0
-----

Total Active and Inactive :      1          Total Cumulative :      50
Device Total VPN Capacity : 10000
Device Load                :      0%
-----

Tunnels Summary
-----
Active : Cumulative : Peak Concurrent
Clientless      :      0 :      1 :      1
AnyConnect-Parent :      1 :      49 :      3
SSL-Tunnel      :      1 :      46 :      3
DTLS-Tunnel     :      1 :      46 :      3
-----
Totals          :      3 :      142
-----

IPv6 Usage Summary
-----
Active : Cumulative : Peak Concurrent
AnyConnect SSL/TLS/DTLS :      :      :
  Tunneler IPv6         :      1 :      20 :      2
-----
```

합니다. 다음은 명령의 샘플 출력입니다.

단계 5 **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

단계 6 **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다

시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

```
> show vpn-sessiondb anyconnect
```


```
Session Type: AnyConnect

Username      : User1|                Index      : 4820
Assigned IP   : 172.18.0.1       Public IP   : 192.168.2.20
Assigned IPv6 : 2009::1
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 27731           Bytes Rx    : 14427
Group Policy  : MyRaVpn|Policy   Tunnel Group : MyRaVpn
Login Time    : 21:58:10 UTC Mon Apr 10 2017
Duration      : 0h:51m:13s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A             VLAN        : none
Audit Sess ID : c0a800fd012d400058ebfff2
Security Grp  : none            Tunnel Zone : 0
```

ASA의 원격 액세스 VPN 구성 세부 정보 보기

단계 1 왼쪽의 CDO 탐색 모음에서 **VPN > ASA/FDM** 원격 액세스 VPN 구성을 클릭합니다.

단계 2 존재하는 VPN 구성 개체를 클릭합니다. 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

- RA VPN 구성을 확장하여 연결된 모든 연결 프로파일을 확인합니다.
 - 추가 + 버튼을 클릭하여 새 연결 프로파일을 추가합니다.
 - 보기 버튼()을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. **Actions**(작업) 아래에서 **Edit**(편집)를 클릭하여 변경 사항을 편집할 수 있습니다.
- **Actions**(작업) 아래의 다음 옵션 중 하나를 클릭하여 추가 작업을 수행할 수 있습니다.
 - 그룹 정책을 할당/추가하려면 **Group Policies**(그룹 정책)를 클릭합니다.
 - 더 이상 필요하지 않은 구성 개체 또는 연결 프로파일을 클릭하고 **Remove**(제거)를 클릭하여 삭제합니다.

ASA 템플릿

템플릿을 사용하면 사용자가 디바이스/서비스 구성을 일반적으로 구성하여 함께 그룹화된 다른 구성에 적용할 수 있습니다. 이러한 템플릿은 함께 그룹화되는 여러 구현에 영향을 주기 위해 변경을 수행할 수 있는 단일 위치를 제공합니다.

ARM 템플릿 매개변수

새 템플릿을 생성할 때 특정 디바이스를 모델로 삼을 수 있습니다. CDO는 템플릿이 모델링되는 디바이스의 구성 내에서 선택한 텍스트 필드를 기반으로 템플릿 매개변수를 설정할 수 있는 기능을 제공합니다. 템플릿 매개변수 보기 내에서 매개변수를 생성하고 기존 매개변수에서 설정하고 검색할 수 있습니다.



Note ASA 템플릿에 대한 구성을 가져오도록 선택하는 경우 구성은 JSON 형식이어야 합니다.

새 매개변수 생성

단계 1 온보딩된 기존 디바이스를 사용하여 CDO 상단에 있는 **Templates**(템플릿) 탭으로 이동합니다.

단계 2 **New Template**(새 템플릿) 또는 **Manage Templates**(템플릿 관리)를 선택합니다.

단계 3 원하는 구성을 선택하여 매개변수를 생성합니다.

단계 4 화면 상단의 **Name**(이름) 필드에 템플릿 이름을 입력합니다.

단계 5 매개변수를 추가할 텍스트 필드를 선택합니다.

단계 6 매개 변수에 설명을 제공하고 값을 추가하고 필요한 메모를 추가합니다.

단계 7 **Name**(이름) 필드 옆에 있는 **Save**(저장)를 클릭하여 매개변수를 저장합니다.

단계 8 그런 다음 **Review Template**(템플릿 검토)를 클릭하여 템플릿을 검토할 수 있습니다.

이제 이 템플릿을 사용하여 온보딩되는 모든 향후 디바이스에 적용되는 저장된 파라미터가 있습니다.

새 ASA, ISR 또는 ASR 템플릿 생성

기본 설정

알려진 ASA, ISR 또는 ASR 기본 구성으로 시작합니다. 템플릿의 매개 변수화를 시작하려면 원하는 구성을 선택합니다. 매개 변수화에는 구성 파일 내에서 필드 또는 특성을 선택하고 구성 파일 인스턴스화에서 선택될 값 목록을 식별하는 작업이 포함됩니다.



Note ASA 템플릿에 대한 구성을 가져오도록 선택하는 경우 구성은 JSON 형식이어야 합니다.

매개변수 추가

기본 구성을 선택하여 매개 변수화 프로세스를 시작할 수 있습니다. 구성 편집기에서 매개 변수화를 위해 원하는 필드를 선택합니다. 선택한 문자열은 이중 괄호로 묶여 있습니다. 왼쪽 창에서 매개 변수의 이름을 변경하고, 설명을 추가하고, 여러 값을 추가할 수 있습니다. **Allow Custom Value**(맞춤형

값 허용)를 선택하면 인스턴스화 시 맞춤형 값을 설정할 수 있습니다. 그렇지 않으면 식별된 값만 선택할 수 있습니다.

매개변수화가 완료되면 템플릿의 이름을 지정하고 **Save(저장)**를 클릭합니다.

매개변수화에 대한 자세한 내용은 [ARM 템플릿 매개변수](#)를 참조하십시오.

검토

템플릿이 저장되면 **Review(검토)**를 클릭하여 검토 프로세스로 이동합니다. 검토에서 템플릿은 매개변수가 있는 값을 포함하여 있는 그대로 내보낼 수 있습니다. 이는 반드시 유효한 구성은 아니지만 CDO에 저장된 템플릿을 검토할 수 있는 수단을 제공한다는 점에 유의하십시오. 필요한 경우 **Edit(편집)**를 클릭하여 템플릿을 편집할 수도 있습니다. **Diff(차이)** 버튼은 저장된 템플릿과 가장 최근 수정 사항 간의 차이점을 보여줍니다.

템플릿에서 ASA 구성 생성

템플릿에서 구성 생성

템플릿에서 사용자 지정 구성을 생성하는 프로세스를 시작하려면 **Config from Template(템플릿에서 구성)** 버튼을 선택합니다. 사용 가능한 템플릿이 나열됩니다. 고른 템플릿을 선택하고 **Choose Template(템플릿 선택)**을 클릭합니다.

대부분의 경우 템플릿에는 사용자 지정 구성을 제공하기 위해 **Export(내보내기)**에서 설정해야 하는 매개변수화된 값이 포함됩니다. 왼쪽 창에서 이 구성에 대해 원하는 대로 각 매개변수와 값을 선택합니다. 값이 편집기에 표시됩니다. 이는 내보낼 때 매개변수를 대체하는 값입니다. 모든 매개변수 값이 설정되면 **Export(내보내기)** 버튼을 클릭하여 구성을 내보내고 다운로드합니다. 템플릿에 매개변수화된 값이 포함되어 있지 않으면 **Export(내보내기)** 버튼을 클릭하여 구성을 있는 그대로 내보냅니다.

ASA 템플릿 관리

Manage Templates(템플릿 관리) 보기에서는 모든 기존 템플릿을 시각화하고 수정 및 삭제할 수 있습니다. 템플릿을 편집하는 동안 매개변수 설정 및 값 구성을 수정할 수 있습니다. 기존 템플릿 위에 마우스를 놓고 **Edit(수정)**를 선택하면 됩니다.

템플릿 수정

편집 보기에서 다음 작업을 수행합니다.

- 편집기에서 텍스트를 두 번 클릭하거나 강조 표시하여 매개변수를 추가합니다.
- **Description(설명)** 텍스트 상자에 입력하여 매개변수를 설명합니다. 그런 다음 **Add Value(값 추가)**를 클릭합니다.
- 값을 제공하고 메모를 작성합니다. **Add(추가)**를 클릭합니다.
- 작업이 완료되면 **Save(저장)**를 클릭합니다.

- 이제 **Review Template**(템플릿 검토)을 클릭하여 템플릿을 검토할 수 있습니다.
 - **Diff**(차이)를 클릭하여 파일을 비교할 수 있습니다.
 - 템플릿을 내보내려면 **Export**(내보내기)를 클릭합니다.

API 토큰

개발자는 CDO REST API 호출을 할 때 CDO API 토큰을 사용합니다. 호출이 성공하려면 REST API 인증 헤더에 API 토큰을 삽입해야 합니다. API 토큰은 만료되지 않는 "장기" 액세스 토큰입니다. 그러나 이를 갱신하고 취소할 수 있습니다.

CDO 내에서 API 토큰을 생성할 수 있습니다. 이러한 토큰은 생성 직후 일반 설정 페이지가 열려 있는 동안에만 표시됩니다. CDO에서 다른 페이지를 열고 일반 설정 페이지로 돌아가면, 토큰이 분명히 발급되었지만 토큰이 더 이상 표시되지 않습니다.

개별 사용자는 특정 테넌트에 대한 자체 토큰을 생성할 수 있습니다. 사용자는 다른 사용자를 대신하여 토큰을 생성할 수 없습니다. 토큰은 계정-테넌트 쌍에 고유하며 다른 사용자-테넌트 조합에 사용할 수 없습니다.

API 토큰 형식 및 클레임

API 토큰은 JSON 웹 토큰(JWT)입니다. JWT 토큰 형식에 대해 자세히 알아보려면 [JSON 웹 토큰 소개](#)를 읽어보십시오.

CDO API 토큰은 다음과 같은 클레임 집합을 제공합니다.

- **id** - 사용자/디바이스 uid
- **parentId** - 테넌트 uid
- **ver** - 공개 키의 버전(초기 버전은 0, 예, `cdo_jwt_sig_pub_key.0`)
- **subscriptions** - 보안 서비스 익스체인지 구독 (선택 사항)
- **client_id** - "api-client"
- **jti** - 토큰 ID

FDM-관리 디바이스 템플릿으로 ASA 구성 마이그레이션



Attention

Firepower Device Manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. [이 플랫폼을 활성화하려면 지원 팀에 요청을 보냅니다.](#)

Cisco Defense Orchestrator는 ASA를 FDM 관리 디바이스로 마이그레이션하는 데 도움이 됩니다. CDO는 ASA에서 실행 중인 구성의 이러한 요소를 FDM 관리 디바이스 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

- 액세스 제어 규칙(ACL)
- 인터페이스
- NAT(네트워크 주소 변환) 규칙
- 네트워크 개체 및 네트워크 그룹 개체
- 경로
- 서비스 개체 및 서비스 그룹 개체
- 사이트 간 VPN

ASA 실행 구성의 이러한 요소가 FDM 관리 디바이스 템플릿으로 마이그레이션되면 FDM 템플릿을 CDO에서 관리하는 새 FDM 관리 디바이스에 적용할 수 있습니다. FDM 관리 디바이스는 템플릿에 정의된 구성을 채택하므로, 이제 FDM 관리 디바이스는 ASA 실행 구성의 일부 측면으로 구성됩니다.

구성을 실행하는 ASA의 다른 요소는 이 프로세스를 사용하여 마이그레이션되지 않습니다. 이러한 다른 요소는 FDM 관리 디바이스 템플릿에서 빈 값으로 표시됩니다. 템플릿이 FDM 관리 디바이스에 적용되면 마이그레이션한 값을 새 FDM 관리 디바이스에 적용하고 빈 값은 무시합니다. 새 FDM 관리 디바이스의 다른 기본값은 그대로 유지됩니다. 마이그레이션하지 않은 구성을 실행하는 ASA의 다른 요소는 마이그레이션 프로세스 외부의 FDM 관리 디바이스에서 다시 생성해야 합니다.

CDO를 사용하여 ASA를 FDM 관리 디바이스로 마이그레이션하는 프로세스에 대한 전체 설명은 [Cisco Defense Orchestrator를 사용하여 ASA를 FDM 매니지드 디바이스로 마이그레이션을 참조하십시오](#).

ASA 인증서 관리

디지털 인증서는 인증 디바이스 및 개별 사용자를 위한 디지털 ID를 제공합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. "디지털 인증서"에 대한 자세한 내용은 [Cisco ASA 시리즈 일반 운영 ASDM 구성, X.Y 문서](#)에서 "디지털 인증서" 장을 참조하십시오.

CA(인증 증명)는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 ID 인증서도 발급합니다.

- ID 인증서 — ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다. CA는 ID 인증서를 발급하는데, 이는 특정 시스템이나 호스트를 위한 인증서입니다.
- 신뢰할 수 있는 CA 인증서 인증서 — 신뢰할 수 있는 CA 인증서는 다른 인증서에 서명하는 데 사용됩니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본

계약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 신뢰할 수 있는 CA 인증서는 자체 서명되며 루트 인증서라고도 합니다.

원격 액세스 VPN은 VPN 연결을 안전하게 설정하기 위해 보안 게이트웨이 및 AnyConnect 클라이언트(종단) 인증에 디지털 인증서를 사용합니다. 자세한 내용은 [원격 액세스 VPN 인증서 기반 인증](#)을 참고하십시오.

인증서 설치 가이드

ASA에서의 인증서 설치에 대한 다음 가이드를 읽어보십시오.

- 인증서는 단일 또는 여러 ASA 디바이스에 동시에 설치할 수 있습니다.
- 한 번에 하나의 인증서만 설치할 수 있습니다.
- 인증서는 라이브 ASA 디바이스에만 설치할 수 있으며 모달 디바이스에는 설치할 수 없습니다.

ASA 인증서 설치

디지털 인증서를 [트러스트 포인트 개체](#)로 업로드하고 CDO에서 관리하는 ASA 디바이스에 설치해야 합니다.



참고 ASA 디바이스에 대역 외 변경 사항이 없으며 모든 단계적 변경 사항이 구축되었는지 확인합니다.

다음에는 CDO에서 지원하는 디지털 인증서 및 형식이 나와 있습니다.

- ID 인증서는 다음 방법을 사용하여 설치할 수 있습니다.
 - PKCS12 파일 가져오기.
 - 자체 서명 인증서
 - CSR(Certificate Signing Request) 가져오기.
- 신뢰할 수 있는 CA 인증서는 PEM 또는 DER 형식을 사용하여 설치할 수 있습니다.

CDO를 사용하여 ASA에 인증서를 설치하는 단계를 보여주는 [스크린캐스트](#)를 시청하십시오. 또한 설치된 인증서를 수정, 내보내기 및 삭제하는 단계를 보여줍니다.

지원되는 인증서 형식

- PKCS12: PKCS#12, P12 또는 PFX 형식은 서버 인증서, 중간 인증서 및 개인 키를 하나의 암호화 가능한 파일에 저장하기 위한 이진 형식입니다. PFX 파일은 일반적으로 **.pfx** 및 **.p12**와 같은 확장자를 갖습니다.
- PEM: PEM(원래 "Privacy Enhanced Mail") 파일은 ASCII(또는 Base64) 인코딩 데이터를 포함하며 인증서 파일은 **.pem**, **.crt**, **.cer** 또는 **.key** 형식일 수 있습니다. 이는 Base64 인코딩 ASCII 파일이며 "-----BEGIN CERTIFICATE-----" 및 "-----END CERTIFICATE-----" 명령문을 포함합니다.

- DER: DER(Distinguished Encoding Rules) 형식은 ASCII PEM 형식이 아닌 인증서의 이진 형식입니다. 파일 확장자가 **.der**인 경우도 있지만 파일 확장자가 **.cer**인 경우도 많습니다. 따라서 DER.cer 파일과 PEM.cer 파일의 차이점을 구분하는 유일한 방법은 텍스트 편집기에서 파일을 열고 BEGIN/END 문을 찾는 것입니다. PEM과 달리 DER 인코딩 파일은 -----BEGIN CERTIFICATE-----와 같은 일반 텍스트 명령문을 포함하지 않습니다.

트러스트 포인트 화면

ASA 디바이스를 CDO에 온보딩한 후 **Devices & Services**(디바이스 및 서비스) 탭에서 ASA 디바이스를 선택하고 왼쪽의 **Management**(관리) 창에서 **Trustpoints**(트러스트 포인트)를 클릭합니다.

Trustpoints(트러스트 포인트) 탭에 디바이스에 이미 설치된 인증서가 표시됩니다.

- "Installed(설치됨)" 상태는 해당 인증서가 디바이스에 성공적으로 설치되었음을 나타냅니다.
- "Unknown(알 수 없음)" 상태는 해당 인증서에 어떤 정보도 포함되어 있지 않음을 나타냅니다. 이를 제거하고 올바른 세부 정보를 사용하여 다시 업로드해야 합니다. CDO는 모든 알 수 없는 인증서를 신뢰할 수 있는 CA 인증서로 검색합니다.
- "Installed(설치됨)"가 표시된 행을 클릭하여 오른쪽 창에서 인증서 세부 정보를 확인합니다. 선택한 인증서의 추가 세부 정보를 보려면 **more**(더 보기)를 클릭합니다.
- 설치된 ID 인증서는 PKCS12 또는 PEM 형식으로 내보내고 다른 ASA 디바이스로 가져올 수 있습니다. ID 인증서 내보내기를 참조하십시오.
- 설치된 인증서에서는 고급 설정만 수정할 수 있습니다.
 - 고급 설정을 수정하려면 **Edit**(편집)를 클릭합니다.
 - 변경한 후 **Send**(전송)를 클릭하여 업데이트된 인증서를 설치합니다.

PKCS12를 사용하여 ID 인증서 설치

PKCS12 형식으로 생성된 기존 트러스트 포인트 개체를 선택하여 ASA 디바이스에 설치할 수 있습니다. 설치 마법사에서 새 트러스트 포인트 개체를 생성하고 ASA 디바이스에 인증서를 설치할 수도 있습니다.

시작하기 전에

- [인증서 설치 가이드](#)를 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.

- a) **Devices**(디바이스) 탭을 클릭합니다.
- b) **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

- c) 오른쪽의 **Management(관리)** 창에서 **Trustpoints(트러스트 포인트)**를 클릭합니다.
- d) **Install(설치)**을 클릭합니다.

참고 여러 ASA 디바이스에 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action(디바이스 작업)**에서 **Install Certificate(인증서 설치)**를 클릭합니다.

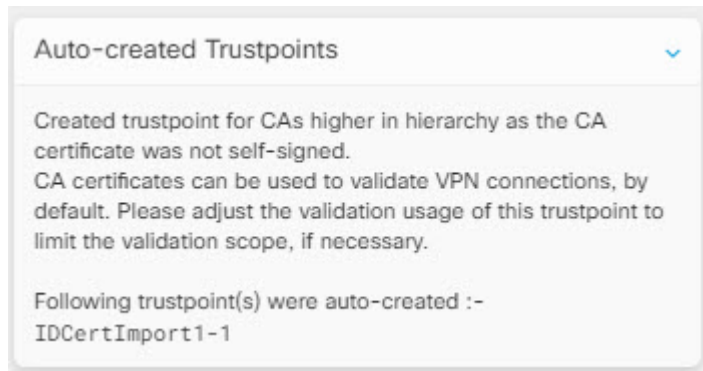
단계 3 **Select Trustpoint Certificate to Install(설치할 트러스트 포인트 인증서 선택)**에서 다음 중 하나를 클릭합니다.

- **Create(생성)**를 클릭하여 새 트러스트 포인트 개체를 추가합니다. 자세한 내용은 [PKCS12를 사용하여 ID 인증서 개체 추가](#)를 참조하십시오.
- **Choose(선택)**를 클릭하여 PKCS 유형의 인증서 등록 개체를 선택합니다.

단계 4 **Send(보내기)**를 클릭합니다.

이렇게 하면 ASA 디바이스에 인증서가 설치됩니다.

참고 중간 CA가 설치된 PKCS12 인증서를 가져오는 경우, ASA에서는 아직 설치되지 않은 모든 중간 CA 인증서에 대해 트러스트 포인트 개체를 자동으로 생성하여 디바이스에 설치합니다. ID 인증서를 클릭하면 다음 예와 같이 오른쪽 창에 메시지가 표시됩니다.



자체 서명 등록을 사용한 인증서 설치

자체 서명 인증서에 대해 생성된 기존 트러스트 포인트 개체를 선택하여 ASA 디바이스에 설치할 수 있습니다. 설치 마법사에서 새 트러스트 포인트 개체를 생성하고 ASA 디바이스에 인증서를 설치할 수도 있습니다.

시작하기 전에

- [인증서 설치 가이드](#)을 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

단계 1 내비게이션 바에서 **Devices & Services(디바이스 및 서비스)**를 클릭합니다.

단계 2 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.

- a) **Devices**(디바이스) 탭을 클릭합니다.
- b) **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.
- c) 오른쪽의 **Management**(관리) 창에서 **Trustpoints**(트러스트 포인트)를 클릭합니다.
- d) **Install**(설치)을 클릭합니다.

참고 여러 ASA 디바이스에 서명된 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action**(디바이스 작업)에서 **Install Certificate**(인증서 설치)를 클릭합니다.

단계 3 **Select Trustpoint Certificate to Install**(설치할 트러스트 포인트 인증서 선택)에서 다음 중 하나를 클릭합니다.

- **Create**(생성)를 클릭하여 새 트러스트 포인트 개체를 추가합니다. 자세한 내용은 [PKCS12를 사용하여 ID 인증서 개체 추가](#)를 참조하십시오.
- **Choose**(선택)를 클릭하여 자체 서명 인증서 유형의 인증서 등록 개체를 선택합니다.

단계 4 **Send**(보내기)를 클릭합니다.

자체 서명된 등록 유형의 트러스트 포인트의 경우 발급자 공통 이름 상태는 항상 ASA 디바이스이며 관리되는 디바이스는 자체 CA로 작동하여 자체 ID를 생성하는 CA 인증서가 필요하지 않습니다.

인증서 서명 요청(CSR) 관리

먼저 CSR 요청을 생성한 다음 신뢰할 수 있는 CA(Certificate Authority)에서 이 요청에 서명을 받아야 합니다. 그런 다음 CA에서 발급한 서명된 ID 인증서를 ASA 디바이스에 설치할 수 있습니다.

- [인증서 설치 가이드](#)을 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

다음 다이어그램은 ASA에서 CSR을 생성하고 인증된 발급 인증서를 설치하는 워크플로우를 보여줍니다.

CSR 요청 생성

-
- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.
- 단계 4 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.
- 단계 5 **Install**(설치)을 클릭합니다.
- 단계 6 **Select Trustpoint Certificate to Install**(설치할 트러스트 포인트 인증서 선택)에서 다음 중 하나를 클릭합니다.
- **Create**(생성)를 클릭하여 새 트러스트 CSR 개체를 추가합니다. 자세한 내용은 [CSR\(Certificate Signing Request\)을 위한 ID 인증서 개체 추가](#)를 참고하십시오.
 - 이미 생성된 CSR 요청 신뢰 지점을 선택하려면 **Choose**(선택)합니다.
- 단계 7 **Send**(보내기)를 클릭합니다.
- 이렇게 하면 서명되지 않은 CSR(인증서 서명 요청)이 생성됩니다.
- 단계 8 복사 아이콘 `copy_icon.png`를 클릭하여 CSR 세부 정보를 복사합니다. CSR 요청을 ".csr" 파일 형식으로 다운로드 할 수도 있습니다.
- 단계 9 **OK**(확인)를 클릭합니다.
- 단계 10 인증서에 서명하려면 인증서 서명 요청(CSR)을 인증 기관에 제출합니다.
-

인증 기관에서 발급한 서명된 ID 인증서 설치

CA가 서명된 인증서를 발급하면 ASA 디바이스에 인증서를 설치합니다.

-
- 단계 1 **Trustpoint**(트러스트 포인트) 화면에서 **Status**(상태)가 "Awaiting Signed Certificate Install(서명된 인증서 설치 대기 중)"인 CSR 요청을 클릭하고 오른쪽의 **Actions**(작업) 창에서 **Install Certified ID Certificate**(인증된 ID 인증서 설치)를 클릭합니다.
- 단계 2 CA에서 수신한 서명된 인증서를 업로드합니다. 파일을 끌어다 놓거나 제공된 필드에 내용을 붙여넣을 수 있습니다. 트러스트 포인트 명령은 선택한 트러스트 포인트를 기반으로 생성됩니다.
- 단계 3 **Send**(보내기)를 클릭합니다.
- 이렇게 하면 서명된 ID 인증서가 ASA 디바이스에 설치됩니다. 인증서를 설치하면 디바이스에 변경 사항이 즉시 구축됩니다.
- 참고 여러 ASA 디바이스에 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action**(디바이스 작업)에서 **Install Certificate**(인증서 설치)를 클릭합니다.
-

ASA에 신뢰할 수 있는 CA 인증서 설치

시작하기 전에

- [인증서 설치 가이드](#)을 읽어보십시오.
- ASA는 "Synced(동기화됨)" 및 "Online(온라인)" 상태여야 합니다.

단계 1 탐색 메뉴에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

단계 4 단일 ASA 디바이스에 ID 인증서를 설치하려면 다음을 수행합니다.

- ASA 디바이스를 선택하고 오른쪽의 **Management**(관리) 창에서 **Trustpoints**(트러스트 포인트)를 클릭합니다.
- Install**(설치)을 클릭합니다.

참고 여러 ASA 디바이스에 인증서를 설치할 수도 있습니다. 여러 ASA 디바이스를 선택하고 오른쪽의 **Devices Action**(디바이스 작업)에서 **Install Certificate**(인증서 설치)를 클릭합니다.

단계 5 **Select Trustpoint Certificate to Install**(설치할 트러스트 포인트 인증서 선택)에서 다음 중 하나를 클릭합니다.

- **Create**(생성)를 클릭하여 새 트러스트 포인트 개체를 추가합니다. 자세한 내용은 [신뢰할 수 있는 CA 인증서 개체 추가](#)을 참고하십시오.
- 신뢰할 수 있는 인증 기관 개체 선택을 **Choose**(선택)합니다.

단계 6 **Send**(보내기)를 클릭합니다.

그러면 ASA 디바이스에 신뢰할 수 있는 CA 파일이 설치됩니다.

ID 인증서 내보내기

신뢰 지점과 연결된 키 쌍 및 발급된 인증서를 PKCS12 또는 PEM 형식으로 내보내고 가져올 수 있습니다. 이 형식은 신뢰 지점 구성을 다른 ASA에서 수동으로 복제하는 데 유용합니다.

SUMMARY STEPS

1. 탐색 메뉴에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
2. **Devices**(디바이스) 탭을 클릭합니다.
3. **ASA**를 클릭합니다.
4. ASA 디바이스를 선택하고 오른쪽의 **Management**(관리)에서 **Trustpoints**(트러스트 포인트)를 클릭합니다.
5. ID 인증서를 클릭하여 인증서 구성을 내보냅니다. 또는 검색 필드에 이름을 입력하여 인증서를 검색할 수 있습니다.

6. 오른쪽의 **Actions**(작업) 창에서 **Export Certificate**(인증서 내보내기)를 클릭합니다.
7. **PKCS12 Format**(PKCS12 형식) 또는 **PEM Format**(PEM 형식)을 클릭하여 인증서 형식을 선택합니다.
8. 내보낼 PKCS12 파일을 암호화하는 데 사용한 암호화 패스프레이즈를 입력합니다.
9. 암호화 패스프레이즈를 확인합니다.
10. **Export**(내보내기)를 클릭하여 인증서 구성을 내보냅니다.

DETAILED STEPS

	명령 또는 동작	목적
단계 1	탐색 메뉴에서 Devices & Services (디바이스 및 서비스)를 클릭합니다.	
단계 2	Devices (디바이스) 탭을 클릭합니다.	
단계 3	ASA 를 클릭합니다.	
단계 4	ASA 디바이스를 선택하고 오른쪽의 Management (관리)에서 Trustpoints (트러스트 포인트)를 클릭합니다.	
단계 5	ID 인증서를 클릭하여 인증서 구성을 내보냅니다. 또는 검색 필드에 이름을 입력하여 인증서를 검색할 수 있습니다.	
단계 6	오른쪽의 Actions (작업) 창에서 Export Certificate (인증서 내보내기)를 클릭합니다.	
단계 7	PKCS12 Format (PKCS12 형식) 또는 PEM Format (PEM 형식)을 클릭하여 인증서 형식을 선택합니다.	
단계 8	내보낼 PKCS12 파일을 암호화하는 데 사용한 암호화 패스프레이즈를 입력합니다.	
단계 9	암호화 패스프레이즈를 확인합니다.	
단계 10	Export (내보내기)를 클릭하여 인증서 구성을 내보냅니다.	정보 대화 상자가 나타나 인증서 컨피그레이션 파일을 지정된 위치에 성공적으로 내보냈음을 알립니다.

설치된 인증서 편집

설치된 인증서의 고급 옵션만 수정할 수 있습니다.

단계 1 탐색 메뉴에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 4 ASA 디바이스를 선택하고 오른쪽의 **Management**(관리)에서 **Trustpoints**(트러스트 포인트)를 클릭합니다.

단계 5 수정할 인증서를 클릭하고 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 6 필수 매개변수를 수정하고 **Save(저장)**를 클릭합니다.

ASA에서 기존 인증서 삭제

인증서를 하나씩 삭제할 수 있습니다. 삭제한 인증서 컨피그레이션은 복원할 수 없습니다.

단계 1 탐색 메뉴에서 **Devices & Services(장치 및 서비스)**를 클릭합니다.

단계 2 ASA 디바이스를 선택하고 오른쪽의 **Management(관리)**에서 **Trustpoints(트러스트 포인트)**를 클릭합니다.

단계 3 삭제할 인증서를 클릭하고 오른쪽의 **Actions(작업)** 창에서 **Remove(제거)**를 클릭합니다.

단계 4 **OK(확인)**를 클릭하여 선택한 인증서를 제거합니다.

ASA 파일 관리

CDO는 ASA 디바이스의 플래시(disk0) 공간에 있는 파일 보기, 업로드 또는 삭제와 같은 기본 파일 관리 작업을 수행하기 위한 파일 관리 툴을 제공합니다.



Note disk1에 있는 파일은 관리할 수 없습니다.

File Management(파일 관리) 화면에는 디바이스의 플래시(disk0)에 있는 모든 파일이 나열됩니다. 파일 업로드에 성공하면 새로 고침 아이콘을 클릭하여 파일을 볼 수 있습니다. 기본적으로 이 화면은 10분마다 자동으로 새로 고쳐집니다. **Disk Space(디스크 공간)** 필드에는 disk0 디렉터리의 디스크 공간이 표시됩니다.

The screenshot shows the File Management interface for device BGL_ASA1. It displays a table of files on disk0 with columns for Name, Size, Path, and Last Modified Date. The first file, 'data-sources.html', is selected. The interface also shows a search bar, a 'Disk Space' indicator (7.82 GB available of 7.98 GB), and an 'Upload' button.

Name	Size	Path	Last Modified Date
<input checked="" type="checkbox"/> data-sources.html	8.58 KB	disk0:/	03:59:18 Nov 23 2020
<input type="checkbox"/> agentlog	26.45 KB	disk0:/smart-log/	05:13:49 Nov 20 2020
<input type="checkbox"/> anyconnect-linux-3.1.14018-k9.pkg	11.77 MB	disk0:/	05:18:29 Oct 28 2020
<input type="checkbox"/> data-sources.html	8.58 KB	disk0:/log/	08:14:24 Oct 27 2020
<input type="checkbox"/> asdm-7141-48.bin	34.09 MB	disk0:/	05:26:50 Sep 29 2020
<input type="checkbox"/> asa9-14-1-10-smp-k8.bin	100.34 MB	disk0:/	05:26:36 Sep 29 2020
<input type="checkbox"/> coredump.cfg	58 Bytes	disk0:/coredumpinfo/	06:25:12 May 29 2020

AnyConnect 이미지를 단일 또는 여러 ASA 디바이스에 업로드할 수 있습니다. 업로드에 성공하면 AnyConnect 이미지가 선택한 ASA 디바이스의 RA VPN 구성과 연결됩니다. 이렇게 하면 새로 릴리스된 AnyConnect 패키지를 여러 ASA 디바이스에 동시에 업로드할 수 있습니다.

플래시 시스템에 파일 업로드

CDO는 원격 서버에서의 URL 기반 파일 업로드만 지원합니다. 파일 업로드에 지원되는 프로토콜은 HTTP, HTTPS, TFTP, FTP, SMB 또는 SCP입니다. AnyConnect 소프트웨어 이미지, DAP.xml, data.xml, 호스트 스캔 이미지 파일 등의 파일을 단일 또는 여러 ASA 디바이스에 업로드할 수 있습니다.



Note 원격 서버의 URL 경로가 유효하지 않거나 발생할 수 있는 문제로 인해 CDO는 선택한 ASA 디바이스에 파일을 업로드하지 않습니다. 자세한 내용은 디바이스 워크플로우로 이동하여 알아보십시오.

디바이스가 고가용성으로 구성되어 있고 CDO가 먼저 스탠바이 디바이스에 파일을 업로드하고 업로드에 성공한 후에만 파일이 액티브 디바이스에 업로드된다고 가정합니다. 파일 제거 프로세스 중에도 동일한 동작이 적용됩니다.

파일 업로드에 지원되는 프로토콜의 syntax(명령문):

프로토콜	Syntax	예
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docsawsamazoncom/amazon/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	ftp://192.168.1.100/ftp/
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[:port]/[path/]filename]	scp://root@10.10.166/rootevents_sendpy

시작하기 전에

- ASA 디바이스에서 원격 서버에 액세스할 수 있는지 확인합니다.
- 파일이 이미 원격 서버에 업로드되었는지 확인합니다.
- ASA 디바이스에서 해당 서버로 연결되는 네트워크 경로가 있는지 확인합니다.
- FQDN이 URL에 사용되는 경우 DNS가 구성되어 있는지 확인합니다.
- 원격 서버의 URL은 인증 프롬프트가 표시되지 않는 직접 링크여야 합니다.
- 원격 서버 IP 주소가 NAT된 경우 원격 서버 위치의 NAT된 공용 IP 주소를 제공해야 합니다.



Note 패일오버에서 피어로 구성된 ASA에 파일을 업로드하는 경우 CDO는 패일오버 쌍의 다른 피어에 대한 새 파일을 승인하지 않으며 디바이스 상태가 **Not Synced**(동기화되지 않음)로 변경됩니다. CDO가 두 디바이스에서 파일을 인식하도록 하려면 두 디바이스 모두에 변경 사항을 수동으로 구축해야 합니다.

단일 ASA 디바이스에 파일 업로드

이 절차를 사용하여 파일을 단일 ASA 디바이스에 업로드합니다.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

단계 4 오른쪽의 **Management**(관리) 창에서 **File Management**(파일 관리)를 클릭합니다. 사용 가능한 디스크 공간 및 ASA 디바이스에 있는 파일을 볼 수 있습니다.

단계 5 오른쪽의 **Upload**(업로드) 버튼을 클릭합니다.

단계 6 **URL** 링크에서 파일이 사전 업로드된 서버의 경로를 지정합니다. **Destination Path**(대상 경로) 필드에는 **disk0** 디렉터리에 업로드되는 파일의 이름이 표시됩니다. **disk0** 내의 특정 디렉터리에 파일을 업로드하려면 이 필드에 파일 이름을 지정합니다. 예를 들어 **dap.xml** 파일을 "**DAPFiles**" 디렉터리에 업로드하려면 필드에 "**disk0:/DAPFiles/dap.xml**"을 지정합니다.

Note CDO ASA CLI 인터페이스에서 **dir** 명령을 실행하여 **disk0** 폴더에 있는 디렉터리를 볼 수 있습니다.

단계 7 지정된 서버 경로가 AnyConnect 파일을 가리키는 경우 **Associate file with RA VPN Configuration**(RA VPN 구성과 파일 연결) 확인란이 활성화됩니다. 참고: 이 확인란은 올바른 명명 규칙을 따르는 AnyConnect 파일 이름(예: 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg' 또는 'anyconnect-mac-xxx.pkg' 형식)에 대해서만 활성화됩니다. 이 확인란을 선택하면 CDO는 업로드에 성공한 후 AnyConnect 파일을 선택한 ASA 디바이스의 RA VPN 구성에 연결합니다.

단계 8 **Upload**(업로드)를 클릭합니다. CDO가 디바이스에 파일을 업로드합니다.

단계 9 5단계에서 AnyConnect 패키지를 RA VPN 구성과 연결하도록 선택한 경우 **CDO에서 ASA로 구성 변경 사항 구축**.

What to do next

디바이스에 구성 변경 사항을 구축할 필요가 없습니다.

여러 ASA 디바이스에 파일 업로드

이 절차를 사용하여 동시에 여러 ASA 디바이스에 파일을 업로드합니다.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 대량 업로드를 수행하려면 **ASA** 탭을 클릭하고 여러 ASA 디바이스를 선택합니다.

단계 4 오른쪽의 **Device Actions**(디바이스 작업)에서 **Upload File**(파일 업로드)를 클릭합니다. 참고: ASA 디바이스가 온라인이어야 **Upload File**(파일 업로드) 링크가 나타납니다.

단계 5 **URL** 링크에서 파일이 사전 업로드된 서버의 경로를 지정합니다. **Destination Path**(대상 경로) 필드에는 **disk0** 디렉터리에 업로드되는 파일의 이름이 표시됩니다. **disk0** 내의 특정 디렉터리에 파일을 업로드하려면 이 필드에 파일

이름을 지정합니다. 예를 들어 `dap.xml` 파일을 "`DAPFiles`" 디렉터리에 업로드하려면 필드에 "`disk0:/DAPFiles/dap.xml`"을 지정합니다.

Note CDO ASA CLI 인터페이스에서 `dir` 명령을 실행하여 `disk0` 폴더에 있는 디렉터리를 볼 수 있습니다.

단계 6 지정된 서버 경로가 AnyConnect 파일을 가리키는 경우 **Associate file with RA VPN Configuration(RA VPN 구성과 파일 연결)** 확인란이 활성화됩니다.

Note 이 확인란은 올바른 명명 규칙을 따르는 AnyConnect 파일 이름(예: '`anyconnect-win-xxx.pkg`', '`anyconnect-linux-xxx.pkg`' 또는 '`anyconnect-mac-xxx.pkg`' 형식)에 대해서만 활성화됩니다. 이 확인란을 선택하면 CDO는 업로드에 성공한 후 AnyConnect 파일을 선택한 ASA 디바이스의 RA VPN 구성에 연결합니다.

단계 7 **Upload(업로드)**를 클릭합니다.

단계 8 4단계에서 AnyConnect 패키지를 RA VPN 구성과 연결하도록 선택한 경우, **CDO에서 ASA로 구성 변경 사항 구축**.

What to do next

개별 디바이스에서 파일을 업로드하는 진행 상황을 볼 수 있습니다. ASA 디바이스를 선택하고 오른쪽의 **Management(관리)** 창에서 **File Management(파일 관리)**를 클릭합니다. 파일 업로드가 진행 중인 경우 작업이 완료될 때까지 기다립니다.

디바이스에 구성 변경 사항을 구축할 필요가 없습니다.

ASA에서 파일 제거

RA VPN 구성과 연결된 AnyConnect 파일은 제거할 수 없습니다. 해당 RA VPN 구성에서 AnyConnect 파일의 연결을 해제한 다음 파일 관리 툴에서 파일을 제거해야 합니다.



Note 페일오버에서 피어로 구성된 ASA에 파일을 업로드하는 경우 CDO는 페일오버 쌍의 다른 피어에 대한 새 파일을 승인하지 않으며 디바이스 상태가 **Not Synced(동기화되지 않음)**로 변경됩니다. CDO가 두 디바이스에서 파일을 인식하도록 하려면 두 디바이스 모두에 변경 사항을 수동으로 구축해야 합니다.

제거 작업은 선택한 파일을 플래시 메모리에서 영구적으로 삭제합니다. 파일을 삭제할 때 확인을 요청하는 메시지가 나타납니다. 선택한 ASA 디바이스에서 파일을 제거하려면 다음 절차를 수행합니다.

단계 1 내비게이션 바에서 **Devices & Services(디바이스 및 서비스)**를 클릭합니다.

단계 2 **Devices(디바이스)** 탭을 클릭합니다.

단계 3 **ASA** 탭을 클릭하고 ASA 디바이스를 선택합니다.

단계 4 오른쪽의 **Management(관리)** 창에서 **File Management(파일 관리)**를 클릭합니다.

단계 5 제거할 파일을 선택하고 오른쪽의 **Actions**(작업) 아래에서 **Remove**(제거)를 클릭합니다. 최대 25개의 파일을 선택할 수 있습니다. CDO가 일부 파일을 제거하지 못한 경우 디바이스 워크플로우를 확인하여 제거된 파일과 보존된 파일을 확인할 수 있습니다.

단계 6 AnyConnect 패키지를 제거하도록 선택한 경우 CDO에서 **ASA로 구성 변경 사항 구축**합니다.

ASA 고가용성 관리

액티브-액티브 페일오버 모드에서 ASA에 적용된 구성 변경 사항

CDO(Cisco Defense Orchestrator)는 CDO에 준비된 ASA의 실행 구성을 변경하거나 CDO에 저장된 구성을 변경할 때 구성의 해당 측면을 CDO GUI로 관리할 수 있으면 구성 파일의 관련 행만 변경하려고 시도합니다. CDO GUI를 사용하여 원하는 구성을 변경할 수 없는 경우, CDO는 변경을 위해 전체 구성 파일을 덮어쓰려고 시도합니다.

다음은 두 가지 예입니다.

- CDO GUI를 사용하여 네트워크 개체를 생성하거나 변경할 수 있습니다. CDO가 해당 변경 사항을 ASA의 구성에 배포해야 하는 경우, 변경이 발생할 때 ASA에서 실행 중인 구성 파일의 관련 줄을 덮어씁니다.
- CDO GUI를 사용하여 새 ASA 사용자를 생성할 수 없습니다. ASA의 ASDM 또는 CLI를 사용하여 새 사용자를 ASA에 추가한 경우, 해당 대역 외 변경 사항이 수락되고 CDO가 저장된 구성 파일을 업데이트하면 CDO는 CDO에 준비된 ASA의 전체 구성 파일을 덮어쓰려고 시도합니다.

ASA가 액티브-액티브 페일오버 모드에서 구성된 경우 이러한 규칙은 준수되지 않습니다. CDO가 액티브-액티브 페일오버 모드에서 구성된 ASA를 관리하는 경우 CDO가 항상 자신의 모든 구성 변경 사항을 ASA로 구축하거나 ASA의 모든 구성 변경 사항을 자신으로 읽을 수는 없습니다. 다음은 두 가지 경우입니다.

- CDO에서 수행한 ASA 구성 파일의 변경 사항(CDO GUI에서 지원하지 않는 경우)은 ASA에 구축할 수 없습니다. 또한 CDO가 지원하지 않는 구성 파일에 대한 변경 사항과 CDO가 지원하는 구성 파일에 대한 변경 사항의 조합은 ASA에 구축할 수 없습니다. 두 경우 모두 "CDO는 현재 페일오버 모드의 디바이스에 대한 전체 구성 교체를 지원하지 않습니다. Cancel(취소)을 클릭하고 디바이스에 변경 사항을 수동으로 적용하십시오." CDO 인터페이스의 메시지와 함께 Replace Configuration(구성 교체) 버튼이 비활성화되어 있습니다.
- 액티브-액티브 페일오버 모드에서 구성된 ASA에 대한 대역 외 변경 사항은 CDO에 의해 거부되지 않습니다. ASA의 실행 중인 구성을 대역 외 변경을 수행하는 경우, ASA는 Devices & Services(디바이스 및 서비스) 페이지에서 "Conflict Detected(충돌 탐지됨)"로 표시됩니다. 충돌을 검토하고 충돌을 거부하려고 하면 CDO가 해당 작업을 차단합니다. "CDO는 이 디바이스에 대한 대역 외 변경 거부를 지원하지 않습니다. 이 디바이스는 지원되지 않는 소프트웨어 버전을 실행하거나 액티브/액티브 페일오버 쌍의 멤버입니다. Continue(계속)를 클릭하여 대역 외 변경 사항을 수락하십시오."



Caution ASA에서 대역 외 변경 사항을 수락해야 하는 경우 CDO에 준비되었지만 아직 ASA에 구축되지 않은 모든 구성 변경 사항이 덮어쓰기되고 손실됩니다.

CDO는 페일오버 모드에서 ASA에 대한 구성 변경 사항이 CDO GUI에서 지원되는 경우 해당 구성 변경 사항을 지원합니다.

관련 정보:

ASA에서 DNS 구성

이 절차를 사용하여 각 ASA에서 도메인 이름 서버(DNS)를 구성합니다.

사전 요구 사항

- ASA는 인터넷에 연결되어야 합니다.
- 시작하기 전에 다음 정보를 수집합니다.
 - DNS 서버에 연결할 수 있는 ASA 인터페이스의 이름(예: 내부, 외부 또는 dmz).
 - 조직에서 사용하는 DNS 서버의 IP 주소 자체 DNS 서버를 유지 관리하지 않는 경우 Cisco Umbrella를 사용할 수 있습니다. Cisco Umbrella의 IP 주소는 208.67.220.220입니다.

절차

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **ASA** 탭을 클릭하고 DNS를 구성할 모든 ASA를 선택합니다.

단계 4 오른쪽의 Actions(작업) 창에서 **Command Line Interface**(명령줄 인터페이스)를 선택합니다.

단계 5 CLI 매크로 즐겨찾기 별을 클릭합니다.

단계 6 **Configure DNS Macro**(DNS 매크로 구성)를 선택합니다.

단계 7 **>_View Parameters**(매개변수 보기)를 선택하고 Parameters(매개변수) 열에서 다음 매개변수의 값을 입력합니다.

- IF_Name - DNS 서버에 연결할 수 있는 ASA 인터페이스의 이름입니다.
- IP_ADDR - 조직에서 사용하는 DNS 서버의 IP 주소

단계 8 **Send to devices**(디바이스로 전송)를 클릭합니다.

CDO 명령줄 인터페이스

CDO는 사용자에게 ASA 디바이스를 관리하기 위한 CLI(명령줄 인터페이스)를 제공합니다. 사용자는 단일 디바이스 또는 여러 디바이스에 동시에 명령을 전송할 수 있습니다.

관련 정보:

- 자세한 ASA CLI 설명서는 [ASA 명령줄 인터페이스 설명서](#)의 내용을 참조하십시오.

명령줄 인터페이스 사용

단계 1 **Inventory**(재고 목록) 페이지를 엽니다.

단계 2 재고 목록 테이블 위에 있는 디바이스 버튼을 클릭합니다.

단계 3 명령줄 인터페이스(CLI)를 사용하여 관리하려는 디바이스를 찾으려면 디바이스 탭과 필터 버튼을 사용합니다.

단계 4 디바이스를 선택합니다.

단계 5 **Device Actions**(장치 작업) 창에서 **> Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 **Command Line Interface**(명령줄 인터페이스) 탭을 클릭합니다.

단계 7 명령 창에 명령을 입력하고 **Send**(보내기)를 클릭합니다. 명령에 대한 디바이스의 응답은 "응답 창" 아래에 표시됩니다.

Note 실행할 수 있는 명령에 제한 사항이 있는 경우 해당 제한 사항은 명령 창 위에 나열됩니다.

Related Topics

[명령줄 인터페이스에 명령 입력](#)

명령줄 인터페이스에 명령 입력

한 줄에 하나의 명령을 입력하거나 여러 줄에 여러 명령을 순차적으로 입력할 수 있으며 CDO는 명령을 순서대로 실행합니다. 다음 ASA 예에서는 세 개의 네트워크 개체와 해당 네트워크 개체를 포함하는 네트워크 개체 그룹을 생성하는 명령 배치를 전송합니다.

```

> object network email_server_north
  host 192.168.10.2
  object network email_server_south
  host 192.168.20.2
  object network email_server_headquarters
  host 192.168.30.2
  object-group network email_servers_all
  network-object object email_server_north
  network-object object email_server_south
  network-object object email_server_headquarters
  
```

Press Cmd+Enter to send command

ASA장치 명령 입력: CDO는 ASA의 전역 구성 모드에서 명령을 실행합니다.

긴 명령: 매우 긴 명령을 입력하면 CDO는 API에 대해 모두 실행할 수 있도록 명령을 여러 명령으로 분할하려고 시도합니다. CDO가 명령을 적절하게 분리할 수 없는 경우 명령 목록을 구분할 위치에 대한 힌트를 묻는 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

오류: CDO가 600자를 초과하는 이 명령의 일부를 실행하려고 시도했습니다. 적절한 명령 구분 지점이 어디인지에 대한 힌트를 CDO에 제공할 수 있습니다. 명령 목록 사이에 빈 행을 추가하면 됩니다.

이 오류가 표시되는 경우:

단계 1 CLI 기록 창에서 오류를 일으킨 명령을 클릭합니다. CDO는 긴 명령 목록으로 명령 상자를 채웁니다.

단계 2 관련 명령 그룹 뒤에 빈 줄을 입력하여 긴 명령 목록을 편집합니다. 예를 들어 네트워크 개체 목록을 정의한 후 빈 줄을 추가하고 위의 예와 같이 그룹에 추가합니다. 명령 목록의 다양한 지점에서 이 작업을 수행할 수 있습니다.

단계 3 **Send**(보내기)를 클릭합니다.

명령 기록 작업


CLI 명령을 보낸 후 CDO는 **Command Line Interface**(명령줄 인터페이스) 페이지의 기록 창에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다.

단계 1 **Inventory**(인벤토리) 페이지에서 구성할 디바이스를 선택합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 **>_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 5 아직 확장되지 않은 경우 시계 아이콘  을 클릭하여 기록 창을 확장합니다.

단계 6 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select**(선택)합니다.

단계 7 명령 창에서 명령을 그대로 재사용하거나 편집하고 **Send**(보내기)를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

Note CDO는 다음 두 가지 상황에서 응답창에 **Done!** (완료!) 메시지를 표시합니다.

- 명령이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 **show** 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 **완료!**를 반환합니다.

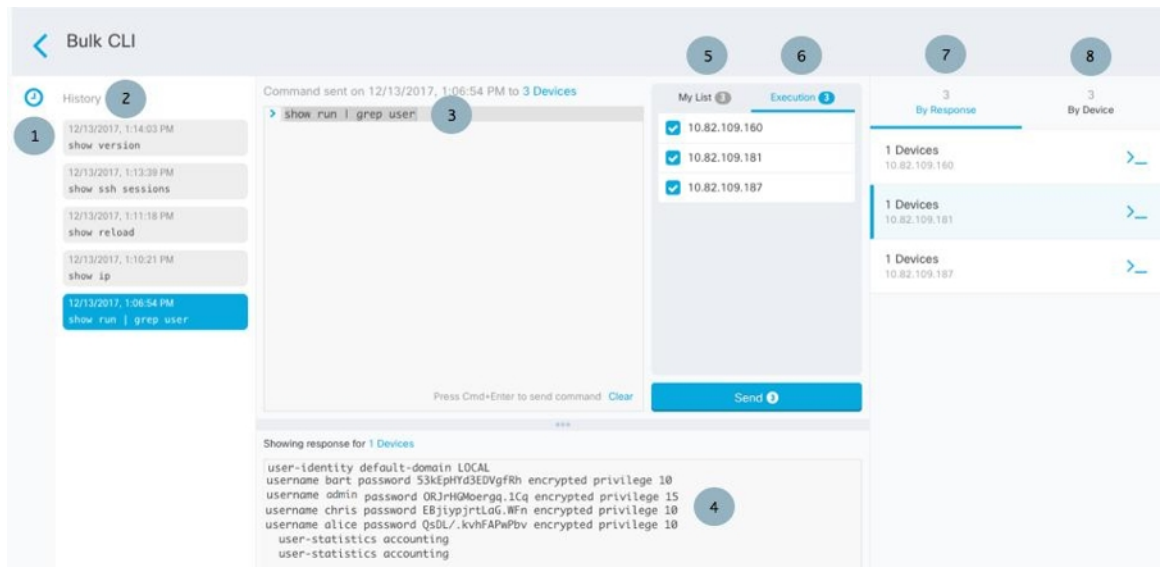
대량 명령줄 인터페이스

CDO는 CLI(command line interface)를 사용하여 Secure Firewall ASA, FDM 관리, 위협 방어, SSH 및 Cisco IOS 디바이스를 관리할 수 있는 기능을 사용자에게 제공합니다. 사용자는 단일 디바이스 또는 같은 종류의 여러 디바이스에 동시에 명령을 보낼 수 있습니다. 이 섹션에서는 한 번에 여러 디바이스에 CLI 명령을 보내는 방법을 설명합니다.

관련 정보:

- ASA CLI 설명서에 대한 자세한 설명서는 [ASA 명령줄 인터페이스 설명서](#)를 참조하십시오.

대량 CLI 인터페이스



Note CDO는 다음 두 가지 상황에서 **Done!(완료!)** 메시지를 표시합니다.

- 명령이 오류 없이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료!를 반환합니다.

숫자	설명
1	시계를 클릭하여 명령 기록 창을 확장하거나 축소합니다.
2	명령 기록. 명령을 보낸 후 CDO는 이 히스토리 창에 명령을 기록하므로 돌아가서 선택하고 다시 실행할 수 있습니다.

숫자	설명
3	명령 창. 이 창의 프롬프트에 명령을 입력합니다.
4	<p>응답 창. CDO는 명령에 대한 디바이스의 응답과 CDO 메시지를 표시합니다. 두 개 이상의 디바이스에 대한 응답이 동일한 경우 응답 창에 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.</p> <p>Note CDO는 다음 두 가지 상황에서 Done!(완료!) 메시지를 표시합니다.</p> <ul style="list-style-type: none"> • 명령이 오류 없이 성공적으로 실행된 후. • 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료!를 반환합니다.
5	My List (내 목록) 탭에는 Inventory (인벤토리) 테이블에서 선택한 디바이스가 표시되며 명령을 보낼 디바이스를 포함하거나 제외할 수 있습니다.
6	위 그림에서 강조 표시된 Execution (실행) 탭은 히스토리 창에서 선택한 명령의 디바이스를 표시합니다. 이 예에서 show run grep user 명령이 기록 창에서 선택되고 실행 탭에 10.82.109.160, 10.82.109.181 및 10.82.10.9.187로 전송된 것으로 표시됩니다.
7	By Response (응답별) 탭을 클릭하면 명령에 의해 생성된 응답 목록이 표시됩니다. 동일한 응답은 한 행에 함께 그룹화됩니다. By Response (응답별) 탭에서 행을 선택하면 CDO는 응답 창에 해당 명령에 대한 응답을 표시합니다.
8	By Device (디바이스별) 탭을 클릭하면 각 디바이스의 개별 응답이 표시됩니다. 목록에서 디바이스 중 하나를 클릭하면 특정 디바이스에서 명령에 대한 응답을 볼 수 있습니다.

대량 명령 전송

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 디바이스를 찾으려면 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 탭을 선택하고 필터 버튼을 사용하여 명령줄 인터페이스를 사용하여 구성할 디바이스를 찾습니다.

단계 4 디바이스를 선택합니다.

단계 5 **Device Actions**(장치 작업) 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 내 목록 필드에서 명령을 보낼 디바이스를 선택하거나 선택 취소할 수 있습니다.

단계 7 명령 창에 명령을 입력하고 **Send**(보내기)를 클릭합니다. 명령 출력은 응답 창에 표시되고 명령은 변경 로그에 기록되며 CDO 명령은 대량 CLI 창의 기록 창에 명령을 기록합니다.

Note 명령은 동기화된 선택된 ASA 디바이스에서 성공하고 동기화되지 않은 디바이스에서는 실패할 수 있습니다. 선택한 ASA 디바이스 중 하나라도 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `write` 및 `copy` 명령만 허용됩니다.

대량 명령 기록 작업

대량 CLI 명령을 보낸 후, CDO는 **대량 CLI 페이지** 기록에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다. 기록 창의 명령은 명령이 실행된 원래 디바이스와 연결됩니다.

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 디바이스를 찾으려면 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 필터 아이콘을 클릭하여 구성하려는 디바이스를 찾습니다.

단계 4 디바이스를 선택합니다.

단계 5 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select**(선택)합니다. 선택하는 명령은 특정 디바이스와 연결되며 반드시 첫 번째 단계에서 선택한 디바이스와 연결되지 않습니다.

단계 7 내 목록 탭을 보고 전송하려는 명령이 예상하는 디바이스로 전송되는지 확인합니다.

단계 8 명령 창에서 명령을 편집하고 **Send**(보내기)를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

Note 명령은 동기화된 선택된 ASA 디바이스에서 성공하고 동기화되지 않은 디바이스에서는 실패할 수 있습니다. 선택한 ASA 디바이스 중 하나라도 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `write` 및 `copy` 명령만 허용됩니다.

대량 명령 필터 작업

대량 CLI 명령을 실행한 후 **By Resonse**(응답별) 필터 및 **By Device**(디바이스별) 필터를 사용하여 계속해서 디바이스를 구성할 수 있습니다.

응답 기준 필터

대량 명령을 실행한 후 CDO는 명령을 보낸 디바이스에서 반환된 응답 목록으로 **By Response**(응답별) 탭을 채웁니다. 응답이 동일한 디바이스는 단일 행에 통합됩니다. **By Response**(응답별) 탭에서 행을 클릭하면 응답 창에 디바이스의 응답이 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. **X devices**(X 디바이스)를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.



명령 응답과 관련된 디바이스 목록에 명령을 보내려면 다음 절차를 따르십시오.

- 단계 1 **By Response**(응답별) 탭에서 행의 명령 기호를 클릭합니다.
- 단계 2 명령 창에서 명령을 검토하고 **Send**(보내기)를 클릭하여 명령을 다시 보내거나 **Clear**(지우기)를 클릭하여 명령 창을 지우고 디바이스로 보낼 새 명령을 입력한 다음 **Send**(보내기)를 클릭합니다.
- 단계 3 명령에서 받은 응답을 검토하십시오.
- 단계 4 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send**(보내기)를 클릭합니다. 이렇게 하면 실행 중인 구성이 시작 구성에 저장됩니다.

디바이스 기준 필터

대량 명령을 실행한 후 CDO는 실행 탭과 디바이스별 탭을 명령을 보낸 디바이스 목록으로 채웁니다. 디바이스별 탭에서 행을 클릭하면 각 디바이스에 대한 응답이 표시됩니다.

동일한 디바이스 목록에서 명령을 실행하려면 다음 절차를 따르십시오.

- 단계 1 **By Device**(디바이스 별) 탭을 클릭합니다.
- 단계 2 **>_Execute a command on these devices**(이 디바이스에서 명령 실행)를 클릭합니다.
- 단계 3 **Clear**(지우기)를 클릭하여 명령 창을 지우고 새 명령을 입력합니다.
- 단계 4 내 목록 창에서 목록의 개별 디바이스를 선택하거나 선택 취소하여 명령을 보낼 디바이스 목록을 지정합니다.
- 단계 5 **Send**(보내기)를 클릭합니다. 명령에 대한 응답이 응답 창에 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.
- 단계 6 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send**(보내기)를 클릭합니다.

명령줄 인터페이스 매크로

CLI 매크로는 즉시 사용할 수 있는 완전한 형식의 CLI 명령이거나 실행 전에 수정할 수 있는 CLI 명령의 템플릿입니다. 모든 매크로는 하나 이상의 ASA 디바이스에서 동시에 실행할 수 있습니다.

여러 디바이스에서 동일한 명령을 동시에 실행하려면 템플릿과 유사한 CLI 매크로를 사용합니다. CLI 매크로는 디바이스 구성 및 관리의 일관성을 유지합니다. 완전한 형식의 CLI 매크로를 사용하여 디바이스에 대한 정보를 가져옵니다. ASA 디바이스에서 즉시 사용할 수 있는 다양한 CLI 매크로가 있습니다.

자주 수행하는 작업을 모니터링하기 위해 CLI 매크로를 생성할 수 있습니다. 자세한 내용은 [CLI 매크로 생성](#)을 참조하십시오.

CLI 매크로는 시스템 정의 또는 사용자 정의입니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다.



Note 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

ASA를 예로 들어 ASA 중 하나에서 특정 사용자를 찾으려면 다음 명령을 실행할 수 있습니다.

```
show running-config | grep username
```

명령을 실행할 때 사용자 이름을 검색할 사용자의 사용자 이름으로 대체합니다. 이 명령으로 매크로를 만들려면 동일한 명령을 사용하고 사용자 이름을 중괄호로 묶습니다.

```
> show running-config | grep {{username}}
```

매개변수의 이름은 원하는 대로 지정할 수 있습니다. 이 매개변수 이름을 사용하여 동일한 매크로를 생성할 수도 있습니다.

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

매개변수 이름은 설명적일 수 있으며 영숫자 문자와 밑줄을 사용해야 합니다. 이 경우 명령 구문은 `show running-config | grep`


명령의 일부이며 명령을 전송하는 디바이스에 대해 적절한 CLI 구문을 사용해야 합니다.

새 명령에서 CLI 매크로 생성

단계 1 CLI 매크로를 생성하기 전에 CDO의 명령줄 인터페이스에서 명령을 테스트하여 명령 구문이 올바른지, 그리고 신뢰할 수 있는 결과를 반환하는지 확인합니다.



Note • 자세한 ASA CLI 설명서는 [ASA 명령줄 인터페이스 설명서](#)의 내용을 참조하십시오.

단계 2 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

- 단계 3 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 4 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.
- 단계 5 **>_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다.
- 단계 7 더하기 버튼  을 클릭합니다.
- 단계 8 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.
- 단계 9 **Command**(명령) 필드에 전체 명령을 입력합니다.
- 단계 10 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.
- 단계 11 **Create**(생성)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.
- 명령을 실행하려면 [디바이스에서 CLI 매크로 실행](#)을 참조하십시오.

CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성

이 절차에서는 이미 실행한 명령, 다른 사용자 정의 매크로 또는 시스템 정의 매크로에서 사용자 정의 매크로를 생성합니다.

- 단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 참고 CLI 기록에서 사용자 정의 매크로를 생성하려면 명령을 실행한 디바이스를 선택합니다. CLI 매크로는 동일한 계정의 디바이스 간에 공유되지만 CLI 기록은 공유되지 않습니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.
- 단계 4 **>_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 5 CLI 매크로를 만들려는 명령을 찾아 선택합니다. 다음 방법 중 하나를 사용합니다.
- 해당 디바이스에서 실행한 명령을 보려면 시계  를 클릭합니다. 매크로로 전환할 항목을 선택하면 명령 창에 명령이 나타납니다.
 - CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다. 변경할 사용자 정의 또는 시스템 정의 CLI 매크로를 선택합니다. 명령 창에 명령이 나타납니다.
- 단계 6 명령 창의 명령을 사용하여 CLI 매크로 금색 별  를 클릭합니다. 이 명령은 이제 새 CLI 매크로의 기본이 됩니다.
- 단계 7 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.
- 단계 8 명령 필드에서 명령을 검토하고 원하는 대로 변경합니다.
- 단계 9 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 10 **Create**(생성)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 [CLI 매크로 실행](#)을 참조하십시오.

CLI 매크로 실행

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 하나 이상의 디바이스를 선택합니다.

단계 4 **>_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 5 명령 패널에서 별표 ★를 클릭합니다.

단계 6 명령 패널에서 CLI 매크로를 선택합니다.

단계 7 다음 두 가지 방법 중 하나로 매크로를 실행합니다.

- 매크로에 정의할 매개변수가 없는 경우 **Send**(전송)를 클릭합니다. 명령에 대한 응답이 응답 창에 나타납니다. 다 됐습니다.
- 아래의 Configure DNS 매크로와 같은 매개변수가 매크로에 포함된 경우 **>_View Parameters**(매개변수 보기)를 클릭합니다.

```
★ Using Macro: Configure DNS
> dns domain-lookup {{IF_NAME}}
  dns server-group DefaultDNS
  name-server {{IP_ADDR}}
```

단계 8 **Parameters**(매개변수) 창의 **Parameters**(매개변수) 필드에 매개변수 값을 입력합니다.

Parameters
✕

Parameters	Payload
IF_NAME <input style="width: 100%;" type="text" value="outside"/>	<pre>dns domain-lookup outside dns server-group DefaultDNS name-server 208.67.220.220</pre>
IP_ADDR <input style="width: 100%;" type="text" value="208.67.220.220"/>	

Review
Send

단계 9 **Send**(보내기)를 클릭합니다. CDO가 성공적으로 명령을 전송하고 디바이스의 구성을 업데이트하면 완료됩니다!

- ASA의 경우 실행 중인 구성이 업데이트됩니다.

단계 10 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

 Some commands may have made changes to the running config Write to Disk Dismiss

- **Write to Disk**(디스크에 쓰기)를 클릭하면 이 명령의 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss**(해제)를 클릭하면 메시지가 사라집니다.

CLI 매크로 편집

사용자 정의 CLI 매크로는 편집할 수 있지만 시스템 정의 매크로는 편집할 수 없습니다. CLI 매크로를 수정하면 모든 ASA 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택합니다.

단계 5 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 편집할 사용자 정의 매크로를 선택합니다.

단계 7 매크로 레이블에서 편집 아이콘을 클릭합니다.

단계 8 Edit Macro(매크로 편집) 대화 상자에서 CLI 매크로를 편집합니다.

단계 9 **Save**(저장)를 클릭합니다.

CLI 매크로를 실행하는 방법에 대한 지침은 [Run CLI Macros\(CLI 매크로 실행\)](#)를 참조하십시오.

CLI 매크로 삭제

사용자 정의 CLI 매크로는 삭제할 수 있지만 시스템 정의 매크로는 삭제할 수 없습니다. CLI 매크로를 삭제하면 모든 디바이스에서 삭제됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.


단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택합니다.

단계 5 **> Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 삭제할 사용자 정의 CLI 매크로를 선택합니다.

단계 7 CLI 매크로 레이블에서 휴지통 아이콘 를 클릭합니다.

단계 8 CLI 매크로를 제거할지 확인합니다.

CDO CLI를 사용하여 ASA 구성

CDO에서 제공하는 CLI 인터페이스에서 CLI 명령을 실행하여 ASA 디바이스를 구성할 수 있습니다. 인터페이스를 사용하려면 **Inventory**(재고 목록) 메뉴에서 디바이스를 선택하고 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다. 자세한 내용은 [CDO 명령줄 인터페이스 사용](#)을 참조하십시오.

새 로깅 서버 추가

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다.

자세한 내용은 [실행 중인 ASA 버전의 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드](#)에서 '로깅' 장의 '모니터링' 섹션을 참조하십시오.

DNS 서버 구성

ASA에서 호스트 이름의 IP 주소를 확인할 수 있도록 DNS 서버를 구성해야 합니다. 또한 액세스 규칙에서 FQDN(Fully Qualified Domain Name) 네트워크 개체를 사용하려면 DNS 서버를 구성해야 합니다.

자세한 내용은 [실행 중인 ASA 버전의 CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드](#)에서 'DNS 서버 구성' 섹션의 '기본 설정' 장을 참조하십시오.

정적 및 기본 경로 추가

비연결 호스트 또는 네트워크에 트래픽을 라우팅하려면 정적 또는 동적 라우팅을 사용하여 해당 호스트 또는 네트워크로 가는 경로를 정의해야 합니다.

자세한 내용은 [CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드](#)의 '정적 및 기본 경로' 장을 참조하십시오.

인터페이스 구성

CLI 명령을 사용하여 관리 및 데이터 인터페이스를 구성할 수 있습니다. 자세한 내용은 [CLI 책 1: Cisco ASA 시리즈 일반 작업 CLI 구성 가이드](#)의 '기본 인터페이스 구성' 장을 참조하십시오.

CDO를 사용하여 ASA 구성 비교

이 절차를 사용하여 두 ASA의 구성을 비교합니다.

- 단계 1 내비게이션 메뉴에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(장치) 탭을 클릭하여 ASA 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 ASA 모델 디바이스를 찾습니다.
- 단계 3 **ASA** 탭을 클릭합니다.
- 단계 4 비교하려는 디바이스에 대한 디바이스 목록을 필터링합니다.
- 단계 5 두 개의 ASA를 선택합니다. 상태는 중요하지 않습니다. Defense Orchestrator에 저장된 ASA의 구성을 비교하고 있습니다.
- 단계 6 오른쪽의 디바이스 작업 창에서 **Compare**(비교)를 클릭합니다.
- 단계 7 구성 비교 대화 상자에서 **Next**(다음) 및 **Previous**(이전)를 클릭하여 구성 파일에서 과란색으로 강조 표시된 차이점을 건너뛸니다.

ASA 대량 CLI 사용 사례

ASA 디바이스에 CDO의 대량 CLI 기능을 사용할 때 발생할 수 있는 워크플로우는 다음과 같습니다.

ASA의 실행 중인 구성에 있는 모든 사용자를 표시한 다음 사용자 중 한 명 삭제

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
 - 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
 - 단계 3 **ASA** 탭을 클릭합니다.
 - 단계 4 사용자를 삭제하려는 디바이스의 디바이스 목록을 검색 및 필터링하고 선택합니다.
- Note** 선택한 디바이스가 동기화되었는지 확인합니다. 디바이스가 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `copy` 및 `write` 명령만 허용됩니다.
- 단계 5 세부 정보 창에서 **>_Command Line Interface**(명령줄 인터페이스)를 클릭합니다. CDO는 내 목록 창에서 선택한 디바이스를 나열합니다. 더 적은 수의 디바이스에 명령을 보내기로 결정한 경우 해당 목록에서 디바이스를 선택 취소하십시오.
 - 단계 6 명령 창에서 `show run | grep user`를 입력하고 **Send**(보내기)를 클릭합니다. 사용자 문자열을 포함하는 실행 중인 구성 파일의 모든 줄이 응답 창에 표시됩니다. 실행 탭이 열리고 명령이 실행된 디바이스가 표시됩니다.
 - 단계 7 **By Response**(응답별) 탭을 클릭하고 응답을 검토하여 삭제할 사용자가 있는 디바이스를 결정합니다.
 - 단계 8 내 목록 탭을 클릭하고 사용자를 삭제할 디바이스 목록을 선택합니다.
 - 단계 9 명령 창에서 `no` 형식의 `user` 명령을 입력하여 `user2`를 삭제한 다음 **Send**(보내기)를 클릭합니다. 이 예에서는 `user2`를 삭제합니다.

```
no user user2 password reallyhardpassword privilege 10
```

단계 10 사용자 이름을 검색하는 데 사용한 `show run | grep user` 명령 인스턴스에 대한 히스토리 패널을 찾습니다. 해당 명령을 선택하고 실행 목록에서 디바이스 목록을 확인한 다음 **Send**(보내기)를 선택합니다. 지정한 디바이스에서 사용자 이름이 삭제된 것을 볼 수 있습니다.

단계 11 실행 중인 구성에서 올바른 사용자를 삭제했고 올바른 사용자가 실행 중인 구성에 남아 있는 것에 만족하는 경우 다음을 수행합니다.

- a. 히스토리 창에서 `no user user2 password reallyhardpassword privilege 10` 명령을 선택합니다.
- b. **By Device**(디바이스 별) 탭을 클릭하고 이 디바이스에서 명령 실행을 클릭합니다.
- c. 명령 창에서 **Clear**(지우기)를 클릭하여 명령 창을 지웁니다.
- d. 배포 메모리 명령을 입력하고 **Send**(보내기)를 클릭합니다.

선택한 ASA에서 모든 SNMP 구성 찾기

이 절차는 ASA의 실행 중인 구성에 있는 모든 SNMP 구성 항목을 보여줍니다.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 4 실행 중인 구성에서 SNMP 구성을 분석하려는 디바이스를 필터링 및 검색하고 선택합니다.

Note 선택한 디바이스가 동기화되었는지 확인합니다. 디바이스가 동기화되지 않은 경우 `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, 및 `dir` 명령만 허용됩니다.

단계 5 세부 정보 창에서 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다. 디바이스는 내 목록 창에서 선택한 디바이스를 나열합니다. 더 적은 수의 디바이스에 명령을 보내기로 결정한 경우 해당 목록에서 디바이스를 선택 취소하십시오.

단계 6 명령 창에서 `show run | grep snmp`를 입력하고 **Send**(보내기)를 클릭합니다. `snmp` 문자열을 포함하는 실행 중인 구성 파일의 모든 줄이 응답 창에 표시됩니다. 실행 탭이 열리고 명령이 실행된 디바이스가 표시됩니다.

단계 7 응답 창에서 명령 출력을 검토합니다.

ASA 명령줄 인터페이스 설명서

CDO는 ASA 명령줄 인터페이스를 완벽하게 지원합니다. Cisco에서는 사용자가 단일 디바이스 및 여러 디바이스에 ASA 명령을 동시에 전송할 수 있도록 CDO 내에서 터미널과 유사한 인터페이스를 제공합니다. ASA 명령줄 인터페이스 설명서는 광범위합니다. CDO 설명서의 일부를 다시 작성하는 대신 Cisco.com의 ASA CLI 설명서에 대한 포인터를 제공합니다.

ASA 명령줄 인터페이스 구성 가이드

ASA 버전 9.1부터는 ASA CLI 구성 가이드가 3개의 별도 책으로 구성됩니다.

- CLI Book 1: Cisco ASA Series 일반 운영 CLI 환경 설정 가이드
- CLI Book 2: Cisco ASA Series Firewall CLI 환경 설정 가이드
- CLI Book 3: Cisco ASA Series VPN CLI 구성 가이드

Cisco.com에서 [Support\(지원\)](#) > [Products by Category\(제품\)](#) > [Security\(보안\)](#) > [Firewalls\(방화벽\)](#) > [ASA 5500\(구성\)](#) > [Configuration Guides\(구성 가이드\)](#)로 이동하여 ASA CLI 구성 가이드에 도달할 수 있습니다.

몇 가지 특정 **ASA** 명령줄 인터페이스 구성 가이드 섹션

show 및 **more** 명령 출력 필터링 정규식을 사용하여 show 명령 출력을 필터링하는 자세한 내용은 CLI 설명서 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 **show** 및 **more** 명령 출력 필터링에서 확인할 수 있습니다.

ASA 명령 참조

ASA 명령 참조 가이드에는 모든 ASA 명령 및 해당 옵션이 알파벳순으로 나열되어 있습니다. ASA 명령 참조는 버전과 관련이 없습니다. 다음의 네 가지 책으로 게시됩니다.

- Cisco ASA Series 명령 참조, A - H 명령
- Cisco ASA Series 명령 참조, I - R 명령
- Cisco ASA Series 명령 참조, S 명령
- Cisco ASA Series 명령 참조, T - Z 명령 및 ASASM에 대한 IOS 명령

Cisco.com에서 [Support\(지원\)](#) > [Products by Category\(범주별 제품\)](#) > [Security\(보안\)](#) > [Firewalls\(방화벽\)](#) > [ASA 5500\(ASA 5500\)](#) > [Reference Guides\(참조 가이드\)](#) > [Command References\(명령 참조\)](#) > [ASA Command References\(ASA 명령 참조\)](#)로 이동하여 ASA 명령 참조 가이드로 이동할 수 있습니다.

CDO CLI 명령 결과 내보내기


독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다. 내보낸 정보에는 다음이 포함됩니다.

- 디바이스
- 날짜
- 사용자
- 명령

- 출력



CLI 명령 결과 내보내기

명령 창에서 방금 실행한 명령의 결과를 .csv 파일로 내보낼 수 있습니다.

-
- 단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
 - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
 - 단계 3 해당 디바이스 탭을 클릭합니다.
 - 단계 4 디바이스를 선택하여 강조 표시하십시오.
 - 단계 5 디바이스에 대한 **Device Actions**(디바이스 작업) 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
 - 단계 6 명령줄 인터페이스 창에서 명령을 입력하고 **Send**(보내기)를 클릭하여 디바이스에 명령을 실행합니다.
 - 단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
 - 단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.
-

CLI 매크로의 결과 내보내기

명령 창에서 실행된 매크로의 결과를 내보낼 수 있습니다. 하나 이상의 디바이스에서 실행된 CLI 매크로의 결과를 .csv 파일로 내보내려면 다음 절차를 따르십시오.

-
- 단계 1 **Devices & Services**(디바이스 및 서비스) 페이지를 엽니다.
 - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
 - 단계 3 해당 디바이스 탭을 클릭합니다.
 - 단계 4 디바이스를 선택하여 강조 표시하십시오.
 - 단계 5 디바이스에 대한 **Device Actions**(디바이스 작업) 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
 - 단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표  를 선택합니다.
 - 단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send**(보내기)를 클릭합니다.
 - 단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
 - 단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.
-

CLI 명령 기록 내보내기

다음 절차를 사용하여 하나 또는 여러 디바이스의 CLI 기록을 .csv 파일로 내보냅니다.


단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.


단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택하여 강조 표시하십시오.

단계 5 디바이스에 대한 디바이스 작업 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 아직 확장되지 않은 경우 시계 아이콘  을 클릭하여 기록 창을 확장합니다.

단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.

단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

관련 정보:

- [CDO 명령줄 인터페이스](#)
- [CLI 매크로 생성](#)
- [CLI 매크로 삭제](#)
- [CLI 매크로 편집](#)
- [CLI 매크로 실행](#)
- [ASA 대량 CLI 활용 사례](#)
- [ASA 명령줄 인터페이스 설명서](#)
- [대량 명령줄 인터페이스](#)

CLI 매크로 목록 내보내기

명령 창에서 실행된 매크로만 내보낼 수 있습니다. 다음 절차를 사용하여 하나 이상의 디바이스의 CLI 매크로를 .csv 파일로 내보냅니다.

단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.


단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택하여 강조 표시하십시오.

단계 5 디바이스에 대한 디바이스 작업 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 ★를 선택합니다.

단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send**(보내기)를 클릭합니다.

단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.

단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.

ASA 구성 복원

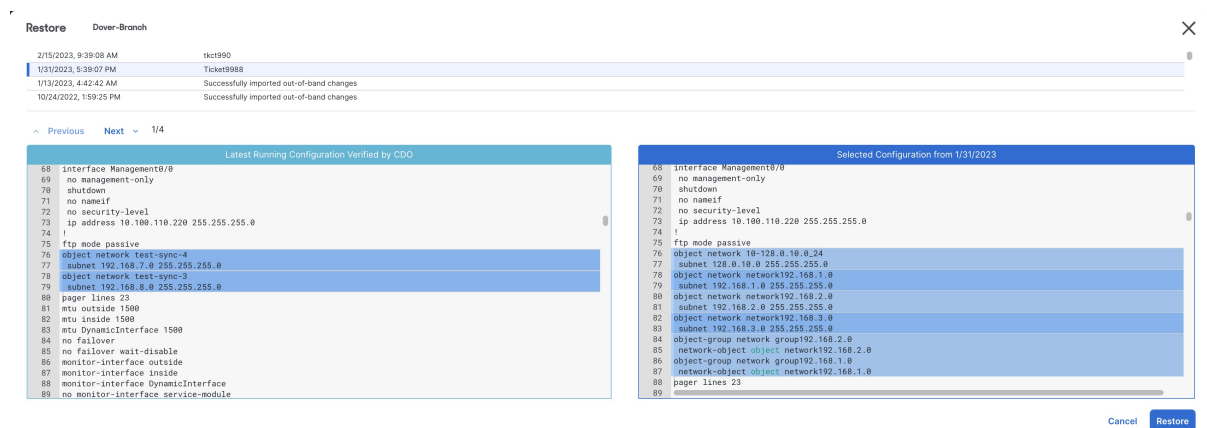
ASA의 구성을 변경하고, 변경 사항을 되돌리고자 하는 경우 ASA의 과거 구성을 복원할 수 있습니다. 이는 예기치 않거나 원치 않는 결과를 초래한 구성 변경 사항을 편리하게 제거할 수 있는 방법입니다.

ASA 구성 복원 정보

구성을 복원하기 전에 다음 참고 사항을 검토합니다.

- CDO는 복원하도록 선택한 구성을 ASA에 배포된 마지막으로 알려진 구성과 비교하지만, 복원하도록 선택한 구성을 준비되었지만 ASA에 배포되지 않은 구성과 비교하지 않습니다. ASA에 배포되지 않은 변경 사항이 있고 과거 구성을 복원하는 경우, 복원 프로세스는 배포되지 않은 변경 사항을 덮어쓰게 되며 해당 변경 사항은 손실됩니다.
- 과거 구성을 복원하기 전에, ASA이 동기화됨 또는 동기화되지 않음 상태일 수 있지만 디바이스가 충돌 감지됨 상태인 경우 과거 구성을 복원하기 전에 충돌을 해결해야 합니다.
- 과거 구성을 복원하면 배포된 모든 중간 구성 변경 사항을 덮어씁니다. 예를 들어 아래 목록에서 2023년 1월 31일의 구성을 복원하면 2023년 2월 15일에 이루어진 구성 변경 사항을 덮어씁니다.
- 다음 및 이전 버튼을 클릭하면 구성 파일을 통해 이동하고 구성 파일 변경 사항을 강조 표시합니다.
- 원래 구성 변경에 변경 요청 레이블을 적용한 경우 해당 레이블이 구성 복원 목록에 나타납니다.

Figure 1: ASA 복원 구성 화면



구성 변경 사항은 얼마 동안 유지됩니까?

1년 이하의 ASA 구성을 복원할 수 있습니다. CDO는 변경 로그에 기록된 구성 변경 사항을 복원합니다. 변경 로그는 ASA에 구성 변경 사항을 쓰거나 읽을 때마다 변경 사항을 기록합니다. CDO는 1년치 변경 로그를 저장하며, 이전 연도 내에 수행된 백업 수에는 제한이 없습니다.

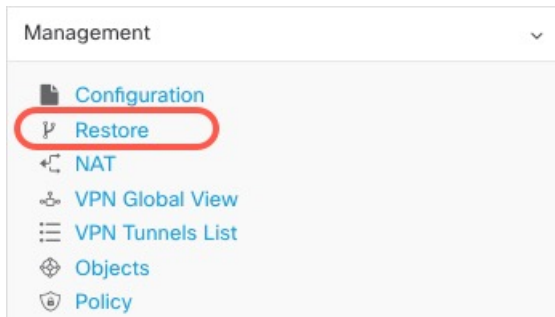
Secure Firewall ASA 구성 복원

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

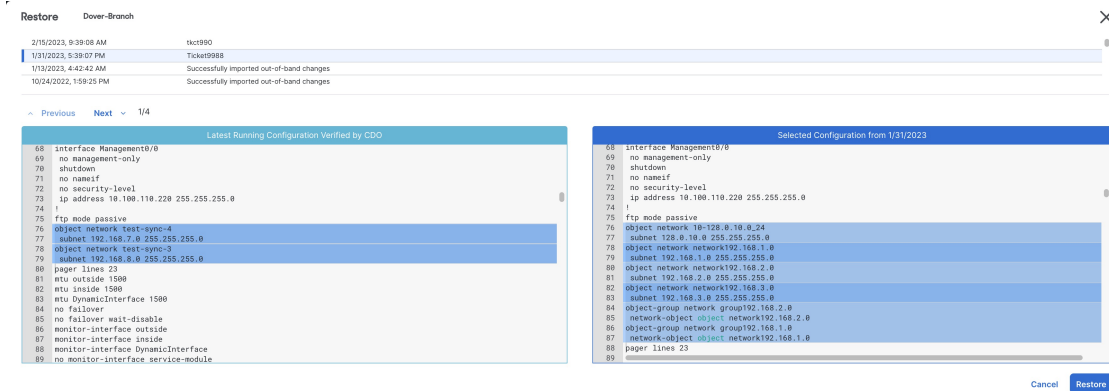
단계 2 ASA 탭을 클릭합니다.

단계 3 복원하려는 ASA 구성을 선택합니다.

단계 4 **Management**(관리) 창에서, **Restore**(복원)를 클릭합니다.



단계 5 **Restore**(복원) 페이지에서 되돌리려는 구성을 선택합니다.



예를 들어 위 그림에서 2023년 1월 31일의 구성이 선택되었습니다.

단계 6 "CDO에서 확인한 최신 실행 구성"과 "<날짜>에서 선택한 구성"을 비교하여 <날짜>에서 선택한 구성 창에 표시된 구성을 복원할 것인지 확인합니다. 이전 및 다음을 사용하여 모든 변경 사항을 비교합니다.

단계 7 **Restore**(복원)을 클릭하면 CDO에서 구성이 준비됩니다. **Inventory**(재고 관리) 페이지에서 디바이스의 구성 상태가 이제 "동기화되지 않음"임을 알 수 있습니다.

단계 8 우측 창에서 **Deploy Changes...**(변경 사항 배포...)를 클릭하여 변경 사항을 배포하고 ASA를 동기화합니다.

문제 해결

잃어버렸지만 유지하고 싶었던 변경 사항을 복원하려면 어떻게 해야 하나요?

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 4 필요한 디바이스를 선택합니다.

단계 5 오른쪽 창에서 **Change Log**(로그 변경)를 클릭합니다.

단계 6 변경 로그에서 변경 사항을 검토합니다. 해당 레코드에서 손실된 구성을 재구성할 수 있습니다.

ASA 및 Cisco IOS 디바이스 구성 파일 관리

ASA 및 Cisco IOS 디바이스와 같은 일부 유형의 디바이스는 해당 구성을 단일 파일에 저장합니다. 이러한 디바이스의 경우 Cisco Defense Orchestrator에서 구성 파일을 보고 다양한 작업을 수행할 수 있습니다.

디바이스의 구성 파일 보기

ASA, SSH 관리 디바이스 및 Cisco IOS를 실행하는 디바이스와 같이 단일 구성 파일에 전체 구성을 저장하는 디바이스의 경우 CDO를 사용하여 구성 파일을 볼 수 있습니다.



참고 SSH 관리 디바이스 및 Cisco IOS 디바이스에는 읽기 전용 구성이 있습니다.

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 보려는 구성이 있는 디바이스 또는 모델을 선택합니다.

단계 5 오른쪽의 관리 창에서 **Configuration**(구성)를 클릭합니다.
전체 구성 파일이 표시됩니다.

관련 정보:

- [디바이스 구성 파일 편집](#)

전체 디바이스 구성 파일 편집

일부 디바이스 유형은 ASA 와 같은 단일 구성 파일에 구성을 저장합니다. 이러한 디바이스의 경우 CDO에서 디바이스 구성 파일을 보고 디바이스에 따라 다양한 작업을 수행할 수 있습니다.

현재 ASA 구성 파일만 CDO를 사용하여 직접 편집할 수 있습니다.



Caution 이 절차는 디바이스 구성 파일의 구문에 익숙한 고급 사용자를 위한 것입니다. 이 방법은 Defense Orchestrator에 저장된 구성 파일의 복사본을 직접 변경합니다.

절차

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **ASA** 탭을 클릭합니다.

단계 4 구성을 편집하려는 디바이스를 선택합니다.

단계 5 오른쪽의 관리 창에서 **Configuration**(구성)를 클릭합니다.

단계 6 **Device Configuration**(디바이스 구성) 페이지에서 **Edit**(편집)를 클릭합니다.

단계 7 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, **Vim** 또는 **Emacs** 텍스트 편집기를 선택합니다.

단계 8 파일을 편집하고 변경 사항을 저장합니다.

단계 9 **Devices & Services**(디바이스 및 서비스) 페이지로 돌아가 변경 사항을 미리 보고 배포합니다.

변경 사항 읽기, 삭제, 확인 및 구축

디바이스를 관리하려면 CDO의 로컬 데이터베이스에 저장된 디바이스 구성의 자체 복사본이 있어야 합니다. CDO는 관리하는 디바이스에서 구성을 "읽을 때" 디바이스 구성의 복사본을 가져와 저장합니다. CDO가 디바이스 구성의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 이러한 선택 항목은 다양한 목적으로 구성을 읽는 것을 설명합니다.

- **Discard Changes**(변경 사항 취소)는 디바이스의 구성 상태가 "Not Synced(동기화되지 않음)"인 경우에 사용할 수 있습니다. Not Synced(동기화되지 않음) 상태에서는 CDO에서 보류 중인 디바이스의 구성에 대한 변경 사항이 있습니다. 이 옵션을 사용하면 보류 중인 모든 변경 사항을 취소할 수 있습니다. 보류 중인 변경 사항이 삭제되고 CDO가 디바이스에 저장된 구성의 복사본으로 구성의 복사본을 덮어씁니다.
- 변경 사항을 확인합니다. 이 작업은 디바이스의 구성 상태가 동기화된 경우에 사용할 수 있습니다. **Checking for Changes**(변경 사항 확인)를 클릭하면 CDO가 디바이스의 구성 복사본을 디바이스에 저장된 구성의 복사본과 비교하게 됩니다. 차이가 있는 경우 CDO는 디바이스에 저장된 복사본으로 디바이스 구성의 복사본을 즉시 덮어씁니다.

- 충돌을 검토하고 검토 없이 수락합니다. 디바이스에서 **Conflict Detection(충돌 탐지)**을 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 디바이스에 저장된 구성의 복사본이 변경된 경우 CDO는 "Conflict Detected(충돌 탐지됨)" 구성 상태를 표시하여 사용자에게 알립니다.
 - 충돌을 검토합니다. **Review Conflict(충돌 검토)**를 클릭하면 디바이스에서 직접 변경 사항을 검토하고 이를 수락하거나 거부할 수 있습니다.
 - 검토 없이 수락합니다. 이 작업은 CDO의 디바이스 구성 복사본을 디바이스에 저장된 구성의 최신 복사본으로 덮어씁니다. CDO에서는 덮어쓰기 작업을 수행하기 전에 구성의 두 복사본에서 차이점을 확인하라는 메시지를 표시하지 않습니다.

모두 읽기는 대량 작업입니다. 상태에 상관없이 둘 이상의 디바이스를 선택하고 **Read All(모두 읽기)**을 클릭하여 CDO에 저장된 모든 디바이스의 구성을 디바이스에 저장된 구성으로 덮어쓸 수 있습니다.

변경 사항 구축

디바이스의 구성을 변경하면 CDO는 변경 사항을 구성의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 구축될 때까지 CDO에서 "보류 중"입니다. 디바이스에 구축되지 않은 설정 변경 사항이 있는 경우 디바이스는 동기화되지 않음 설정 상태가 됩니다.

보류 중인 구성 변경 사항은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 구축한 후에야 적용됩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다. 구축은 단일 디바이스 또는 둘 이상의 디바이스에서 동시에 시작할 수 있습니다.



참고 구축 또는 반복 구축을 예약할 수 있습니다. 자세한 내용은 [자동 구축 예약, 219 페이지](#)를 참조하십시오.

Discard All(모두 취소)은 **Preview and Deploy(미리보기 및 구축)...**를 클릭한 후에만 사용할 수 있는 옵션입니다. **Preview and Deploy(미리보기 및 구축)**를 클릭하면 CDO는 CDO에 보류 중인 변경 사항의 미리보기를 표시합니다. **Discard All(모두 취소)**을 클릭하면 CDO에서 보류 중인 모든 변경 사항이 삭제되며 선택한 디바이스에 어떤 것도 구축되지 않습니다. 위의 "변경 사항 취소"와 달리 보류 중인 변경 사항을 삭제하면 작업이 종료됩니다.

모든 디바이스 구성 읽기

CDO(Cisco Defense Orchestrator) 외부의 디바이스에 대한 구성이 변경되면 CDO에 저장된 디바이스의 구성과 디바이스 구성의 로컬 복사본은 더 이상 동일하지 않습니다. 구성을 다시 동일하게 만들기 위해 디바이스에 저장된 구성으로 CDO의 디바이스 구성 복사본을 덮어쓰려는 경우가 많습니다.

Read All(모두 읽기) 링크를 사용하여 여러 디바이스에서 동시에 이 작업을 수행할 수 있습니다.

CDO에서 디바이스 구성의 두 복사본을 관리하는 방법에 대한 자세한 내용은 [변경 사항 읽기, 삭제, 확인 및 구축](#)을 참조하십시오.

다음은 **Read All**(모두 읽기)을 클릭하면 CDO의 디바이스 구성 복사본을 디바이스의 구성 복사본으로 덮어쓰는 세 가지 구성 상태입니다.

- 충돌 탐지 - 충돌 탐지가 활성화된 경우 CDO는 구성 변경 사항에 대해 10분마다 관리하는 디바이스를 폴링합니다. CDO는 디바이스의 구성이 변경된 것을 발견하면 디바이스에 대한 구성 상태를 "충돌 탐지됨"으로 표시합니다.
- 동기화됨 - 디바이스가 동기화된 상태인 경우 **Read All**(모두 읽기)을 클릭하면 CDO는 즉시 디바이스를 확인하여 구성이 직접 변경되었는지 확인합니다. **Read All**(모두 읽기)을 클릭하면 CDO가 디바이스 구성의 복사본을 덮어쓸 것임을 확인한 다음 덮어쓰기를 수행합니다.
- 동기화되지 않음 - 디바이스가 Not Synced(동기화되지 않음) 상태인 경우 **Read All**(모두 읽기)을 클릭하면 CDO는 CDO를 사용하는 디바이스의 구성에 대해 보류 중인 변경 사항이 있으며 **Read All**(모두 읽기) 작업을 진행하면 해당 변경 사항이 삭제되고 디바이스의 구성이 포함된 CDO의 구성 복사본입니다. 이 **Read All**(모두 읽기)은 [변경 사항 취소](#)와 같은 기능을 합니다.

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 (선택 사항) 변경 로그에서 이 대량 작업의 결과를 쉽게 식별할 수 있도록 [변경 요청 레이블](#)을 생성합니다.

단계 5 CDO를 저장할 디바이스를 선택합니다. CDO는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 6 **Read All**(모두 읽기)을 클릭합니다.

단계 7 CDO는 CDO에 준비된 구성 변경 사항이 있는 경우 선택한 디바이스에 대해 경고하고, 구성 대량 읽기 작업을 계속할 것인지 묻습니다. 계속하려면 **Read All**(모두 읽기)을 클릭합니다.

단계 8 **Read All**(모두 읽기) 구성 작업의 진행 상황은 [알림 탭](#)에서 확인합니다. 대량 작업의 개별 작업이 성공하거나 실패한 방식에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 [Jobs\(작업\)](#) 페이지로 이동합니다.

단계 9 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

관련 정보

- [변경 사항 읽기, 삭제, 확인 및 구축](#)
- [변경 사항 취소](#)
- [구성 변경 사항 확인](#)

ASA에서 CDO로 구성 변경 사항 읽기

Cisco Defense Orchestrator가 ASA 구성을 "읽는" 이유는 무엇입니까?

ASA를 관리하려면, CDO에 ASA의 실행 중인 구성 파일의 자체 저장된 복사본이 있어야 합니다. CDO가 디바이스 구성 파일의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 이후에 CDO가 ASA에서 구성을 읽을 때, 변경 사항 확인, 검토 없이 수락 또는 구성 읽기를 선택하게 됩니다. 자세한 내용은 [변경 사항 읽기](#), [삭제](#), [확인 및 구축](#)를 참조하십시오.

CDO는 또한 다음과 같은 상황에서 ASA 구성을 읽어야 합니다.

- 구성 변경 사항을 ASA에 배포하지 못했고 디바이스 상태가 목록에 없거나 동기화되지 않음입니다.
- 디바이스 온보딩에 실패했으며 디바이스 상태가 구성 없음입니다.
- CDO 외부에서 디바이스 구성을 변경했으며 변경 사항이 폴링되거나 감지되지 않았습니다. 디바이스 상태는 동기화됨 또는 충돌 감지됨입니다.

이러한 경우 CDO는 디바이스에 저장된 마지막으로 알려진 구성의 복사본이 필요합니다.

ASA에서 구성 변경 사항 읽기

ASA에서 구성 변경 사항을 읽으라는 메시지가 표시되는 경우:

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 CDO가 최근 온보딩에 실패한 디바이스 또는 CDO가 변경 사항을 배포하지 못한 디바이스를 선택합니다.

단계 5 오른쪽의 동기화됨 창에서 **Read Configuration**(구성 읽기)를 클릭합니다. 이 옵션은 현재 CDO에 저장된 구성을 덮어씁니다.

모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축

테넌트의 디바이스에 대한 구성을 변경했지만 해당 변경 사항을 구축하지 않은 경우 **Deploy**(구축) 아이콘




. 이러한 변경의 영향을 받는 디바이스는 **Devices and Services**(디바이스 및 서비스) 페이지에서 "Not Synced(동기화되지 않음)" 상태로 표시됩니다. **Deploy**(구축)를 클릭하면 보류 중인 변경 사항이 있는 디바이스를 검토하고 해당 디바이스에 변경 사항을 구축할 수 있습니다.



참고 사용자가 생성하고 변경하는 모든 새로운 FDM 또는 FTD 네트워크 개체 또는 그룹에 대해 CDO는 CDO에서 관리하는 모든 온프레미스 Management Center에 대해 이 페이지에서 항목을 생성합니다.

이 구축 방법은 지원되는 모든 디바이스에서 사용할 수 있습니다.

단일 구성 변경 사항에 이 구축 방법을 사용하거나, 기다렸다가 여러 변경 사항을 한 번에 구축할 수 있습니다.

- 단계 1 화면의 오른쪽 상단에서 **Deploy**(구축) 아이콘  을 클릭합니다.
- 단계 2 구축하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 구축할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 구축할 수 없는 이유를 확인할 수 있습니다.
- 단계 3 (선택 사항) 보류 중인 변경 사항에 대한 자세한 정보를 보려면 **View Detailed Changelog**(자세한 변경 로그 보기) 링크를 클릭하여 해당 변경과 관련된 변경 로그를 엽니다. **Deploy**(구축) 아이콘을 클릭하여 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지로 돌아옵니다.
- 단계 4 (선택 사항) **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에서 나가지 않고 변경 사항을 추적하려면 **변경 요청을 생성**합니다.
- 단계 5 선택한 디바이스에 변경 사항을 즉시 구축하려면 **Deploy Now**(지금 구축)를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.
- 단계 6 (선택 사항) 구축이 완료되면 CDO 탐색 모음에서 **Jobs**(작업)를 클릭합니다. 구축 결과를 보여주는 최근 "Deploy Changes(변경 사항 구축)" 작업이 표시됩니다.
- 단계 7 변경 요청 레이블을 생성했으며 더 이상 연결할 구성 변경 사항이 없는 경우 해당 레이블을 지웁니다.

다음에 수행할 작업

- 예약된 자동 배포
- CDO에서 ASA로 구성 변경 사항 구축, 213 페이지
- ASA에 구축한 후 로그 항목 변경

CDO에서 ASA로 구성 변경 사항 구축

CDO가 ASA에 변경 사항을 구축하는 이유

CDO(Cisco Defense Orchestrator)를 사용하여 디바이스의 구성을 관리하고 변경하면 CDO는 변경 사항을 구성 파일의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 "구축"될 때까지 CDO에서 "준비된" 것으로 간주됩니다. 준비된 구성 변경은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 "구축"한 후에야 디바이스를 통해 실행되

는 트래픽에 영향을 미칩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다.

ASA에는 "실행 중인" 구성 파일("실행 중인 구성"이라고도 함)과 "시작" 구성 파일("시작 구성"이라고도 함)이 있습니다. 실행 중인 구성 파일에 저장된 구성은 ASA를 통과하는 트래픽에 적용됩니다. 실행 중인 구성을 변경하고 해당 변경 사항이 생성하는 동작에 만족하면 시작 구성에 구축할 수 있습니다. ASA가 재부팅된 경우 시작 구성을 구성 시작점으로 사용합니다. 시작 구성에 저장되지 않은 실행 중인 구성에 대한 변경 사항은 ASA가 재부팅된 후 손실됩니다.

CDO에서 ASA로 변경 사항을 구축할 때는 실행 중인 구성 파일에 해당 변경 사항을 기록합니다. 이러한 변경 사항으로 인해 생성되는 동작에 만족하면 해당 변경 사항을 시작 구성 파일에 구축할 수 있습니다.

구축은 단일 디바이스 또는 둘 이상의 디바이스에서 동시에 시작할 수 있습니다. 단일 디바이스에 대해 개별 구축 또는 반복 구축을 예약할 수 있습니다.

일부 변경 사항은 ASA에 직접 구축됩니다.

CDO에서 CLI 인터페이스 CLI 매크로 인터페이스를 사용하여 ASA를 변경하는 경우 이러한 변경 사항은 CDO에서 "스테이징"되지 않습니다. ASA의 실행 중인 구성에 직접 구축됩니다. 이러한 방식으로 변경하면 디바이스는 CDO와 "동기화"된 상태로 유지됩니다.

구성 변경 사항 배포 정보

이 섹션에서는 CDO의 GUI를 사용하거나 CDO의 CLI 인터페이스 또는 CLI 매크로 인터페이스를 사용하지 않고 디바이스 구성 페이지를 편집하여 ASA 구성 파일을 변경한다고 가정합니다.

ASA 구성 업데이트는 2단계 프로세스입니다.

단계 1 다음 방법 중 하나를 사용하여 CDO를 변경합니다.

- CDO GUI
- 디바이스 구성 페이지의 디바이스 구성

단계 2 변경한 후 **Inventory**(재고 목록) 페이지로 돌아간 다음 디바이스에 대한 변경 사항을 미리 보고 구축...합니다.

다음에 수행할 작업

CDO가 ASA의 실행 구성을 CDO에 준비된 구성으로 업데이트하거나 ASA에 저장된 실행 구성으로 CDO의 구성을 변경할 때 구성의 해당 측면을 CDO GUI로 관리할 수 있으면 구성 파일의 관련 행만 변경하려고 시도합니다. CDO GUI를 사용하여 원하는 구성을 변경할 수 없는 경우, CDO는 변경을 위해 전체 구성 파일을 덮어쓰려고 시도합니다.

다음은 두 가지 예입니다.

- CDO GUI를 사용하여 네트워크 개체를 생성하거나 변경할 수 있습니다. CDO가 해당 변경 사항을 ASA의 구성에 배포해야 하는 경우, 변경이 발생할 때 ASA에서 실행 중인 구성 파일의 관련 줄을 덮어씁니다.
- CDO GUI를 사용하여 새 로컬 ASA 사용자를 생성할 수 없지만, 디바이스 구성 페이지에서 ASA의 구성을 편집하여 생성할 수 있습니다. 디바이스 구성 페이지에서 사용자를 추가하고 해당 변경 사항을 ASA에 배포하는 경우, CDO는 실행 중인 전체 구성 파일을 덮어써 해당 변경 사항을 ASA에서 실행 중인 구성 파일에 저장하려고 합니다.


CDO GUI를 사용하여 구성 변경 사항 구축

단계 1 CDO GUI를 사용하여 구성을 변경하고 변경 사항을 저장하면 해당 변경 사항은 실행 중인 ASA 구성 파일의 CDO에 저장된 버전에 저장됩니다.

단계 2 **Inventory**(재고 목록) 페이지의 디바이스로 돌아갑니다.

단계 3 **Devices**(디바이스) 탭을 클릭합니다. 이제 디바이스가 "동기화되지 않음"으로 표시됩니다.

단계 4 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면의 오른쪽 상단에 있는 **Deploy**(구축) 아이콘  을 클릭합니다. 이렇게 하면 디바이스에 대한 변경 사항을 구축하기 전에 검토할 수 있습니다. 변경한 디바이스를 확인하고 디바이스를 확장하여 변경 사항을 검토한 후 **Deploy Now**(지금 구축)를 클릭하여 변경 사항을 구축합니다.

참고 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 변경 사항을 구축할 수 없습니다. 디바이스에 변경 사항을 구축할 수 없는 이유를 알아보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- **Not Synced**(동기화되지 않음) 창에서 **Preview and Deploy**(미리보기 및 구축)...를 클릭합니다.

1. ASA 구성 파일을 변경하는 명령을 검토합니다.
2. 명령에 만족하는 경우 **Configuration Recovery Preference**(구성 복구 기본 설정)를 선택합니다.

참고 "알려주시면 구성을 수동으로 복원하겠습니다."를 선택합니다. 계속하기 전에 **View Manual Synchronization Instructions**(수동 동기화 지침 보기)를 클릭합니다.

3. **Apply Changes to Device**(변경 사항 적용)를 클릭합니다.
4. 성공 메시지에서 확인하려면 **OK**(확인)를 클릭합니다.

자동 배포 예약

또한 **자동 구축 예약**하여 단일 디바이스 또는 보류 중인 변경 사항이 있는 모든 디바이스에 대한 배포를 예약하도록 테넌트를 구성할 수 있습니다.

CDO의 CLI 인터페이스를 사용하여 구성 변경 사항 배포

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 구성을 변경하려는 디바이스를 선택합니다.

단계 5 **Actions**(작업) 창에서 **>_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 명령줄 인터페이스 테이블에 명령이 있으면 **Clear**(지우기)를 클릭하여 제거합니다.

단계 7 명령줄 인터페이스 테이블의 상단 상자에 명령 프롬프트에 명령을 입력합니다. 각 명령을 해당 줄에 입력하거나 구성 파일의 섹션을 명령으로 입력하여 단일 명령 또는 여러 명령을 일괄적으로 실행할 수 있습니다. 다음은 명령줄 인터페이스 테이블에 입력할 수 있는 몇 가지 명령의 예입니다.

네트워크 개체 "albany"를 생성하는 단일 명령

```
object network albany
host 209.165.30.2
```

여러 명령이 함께 전송됨:

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

명령으로 입력된 실행 중인 구성 파일의 섹션:

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

참고 CDO는 EXEC 모드, Privileged EXEC 모드 및 전역 구성 모드 사이를 이동할 필요가 없습니다. 적절한 맥락에서 입력한 명령을 해석합니다.

단계 8 명령을 입력한 후 **Send**(보내기)를 클릭합니다. CDO가 ASA에서 실행 중인 구성 파일에 대한 변경 사항을 성공적으로 배포한 후 **Done!**(완료!)를 수신합니다.

단계 9 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

- **Deploy to Disk**(디스크에 배포)를 클릭하면 이 명령에 의해 변경된 사항과 실행 중인 구성의 다른 모든 변경 사항이 ASA의 시작 구성에 저장됩니다.
- **Dismiss**(해제)를 클릭하면 메시지가 사라집니다.

디바이스 구성을 편집하여 구성 변경 사항 배포




주의 이 절차는 ASA 구성 파일의 구문에 익숙한 고급 사용자를 위한 것입니다. 이 방법은 CDO에 저장된 실행 중인 구성 파일을 직접 변경합니다.

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 구성을 변경하려는 디바이스를 선택합니다.
- 단계 5 작업 창에서 **View Configuration**(구성 보기)를 클릭합니다.
- 단계 6 **Edit**(편집)를 클릭합니다.
- 단계 7 실행 중인 구성을 변경하고 **Save**(저장)합니다.
- 단계 8 **Inventory**(재고 목록) 페이지로 돌아갑니다. 동기화되지 않은 창에서 **Preview and Deploy...**(미리보기 및 배포...)를 클릭합니다.
- 단계 9 디바이스 동기화 창에서 변경 사항을 검토합니다.
- 단계 10 변경 종류에 따라 **Replace Configuration**(구성 대체) 또는 **Apply Changes to Device**(디바이스에 변경 적용)를 클릭합니다.

여러 디바이스에서 공유 개체에 대한 구성 변경 사항 배포

두 개 이상의 디바이스에서 공유하는 정책 또는 개체를 변경할 때 이 절차를 사용합니다. 그러나 많은 디바이스에서 공통 정책을 사용하는 경우 공통 정책을 변경할 수 있습니다.

- 단계 1 편집할 공유 개체가 포함된 정책 페이지 또는 개체 페이지를 열고 편집합니다.
- 단계 2 공유 디바이스 목록을 검토하고 언급된 모든 디바이스에서 변경할 것인지 확인합니다.
- 단계 3 **OK**(확인)를 클릭합니다.
- 단계 4 **Save**(저장)를 클릭합니다.
- 단계 5 **Deploy**(배포) 아이콘  을 클릭하고 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

디바이스 구성 대량 구축

예를 들어 공유 개체를 수정하여 여러 디바이스를 변경한 경우 해당 변경 사항을 영향을 받는 모든 디바이스에 한 번에 적용할 수 있습니다.


단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.


단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 CDO에서 구성을 변경한 모든 디바이스를 선택합니다. 이러한 디바이스는 "동기화되지 않음" 상태로 표시되어야 합니다.

단계 5 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면 오른쪽 상단의  버튼을 클릭하여 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 창을 엽니다. 이렇게 하면 구축하기 전에 선택한 디바이스에서 보류 중인 변경 사항을 검토할 수 있습니다. **Deploy Now**(지금 구축)를 클릭하여 변경 사항을 구축합니다.

Note **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 해당 디바이스에 변경 사항을 구축할 수 없습니다. 변경 사항을 해당 디바이스에 구축할 수 없는 이유에 대한 정보를 보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- 세부 정보 창에서 **Deploy All**(모두 구축)  을 클릭합니다. 경고를 검토하고 **OK**(확인)를 클릭합니다. 대량 구축은 변경 사항을 검토하지 않고 즉시 시작됩니다.

단계 6 (선택 사항) 탐색 모음에서 **Jobs**(작업) 아이콘  을 클릭하여 대량 구축의 결과를 확인합니다.

관련 정보:

- [자동 구축 예약, on page 219](#)

예약된 자동 배포

CDO를 사용하면 CDO에서 관리하는 하나 이상의 디바이스에 대한 구성을 변경한 다음 편리한 시간에 해당 디바이스에 변경 사항을 배포하도록 예약할 수 있습니다.

Settings(설정) 페이지의 **Tenant Settings**(테넌트 설정) 탭에 **자동 구축 예약 옵션 활성화** 있는 경우에만 배포를 예약할 수 있습니다. 이 옵션이 활성화되면 예약된 배포를 생성, 편집 또는 삭제할 수 있습니다. 예약된 배포는 CDO에 저장된 모든 단계적 변경 사항을 설정된 날짜 및 시간에 배포합니다. **Jobs**(작업) 페이지에서 예약된 배포를 보고 삭제할 수도 있습니다.

CDO에서 **변경 사항 읽기, 삭제, 확인 및 구축** 않은 디바이스 변경 사항이 있는 경우 충돌이 해결될 때까지 예약된 배포를 건너뛵니다. 예약된 배포가 실패한 인스턴스가 **Jobs**(작업) 페이지에 나열됩니다.

Enable the Option to Schedule Automatic Deployments(자동 구축 예약 옵션 활성화)가 해제된 경우 예약된 모든 배포가 삭제됩니다.



Caution 여러 디바이스에 대해 새 배포를 예약하는 경우 해당 디바이스 중 일부가 이미 배포를 예약한 경우, 새로 예약된 배포가 기존의 예약된 배포를 덮어씁니다.



Note 예약된 배포를 생성하면 디바이스의 표준 시간대가 아닌 현지 시간으로 일정이 생성됩니다. 예약된 배포는 일광 절약 시간에 맞게 자동으로 조정되지 않습니다.

자동 구축 예약

구축 일정은 단일 이벤트 또는 반복 이벤트일 수 있습니다. 반복 자동 구축을 사용하면 유지 보수 기간에 맞춰 반복 구축을 편리하게 이용할 수 있습니다. 단일 디바이스에 대해 일회성 또는 반복 구축을 예약하려면 다음 절차를 따르십시오.



Note 기존 구축이 예약된 디바이스에 대한 구축을 예약하는 경우 새로 예약된 구축이 기존 구축을 덮어씁니다.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 하나 이상의 디바이스를 선택합니다.

단계 5 **Device Details**(디바이스 세부 정보) 창에서 **Scheduled Deployments**(예약된 구축) 탭을 찾아 **Schedule**(예약)을 클릭합니다.

단계 6 구축을 수행해야 하는 시기를 선택합니다.

- 일회성 구축의 경우 **Once on**(한 번) 옵션을 클릭하여 달력에서 날짜와 시간을 선택합니다.
- 반복 구축의 경우 **Every**(마다) 옵션을 클릭합니다. 매일 또는 일주일에 한 번 구축을 선택할 수 있습니다. 구축을 수행해야 하는 날짜와 시간을 선택합니다.

단계 7 **Save**(저장)를 클릭합니다.

예약된 배포 편집

예약된 배포를 편집하려면 다음 절차를 따르십시오.

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 하나 이상의 디바이스를 선택합니다.

단계 5 **Device Details**(디바이스 세부 정보) 창에서 예약된 배포 탭을 찾아 **Edit**(편집)를 클릭합니다.



단계 6 예약된 배포의 반복, 날짜 또는 시간을 편집합니다.

단계 7 **Save**(저장)를 클릭합니다.

예약된 배포 삭제

예약된 배포를 삭제하려면 다음 절차를 따르십시오.




Note 여러 디바이스에 대한 배포를 예약한 다음 일부 디바이스에 대한 일정을 변경하거나 삭제하면 나머지 디바이스에 대한 원래 예약된 배포가 유지됩니다.

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 하나 이상의 디바이스를 선택합니다.

단계 5 **Device Details**(장치 세부 정보)창에서 예약된 배포 탭을 찾아 **Delete**(삭제) 를 클릭합니다.

What to do next

- 변경 사항 읽기, 삭제, 확인 및 구축
- 모든 디바이스 구성 읽기, [on page 210](#)
- CDO에서 ASA로 구성 변경 사항 구축, [on page 213](#)
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, [on page 212](#)

구성 변경 사항 확인

디바이스의 구성이 디바이스에서 직접 변경되었으며 CDO에 저장된 구성의 복사본과 더 이상 동일하지 않은지 확인하려면 변경 사항을 확인합니다. 디바이스가 "Synced(동기화됨)" 상태일 때 이 옵션이 표시됩니다.

변경 사항을 확인하려면 다음을 수행합니다.

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 구성이 디바이스에서 직접 변경되었을 가능성이 있는 디바이스를 선택합니다.

단계 5 오른쪽의 Synced(동기화) 창에서 **Check for Changes**(변경 사항 확인)를 클릭합니다.

단계 6 다음 동작은 디바이스에 따라 약간 다릅니다.

- 디바이스의 경우 디바이스의 구성이 변경된 경우 다음 메시지가 표시됩니다.

디바이스에서 정책을 읽는 중입니다. 디바이스에 활성 구축이 있는 경우 완료 후 읽기가 시작됩니다.

- 계속하려면 **OK**(확인)를 클릭하십시오. 디바이스의 구성이 CDO에 저장된 구성을 덮어씁니다.
- 작업을 취소하려면 **Cancel**(취소)을 클릭합니다.

- ASA 디바이스의 경우:

- a. 표시되는 두 가지 구성을 비교합니다. **Continue**(계속)를 클릭합니다. **Last Known Device Configuration**(마지막으로 알려진 디바이스 구성) 레이블이 지정된 구성은 CDO에 저장된 구성입니다. **Found on Device**(디바이스에서 발견) 레이블이 지정된 구성은 ASA에 저장된 구성입니다.
- b. 다음 중 하나를 선택합니다.
 1. "마지막으로 알려진 디바이스 구성"을 유지하려면 대역 외 변경 사항을 거부합니다.
 2. 대역 외 변경 사항을 수락하여 CDO에 저장된 디바이스의 구성을 디바이스에 있는 구성으로 덮어씁니다.
- c. **Continue**(계속)를 클릭합니다.

변경 사항 취소

CDO를 사용하여 디바이스의 구성에 적용한 구축 해제된 구성 변경 사항을 모두 "실행 취소"하려면 **Discard Changes**(변경 사항 취소)를 클릭합니다. **Discard Changes**(변경 사항 취소)를 클릭하면 CDO는 디바이스 구성의 로컬 복사본을 디바이스에 저장된 구성으로 완전히 덮어씁니다.

Discard Changes(변경 사항 취소)를 클릭하면 디바이스의 구성 상태가 **Not Synced**(동기화되지 않음) 상태가 됩니다. 변경 사항을 취소하면 CDO의 구성 복사본이 디바이스의 구성 복사본과 동일하게 되며 CDO의 구성 상태는 **Synced**(동기화)로 돌아갑니다.

디바이스에 대해 구축되지 않은 모든 구성 변경 사항을 취소하거나 "실행 취소"하려면 다음을 수행합니다.

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 구성을 변경한 디바이스를 선택합니다.

단계 5 오른쪽의 **Not Synced**(동기화되지 않음) 창에서 **Discard Changes**(변경 사항 취소)를 클릭합니다.

- FDM 관리 디바이스의 경우 CDO는 "CDO에서 보류 중인 변경 사항이 취소되고 이 디바이스에 대한 CDO 구성 이 디바이스에서 현재 실행 중인 구성으로 교체됩니다."라고 경고합니다. 변경 사항을 취소하려면 **Continue**(계속)를 클릭합니다.
- Meraki 디바이스의 경우 CDO가 변경 사항을 즉시 삭제합니다.
- AWS 디바이스의 경우 CDO는 삭제하려는 항목을 표시합니다. **Accept**(수락) 또는 **Cancel**(취소)을 클릭합니다.

디바이스의 대역 외 변경 사항

대역 외 변경 사항은 CDO를 사용하지 않고 디바이스에서 직접 변경한 사항을 의미합니다. 이러한 변경은 SSH 연결을 통해 디바이스의 명령줄 인터페이스를 사용하거나 ASA용 ASDM(Adaptive Security Device Manager), FDM 관리 디바이스용 또는 온프레미스 Firewall Management Center 사용자 인터페이스의 온프레미스 Firewall Management Center용 FDM과 같은 로컬 관리자를 사용하여 수행할 수 있습니다. 대역 외 변경은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

디바이스에서 대역 외 변경 탐지

ASA, FDM 관리 디바이스, Cisco IOS 디바이스 또는 온프레미스 Firewall Management Center에 대해 Conflict Detection(충돌 탐지)이 활성화된 경우 CDO는 10분마다 디바이스를 확인하여 CDO 외부에서 디바이스의 구성에 직접 적용된 새로운 변경 사항을 검색합니다.

CDO에 저장되지 않은 디바이스 구성 변경 사항이 있음을 발견하면 CDO는 해당 디바이스의 구성 상태를 "충돌 탐지됨" 상태로 변경합니다.

Defense Orchestrator에서 충돌을 탐지하는 경우 다음 두 가지 조건 중 하나가 발생할 수 있습니다.

- CDO의 데이터베이스에 저장되지 않은 디바이스에 직접 적용된 구성 변경 사항이 있습니다.
- FDM 관리 디바이스의 경우 구축되지 않은 FDM 관리 디바이스에 "보류 중인" 구성 변경 사항이 있을 수 있습니다.
- 온프레미스 Firewall Management Center의 경우, 예를 들어 CDO 외부의 개체에 변경 사항이 있어 CDO와의 동기화를 위해 보류 중이거나 CDO에서 변경 사항이 있어 온프레미스 Firewall Management Center에 구축하기 위해 보류 중일 수 있습니다.

Defense Orchestrator와 디바이스 간 구성 동기화

구성 충돌 정보

Inventory(재고 목록) 페이지에서 디바이스 또는 서비스의 상태가 "Synced(동기화됨)", "Not Synced(동기화되지 않음)" 또는 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. CDO를 사용하여

관리하는 온프레미스 Firewall Management Center의 상태를 확인하려면 **Tools & Services**(도구 및 서비스) > **Firewall Management Center**로 이동하십시오.

- 디바이스가 동기화되면 CDO(Cisco Defense Orchestrator)의 구성과 디바이스에 로컬로 저장된 구성이 동일합니다.
- 디바이스가 동기화되지 않은 경우 CDO에 저장된 구성이 변경되었으며 이제 디바이스에 로컬로 저장된 구성이 다릅니다. CDO에서 디바이스로 변경 사항을 구축하면 CDO의 버전과 일치하도록 디바이스의 구성이 변경됩니다.
- CDO 외부에서 디바이스에 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경이 수행되면 디바이스에 대해 충돌 탐지가 활성화된 경우 디바이스 상태가 "Conflict Detected(충돌 탐지됨)"로 변경됩니다. 대역 외 변경 사항을 수락하면 는 CDO의 구성을 디바이스의 구성과 일치하도록 변경합니다.

충돌 탐지

충돌 탐지가 활성화된 경우 CDO(Cisco Defense Orchestrator)는 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO는 변경 사항을 탐지하면 디바이스의 구성 상태를 **Conflict Detected**(충돌 탐지됨)로 변경합니다. CDO 외부에서 디바이스에 적용된 변경 사항을 "대역 외" 변경 사항이라고 합니다.

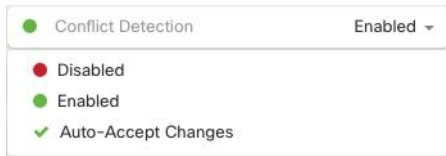
CDO에서 관리하는 온프레미스 Firewall Management Center의 경우, 준비되는 변경 사항이 있고 디바이스가 **Not Synced**(동기화되지 않음) 상태이면 CDO는 디바이스 폴링을 중지하여 변경 사항을 확인합니다. CDO 외부에서 이루어진 변경 사항 중 CDO와의 동기화를 위해 보류 중인 변경 사항과 CDO에서 수행된 변경 사항 중 온프레미스 Management Center에 구축되기 위해 보류 중인 사항이 있는 경우, CDO는 온프레미스 Management Center이 **Conflict Detected**(충돌 탐지됨) 상태임을 선언합니다.

이 옵션이 활성화되면 디바이스별로 충돌 또는 OOB 변경 사항이 탐지되는 빈도를 구성할 수 있습니다. 자세한 내용은 [디바이스 변경 사항에 대한 폴링 예약](#), on page 227를 참조하십시오.

충돌 탐지 활성화

충돌 감지를 활성화하면 Defense Orchestrator 외부의 디바이스가 변경된 인스턴스에 대해 경고합니다.

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 선택합니다.
- 단계 4 충돌 탐지를 활성화할 디바이스를 선택합니다.
- 단계 5 디바이스 테이블 오른쪽에 있는 충돌 감지 상자의 목록에서 **Enabled**(활성화됨)을 선택합니다.



디바이스에서 대역외 변경 사항 자동 수락

변경 사항 자동 수락을 활성화하여 매니지드 디바이스에 대한 직접 변경 사항을 자동으로 수락하도록 CDO(Cisco Defense Orchestrator)를 구성할 수 있습니다. CDO를 사용하지 않고 디바이스에 직접 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

자동 수락 변경 기능은 충돌 탐지를 개선한 것입니다. 디바이스에서 변경 사항 자동 수락이 활성화된 경우 CDO는 10분마다 변경 사항을 확인하여 디바이스의 구성에 대한 대역 외 변경 사항이 있는지 확인합니다. 구성이 변경된 경우 CDO는 사용자에게 확인 상자를 표시하지 않고 디바이스 구성의 로컬 버전을 자동으로 업데이트합니다.

CDO에서 아직 디바이스에 구축되지 않은 구성 변경 사항이 있는 경우 CDO는 구성 변경을 자동으로 수락하지 않습니다. 화면의 프롬프트에 따라 다음 작업을 결정합니다.

자동 수락 변경 사항을 사용하려면 먼저 테넌트가 **Inventory**(재고 목록) 페이지의 **Conflict Detection**(충돌 탐지) 메뉴에서 **auto-accept**(자동 수락) 옵션을 표시하도록 활성화합니다. 그런 다음 개별 디바이스에 대한 변경 사항 자동 수락을 활성화합니다.

CDO가 대역 외 변경 사항을 탐지하지만 수동으로 수락하거나 거부할 수 있는 옵션을 제공하도록하려면 대신 **충돌 탐지**, [on page 223](#)를 활성화합니다.

변경 사항 자동 수락 구성

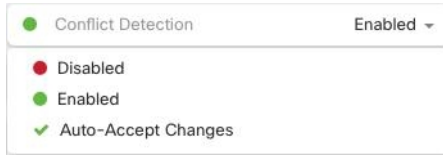
단계 1 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 **Settings**(설정) > **General Settings**(일반 설정)를 탐색합니다.

단계 3 **Tenant Settings**(테넌트 설정) 영역에서, 토글을 클릭하여 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"로 전환합니다. 이렇게 하면 변경 사항 자동 수락 메뉴 옵션이 **Inventory**(인벤토리) 페이지의 충돌 감지 메뉴에 표시됩니다.

단계 4 **Inventory**(인벤토리) 페이지를 열고 대역 외 변경을 자동으로 수락할 디바이스를 선택합니다.

단계 5 **Conflict Detection**(충돌 감지) 메뉴의 드롭다운 메뉴에서 **Auto-Accept Changes**(변경 사항 자동 수락)을 선택합니다.



테넌트의 모든 디바이스에 대한 변경 사항 자동 수락 비활성화

단계 1 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 **Settings**(설정) > **General Settings**(일반 설정)를 탐색합니다.

단계 3 **Tenant Settings**(테넌트 설정) 영역에서 회색 X가 표시되도록 토글을 왼쪽으로 밀어 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"를 비활성화합니다. 이렇게 하면 충돌 감지 메뉴에서 변경 사항 자동 수락 옵션이 비활성화되고 테넌트의 모든 디바이스에 대한 기능이 비활성화 됩니다.

Note "자동 수락"을 비활성화하면 CDO에 수락하기 전에 각 디바이스 충돌을 검토해야 합니다. 여기에는 이전에 변경 사항을 자동으로 수락하도록 구성된 디바이스가 포함됩니다.

구성 충돌 해결

이 섹션에서는 디바이스에서 발생하는 구성 충돌을 해결하는 방법에 대한 정보를 제공합니다.

"동기화되지 않음" 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.

Note 온프레미스 Firewall Management Center의 경우, **Tools & Services**(도구 및 서비스) > **Firewall Management Center**로 이동하여 **Not Synced**(동기화되지 않음) 상태인 FMC를 선택하고 5단계부터 계속 진행합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 5 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- **미리보기 및 배포...** - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.

- 변경 사항 취소 - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

"충돌 탐지됨" 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. [충돌 탐지, on page 223](#)이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected**(충돌 탐지됨)로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.

Note 온프레미스 Firewall Management Center의 경우, **Tools & Services**(도구 및 서비스) > **Firewall Management Center**로 이동하여 **Conflict Detected**(충돌 탐지됨) 상태인 FMC를 선택하고 4단계부터 계속 진행합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict**(충돌 검토)를 클릭합니다.

단계 5 **Device Sync**(디바이스 동기화) 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 6 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes**(디바이스 변경 사항 수락): 구성 및 CDO에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

Note CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 배포하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review**(검토 없이 수락)를 선택하는 것입니다.

- **Reject Device Changes**(디바이스 변경 거부): 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

Note 거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

디바이스 변경 사항에 대한 폴링 예약

충돌 탐지, on page 223를 활성화했거나 Settings(설정) 페이지에서 **Enable device changes to auto-accept device changes**(디바이스 변경 자동 수락 옵션 활성화)를 선택한 경우 CDO는 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO가 디바이스별로 변경 사항을 폴링하는 빈도를 맞춤화할 수 있습니다. 이러한 변경 사항은 둘 이상의 디바이스에 적용할 수 있습니다.

디바이스에 대해 구성된 선택 항목이 없으면 "테넌트 기본값"에 대한 간격이 자동으로 구성됩니다.



Note **Devices & Services**(디바이스 및 서비스) 페이지에서 디바이스별 간격을 맞춤 설정하면 **General Settings**(일반 설정) 페이지에서 **Default Conflict Detection Interval**(기본 충돌 탐지 간격)로 선택한 폴링 간격이 재정의됩니다.

Devices & Services(디바이스 및 서비스) 페이지에서 **Conflict Detection**(충돌 탐지)을 활성화하거나 Settings(설정) 페이지에서 디바이스 변경 사항을 자동 수락하는 옵션을 활성화한 후 다음 절차를 사용하여 CDO가 디바이스를 폴링할 빈도를 예약합니다.

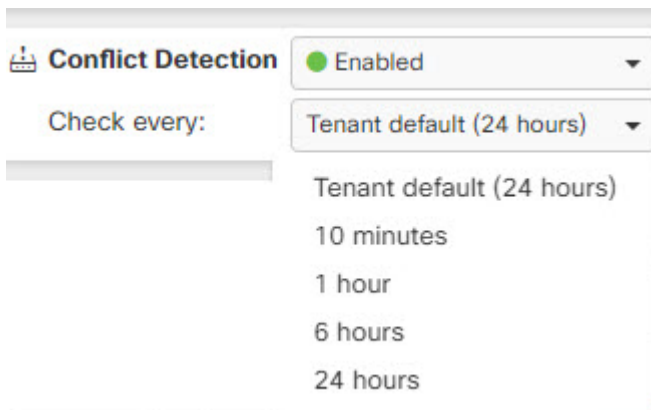
단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 충돌 탐지를 활성화할 디바이스를 선택합니다.

단계 5 **Conflict Detection**(충돌 탐지)과 동일한 영역에서 **Check every**(확인 간격)의 드롭다운 메뉴를 클릭하고 원하는 폴링 간격을 선택합니다.



번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.