네트워크 악성코드 보호 및 파일 정책

다음 주제에서는 파일 제어, 파일 정책, 파일 규칙, Advanced Malware Protection(AMP), 클라우드 연결, 동적 분석 연결의 개요를 제공합니다.

네트워크 악성코드 보호 및 파일 정책 정보

악성 코드를 탐지하고 차단하려면 파일 정책을 사용해야 합니다. 파일 정책을 사용하면 트래픽을 파일 유형별로 탐지하고 제어할 수 있습니다.

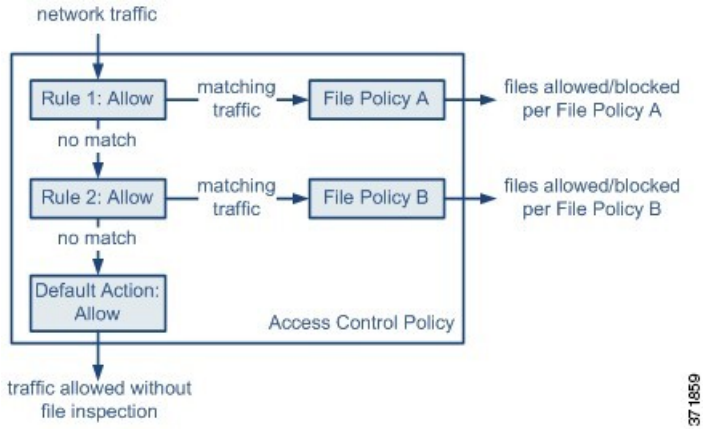
Firepower의 Advanced Malware Protection(AMP)은 네트워크에서 악성코드 전송을 탐지, 캡처, 추적, 분석, 로깅하고 선택적으로 차단할 수 있습니다. Secure Firewall Management Center 웹 인터페이스에서 이 기능은 악성코드 대응 라고 하며 이전에는 *AMP for Firepower*라고 했습니다. AMP(Advanced Malware Protection)는 인라인으로 구축된 매니지드 디바이스와 Cisco Cloud의 위협 데이터를 사용하여 악성코드를 식별합니다.

파일 정책을 전반적 액세스 제어 구성의 일환으로 네트워크 트래픽을 처리하는 액세스 제어 규칙에 연결합니다.

시스템은 네트워크에서 악성코드를 탐지하면 파일 및 악성코드 이벤트를 생성합니다. 파일 및 악성코드 이벤트 데이터를 분석하려면 Cisco Secure Firewall Management Center 관리 가이드의 파일/악성코드 이벤트 및 네트워크 파일 경로 분석 장을 참조하십시오 .

파일 정책

파일 정책은 악성코드 차단 및 파일 제어를 수행하기 위해 시스템에서 전체 액세스 제어 설정의 일부로 사용하는 구성 집합입니다. 이 연결은 시스템이 액세스 제어 규칙의 조건에 일치하는 트래픽에 파일을 통과시키기 전에 먼저 파일을 검사하도록 합니다. 인라인 배포에서 간단한 액세스 제어 정책의 다음 다이어그램을 참고하십시오.



정책에 두 개의 액세스 제어 규칙이 있으며, 두 규칙 모두 Allow(허용) 작업을 사용하고 파일 정책과 연결되어 있습니다. 정책의 기본 작업은 또한 파일 정책 검사 없이 트래픽을 허용하는 것입니다. 이 시나리오에서, 트래픽은 다음과 같이 처리됩니다.

- `Rule 1(규칙 1)`에 일치하는 트래픽은 `File Policy A(파일 정책 A)`로 검사합니다.
- `Rule 1(규칙 1)`에 일치하지 않는 트래픽은 `Rule 2(규칙 2)`에 대해 평가됩니다. `Rule 2(규칙 2)`에 일치하는 트래픽은 `File Policy B(파일 정책 B)`로 검사합니다.
- 둘 중 어느 규칙과도 일치하지 않는 트래픽은 허용됩니다. 파일 정책을 기본 작업과 연결할 수 없습니다.

다양한 파일 정책을 서로 다른 액세스 제어 규칙과 연결할 경우, 네트워크에 전송된 파일을 식별하고 차단하는 방법을 세부적으로 제어할 수 있습니다.

파일 정책 요구 사항 및 사전 요건

모델 지원

Any(모든)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자

파일 및 악성코드 정책을 위한 라이선스 요구 사항

수행할 작업	필요한 라이선스	파일 규칙 작업
특정 유형의 모든 파일 차단 또는 허용(예: 모든 .exe 파일 차단)	위협(threat defense 디바이스용) 보호(클래식 디바이스의 경우)	허용, 차단, 차단 후 재설정
악성 코드를 포함하거나 포함할 가능성이 있다는 판단에 따라, 선택적으로 파일을 허용하거나 차단합니다.	위협(threat defense 디바이스용) 보호(클래식 디바이스의 경우) 악성코드	악성코드 클라우드 조회, 악성코드 차단
파일 저장	위협(threat defense 디바이스용) 보호(클래식 디바이스의 경우) 악성코드	**Store Files(**파일 저장**)**를 선택한 모든 파일 규칙 작업

악성코드 라이선스 관련 정보는 다음을 참조하십시오.

- Cisco Secure Firewall Management Center 관리 가이드의 악성코드 방어 라이선스

파일 정책 및 악성코드 탐지 모범 사례

아래에 설명된 항목 외에도 악성코드 차단 설정 방법, 6 페이지의 단계 및 참조 주제를 따르십시오.

파일 규칙 모범 사례

파일 규칙을 구성할 때 다음 지침 및 제한 사항에 유의하십시오.

- 수동 배포에 파일을 차단하기 위해 구성된 규칙은 일치하는 파일을 차단하지 않습니다. 연결이 계속해서 파일을 전송하므로, 연결의 시작을 로깅하는 규칙을 구성하는 경우, 이 연결에 대해 로깅된 여러 이벤트를 볼 수 있습니다.

- 정책에는 여러 규칙이 포함될 수 있습니다. 규칙을 만들 때는 이전 규칙에 의해 "숨겨진" 규칙이 없는지 확인합니다.
- 동적 분석이 지원되는 파일 유형은 다른 분석 유형이 지원되는 파일 유형의 하위 집합입니다. 각 분석 유형이 지원되는 파일 유형을 보려면 파일 규칙 구성 페이지로 이동하여 **Block Malware(**악성코드 차단**)** 작업을 선택하고 관심 있는 확인란을 선택합니다.

  시스템이 모든 파일 유형을 검사하도록 하려면 동적 분석을 위한 규칙과 기타 분석 유형을 위한 규칙을 동일 정책 내에서 별도로 생성합니다.
- 파일 규칙이 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 작업으로 구성되어 있고 management center이 AMP 클라우드와의 연결을 설정할 수 없는 경우, 연결이 복원될 때까지 시스템은 구성된 어떤 규칙 작업도 수행할 수 없습니다.
- Cisco는 TCP 연결이 재설정될 때까지 차단된 애플리케이션 세션이 계속 열려 있는 것을 방지하기 위해 **Block Files(**파일 차단**)** 및 **Block Malware(**악성코드 차단**)** 작업을 위한 **Reset Connection(**연결 재설정**)**을 활성화할 것을 권장합니다. 연결을 재설정하지 않으면 TCP 연결이 자체적으로 재설정될 때까지 클라이언트 세션이 계속 열려 있게 됩니다.
- 대량의 트래픽을 모니터링하는 경우, 모든 캡처 파일을 저장하거나 동적 분석을 위해 모든 캡처 파일을 전송하지 마십시오. 이렇게 하면 시스템 성능에 부정적인 영향을 줄 수 있습니다.
- 시스템에서 탐지된 모든 파일 유형에서 악성코드 분석을 수행할 수는 없습니다. 사용자가 **Application Protocol(**애플리케이션 프로토콜**)**, **Direction of Transfer(**전송 방향**)**, 및 **Action(**작업**)** 드롭다운 목록에서 값을 선택한 후에는 시스템이 파일 유형 목록을 제한합니다.

파일 탐지 모범 사례

파일 탐지에 대한 다음 참고 사항 및 제한 사항을 고려하십시오.

- 적응형 프로파일이 활성화되지 않은 경우, 액세스 제어 규칙은 AMP를 포함한 파일 제어를 수행할 수 없습니다.
- 파일이 애플리케이션 프로토콜 조건을 갖춘 규칙에 일치하는 경우, 파일 이벤트 생성은 시스템이 파일의 애플리케이션 프로토콜을 확인한 후에 발생합니다. 확인되지 않은 파일은 파일 이벤트를 생성하지 않습니다.
- FTP는 다른 채널에 명령 및 데이터를 전송합니다. 패시브 또는 인라인 탭 모드 구축에서 FTP 데이터 세션 및 제어 세션의 트래픽은 동일한 내부 리소스로 부하 분산되지 않을 수 있습니다.
- POP3, POP, SMTP 또는 IMAP 세션에서 파일에 대한 모든 파일 이름의 총 바이트 수가 1024를 초과할 경우, 세션에서 파일 이벤트는 파일 이름 버퍼가 채워진 후 발견된 파일의 정확한 파일 이름을 반영하지 않을 수 있습니다.
- 텍스트 기반의 파일을 SMTP에 전송할 경우, 일부 메일 클라이언트는 줄 바꿈을 CRLF 줄 바꿈 문자 표준으로 변환합니다. Mac 기반의 호스트가 캐리지 리턴(CR) 문자를 사용하고 Unix/Linux 기반의 호스트가 라인 피드(LF) 문자를 사용하기 때문에 메일 클라이언트에 의한 줄 바꿈 변환은 파일의 크기를 변경할 수 있습니다. 인식 불가능한 파일 유형을 처리할 때 일부 메일 클라이언트가 줄 바꿈 변환을 기본값으로 설정한다는 점에 유의하십시오.

- ISO 파일을 탐지하려면 "Limit the number of bytes inspected when doing file type detection(파일 유형 탐지를 수행할 때 검사되는 바이트 수 제한)" 옵션을 파일 및 악성코드 탐지 성능 및 저장 옵션, 37 페이지의 설명처럼 36870보다 큰 값으로 설정하십시오.
- rar5를 포함하여 일부 .rar 아카이브 내의 .Exe 파일을 검색할 수 없습니다.

파일 차단 모범 사례

파일 차단에 대한 다음 참고 사항 및 제한 사항을 고려하십시오.

- 파일의 파일 종료 마커가 탐지되지 않는 경우, 전송 프로토콜에 상관없이 해당 파일은 **Block Malware(**악성코드 차단**)** 규칙 또는 맞춤형 탐지 목록에 의해 차단되지 않습니다. 시스템은 파일 종료 마커에 표시된 대로 전체 파일을 받을 때까지 파일을 차단하기 위해 대기하며, 마커가 탐지된 후 파일을 차단합니다.
- FTP 파일 전송을 위한 파일 종료 마커가 마지막 데이터 세그먼트와 별도로 전송되는 경우, 마커는 차단되며 FTP 클라이언트는 파일 전송이 실패했다고 표시하지만 실제로 파일은 디스크에 완전히 전송됩니다.
- **Block Files(**파일 차단**)** 및 **Block Malware(**악성코드 차단**)** 작업을 가진 파일 규칙은 초기 파일 전송 시도가 발생한 후 24시간 동안 탐지된 동일한 파일, URL, 서버 및 클라이언트 애플리케이션의 새로운 세션을 차단함으로써 HTTP를 통한 파일 다운로드가 자동으로 재개되는 것을 차단합니다.
- 드물게 HTTP 업로드 세션의 트래픽이 작동하지 않는 경우, 시스템은 트래픽을 제대로 다시 어셈블할 수 없으므로 트래픽을 차단하거나 파일 이벤트를 생성하지 않습니다.
- **Block Files(**파일 차단**)** 규칙으로 차단된 파일을 NetBIOS-ssn으로 전송하는 경우(SMB 파일 전송 등), 대상 호스트에서 파일을 확인할 수 있습니다. 그러나, 파일은 다운로드가 시작된 후 차단되기 때문에 사용할 수 없으며, 그 결과 파일 전송은 완료되지 않습니다.
- NetBIOS ssn을 통해 전송되는 파일(예: SMB 파일 전송)을 탐지하거나 차단하는 규칙을 생성하는 경우, 시스템은 진행 중인 파일 전송을 검사하지 않습니다. 하지만 파일 정책을 호출하는 액세스 제어 정책을 구축한 후 전송되는 새 파일은 검사합니다.
- SMB에는 IP 주소는 같고 포트는 다른 여러 병렬 세션을 생성하는 다중 채널이라는 기능이 있습니다. 다중 채널을 통한 트랜잭션의 경우, 시스템에 의해 단일 파일로 검사되지 않는 이러한 세션에서 파일 다운로드가 멀티플렉싱됩니다.
- 단일 TCP 또는 SMB 세션에서 동시에 전송되는 파일은 검사되지 않습니다.
- 클러스터 환경에서 클러스터 역할 변경 또는 디바이스 장애로 인해 기존 SMB 세션을 새로운 디바이스로 이동하는 경우, 진행 중인 파일 전송의 파일은 검사되지 않을 수 있습니다.
- Microsoft Windows 시스템 간의 일부 SMB 파일 전송은 빠른 파일 전송을 위해 매우 높은 TCP 창 크기를 사용합니다. 이러한 파일 전송을 탐지하거나 차단하려면 **Network Analysis Policy(**네트워크 분석 정책**)** > **TCP Stream Configuration(TCP** 스트림 구성**)** > **Troubleshooting Options(**문제해결 옵션**)** 아래에서 **Maximum Queued Bytes(**최대 대기열 바이트**)**와 **Maximum Queued Segments(**최대 대기열 세그먼트**)**의 값을 늘리는 것이 좋습니다.

- Firepower Threat Defense 고가용성을 구성하고 원래 활성 디바이스가 파일을 식별하는 동안 페일오버가 발생하는 경우, 파일 유형이 동기화되지 않습니다. 따라서 파일 정책에서 해당 파일 유형을 차단하더라도 새 액티브 디바이스는 파일을 다운로드합니다.

파일 정책 모범 사례

파일 정책을 구성할 때 다음 지침 및 제한 사항에 유의하십시오.

- **Allow(**허용**)**, **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재시작**)**의 작업을 가진 액세스 제어 규칙과 단일 파일 정책을 연결할 수 있습니다.
- 액세스 기본 작업에 의해 처리된 트래픽을 파일 정책을 사용하여 검사할 수 없습니다.
- 새로운 정책의 경우, 웹 인터페이스에 정책이 사용 중이 아닌 것으로 표시됩니다. 사용 중인 파일 정책을 수정하는 경우, 해당 파일 정책을 사용 중인 액세스 제어 정책의 수가 웹 인터페이스에 표시됩니다. 어느 경우든 텍스트를 클릭하면 Access Control Policies(액세스 제어 정책) 페이지로 이동할 수 있습니다.
- 파일 차단이 작동하려면 액세스 제어 정책에 적용하는 NAP 정책이 보호 모드(인라인 모드라고도 함)에서 작동해야 합니다.
- 구성에 따라 시스템이 처음 탐지할 때 파일을 검사하고 클라우드 조회 결과를 기다리거나 클라우드 조회 결과를 기다리지 않고 이 첫 번째 탐지에서 파일을 전달할 수 있습니다.
- 기본적으로 암호화된 페이로드의 파일 검사를 비활성화합니다. 이는 암호화 연결이 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

악성코드 차단 설정 방법

이 항목에서는 악성 소프트웨어로부터 네트워크를 보호하기 위해 시스템을 설정이라는 단계를 요약하여 설명합니다.

프로시저

단계 **1** 악성 코드 차단 계획 및 준비, 7 페이지

단계 **2** 파일 정책 구성, 8 페이지

단계 **3** 액세스 제어 구성에 파일 정책 추가, 9 페이지

단계 **4** 파일 및 악성코드 이벤트를 네트워크의 호스트에 연결할 수 있도록 네트워크 검색 정책을 구성합니다.

(네트워크 검색을 설정하기만 해선 안 됩니다. 네트워크의 호스트를 검색해 조직의 네트워크 맵을 구축하도록 구성해야 합니다.)

네트워크 검색 정책 및 하위 항목을 참조하십시오.

단계 **5** 매니지드 디바이스에 정책을 구축합니다.

구성 변경 사항 구축의 내용을 참조하십시오.

단계 **6** 시스템을 테스트하여 악성 파일이 예상대로 처리되는지 확인합니다.

단계 **7** 악성코드 차단 유지 보수 및 모니터링 설정, 10 페이지

다음에 수행할 작업

- (선택 사항) 네트워크상의 악성코드 탐지를 강화할 수 있도록, Cisco의 AMP for Endpoints 제품을 구축하고 통합합니다. (선택 사항) AMP for Endpoints를 사용한 악성코드 방지, 40 페이지 및 하위 항목을 참조하십시오.

악성 코드 차단 계획 및 준비

이 절차는 악성코드 차단을 제공하도록 시스템을 구성하는 전체 프로세스의 첫 번째 단계입니다.

프로시저

단계 **1** 라이선스 구입해 설치합니다.

Cisco Secure Firewall Management Center 관리 가이드의 파일 및 악성코드 정책을 위한 라이선스 요구 사항, 3 페이지 및 라이선스를 참조하십시오.

단계 **2** 파일 정책과 악성코드 방지가 액세스 제어 계획에 어떻게 부합하는지 이해합니다.

액세스 제어 개요 장을 참조하십시오.

단계 **3** 파일 분석 및 악성 코드 보호 도구를 확인합니다.

파일 규칙 작업, 28 페이지 및 하위 항목을 참조하십시오.

고급 및 아카이브 파일 검사 옵션, 22 페이지도 고려하십시오.

단계 **4** 악성코드 차단(파일 분석 및 동적 분석)에 퍼블릭 클라우드를 사용할지 프라이빗(온프레미스) 클라우드를 사용할지 결정합니다.

악성코드 차단을 위한 클라우드 연결, 11 페이지 및 하위 항목을 참조하십시오.

단계 **5** 악성코드 차단을 위해 프라이빗(온프레미스) 클라우드를 사용한다면, 이러한 제품을 구입, 구축 및 테스트합니다.

자세한 내용은 Cisco 영업 담당자 또는 공인 대리점에 문의하십시오.

단계 **6** 선택한 클라우드와의 통신을 허용하도록 방화벽을 구성합니다.

Cisco Secure Firewall Management Center 관리 가이드의 보안, 인터넷 액세스 및 통신 포트를 참조하십시오.

단계 **7** Firepower와 악성코드 차단 클라우드(퍼블릭 또는 프라이빗) 간의 연결을 구성합니다.

- AMP 클라우드의 경우에는 AMP 옵션 변경, 17 페이지의 내용을 참조하십시오.
- 온프레미스 Secure Malware Analytics 어플라이언스를 구축한 경우, 온프레미스 동적 분석 어플라이언스에 연결, 18 페이지의 내용을 참조하십시오. (퍼블릭 Secure Malware Analytics 클라우드에 액세스하는 데는 구성이 필요하지 않습니다.)

다음에 수행할 작업

악성코드 차단 워크플로의 다음 단계를 계속 진행합니다.

악성코드 차단 설정 방법, 6 페이지의 내용을 참조하십시오.

파일 정책 구성

시작하기 전에

악성코드 차단 워크플로의 이 단계까지 작업을 완료합니다.

악성코드 차단 설정 방법, 6 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 파일 정책 및 파일 규칙 제한 사항을 검토합니다.

파일 정책 및 악성코드 탐지 모범 사례 , 3 페이지 및 하위 항목을 참조하십시오.

단계 **2** 파일 정책을 생성합니다.

파일 정책 생성 또는 수정, 21 페이지의 내용을 참조하십시오.

단계 **3** 파일 정책 내에 규칙을 생성합니다.

파일 규칙, 26 페이지 및 하위 항목을 참조하십시오.

단계 **4** 고급 옵션을 구성합니다.

고급 및 아카이브 파일 검사 옵션, 22 페이지의 내용을 참조하십시오.

다음에 수행할 작업

악성코드 차단 워크플로의 다음 단계를 계속 진행합니다.

악성코드 차단 설정 방법, 6 페이지의 내용을 참조하십시오.

액세스 제어 구성에 파일 정책 추가

액세스 제어 정책에는 파일 정책과 연결된 여러 액세스 제어 규칙이 포함될 수 있습니다. 모든 Allow or Interactive Block (허용 또는 인터랙티브 차단) 액세스 제어 규칙에 대해 파일 검사를 구성할 수 있습니다. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크 상에 있는 다양한 유형의 트래픽에 대해 다양한 파일 및 악성코드 검사 프로파일과 맞춰볼 수 있습니다.

시작하기 전에

악성코드 차단 워크플로의 이 단계까지 작업을 완료합니다.

악성코드 차단 설정 방법, 6 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 액세스 제어 정책의 파일 정책 지침을 검토합니다. (이것은 앞에서 살펴본 파일 규칙 및 파일 정책 지침과는 다릅니다.)

파일 및 침입 검사 순서를 검토합니다.

단계 **2** 파일 정책을 액세스 제어 정책에 연결합니다.

악성코드 보호를 수행하는 액세스 제어 규칙 구성, 9 페이지의 내용을 참조하십시오.

단계 **3** 액세스 제어 정책을 매니지드 디바이스에 할당합니다.

액세스 제어 정책에 대한 대상 디바이스 설정의 내용을 참조하십시오.

다음에 수행할 작업

악성코드 차단 워크플로의 다음 단계를 계속 진행합니다.

악성코드 차단 설정 방법, 6 페이지의 내용을 참조하십시오.

악성코드 보호를 수행하는 액세스 제어 규칙 구성

주의 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 **Store Files(**파일 저장**)**를 활성화 또는 비활성화하거나 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)** 또는 **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**), Unknown(**알 수 없음**)**, **Clean(**정리**)** 또는 **Custom(**맞춤형**)**), 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.과 결합하는 첫 번째 파일 규칙을 추가하거나 마지막 파일 규칙을 제거

참고 파일 정책이 액세스 제어 규칙에 포함되면 인라인 표준화가 자동으로 활성화됩니다. 자세한 내용은 인라인 정상화 전처리기를 참고하십시오.

시작하기 전에

- 액세스 제어 규칙이 AMP를 비롯한 파일 제어를 수행하기 위해서는 적응형 프로파일 구성에 설명된 것처럼 적응형 프로파일이 반드시 활성화(기본 상태)되어 있어야 합니다.
- 이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자 사용자여야 합니다.

프로시저

단계 **1** 액세스 제어 규칙 편집기(**Policies(**정책**) > Access Control(**액세스 제어**))**에서 **Allow(**허용**)**, **Interactive Block(**인터랙티브 차단**)**, **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 중 **Action(**작업**)**을 선택합니다.

단계 **2** **File Policy(**파일 정책**)**를 선택하여 액세스 제어 규칙과 일치하는 트래픽을 검사하거나 **None(**없음**)**을 선택하여 일치하는 트래픽 파일 검사를 비활성화합니다.

단계 **3** (선택 사항) **Logging(**로깅**)**을 클릭하고 **Log Files(**로그 파일**)** 선택을 취소하여 일치하는 연결의 파일 또는 악성코드 이벤트 로깅을 비활성화합니다.

참고 Cisco는 파일 및 악성코드 이벤트 로깅 활성화를 유지하는 것을 권장합니다.

단계 **4** 규칙을 저장합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

관련 항목

파일 정책 생성 또는 수정, 21 페이지
Snort® 재시작 시나리오

악성코드 차단 유지 보수 및 모니터링 설정

네트워크를 보호하려면 지속적인 유지 관리가 필수입니다.

시작하기 전에

악성코드로부터 네트워크를 보호하도록 시스템을 구성합니다.

악성코드 차단 설정 방법, 6 페이지 및 참조된 절차를 참조하십시오.

프로시저

단계 **1** 시스템이 유효한 최신 보호 수단을 항상 갖추고 있는지 확인합니다.

시스템 유지 관리: 동적 분석 대상인 파일 유형 업데이트, 20 페이지의 내용을 참조하십시오.

단계 **2** 악성코드 관련 이벤트 및 상태 모니터링에 대한 알림을 구성합니다.

악성코드 대응 알림 구성에 대한 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 내용을 참조하고 다음 모듈에 대한 자세한 내용은 다음을 참조하십시오.

- 로컬 악성코드 분석
- 보안 인텔리전스
- 디바이스에서 위협 데이터 업데이트
- 침입 및 파일 이벤트 비율
- AMP for Firepower 상태
- AMP for Endpoints 상태

다음에 수행할 작업

악성코드 차단 워크플로에서 'What to do next items(다음 작업 항목)'를 검토합니다.

악성코드 차단 설정 방법, 6 페이지의 내용을 참조하십시오.

악성코드 차단을 위한 클라우드 연결

악성코드로부터 네트워크를 보호하려면 퍼블릭 또는 프라이빗 클라우드와의 연결이 필요합니다.

AMP 클라우드

Advanced Malware Protection(AMP) 클라우드는 Cisco가 호스팅하는 서버로서 빅 데이터 분석과 지속적 분석을 사용하여 시스템이 네트워크에서 악성코드 탐지와 차단에 사용하는 인텔리전스를 제공합니다.

AMP 클라우드는 매니지드 디바이스에 의해 네트워크 트래픽에서 탐지되는 잠재적 악성코드의 속성뿐 아니라 로컬 악성코드 분석 및 파일 사전 분류를 위한 데이터 업데이트도 제공합니다.

조직에서 AMP for Endpoints를 구축하고 그 데이터를 가져오도록 Firepower를 구성한 경우, 시스템은 AMP 클라우드에서 스캔 레코드, 악성코드 탐지, 격리, 보안 침해 지표(IOC) 등의 데이터를 가져옵니다.

Cisco에서는 Cisco Cloud에서 알려진 악성 코드 위협 관련 데이터를 얻는 다음과 같은 방법을 제공합니다.

- **AMP** 퍼블릭 클라우드

  Secure Firewall Management Center은(는) 공용 Cisco Cloud와 직접 통신합니다. 미국, 유럽, 아시아에는 3가지 공용 AMP 클라우드가 있습니다.

- **AMP** 프라이빗 클라우드

  AMP 프라이빗 클라우드는 네트워크에 구축되며, 압축된 온프레미스 AMP 클라우드 역할뿐 아니라 퍼블릭 AMP 클라우드에 연결하는 익명화된 프록시 역할도 합니다. 자세한 내용은 Cisco AMP Private Cloud, 14 페이지 섹션을 참조해 주십시오.

  AMP for Endpoints와 통합할 경우, AMP 프라이빗 클라우드에는 몇 가지 제한 사항이 있습니다. AMP for Endpoints 및 AMP Private Cloud, 42 페이지의 내용을 참조하십시오.

동적 분석 클라우드

- **Secure Malware Analytics** 클라우드

  퍼블릭 클라우드는 동적 분석을 위해 전달하는 적격 파일을 처리하고 위협 점수 및 동적 분석 보고서를 제공합니다. Firepower는 Secure Malware Analytics 분석을 위해 매일 200개의 샘플을 지원합니다.

- 온프레미스 **Secure Malware Analytics** 어플라이언스

  조직의 보안 정책에서 시스템이 네트워크 외부로 파일을 전송하는 것을 허용하지 않는다면, 온프레미스 어플라이언스를 구축할 수 있습니다. 이 어플라이언스는 퍼블릭 Secure Malware Analytics 클라우드에 접속하지 않습니다.

  자세한 내용은 동적 분석 온프레미스 어플라이언스(Cisco Secure Malware Analytics), 18 페이지를 참고하십시오.

AMP 및 **Secure Malware Analytics** 클라우드에 대한 연결 구성

- AMP 클라우드 연결 구성, 12 페이지
- 동적 분석 연결, 17 페이지

AMP 클라우드 연결 구성

다음 주제에서는 다양한 시나리오의 AMP 클라우드 연결 구성을 설명합니다.

- AMP 클라우드 선택, 13 페이지
- AMP 프라이빗 클라우드에 연결, 15 페이지
- Firepower 및 Secure Endpoint 통합, 42 페이지

다음 주제는 다음과도 관련됩니다.

- Cisco AMP Private Cloud, 14 페이지
- AMP 클라우드 연결 요구 사항 및 모범 사례, 13 페이지

• (퍼블릭 또는 프라이빗) AMP 클라우드와의 연결 관리 , 16 페이지

AMP 클라우드 연결 요구 사항 및 모범 사례

AMP 클라우드 연결 요구 사항

AMP 클라우드를 설정하려면 관리자 사용자여야 합니다.

management center가 AMP 클라우드와 통신할 수 있도록 하려면 Cisco Secure Firewall Management Center 관리 가이드의 보안, 인터넷 액세스 및 통신 포트 항목을 참조하십시오.

AMP 통신에 레거시 포트를 사용하려면 Cisco Secure Firewall Management Center 관리 가이드 의 통신 포트 요구 사항을 참조하십시오.

AMP 및 고가용성

고가용성 쌍의 management center는 파일 정책 및 관련 구성은 공유하지만 클라우드 연결이나 캡처 파일, 파일 이벤트, 악성코드 이벤트를 공유하지 않습니다. 운영 연속성을 보장하고 탐지된 파일의 악성코드 속성이 두 management center에서 동일하려면 Acitve(활성) 및 Standby(대기) management center에 클라우드에 대한 액세스 권한이 있어야 합니다.

고가용성 컨피그레이션의 경우 Firepower Management Center의 액티브 및 스탠바이 인스턴스에서 독립적으로 AMP 클라우드 연결을 구성해야 합니다. 이러한 컨피그레이션은 동기화되지 않습니다.

이러한 요구 사항은 퍼블릭 및 프라이빗 AMP 클라우드에 적용됩니다.

AMP 클라우드 연결 및 멀티테넌시

다중 도메인 구축에서는 전역 수준에서만 악성코드 대응 연결을 구성합니다. 각 management center에는 하나의 악성코드 대응 연결만 있을 수 있습니다.

AMP 클라우드 선택

기본적으로 시스템에서는 미국(US) AMP 퍼블릭 클라우드와의 연결이 구성 및 활성화되어 있습니다. (이 연결은 웹 인터페이스에 악성코드 대응 로 표시되며 경우에 따라 AMP for Firepower로 표시됩니다.) 악성코드 대응 클라우드 연결을 삭제하거나 비활성할 수는 없지만, 서로 다른 지리적 AMP 클라우드 간에 전환하거나 AMP 프라이빗 클라우드 연결을 구성할수 있습니다.

시작하기 전에

- AMP 프라이빗 클라우드를 사용할 계획이라면 이 항목 대신 AMP 프라이빗 클라우드에 연결, 15 페이지 항목을 참조하십시오.
- Firepower를 AMP for Endpoints와 통합하지 않으면, AMP 클라우드 연결은 하나만 구성할 수 있습니다. 이 연결은 **AMP for Networks** 또는 **AMP for Firepower**라고 표시됩니다.
- AMP for Endpoints를 구축했고 하나 이상의 AMP 클라우드를 추가해 해당 애플리케이션을 Firepower와 통합하고 싶다면, Firepower 및 Secure Endpoint 통합, 42 페이지의 내용을 참조하십시오.

- AMP 클라우드 연결 요구 사항 및 모범 사례, 13 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Integration(**통합**)** > **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** 연필을 클릭하여 기존 클라우드 연결을 편집합니다.

단계 **3** **Cloud Name(**클라우드 이름**)** 드롭다운 목록에서 Secure Firewall Management Center와(과) 가장 가까이에 있는 지역 클라우드를 선택합니다.

APJC는 아시아/태평양/일본/중국입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구축이 고가용성 구성인 경우, AMP 클라우드 연결 요구 사항 및 모범 사례, 13 페이지를 참조하십시오.
- (선택 사항) AMP 옵션 변경, 17 페이지

Cisco AMP Private Cloud

management center는 네트워크 트래픽에서 탐지된 파일의 속성 쿼리와 회귀적 악성코드 이벤트 수신을 위해 AMP 클라우드에 연결해야 합니다. 이 클라우드는 퍼블릭 클라우드이거나 프라이빗 클라우드일 수 있습니다.

조직에 개인 정보 또는 보안 문제가 있을 경우, 이는 모니터링된 네트워크와 AMP 클라우드 서버 간에 연결이 잘되지 않거나 아예 불가능한 상황이 자주 발생하는 원인이 됩니다. 이런 상황에서는 AMP 클라우드의 압축된 온프레미스 버전이자 네트워크와 AMP 클라우드 사이에서 안전한 중재자 역할을 하는 독점 Cisco 제품인 Cisco AMP Private Cloud를 설정할 수 있습니다. management center를 AMP 프라이빗 클라우드에 연결하면 퍼블릭 AMP 클라우드와의 기존의 직접 연결이 비활성화됩니다.

AMP 클라우드와의 모든 연결은 모니터링되는 네트워크의 보안 및 개인 정보 보호를 위해 익명화된 프록시 역할을 하는 AMP 프라이빗 클라우드를 거칩니다. 여기에는 네트워크 트래픽에서 탐지된 파일의 속성 쿼리, 회귀적 악성코드 이벤트 수신 등이 포함됩니다. AMP 프라이빗 클라우드는 외부 연결을 통해 기존 엔드포인트 데이터를 공유하지 않습니다.

참고 AMP 프라이빗 클라우드는 동적 분석을 수행하지 않으며, URL 및 보안 인텔리전스 필터링 같이 Cisco Collective Security Intelligence(CSI)에 의존하는 그 밖의 기능을 위한 위협 인텔리전스의 익명화된 검색을 지원하지 않습니다.

AMP 프라이빗 클라우드("AMPv"라고도 함)에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html를 참조하십시오.

AMP 프라이빗 클라우드에 연결

시작하기 전에

- 제품 설명서의 지침에 따라 Cisco AMP 프라이빗 클라우드를 구성합니다. 구성 도중 프라이빗 클라우드 호스트 이름을 적어둡니다. management center에서 연결을 구성하려면 이 호스트 이름이 필요합니다.
- management center가 AMP 프라이빗 클라우드와 통신할 수 있는지 확인하고, 프라이빗 클라우드가 인터넷에 연결해 퍼블릭 AMP 클라우드와 통신할 수 있는지 확인합니다. Cisco Secure Firewall Management Center 관리 가이드의 보안, 인터넷 액세스 및 통신 포트 아래에 있는 항목을 참조하십시오.
- 구축을 AMP for Endpoints와 통합하지 않으면, 각 management center에는 AMP 클라우드 연결을 하나만 구성할 수 있습니다. 이 연결은 **AMP for Networks** 또는 **AMP for Firepower**라고 표시됩니다.

  AMP for Endpoints와 통합한다면, 여러 AMP for Endpoints 클라우드 연결을 구성할 수 있습니다.

프로시저

단계 **1** **Integration(**통합**)** > **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** **Add AMP Cloud Connection(AMP** 클라우드 연결 추가**)**를 클릭합니다.

단계 **3** **Cloud Name(**클라우드 이름**)** 드롭다운 목록에서 **Private Cloud(**프라이빗 클라우드**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

이 정보는 AMP 프라이빗 클라우드에서 생성하거나 전송한 악성코드 이벤트에 표시됩니다.

단계 **5** **Host(**호스트**)** 필드에 프라이빗 클라우드를 설정할 때 구성한 프라이빗 클라우드 호스트 이름을 입력합니다.

단계 **6** **Certificate Upload Path(**인증서 업로드 경로**)**필드 옆의 **Browse(**찾아보기**)**를 클릭하여 프라이빗 클라우드의 유효한 TLS 또는 SSL 암호화 인증서가 있는 위치로 이동합니다. 자세한 내용은 AMP 프라이빗 클라우드 설명서를 참조하십시오.

단계 **7** 악성코드 대응 와 AMP for Endpoints 모두에 프라이빗 클라우드를 사용하려는 경우, **Use for AMP for Firepower(AMP for Firepower**에 사용**)** 확인란을 선택합니다.

악성코드 대응 통신을 처리할 다른 프라이빗 클라우드를 구성한 경우에는 이 확인란 선택을 취소할 수 있지만 이것이 유일한 AMP 프라이빗 클라우드 연결이라면 선택을 취소할 수 없습니다.

다중 도메인 구축에서 이 확인란은 전역 도메인에만 표시됩니다. 각 management center에는 하나의 악성코드 대응 연결만 있을 수 있습니다.

단계 **8** 프록시를 사용하여 AMP 프라이빗 클라우드와 통신하려면 **Use Proxy for Connection(**연결에 프록시 사용**)** 확인란을 선택합니다.

단계 **9** **Register(**등록**)**를 클릭하고 AMP 클라우드와의 기존 직접 연결을 비활성화한다고 확인한 다음 마지막으로 등록 완료를 위해 AMP 프라이빗 클라우드 관리 콘솔로 이동한다고 확인합니다.

단계 **10** 관리 콘솔에 로그인하고 등록 프로세스를 완료합니다. 자세한 지침은 AMP 프라이빗 클라우드 설명서를 참조하십시오.

다음에 수행할 작업

고가용성 컨피그레이션의 경우 Firepower Management Center의 액티브 및 스탠바이 인스턴스에서 독립적으로 AMP 클라우드 연결을 구성해야 합니다. 이러한 컨피그레이션은 동기화되지 않습니다.

(퍼블릭 또는 프라이빗) AMP 클라우드와의 연결 관리

management center을 사용하여 악성코드 대응 또는 AMP for Endpoints 또는 둘 모두에 사용되는 퍼블릭 및 프라이빗 AMP 클라우드 연결을 관리합니다.

더 이상 클라우드에서 악성코드 관련 정보를 수신하지 않으려는 경우, 퍼블릭 또는 프라이빗 AMP 클라우드와의 연결을 삭제할 수 있습니다. AMP for Endpoints 또는 AMP 프라이빗 클라우드 관리 콘솔을 사용하여 연결 등록을 취소하더라도 해당 연결은 시스템에서 제거되지 않습니다. 등록 취소된 연결은 Secure Firewall Management Center 웹 인터페이스에서 실패 상태를 표시합니다.

연결을 일시적으로 비활성화할 수도 있습니다. 클라우드 연결을 다시 활성화하는 경우, 클라우드는 비활성된 기간의 대기 중 데이터를 포함한 데이터를 시스템에 다시 전송하기 시작합니다.

주의 비활성화된 연결의 경우, 퍼블릭 또는 프라이빗 AMP 클라우드는 연결이 다시 활성화될 때까지 악성코드 이벤트, 보안 침해 지표 등을 저장할 수 있습니다. 예를 들어 이벤트 발생률이 매우 높거나 오랫동안 연결이 비활성화되는 드문 경우에는 연결이 비활성화된 동안 생성된 모든 정보를 클라우드에서 저장하지 못할 수도 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 연결을 표시하며 이러한 연결은 관리할 수 있습니다. 상위 도메인에서 생성된 연결도 표시되지만 이러한 연결은 관리할 수 없습니다. 하위 도메인의 연결을 관리하려면 해당 도메인으로 전환하십시오. 각 management center에는 전역 도메인에 속하는 하나의 악성코드 대응 연결만 있을 수 있습니다.

프로시저

단계 **1** **Integration(**통합**)** > **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** AMP 클라우드 연결 관리:

- 삭제 - **Delete(**삭제**)** ( )을 클릭한 다음 선택 내용을 확인합니다.
- 활성화 또는 비활성화 - 슬라이더를 클릭한 다음 선택 내용을 확인합니다.

다음에 수행할 작업

고가용성 컨피그레이션의 경우 Firepower Management Center의 액티브 및 스탠바이 인스턴스에서 독립적으로 AMP 클라우드 연결을 구성해야 합니다. 이러한 컨피그레이션은 동기화되지 않습니다.

AMP 옵션 변경

프로시저

단계 **1** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**를 선택합니다.

단계 **2** 클라우드 서비스 버튼을 클릭합니다.

단계 **3** 옵션을 선택합니다.

표 ***1: AMP for Networks*** 옵션

옵션	설명
자동 로컬 악성코드 탐지 업데이트 활성화	로컬 악성코드 탐지 엔진은 Cisco가 제공하는 서명을 사용하여 파일을 정적으로 분석하고 사전 분류합니다. 이 옵션을 활성화하면 Secure Firewall Management Center는 30분마다 서명 업데이트를 확인합니다.
악성코드 이벤트의 URI를 Cisco와 공유	시스템은 네트워크 트래픽에서 탐지된 파일에 대한 정보를 AMP 클라우드로 전송할 수 있습니다. 이러한 정보에는 탐지된 파일 및 SHA-256 해시 값과 관련된 URI 정보가 포함됩니다. 공유는 선택 사항이지만 이러한 정보를 Cisco에 전송하면 추후에 악성코드를 식별하고 추적하는 데 도움이 됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

동적 분석 연결

동적 분석 요구 사항

동적 분석을 사용하려면 Admin, Access Admin 또는 Network Admin 사용자여야 하며 전역 도메인에 있어야 합니다.

Firepower System은 적절한 라이선스를 사용하여 자동으로 Secure Malware Analytics 클라우드에 액세스합니다.

동적 분석을 수행하려면 매니지드 디바이스가 포트 443에서 Secure Malware Analytics 클라우드 또는 온프레미스 Secure Malware Analytics 어플라이언스에 직접 또는 프록시를 통해 액세스할 수 있어야 합니다.

어떤 파일이 동적 분석에 적합합니까?, 33 페이지도 참조하십시오.

온 프레미스 Secure Malware Analytics 어플라이언스에 연결할 계획이라면, 온프레미스 동적 분석 어플라이언스에 연결, 18 페이지에서 설명하는 사전 요건도 참조하십시오.

기본 동적 분석 연결 보기

기본적으로 Secure Firewall Management Center는 파일 제출 및 보고서 검색을 위해 퍼블릭 Secure Malware Analytics 클라우드에 연결할 수 있습니다. 이 연결은 구성하거나 삭제할 수 없습니다.

프로시저

단계 **1** **Integration(**통합**)** > **AMP** > **Dynamic Analysis Connections(**동적 분석 연결**)**를 선택합니다.

단계 **2** **Edit(**수정**)** ( ) 버튼을 클릭합니다.

참고 **Integration(**통합**)** > **AMP** > **Dynamic Analysis Connections(**동적 분석 연결**)** 페이지의 **Associate(**연결**)**( )**Associate(**연결**)**( )에 대한 자세한 내용은 퍼블릭 클라우드의 동적 분석 결과에 대한 액세스 활성화, 20 페이지의 내용을 참조하십시오.

동적 분석 온프레미스 어플라이언스**(Cisco Secure Malware Analytics)**

퍼블릭 Secure Malware Analytics 클라우드에 파일을 제출하는 것과 관련된 개인 정보 보호 또는 보안 우려가 조직에 있는 경우, 온프레미스 Secure Malware Analytics 어플라이언스를 구축할 수 있습니다. 온프레미스 어플라이언스는 퍼블릭 클라우드와 마찬가지로 샌드박스 환경에서 적격 파일을 실행하고 위협 점수와 동적 분석 보고서를 시스템에 반환합니다. 다만 온프레미스 어플라이언스는 퍼블릭 클라우드 또는 네트워크 외부의 다른 시스템과 통신하지 않습니다.

온프레미스 Secure Malware Analytics 어플라이언스에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/threat-grid/index.html의 내용을 참조하십시오.

온프레미스 동적 분석 어플라이언스에 연결

온프레미스 Secure Malware Analytics 어플라이언스를 네트워크에 설치하면 동적 분석 연결을 구성하여 파일을 제출하고 어플라이언스에서 보고서를 가져올 수 있습니다. 온프레미스 어플라이언스 동적 분석 연결을 구성할 때 Secure Firewall Management Center를 온프레미스 어플라이언스에 등록합니다.

시작하기 전에

- 온프레미스 Secure Malware Analytics 어플라이언스를 설정합니다.

  이 어플라이언스의 설명서는 https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html에서 구할 수 있습니다.

  버전 요구 사항은 *Cisco Firepower* 호환성 가이드를 참조하십시오.

- Secure Malware Analytics 어플라이언스가 자체 서명된 공개 키 인증서를 사용하는 경우 Secure Malware Analytics 어플라이언스에서 인증서를 다운로드합니다. 자세한 내용은 Secure Malware Analytics 어플라이언스용 관리자 가이드를 참조하십시오.

  CA(Certificate Authority)에서 서명한 인증서를 사용하는 경우 인증서는 다음 요구 사항을 충족해야 합니다.

  - 서버 키 및 서명된 인증서는 Secure Malware Analytics 어플라이언스에 설치해야 합니다. Secure Malware Analytics 어플라이언스용 관리자 가이드의 업로드 지침을 따릅니다.
  - CA의 다중 레벨 서명 체인이 있는 경우 모든 필수 중간 인증서 및 루트 인증서가 management center에 업로드될 단일 파일에 포함되어야 합니다.
  - 모든 인증서는 PEM으로 인코딩되어야 합니다.
  - 파일의 줄 바꿈은 DOS가 아닌 UNIX여야 합니다.

- 매니지드 디바이스는 포트 443에서 Secure Malware Analytics 어플라이언스에 직접 또는 프록시를 경유하여 액세스할 수 있어야 합니다

프로시저

단계 **1** **Integration(**통합**)** > **AMP** > **Dynamic Analysis Connections(**동적 분석 연결**)**을(를) 선택합니다.

단계 **2** **Add New Connection(**새 연결 추가**)**을 클릭합니다.

단계 **3** **Name(**이름**)**을 입력합니다.

단계 **4** **Host URL(**호스트 **URL)**을 입력합니다.

단계 **5** **Certificate Upload(**인증서 업로드**)** 옆의 **Browse(**찾아보기**)**를 클릭하여 온프레미스 어플라이언스와의 연결 설정에 사용할 퍼블릭 키 인증서를 업로드합니다.

Secure Malware Analytics 어플라이언스가 자체 서명 인증서를 제시할 경우, 해당 어플라이언스에서 다운로드한 인증서를 업로드합니다.

Secure Malware Analytics 어플라이언스가 CA 서명 인증서를 제시할 경우, 인증서 서명 체인을 포함하는 파일을 업로드합니다.

단계 **6** 구성된 프록시를 사용하여 연결을 설정하려면 **Use Proxy When Available(**사용 가능한 경우 프록시 사용**)**를 선택합니다.

단계 **7** **Register(**등록**)**를 클릭합니다.

단계 **8** **Yes(**예**)**를 클릭하여 온프레미스 Secure Malware Analytics 어플라이언스 로그인 페이지를 표시합니다.

단계 **9** 온프레미스 Secure Malware Analytics 어플라이언스에 사용자 이름과 암호를 입력합니다.

단계 **10** **Sign in(**로그인**)**을 클릭합니다.

단계 **11** 다음 옵션을 이용할 수 있습니다.

- 이전에 Secure Firewall Management Center를 온프레미스 어플라이언스에 등록했다면 **Return(**돌아가기**)**을 클릭합니다.

- Secure Firewall Management Center를 등록하지 않았다면 **Activate(**활성화**)**를 클릭합니다.

퍼블릭 클라우드의 동적 분석 결과에 대한 액세스 활성화

Secure Malware Analytics는 분석된 파일에 대해 management center에서 제공하는 것보다 자세한 보고를 제공합니다. 조직이 Secure Malware Analytics 클라우드 계정을 가지고 있다면 Secure Malware Analytics 포털에 직접 액세스하여 매니지드 디바이스에서 분석을 위해 전송한 파일에 대한 추가 세부 정보를 볼 수 있습니다. 하지만 개인 정보 보호를 위해 파일 분석 세부 정보는 해당 파일을 제출한 조직만 볼 수 있습니다. 따라서 이 정보를 보려면 먼저 management center를 매니지드 디바이스에서 제출한 파일에 연결해야 합니다.

시작하기 전에

Secure Malware Analytics 클라우드에 계정이 있어야 하며, 계정 자격 증명을 준비해야 합니다.

프로시저

단계 **1** **Integration(**통합**)** > **AMP** > **Dynamic Analysis Connections(**동적 분석 연결**)**을 선택합니다.

단계 **2** Secure Malware Analytics 클라우드에 해당하는 테이블 열에서 **Associate(**연결**)(**)를 클릭합니다.

Secure Malware Analytics 포털 창이 열립니다.

단계 **3** Secure Malware Analytics 클라우드에 로그인합니다.

단계 **4** **Submit Query(**쿼리 제출**)**를 클릭합니다.

참고 **Devices(**디바이스**)** 필드의 기본값은 변경하지 마십시오.

이 프로세스와 관련하여 어려움이 있다면 Cisco TAC의 Secure Malware Analytics 담당자에게 문의하십시오.

이 변경 사항이 적용되려면 최대 24시간이 소요될 수 있습니다.

다음에 수행할 작업

연결이 활성화되면 Cisco Secure Firewall Management Center 관리 가이드 의 *Cisco Cloud*에서 동적 분석 결과 보기를 참조하십시오.

시스템 유지 관리: 동적 분석 대상인 파일 유형 업데이트

동적 분석 대상 파일 유형 목록은 주기적으로 업데이트되는(단, 하루에 한 번 이상 업데이트되지 않음) 취약성 데이터베이스(VDB)에 의해 결정됩니다. 관리자인 경우 동적 분석에 적합한 파일 유형을 업데이트할 수 있습니다.

시스템에 최신 목록이 있는지 확인하려면

프로시저

단계 **1** 다음 중 하나를 수행합니다.

- (권장 사항) Cisco Secure Firewall Management Center 관리 가이드에 설명된 대로 취약성 데이터베이스 업데이트 자동화를 참조하십시오.
- 새 VDB 업데이트를 정기적으로 확인하고, 필요한 경우 Cisco Secure Firewall Management Center 관리 가이드에 설명된 대로 *VDB*를 수동으로 업데이트합니다.

  이 옵션을 선택하는 경우, 이 작업을 수행하도록 정기적인 미리 알림을 예약하는 것이 좋습니다.

단계 **2** 파일 정책에서 **Dynamic Analysis Capable(**동적 분석 가능**)** 파일 유형 카테고리 대신 개별 파일 유형이 지정된 경우, 새로 지원되는 파일 유형을 사용할 수 있도록 파일 정책을 업데이트합니다.

단계 **3** 동적 분석 대상 파일 유형 목록이 변경되는 경우, 매니지드 디바이스에 이 목록을 구축합니다.

파일 정책 및 파일 규칙

파일 정책 생성 또는 수정

시작하기 전에

악성 코드 보호를 위한 정책을 구성한다면 파일 정책 구성, 8 페이지에서 모든 필수 절차를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)** 을(를) 선택합니다.

단계 **2** 새 정책을 만들거나 기존 정책을 편집합니다.

기존 정책을 수정하는 경우: **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

팁 기존 파일 정책의 복사본을 만들려면 **Copy(**복사**)** ( )을 클릭한 다음 표시되는 대화 상자에서 새로운 정책의 고유한 이름을 입력합니다. 그러면 복사본을 수정할 수 있습니다.

단계 **3** 파일 규칙 생성, 36 페이지에 설명된 것처럼 파일 정책에 하나 이상의 규칙을 추가합니다.

단계 **4** 아니면 Advanced(고급) 탭을 선택하고 고급 및 아카이브 파일 검사 옵션, 22 페이지에 설명된 것처럼 고급 옵션을 구성합니다.

단계 **5** 파일 정책을 저장합니다.

다음에 수행할 작업

- 악성 코드 보호를 위한 정책을 구성한다면 파일 정책 구성, 8 페이지에서 다른 필수 절차를 참조하십시오.
- 그렇지 않을 경우,
  - 액세스 제어 구성에 파일 정책 추가, 9 페이지에 설명된 것처럼 액세스 제어 규칙에 파일 정책을 추가합니다.
  - Deploy configuration changes(구성 변경 사항 구축)참조.

고급 및 아카이브 파일 검사 옵션

파일 정책 편집기의 Advanced(고급) 설정에는 다음과 같은 일반 옵션이 있습니다.

- **First Time File Analysis(**최초 파일 분석**)** - AMP 클라우드 처리가 보류 중인 동안 처음 보는 파일을 분석하려면 이 옵션을 선택합니다. 악성코드 클라우드 조회 및 Spero 분석, 로컬 악성코드 분석 또는 동적 분석을 수행하려면 구성된 규칙과 파일이 일치해야 합니다. 이 옵션을 선택 취소하면 처음으로 탐지된 파일이 Unknown(알 수 없음) 속성으로 표시됩니다.
- **Enable Custom Detection List(**맞춤형 탐지 목록 활성화**)** - 맞춤형 탐지 목록에 있는 파일을 차단합니다.
- **Enable Clean List(**클린 목록 활성화**)** - 이 정책을 활성화하면 클린 목록에 있는 파일이 허용됩니다.
- **AMP** 클라우드 속성이 알 수 없음인 경우 위협 점수를 기준으로 속성을 재정의합니다**.** - 옵션 선택:
  - **Disabled(**비활성화됨**)**를 선택한 경우, 시스템은 AMP 클라우드에서 제공한 속성을 재정의하지 않습니다.
  - 한계치 위협 점수를 설정한 경우 동적 분석 점수가 한계치와 같거나 이보다 나쁘면 AMP 클라우드가 알 수 없음으로 판정된 파일은 악성코드로 간주됩니다.
  - 낮은 임계값을 선택하면 악성코드로 처리되는 파일 수가 늘어납니다. 파일 정책에서 선택한 작업에 따라서는 이렇게 할 경우, 차단되는 파일의 수가 늘어날 수 있습니다.

파일 정책 편집기의 Advanced(고급) 설정에는 다음과 같은 아카이브 파일 검사 옵션이 있습니다.

- **Inspect Archives(**아카이브 검사**) - Maximum file size to store(**최대 저장 파일 크기**)** 고급 액세스 제어 설정만큼 큰 아카이브 파일의 경우, 아카이브 파일의 내용 검사를 활성화합니다.
- **Block Encrypted Archives(**암호화된 아카이브 차단**)** - 암호화된 내용이 있는 아카이브 파일을 차단합니다.
- **Block Uninspectable Archives(**검사할 수 없는 아카이브 차단**)** - 암호화 이외의 이유로 시스템이 검사할 수 없는 내용이 있는 아카이브 파일을 차단합니다. 이것은 일반적으로 손상된 파일이나 지정된 최대 아카이브 깊이를 초과하는 파일에 적용됩니다.

- **Max Archive Depth(**최대 아카이브 깊이**)** - 지정된 깊이를 초과하는 중첩된 아카이브 파일을 차단합니다. 최상위 아카이브 파일은 이 계산에서 고려되지 않으며, 깊이는 처음 중첩된 파일을 기점으로 1부터 시작합니다.

아카이브 파일

아카이브 파일이란 `.zip` 또는 `.rar` 파일처럼 다른 파일을 포함하는 파일입니다.

아카이브에 있는 개별 파일이 차단 작업이 포함된 파일 규칙과 일치하는 경우, 시스템은 개별 파일만이 아니라 전체 아카이브를 차단합니다.

아카이브 파일 검사 옵션에 대한 자세한 내용은 고급 및 아카이브 파일 검사 옵션, 22 페이지를 참조하십시오.

검사할 수 있는 아카이브 파일

- 파일 유형

  검사할 수 있는 아카이브 파일 유형의 전체 목록은 FMC 웹 인터페이스 파일 규칙 구성 페이지에 나와 있습니다. 해당 페이지를 보려면 파일 규칙 생성, 36 페이지를 참조하십시오.

  검사할 수 있는 포함된 파일도 같은 페이지에 표시됩니다.

- 파일 크기

  Maximum file size to store(최대 저장 파일 크기**)** 파일 정책 고급 액세스 제어 설정만큼 큰 아카이브 파일을 검사할 수 있습니다.

- 중첩된 아카이브

  아카이브 파일에는 다른 아카이브 파일이 포함될 수 있고, 이 아카이브 파일에도 아카이브 파일이 포함될 수 있습니다. 파일이 중첩되는 수준이 아카이브 파일 깊이입니다. 최상위 아카이브 파일은 깊이 계산에 포함되지 않으며, 깊이는 처음 중첩된 파일을 기점으로 1부터 시작합니다.

  시스템은 가장 바깥의 아카이브 파일(수준 0) 아래 있는 중첩된 파일을 3개 수준까지 검사할 수 있습니다. 이 깊이(또는 사용자가 지정하는 이보다 낮은 최대 깊이)를 초과하는 아카이브 파일을 차단하도록 파일 정책을 구성할 수 있습니다.

  최대 아카이브 파일 깊이인 3을 초과하는 파일을 차단하지 않도록 선택하는 경우, 추출 가능한 일부 내용과 3 이상의 깊이에서 중첩된 일부 내용을 포함하는 아카이브 파일이 모니터링되는 트래픽에 나타나면 시스템은 검사 가능한 파일의 데이터만 검사하고 보고합니다.

  압축되지 않은 파일에 적용 가능한 모든 기능(예: 동적 분석 및 파일 저장)은 아카이브 파일 내부의 중첩된 파일에도 사용할 수 있습니다.

- 암호화된 파일

  내용이 암호화되거나 그 밖에 검사할 수 없는 아카이브 파일을 차단하도록 시스템을 구성할 수 있습니다.

- 검사되지 않는 아카이브

보안 인텔리전스 차단 또는 차단 금지 목록에 추가된 아카이브 파일이 트래픽에 포함되어 있거나 최상위 아카이브 파일의 SHA-256 값이 맞춤형 탐지 목록에 있는 경우 시스템은 아카이브 파일의 내용을 검사하지 않습니다.

중첩된 파일이 차단되면 전체 아카이브가 차단됩니다. 하지만 중첩된 파일이 허용되더라도 아카이브가 자동으로 통과되지는 않습니다(다른 중첩된 파일 및 특성에 따라 달라짐).

rar5를 포함하여 일부 .rar 아카이브 내의 .Exe 파일을 검색할 수 없습니다.

아카이브 파일 속성

아카이브 파일 속성은 아카이브 내부의 파일에 할당된 속성을 기준으로 합니다. 식별된 악성코드 파일을 포함하는 모든 아카이브에는 `Malware`라는 속성이 제공됩니다. 식별된 악성코드 파일이 없는 아카이브의 경우, 알 수 없는 파일이 포함되어 있으면 `Unknown`이라는 속성이 제공되고, 안전한 파일만 포함되어 있으면 `Clean`이라는 속성이 제공됩니다.

표 ***2:*** 내용별 아카이브 파일 속성

아카이브 파일 속성	알 수 없는 파일 수	안전한 파일 수	악성코드 파일 수
알 수 없음	1개 이상	Any(모든)	0
정상	0	1개 이상	0
악성코드	Any(모든)	Any(모든)	1개 이상

다른 파일과 마찬가지로 아카이브 파일은 `Custom Detection` 또는 `Unavailable` 속성의 조건이 적용될 경우, 해당 속성을 가질 수 있습니다.

아카이브 내용 및 세부 정보 보기

아카이브 파일 내용을 검사하도록 파일 정책을 구성할 경우, Analysis(분석) > Files(파일) 메뉴 아래 테이블의 컨텍스트 메뉴 및 네트워크 파일 전파 흔적 분석 뷰어를 사용하면 아카이브 파일이 파일 이벤트, 악성코드 이벤트에 표시되거나 캡처 파일로 표시될 때 아카이브 내부의 파일에 대한 정보를 볼 수 있습니다.

아카이브의 모든 파일 내용은 테이블 형식으로 나열되며, 관련 정보(이름, SHA-256 해시 값, 유형, 카테고리, 아카이브 깊이)가 짧게 요약되어 있습니다. 네트워크 파일 전파 흔적 분석 아이콘은 각 파일 옆에 표시되며, 클릭하면 해당 특정 파일에 대한 추가 정보를 볼 수 있습니다.

맞춤형 목록을 사용한 파일 속성 재정의

AMP 클라우드의 파일에 잘못된 속성이 있는 경우, 클라우드의 속성을 재정의하는 파일의 SHA-256 값을 파일 목록에 추가할 수 있습니다.

- AMP 클라우드가 안전 속성을 할당한 것처럼 파일을 처리하려면 파일을 안전 목록에 추가합니다.
- AMP 클라우드가 악성코드 속성을 할당한 것처럼 파일을 처리하려면 파일을 맞춤형 탐지 목록에 추가합니다.

후속 탐지 시 디바이스는 파일의 속성을 다시 평가하지 않고 파일을 허용하거나 차단합니다. 파일 정책별로 안전 목록 또는 맞춤형 탐지 목록을 사용할 수 있습니다.

참고 파일의 SHA-256 값을 계산하려면 파일 정책에서 규칙을 구성하여 악성코드 클라우드 조회를 수행하거나 일치하는 파일의 악성코드를 차단해야 합니다.

Firepower에서 파일 목록을 사용하는 방법에 대한 자세한 내용은 파일 목록를 참조하십시오.

또는 해당하는 경우, AMP for Endpoints의 중앙 집중식 파일 목록, 25 페이지를 사용합니다.

*AMP for Endpoints*의 중앙 집중식 파일 목록

조직이 AMP for Endpoints를 구축한 경우, Firepower는 AMP 클라우드에서 파일 속성을 쿼리할 때 AMP for Endpoints에 생성된 차단 목록과 허용 목록을 사용할 수 있습니다.

요건:

- 조직이 AMP 퍼블릭 클라우드를 사용해야 합니다.
- 조직이 AMP for Endpoints를 구축했습니다.
- Firepower 및 Secure Endpoint 통합, 42 페이지의 절차를 사용하여 Firepower 시스템을 AMP for Endpoints에 등록했습니다.

이러한 목록을 생성하고 구축하려면 AMP for Endpoints 설명서 또는 온라인 도움말을 참조하십시오.

참고 Firepower에서 생성된 파일 목록은 AMP for Endpoints에서 생성된 파일 목록을 재정의합니다.

파일 정책 관리

File Policies(파일 정책) 페이지에는 기존 파일 정책의 목록이 최종 수정 날짜와 함께 표시됩니다. 이 페이지를 사용하여 파일 정책을 관리할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

참고 시스템에서는 동적 분석에 적합한 파일 유형의 목록이 업데이트되었는지 확인합니다(하루에 한 번만 수행). 적합한 파일 유형 목록이 변경되면 파일 정책이 변경됩니다. 해당 파일 정책을 사용하는 모든 액세스 제어 정책은 디바이스에 구축되는 경우, 기한이 지난 것으로 표시됩니다. 업데이트된 파일 정책이 디바이스에 적용되려면 먼저 정책을 구축해야 합니다. 시스템 유지 관리: 동적 분석 대상인 파일 유형 업데이트, 20 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)** 을(를) 선택합니다.

단계 **2** 파일 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교를 참조하십시오.
- 생성 - 파일 정책을 생성하려면 **New File Policy(**새 파일 정책**)**를 클릭하고 파일 정책 생성 또는 수정, 21 페이지에 설명된 대로 진행합니다.
- 복사 - 파일 정책을 복사하려면 **Copy(**복사**)** ( )을 클릭합니다.

  View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - 파일 정책을 삭제하려면 **Delete(**삭제**)** ( )을 클릭한 다음 표시되는 메시지에 따라 **Yes(**예**)** 및 **OK(**확인**)**를 클릭합니다.

  컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 구성 변경 사항 구축의 내용을 참조하십시오.
- 수정 - 기존 파일 정책을 수정하려면 **Edit(**수정**)** ( )을 클릭합니다.
- 보고서- **Report(**보고서**)** ( )를 클릭합니다. 현재 정책 보고서 생성를 참조하십시오.

파일 규칙

상위 액세스 제어 정책과 마찬가지로, 파일 정책에는 각 규칙의 조건과 일치하는 파일을 처리하는 방식을 결정하는 규칙이 포함됩니다. 별도의 파일 규칙을 구성하여 각기 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향마다 다른 작업을 실행할 수 있습니다.

예를 들어 파일이 규칙과 일치할 경우, 규칙은 다음을 수행할 수 있습니다.

- 간단한 파일 유형 일치를 기준으로 파일 허용 또는 차단
- 처리(평가에서 악성임이 나타나는지의 여부)를 기준으로 파일 차단
- 디바이스에 파일 저장 (자세한 내용은 참조 캡처된 파일 및 파일 스토리지, 33 페이지)
- 로컬 악성코드 분석, Spero 분석 또는 동적 분석을 위해 저장(캡처)된 파일 제출

또한 파일 정책으로 다음을 수행할 수 있습니다.

- 정상 목록 또는 맞춤형 탐지 목록의 항목을 기준으로 파일을 안전한 파일 또는 악성코드로 자동 처리

- 파일의 위협 점수가 구성 가능한 임계값을 초과할 경우 파일을 악성코드로 처리
- `.zip` 또는 `.rar` 같은 아카이브 파일의 내용 검사
- 내용이 암호화되거나 지정된 최대 보관 깊이를 넘어 중첩되거나 그 밖에 검사할 수 없는 아카이브 파일을 차단

파일 규칙 구성 요소

표 *3:* 파일 규칙 구성 요소

파일 규칙 구성 요소	설명
애플리케이션 프로토콜:	시스템에서는 FTP, HTTP, SMTP, IMAP, POP3, NetBIOS-ssn(SMB)을 통해 전송된 파일을 탐지하고 검사할 수 있습니다. 기본값인 **Any(**모두**)**는 HTTP, SMTP, IMAP, POP3, FTP 및 NetBIOS-ssn(SMB) 트래픽에서 파일을 탐지합니다. 성능 향상을 위해 파일별 규칙을 기반으로 한 애플리케이션 프로토콜 중 하나만 대상으로 하여 파일 탐지를 제한할 수 있습니다.
전송 방향	다운로드한 파일에 대해 수신 FTP, HTTP, POP3, IMAP 및 NetBIOS-ssn(SMB) 트래픽을 검사할 수 있으며, 업로드한 파일에 대해서는 발신 FTP, HTTP, SMTP 및 NetBIOS-ssn(SMB) 트래픽을 검사할 수 있습니다. 팁 사용자가 전송하는지 또는 수신하는지에 상관없이, **Any(**모두**)**를 사용하여 여러 애플리케이션 프로토콜에서 파일을 탐색합니다.
파일 카테고리 및 유형	시스템에서는 다양한 유형의 파일을 탐지할 수 있습니다. 이러한 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent), PDF를 비롯한 기본적인 카테고리로 그룹화됩니다. 개별 파일 유형을 탐지하거나, 파일 유형의 전체 카테고리를 탐지하는 파일 규칙을 구성할 수 있습니다. 예를 들어, 모든 멀티미디어 파일을 차단할 수도 있고, ShockWave Flash(swf) 파일만 차단할 수도 있습니다. 또는 사용자가 BitTorrent(torrent) 파일을 다운로드할 경우 알림을 제공하도록 시스템을 구성할 수 있습니다. 실행 파일은 악성코드가 포함될 수 있으므로 매크로 및 스크립트를 실행할 수 있는 파일 유형으로 구성됩니다. 시스템이 검사할 수 있는 파일 유형 목록의 경우, **Policies(**정책**) > Access Control(**액세스 제어**) > Malware & File(**악성코드 및 파일**)**을 선택하고 임시 새 파일 정책을 생성한 다음 **Add Rule(**규칙 추가**)**를 클릭합니다. 파일 유형 카테고리를 선택하면 시스템이 검사할 수 있는 파일 유형이 **File Types(**파일 유형**)** 목록에 나타납니다. 참고 빈번하게 트리거되는 파일 규칙은 시스템 성능에 영향을 줄 수 있습니다. 예를 들어, HTTP 트래픽(예: 상당량의 Flash 콘텐츠를 전송하는 YouTube)의 멀티미디어 파일을 탐지할 경우 지나치게 많은 이벤트가 생성될 수 있습니다.

파일 규칙 구성 요소	설명
파일 규칙 작업	파일 규칙 작업에서는 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정합니다. 선택한 작업에 따라 시스템이 파일을 저장할지 또는 파일에서 Spero, 로컬 악성코드 또는 동적 분석을 수행할지 구성할 수 있습니다. 차단 작업을 선택하는 경우, 시스템이 차단된 연결을 재설정하는지도 구성할 수 있습니다. 이러한 작업과 옵션에 대한 설명은 파일 규칙 작업, 28 페이지를 참조하십시오. 파일 규칙은 숫자나 순서가 아닌 규칙 작업으로 평가됩니다. 자세한 내용은 파일 규칙 작업: 평가 순서, 35 페이지를 참조하십시오.

파일 규칙 작업

파일 규칙은 악성코드 탐지를 위해 어떤 파일 유형을 로깅하거나, 차단, 확인하기를 원하는지에 대해 세분화된 제어 기능을 제공합니다. 각 파일 규칙에는 시스템이 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정하는 관련 작업이 포함됩니다. 파일 정책은 하나 이상의 규칙을 포함해야 적용할 수 있습니다. 파일 정책 내에서 별도의 규칙을 사용하여 서로 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향에 맞는 다양한 작업을 실행할 수 있습니다.

파일 규칙 작업

- *Detect Files(*파일 탐지*)* 규칙을 사용하면 데이터베이스에 특정 파일 유형의 탐지를 로깅할 수 있지만 여전히 해당 전송을 허용합니다.
- *Block Files(*파일 차단*)* 규칙을 사용하면 특정 파일 유형을 차단할 수 있습니다. 파일 전송이 차단되었을 때 연결을 재설정하는 옵션을 구성하고 캡처된 파일을 매니지드 디바이스에 저장할 수 있습니다.
- *Malware Cloud Lookup(*악성코드 클라우드 조회*)* 규칙을 사용하면 네트워크를 통과하는 파일의 속성을 가져오고 로깅하면서 전송을 허용할 수 있습니다.
- *Block Malware(*악성코드 차단*)* 규칙을 사용하면 특정 파일 유형의 SHA-256 해시 값을 계산하고 AMP 클라우드를 조회하여 네트워크를 통과하는 파일이 악성코드를 포함하는지 확인한 다음 위협을 나타내는 파일을 차단할 수 있습니다.

파일 규칙 작업 옵션

선택하는 작업에 따라 여러 옵션이 있습니다.

파일 규칙 작업 옵션	파일 차단 가능?	악성 코드 차단 가능?	파일 탐지 가능?	악성코드 클라우드 조회 가능?
MSEXE의 Spero 분석*	아니요	예, 실행 파일을 제출할 수 있음	아니요	예, 실행 파일을 제출할 수 있음

파일 규칙 작업 옵션	파일 차단 가능?	악성 코드 차단 가능?	파일 탐지 가능?	악성코드 클라우드 조회 가능?
동적 분석*	아니요	예, 파일 속성이 Unknown인 실행 파일을 제출할 수 있음	아니요	예, 파일 속성이 Unknown인 실행 파일을 제출할 수 있음
용량 처리	아니요	예	아니요	예
로컬 악성코드 분석*	아니요	예	아니요	예
연결 재설정	예(권장)	예(권장)	아니요	아니요
파일 저장	예, 일치하는 모든 파일 유형을 저장할 수 있음	예, 선택한 파일 속성과 일치하는 파일 유형을 저장할 수 있음	예, 일치하는 모든 파일 유형을 저장할 수 있음	예, 선택한 파일 속성과 일치하는 파일 유형을 저장할 수 있음

* 이러한 옵션에 대한 자세한 내용은 (파일 규칙 작업의) 악성코드 차단 옵션, 29 페이지 및 하위 항목을 참조하십시오.

주의 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 Enabling or disabling **Store Files(**파일 저장 활성화 또는 비활성화**)**를 활성화하거나 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)** 또는 **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**), Unknown(**알 수 없음**)**, **Clean(**정상**)** 또는 **Custom(**맞춤형**))**과 결합하는 첫 번째 파일 규칙을 추가하거나 마지막 파일 규칙을 제거, 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.

(파일 규칙 작업의) 악성코드 차단 옵션

시스템은 여러 파일 검사 및 분석 방법을 사용하여 파일에 악성코드가 포함되어 있는지 확인합니다.

파일 규칙에서 활성화한 옵션에 따라 시스템은 다음 도구를 다음 순서로 사용하여 파일을 검사합니다.

1. Spero 분석, 31 페이지 및 AMP 클라우드 조회, 31 페이지
2. 로컬 악성코드 분석, 32 페이지
3. 동적 분석, 32 페이지

이러한 도구를 비교하려면 악성코드 차단 옵션 비교, 30 페이지를 참조하십시오.

(원하는 경우, 파일 유형에 따라 모든 파일을 차단할 수도 있습니다. 자세한 내용은 유형별로 모든 파일 차단, 35 페이지를 참고하십시오.

(선택 사항) AMP for Endpoints를 사용한 악성코드 방지, 40 페이지 및 하위 항목에서 Cisco의 AMP for Endpoints 제품에 대한 정보도 참조하십시오.

악성코드 차단 옵션 비교

다음 표에서는 각 파일 분석 유형의 장단점과 각 악성코드 방지 방법이 파일 속성을 결정하는 방식을 자세히 설명합니다.

분석 유형	이점	제한 사항	악성코드 식별
Spero 분석	실행 파일의 구조 분석으로서 분석을 위해 Spero 서명을 AMP 클라우드로 전송	로컬 악성코드 분석 또는 동적 분석보다 덜 정밀하며 실행 파일만 분석	악성코드로 확인되는 경우에만 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
로컬 악성코드 분석	동적 분석보다 적은 리소스를 사용하며, 특히 탐지된 악성코드가 일반적인 경우, 결과를 보다 빨리 반환합니다.	동적 분석보다 덜 정밀한 결과	악성코드로 확인되는 경우에만 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
동적 분석	다음을 사용하여 알 수 없는 파일을 정밀 분석 Secure Malware Analytics	적격 파일은 퍼블릭 클라우드 또는 현장 어플라이언스에 업로드됩니다. 분석을 완료하는 데 시간이 소요됩니다	위협 점수는 파일의 악성 정도를 결정합니다. 속성은 파일 정책에서 구성된 위협 점수 임계값에 기반을 둘 수 있습니다.
Spero 분석 및 로컬 악성코드 분석	로컬 악성코드 분석 및 동적 분석 구성보다 적은 리소스를 사용하면서 AMP 클라우드를 사용하여 악성코드를 식별합니다	동적 분석보다 덜 정밀하며 Spero 분석은 실행 파일만 분석합니다	악성코드로 확인되는 경우에만 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
Spero 분석 및 동적 분석	파일 및 Spero 서명 제출에 AMP 클라우드의 모든 기능 사용	로컬 악성코드 분석을 사용하는 경우보다 결과를 얻는 속도가 느림	가능한 악성코드로 사전 분류된 파일에 대한 동적 분석 결과에 따라 위협 점수가 변경됩니다. 파일 정책에서 구성된 위협 점수 임계값에 따라 속성이 변경되며, Spero 분석이 악성코드를 식별하면 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.

분석 유형	이점	제한 사항	악성코드 식별
로컬 악성코드 분석 및 동적 분석	두 가지 파일 분석 유형 사용 시 정밀한 결과	하나만 사용하는 것보다 많은 리소스를 사용	가능한 악성코드로 사전 분류된 파일에 대한 동적 분석 결과에 따라 위협 점수가 변경됩니다. 로컬 악성코드 분석에서 악성코드를 식별하는 경우, 또는 파일 정책에서 구성된 위협 점수 임계값에 따라 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
Spero 분석, 로컬 악성코드 분석, 동적 분석	가장 정밀한 결과	세 가지 유형의 파일 분석을 모두 실행 시 가장 많은 리소스 사용	가능한 악성코드로 사전 분류된 파일에 대한 동적 분석 결과에 따라 위협 점수가 변경됩니다. Spero 분석이나 로컬 악성코드 분석에서 악성코드를 식별하는 경우, 또는 파일 정책에서 구성된 위협 점수 임계값에 따라 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 변경됩니다.
(지정된 파일 유형의 모든 파일 전송을 차단)	악성코드 라이선스 필요 없음 (이 옵션은 기술적으로 악성코드 방지 옵션이 아닙니다.)	적법한 파일도 차단됩니다.	(분석이 수행되지 않습니다.)

참고 사전 분류 자체는 파일의 속성을 확인하지 않으며, 파일이 동적 분석에 적합한지 결정하는 요소 중 하나일 뿐입니다.

Spero 분석

Spero 분석은 실행 파일의 메타데이터 및 헤더 정보와 같은 구조적 특성을 검사합니다. 이 정보를 기반으로 Spero 서명을 생성한 후 파일이 적격 실행 파일인 경우, 디바이스는 이를 AMP 클라우드의 Spero 휴리스틱 엔진에 제출합니다. Spero 엔진은 Spero 서명을 기반으로 파일이 악성코드인지 확인합니다. 또한 파일을 AMP 클라우드에 제출하지 않고 Spero 분석을 위해 제출하도록 규칙을 구성할 수도 있습니다.

Spero 분석을 위해 수동으로 파일을 제출할 수는 없습니다.

AMP 클라우드 조회

Advanced Malware Protection를 사용한 평가 대상 파일의 경우, management center는 악성코드 클라우드 조회를 수행하여 파일의 SHA-256 해시 값을 기반으로 파일의 속성을 AMP 클라우드에서 쿼리합니다.

시스템은 성능 향상을 위해 클라우드가 반환한 속성을 캐시하고 알려진 파일의 경우, AMP 클라우드를 쿼리하는 대신 캐시된 속성을 사용합니다. 이 캐시에 대한 자세한 내용은 캐시된 속성 수명, 32 페이지를 참조하십시오.

로컬 악성코드 분석

로컬 악성코드 분석을 통해 매니지드 디바이스는 Talos 인텔리전스 그룹가 제공하는 탐지 규칙 세트을 사용하여 실행 파일, PDF, Office 문서 및 기타 파일 유형에서 가장 일반적인 유형의 악성코드를 로컬로 검사할 수 있습니다. 로컬 악성코드 분석은 AMP 클라우드를 쿼리하지 않고 파일을 실행하지 않기 때문에 시간과 시스템 리소스가 절약됩니다.

시스템이 로컬 악성코드 분석을 통해 악성코드를 식별하는 경우, 기존 악성코드 속성이 Unknown(알 수 없음)에서 Malware(악성코드)로 업데이트됩니다. 그러면 시스템이 새로운 악성코드 이벤트를 생성합니다. 시스템이 악성코드를 식별하지 않으면 파일 속성이 Unknown(알 수 없음)에서 Clean(안전)으로 업데이트되지 않습니다. 시스템은 로컬 악성코드 분석을 실행한 후 SHA-256 해시 값, 타임스탬프, 속성 같은 파일 정보를 캐시하므로 일정 기간 내에 다시 탐지될 경우, 추가 분석 없이 악성코드를 식별할 수 있습니다. 캐시에 대한 자세한 내용은 캐시된 속성 수명, 32 페이지를 참조하십시오.

로컬 악성 코드 분석은 Secure Malware Analytics 클라우드와의 통신이 필요하지 않습니다. 하지만 동적 분석을 위해 파일을 제출하고 로컬 악성코드 분석 규칙 집합 업데이트를 다운로드하려면 클라우드와의 통신을 구성해야 합니다.

캐시된 속성 수명

AMP 클라우드 쿼리에서 반환된 속성, 관련 위협 점수, 로컬 악성코드 분석에 의해 할당된 속성은 TTL(time-to-live) 값을 갖습니다. TTL 값에 지정된 기간 동안 속성이 업데이트되지 않고 유지될 경우, 시스템에서는 캐시된 정보를 삭제합니다. 속성 및 관련 위협 점수에는 다음과 같은 TTL 값이 포함됩니다.

- 안전 - 4시간
- 알 수 없음 - 1시간
- 악성코드 - 1시간

캐시에 대한 쿼리에서 시간 초과된 캐시된 속성이 식별되는 경우, 시스템은 로컬 악성코드 분석 데이터베이스와 AMP 클라우드에서 새로운 속성을 다시 쿼리합니다.

동적 분석

Secure Malware Analytics (이전의 Threat Grid), Cisco의 파일 분석, 위협 인텔리전스 플랫폼을 사용하여 동적 분석을 위해 자동으로 파일을 제출하도록 파일 정책을 구성할 수 있습니다.

디바이스는 디바이스에 파일이 저장되어 있는지 여부에 상관없이 적격 파일을 Secure Malware Analytics(사용자가 지정한 퍼블릭 클라우드 또는 현장 어플라이언스)에 제출합니다.

Secure Malware Analytics 파일을 샌드박스 환경에서 실행하고 파일의 동작을 분석해 파일이 악성인지 확인하고 파일에 악성코드가 포함되었을 가능성을 나타내는 위협 점수를 반환합니다. 위협 점수

에서 동적 분석 요약 보고서와 함께 할당된 위협 점수의 이유를 볼 수 있습니다. 또한 Secure Malware Analytics에서 조직이 제출한 파일의 상세한 보고서를 볼 수 있을 뿐 아니라 조직이 제출하지 않은 파일에 대한 삭제된 보고서를 제한된 데이터와 함께 볼 수 있습니다.

Cisco Secure Malware Analytics에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/threat-grid/index.html를 참조하십시오

동적 분석을 수행하도록 시스템을 구성하려면 동적 분석 연결, 17 페이지 아래의 주제를 참조하십시오.

어떤 파일이 동적 분석에 적합합니까?

파일이 동적 분석에 적합한지 여부는 다음에 따라 달라집니다.

- 파일 형식
- 파일 크기
- 파일 규칙 작업

또한

- 시스템은 사용자가 구성하는 파일 규칙에 일치하는 파일만 제출합니다.
- 분석을 위해 전송될 때 파일에는 Unknown(알 수 없음) 또는 Unavailable(사용할 수 없음)의 악성코드 클라우드 조회 속성이 있어야 합니다.
- 시스템은 파일을 잠재적 악성코드로 사전 분류해야 합니다.

동적 분석 및 용량 처리

용량 처리를 사용하면 디바이스가 클라우드와 통신할 수 없거나 최대 제출 수에 도달했기 때문에 시스템이 일시적으로 클라우드에 파일을 전송할 수 없는 경우, 그렇지 않았다면 동적 분석되었을 파일을 일시적으로 저장할 수 있습니다. 전송을 방해하는 조건이 지나가면 시스템은 저장된 파일을 제출합니다.

일부 디바이스는 디바이스 하드 드라이브 또는 악성코드 스토리지 팩에 파일을 저장할 수 있습니다. 악성코드 스토리지 팩, 34 페이지도 참조하십시오.

캡처된 파일 및 파일 스토리지

파일 스토리지 기능을 사용하면 트래픽에서 탐지된 선택된 파일을 캡처한 다음 디바이스의 하드 드라이브 또는 악성코드 스토리지 팩(설치된 경우)에 파일의 사본을 자동으로 임시 저장할 수 있습니다.

디바이스가 파일을 캡처한 후 다음을 수행할 수 있습니다.

- 나중에 분석하기 위해 캡처한 파일을 디바이스의 하드 드라이브에 저장합니다.
- 저장된 파일을 추가 수동 분석 또는 아카이브를 위해 로컬 컴퓨터로 다운로드합니다.
- AMP 클라우드 조회 또는 동적 분석을 위해 캡처된 적격 파일을 수동으로 제출합니다.

디바이스는 파일을 저장한 경우, 나중에 해당 파일이 탐지되었을 때 여전히 저장되어 있으면 다시 캡처하지 않습니다.

참고 네트워크에서 처음으로 파일이 탐지되면 파일의 탐지를 나타내는 파일 이벤트를 생성할 수 있습니다. 하지만 파일 규칙이 악성코드 클라우드 조회를 수행하는 경우, AMP 클라우드를 쿼리하고 속성을 반환하기 위한 추가 시간이 필요합니다. 이 지연으로 인해 시스템은 이 파일이 네트워크에 두 번째로 나타날 때까지 해당 파일을 저장할 수 없으며, 파일의 속성을 즉시 결정할 수 있습니다.

시스템이 파일을 캡처하든 저장하든 사용자는 다음을 수행할 수 있습니다.

- 파일이 저장되었는지 동적 분석을 위해 제출되었는지 여부, 파일 속성, 위협 점수 등 캡처된 파일에 대한 정보를 Analysis(분석) > Files(파일) > Captured Files(캡처된 파일)에서 검토할 수 있으며, 이를 통해 사용자는 네트워크에서 탐지된 악성코드 위협 가능성을 신속하게 검토할 수 있습니다.
- 파일의 전파 흔적을 보고 파일이 네트워크에서 어떻게 이동했고 어떤 호스트에 복사본이 있는지를 확인할 수 있습니다.
- 향후 탐지에서 정상 또는 악성코드 속성이 있는 것으로 항상 취급하려면 파일을 정상 목록 또는 맞춤형 탐지 목록에 추가하십시오.

사용 가능한 경우, 특정 유형 또는 특정 속성의 파일을 캡처 및 저장하도록 파일 정책에서 파일 규칙을 구성할 수 있습니다. 파일 정책을 액세스 제어 정책과 연결하고 디바이스에 구축하면 트래픽에서 일치하는 파일이 캡처 및 저장됩니다. 또한 저장할 최소 및 최대 파일 크기를 제한할 수도 있습니다.

저장된 파일은 시스템 백업에 포함되지 않습니다.

Analysis(분석) > Files(파일) > Captured Files(캡처된 파일)에서 캡처된 파일 정보를 보고 오프라인 분석을 위해 복사본을 다운로드할 수 있습니다.

악성코드 스토리지 팩

디바이스에서는 파일 정책 구성을 기반으로 상당한 양의 파일 데이터를 하드 드라이브에 저장할 수 있습니다. 디바이스에 악성코드 스토리지 팩을 설치할 수 있습니다. 시스템은 파일을 악성코드 스토리지 팩에 저장하므로 기본 하드 드라이브에 이벤트와 구성 파일을 저장하기 위한 공간이 좀 더 확보됩니다. 시스템은 주기적으로 오래된 파일을 삭제합니다. 디바이스의 기본 하드 드라이브에 여유 공간이 충분하지 않고 악성코드 스토리지 팩이 설치되어 있지 않으면 파일을 저장할 수 없습니다.

주의 Cisco에서 제공하지 않은 하드 드라이브를 디바이스에 설치하려고 하지 마십시오. 지원되지 않는 하드 드라이브를 설치하면 디바이스가 손상될 수 있습니다. 악성코드 스토리지 팩 키트는 Cisco에서만 구입할 수 있습니다. 악성코드 스토리지 팩과 관련하여 도움이 필요하면 고객 지원에 문의하십시오. 자세한 내용은 *Firepower System* 악성코드 스토리지 팩 설명서을 참조하십시오.

악성코드 스토리지 팩이 설치되지 않은 상태에서 파일을 저장하도록 디바이스를 구성하면 기본 하드 드라이브 공간의 일정 부분이 캡처된 파일 스토리지에 할당됩니다. 동적 분석을 위해 임시로 파일

을 저장하도록 용량 처리를 구성하는 경우, 시스템은 클라우드에 파일을 다시 전송할 수 있을 때까지 동일한 하드 드라이브 할당을 사용하여 이 파일을 저장합니다.

디바이스에 악성코드 스토리지 팩을 설치하고 파일 저장소 또는 용량 처리를 구성하는 경우, 디바이스는 이러한 파일을 저장하기 위해 전체 악성코드 스토리지 팩을 할당합니다. 디바이스는 악성코드 스토리지 팩에 다른 정보를 저장할 수 없습니다.

캡처된 파일 스토리지에 할당된 공간이 다 차면 시스템은 할당된 공간이 시스템 정의 임계값에 도달할 때까지 저장된 파일 중 가장 오래된 파일을 삭제합니다. 저장된 파일 수를 기준으로 시스템이 파일을 삭제한 후 디스크 사용량이 상당히 줄어든 것을 볼 수 있습니다.

디바이스가 이미 파일을 저장한 상태에서 악성코드 스토리지 팩을 설치하면 디바이스를 다음에 다시 시작할 때 기본 하드 드라이브에 저장된 캡처된 파일 또는 용량 처리 파일이 악성코드 스토리지 팩으로 이동합니다. 이후 디바이스에서 저장하는 파일은 악성코드 스토리지 팩에 저장됩니다.

유형별로 모든 파일 차단

조직에서 악성코드뿐만 아니라 특정 유형의 모든 파일(파일의 악성코드 여부 포함 여부에 상관없이)의 전송을 차단하려는 경우, 차단이 가능합니다.

파일 제어는 시스템이 악성코드와 더불어 다양한 추가 파일 유형을 탐지할 수 있는 경우 모든 파일 유형을 지원합니다. 이러한 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent), PDF와 같은 기본적인 카테고리로 그룹화됩니다.

유형을 기준으로 모든 파일을 차단하는 것은 기술적으로는 악성코드 방지 기능이 아닙니다. 즉, 악성코드 라이선스가 필요하지 않고 AMP 클라우드를 쿼리하지 않습니다.

파일 규칙 작업: 평가 순서

파일 정책에는 상황마다 서로 다른 작업이 포함된 여러 규칙이 포함될 가능성이 높습니다. 특정 상황에 둘 이상의 규칙이 적용될 수 있는 경우, 이 주제에 설명된 평가 순서가 적용됩니다. 일반적으로 단순 차단은 악성코드 탐지 및 차단보다 우선하는데, 이는 단순 탐지 및 로깅에 우선하는 것입니다.

파일 규칙 작업의 우선 순위는 다음과 같습니다.

- 파일 차단
- 악성코드 차단
- 악성코드 클라우드 조회
- 파일 탐지

파일 규칙 생성

주의 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 Enabling or disabling **Store Files(**파일 저장 활성화 또는 비활성화**)**를 활성화하거나 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)** 또는 **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**), Unknown(**알 수 없음**)**, **Clean(**정상**)** 또는 **Custom(**맞춤형**))**과 결합하는 첫 번째 파일 규칙을 추가하거나 마지막 파일 규칙을 제거, 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.

시작하기 전에

악성 코드 보호를 위한 규칙을 구성한다면, 파일 정책 구성, 8 페이지 섹션을 참조하십시오.

프로시저

단계 **1** 파일 정책 편집기에서 파일 규칙 추가클릭 합니다.

단계 **2** 파일 규칙 구성 요소, 27 페이지에 설명된 대로 **Application Protocol(**애플리케이션 프로토콜**)**과 **Direction of Transfer(**전송 방향**)**을 선택합니다.

단계 **3** 하나 이상의 **File Types(**파일 유형**)**를 선택합니다.

표시되는 파일 유형은 선택한 애플리케이션 프로토콜, 전송 방향, 작업에 따라 달라집니다.

파일 유형 목록을 다음 방법으로 필터링할 수 있습니다.

- 하나 이상의 **File Type Categories(**파일 유형 카테고리**)**를 선택한 다음 **All types in selected Categories(**선택한 카테고리의 모든 유형**)**를 클릭합니다.
- 해당 이름 또는 설명으로 파일 유형을 검색합니다. 예를 들어, Microsoft Windows 특유의 파일 목록을 표시하려면 **`Windows`**를 **Search name and description(**이름 및 설명 검색**)** 필드에 입력합니다.

팁 해당 설명을 확인하려면 파일 유형 위에 마우스 포인터를 올려놓습니다.

단계 **4** 파일 규칙 작업, 28 페이지S에 설명된 대로 파일 규칙 작업: 평가 순서, 35 페이지을 고려하여 파일 규칙 **Action(**작업**)**을 선택합니다.

사용 가능한 작업은 설치한 라이선스에 따라 달라집니다. 파일 및 악성코드 정책을 위한 라이선스 요구 사항, 3 페이지의 내용을 참조하십시오.

단계 **5** 선택한 작업에 따라 옵션을 구성합니다.

- 파일 차단 후 연결을 재설정

- 규칙과 일치하는 파일 저장
- Spero 분석* 활성화
- 로컬 악성 코드 분석* 활성화
- 동적 분석* 및 용량 처리 활성화

* 이러한 옵션에 대한 자세한 내용은 파일 규칙 작업, 28 페이지과 (파일 규칙 작업의) 악성코드 차단 옵션, 29 페이지 및 하위 항목을 참조하십시오.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 악성 코드 보호를 위한 정책을 구성한다면, 파일 정책 구성, 8 페이지 섹션으로 돌아가십시오.
- Deploy configuration changes(구성 변경 사항 구축)참조.

악성 코드 차단을 위한 액세스 제어 규칙 로깅

시스템이 파일 정책의 설정에 따라 (악성코드 등) 금지된 파일을 탐지하면 자동으로 Secure Firewall Management Center 데이터베이스에 이벤트가 로깅됩니다. 파일 또는 악성코드 이벤트를 로깅하지 않으려는 경우, 액세스 제어 규칙마다 이러한 로깅을 비활성화할 수 있습니다.

시스템은 또한 액세스 제어 규칙 호출의 로깅 구성에 관계없이 Secure Firewall Management Center 데이터베이스와 관련된 연결의 종료를 로깅합니다.

회귀적 속성 변경

파일 속성은 변경될 수 있습니다. 예를 들어 새로운 정보가 발견됨에 따라 AMP 클라우드는 이전에는 정상으로 간주되었던 파일이 지금은 악성코드로 식별되는 경우 또는 그 반대의 경우(악성코드로 식별된 파일이 실제로 정상임)를 결정할 수 있습니다. 지난주에 쿼리한 파일의 속성이 변경되는 경우, AMP 클라우드는 시스템에 이를 알려 시스템이 다음에 해당 파일의 전송을 탐지할 경우 적절한 조치를 취할 수 있도록 합니다. 변경된 속성은 회귀적 속성이라고 합니다.

파일 및 악성코드 탐지 성능 및 저장 옵션

파일 크기를 늘리면 시스템의 성능에 영향을 미칠 수 있습니다.

표 *4:* 고급 액세스 제어 파일 및 악성코드 대응 옵션

필드	설명	지침 및 제한 사항
파일 유형 탐지 중에 검사되는 바이트 수 제한	파일 유형 탐지를 수행할 때 검사되는 바이트 수를 지정합니다.	0-4294967295(4GB) 0은 제한을 제거합니다. 기본값은 TCP 패킷의 최대 세그먼트 크기입니다(1460바이트). 대부분의 경우 시스템은 첫 번째 패킷을 사용하여 공용 파일 유형을 확인할 수 있습니다. ISO 파일을 탐지하려면 36870보다 큰 값을 입력합니다.
악성코드 차단을 위한 클라우드 조회가 다음보다 오래 걸리는 경우 파일 허용(초)	악성코드 클라우드 조회가 이루어지는 동안 **Block Malware(**악성코드 차단**)** 규칙과 일치하고 캐시된 속성이 없는 파일의 최종 바이트가 시스템에 유지되는 기간을 지정합니다. 시스템이 속성을 보유하지 못하고 시간이 경과하면, 파일은 통과됩니다. 사용할 수 없는 속성은 캐시되지 않습니다.	0-30초 지원 팀에 문의하지 않고 이 옵션을 0으로 설정하지 마십시오. Cisco는 연결 실패로 인한 트래픽 차단을 방지하기 위해 기본값을 사용할 것을 권장합니다.
(바이트)보다 큰 파일의 **SHA-256** 해시 값을 계산하지 마십시오**.**	맞춤형 탐지 목록에 추가된 경우, 시스템이 특정 크기보다 큰 파일을 저장하거나 파일에 대한 클라우드 조회를 하거나 파일을 차단하지 않도록 합니다.	0-4294967295(4GB) 0은 제한을 제거합니다. 이 값은 **Maximum file size to store (bytes)** 및 **Maximum file size for dynamic analysis testing (bytes)**보다 크거나 같아야 합니다.

Minimum file size for advanced file inspection and storage (bytes)	이러한 설정은 다음을 지정합니다.
	• 시스템이 다음 탐지기를 사용하여 검사할 수 있는 파일 크기:
	  • Spero 분석
	  • 샌드박싱 및 사전 분류
	  • 로컬 악성코드 분석/ClamAV
	  • 아카이브 검사
	• 시스템이 파일 규칙을 사용하여 저장할 수 있는 파일 크기.
		0 - 10485760(10MB)
		0은 파일 스토리지를 비활성화합니다.
		Maximum file size to store (bytes) 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.

Maximum file size for advanced file inspection and storage (bytes)		0 - 10485760(10MB) 0은 파일 스토리지를 비활성화합니다. **Minimum file size to store (bytes)**보다 크거가 같고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.

필드	설명	지침 및 제한 사항
Minimum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 AMP 클라우드에 제출할 수 있는 최소 파일 크기를 지정합니다.	0 -10485760(10MB) **Maximum file size for dynamic analysis testing (bytes)** 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다. 동적 분석을 위한 파일 크기는 파일 분석의 최소 및 최대 설정에서 정의된 한도 이내여야 합니다. 시스템은 제출할 수 있는 최소 파일 크기에 대한 업데이트를 AMP 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최소 크기가 현재 값보다 큰 경우, 현재 값이 새 최소값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.
Maximum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 AMP 클라우드에 제출할 수 있는 최대 파일 크기를 지정합니다.	0-10485760(10MB) **Minimum file size for dynamic analysis testing (bytes)** 보다 크거나 같고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다. 동적 분석을 위한 파일 크기는 파일 분석의 최소 및 최대 설정에서 정의된 한도 이내여야 합니다. 시스템은 제출할 수 있는 최대 파일 크기에 대한 업데이트를 AMP 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최대 크기가 현재 값보다 작은 경우, 현재 값이 새 최대값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.

파일 및 악성코드 탐지 성능 및 저장 조정

이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자 사용자여야 합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **Files and Malware Settings(**파일 및 악성코드 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘(**View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** 파일 및 악성코드 탐지 성능 및 저장 옵션, 37 페이지에 설명된 옵션을 설정합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

(선택 사항) AMP for Endpoints를 사용한 악성코드 방지

Cisco의 AMP for Endpoints는 Firepower 시스템에서 제공하는 악성 코드 방지를 보완하고 Firepower 구축과 통합할 수 있는 별도의 악성 코드 방지 제품입니다.

AMP for Endpoints는 개별 사용자의 엔드포인트(컴퓨터 및 모바일 디바이스)에서 경량 커넥터로 실행되어 지능형 악성 코드 발생, 지능형 지속 위협 공격(APT) 표적 공격을 발견, 파악, 차단하는 Cisco의 엔터프라이즈급 지능형 악성코드 방지 솔루션입니다.

AMP for Endpoints의 이점은 다음과 같습니다.

- 조직 전체에 맞춤형 악성코드 탐지 정책 및 프로파일을 구성하고 모든 사용자의 파일에서 신속한 전체 검사 수행
- 보기 히트 맵, 자세한 파일 정보, 네트워크 파일 전파 흔적 분석, 위협 근본 원인을 비롯한 악성코드 분석 수행
- 자동 격리, 격리되지 않은 실행 파일의 실행을 막는 애플리케이션 차단, 제외 목록을 비롯하여 아웃브레이크 제어의 다양한 측면 구성
- 맞춤형 보호를 생성하고, 그룹 정책을 기반으로 특정 애플리케이션의 실행을 차단하며, 맞춤형 허용 애플리케이션 목록을 생성
- AMP for Endpoints 관리 콘솔을 사용하여 악성 코드의 영향을 완화하도록 지원 관리 콘솔은 AMP for Endpoints 구축의 모든 부분을 제어하고 침투의 모든 단계를 관리할 수 있는 강력하고 유연한 웹 인터페이스를 제공합니다.

AMP for Endpoints에 대한 자세한 내용은 다음을 참조하십시오.

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html.
- AMP for Endpoints 관리 콘솔의 온라인 도움말.
- http://docs.amp.cisco.com에서 구할 수 있는 AMP for Endpoints 설명서.

악성코드 방지 비교: **Firepower** 대 **AMP for Endpoints**

표 ***5:*** 탐지 제품별 고급 악성코드 방지 차이점

기능	**Firepower** 악성코드 방지**(**악성코드 대응 **)**	**AMP for Endpoints**
파일 유형 탐지 및 차단 방법(파일 제어)	네트워크 트래픽에서 액세스 제어 및 파일 정책 사용	지원되지 않음
악성코드 탐지 및 차단 방법	네트워크 트래픽에서 액세스 제어 및 파일 정책 사용	개별 엔드포인트(최종 사용자 컴퓨터 및 모바일 디바이스)에서 AMP 클라우드와 통신하는 커넥터 사용
검사되는 네트워크 트래픽	매니지드 디바이스를 통과하는 트래픽	없음, 엔드포인트에 설치된 커넥터가 파일을 직접 검사
악성코드 인텔리전스 데이터 소스	AMP 클라우드(퍼블릭 또는 프라이빗)	AMP 클라우드(퍼블릭 또는 프라이빗)
악성코드 탐지 견고성	제한된 파일 유형	모든 파일 유형
악성코드 분석 선택	management center기반 및 AMP 클라우드 내 분석 기반	management center및 AMP for Endpoints 관리 콘솔의 추가 옵션
악성코드 완화	네트워크 트래픽에서 악성코드 차단, management center에서 위협 요소 제거 시작	AMP for Endpoints 기반 격리 및 침투 제어 옵션 management center에서 위협 요소 제거 시작
생성되는 이벤트	파일 이벤트, 캡처된 파일, 악성코드 이벤트, 회귀적 악성코드 이벤트	악성코드 이벤트
악성코드 이벤트의 정보	기본적인 악성코드 이벤트 정보 및 연결 데이터(IP 주소, 포트, 애플리케이션 프로토콜)	심층적인 악성코드 이벤트 정보, 연결 데이터 없음
네트워크 파일 경로	management center기반	management center 및 AMP for Endpoints 관리 콘솔에는 각각 네트워크 파일 경로 분석이 있습니다. 두 가지 모두 유용합니다.
필수 라이선스 또는 서브스크립션	파일 제어를 수행하는 데 필요한 라이선스 및 악성코드 대응	AMP for Endpoints 서브스크립션. AMP for Endpoints 데이터를 FMC로 가져오는 데는 라이선스가 필요하지 않습니다.

Firepower와 **AMP for Endpoints** 통합 정보

조직이 AMP for Endpoints를 구축한 경우, 필요하다면 해당 제품을 Firepower 구축에 통합할 수 있습니다.

AMP for Endpoints와의 통합에는 전용 Firepower 라이선스가 필요하지 않습니다.

Firepower와 AMP for Endpoints 통합의 이점

AMP for Endpoints 구축을 시스템과 통합하면 다음과 같은 이점이 있습니다.

- AMP for Endpoints에서 구성된 중앙 집중식 차단 애플리케이션 및 허용 애플리케이션 리스트는 속성 분석을 위해 Firepower에서 AMP 클라우드로 전송된 파일 SHA 결과를 결정할 수 있습니다.

  AMP for Endpoints의 중앙 집중식 파일 목록, 25 페이지의 내용을 참조하십시오.

- 시스템은 AMP for Endpoints가 탐지한 악성코드 이벤트를 Secure Firewall Management Center로 가져올 수 있으므로 사용자는 시스템에 의해 생성된 악성코드 이벤트와 함께 이러한 이벤트를 관리할 수 있습니다. 이러한 이벤트에 대해 가져온 데이터에는 스캔, 악성코드 탐지, 격리, 차단된 실행, 클라우드 리콜 및 management center가 모니터링하는 호스트에 대해 표시하는 IOC(Indications of Compromise)가 포함됩니다.
- AMP for Endpoints 콘솔에서 파일 경로 분석 및 기타 세부 정보를 볼 수 있습니다.

중요 Cisco AMP Private Cloud를 사용하는 경우, AMP for Endpoints 및 AMP Private Cloud, 42 페이지에서 제한 사항을 참조하십시오.

AMP for Endpoints 및 AMP Private Cloud

엔드포인트 커넥터에 대 한 모든 AMP 데이터를 해당 데이터를 전달 하는 프라이빗 클라우드를 보낼 네트워크에서 AMP 엔드포인트 데이터를 수집 하려면 Cisco AMP 프라이빗 클라우드를 구성 하는 경우는 Secure Firewall Management Center합니다. 프라이빗 클라우드는 외부 연결을 통해 엔드포인트 데이터를 공유하지 않습니다.

조직이 AMP 프라이빗 클라우드를 구축한 경우, AMP 클라우드와의 모든 연결은 모니터링되는 네트워크의 보안 및 개인 정보 보호를 위해 익명화된 프록시 역할을 하는 프라이빗 클라우드를 거칩니다. 여기에는 AMP for Endpoints 데이터 가져오기가 포함됩니다. 프라이빗 클라우드는 외부 연결을 통해 기존 엔드포인트 데이터를 공유하지 않습니다.

AMP 프라이빗 클라우드를 사용하는 경우, 다음 통합 기능은 제공되지 않습니다.

- AMP for Endpoints에 설정되어 있는 차단된 애플리케이션 및 허용된 애플리케이션 목록 사용 (이 목록은 파일을 차단하거나 허용하는 데 사용됩니다.)
- Firepower에서 생성된 악성코드 이벤트의 AMP for Endpoints에 대한 가시성

필요한 용량을 지원하기 위해 여러 프라이빗 클라우드를 구성할 수 있습니다.

Firepower 및 Secure Endpoint 통합

조직이 Cisco의 Secure Endpoint 제품을 구축한 경우, 해당 제품을 Firepower와 통합하여 Firepower와 AMP for Endpoints 통합의 이점, 42 페이지에 설명된 이점을 얻을 수 있습니다.

Secure Endpoint와 통합할 때 이미 악성코드 대응 (AMP for Firewall) 연결이 구성되어 있더라도 Secure Endpoint 연결을 구성해야 합니다. 여러 Secure Endpoint 클라우드 연결을 구성할 수 있습니다.

주의 다중 도메인 구축에서는, 특히 리프 도메인에 겹치는 IP 공간이 있다면 Secure Endpoint 연결은 리프 수준에서만 구성해야 합니다. 여러 서브도메인에 IP-MAC 주소 쌍이 동일한 호스트가 있는 경우, 시스템은 Secure Endpoint가 생성하는 악성코드 이벤트를 잘못된 리프 도메인에 저장하거나 IOC를 잘못된 호스트에 연결할 수 있습니다.

하지만 연결마다 별도의 Secure Endpoint 계정을 사용한다면 어떤 도메인 수준에서도 Secure Endpoint 연결을 구성할 수 있습니다. 예를 들어 MSSP의 각 클라이언트에는 자체 Secure Endpoint 구축이 있을 수 있습니다.

참고 성공적으로 등록되지 않은 Secure Endpoint 연결은 악성코드 대응 에 영향을 주지 않습니다.

시작하기 전에

- 이 작업을 수행하려면 관리자 사용자여야 합니다.
- 구축에서 Cisco AMP 프라이빗 클라우드를 사용하는 경우, AMP for Endpoints 및 AMP Private Cloud, 42 페이지에서 제한 사항을 참조하십시오.
- Secure Endpoint 가 설정되고 네트워크에서 정상적으로 작동해야 합니다.
- management center이 인터넷에 직접 액세스할 수 있어야 합니다.
- management center와 Secure Endpoint가 서로 통신할 수 있는지 확인합니다. Cisco Secure Firewall Management Center 관리 가이드의 보안, 인터넷 액세스 및 통신 포트 아래에 있는 항목을 참조하십시오.
- Secure Firewall Management Center를 공장 기본값으로 복원하거나 이전 버전으로 되돌린 후 AMP 클라우드에 연결하는 경우, AMP for Endpoints 관리 콘솔을 사용하여 이전 연결을 제거합니다.
- 이 절차 도중 Secure Endpoint 콘솔에 로그인하려면 Secure Endpoint 자격 증명이 필요합니다.

프로시저

단계 **1** **Integration(**통합**)** > **AMP** > **AMP Management(AMP** 관리**)**을(를) 선택합니다.

단계 **2** **Add AMP Cloud Connection(AMP** 클라우드 연결 추가**)**를 클릭합니다.

단계 **3** **Cloud Name(**클라우드 이름**)** 드롭다운 목록에서 사용할 클라우드를 선택합니다.

- Secure Firewall Management Center의 지리적 위치에 가장 가까운 AMP 클라우드를 선택합니다.

  APJC는 아시아/태평양/일본/중국입니다.

- AMP 프라이빗 클라우드(AMPv)의 경우, **Private Cloud(**프라이빗 클라우드**)**를 선택하고 Cisco AMP Private Cloud, 14 페이지에 설명된 대로 진행합니다.

단계 **4** 악성코드 대응 와 Secure Endpoint 모두에 클라우드를 사용하려면, **Use for AMP for Firepower(AMP for Firepower**에 사용**)** 확인란을 선택합니다.

악성코드 대응 (AMP for Firepower) 통신을 처리할 다른 클라우드를 구성한 경우에는 이 확인란 선택을 취소할 수 있지만 이것이 유일한 AMP 클라우드 연결이라면 선택을 취소할 수 없습니다.

다중 도메인 구축에서 이 확인란은 전역 도메인에만 표시됩니다. 각 Secure Firewall Management Center에는 하나의 악성코드 대응 연결만 있을 수 있습니다.

단계 **5** **Register(**등록**)**를 클릭합니다.

회전하는 상태 아이콘은 연결이 보류 중(예를 들어 Secure Firewall Management Center에서 연결을 구성한 후 Secure Endpoint 관리 콘솔을 사용하여 권한을 부여하기 전)임을 나타냅니다. **Denied(**거부됨**)** ( )은 클라우드가 연결을 거부했거나 다른 이유로 연결이 실패했음을 나타냅니다.

단계 **6** 계속해서 Secure Endpoint 관리 콘솔로 이동한다고 확인한 다음 관리 콘솔에 로그인합니다.

단계 **7** 관리 콘솔을 사용하여 AMP 클라우드가 Secure Endpoint 데이터를 management center에 전송하도록 권한을 부여합니다.

단계 **8** management center가 수신하는 데이터를 제한하려면 정보를 수신할 조직 내 특정 그룹을 선택합니다.

기본적으로 AMP 클라우드는 모든 그룹에 대해 데이터를 전송합니다. 그룹을 관리하려면 Secure Endpoint 관리 콘솔에서 **Management** > **Groups(**관리 그룹**)**를 선택합니다. 자세한 내용은 관리 콘솔 온라인 도움말을 참조하십시오.

단계 **9** 연결을 활성화하고 데이터 전송을 시작하려면 **Allow(**허용**)**를 클릭합니다.

Deny(거부**)**를 클릭하면 Secure Firewall Management Center로 되돌아가며, 여기서는 연결이 거부된 것으로 표시됩니다. Secure Endpoint 콘솔의 Applications(애플리케이션) 페이지에서 다른 곳으로 이동하고 연결을 거부하지도 허용하지도 않는 경우, 연결은 Secure Firewall Management Center의 웹 인터페이스에서 보류 중으로 표시됩니다. 이런 상황에서는 상태 모니터가 연결 실패를 알리지 않습니다. 나중에 AMP 클라우드에 연결하려면 실패하거나 보류 중인 연결을 삭제한 다음 다시 생성하십시오.

Secure Endpoint 연결의 등록이 완료되지 않아도 악성코드 대응 연결은 비활성화되지 않습니다.

단계 **10** 연결이 올바로 구성되어 있는지 확인하려면,

a) **Integration(**통합**)** > **AMP** > **AMP Management(AMP** 관리**)** 페이지의 **Cisco AMP Solution Type(Cisco AMP** 솔루션 유형**)** 열에서 **`AMP for Endpoints`**를 포함하는 클라우드 이름을 선택합니다.

b) 표시되는 AMP for Endpoints 콘솔 창에서 **Accounts(**계정**)** > **Applications(**애플리케이션**)**를 선택합니다.

c) management center가 목록에 있는지 확인합니다.

d) AMP for Endpoints 콘솔 창에서 **Manage(**관리**)** > **Computers(**컴퓨터**)**를 선택합니다.

e) management center가 목록에 있는지 확인합니다.

다음에 수행할 작업

- AMP for Endpoints 콘솔 창에서 필요에 따라 설정을 구성합니다. 예를 들어 관리 센터의 그룹 구성원 자격을 정의하고 정책을 할당합니다. 자세한 내용은 AMP for Endpoints 온라인 도움말이나 기타 설명서를 참조하십시오.
- 고가용성 컨피그레이션의 경우 Firepower Management Center의 액티브 및 스탠바이 인스턴스에서 독립적으로 AMP 클라우드 연결을 구성해야 합니다. 이러한 컨피그레이션은 동기화되지 않습니다.
- 기본 상태 정책은 성공적인 초기 연결 후 management center가 AMP for Endpoints 포털에 연결할 수 없거나 연결이 등록 취소된 경우, AMP 포털을 사용하여 사용자에게 경고합니다.

  System(시스템**) > Health(**상태**) > Policy(**정책**)** 아래에서 **AMP for Endpoints Status(AMP for Endpoints** 상태**)** 모니터가 활성화되어 있는지 확인합니다.