파일 및 악성코드 탐지 성능 및 저장 조정

다음 주제에서는 파일 및 악성코드 검사 성능과 저장을 구성하는 방법을 설명합니다.

- 파일 및 악성코드 탐지 성능 및 저장 옵션, 1 페이지
- 파일 및 악성코드 탐지 성능 및 저장 조정, 3 페이지

파일 및 악성코드 탐지 성능 및 저장 옵션

파일 크기를 늘리면 시스템의 성능에 영향을 미칠 수 있습니다.

표 *1:* 고급 액세스 제어 파일 및 ***AMP for Networks*** 옵션

필드	설명	지침 및 제한 사항
파일 유형 탐지 중에 검사되는 바이트 수 제한	파일 유형 탐지를 수행할 때 검사되는 바이트 수를 지정합니다.	0-4294967295(4GB) 0은 제한을 제거합니다. 기본값은 TCP 패킷의 최대 세그먼트 크기입니다(1460바이트). 대부분의 경우 시스템은 첫 번째 패킷을 사용하여 공용 파일 유형을 확인할 수 있습니다. ISO 파일을 탐지하려면 36870보다 큰 값을 입력합니다.
악성코드 차단을 위한 클라우드 조회가 다음보다 오래 걸리는 경우 파일 허용(초)	악성코드 클라우드 조회가 이루어지는 동안 **Block Malware**(악성코드 차단) 규칙과 일치하고 캐시된 속성이 없는 파일의 최종 바이트가 시스템에 유지되는 기간을 지정합니다. 시스템이 속성을 보유하지 못하고 시간이 경과하면, 파일은 통과됩니다. 사용할 수 없는 속성은 캐시되지 않습니다.	0-30초 지원 팀에 문의하지 않고 이 옵션을 0으로 설정하지 마십시오. Cisco는 연결 실패로 인한 트래픽 차단을 방지하기 위해 기본값을 사용할 것을 권장합니다.

필드	설명	지침 및 제한 사항
(바이트**)**보다 큰 파일의 **SHA-256** 해시 값을 계산하지 마십시오**.**	맞춤형 탐지 목록에 추가된 경우, 시스템이 특정 크기보다 큰 파일을 저장하거나 파일에 대한 클라우드 조회를 하거나 파일을 차단하지 않도록 합니다.	0-4294967295(4GB) 0은 제한을 제거합니다. 이 값은 **Maximum file size to store (bytes)** 및 **Maximum file size for dynamic analysis testing (bytes)**보다 크거나 같아야 합니다.
Minimum file size for advanced file inspection and storage (bytes)	이러한 설정은 다음을 지정합니다. • 시스템이 다음 탐지기를 사용하여 검사할 수 있는 파일 크기: • Spero 분석 • 샌드박싱 및 사전 분류 • 로컬 악성코드 분석/ClamAV • 아카이브 검사 • 시스템이 파일 규칙을 사용하여 저장할 수 있는 파일 크기.	0 - 10485760(10MB) 0은 파일 스토리지를 비활성화합니다. **Maximum file size to store (bytes)** 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.
Maximum file size for advanced file inspection and storage (bytes)		0 - 10485760(10MB) 0은 파일 스토리지를 비활성화합니다. **Minimum file size to store (bytes)**보다 크거가 같고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.
Minimum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 AMP 클라우드에 제출할 수 있는 최소 파일 크기를 지정합니다.	0 -10485760(10MB) **Maximum file size for dynamic analysis testing (bytes)** 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다. 동적 분석을 위한 파일 크기는 파일 분석의 최소 및 최대 설정에서 정의된 한도 이내여야 합니다. Firepower 5.x 버전을 실행하는 장치를 구축하는 경우, 시스템은 15360보다 작은 모든 값을 15360으로 변경합니다. 시스템은 제출할 수 있는 최소 파일 크기에 대한 업데이트를 AMP 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최소 크기가 현재 값보다 큰 경우, 현재 값이 새 최소값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.

파일 및 악성코드 탐지 성능 및 저장 조정

필드	설명	지침 및 제한 사항
Maximum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 AMP 클라우드에 제출할 수 있는 최대 파일 크기를 지정합니다.	0-10485760(10MB) **Minimum file size for dynamic analysis testing (bytes)** 보다 크거나 같고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다. 동적 분석을 위한 파일 크기는 파일 분석의 최소 및 최대 설정에서 정의된 한도 이내여야 합니다. Firepower 버전 5.x를 실행하는 장치를 구축하는 경우, 시스템은 2097152보다 큰 모든 값을 2097152로 변경합니다. 시스템은 제출할 수 있는 최대 파일 크기에 대한 업데이트를 AMP 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최대 크기가 현재 값보다 작은 경우, 현재 값이 새 최대값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.

파일 및 악성코드 탐지 성능 및 저장 조정

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

프로시저

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

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

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

단계 **3** 파일 및 악성코드 탐지 성능 및 저장 옵션, 1 페이지에 설명된 옵션을 설정합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

파일 및 악성코드 탐지 성능 및 저장 조정

관련 항목

Snort® 재시작 시나리오