FirePOWER Module for Network AMP 또는 File Control with ASDM을 구성합니다.

목차

소개

이 문서에서는 FirePOWER 모듈의 AMP(Network Advanced Malware Protection)/파일 액세스 제어 기능 및 ASDM(Adaptive Security Device Manager)을 사용하여 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA(Adaptive Security Appliance) 방화벽 및 ASDM에 대한 지식
- FirePOWER 어플라이언스 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 5.4.1 이상을 실행하는 ASA Firepower 모듈(ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)
- 소프트웨어 버전 6.0.0 이상을 실행하는 ASA Firepower 모듈(ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X)
- ASDM 7.5.1 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

악성 소프트웨어/악성코드는 다양한 방법으로 조직의 네트워크에 진입할 수 있습니다.이 악성 소프트웨어 및 악성코드의 영향을 식별하고 완화하기 위해 FirePOWER의 AMP 기능을 사용하여 네트워크에서 악성 소프트웨어 및 악성코드의 전송을 탐지하고 선택적으로 차단할 수 있습니다.

파일 제어 기능을 사용하면 파일 업로드 및 다운로드를 모니터링(탐지), 차단 또는 허용하도록 선택할 수 있습니다.예를 들어 사용자가 실행 파일의 다운로드를 차단하는 파일 정책을 구현할 수 있습니다.

Network AMP 기능을 사용하면 일반적으로 사용되는 프로토콜을 통해 모니터링할 파일 유형을 선택하고 SHA 256 해시, 파일의 메타데이터 또는 악성코드 분석을 위해 Cisco Security Intelligence Cloud로 파일 자체 사본을 전송할 수 있습니다.클라우드는 파일 분석을 기반으로 파일 해시의 속성을 정상 또는 악성으로 반환합니다.

파일 제어 및 AMP for Firepower는 파일 정책으로 구성하고 전체 액세스 제어 컨피그레이션의 일부로 사용할 수 있습니다.액세스 제어 규칙과 연결된 파일 정책은 규칙 조건을 충족하는 네트워크 트래픽을 검사합니다.

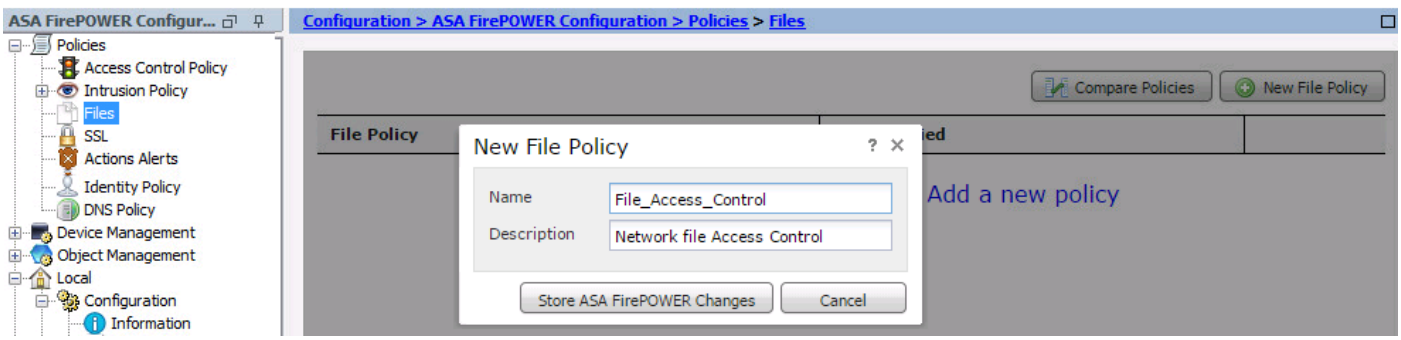
> **참고:**이 기능을 구성하려면 FirePOWER Module에 Protect/Control/Malware 라이센스가 있어야 합니다.라이센스를 확인하려면 Configuration(컨피그레이션) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > License(라이센스)를** 선택합니다.

파일 제어/네트워크 AMP용 파일 정책 구성

파일 액세스 제어 구성

ASDM에 로그인하고 Configuration(컨피그레이션) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Files(파일)를** 선택합니다. New **File Policy(새 파일 정책**) 대화 상자가 나타납니다.

새 정책에 대한 Name(이름) 및 Description(설명)(선택 사항)을 입력한 다음 Store **ASA Firepower Changes(ASA Firepower 변경 사항 저장)** 옵션**을** 클릭합니다.File Policy Rule 페이지가 나타납니다.



파일 정책에 규칙을 추가하려면 Add File Rule을 클릭합니다.파일 규칙을 사용하면 악성코드를 로깅, 차단 또는 스캔할 파일 유형을 세부적으로 제어할 수 있습니다.

애플리케이션 프로토콜: 애플리케이션 프로토콜을 **Any**(기본값) 또는 특정 프로토콜(HTTP, SMTP, IMAP, POP3, FTP, SMB)로 지정합니다.

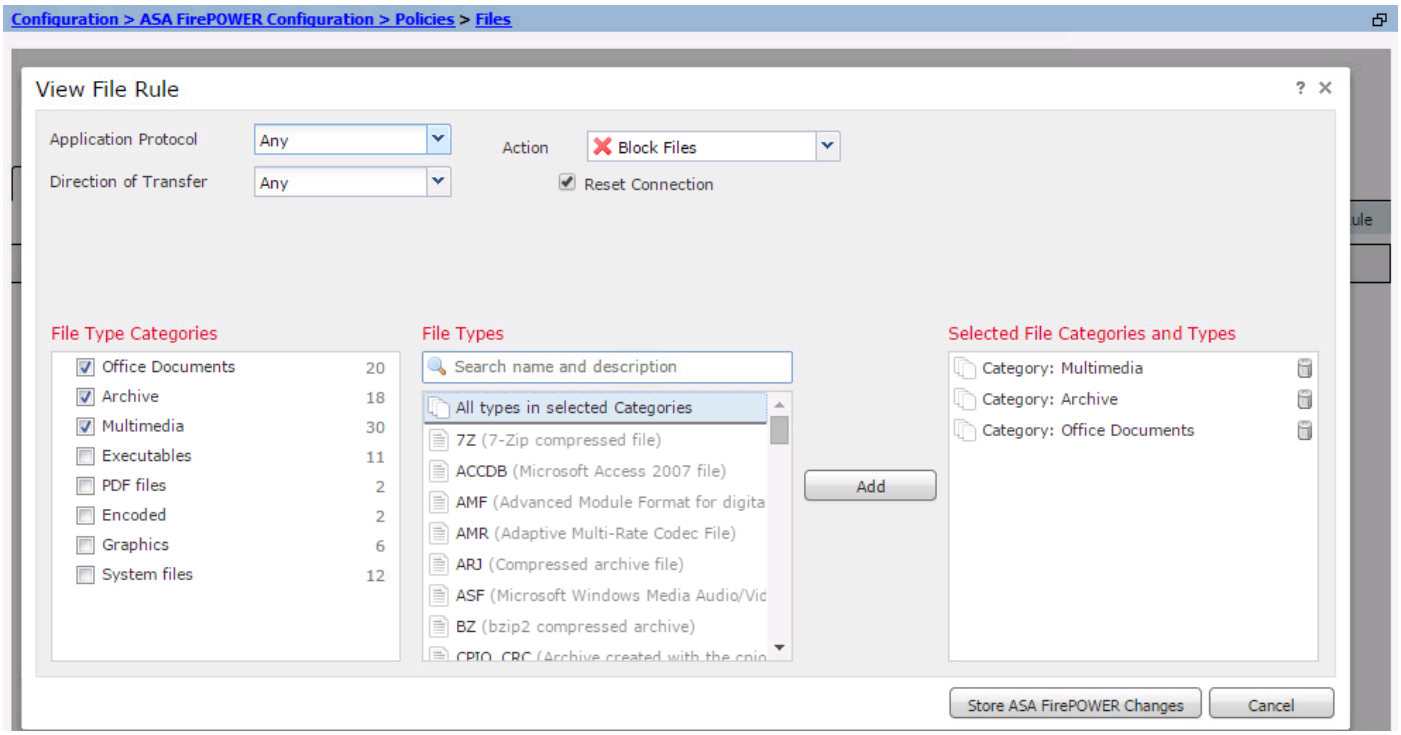
전송 방향:파일 전송 방향을 지정합니다.애플리케이션 프로토콜에 따라 Any 또는 Upload/Download일 수 있습니다.파일 업로드를 위해 파일 다운로드 및 프로토콜(HTTP, IMAP, POP3, FTP, SMB)에 대한 프로토콜(HTTP, SMTP, FTP, SMB)을 검사할 수 있습니다.사용자가 **파일을** 전송하거나 수신하는지 여부에 관계없이 여러 애플리케이션 프로토콜을 통해 파일을 탐지하려면 Any 옵션을 사용합니다.

작업:파일 액세스 제어 기능에 대한 작업을 지정합니다.작업은 **파일 탐지 또는 파일 차단**이 됩니다. **파일 탐지 작업은 이벤트를 생성하고 파일 차단 작업은** 이벤트를 생성하고 파일 전송을 차단합니다 .Block **Files** 작업을 사용하여 선택적으로 **Reset Connection을** 선택하여 연결을 종료할 수 있습니다 .

파일 유형 범주: 파일을 차단하거나 경고를 생성할 파일 유형 범주를 선택합니다.

파일 유형:파일 유형을 선택합니다.File Types(파일 유형) 옵션을 사용하면 특정 파일 유형을 선택할 수 있는 보다 세부적인 옵션이 제공됩니다.

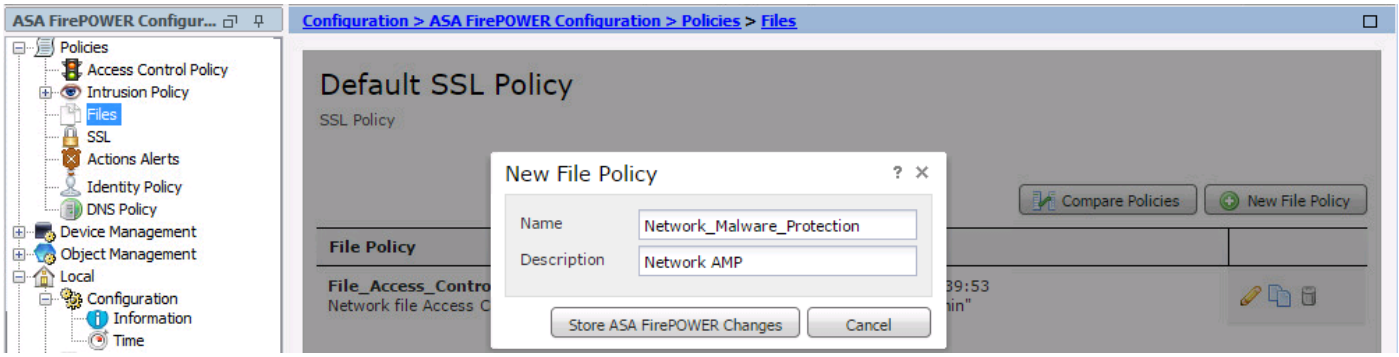
컨피그레이션**을** 저장하려면 Store ASA Firepower Changes 옵션을 선택합니다.



네트워크 악성코드 차단(네트워크 AMP) 구성

ASDM에 로그인하고 Configuration(컨피그레이션) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Files(파일)로 이동합니다.** File Policy 페이지가 나타납니다.이제 The New File Policy 대화 상자가 나타납니다.

새 정책에 대한 **Name** 및 선택적 **Description**을 입력한 다음 Store ASA Firepower Changes 옵션**을 클릭합니다**.File Policy Rules 페이지가 나타납니다.



파일 정책에 규칙을 추가하려면 **Add File Rule** 옵션을 클릭합니다.파일 규칙을 사용하면 악성코드를 로깅, 차단 또는 스캔할 파일 유형을 세부적으로 제어할 수 있습니다.

애플리케이션 프로토콜: Any(기본값) 또는 특정 프로토콜(HTTP, SMTP, IMAP, POP3, FTP, SMB)을 지정합니다.

전송 방향:파일 전송 방향을 지정합니다.애플리케이션 프로토콜에 따라 Any 또는 Upload/Download일 수 있습니다.파일 업로드를 위해 프로토콜(HTTP, IMAP, POP3, FTP, SMB)을 파일 다운로드 및 프로토콜(HTTP, SMTP, FTP, SMB)에 검사할 수 있습니다.파일을 보내거나 받는 사용자와 상관없이 여러 애플리케이션 프로토콜을 통해 파일을 탐지하려면 Any 옵션을 사용합니다.

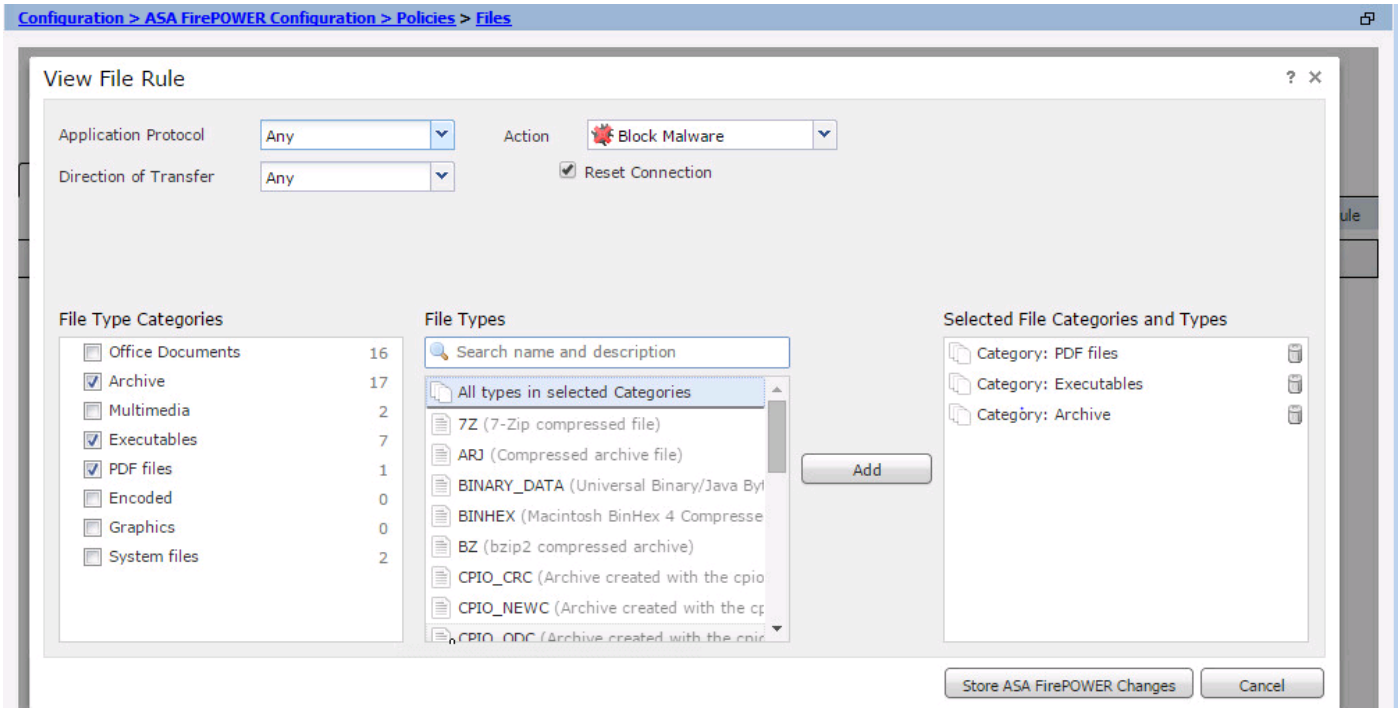
작업:네트워크 악성코드 차단 기능의 경우 작업은 **악성코드 클라우드 조회** 또는 **악성코드 차단이** 됩니다. 조치 **악성코드 클라우드 조회**는 이벤트만 생성하는 반면, 조치 **차단 악성코드는** 이벤트를 생성하고 악성코드 파일 전송을 차단합니다.

> **참고:Malware Cloud Lookup 및 Block Malware** 규칙을 사용하면 Firepower에서 SHA-256 해시를 계산하고 이를 클라우드 조회 프로세스에 전송하여 네트워크를 통과하는 파일에 악성코드가 포함되어 있는지 확인할 수 있습니다.

파일 유형 범주: 특정 파일 범주를 선택합니다.

파일 유형: 특정 **파일 유형**을 선택하여 보다 세분화된 파일 유형을 선택합니다.

Store **ASA Firepower Changes(ASA Firepower 변경 사항 저장**) 옵션을 선택하여 컨피그레이션을 저장합니다.

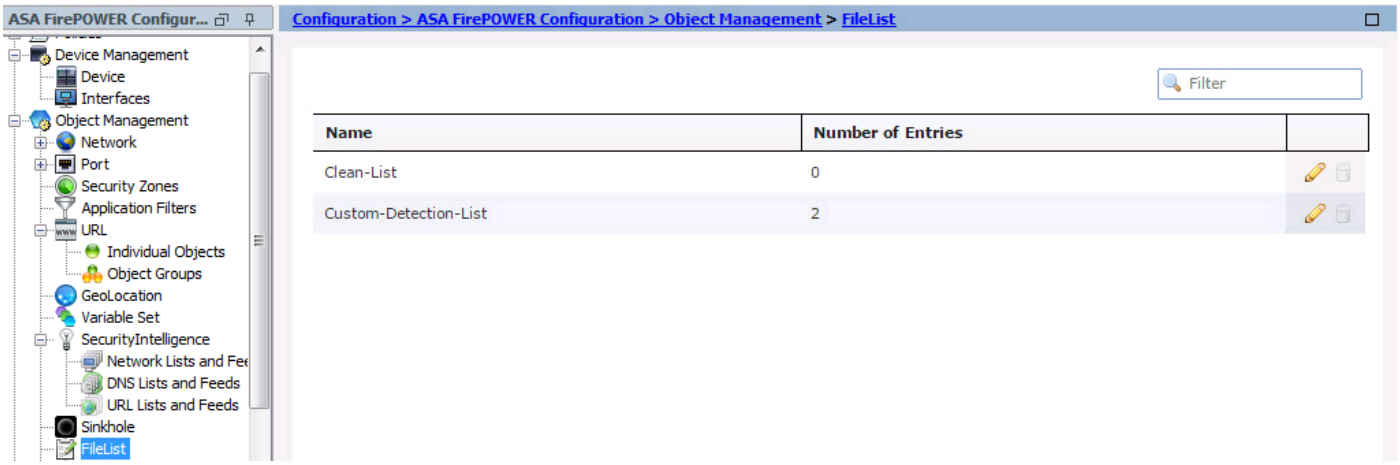


참고:파일 정책은 다음 규칙 작업 순서의 파일을 처리합니다.차단은 악성코드 검사보다 우선하며, 이는 단순한 탐지 및 로깅보다 우선합니다.

네트워크 기반 AMP(Advanced Malware Protection)를 구성하고 Cisco Cloud가 파일의 속성을 잘못 탐지하면 SHA-256 해시 값을 사용하여 파일을 파일 목록에 추가하여 향후 파일 속성을 더 효과적으로 탐지할 수 있습니다.파일 목록 유형에 따라 다음을 수행할 수 있습니다.

- 클라우드에서 정상 성향을 할당한 것처럼 파일을 처리하려면 파일을 정상 목록에 추가합니다.
- 클라우드에서 악성코드 성향을 할당한 것처럼 파일을 처리하려면 파일을 사용자 지정 목록에 추가합니다.

이를 구성하려면 Configuration(컨피그레이션) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Object Management(개체 관리) > File List(파일 목록)로 이동하여** 목록을 편집하여 SHA-256을 추가합니다.



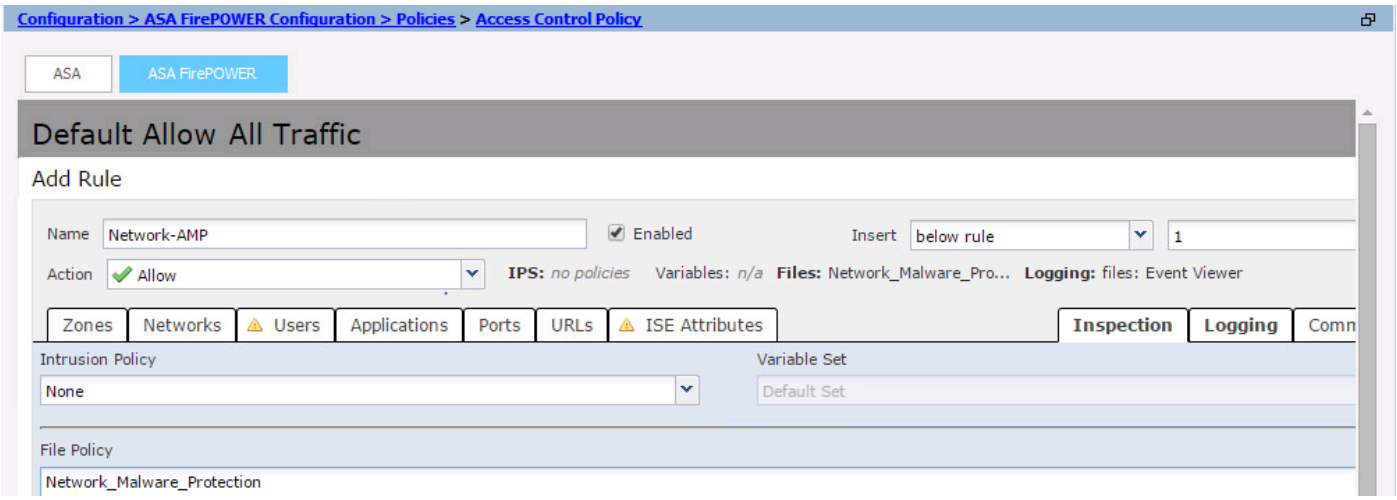
파일 정책에 대한 액세스 제어 정책 구성

Configuration(**구성) > ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Access Control Policy(액세스 제어 정책)로 이동하고** 새 **액세스 규칙**을 생성하거나 이 이미지에 표시된 대로 기존 **액세스 규칙을** 수정합니다.

파일 정책을 구성하려면 Action(작업)이 **Allow(허용)**여야 합니다.Inspection(**검사**) 탭으로 이동하고 드롭다운 메뉴에서 File Policy(파일 정책)를 선택합니다.

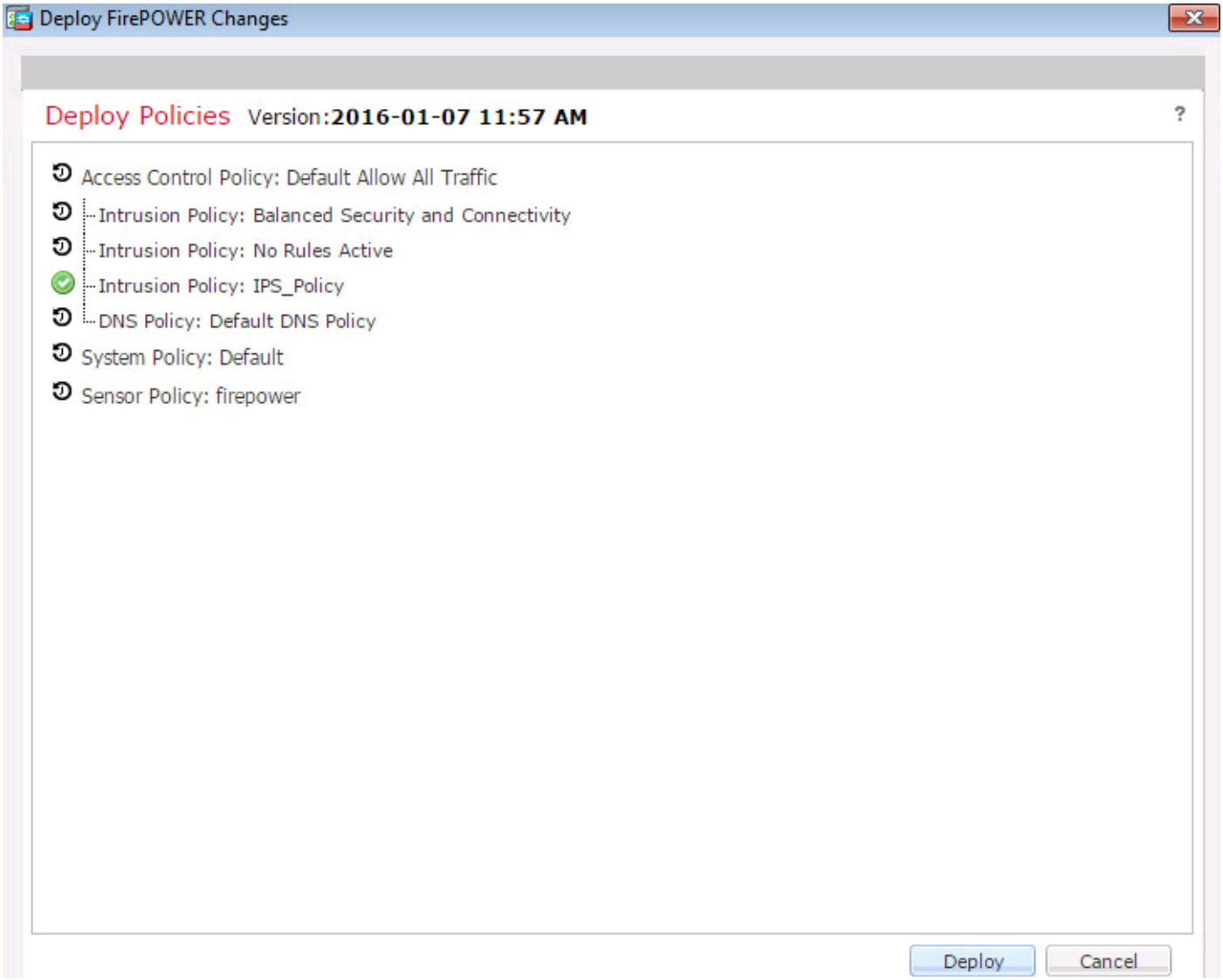
로깅을 활성화하려면 logging 옵션으로 이동하고 적절한 로깅 옵션 및 **Log Files** 옵션**을** 선택합니다 .Save**/Add** 버튼을 클릭하여 컨피그레이션을 저장합니다.

Store **ASA Firepower Changes** 옵션을 선택하여 AC 정책 변경 사항을 저장합니다.



액세스 제어 정책 구축

ASDM의 **Deploy** 옵션으로 이동하고 드롭다운 메뉴에서 Deploy Firepower Change 옵션을 선택합니다.Deploy(구축) 옵션을 클릭하여 변경 사항을 구축합니다.

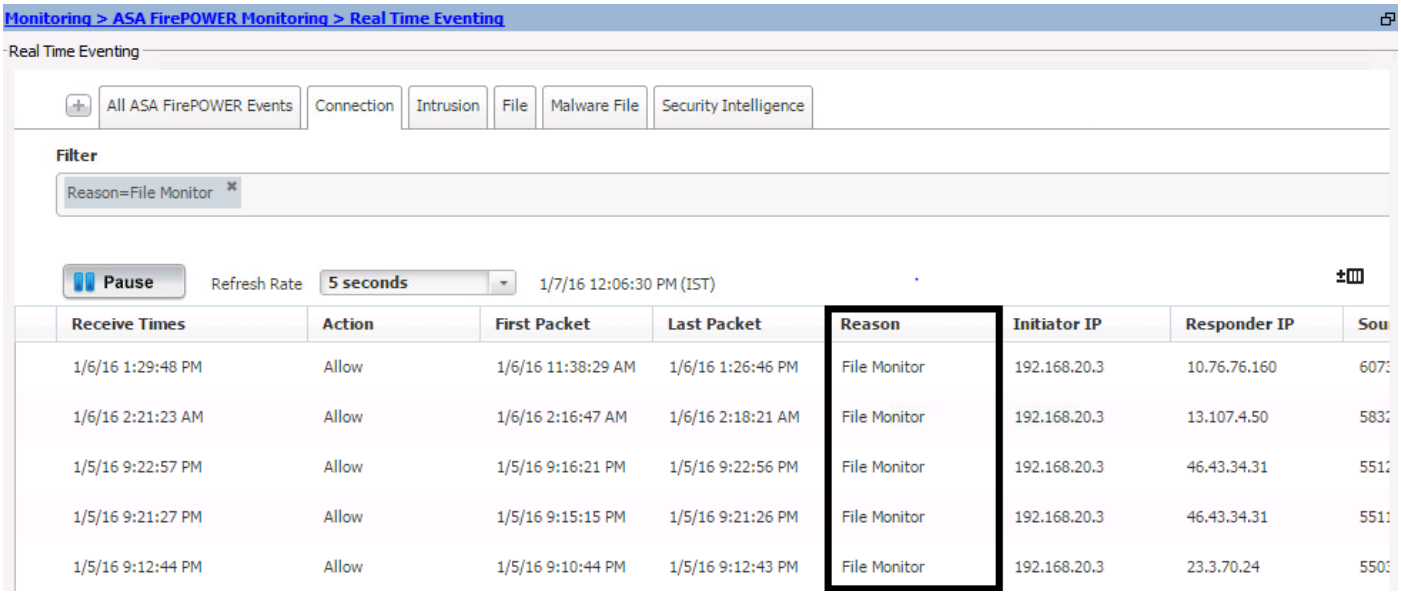


Monitoring(**모니터링**) > **ASA Firepower Monitoring(ASA Firepower 모니터링)** > **Task Status(작업 상태)로 이동합니다.** 구성 변경 사항을 적용하려면 작업을 완료해야 합니다.

> **참고:**버전 5.4.x에서 센서에 액세스 정책을 적용하려면 Apply **ASA FirePOWER Changes(ASA FirePOWER 변경 사항 적용)를 클릭해야** 합니다.

파일 정책 이벤트에 대한 연결 모니터링

파일 정책과 관련된 Firepower Module에서 생성된 이벤트를 보려면 Monitoring(모니터링) > **ASA Firepower Monitoring(ASA Firepower 모니터링)** > **Real Time Eventing(실시간 이벤트)으로 이동합니다.**



다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

파일 정책이 프로토콜/방향/작업/파일 유형으로 올바르게 구성되었는지 확인합니다. 액세스 규칙에 올바른 파일 정책이 포함되어 있는지 확인합니다.

액세스 제어 정책 배포가 성공적으로 완료되었는지 확인합니다.

연결 이벤트 및 파일 이벤트(**Monitoring(모니터링) > ASA Firepower Monitoring(ASA Firepower 모니터링) > Real Time Eventing**)를 모니터링하여 트래픽 흐름이 올바른 규칙에 도달하는지 확인합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems