Configureer de FirePOWER-module voor AMP van het netwerk of bestandscontrole met ASDM.

Inhoud

Inleiding

In dit document wordt de functionaliteit voor Network Advanced Malware Protection (AMP)/bestandstoegang van de FirePOWER-module beschreven, evenals de methode om deze te configureren met Adaptieve Security Devices Manager (ASDM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van de adaptieve security applicatie (ASA) firewall en ASDM.
- Kennis van FirePOWER-apparaat.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) software versie 5.4.1 en hoger.
- ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5555-X) die software versie 6.0.0 en hoger uitvoeren.
- ASDM 7.5.1 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Kwaadaardige software/malware kan op meerdere manieren in het netwerk van een organisatie worden ingevoerd. Om de effecten van deze kwaadaardige software en malware te identificeren en te verzachten, kunnen de AMP-functies van FirePOWER worden gebruikt om de transmissie van kwaadaardige software en malware in het netwerk te detecteren en optioneel te blokkeren.

Met functionaliteit voor bestandscontrole kunt u ervoor kiezen om bestanden te controleren (detecteren), te blokkeren of de overdracht van het uploaden en downloaden van bestanden toe te staan. Een bestandsbeleid kan bijvoorbeeld worden uitgevoerd waardoor het downloaden van uitvoerbare bestanden door de gebruiker wordt geblokkeerd.

Dankzij de AMP-functie van het netwerk kunt u bestandstypen selecteren die u wilt bewaken via algemeen gebruikte protocollen en SHA 256-hashes, metagegevens uit de bestanden of zelfs kopieën van de bestanden zelf naar de Cisco Security Intelligence Cloud sturen voor malware analyse. Cloud retourneert dispositie voor bestandshashes als schoon of kwaadaardig, gebaseerd op bestandsanalyse.

Bestandscontrole en AMP voor Firepower kunnen worden ingesteld als bestandsbeleid en worden gebruikt als onderdeel van de configuratie van uw algemene toegangscontrole. Bestandsbeleid dat is gekoppeld aan toegangscontroleregels, inspecteert netwerkverkeer dat voldoet aan regelvoorwaarden.

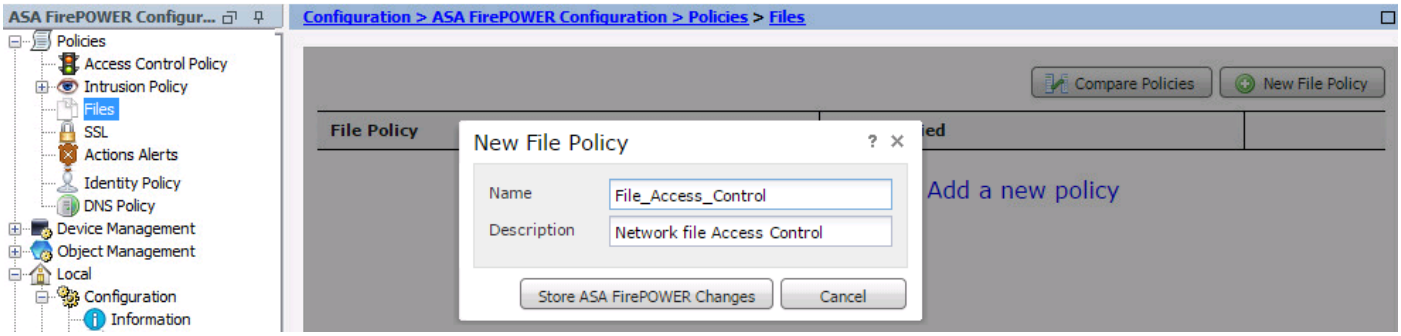
> Opmerking: Zorg ervoor dat de FirePOWER-module een Protect/Control/Malware-licentie heeft om deze functie te configureren. Selecteer **Configuration > ASA FirePOWER Configuration > Licentie** om de licenties te controleren.

Configuratie van het bestandsbeleid voor IP-beheer/netwerk

Bestandstoegangscontrole instellen

Meld u aan bij ASDM en kies **Configuratie > ASA Firepower Configuration > Policy > Files.** Het dialoogvenster **Nieuw bestandsbeleid** verschijnt.

Voer een naam en optionele beschrijving in voor uw nieuwe beleid en klik vervolgens op **Store ASA Firepower Change** optie. De pagina Bestandsbeleid wordt weergegeven.



Klik op **Bestandsregel toevoegen** om een regel aan het bestandsbeleid toe te voegen. De bestandregel geeft u de granulaire controle over bestandstypen die u wilt loggen, blokkeren of scannen voor malware.

Toepassingsprotocol: Specificeer het toepassingsprotocol als **Any** (standaard) of het specifieke protocol (HTTP, MTP, IMAP3, POP3, FTP, MKB).

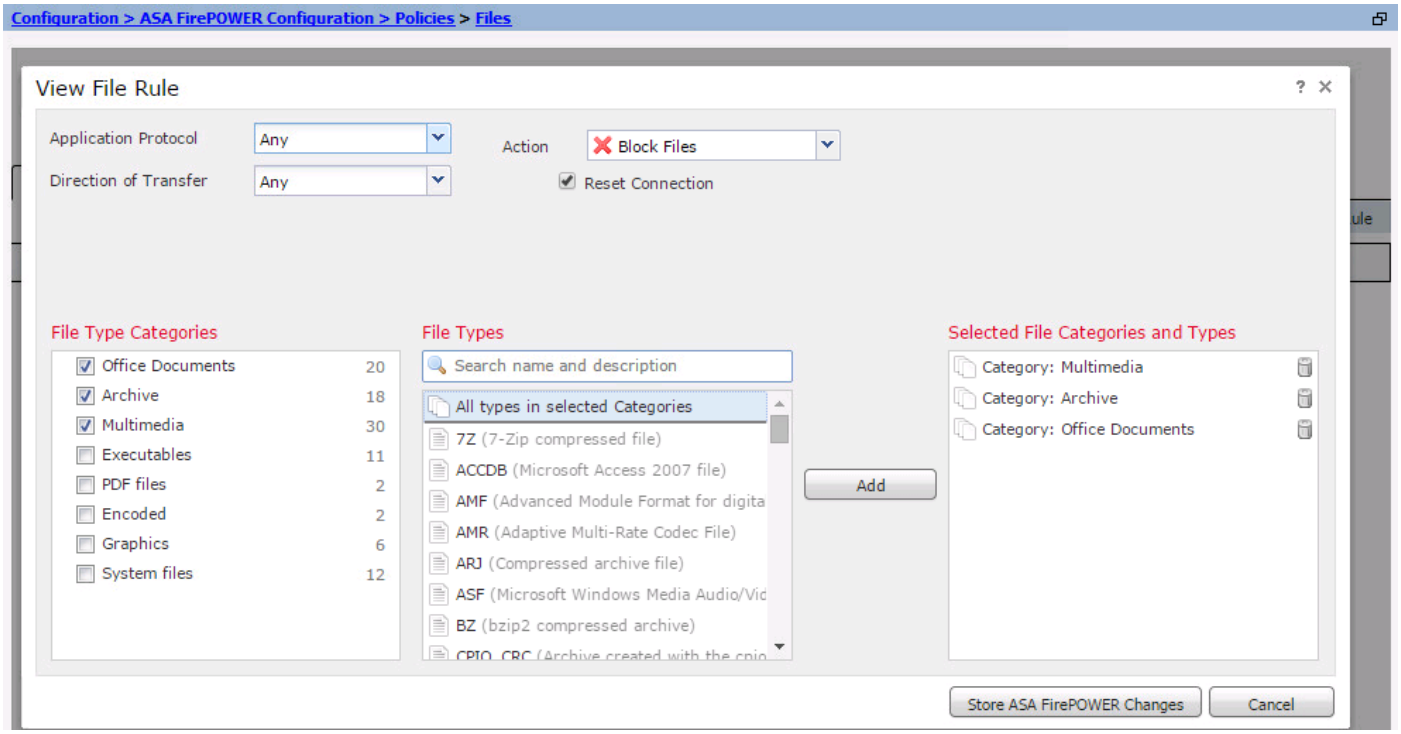
Richting van overdracht: Specificeer de richting van bestandsoverdracht. Het kan zijn, of Upload/Download zijn op basis van het Toepassingsprotocol. U kunt het protocol (HTTP, IMAP, POP3, FTP, MKB) inspecteren voor het downloaden van bestanden en het protocol (HTTP, MTP, FTP, MKB) voor het uploaden van bestanden. Gebruik de optie Any optie om bestanden te detecteren via meerdere toepassingsprotocollen, ongeacht of gebruikers het bestand verzenden of ontvangen.

Actie: Specificeer de actie voor de functie Bestandstoegangscontrole. Handeling moet **Bestanden** detecteren of **Bestanden blokkeren. Detect File** action genereert de gebeurtenis en **Block Files** actie genereert de gebeurtenis en blokkeert de bestandsoverdracht. Met de actie **Block Files** kunt u optioneel **Reset Connection** selecteren om de verbinding te beëindigen.

Categorieën bestandstypen: selecteer de categorieën bestandstype waarvoor u het bestand wilt blokkeren of de waarschuwing wilt genereren.

Bestandstypen: Selecteer de bestandstypen. De optie Bestandstypen biedt een meer gedetailleerde optie om het specifieke bestandstype te kiezen.

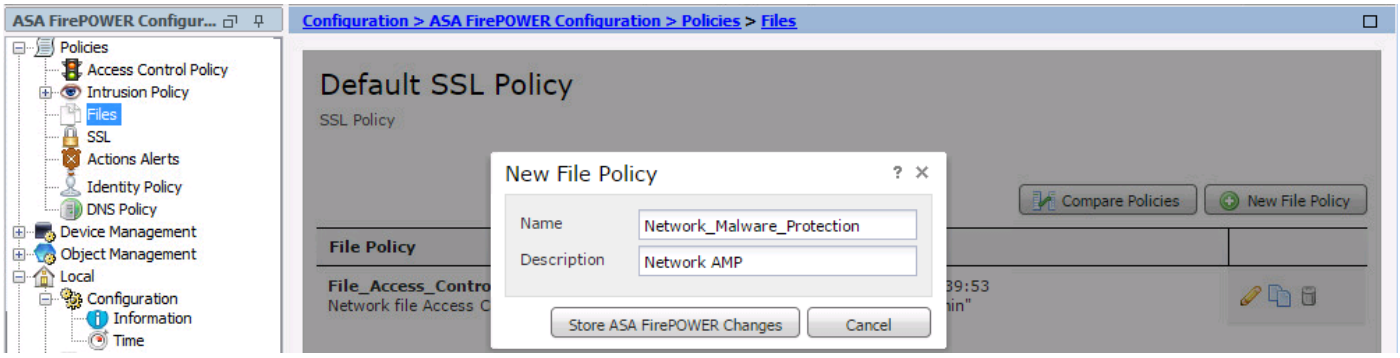
Kies **de** optie **ASA FirePOWER Verandert** om de configuratie op te slaan.



Network Malware Protection configureren

Meld u aan bij ASDM en navigeer naar **Configuration > ASA Firepower Configuration > Policy > Files.** De pagina Bestandsbeleid wordt weergegeven. Klik nu op het dialoogvenster Nieuw bestandsbeleid.

Voer een **naam** en optionele **Description in** voor uw nieuwe beleid en klik vervolgens op de optie **Store ASA Firepower Wijzigingen**. De pagina Bestandsbeleidsregels verschijnt.



Klik op de optie **Bestandsregel toevoegen** om een regel aan bestandsbeleid toe te voegen. Bestandsregel geeft u de granulaire controle over bestandstypen die u wilt loggen, blokkeren of scannen voor malware.

Toepassingsprotocol: Specificeer of om het even welk (standaard) of specifiek protocol (HTTP, MTP, IMAP3, POP3, FTP, MKB)

Richting van overdracht: Specificeer de richting van bestandsoverdracht. Het kan zijn, of Upload/ Download zijn op basis van het Toepassingsprotocol. U kunt het protocol (HTTP, IMAP, POP3, FTP, MKB) inspecteren voor het downloaden van bestanden en het protocol (HTTP, mtp, FTP, MKB) voor het uploaden van bestanden. Gebruik **een** optie om bestanden te detecteren via meerdere toepassingsprotocollen, ongeacht of gebruikers het bestand verzenden of ontvangen.

Actie: Voor de functionaliteit voor Network Malware Protection is Action **Malware Cloud** Cloud

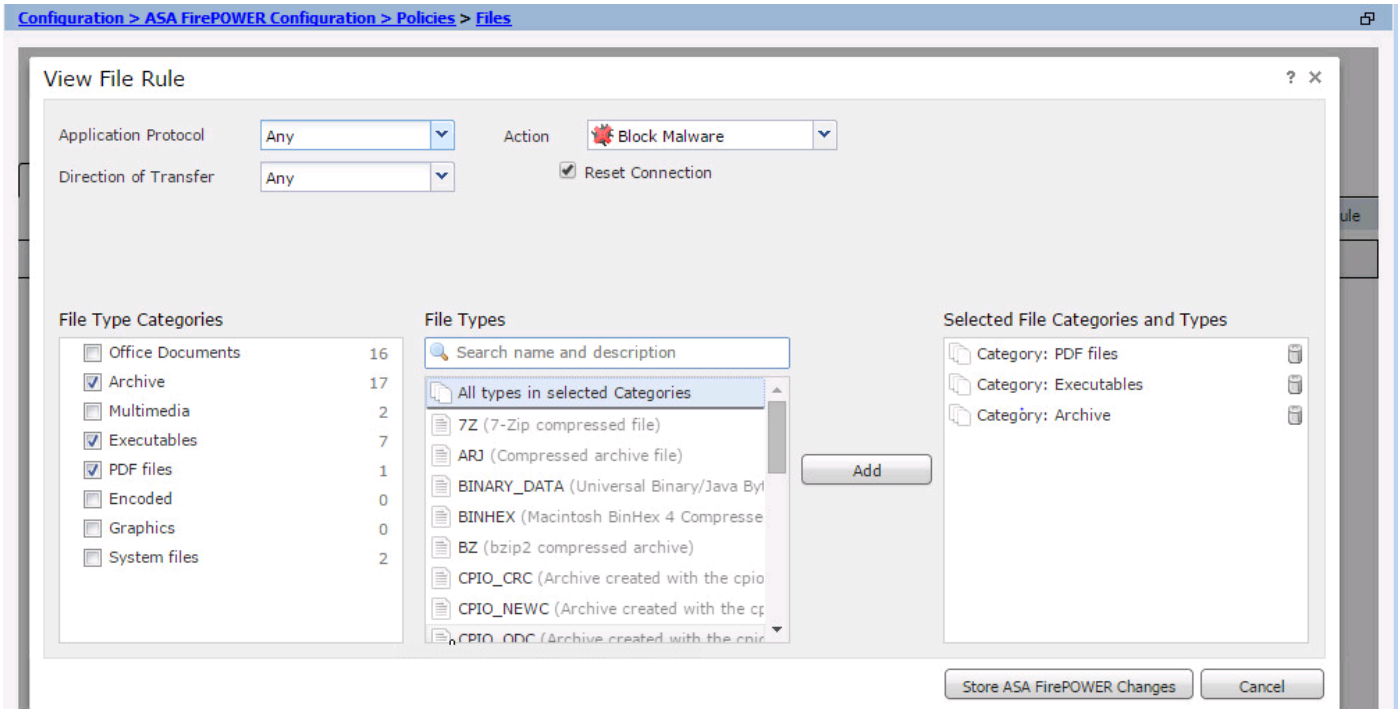
Cloud or **Block Malware**. Action **Malware Cloud Upload** genereert slechts een gebeurtenis terwijl Action **Block Malware** de gebeurtenis genereert en de malware bestandsoverdracht blokkeert.

> Opmerking: Met **de** regels **van de Cloud en de** Blok van **Malware** staat de Firepower toe om de SHA-256 hash te berekenen en het voor het proces van de cloud te verzenden om te bepalen of bestanden die het netwerk oversteken malware bevatten.

Categorieën bestandstypen: selecteer de specifieke bestandscategorieën.

Bestandstypen: Selecteer de specifieke **bestandstypen** voor meer gedetailleerde bestanden.

Kies optie **ASA Firepower Wijzigingen opslaan** om de configuratie op te slaan.

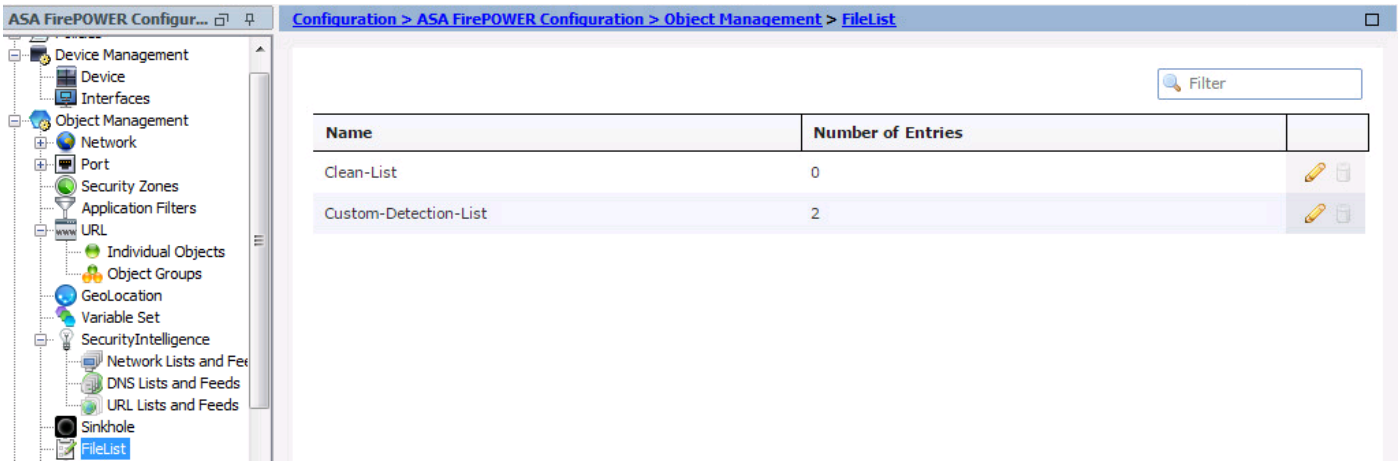


> Opmerking: Bestandsbeleid behandelt bestanden in de volgende regel-actieregel: Blokkeren heeft voorrang op malware inspectie, wat voorrang heeft op eenvoudige detectie en vastlegging.

Als u op netwerk gebaseerde Advanced Malware Protection (AMP) configureren en Cisco Cloud de verwerking van een bestand onjuist detecteert, kunt u het bestand aan een lijst toevoegen met een SHA-256-hashwaarde om de bestandsindeling in de toekomst te verbeteren. Afhankelijk van het type bestandslijst kunt u:

- Als u een bestand wilt behandelen alsof de cloud een schone locatie heeft toegewezen, voegt u het bestand toe aan de lijst met regels.
- Als u een bestand wilt behandelen alsof de cloud een slechte dispositie heeft toegewezen, voegt u het bestand toe aan de aangepaste lijst.

Om dit te configureren navigeer u naar **Configuratie > ASA FirePOWER Configuration > Objectbeheer > Bestandslijst** en bewerkt de lijst om SHA-256 toe te voegen.



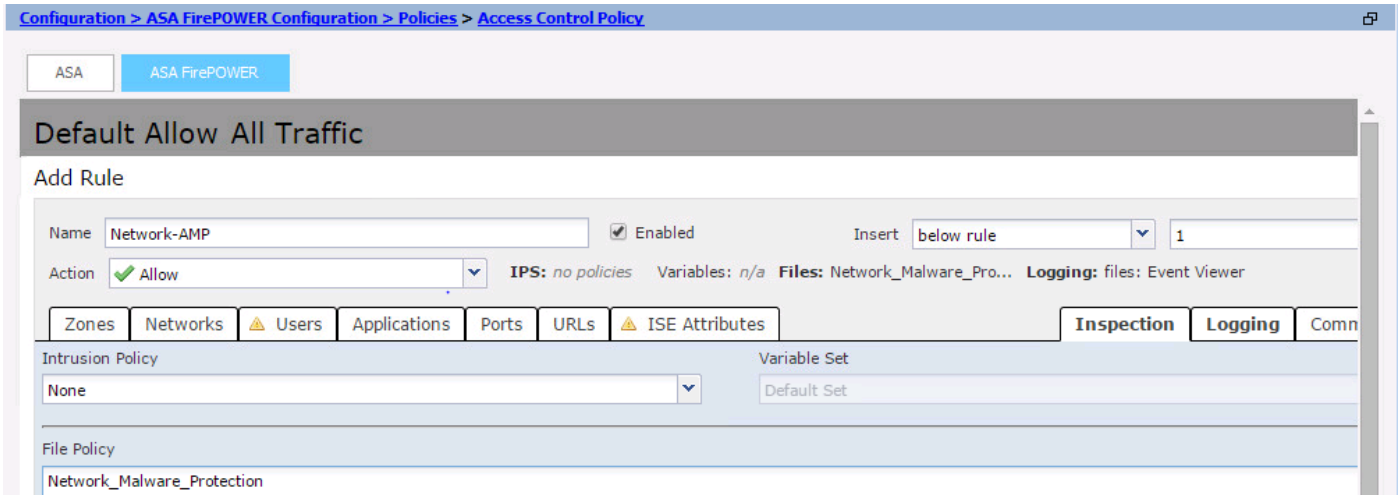
Toegangsbeheerbeleid voor bestanden configureren

Navigeer naar **Configuratie > ASA Firepower Configuration > Policy > Access Control Policy,** en maak een nieuwe **toegangsregel** of bewerk bestaande **toegangsregel,** zoals in deze afbeelding wordt getoond.

Om het bestandsbeleid aan te passen, dient actie **toegestaan** te zijn. Navigeer naar het tabblad **Inspectie** en selecteer het **Bestandsbeleid** in het vervolgkeuzemenu.

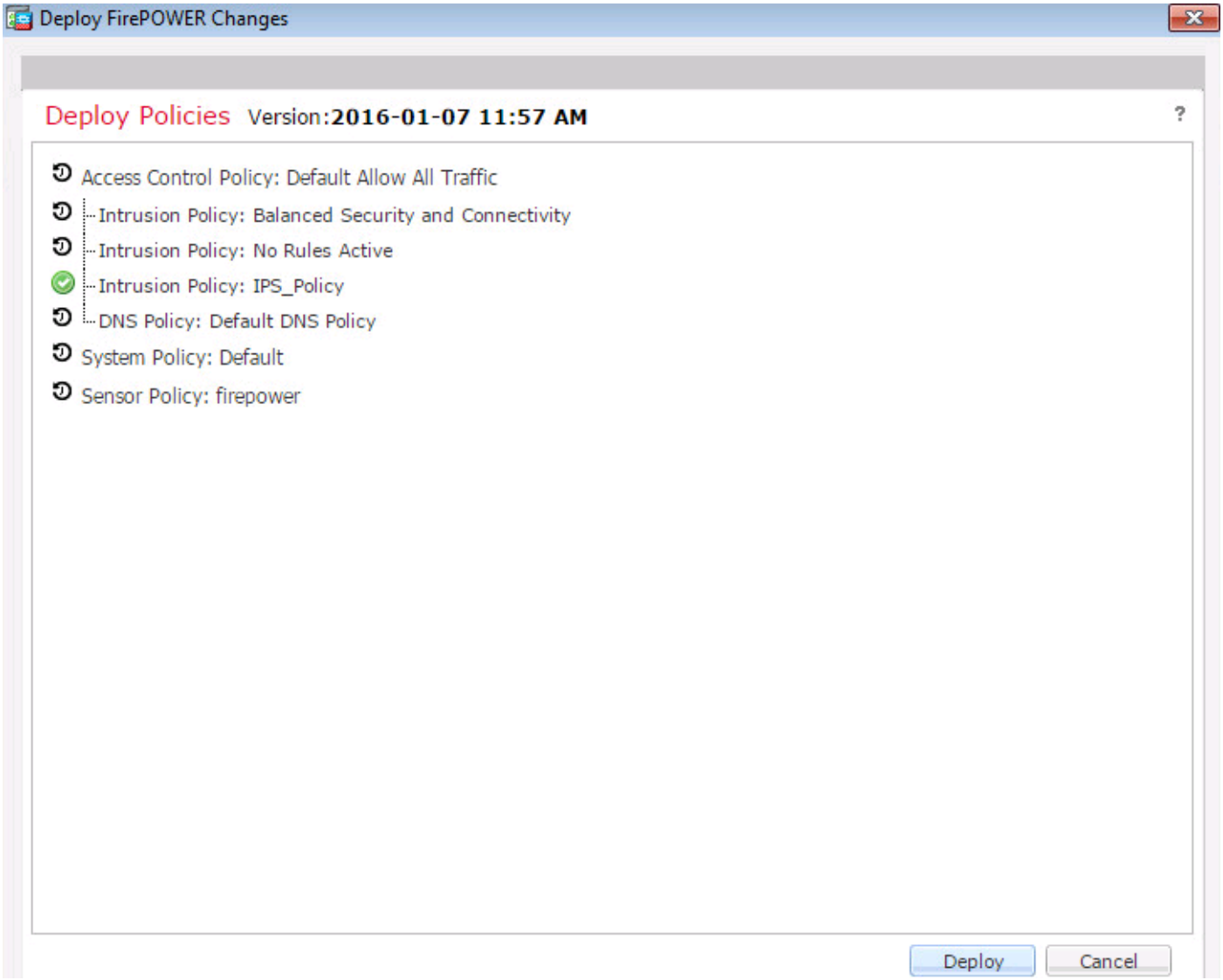
Om loggen mogelijk te maken, navigeer de optie **loggen** en selecteer de gewenste logoptie en optie **Log bestanden**. Klik op de knop **Opslaan/toevoegen** om de configuratie op te slaan.

Kies optie **ASA Firepower Wijzigingen opslaan** om de wijzigingen in het AC-beleid op te slaan.



Toegangsbeheerbeleid implementeren

Navigeer naar de **optie** van ASDM **implementeren** en kies de optie **Firepower Change** implementeren in het uitrolmenu. Klik op de optie Importeren om de wijzigingen in te voeren.

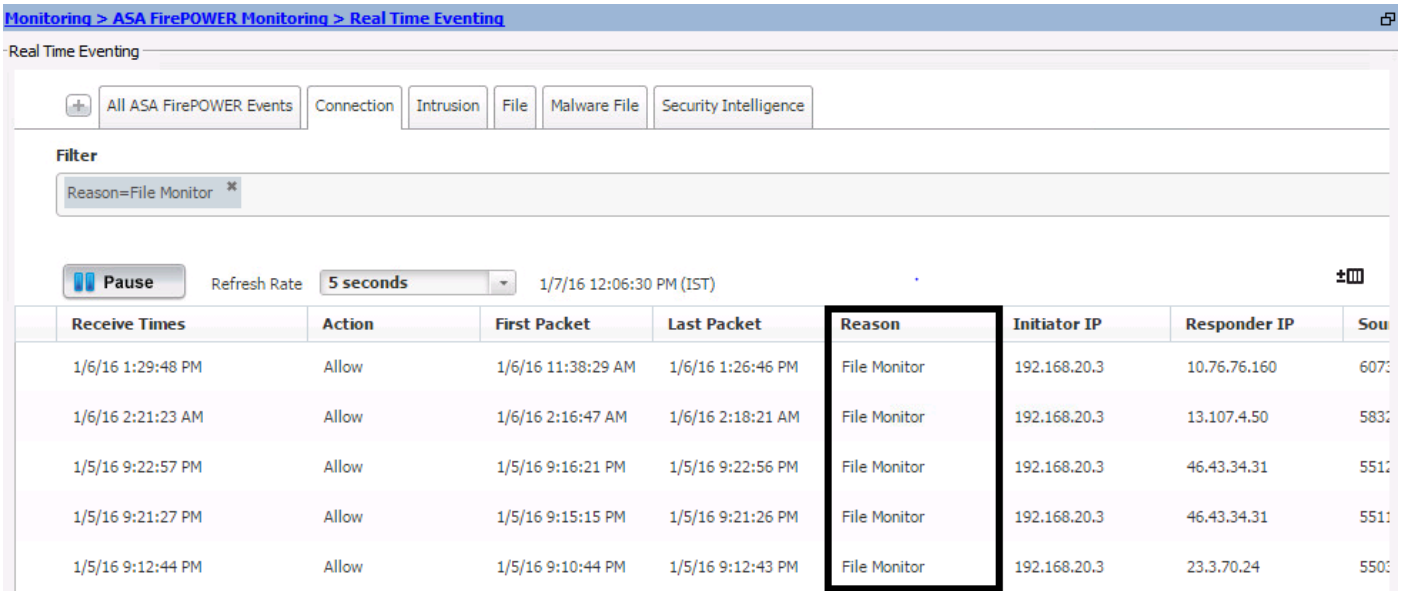


Navigeer naar **bewaking > ASA FirePOWER Monitoring > Task Status.** Zorg ervoor dat deze taak voltooid moet zijn om de configuratie verandering toe te passen.

> Opmerking: In versie 5.4.x moet u om het toegangsbeleid op de sensor toe te passen **klikken** om **ASA FirePOWER Wijzigingen toepassen.**

Monitorverbinding voor gebeurtenissen in het bestandsbeleid

Om de gebeurtenissen te zien die door de Firepower Module met betrekking tot bestandsbeleid worden gegenereerd, navigeer naar **bewaking > ASA Firepower Monitoring > Real Time Eventing.**



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Zorg ervoor dat het bestandsbeleid correct is geconfigureerd met protocol/richting/actie/bestandstypen. Zorg ervoor dat het juiste bestandsbeleid in toegangsregels is opgenomen.

Zorg ervoor dat de implementatie van het toegangsbeheerbeleid is voltooid.

Controleer de Connection gebeurtenissen & File events (**bewaking > ASA FirePOWER-bewaking > Real Time Eventing**) om te controleren of de verkeersstroom de juiste regel heeft of niet.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems