# IP-Zwarte Lijst configureren met behulp van Cisco Security Intelligence via ASDM (On-Box Management)

## Inhoud



## Inleiding

Dit document beschrijft de reputatie van Cisco Security Intelligence/IP-adres en de configuratie van IP-zwarte lijst (blokkering) bij het gebruik van aangepaste/automatische feed van een IP-adres met een lage reputatie.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van ASA (adaptieve security applicatie) firewall, ASDM (adaptieve security applicatie Manager)
- kennis van FirePOWER-apparaat

Opmerking: Beveiligingsinformatie-filtering vereist een beschermingslicentie.

### Gebruikte componenten

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

- ASA FirePOWER-modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) met software versie 5.4.1 en hoger

- ASA FirePOWER-module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) met software versie 6.0.0 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

Cisco Security Intelligence bestaat uit meerdere regelmatig bijgewerkte verzamelingen IP-adressen die door het Cisco TALOS-team een slechte reputatie blijken te hebben. Het team van Cisco TALOS bepaalt de lage reputatie als om het even welke kwaadwillige activiteit van die IP adressen zoals spams, malware, phishing aanvallen enz. wordt voortgebracht.

Cisco IP Security Intelligence-feed volgt de database van aanvallers, Bogon, Bots, CnC, Dga, ExploitKit, Malware, Open_proxy, Open_relais, Phishing, Response, Spam, Suspicious. De Firepower module biedt de optie om de aangepaste feed van een laag IP-adres te maken.

# Overzicht van de veiligheidsinformatieinvoer

Hier is meer informatie over het type IP-adresverzamelingen die als verschillende categorieën in de Security Intelligence kunnen worden geclassificeerd.

**Aanvallers: Verzameling van IP-adressen die voortdurend op kwetsbaarheden scannen of proberen andere systemen te exploiteren.**

**Malware: Een verzameling IP-adressen die malware proberen te propageren of die actief iedereen aanvallen die hen bezoekt.**

**Phishing: Een verzameling hosts die actief proberen de eindgebruikers te belasten met het invoeren van vertrouwelijke informatie zoals gebruikersnamen en wachtwoorden.**

**Spam:** Een verzameling hosts die is geïdentificeerd als de bron van het verzenden van spam-e-mailberichten.

**Bots:** Een verzameling hosts die actief deelneemt als deel van een net, en wordt gecontroleerd door een bekende automatische controller.

**CnC:** Verzameling van hosts die zijn geïdentificeerd als controleservers voor een bekend net.

**OpenProxy:** Een verzameling hosts die bekend zijn om Open Web Proxies te runnen en anonieme webbrowseringsservices aan te bieden.

**OpenRelay:** Een verzameling hosts die bekend zijn om anonieme e-mailservices aan te bieden die gebruikt worden door spam- en phishing-aanvallers.

**TorExitNode:** Een verzameling hosts die bekend zijn om de diensten van de exitknooppunten aan

te bieden voor het netwerk van de Tor Anonymizer.

**Bogon:** Verzameling van IP-adressen die niet zijn toegewezen maar verkeer verzenden.

**Verdachtzaam:** Een verzameling IP-adressen die verdachte activiteit weergeven en actief worden onderzocht.

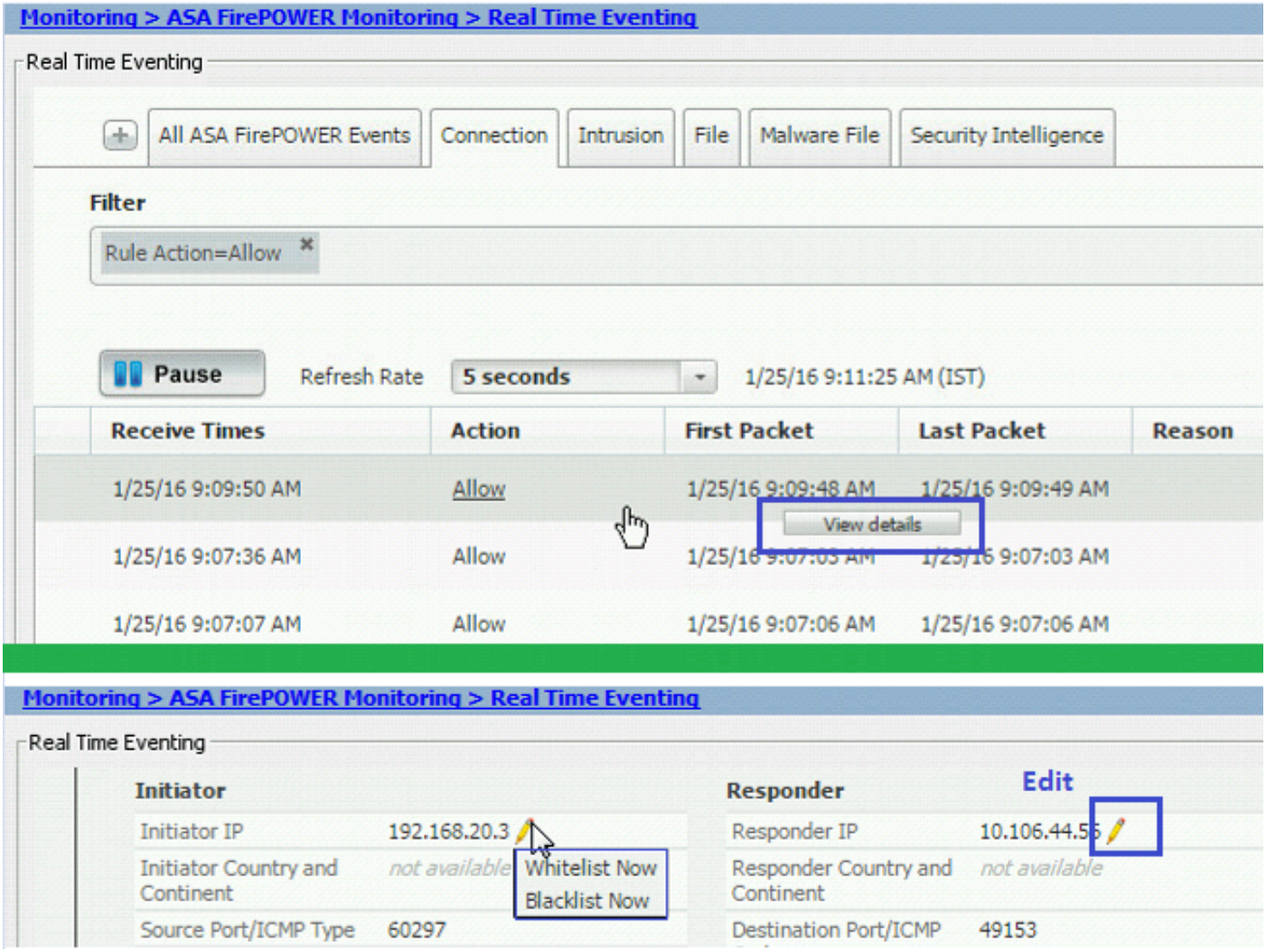
**Reactie:** Verzameling van IP-adressen die herhaaldelijk zijn waargenomen bij het verdachte of kwaadwillige gedrag.

# Voeg handmatig IP-adressen toe aan Global-Blacklist en Global-Whitelist

Met de FireSIGHT-module kunt u bepaalde IP-adressen toevoegen aan Global-Blacklist wanneer u weet dat ze onderdeel zijn van een of andere kwaadaardige activiteit. IP-adressen kunnen ook aan Global-Whitelist worden toegevoegd, als u het verkeer naar bepaalde IP-adressen wilt toestaan die geblokkeerd zijn door IP-adressen met een zwarte lijst. Als u een IP-adres toevoegt aan Global-Blacklist/Global-Whitelist, dan gebeurt dit meteen zonder dat u het beleid moet toepassen.

Als u het IP-adres aan Global-Blacklist/Global-Whitelist wilt toevoegen, **volgt u bewaking > ASA FirePOWER Monitoring > Real Time Eventing**, wacht dan de muis op aansluitingsgebeurtenissen en selecteer **Details bekijken**.

U kunt het IP-adres van de bron of van het bestemming toevoegen aan Global-Blacklist/Global-Whitelist. Klik op de knop **Bewerken** en selecteer **nu Whitelist/Blacklist Nu** om het IP-adres aan de respectievelijke lijst toe te voegen, zoals in de afbeelding.




Om te controleren of het IP-adres van de bron of bestemming wordt toegevoegd aan de Global-Blacklist/Global-Whitelist, navigeer naar **Configuration > ASA Firepower Configuration > Security Management > Security Intelligence > Network Lists en Feeds** en **bewerkt Global-Blacklist/Global Whitelist**. U kunt ook de knop Verwijderen gebruiken om een IP-adres uit de lijst te verwijderen.

# De aangepaste lijst met IP-adres maken

Met Firepower kunt u een aangepaste lijst met IP-adressen maken die kan worden gebruikt in een zwarte lijst (blokkering). Dit kan op drie manieren worden gedaan:

1. U kunt de IP-adressen naar een tekstbestand schrijven (één IP-adres per regel) en het bestand uploaden naar Firepower Module. Als u het bestand wilt uploaden, navigeer dan naar **Configuratie > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists en feeds** en klik vervolgens op **Add Network Lists en Feeds** Name: Specificeer de naam van de Aangepaste lijst. Type: Selecteer **Lijst** in de vervolgkeuzelijst. **Uploadlijst:** Kies **Bladeren** om het tekstbestand in uw systeem te vinden. Selecteer optie **Upload** om het bestand te uploaden.
2. U kunt een database van derden gebruiken voor de aangepaste lijst waarvoor de Firepower module contact opneemt met de server van derden om de IP-adreslijst op te halen. Om dit te configureren stuurt u naar **configuratie > ASA FirePOWER Configuration > Objectbeheer > Security Intelligence > Netwerklijsten en -voedingen** en klikt u vervolgens op **Netwerklijsten en -voedingen toevoegen**

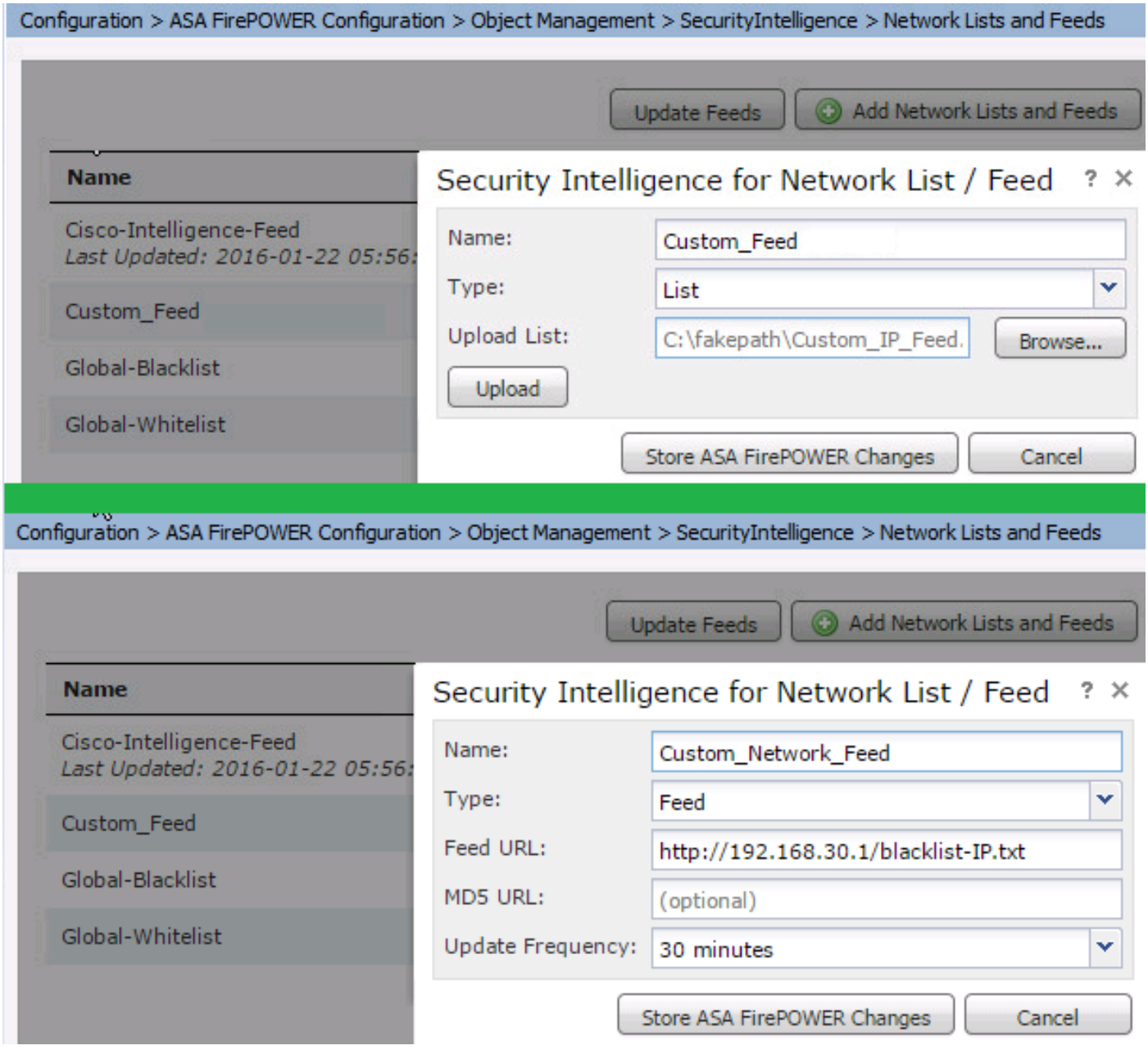
Name: Specificeer de naam van de Aangepaste diervoeders.

Type: Selecteer de optie **Voeding** uit de vervolgkeuzelijst.

**URL:** Specificeer de URL van de server waarop de Firepower module de feed moet aansluiten en downloaden.

**MD5 URL:** Specificeer de hashwaarde om het URL-pad voor invoer te valideren.

**Frequentie bijwerken:** Specificeer het tijdsinterval waarin het systeem verbinding maakt met de URL-server.




# De beveiligingsinformatie configureren

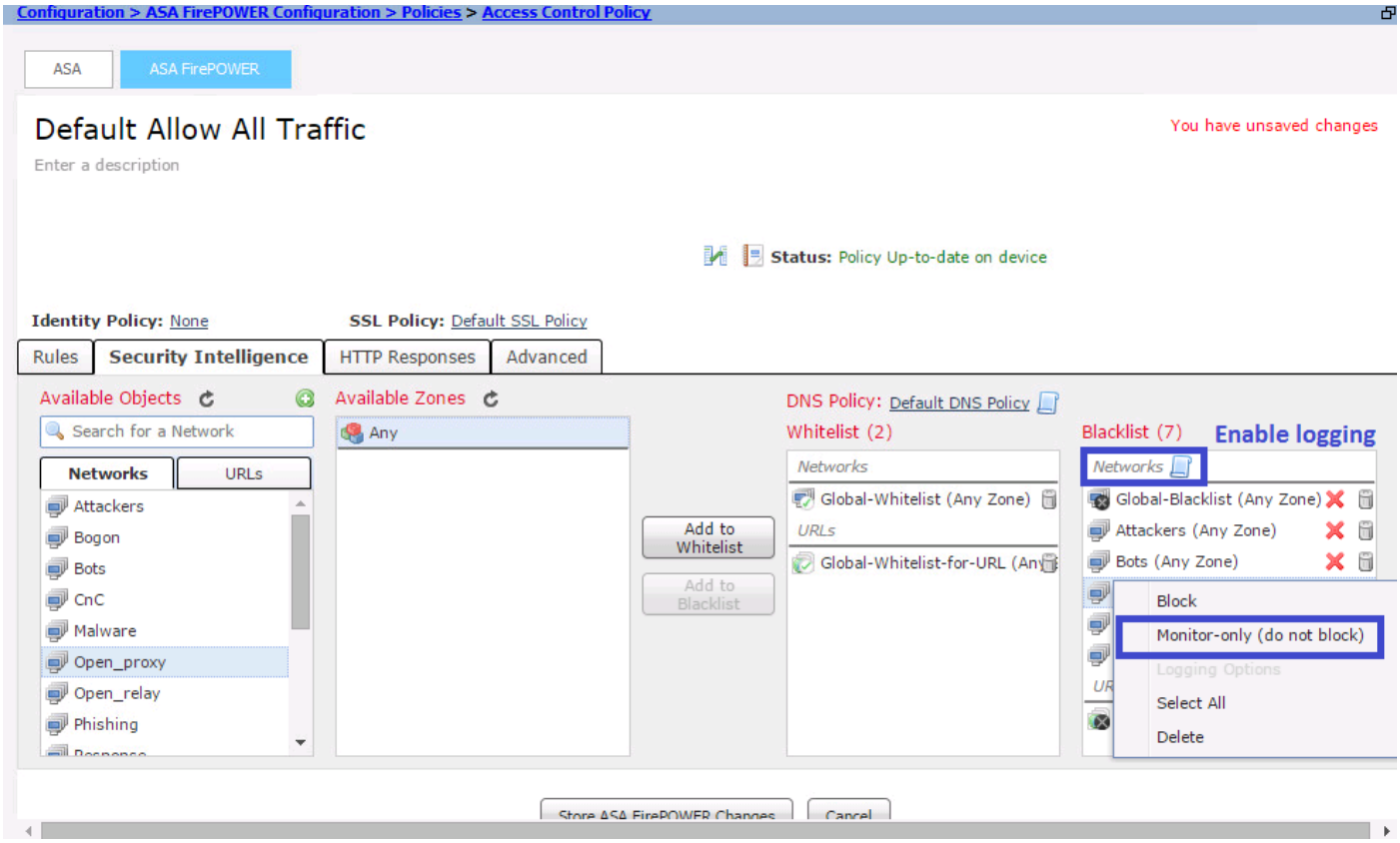
Om veiligheidsintelligentie te configureren **navigeer** naar **Configuratie > ASA Firepower Configuration > Policy > Access Control Policy,** selecteer **Security Intelligence** tabblad.

Kies het voer uit het object Network Available en verplaats naar de kolom **Whitelist/Blacklist** om de

verbinding met het kwaadaardige IP-adres toe te staan of te blokkeren.

U kunt op het pictogram klikken en de vastlegging inschakelen zoals in de afbeelding gespecificeerd.

Als u de gebeurtenis voor kwaadaardige IP-verbindingen wilt genereren in plaats van de verbinding te blokkeren, dan klikt u met de rechtermuisknop op de feed en kiest u **alleen monitor (niet blokkeren)**, zoals in de afbeelding:

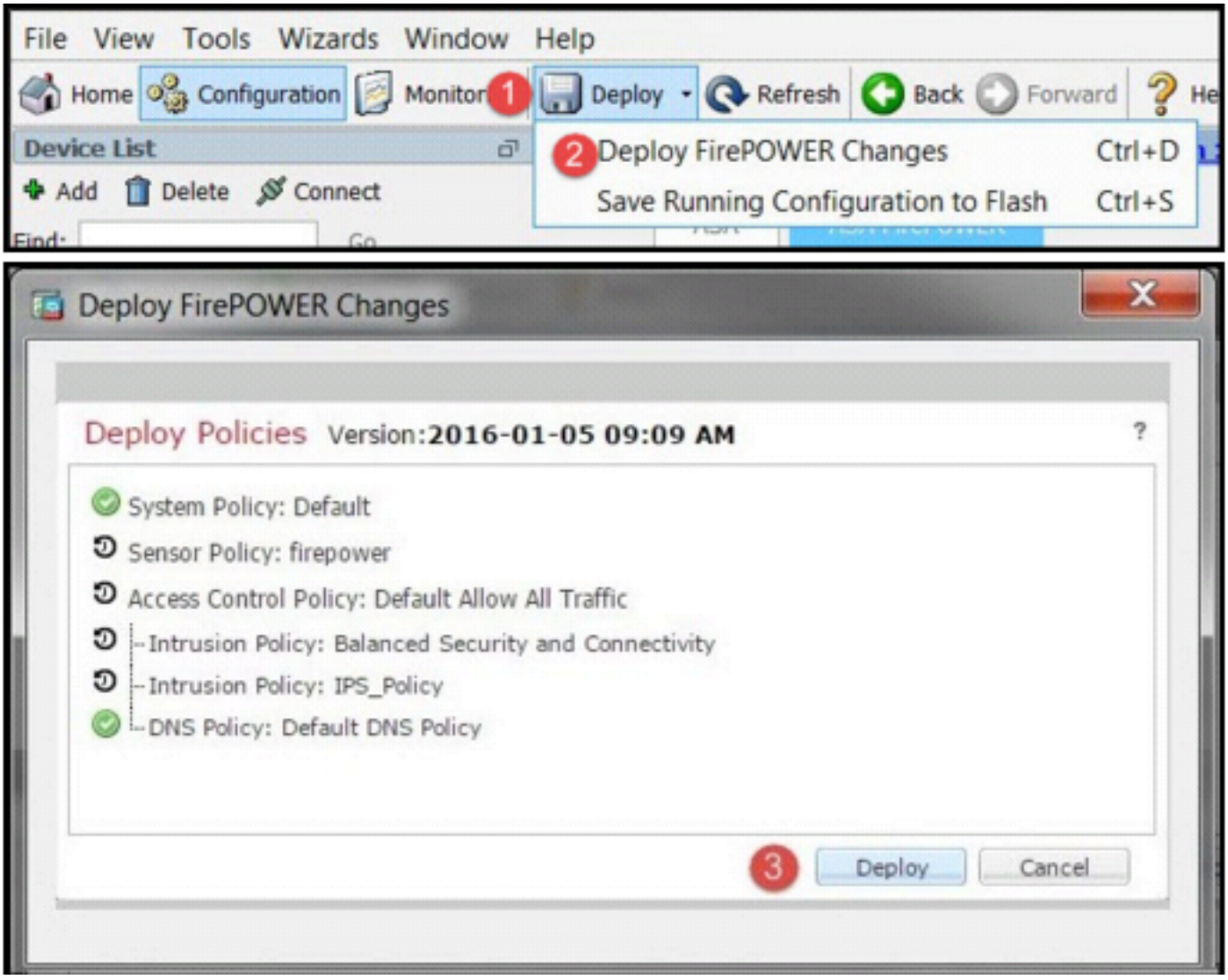



Kies optie Store ASA Firepower Change om de wijzigingen in het AC-beleid op te slaan.

# Toegangsbeheerbeleid implementeren

U moet het beleid voor toegangscontrole implementeren om veranderingen van kracht te laten worden. Voordat u het beleid toepast, zie dan een indicatie dat het toegangscontrolebeleid achterhaald is op het apparaat.

Om de wijzigingen in de sensor in te voeren, cKlik op **Importeren** en kies **Wijzigingen in FirePOWER implementeren** en selecteer **Afdrukken** in het pop-upvenster om de wijzigingen in te voeren.

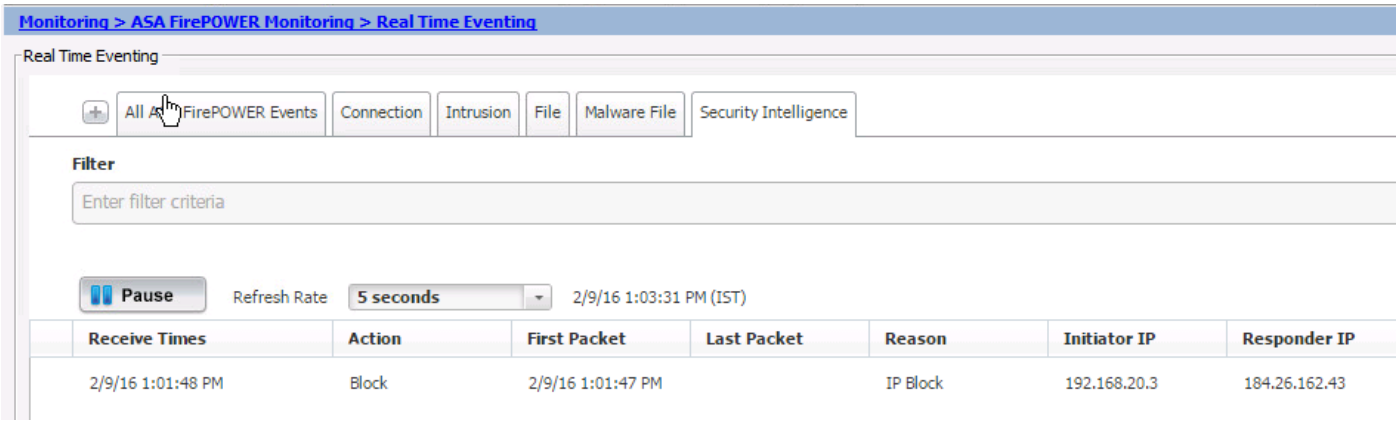



**Opmerking**: In versie 5.4.x moet u om het toegangsbeleid op de sensor toe te passen op **ASA FirePOWER Wijzigingen toepassen**

Opmerking: Navigeer naar **Controle > ASA Firepower Monitoring > Task Status.** Zorg ervoor dat deze taak voltooid moet zijn om de configuratie wijzigingen toe te passen.

## Bewaking van de gebeurtenissen van de veiligheidsinlichtingendienst

Om de Security Intelligence te zien door de FirePOWER-module te bladeren naar **bewaking > ASA FirePOWER-bewaking > Real Time Uiteindelijk**. Selecteer het tabblad **Security Intelligence**. De gebeurtenissen worden weergegeven zoals in de afbeelding:

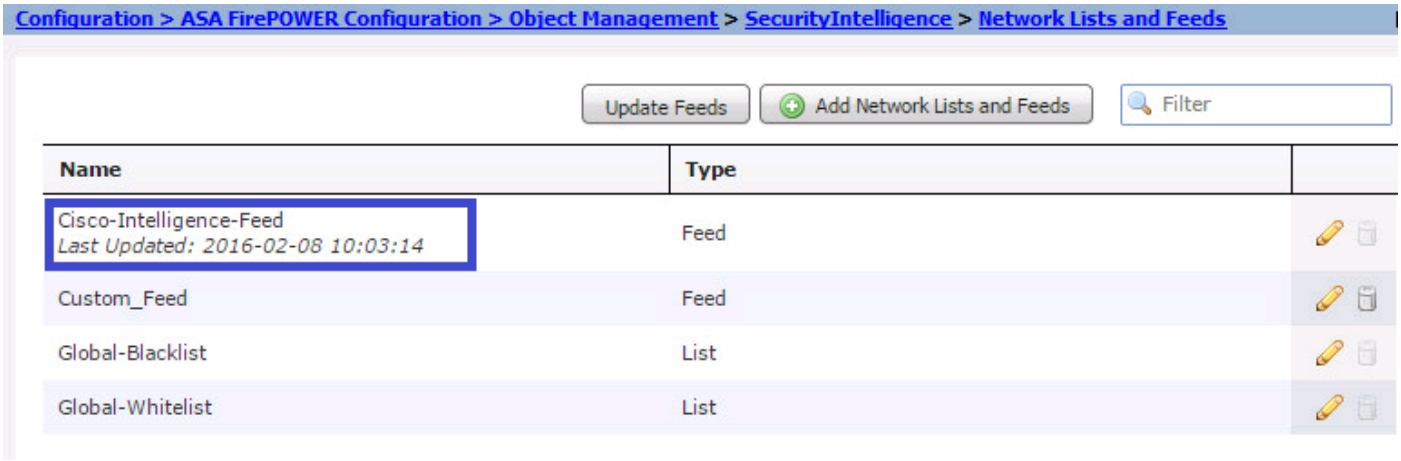



# Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

# Problemen oplossen

Om ervoor te zorgen dat de Security Intelligence Feeds bijgewerkt is, navigeer naar **Configuratie > ASA FirePOWER Configuration > Objectbeheer > Security Intelligence > Netwerklijsten en -voedingen** en controleer het tijdstip waarop de feed voor het laatst is bijgewerkt. U kunt de knop Bewerken kiezen om de frequentie van de update in te stellen.




Zorg ervoor dat de implementatie van het Toegangsbeheerbeleid met succes is voltooid.

Controleer de veiligheidsinlichtingen om te zien of het verkeer blokkeert of niet.

## Gerelateerde informatie

- **Cisco ASA FirePOWER-module - Snel startgids**
- **Technische ondersteuning en documentatie – Cisco Systems**