Domain Based Security Intelligence (DNS-beleid) configureren in FirePOWER-module met ASDM (On-Box Management)

Inhoud

Inleiding

Dit document beschrijft hoe u Domain Based Security Intelligence (SI) kunt configureren met FirePOWER-module met behulp van Adaptieve Security Devices Manager (ASDM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van ASA (adaptieve security applicatie) firewall
- ASDM (adaptieve security apparaatbeheer)
- Kennis van FirePOWER-module

Opmerking: Security Intelligence filter vereist een beschermingslicentie.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- ASA FirePOWER-modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) met softwareversie 6.0.0 en hoger
- ASA FirePOWER-module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) met softwareversie 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

Firepower systeem biedt de mogelijkheid om DNS-verkeersverzoeken te onderscheppen en zoekt de kwaadaardige domeinnaam. Als de Firepower module een kwaadaardig domein vindt, neemt de Firepower passende actie om het verzoek te verzachten zoals per configuratie van DNS-beleid.

Nieuwe aanvalmethodes die worden ontworpen om op IP gebaseerde intelligentie te breken, misbruiken de eigenschappen van de DNS belastingbalans om het eigenlijke IP adres van een kwaadaardige server te verbergen. Terwijl de IP adressen verbonden aan de aanval vaak binnen en uit worden geruild, wordt de domeinnaam zelden veranderd.

Firepower biedt de mogelijkheid om het kwaadwillige verzoek om te sturen naar een server met een gat die een server kan zijn om te detecteren, af te leiden of te bestuderen pogingen om meer over het aanvalsverkeer te weten te komen.

Overzicht van domeinlijsten en -snelheden

Domain Lists and Feeds bevatten de lijst van de kwaadaardige domeinnaam die verder in de verschillende categorie wordt ingedeeld op basis van het aanvalstype. Meestal kunt u de velden in twee typen categoriseren.

Cisco TALOS voorzag in domeinlijsten en -snelheden

DNS-aanvallers: verzameling van domeinnamen die voortdurend op kwetsbaarheden scannen of proberen andere systemen te exploiteren.

DNS-band**:** verzameling van domeinnamen die het verkeer niet toewijzen maar resetten, ook bekend als Fake IP's,

DNS-Bots: verzameling van domeinnamen die actief deelnemen als deel van een net en die

worden gecontroleerd door een bekende actieve controller.

DNS CnC: verzameling van domeinnamen die worden geïdentificeerd als de controleservers van een bekend net.

DNS-exploset: Inzameling van domeinnamen die proberen andere systemen te exploiteren.

DNS Malware: verzameling van domeinnamen die malware proberen te propageren of die actief iedereen aanvallen die ze bezoekt.

DNS Open_proxy: verzameling domeinnamen die Open Web Proxies uitvoeren en anonieme webbrowse-services aanbieden.

DNS Open_relais: Verzameling van domeinnamen die anonieme e-mailrelais diensten bieden die door spam en phish aanvallers worden gebruikt.

DNS-fase: verzameling van domeinnamen die actief proberen een eindgebruiker om vertrouwelijke informatie als gebruikersnamen en wachtwoorden te gooien.

DNS-respons: verzameling domeinnamen die herhaaldelijk zijn waargenomen bij verdacht of kwaadwillig gedrag.

DNS-spam: verzameling van domeinnamen die worden geïdentificeerd als de bron die spam-e-mailberichten verstuurt.

DNS Verdachte: Verzameling van domeinnamen die verdachte activiteit tonen en actief onderzoek ondergaan.

DNS Tor_exit_Knop: Verzameling van domeinnamen die de diensten van de exit knooppunt voor het netwerk van de Tor Anonymizer aanbieden.

Aangepaste domeinlijsten en -snelheden

Global Blacklist voor DNS: Verzameling van de aangepaste lijst van domeinnamen die door de beheerder als kwaadaardig zijn geïdentificeerd.

Global whitelist voor DNS: Verzameling van de aangepaste lijst van domeinnamen die door de beheerder als echt zijn geïdentificeerd.

DNS-beveiligingsinformatie configureren

Er zijn meerdere stappen om de Domain Name-gebaseerde security intelligentie te configureren.

1. Configuratie van de aangepaste DNS-voeding/lijst (optioneel)
2. Het object Songgat configureren (optioneel)
3. Het DNS-beleid configureren

4. Het toegangscontrolebeleid configureren
5. Het toegangscontrolebeleid implementeren

Stap 1. Configuratie van Aangepaste DNS-voeding/lijst (optioneel).

Er zijn twee vooraf gedefinieerde lijsten die het mogelijk maken de domeinen eraan toe te voegen. U maakt uw eigen lijsten en diervoeders voor de domeinen die u wilt blokkeren.

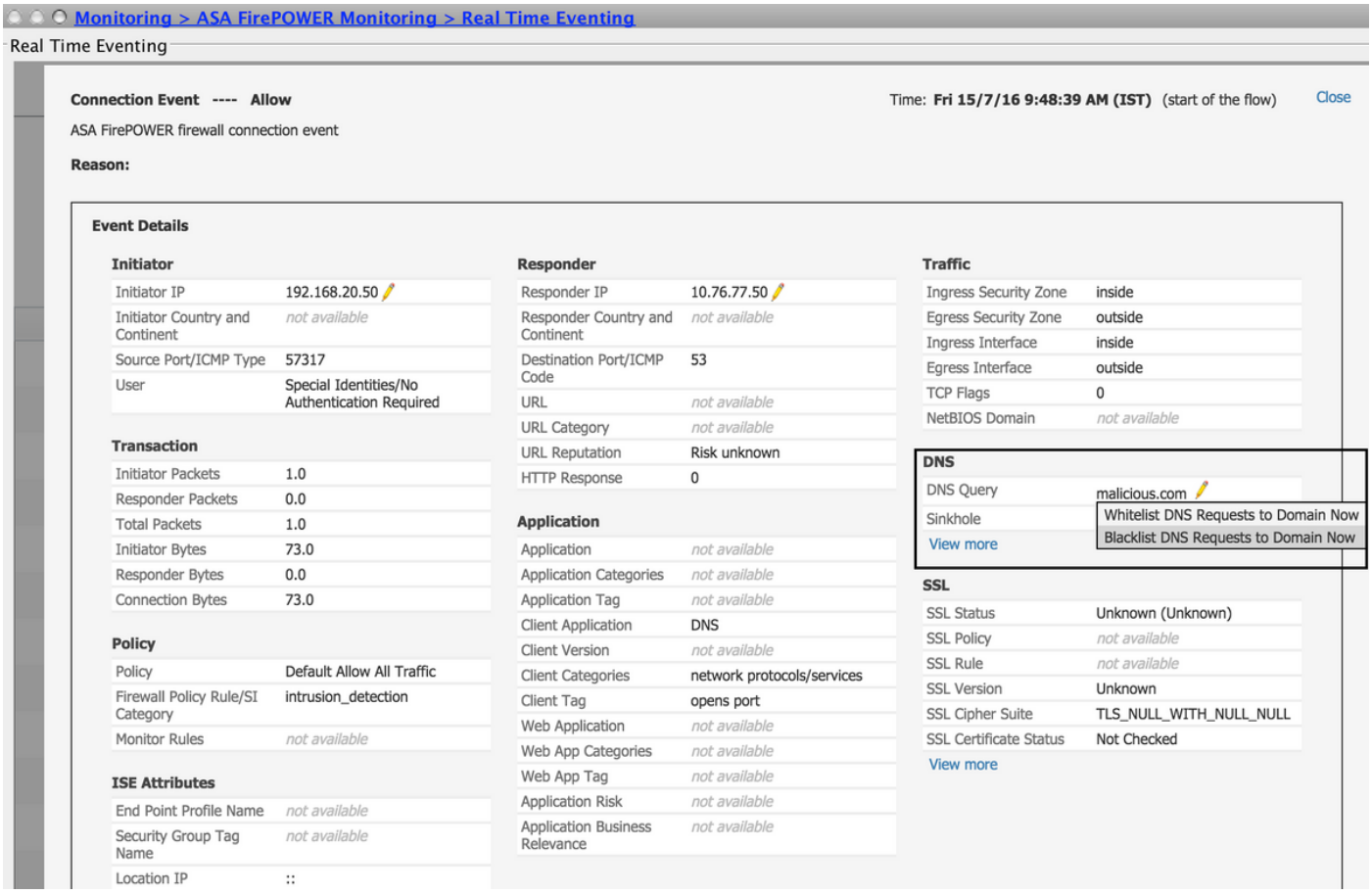
- Global Blacklist voor DNS
- Global Whitelist voor DNS

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

Met de Firepower module kunt u bepaalde domeinen aan Global-Blacklist toevoegen als je weet dat ze onderdeel zijn van een kwaadaardige activiteit. Domeinen kunnen ook worden toegevoegd aan Global Whitelist als je het verkeer naar bepaalde domeinen wilt toestaan die geblokkeerd zijn door gebieden met een zwarte lijst. Als je een domein toevoegt aan Global-Blacklist/Global-Whitelist, dan gebeurt het meteen zonder dat je 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 domeinen toevoegen aan Global-Blacklist/Global-Whitelist. Klik op **Bewerken** op DNS-gedeelte en selecteer **Whitelist DNS-aanvragen om nu te domeinnaam/Blacklist DNS-aanvragen om nu te domeinnamen** om het domein aan de respectievelijke lijst toe te voegen, zoals in de afbeelding weergegeven.



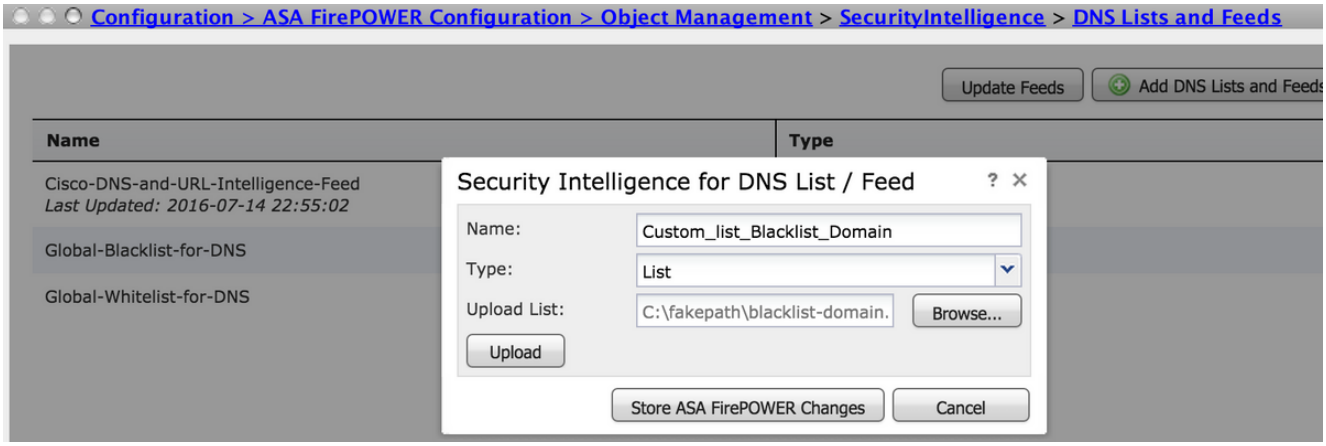
Om te controleren of er domeinen worden toegevoegd aan Global-Blacklist/Global-Whitelist, navigeer dan naar **Configuration > ASA FirePOWER Configuration > Objectbeheer > SecurityIntelligence > DNS-lijsten en voedingen** en **Bewerk Global-Blacklist voor DNS/Global Whitelist voor DNS**. U kunt ook de knop Verwijderen gebruiken om een domein uit de lijst te verwijderen.

De aangepaste lijst met zwarte lijstdomeinen maken

Met FirePOWER kunt u een lijst met aangepaste domeinnamen maken, die u met twee verschillende methoden kunt gebruiken om een lijst van gescande gegevens op te slaan (blokkeren).

1. U kunt domeinnamen naar een tekstbestand schrijven (één domein per regel) en het bestand naar FirePOWER-module uploaden.

   Als u het bestand wilt uploaden, navigeer dan naar **Configuratie > ASA FirePOWER Configuration > Objectbeheer > Security Intelligence > DNS-lijsten en -voedingen** en selecteer **DNS-lijsten en -voedingen toevoegen** 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 **Upload** om het bestand te uploaden.



   Klik op **Store ASA FirePOWER Wijzigingen** om de wijzigingen op te slaan.

2. U kunt elk derdengebied gebruiken voor de aangepaste lijst waarvoor de module van de Firepower de server van de derde kan verbinden om de domeinlijst te halen.

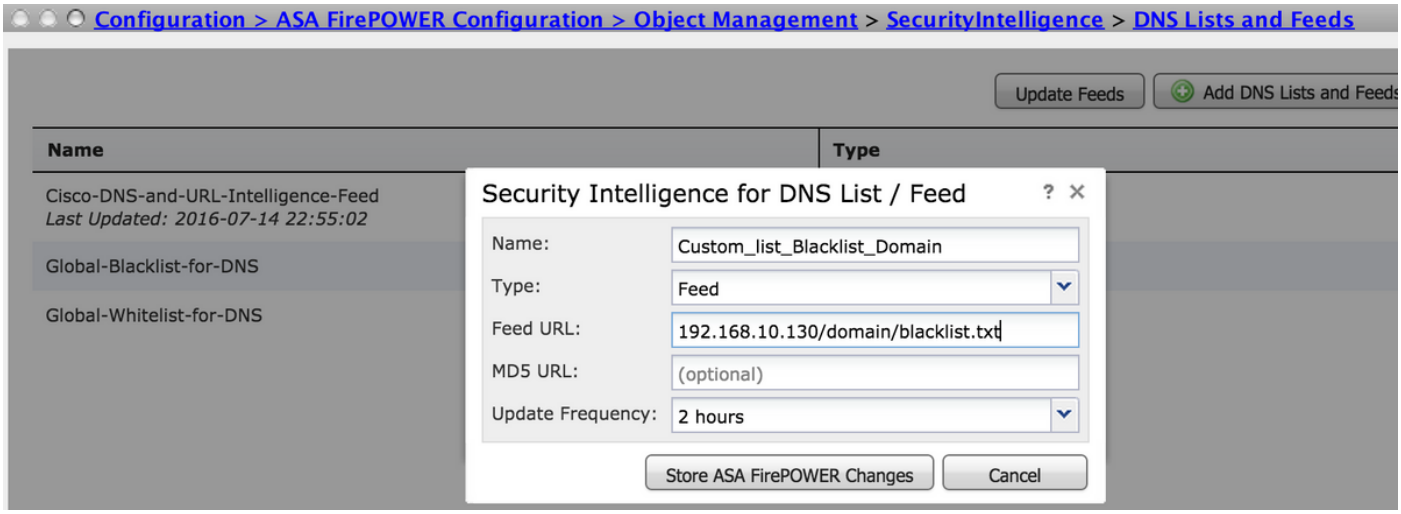
   Om dit te configureren **navigeer** naar **Configuratie > ASA FirePOWER Configuration > Objectbeheer > Security Intelligence > DNS Lists en feeds** en selecteer vervolgens **DNS-lijsten en -voedingen toevoegen**
   Name: Specificeer de naam van de Aangepaste diervoeders.

   Type: Selecteer Voeding in de vervolgkeuzelijst.

   URL: Specificeer de server-URL waarop de FirePOWER-module de feed kan aansluiten en downloaden.

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

Frequentie bijwerken: Specificeer het tijdsinterval waarin de module zich verbindt met de URL-server.



Selecteer **Store ASA FirePOWER Wijzigingen** om de wijzigingen op te slaan.

Stap 2. Het configureren van een object dat een gat vormt (optioneel).

IP-adres kan worden gebruikt als antwoord op een kwaadaardig DNS-verzoek. De client krijgt het IP-adres van de server van het gat voor kwaadaardige domeinraadpleging en de machine probeert in het eindapparaat verbinding te maken met de server van het gat. Het gat kan dus fungeren als de Honeypot om het aanvalsverkeer te onderzoeken. Het gat kan worden geconfigureerd om een indicator van het compromis te activeren (IOC).

Als u de server voor het **putgat** wilt toevoegen, **configuratie > ASA FirePOWER Configuration > Objectbeheer > Sinkopening** en klikt u op de optie **Toevoegen-gat**.

Name: Specificeer de naam van de server voor het putgat.

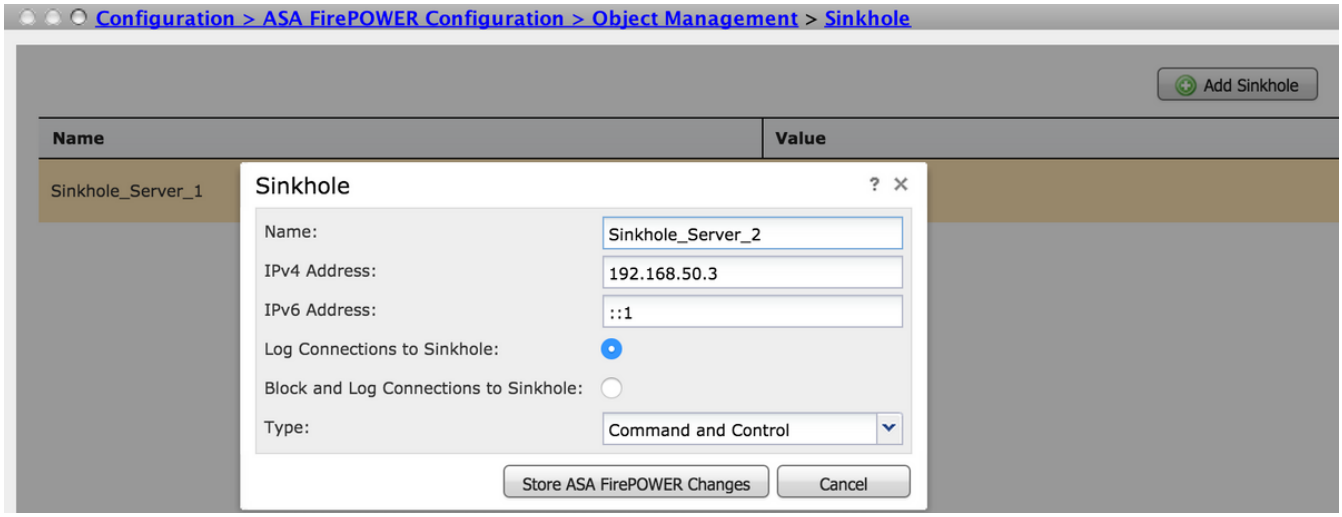
IP-adres: Specificeer het IP-adres van de server voor het putje.

Logaansluitingen op Sinkopening: Schakel deze optie in om alle verbindingen tussen het eindpunt en de server met het gat te registreren.

Blokkeer en log-verbindingen naar Sinkopening: Schakel deze optie in om de verbinding te blokkeren en alleen loggen aan het begin van een stroomverbinding. Als er geen fysieke server van het zinkgat is, kunt u om het even welk IP adres specificeren en u kunt de verbindingsgebeurtenissen en IOC trigger zien.

Type: Specificeer het voer in de vervolgkeuzelijst waarvoor u het type IOC (Indicatie van het compromis) wilt selecteren dat gekoppeld is aan gebeurtenissen in het gat. Er zijn drie soorten IOC-holtes die gelabeld kunnen worden.

- Malware
- Opdracht en controle
- Phish



Stap 3. Configuratie van DNS-beleid.

DNS-beleid moet worden geconfigureerd om de actie voor de DNS-feed/lijst te bepalen. Navigeer naar **configuratie > ASA FirePOWER Configuration > Policy > DNS Policy.**

Het standaard DNS-beleid bevat twee standaardregels. De eerste regel, **Global Whitelist voor DNS**, bevat de aangepaste lijst van het toegestane domein (**Global-Whitelist-for-DNS**). Deze regel staat bovenaan om eerst te matchen voordat het systeem probeert om het even welk zwart list domein te evenaren. De tweede regel, **Global Blacklist voor DNS**, bevat de aangepaste lijst van het geblokkeerde domein (**Global-Blacklist-for-DNS**).

U kunt meer regels toevoegen om de verschillende acties voor **Cisco TALOS** te definiëren **die Domain Lists en Feeds hebben geleverd**. Als u een nieuwe regel wilt toevoegen, selecteert u **DNS-regel toevoegen.**

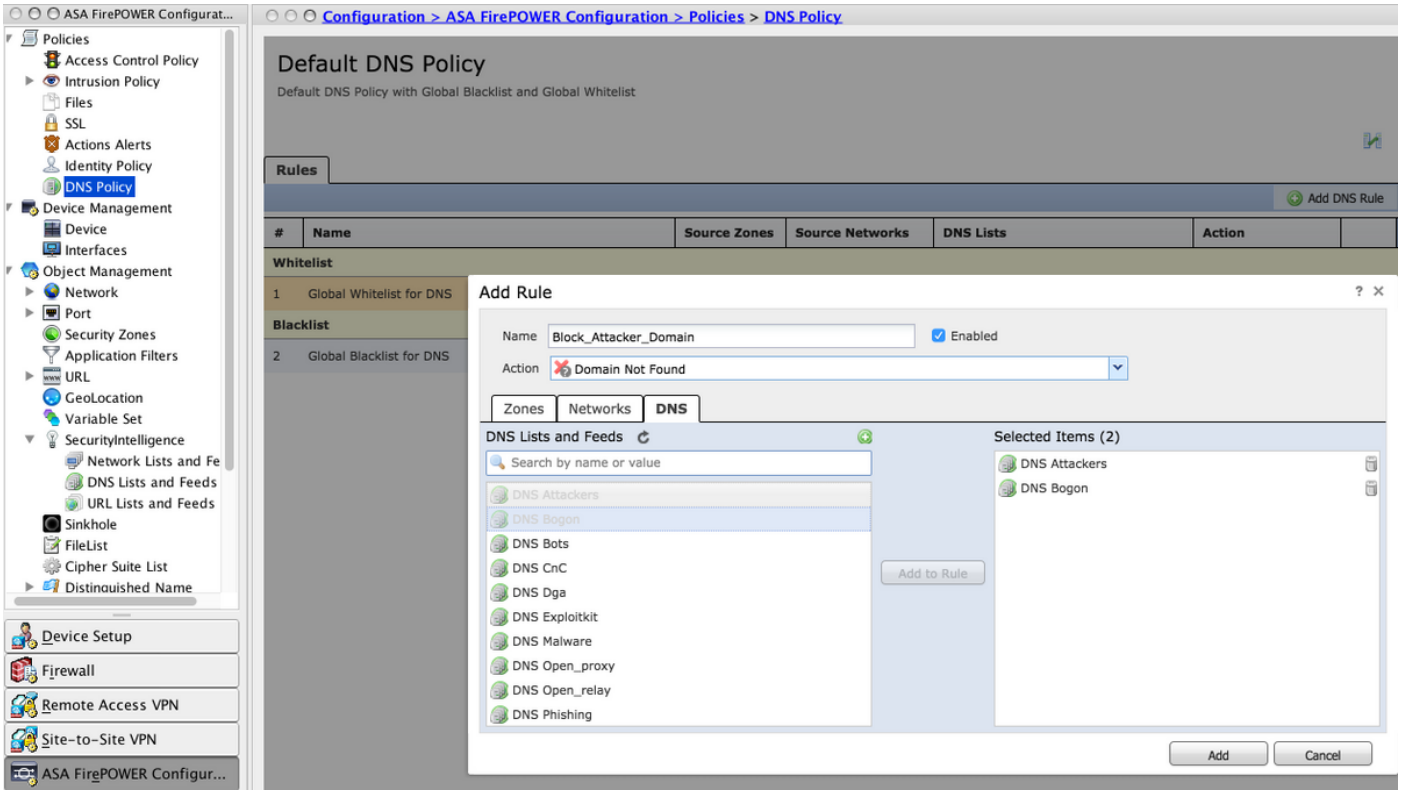
Naam: Specificeer de regelnaam.

Actie: Specificeer de actie om te starten wanneer deze regel overeenkomt.

- **Whitelist:** Hiermee kan de DNS-query worden uitgevoerd.
- **Monitor:** Deze actie genereert de gebeurtenis voor DNS-zoekopdracht en verkeer blijft voldoen aan de volgende regels.
- **Domain Not found:** Deze actie stuurt DNS-respons als Domain Not found (niet-bestaand domein).
- **Drop:** Deze actie blokkeert de DNS-query stilletjes en laat deze vallen.
- **Sinkopening:** Deze actie verstuurt het IP-adres van de server van Sinkopening als antwoord op een DNS-verzoek.

Specificeer de **Gebieden/Netwerk** om de regelvoorwaarden te definiëren. Kies op het tabblad DNS de **DNS-lijsten en -voedingen** en verplaats naar de optie **Geselecteerde items** waar u de ingestelde actie kunt toepassen.

U kunt de meerdere DNS-regels voor verschillende DNS-lijsten en -velden configureren met een andere actie op basis van uw organisatie-behoeften.

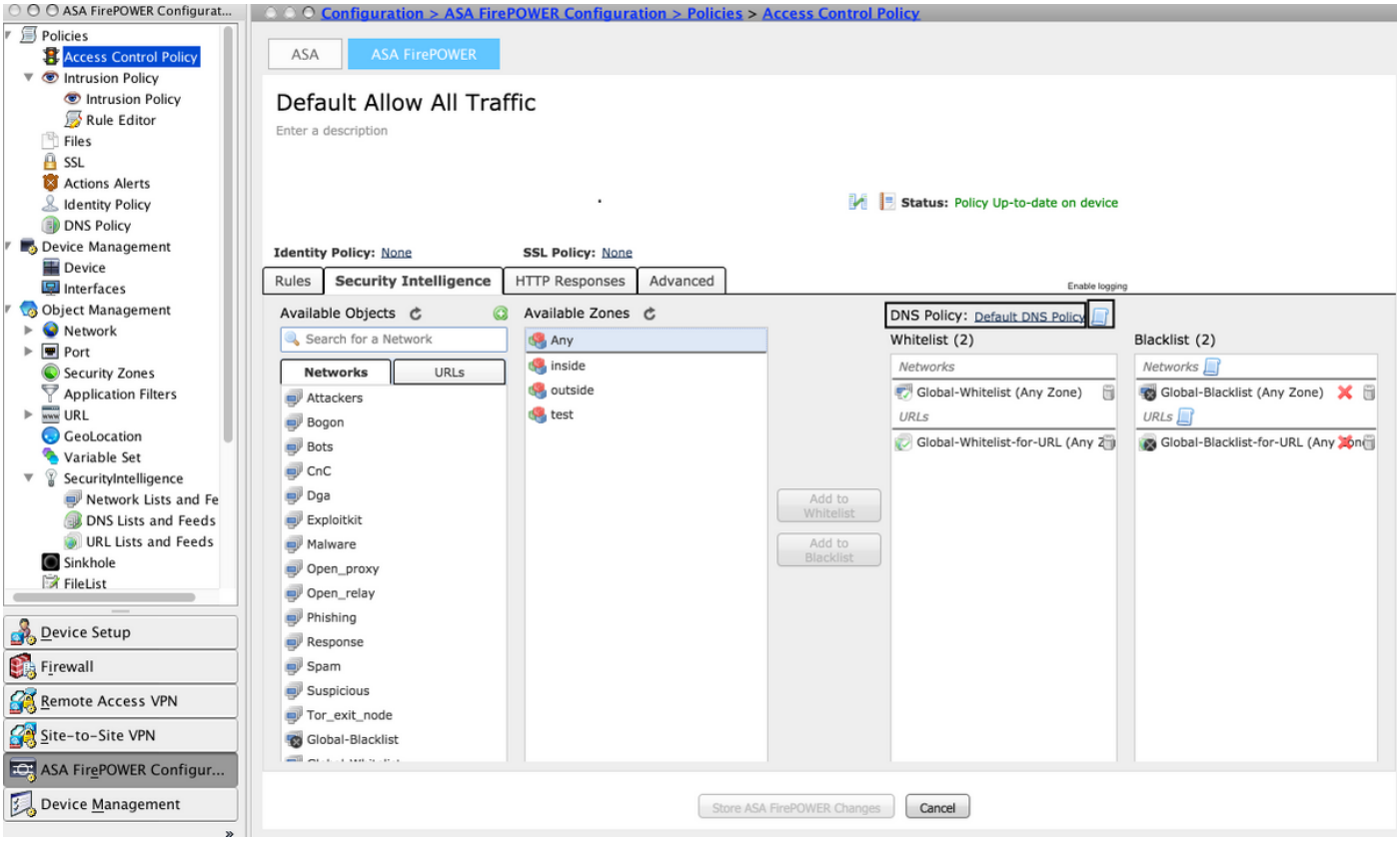


Klik op de optie **Toevoegen** om de regel toe te voegen.

Stap 4. Configureer het toegangscontrolebeleid.

Om de DNS-gebaseerde security Intelligentie te configureren **volgt u** op **Configuration > ASA Firepower Configuration > Policy > Access Control Policy,** selecteert u **Security Intelligence** tabblad.

Zorg ervoor dat DNS Policy is ingesteld en optioneel, u kunt de logbestanden inschakelen terwijl u op het pictogram voor logbestanden klikt zoals in de afbeelding.



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

Stap 5. Plaats het toegangscontrolebeleid in.

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.

Als u de wijzigingen in de sensor wilt inzetten, klikt u op **Importeren** en vervolgens kiest u **Wijzigingen in FirePOWER implementeren** en vervolgens selecteert u **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**.

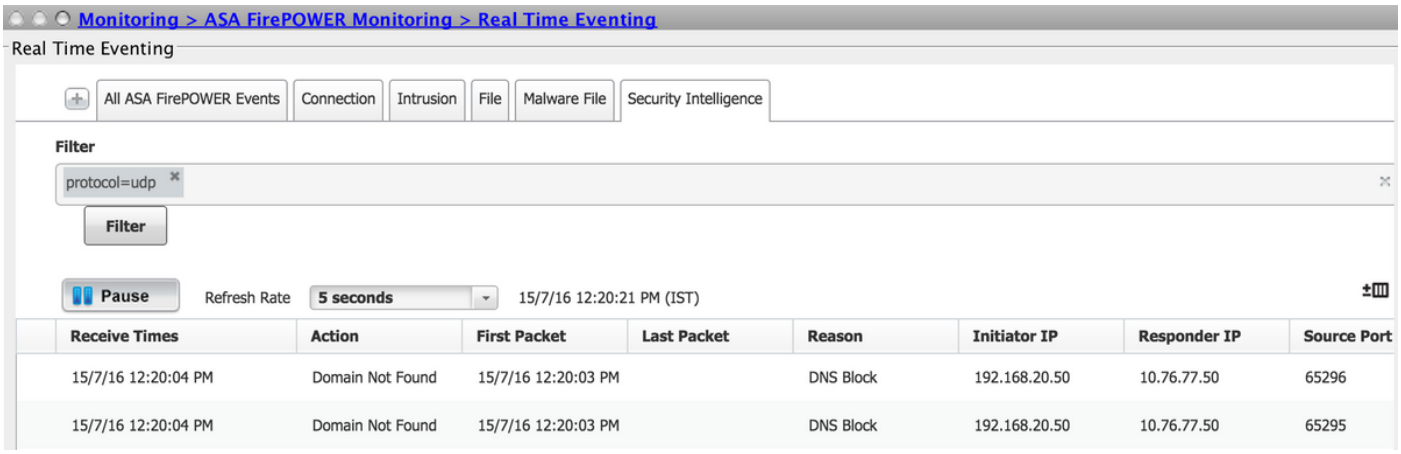
> Opmerking: Navigeer naar **Controle > ASA Firepower Monitoring > Task Status.** Zorg ervoor dat de taak compleet is om de configuratiewijzigingen te bevestigen.

Verifiëren

Configuratie kan slechts worden geverifieerd als een gebeurtenis wordt geactiveerd. Hiervoor kunt u een DNS query op een machine forceren. Wees echter voorzichtig met de repercussies wanneer een bekende kwaadaardige server is gericht. Nadat u deze query genereert, kunt u de gebeurtenis zien in de sectie **Real Time Eventing**.

Monitoring van DNS-beveiligingsinformatie

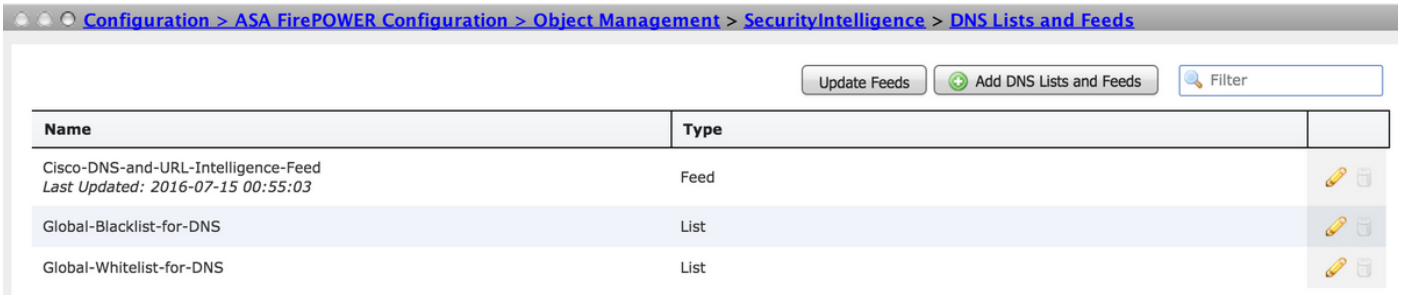
Om de Security Intelligence te zien door de FirePOWER-module te bladeren naar **bewaking > ASA FirePOWER-bewaking > Real Time Uiteindelijk**. Selecteer het tabblad **Security Intelligence**. Dit toont de gebeurtenissen zoals in de afbeelding weergegeven:



Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

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



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

Controleer de Security Intelligence Real Time tab om te zien of het verkeer is geblokkeerd of niet.

Gerelateerde informatie

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