Configuratie van inbraakbeleid en handtekeningen in FirePOWER-module (On-Box Management)

Inhoud

Inleiding

Dit document beschrijft de functionaliteit van het Inbraakpreventiesysteem (IPS)/Inbraakdetectiesysteem (IDS) van FirePOWER-module en de elementen van het inbraakbeleid die een detectiebeleid in FirePOWER-module maken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

* Kennis van adaptieve security applicatie (ASA) firewall, adaptieve security applicatie Manager (ASDM).

* Kennis van FirePOWER-applicatie.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

FirePOWER IDS/IPS is ontworpen om het netwerkverkeer te onderzoeken en kwaadaardige patronen (of handtekeningen) te identificeren die op een netwerk-/systeemaanval duiden. FirePOWER-module werkt in IDS-modus als het ASA-beleid specifiek is geconfigureerd in de monitormodus (veelbelovend) anders, dan werkt het in de inline modus.

FirePOWER IPS/IDS is een op handtekeningen gebaseerde detectiebenadering. FirePOWERmodule in IDS-modus genereert een waarschuwing wanneer signatuur het kwaadaardige verkeer aanpast, terwijl FirePOWER-module in IPS-modus alert is en kwaadaardig verkeer blokkeert.

> **Opmerking**: Zorg ervoor dat FirePOWER Module een **Protect** licentie moet hebben om deze functionaliteit te configureren. Om de licentie te controleren dient u te navigeren naar **Configuration > ASA FirePOWER Configuration > Licentie.**

Configuratie

Stap 1. Inbraakbeleid instellen

Stap 1.1. Inbraakbeleid maken

U kunt als volgt inbraakbeleid instellen door in te loggen op Adapter Security Manager (ASDM) en de volgende stappen uit te voeren:

Stap 1. Navigeer naar **Configuration > ASA FirePOWER Configuration > Policy > Inbraakbeleid > Inbraakbeleid**.

Stap 2. Klik op het **beleid maken**.

Stap 3. Voer de **naam** van het inbraakbeleid in.

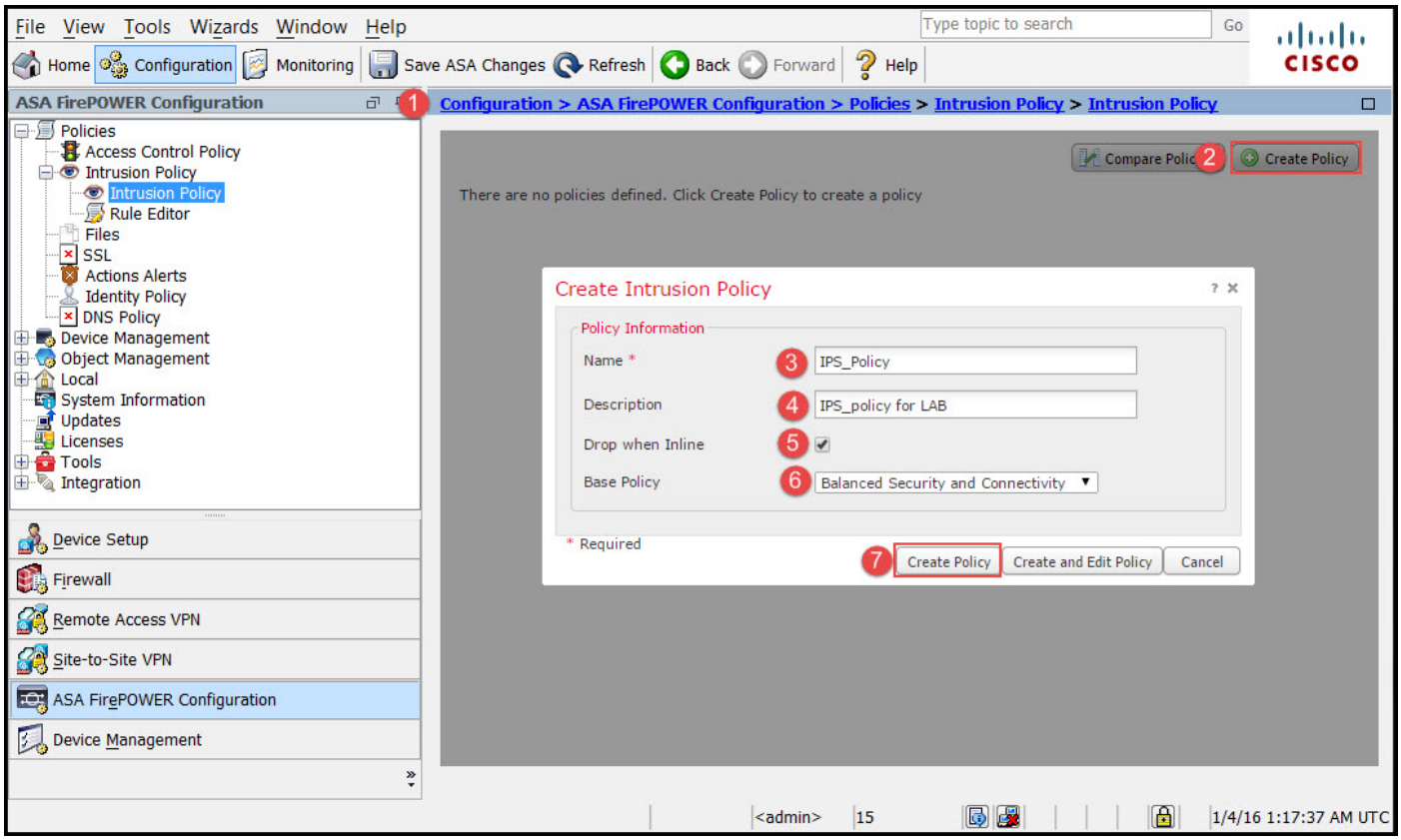
Stap 4. Voer de **beschrijving** van het inbraakbeleid in (optioneel).

Stap 5. Specificeer de **optie Drop wanneer** u **inline** hebt.

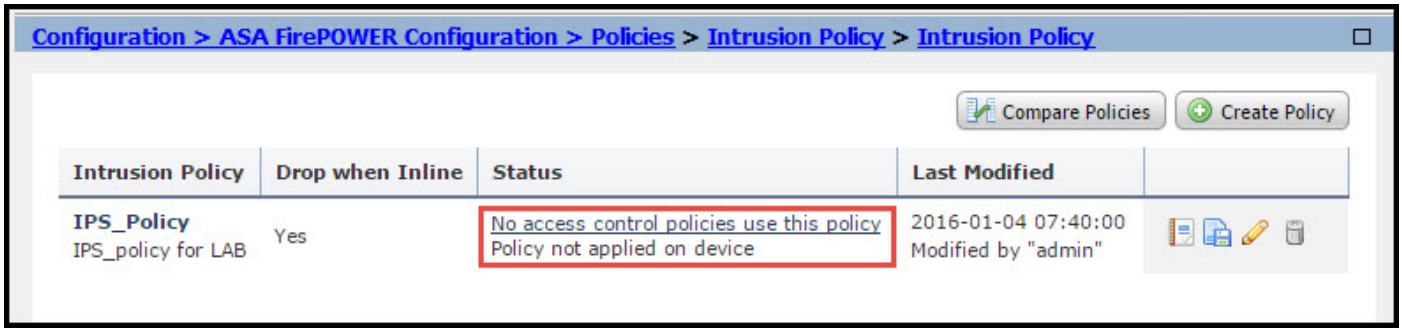
Stap 6. Selecteer het **basisbeleid** in de vervolgkeuzelijst.

Stap 7. Klik op **Beleid maken** om de creatie van het Inbraakbeleid te voltooien.

> **Tip**: Laat vallen wanneer optie Inline is essentieel in bepaalde scenario's wanneer de sensor in Inline modus is geconfigureerd en het verkeer niet hoeft te worden verlaagd, ook al komt deze bij een handtekening met een uitrolactie.

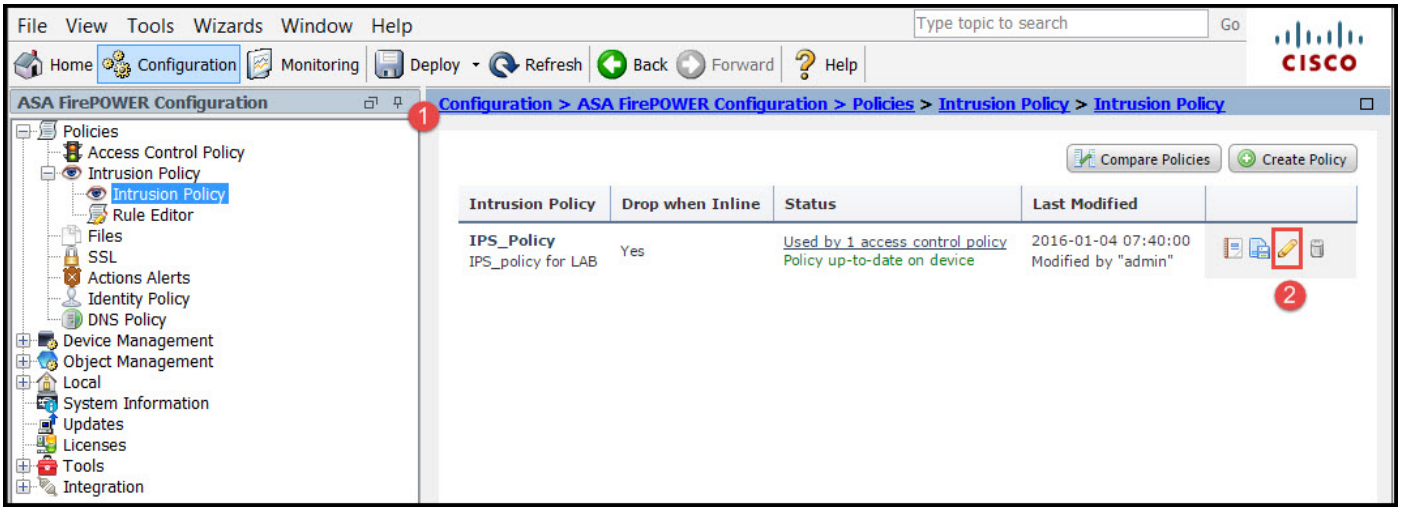


U kunt opmerken dat het beleid is geconfigureerd, maar het is niet van toepassing op welk apparaat dan ook.



Stap 1.2. Het inbraakbeleid wijzigen

Als u inbraakbeleid wilt wijzigen, navigeer dan naar **Configuration > ASA FirePOWER Configuration > Policy > Inbraakbeleid > Inbraakbeleid** en selecteer de optie **Bewerken**.

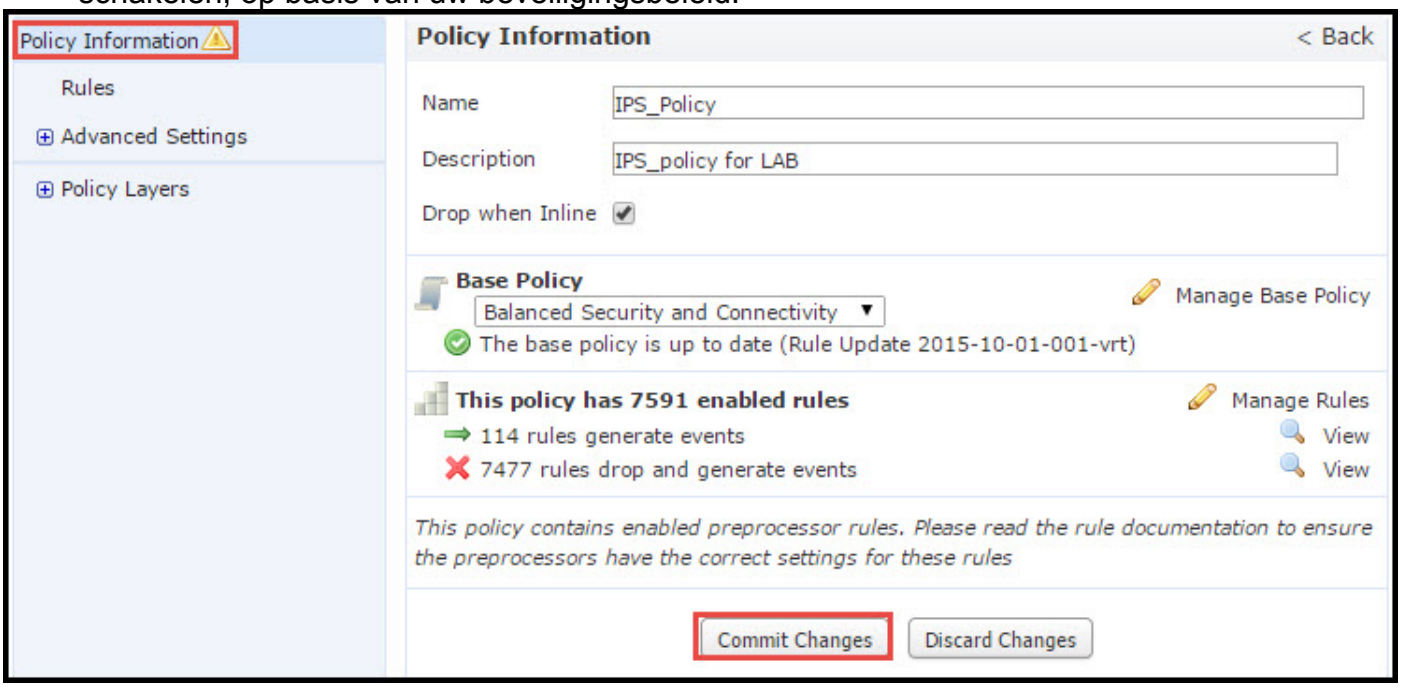


Stap 1.3. Het basisbeleid wijzigen

De pagina Inbraakbeleid Management geeft de optie om het basisbeleid/de optie Drop te wijzigen wanneer Inline/Save and Discard optie.

Het basisbeleid bevat een aantal systeemrelevante beleidslijnen, die ingebouwd beleid zijn.

1. Een gebalanceerde beveiliging en connectiviteit: Het is een optimaal beleid op het gebied van veiligheid en connectiviteit. Dit beleid heeft zo'n 7500 regels mogelijk, waarvan sommige alleen maar gebeurtenissen veroorzaken, terwijl andere gebeurtenissen veroorzaken en het verkeer verminderen.
2. Beveiliging boven connectiviteit: Als uw voorkeur beveiliging is, kunt u veiligheid boven connectiviteit beleid kiezen, wat het aantal enabled regels verhoogt.
3. Connectiviteit over veiligheid: als uw voorkeur connectiviteit in plaats van beveiliging is, kunt u connectiviteit boven veiligheidsbeleid kiezen wat het aantal toegelaten regels zal verminderen.
4. Maximale detectie - selecteer dit beleid om een maximale detectie te verkrijgen.
5. Geen regel actief - Deze optie schakelt alle regels uit. U dient de regels handmatig in te schakelen, op basis van uw beveiligingsbeleid.



Stap 1.4. Signaalfiltering met optie van filterbalk

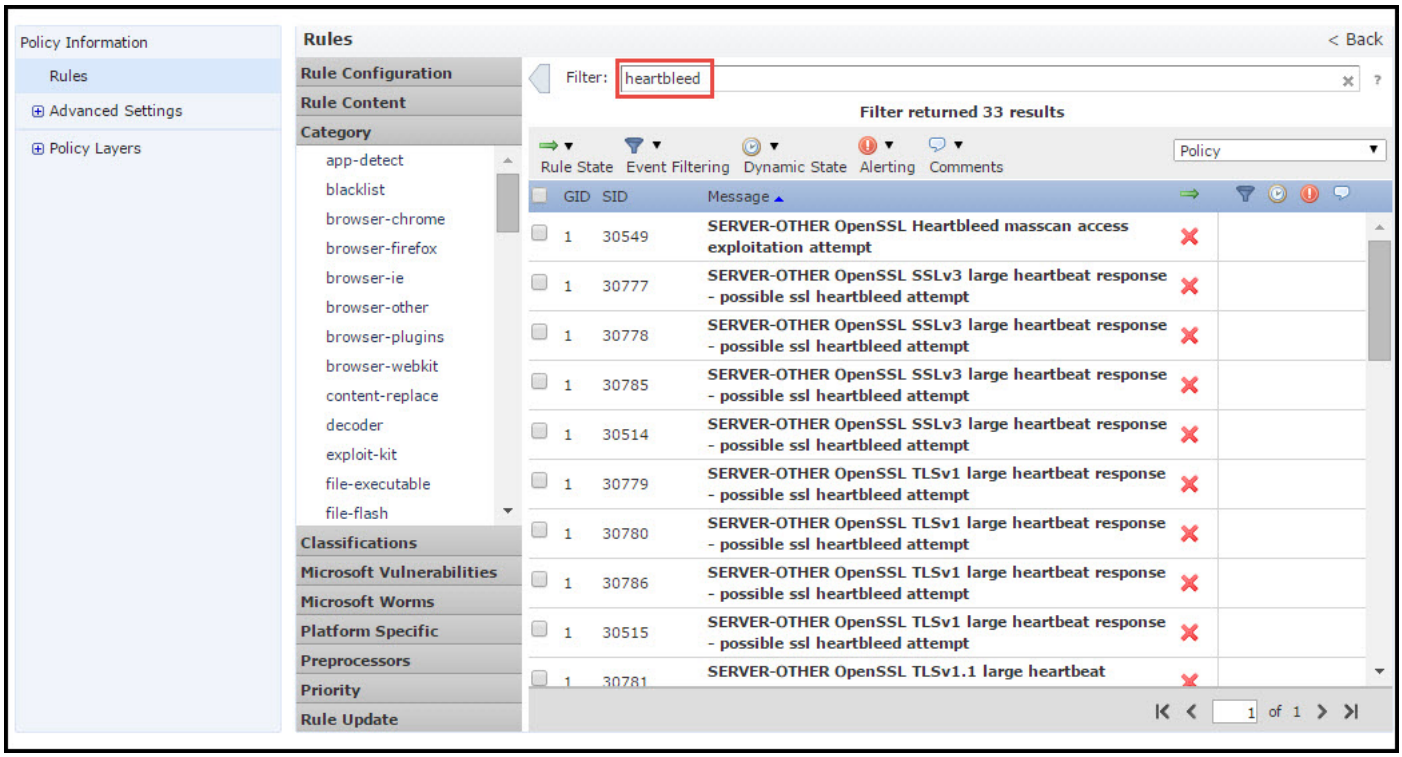
Navigeer naar de optie **Regels** in een navigatiedeelvenster en de pagina Regelbeheer verschijnt. Duizenden regels zijn in de database van regels. De filterbalk biedt een goede zoekmachine optie om de regel effectief te doorzoeken.

U kunt elk trefwoord in de filterbalk invoegen en het systeem geeft de resultaten voor u door. Als er een vereiste is om de signatuur te vinden voor Secure Socket Layer (SSL) genegeerde kwetsbaarheid, kunt u sleutelwoord zoeken in de filterbar en zal het de handtekening voor de hartverscheurde kwetsbaarheid krijgen.

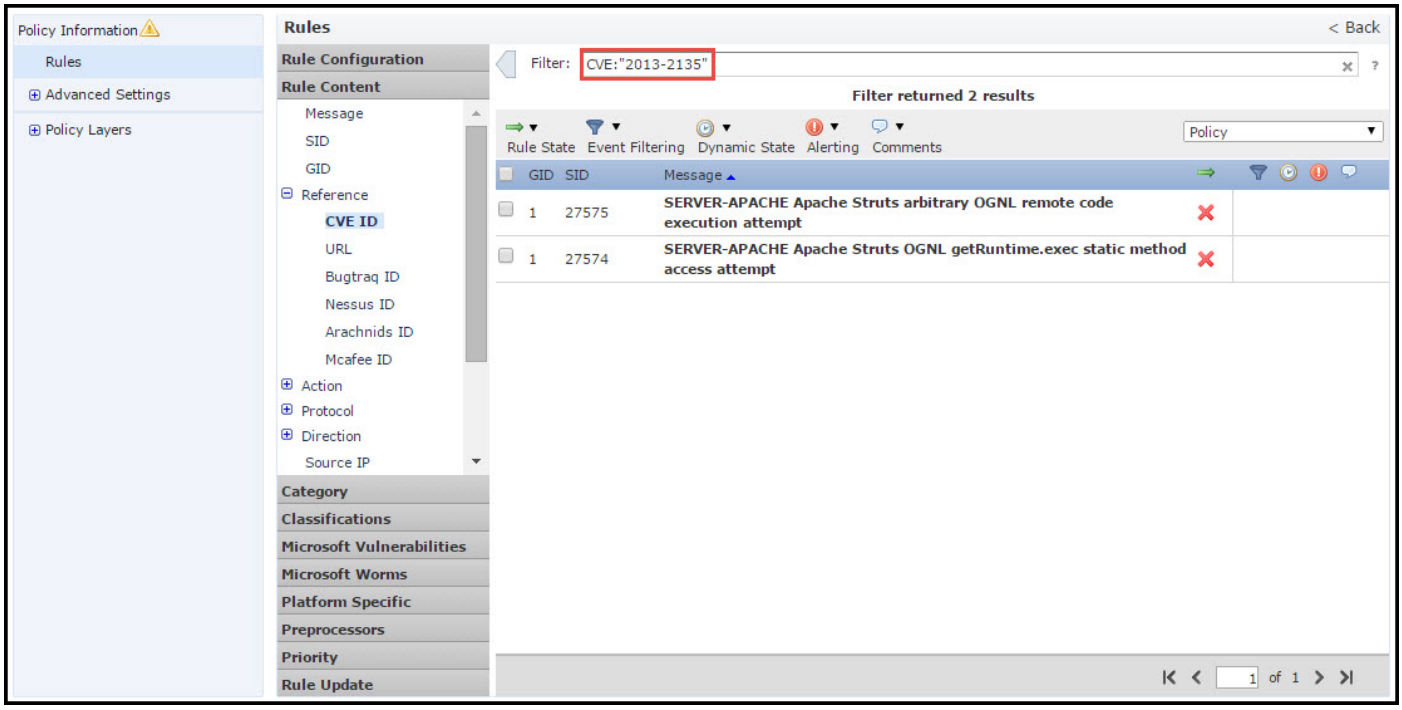
> **Tip**: Als in de filterbalk meerdere zoekwoorden worden gebruikt, combineert het systeem deze met behulp van EN met behulp van logica om een samengestelde zoekopdracht te maken.

U kunt de regels ook doorzoeken met Signature ID (SID), Generator-ID (GID) en Category: do enz.

De regels zijn effectief verdeeld in meerdere manieren zoals gebaseerd op categorie/classificaties/Microsoft kwetsbaarheden / Microsoft Wormen/Platform Specific. Een dergelijke associatie van regels helpt de klant om de juiste handtekening op een eenvoudige manier te verkrijgen en helpt de klant om de handtekeningen effectief aan te passen.



U kunt ook zoeken met CVE-nummer om de regels te vinden die op deze regels van toepassing zijn. U kunt de syntaxis van **CVE** gebruiken: **<cve-number>.**



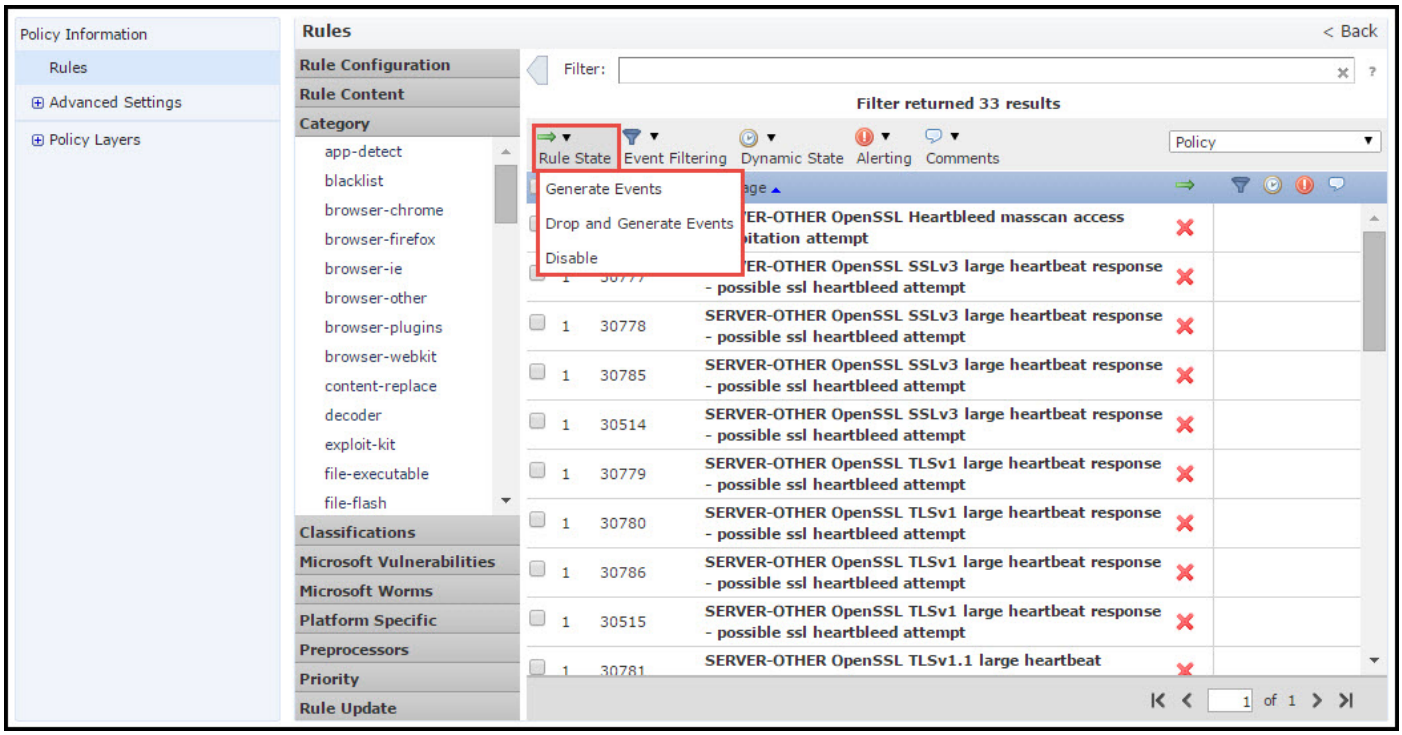
Stap 1.5. De regel instellen

Navigeren in om **Regels** optie in een navigatiedeelvenster en op een pagina met regelbeheer verschijnt. Selecteer de regels en kies optie **Regel State** om de status van de regels te configureren. Er zijn drie staten die voor een regel kunnen worden geconfigureerd:

1. **Evenementen genereren:** Deze optie genereert gebeurtenissen wanneer de regel overeenkomt met het verkeer.

2. **Drop and Generate Events:** Deze optie genereert gebeurtenissen en laat verkeer vallen wanneer de regel overeenkomt met het verkeer.

3. **Uitschakelen:** Deze optie schakelt de regel uit.



Stap 1.6. Configuratie van Event Filter

Het belang van een inbraakgebeurtenis kan worden gebaseerd op de frequentie van voorkomen, of op de bron of het bestemming IP-adres. In sommige gevallen kunt u zich geen zorgen maken over een gebeurtenis totdat deze een bepaald aantal keren heeft plaatsgevonden. U maakt zich bijvoorbeeld mogelijk geen zorgen als iemand probeert in te loggen op een server totdat een aantal keren is mislukt. In andere gevallen hoeft u alleen maar een paar gevallen van regelgeving te zien aanslaan om te controleren of er een wijdverbreid probleem is.

Er zijn twee manieren om dit te bereiken:

1. Drempel voor gebeurtenissen.

2. Voorvallen onderdrukken.

Drempel voor gebeurtenis

U kunt drempelwaarden instellen die bepalen hoe vaak een gebeurtenis wordt weergegeven, op basis van het aantal gebeurtenissen. U kunt de drempelwaarden per gebeurtenis en per beleid configureren.

Stappen om gebeurtenis Drempel te configureren:

Stap 1. Selecteer de **regel(en)** waarvoor u de drempelwaarde voor gebeurtenis wilt configureren.

Stap 2. Klik op het **Event Filtering**.

Stap 3. Klik op de **drempelwaarde**.

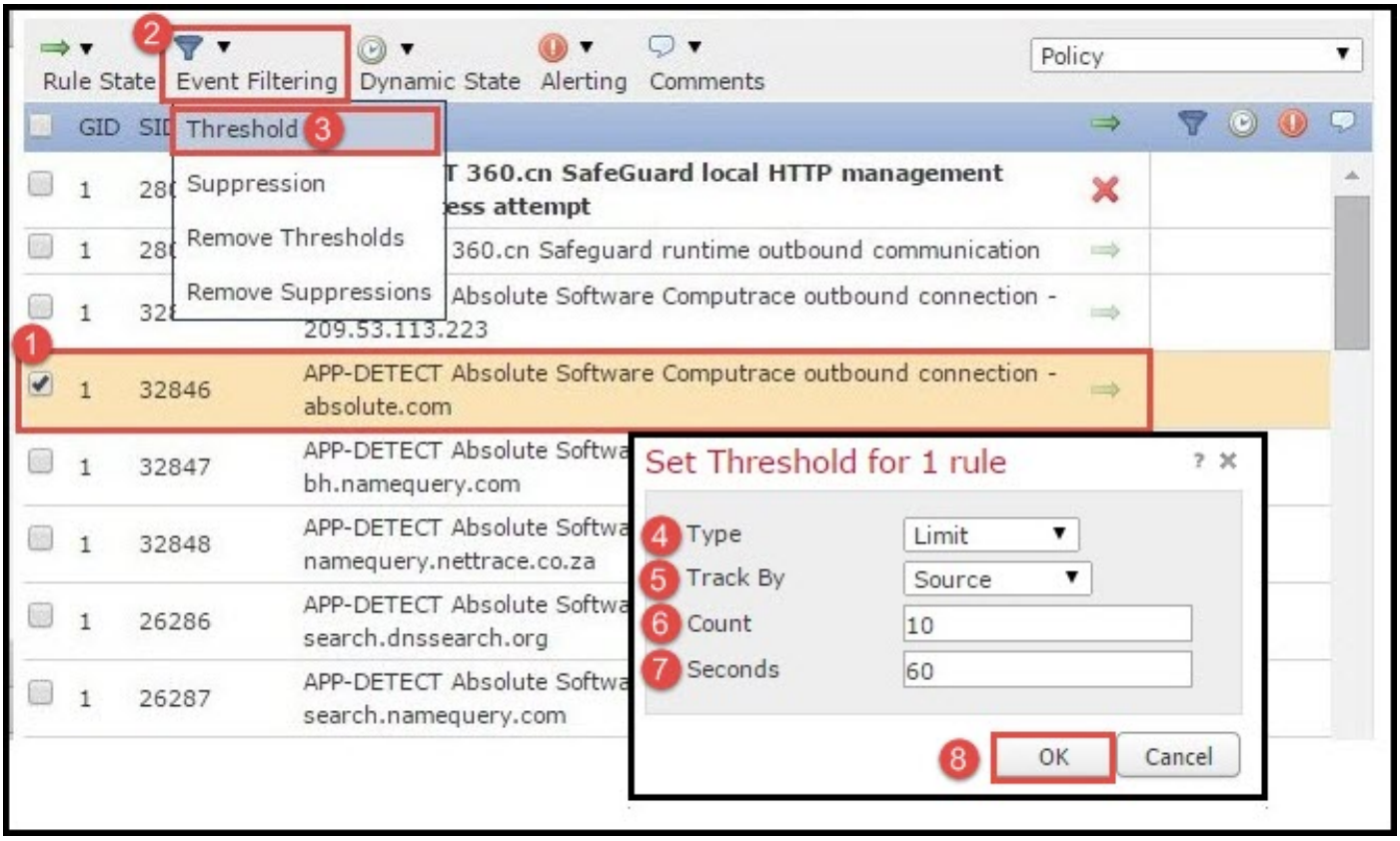
Stap 4. Selecteer het **type** in de vervolgkeuzelijst. (Limiet of drempel of beide).

Stap 5. Selecteer hoe u vanaf **Train** bij uitrolvak wilt volgen. (Bron of bestemming).

Stap 6. Voer het **aantal** gebeurtenissen in om de drempel te halen.

Stap 7. Voer de te verlopen **seconden** in voordat de telfunctie opnieuw wordt ingesteld.

Stap 8. Klik op **OK** om dit te voltooien.



Nadat een filter aan een regel is toegevoegd, dient u een filterpictogram naast de regelindicatie te kunnen zien, waaruit blijkt dat er een filter is dat voor deze regel is ingeschakeld.

Event Super

Meldingen van specifieke gebeurtenissen kunnen worden onderdrukt op basis van IP-adres van bron/bestemming of per regel.

Opmerking: Wanneer u voor een regel gebeurtenis suppressie toevoegt. De inspectie van handtekeningen werkt zoals gewoonlijk, maar het systeem genereert de gebeurtenissen niet indien het verkeer overeenkomt met de handtekening. Als u een specifieke bron/bestemming specificeert, verschijnen de gebeurtenissen niet alleen voor de specifieke bron/bestemming voor deze regel. Als u ervoor kiest de volledige regel te onderdrukken dan genereert het systeem geen gebeurtenis voor deze regel.

Stappen om gebeurtenis Drempel te configureren:

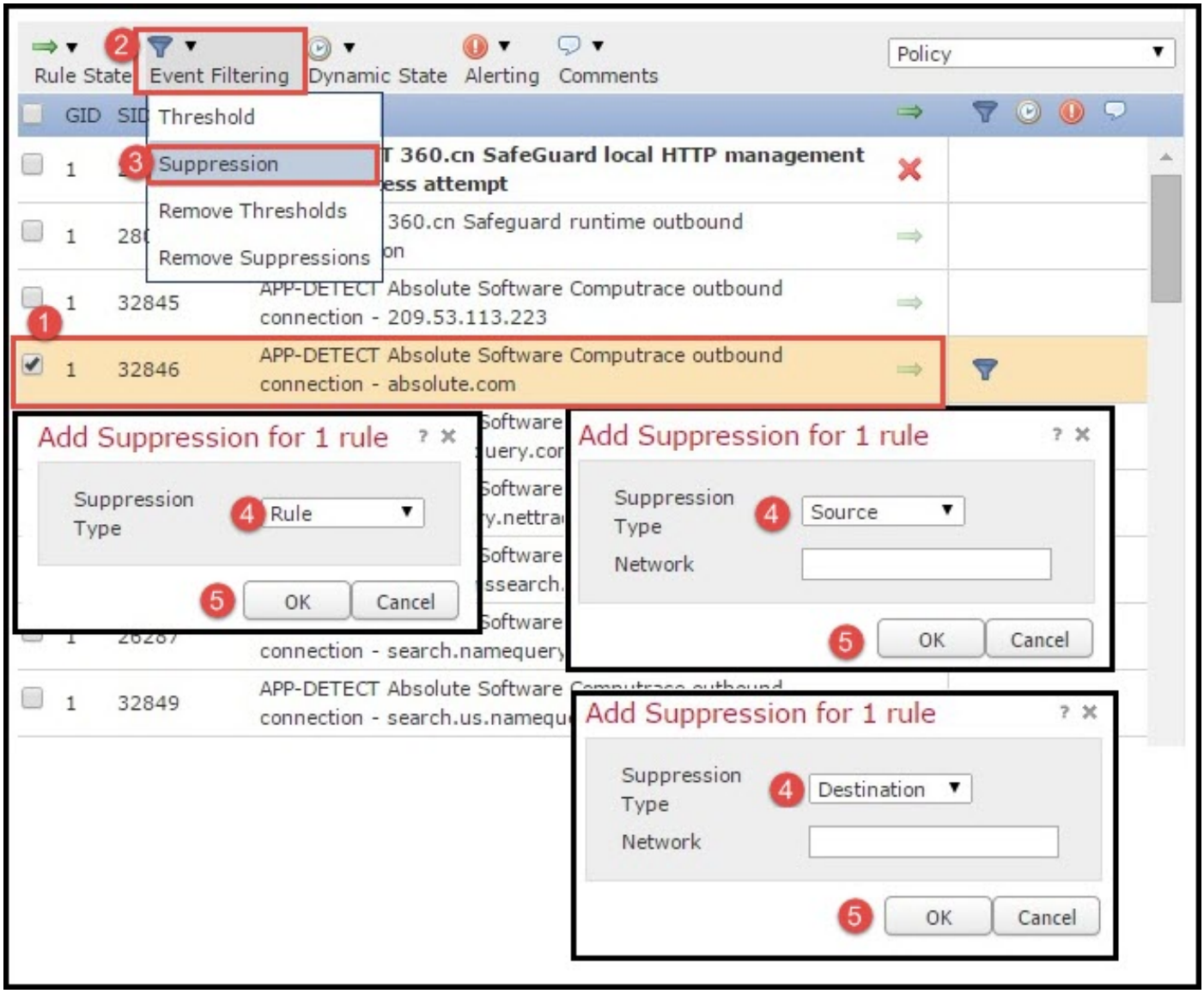
Stap 1. Selecteer de **regel(en)** waarvoor u de Event Drempel wilt configureren.

Stap 2. Klik op **Event Filtering**.

Stap 3. Klik op **Suppression.**

Stap 4. Selecteer **het type onderdrukking** in de vervolgkeuzelijst. (regel of bron of bestemming).

Stap 5. Klik op **OK** om dit te voltooien.



Nadat het filter van de gebeurtenis aan deze regel wordt toegevoegd, zou u een filterpictogram moeten kunnen zien met telling twee naast de regelindicatie, die toont dat er twee van de gebeurtenissen filters voor deze regel zijn ingeschakeld.

Stap 1.7. Dynamische toestand configureren

Het is een eigenschap waar we de staat van een regel kunnen veranderen als de gespecificeerde voorwaarde aansluit.

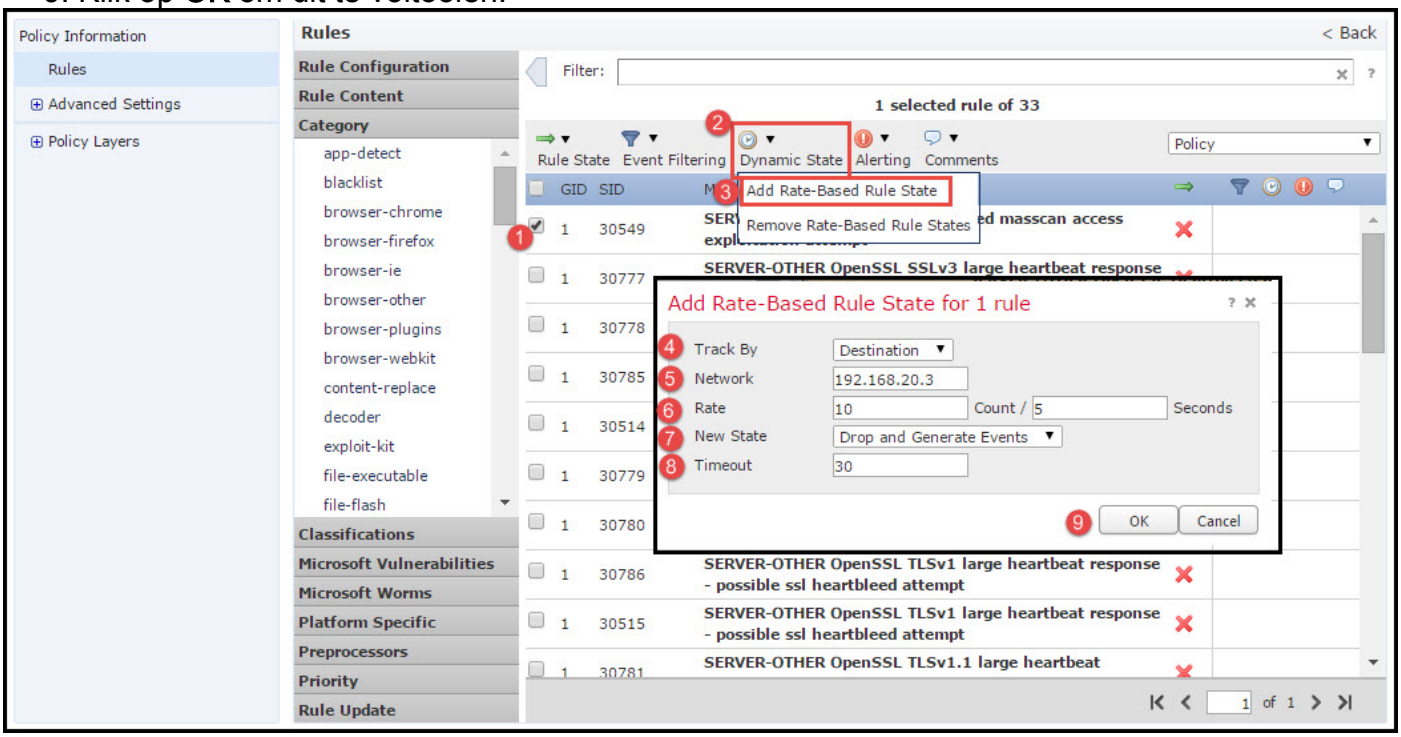
Stel een scenario van brute krachtaanval voor om het wachtwoord te kraken. Als een signatuur een wachtwoord herkent, faalt de poging en de regelactie is om een gebeurtenis te genereren. Het systeem blijft de waarschuwing genereren voor een wachtwoord faalpoging. Voor deze situatie kunt u de **Dynamische status** gebruiken waar een actie van **Generate Events** kan worden gewijzigd in **Drop en Generate Events** om de brute krachtaanval te blokkeren.

Navigeren in om **Regels** optie in een navigatiedeelvenster en op een pagina met regelbeheer verschijnt. Selecteer de regel waarvoor u de Dynamische status wilt in- en uitschakelen en opties **Dynamische status** kiest **> Een status op basis van snelheid toevoegen.**

U configureren als volgt een op snelheid gebaseerde regel:

1. Selecteer de **regel(en)** waarvoor u de drempelwaarde voor gebeurtenis wilt configureren.

2. Klik op de **Dynamische status**.
3. Klik op de **op Toevoegen gebaseerde regelstatus**.
4. Stel in hoe u de regelstatus wilt volgen vanuit het uitrolvak '**Train**'. (**regel of bron of bestemming**).
5. Voer het **netwerk in**. U kunt één enkel IP adres, adresblok, variabele of een komma-gescheiden lijst specificeren die uit om het even welke combinatie van deze bestaat.
6. Voer de **Count** van gebeurtenissen in en de timestamp in seconden.
7. Selecteer de **Nieuwe Staat,** u wilt definiëren voor de regel.
8. Voer de **Time-out in** waarna de status van de regel wordt teruggedraaid.
9. Klik op **OK** om dit te voltooien.



Stap 2. Configureer het beleid voor netwerkanalyse (NAP) en variabele reeksen (optioneel)

Beleid voor netwerkanalyse

Het beleid van de Toegang van het netwerk is ook gekend als preprocessoren. De preprocessor herassembleert en normaliseert het verkeer. Het helpt om netwerklaag en de protocol van de transportlaag anomalieën bij identificatie van ongepaste kopbalopties te identificeren.

NAP defragmentatie van IP datagrammen, verstrekt TCP stateful inspection en stream herassemblage en validatie van checksum. De preprocessor normaliseert het verkeer, valideert en verifieert de protocolstandaard.

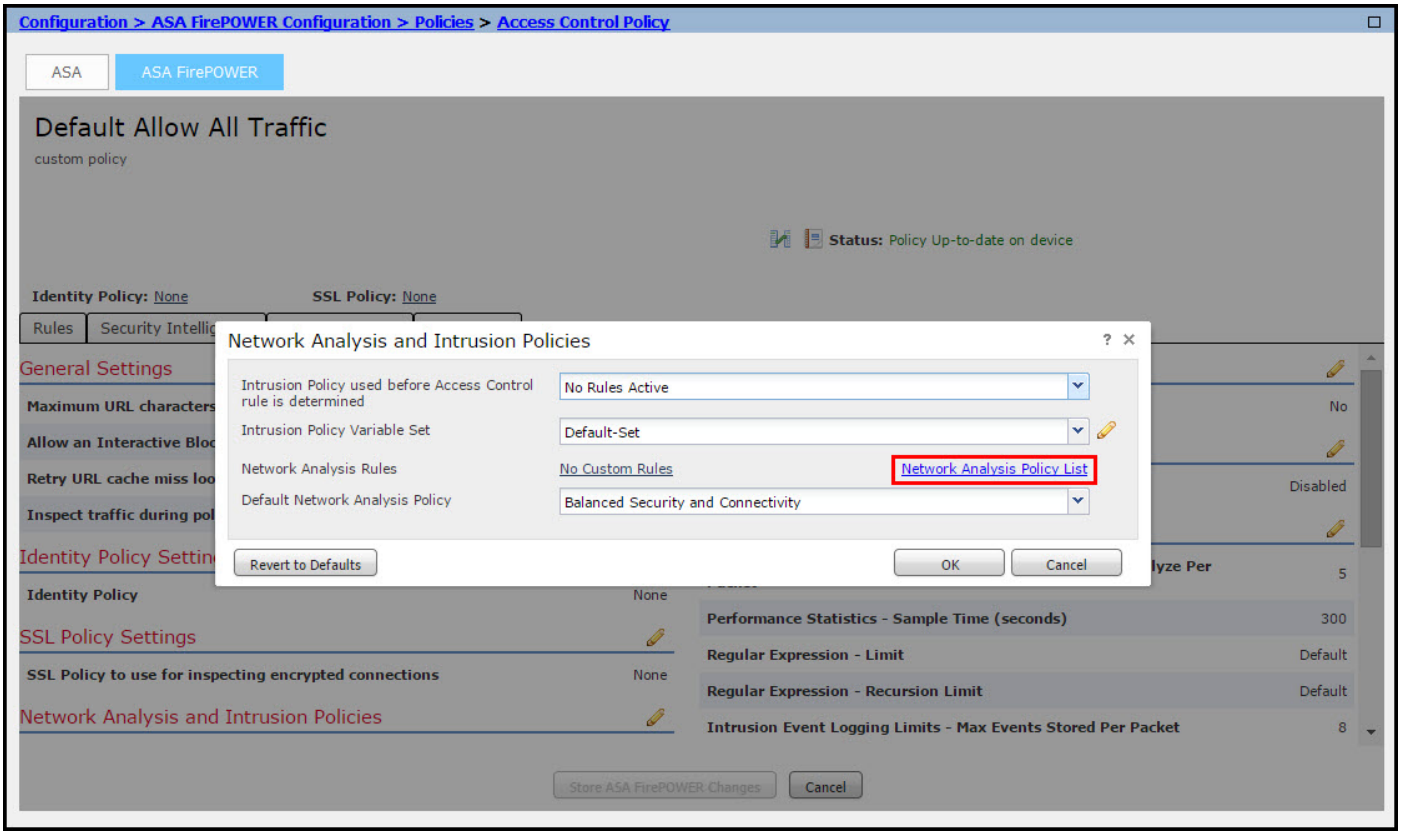
Elke preprocessor heeft zijn eigen GID-nummer. Het representeert welke preprocessor door het pakje is geactiveerd.

Om het beleid voor netwerkanalyse te configureren **navigeer** naar **configuratie > ASA FirePOWER Configuration > Policy > Access Control Policy > Advanced > Network Analysis and Inbraakbeleid**

Het beleid voor standaard netwerkanalyse is gebalanceerd voor beveiliging en connectiviteit, wat een optimaal aanbevolen beleid is. Er zijn nog drie andere systemen die het NAP-beleid bieden en

die uit de vervolgkeuzelijst kunnen worden geselecteerd.

Selecteer de optie **Network Analysis Policy** List om een aangepast NAP-beleid te maken.



Variabele reeksen instellen

Variabele sets worden gebruikt in inbraakregels om de bron- en doeladressen en -poorten te identificeren. Regels zijn effectiever wanneer variabelen de netwerkomgeving nauwkeuriger weergeven. Variabele speelt een belangrijke rol bij het afstemmen van prestaties.

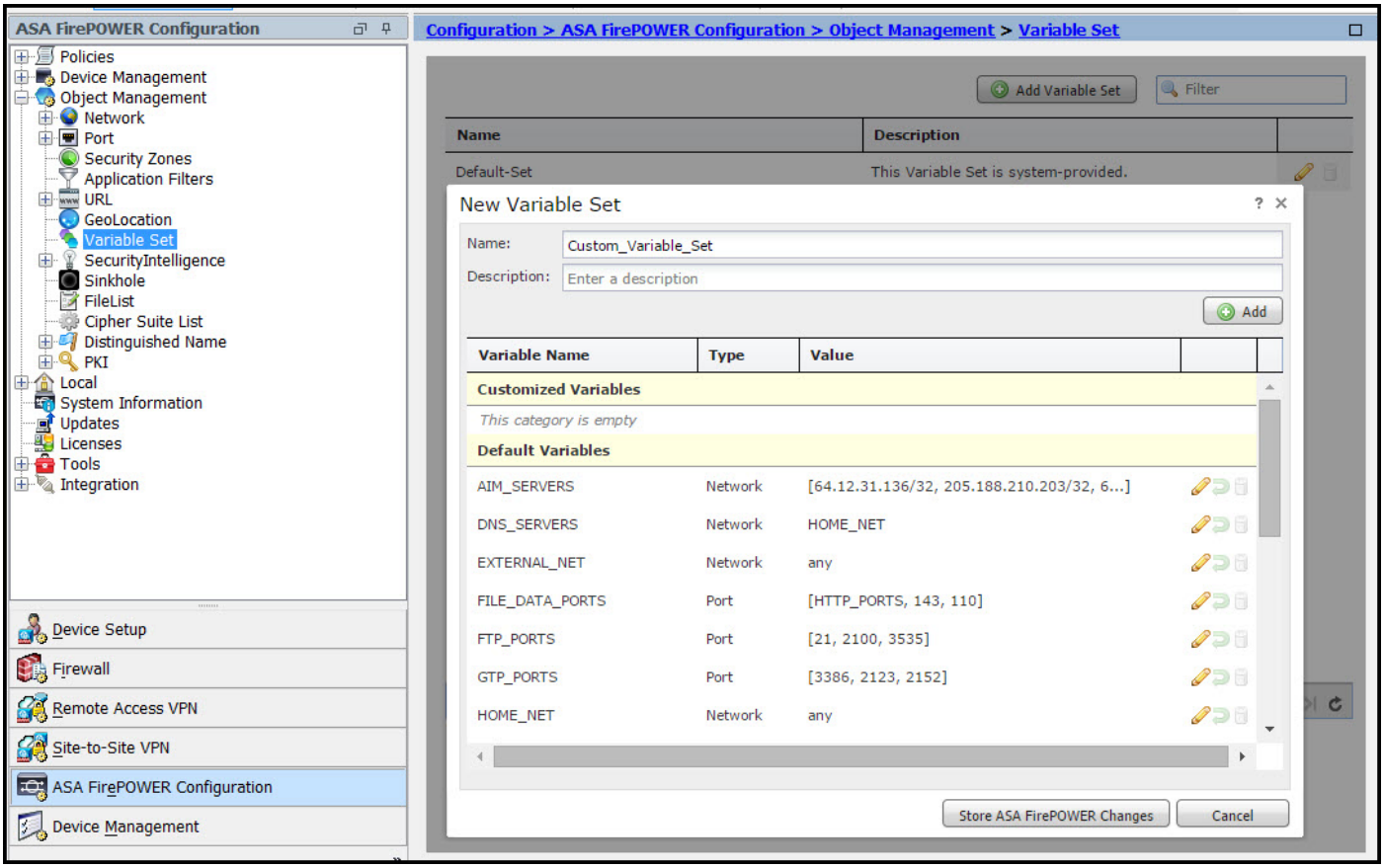
Variabele sets zijn al ingesteld met de standaardoptie (Netwerk/poort). Voeg nieuwe Variabele reeksen toe als u de standaardconfiguratie wilt veranderen.

Om de variabelen te configureren **navigeer** naar **Configuratie > ASA Firepower Configuration > Objectbeheer > Variable Set**. Selecteer optie **Variabele set toevoegen** om nieuwe variabele sets toe te voegen. Typ de **naam** van de variabele en specificeer de **beschrijving.**

Als een aangepaste toepassing op een bepaalde poort werkt, definieert u het poortnummer in het veld Poortnummer. Configuratie van de netwerkparameter.

$Home_NET specificeert het interne netwerk.

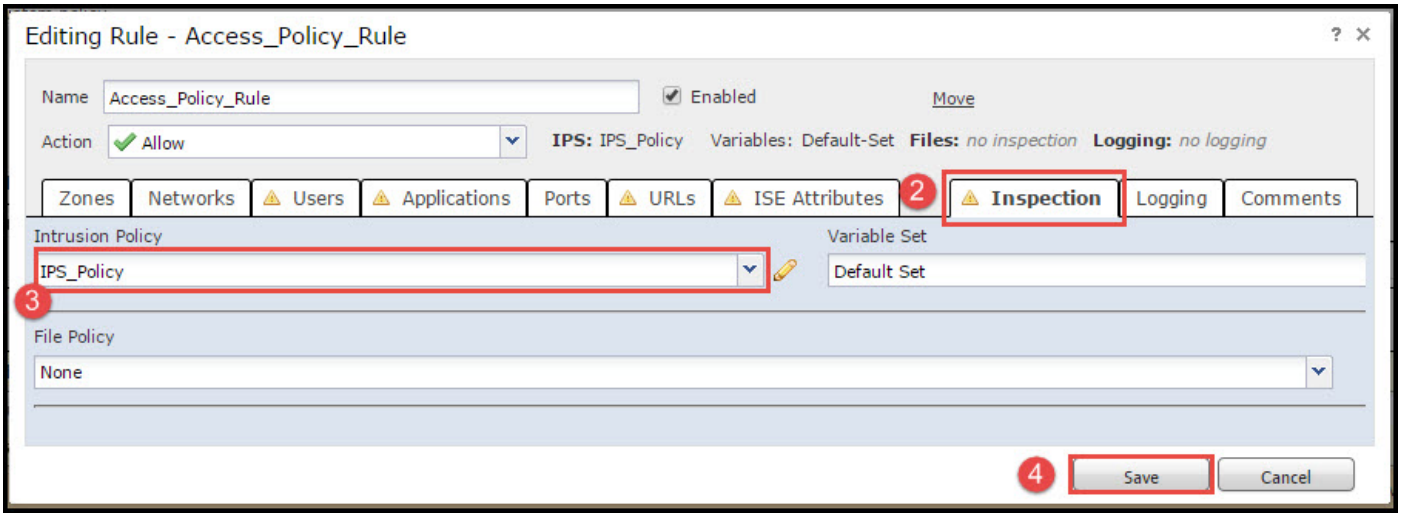
$Extern_NET specificeert het externe netwerk.



Stap 3: Het instellen van toegangscontrole om inbraakbeleid/NAP/Variable sets op te nemen

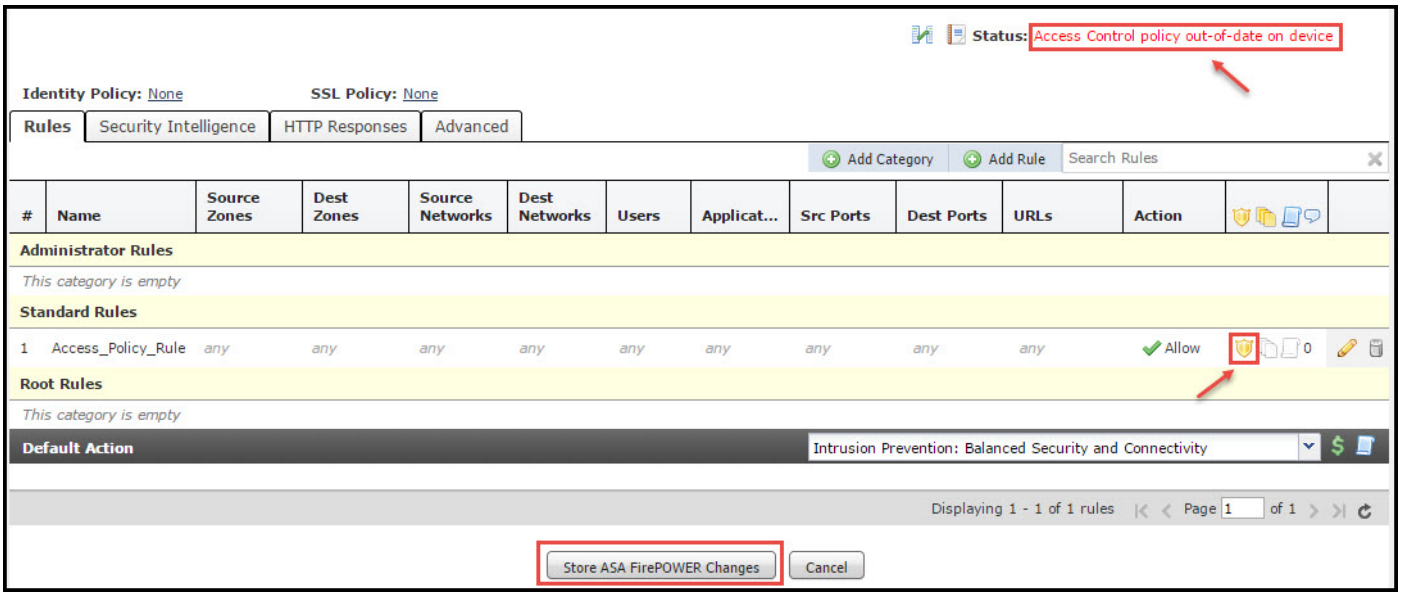
Navigeer naar **Configuratie > ASA Firepower Configuration > Policy > Access Control Policy.** U moet deze stappen voltooien:

1. Bewerk de regel Toegangsbeleid waar u het inbraakbeleid wilt toewijzen.
2. Kies het tabblad **Inspectie.**
3. Kies het **Inbraakbeleid** in de vervolgkeuzelijst en kies de **Variabele** reeks
4. Klik op **Opslaan**.



Omdat een inbraakbeleid aan deze regel van het toegangsbeleid is toegevoegd. U kunt het

schermpictogram zien in Gouden Kleur die aangeeft dat het inbraakbeleid is ingeschakeld.

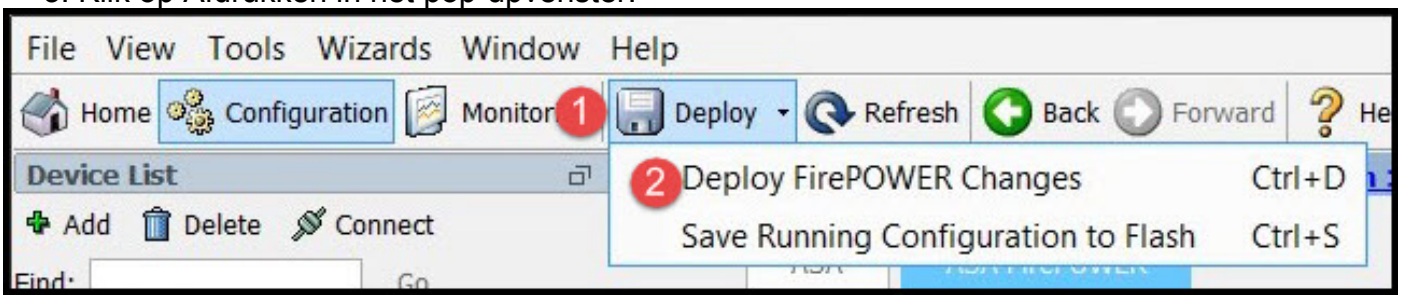


Klik op **Store ASA FirePOWER om** de wijzigingen op te slaan.

Stap 4. Beleidsmaatregelen voor toegangscontrole implementeren

Nu moet je het toegangscontrolebeleid inzetten. Voordat u het beleid toepast, ziet u een indicatie Toegangsbeheer beleid achterhaald op het apparaat. Om de wijzigingen in de sensor in te voeren:

1. Klik op **Uitvoeren**.
2. Klik op **FirePOWER-wijzigingen implementeren**.
3. Klik op Afdrukken in het pop-upvenster.

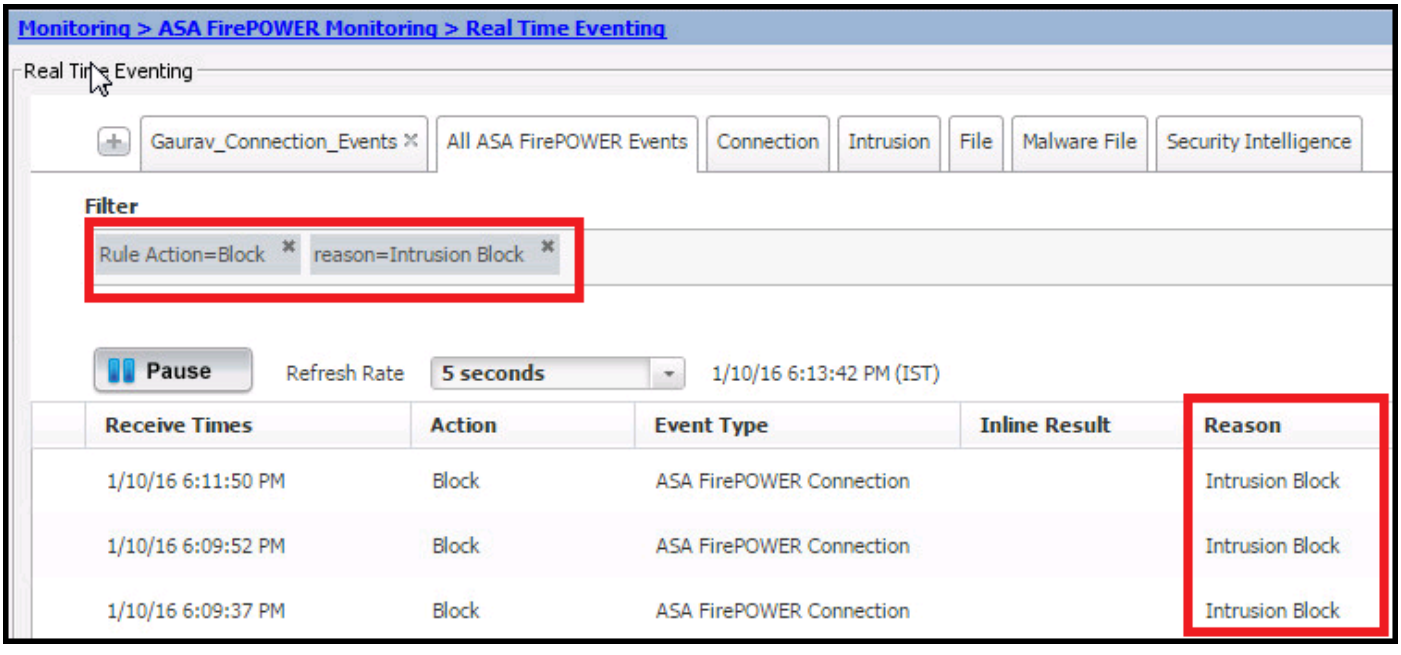


Opmerking: In versie 5.4.x, om het toegangsbeleid op de sensor toe te passen, moet u ASA FirePOWER Wijzigingen toepassen

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

Stap 5. Controleer de inbraakgebeurtenissen

Om de inbraakgebeurtenissen te zien die door de FirePOWER-module zijn gegenereerd, navigeer naar **Bewaking > ASA FirePOWER-bewaking > Real-time ultimo.**



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Stap 1. Zorg ervoor dat de regels van de Commissie correct zijn opgesteld.

Stap 2. Zorg ervoor dat het juiste IPS-beleid is opgenomen in de toegangsregels.

Stap 3. Zorg ervoor dat de sets variabelen correct zijn geconfigureerd. Als de variabelen niet correct zijn ingesteld, komen de handtekeningen niet overeen met het verkeer.

Stap 4. Zorg ervoor dat de implementatie van het toegangscontrolebeleid met succes voltooid is.

Stap 5. Controleer de verbindingsgebeurtenissen en inbraakgebeurtenissen om te controleren of de verkeersstroom de juiste regel heeft of niet.

Gerelateerde informatie

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