Begrijp de regeluitbreiding op FirePOWER-apparaten

Inhoud

Inleiding

In dit document wordt de vertaling van de toegangscontroleregels naar de sensor beschreven wanneer deze vanuit het FireSIGHT Management Center (FMC) wordt gebruikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van vuurstechnologie
- Kennis over het configureren van toegangscontrolebeleid op FMC

Gebruikte componenten

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

- Firepower Management Center versie 6.0.0 en hoger
- ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5555-X, ASA 5585-X) software versie 6.0.1 en hoger

- ASA Firepower SFR Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) met actieve softwareversie 6.0.0 en hoger

- Firepower 7000/8000 Series sensorversie 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

Een toegangscontroleregel wordt gecreëerd met het gebruik van een of meerdere combinaties van deze parameters:

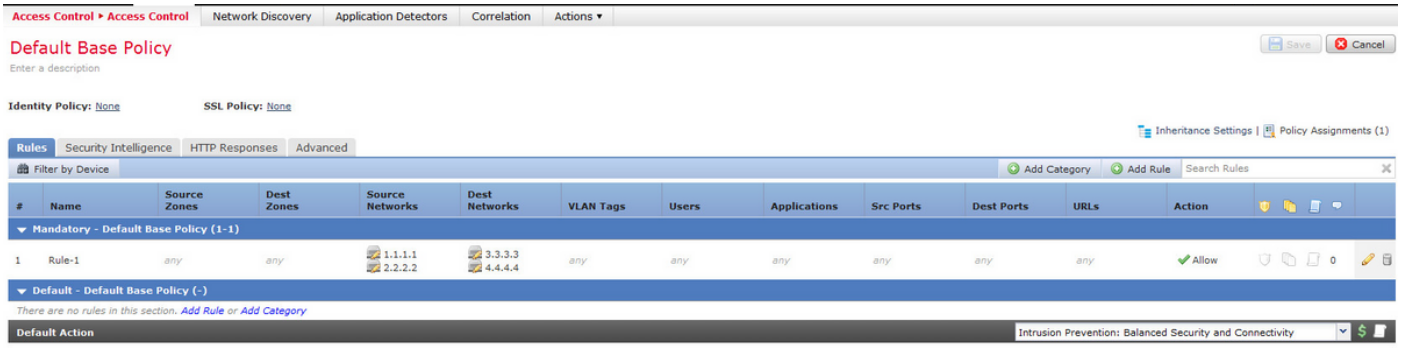
- IP-adres (bron en bestemming)
- Poorten (bron en bestemming)
- URL (systeemrelevante categorieën en aangepaste URL's)
- Toepassingsdetectie
- VLAN's
- Zones

Gebaseerd op de combinatie van parameters gebruikt in de toegangsregel, verandert de regelexpansie op de sensor. In dit document worden verschillende combinaties van regels voor het VCC en de daarmee verband houdende uitbreidingen van de sensoren beschreven.

Uitbreiding van regels begrijpen

Uitbreiding van een IP-gebaseerde regel

Overweeg de configuratie van een toegangsregel van het FMC, zoals getoond in de afbeelding:



Dit is één regel voor het Management Center. Nadat het in de sensor is geplaatst, breidt het zich echter uit in **vier** regels zoals weergegeven in het beeld:

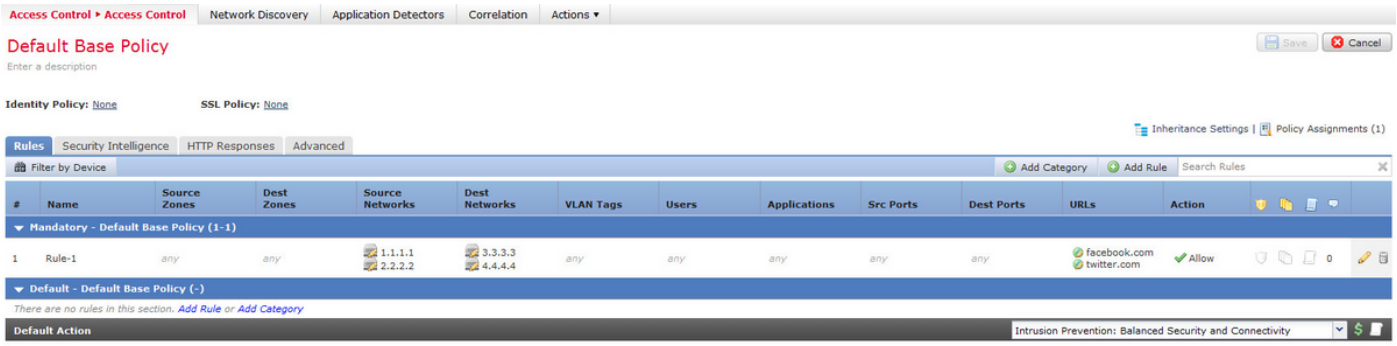
```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Wanneer u een regel implementeert met twee sub die als Bron en twee hosts zijn ingesteld als doeladressen, wordt deze regel uitgebreid tot vier regels op de sensor.

> Opmerking: Als de vereiste is om toegang op basis van doelnetwerken te blokkeren, is een betere manier om dit te doen het gebruiken van de eigenschap van Blacklist onder Security Intelligence.

Uitbreiding van een IP-gebaseerde regel met aangepaste URL

Overweeg de configuratie van een toegangsregel van het FMC zoals getoond in de afbeelding:



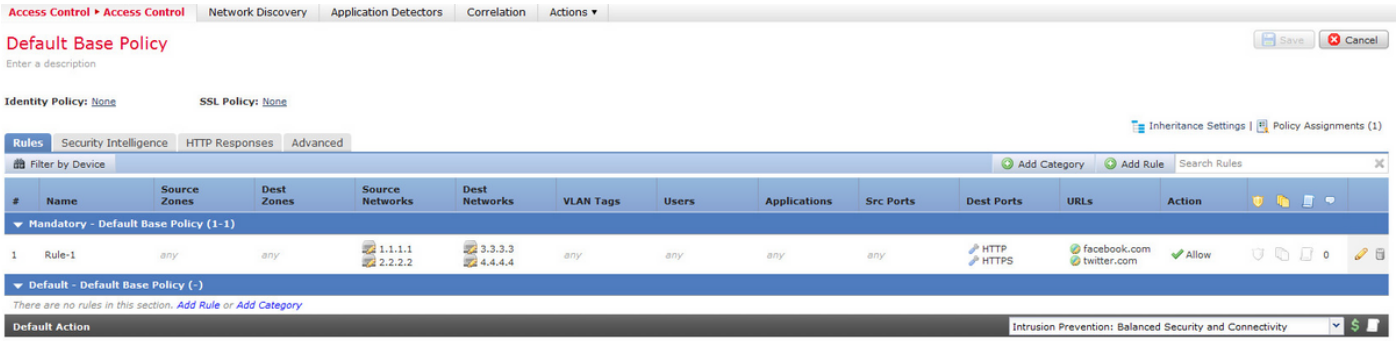
Dit is één regel voor het Management Center. Nadat het in de sensor is geïnstalleerd, wordt het in acht regels uitgebreid zoals in het beeld wordt getoond:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Wanneer u een regel implementeert met twee sub die als Bron zijn ingesteld, twee hosts ingesteld als doeladressen en twee aangepaste URL objecten in één enkele regel op het Management Center, wordt deze regel uitgebreid tot acht regels op de sensor. Dit betekent dat voor elke aangepaste URL categorie een combinatie van bron- en IP/poortbereik is, die worden geconfigureerd en gemaakt.

Uitbreiding van een IP-gebaseerde regel met poorten

Overweeg de configuratie van een toegangsregel van het FMC zoals getoond in de afbeelding:



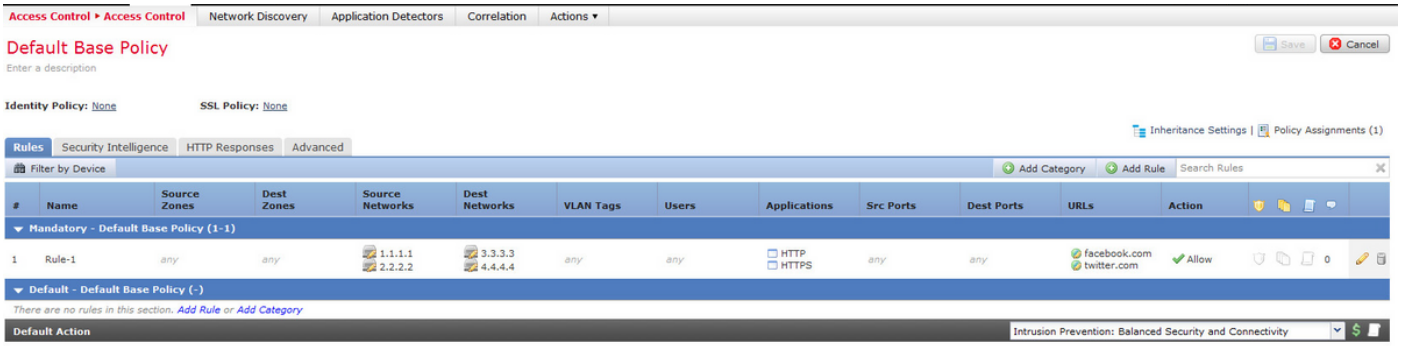
Dit is één regel voor het Management Center. Nadat het naar de sensor is geïmplementeerd, wordt het uitgebreid tot zestien regels zoals in het beeld:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any any any any any any any (ipspolicy 2)
```

Wanneer u een regel implementeert met twee subnets die als Bron worden gevormd, twee die als bestemmingsadressen en twee aangepaste URL voorwerpen die voorbestemd zijn om twee poorten in te zetten, breidt deze regel uit tot zestien regels over de sensor.

> **Opmerking**: Indien de havens in de toegangsregel moeten worden gebruikt, gebruik dan **toepassingsdetectoren** die aanwezig zijn voor standaardtoepassingen. Dit helpt reguliere expansie op een efficiënte manier te laten gebeuren.

Overweeg de configuratie van een toegangsregel van het FMC zoals getoond in de afbeelding:

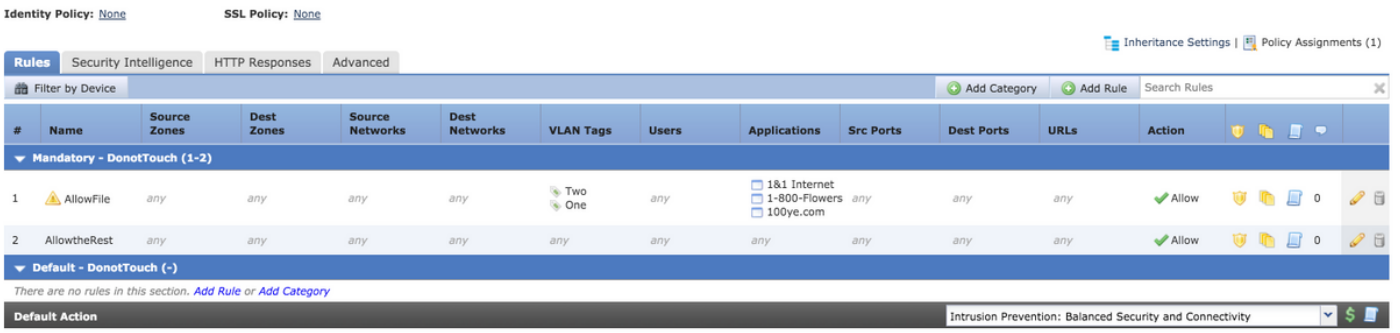


Wanneer u toepassingsdetectoren in plaats van havens gebruikt, wordt het aantal uitgebreide regels verminderd van zestien tot acht zoals in het beeld wordt weergegeven:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
```

Uitbreiding van een IP-gebaseerde regel met VLAN's

Overweeg de configuratie van een toegangsregel van het FMC zoals getoond in de afbeelding:



De regel **AllowFile** heeft één lijn die twee VLAN-bestanden met bepaalde toepassingsdetectoren, inbraakbeleid en bestandsbeleid aansluit. De regel AllowFile gaat uit naar twee regels.

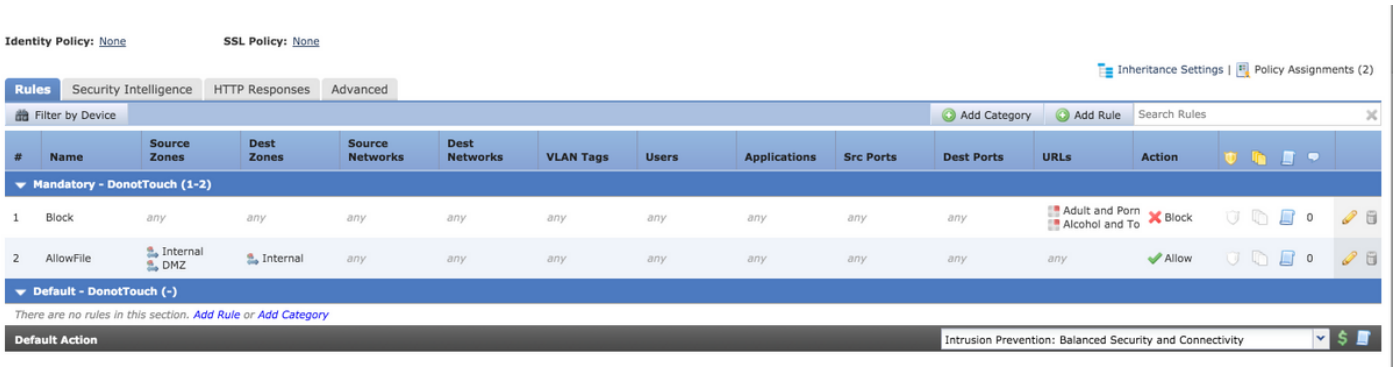
```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

Het IPS-beleid en het bestandbeleid zijn uniek voor elke toegangscontroleregel, maar meerdere toepassingsdetectoren worden in dezelfde regel verwezen en nemen dus niet deel aan de uitbreiding. Wanneer u een regel met twee ids van VLAN en drie toepassingsdetectoren

overweegt, zijn er slechts twee regels, één voor elk VLAN.

Uitbreiding van een IP-gebaseerde regel met URL-categorieën

Overweeg de configuratie van een toegangsregel van het FMC zoals getoond in de afbeelding:



De blokregel blokkeert URL-categorieën voor **volwassenen en pornografie Elke reputatie** en **alcohol- en tabaksreparatie 1-3.** Dit is één enkele regel voor het Management Center, maar wanneer je het in de sensor implementeert, wordt het uitgebreid tot twee regels, zoals in dit voorbeeld wordt getoond:

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep
le 60)
```

Wanneer u één enkele regel met twee die als Bron en twee die als bestemmingsadressen worden gevormd in, samen met twee aangepaste URL voorwerpen die voorbestemd zijn aan twee poorten met twee URL categorieën, zet deze regel uit tot tweeëndertig regels op de sensor.

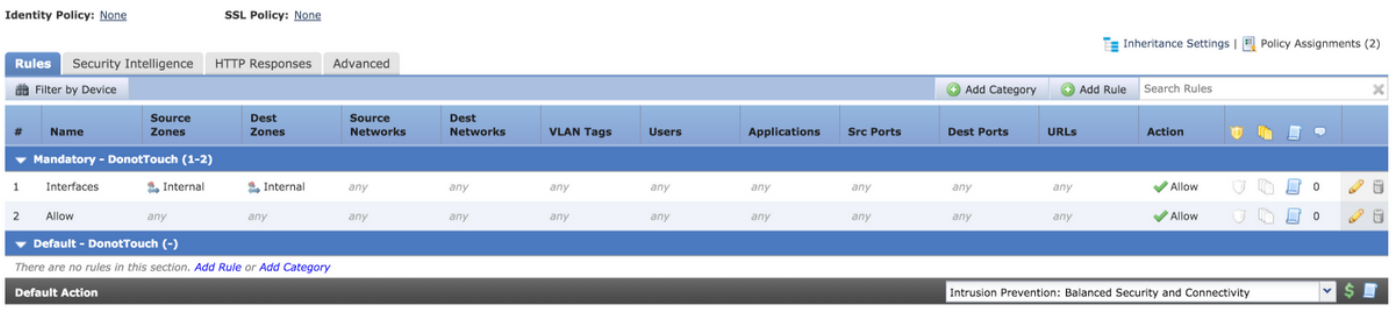
Uitbreiding van een IP-gebaseerde regel met zones

Zones zijn toegewezen nummers die in beleid worden vermeld.

Als een zone in een beleidsgebied wordt genoemd maar die zone niet wordt toegewezen aan een interface op het apparaat waarop het beleid wordt geduwd, wordt de zone beschouwd als een **gebied** en **elke zone** leidt niet tot uitbreiding van de regels.

Indien de bronzone en de bestemmingszone dezelfde zijn in de regel, wordt zonefactor als **elke** andere beschouwd en wordt slechts één regel toegevoegd, aangezien ELKE zone niet leidt tot uitbreiding van de regels.

Overweeg de configuratie van een toegangsregel van het FMC zoals getoond in de afbeelding:



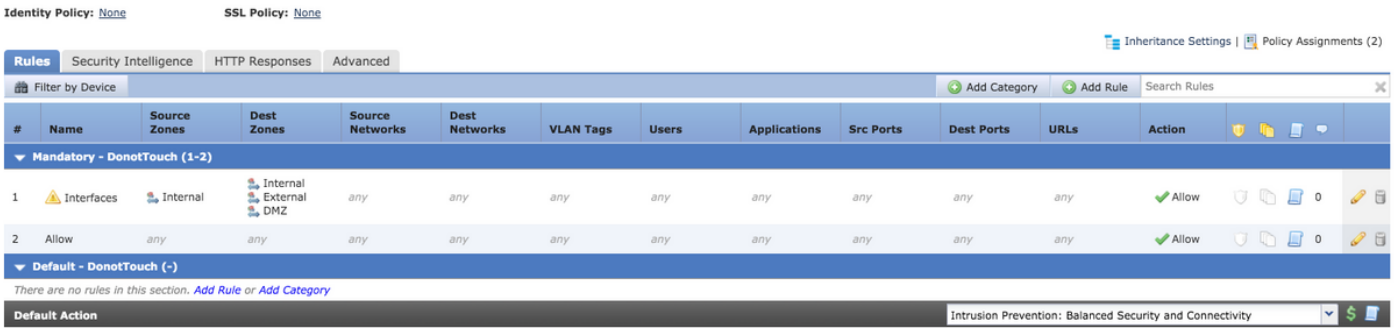
Er zijn twee regels. Eén regel heeft zones ingesteld, maar de bron- en doelzone zijn hetzelfde. De andere regel heeft geen specifieke configuratie. In dit voorbeeld vertaalt de toegangsregel **Interfaces** niet in een regel.

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
---Default Intrusion Prevention Rule
```

Op de sensor lijken beide regels hetzelfde omdat zonegebaseerde controle met dezelfde interfaces niet leidt tot een uitbreiding.

Uitbreiding van regels voor toegang tot zone-gebaseerde toegangscontroleregel gebeurt wanneer de zone waarnaar in de regel wordt verwezen wordt toegewezen aan een interface op het apparaat.

Overweeg de configuratie van een toegangsregel van het VCC zoals hieronder wordt getoond:



De regel Interfaces omvatten zone-gebaseerde regels met bronzone als interne en bestemmingszones als interne, externe en DMZ. In deze regel worden de interface-zones van Internet en van DMZ ingesteld op de interfaces en bestaat de Extern niet op het apparaat.Dit is de uitbreiding van hetzelfde:

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal
to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access
rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
-Default Intrusion Prevention: Balanced Security over Connectivity
```

Er wordt een regel gemaakt voor een specifiek interface-paar dat **intern > DMZ** is met een duidelijke zone specificatie en er wordt geen **interne > interne** regel gemaakt.

Het aantal regels dat wordt uitgebreid is evenredig aan het aantal zonnecentrales en doelparen

dat kan worden gecreëerd voor **geldige** geassocieerde gebieden en dit omvat dezelfde bron- en doelzoneregels.

> Opmerking: Gehandicapte regels van het VCC worden niet verspreid en niet uitgebreid naar de sensor tijdens de uitzetting van het beleid.

Algemene formule voor de uitbreiding van de regel

Aantal regels voor de sensor = (aantal bronsubnetten of hosts) * (aantal bestemmingen S) * (aantal bronpoorten) * (aantal doelpoorten) * (aantal aangepaste URL's)* (aantal VLAN-tags)* (aantal URL-categorieën)* (aantal geldige bron- en doelzoneparen)

> Opmerking: Voor de berekeningen wordt **elke** waarde in het veld vervangen door 1.De waarde **welke** dan ook in de rechtscombinatie wordt beschouwd als 1 en verhoogt of verruimt de regel niet.

implementatiefout van probleemoplossing door bestuursuitbreiding

Wanneer er sprake is van een uitzettingsstoring nadat de toegangsregel is aangevuld, volgt u de onderstaande stappen voor de gevallen waarin de limiet voor uitbreiding van de regel is bereikt

Controleer het **/var/log/action.queue.log** voor berichten met de volgende trefwoorden:

Fout - te veel regels - schrijfregel 28, max. regels 9094

Het bovenstaande bericht geeft aan dat er een probleem is met het aantal regels dat wordt uitgebreid. Controleer de configuratie op de FMC om de regels te optimaliseren op basis van de hierboven besproken scenario's.

Gerelateerde informatie

- Firepower Management Center Configuration Guide, versie 6.0
- Technische ondersteuning en documentatie – Cisco Systems