Controleer de aangepaste SID-lijst van FirePOWER-sensoren met CLI en FMC GUI

Inleiding

Dit document beschrijft hoe u een aangepaste SID-lijst kunt krijgen van Firepower Threat Defense (FTD) of FirePOWER-module met behulp van CLI en FMC GUI. De informatie van SID kan op FMC GUI worden gevonden als u naar *Voorwerpen > Inbraakregels* navigeert. In sommige gevallen is een lijst van beschikbare SID's van het CLI noodzakelijk.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco Firepower Threat Defense (FTD)
- Cisco ASA met FirePOWER-services
- Cisco FireSIGHT Management Center (FMC)
- Linux-basiskennis

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversie:

- Firepower Management Center 6.6.0
- Firepower Threat Defense versie 6.4.0.9
- FirePOWER-module 6.2.3.2

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

Een *inbraakregel* is een reeks sleutelwoorden en argumenten die het systeem gebruikt om pogingen te detecteren om kwetsbaarheden op uw netwerk te exploiteren. Aangezien het systeem netwerkverkeer analyseert, vergelijkt het pakketten met de voorwaarden in elke regel die worden gespecificeerd. Als de pakketgegevens overeenkomen met alle voorwaarden die in een regel zijn gespecificeerd, wordt de regel geactiveerd. Als een regel een alarmregel is, genereert deze een inbraakgebeurtenis. Als het om een pass-regel gaat, negeert hij het verkeer. Voor een lagere regel in een inline plaatsing, laat het systeem het pakket vallen en genereert een gebeurtenis. U kunt inbraakgebeurtenissen vanuit de webconsole van het FireSIGHT Management Center bekijken en evalueren.

Het Firepower System biedt twee soorten inbraakregels: *gedeelde objectregels* en

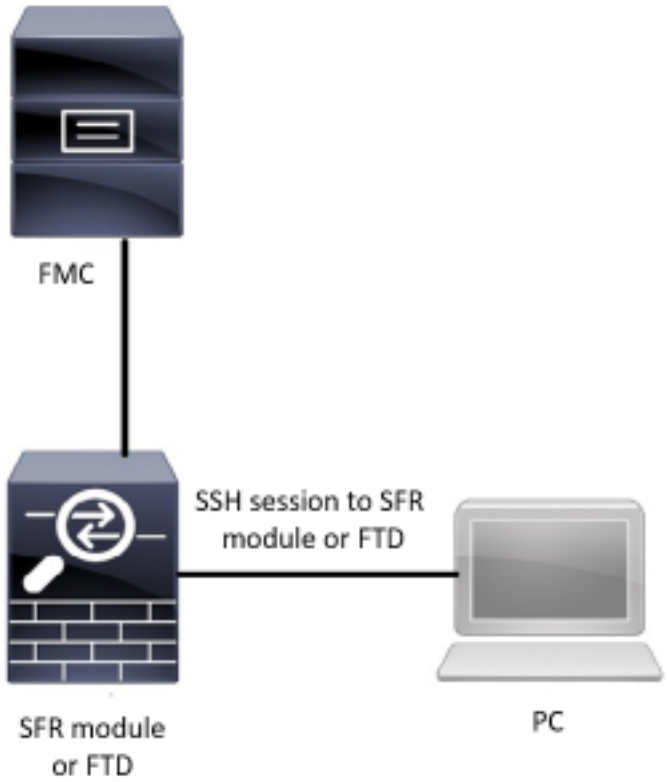
standaardtekstregels. De Cisco Talos Security Intelligence and Research Group (Talos) kan gedeelde objectregels gebruiken om aanvallen op kwetsbaarheden te detecteren op manieren waarop traditionele standaard tekstregels niet kunnen worden toegepast. Het is niet mogelijk om gedeelde objectregels te maken. Wanneer de inbraakregels op uw eigen computer geschreven zijn, moet er een standaard tekstregel gemaakt worden. Aangepaste standaard tekstregels voor het aanpassen van de soorten gebeurtenissen die u waarschijnlijk zult zien. Door regels te schrijven en het de gebeurtenis bericht van de regel te specificeren, kunt u makkelijker verkeer identificeren dat aanvallen en beleidsontduikingen betekent.

Wanneer u een aangepaste standaardtekstregel in een beleid van het op- en inbraakbeleid toelaat, houd in gedachten dat sommige regelsleutelwoorden en argumenten vereisen dat het verkeer eerst op een bepaalde manier wordt gedecodeerd of voorverwerkt.

Een *aangepaste lokale regel* op een FirePOWER-systeem is een aangepaste standaardregel voor snort die u in een ASCII-tekstformaat uit een lokale machine importeert. Met een FirePOWER-systeem kunt u lokale regels importeren via de webinterface. De stappen om lokale regels in te voeren zijn heel eenvoudig. Om echter een optimale lokale regel te kunnen schrijven, heeft een gebruiker diepgaande kennis nodig van de SNA- en netwerkprotocollen.

> **Waarschuwing**: Zorg ervoor dat u een beheerste netwerkomgeving gebruikt om inbraakregels te testen die u schrijft voordat u de regels in een productieomgeving gebruikt. Slecht geschreven inbraakregels kunnen de prestaties van het systeem ernstig schaden

Netwerkdiagram

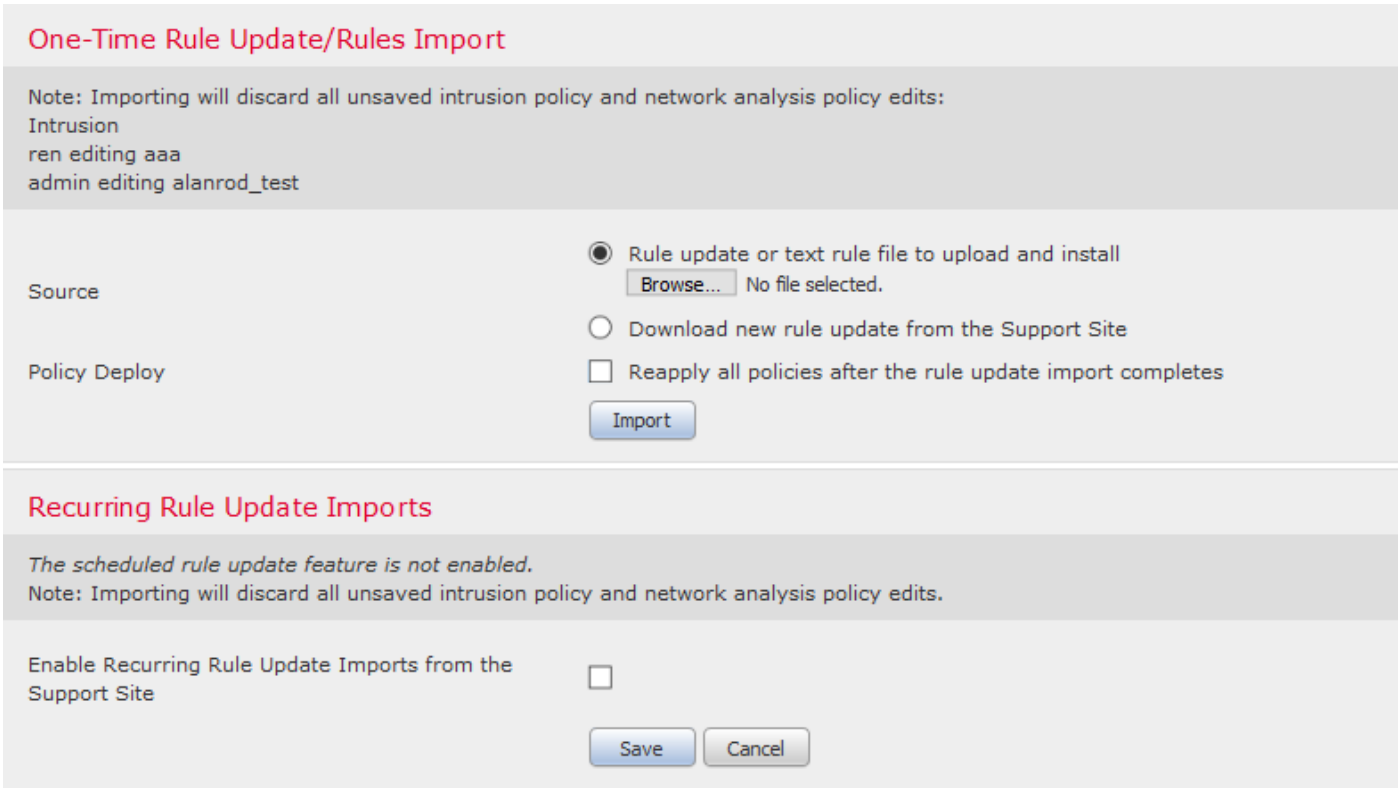


Configureren

Lokale regels importeren

Voordat u begint, moet u ervoor zorgen dat de regels in uw aangepaste bestand geen speciale tekens bevatten. De regel importeur vereist dat alle douaneregels worden ingevoerd met behulp van ASCII of UTF-8 encodering. De onderstaande procedure verklaart hoe u lokale standaardtekstregels uit een lokale machine kunt importeren.

Stap 1 . Toegang tot het tabblad **Importieregels** door naar **objecten te** navigeren **> Inbraakregels > Importieregels.** De pagina **Regelupdates** wordt weergegeven in de onderstaande afbeelding:



Stap 2. Selecteer **Regel update of tekstregelbestand om te uploaden en te installeren** en klik op **Bladeren** om het aangepaste regelbestand te selecteren

> Opmerking: Alle geüploade regels worden in de categorie **lokale regels** opgeslagen

Stap 3. Klik op **Importeren**. Het regelbestand wordt geïmporteerd

> **Opmerking**: De FirePOWER-systemen gebruiken de nieuwe regel niet die voor inspectie is ingesteld. Om een lokale regel in werking te stellen, moet u deze in het Inbraakbeleid inschakelen en het beleid vervolgens toepassen.

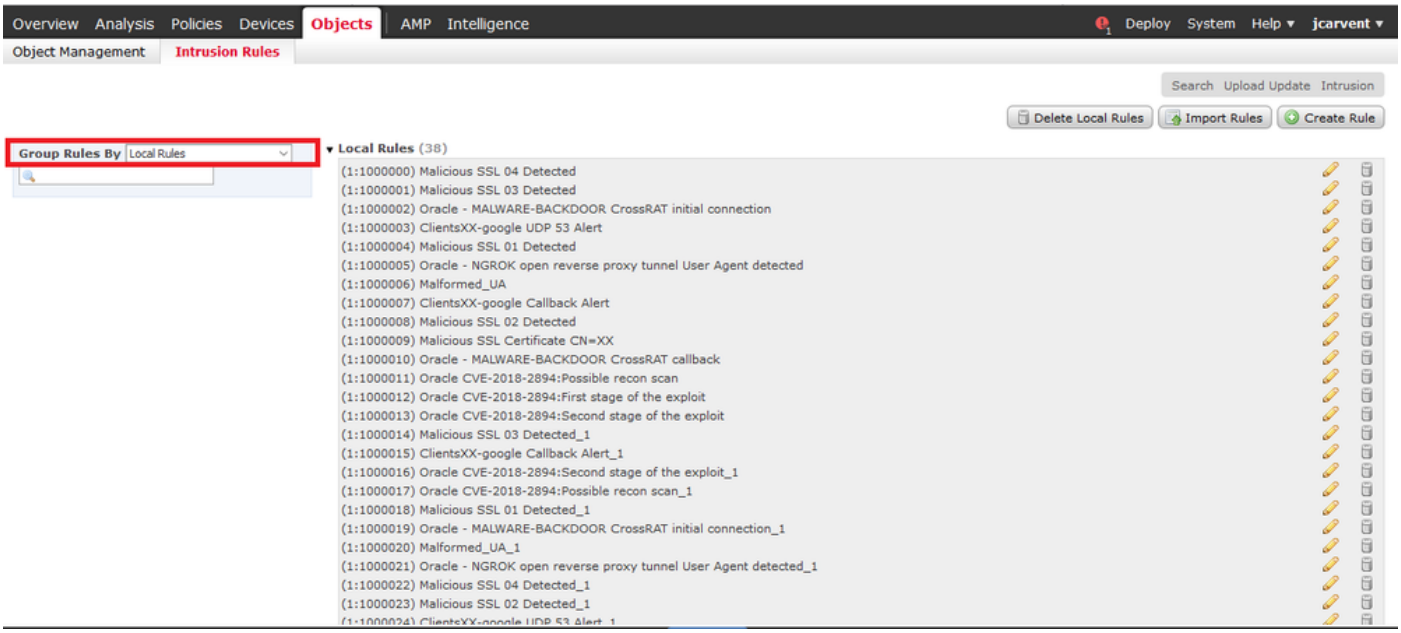
Verifiëren

Van FMC GUI

1. Bekijk lokale regels die zijn geïmporteerd vanuit FMC GUI

Stap 1. Navigeer naar **objecten > Inbraakregels**

Stap 2. Selecteer **Lokale regels** uit **groepsregels**



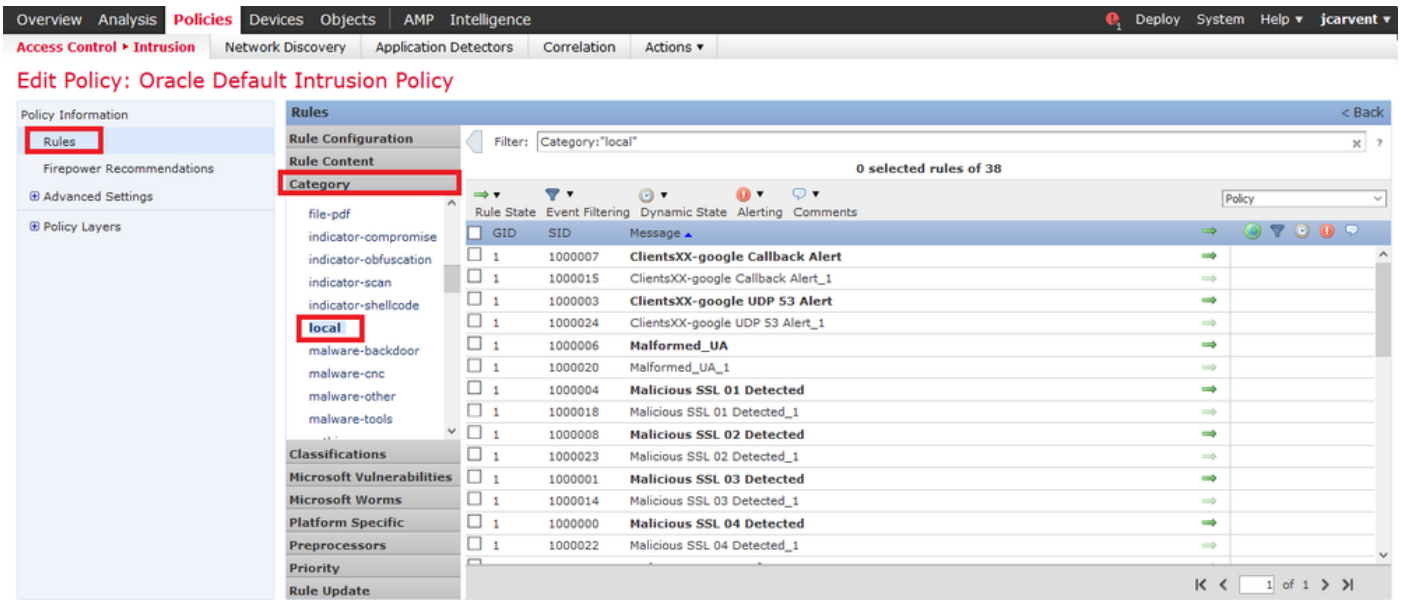
Standaard stelt het FirePOWER-systeem de lokale regels in in een uitgeschakeld toestand in. Deze lokale regels moeten handmatig de status van lokale regels instellen voordat u ze in uw inbraakbeleid kunt gebruiken.

2. Een lokale regel uit het inbraakbeleid inschakelen

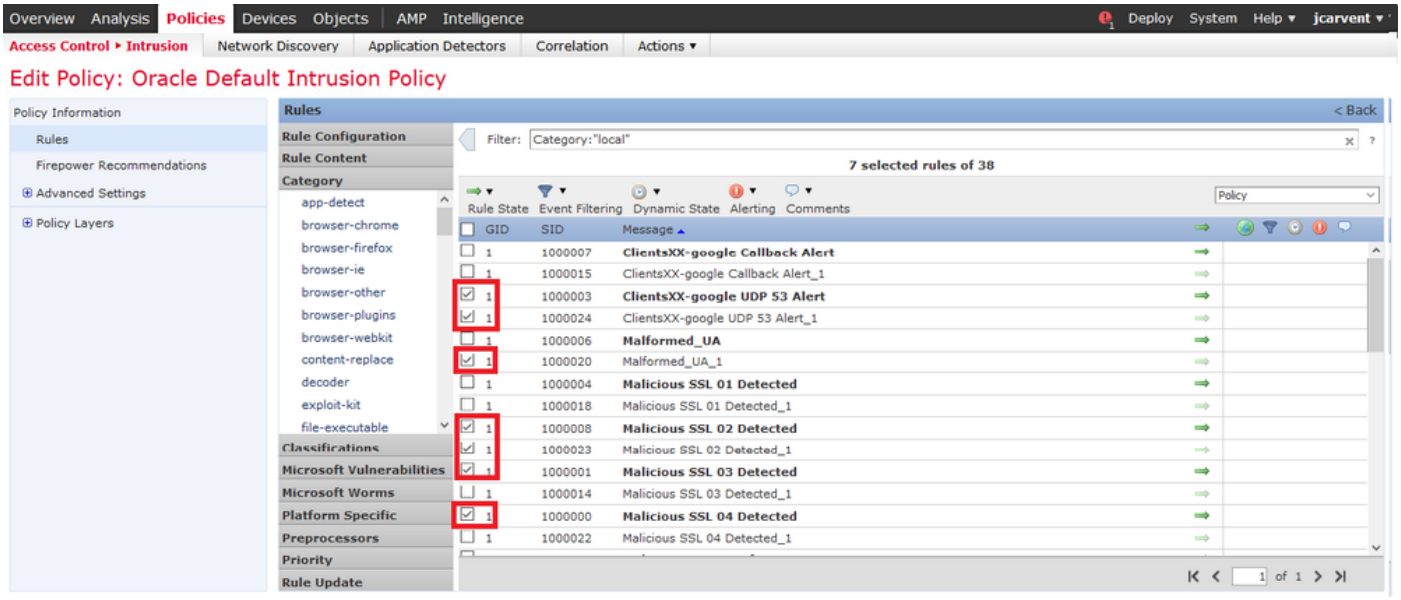
Stap 1. Navigeer naar pagina Beleidseditor onder **Beleid > Inbraakbeleid > Inbraakbeleid**

Stap 2. Selecteer **Regels** in het linker paneel

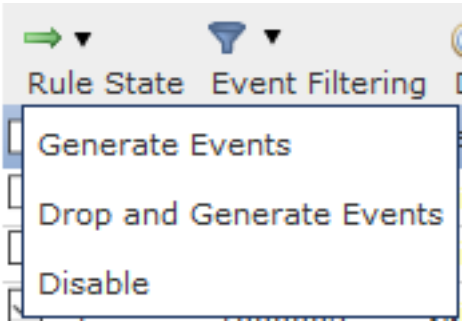
Stap 3. Onder het **programma Category**, selecteert u **lokaal.** Alle lokale regels moeten verschijnen indien beschikbaar:



Stap 4. Selecteer de gewenste lokale regels:



Stap 5. Selecteer na het selecteren van de gewenste lokale regels een status uit de **regelstaat**



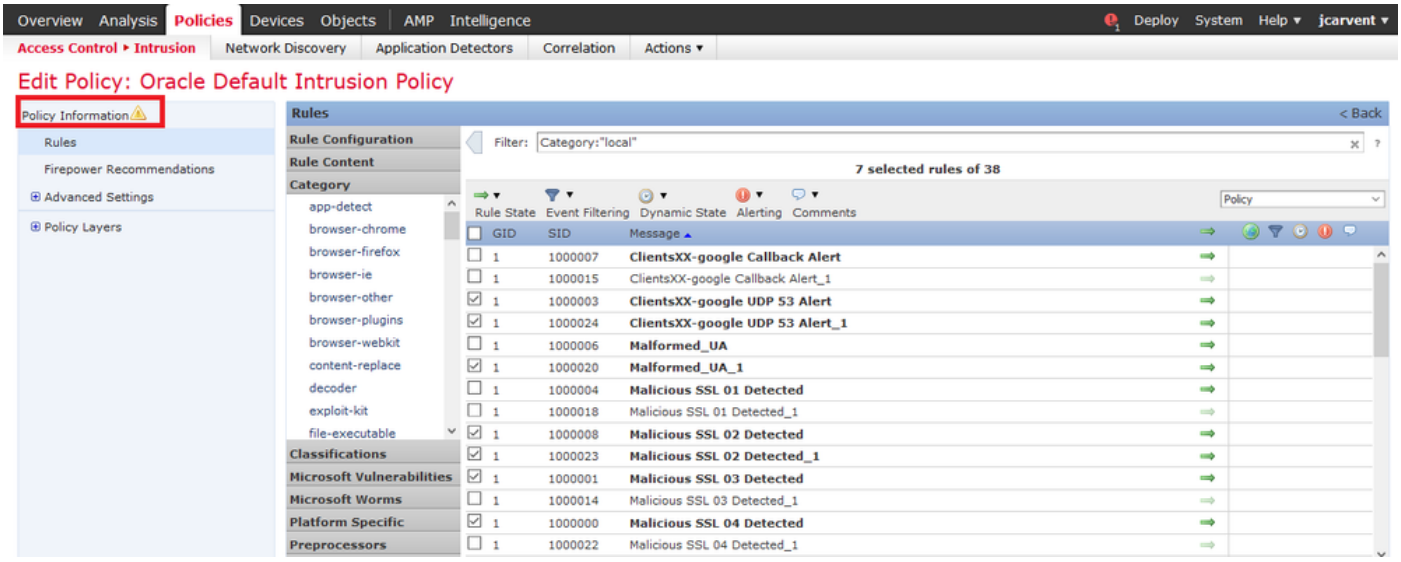
De volgende opties zijn beschikbaar:

- Evenementen genereren: Laat de regel toe en genereer een gebeurtenis

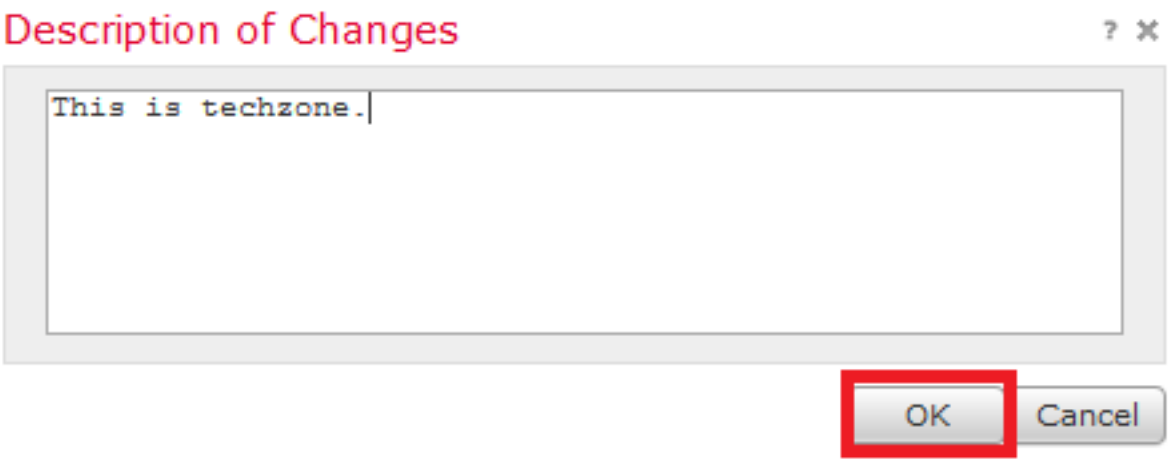
- gebeurtenissen neerzetten en genereren: Schakel de regel in, laat het verkeer vallen en genereer een gebeurtenis

- Uitschakelen: Laat de regel niet toe, geen gebeurtenissen

Stap 6. Klik op de volgende regel: Opties **voor beleidsinformatie** in het linker paneel



Stap 7. Selecteer de knop **Wijzigingen** aan **het** woord en specificeer een korte beschrijving van de wijzigingen. Klik later op **OK**. Het inbraakbeleid is gevalideerd.



Opmerking: de beleidsvalidatie faalt als u een geïmporteerde lokale regel toestaat die het afgekeurde drempelsleutelwoord in combinatie met de vodden van de inbraakgebeurtenis in een inbraakbeleid gebruikt.

Stap 8. Implementeer de wijzigingen

Van FTD of SFR module CLI

1. Bekijk de lokale regels die zijn geïmporteerd uit FTD of SFR module CLI

Stap 1. Stel een SSH- of CLI-sessie van uw SFR-module of FTD in

Stap 2. Navigeer naar modus van expert

```
> expert
admin@firepower:~$
```

Stap 3. Verkrijg administratorrechten

```
admin@firepower:~$ sudo su -
```

Stap 4. Typ uw wachtwoord

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

Stap 5. Navigeer naar **/ngfw/var/sf/detectie_engine/UID/Inbraaklegging/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

Opmerking: Als u SFR-module gebruikt, gebruik dan geen /ngfw/var/sf/detectie_engine/*/inbraakpad. Insted **gebruik/var/sf/detectie_motoren/*/inbraak**

Stap 6. Inleiding de volgende opdracht

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

Raadpleeg de afbeelding hieronder als werkvoorbeeld:

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

Dit maakt een lijst van de klant SID lijst die door de FTD of de SFR module wordt toegelaten.

Problemen oplossen

Stap 1. Controleer of de SSH-sessie is ingesteld op de SFR-module of FTD, van FMC-detectie_motoren is niet vermeld

Stap 2. De commandogrep -Eo "sid:* ([0-9] {1,8})" */*local.rules zullen alleen werken onder een indringingsfolder, kan de opdracht niet van een andere folder worden gebruikt

Stap 3. Gebruik de opdrachtbalk -Eo "sid:* ([0-9] {1,8})" */*.regels om een volledige SID-lijst van alle categorieën te krijgen

Beste praktijken voor de invoer van plaatselijke inbraakregels

Volg de richtlijnen op wanneer u een lokaal regelbestand importeert:

- De regels importeur vereist dat alle douaneregels worden ingevoerd in een onbeperkt tekstbestand dat is gecodeerd in ASCII of UTF-8
- De naam van het tekstbestand kan alfanumerieke tekens, spaties en geen speciale tekens bevatten anders dan onderstreept (_), punt (.) en stippelrand (-)
- Het systeem importeert lokale regels voorafgegaan door één liggend teken (#), maar ze worden gemarkeerd als verwijderd
- Het systeem importeert lokale regels die voorafgaan aan een enkel pound-teken (#) en importeert geen lokale regels die voorafgegaan zijn door twee-pound tekens (##)
- Regels kunnen geen ontsnappingstekens bevatten
- U hoeft geen generator-ID (GID) te specificeren wanneer u een lokale regel importeert. Als u dit wel doet, specificeert u alleen GID 1 voor een standaard tekstregel
- Wanneer u voor het eerst een regel importeert, dient u *niet* specificeren ID SNELHEID (SID) of herzieningsnummer. Dit vermijdt botsingen met SID's van andere regels, waaronder verwijderde regels. Het systeem zal automatisch de regel toekennen van de volgende beschikbare douaneregel SID van 1000000 of meer en een herzieningsnummer van 1
- Als u regels met SID’s moet importeren, moeten de SID’s unieke getallen zijn tussen 1.000.000 en 9.999.999

- In een multidomein plaatsing, wijst het systeem SIDs toe aan ingevoerde regels van een gedeeld pool die door alle domeinen op het gebied wordt gebruikt FireSIGHT Management Center. Als meerdere beheerders tegelijkertijd lokale regels importeren, kunnen SIDs's binnen een individueel domein niet sequentieel lijken te zijn, omdat het systeem de geïntervenieerde getallen in de sequentie aan een ander domein toegewezen heeft
- Wanneer u een bijgewerkte versie van een lokale regel invoert die u eerder hebt geïmporteerd, of wanneer u een lokale regel opnieuw installeert, hebt u verwijderd, ***moet*** u de door het systeem toegewezen SID en een herzieningsnummer toevoegen dat groter is dan het huidige herzieningsnummer. U kunt het herzieningsnummer voor een huidige of verwijderde regel bepalen door de regel te bewerken

  Opmerking: het systeem verhoogt automatisch het revisienummer wanneer u een lokale regel verwijdert; dit is een apparaat waarmee je lokale regels kunt herstellen . Alle verwijderde lokale regels worden verplaatst van de lokale categorie naar de verwijderde categorie.

- Importeer lokale regels op het primaire centrum van het Firepower Management in een hoge beschikbaarheid paar om SID nummerkwesties te vermijden
- De invoer mislukt als een regel een van de volgende onderdelen bevat:Een SID is groter dan 2147483647Een lijst met bron- of doelpoorten die langer zijn dan 64 tekens
- Beleidsvalidatie faalt als u een geïmporteerde lokale regel toestaat die het trefwoord afgekeurde drempelwaarde gebruikt in combinatie met de vodden van de inbraakgebeurtenis in een inbraakbeleid
- Alle geïmporteerde lokale regels worden automatisch opgeslagen in de categorie lokale regels
- Het systeem stelt altijd lokale regels in die u naar de gehandicaptenregelstaat importeert. U moet de status van de lokale regels handmatig instellen voordat u deze in het inbraakbeleid kunt gebruiken

Gerelateerde informatie

Hier zijn enkele documenten ter referentie met betrekking tot snort SID:

Inbraakregels bijwerken

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

De redacteur van de inbraakregels

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html