Configureer aangepaste lokale snortregels in Snort2 op FTD

Inhoud

Inleiding

In dit document wordt de procedure beschreven om Aangepaste lokale snelregels te configureren in Snort2 op Firewall Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defence (FTD)

Gebruikte componenten

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

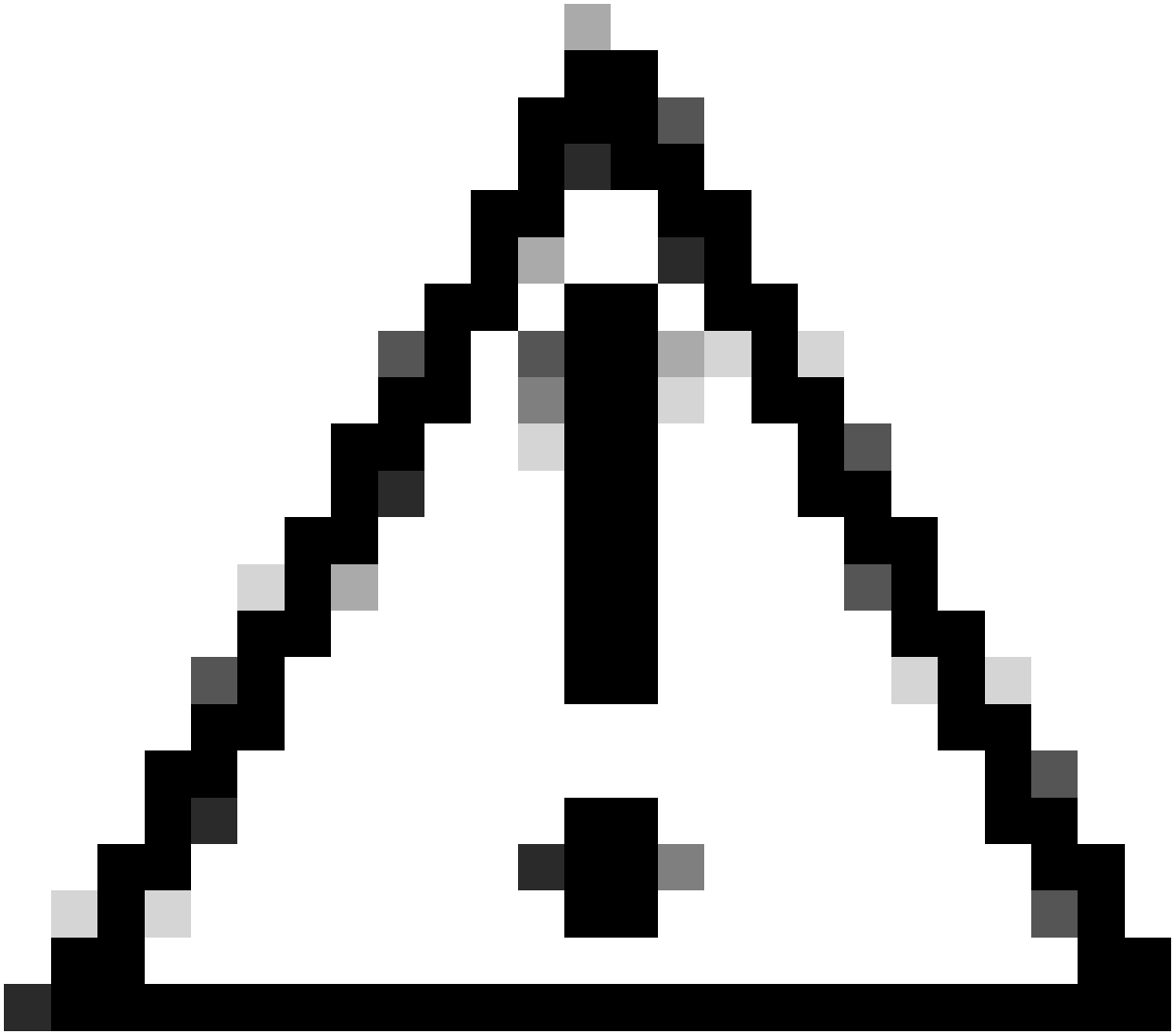
- Cisco Firepower Management Center voor VMware 7.4.1
- Cisco FirePOWER-applicatie 2120 7.4.1

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Custom Local Snort Rule verwijst naar een door de gebruiker gedefinieerde regel die u kunt maken en implementeren binnen het snort inbraakdetectie- en preventiesysteem dat is geïntegreerd in de FTD. Wanneer u een aangepaste lokale snortregel in Cisco FTD maakt, definieert u in wezen een nieuw patroon of een nieuwe reeks voorwaarden waarop de snortengine kan letten. Als het netwerkverkeer voldoet aan de voorwaarden die in uw aangepaste regel zijn gespecificeerd, kunt u de actie uitvoeren die in de regel is gedefinieerd, zoals een waarschuwing genereren of het pakket laten vallen. Beheerders gebruiken aangepaste lokale Snortregels om specifieke bedreigingen aan te pakken die niet worden gedekt door de algemene regelsets.

In dit document, wordt u geïntroduceerd hoe te om een Douane Lokale Snelregel te vormen en te verifiëren die wordt ontworpen om HTTP- reactiepakketten te ontdekken en te laten vallen die een specifiek koord (gebruikersbenaming) bevatten.

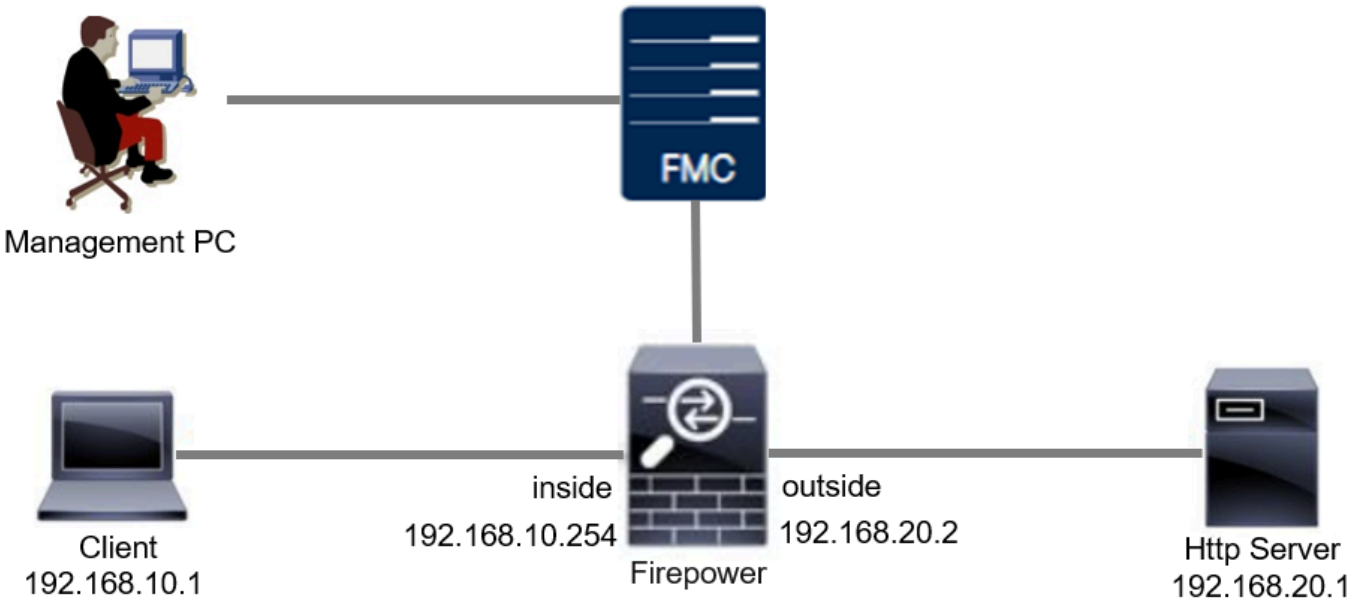


Waarschuwing: het maken van aangepaste lokale snelregels en het bieden van ondersteuning ervoor valt buiten de TAC ondersteuning dekking. Daarom kan dit document alleen als referentie worden gebruikt en u vragen deze aangepaste regels naar eigen goeddunken en op eigen verantwoordelijkheid te maken en te beheren.

Configureren

Netwerkdiagram

Dit document introduceert de configuratie en verificatie voor Aangepaste lokale snortregel in Snort2 in dit diagram.

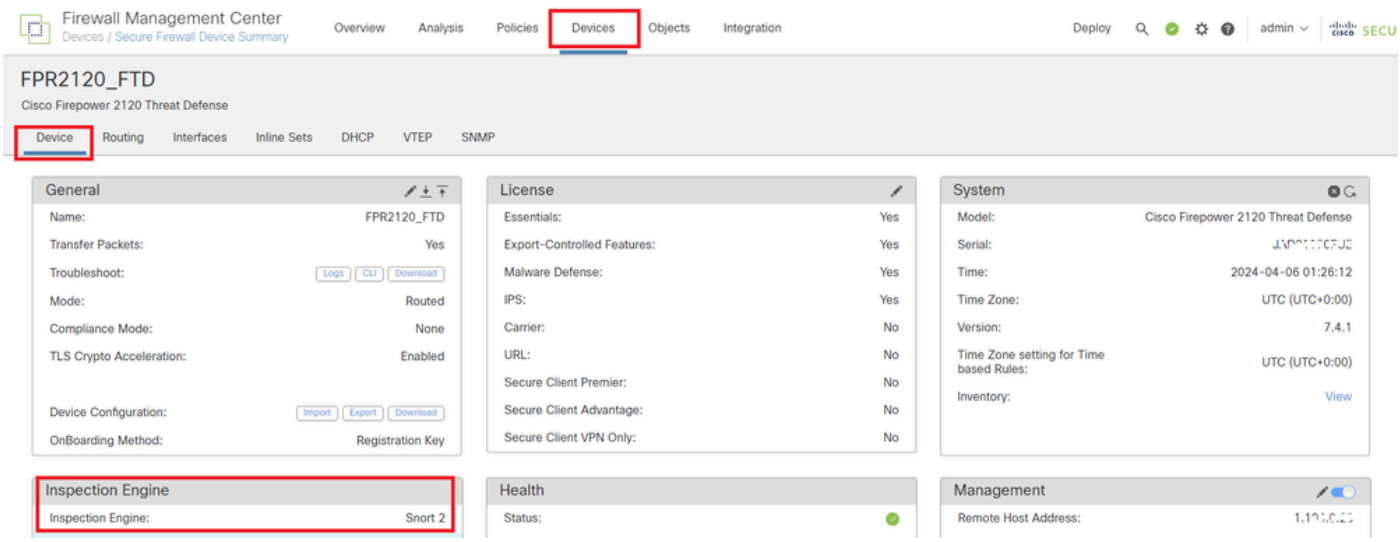


Configuratie

Dit is de configuratie van Aangepaste lokale snortregel om HTTP-reactiepakketten met een specifieke string (gebruikersnaam) te detecteren en te laten vallen.

Stap 1. Snelversie bevestigen

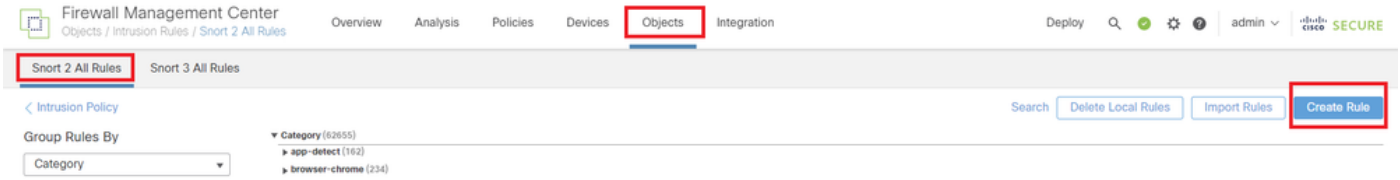
Navigeren naar Apparaten > Apparaatbeheer op FMC, klik op Apparaat tabblad. De snortversie bevestigen is Snort2.



Snelversie

Stap 2. Een aangepaste lokale-snortregel maken in kleur 2

Navigeer naar objecten > Inbraakregels > Sneltoets 2 Alle regels op FMC, klik op Regel maken knop.

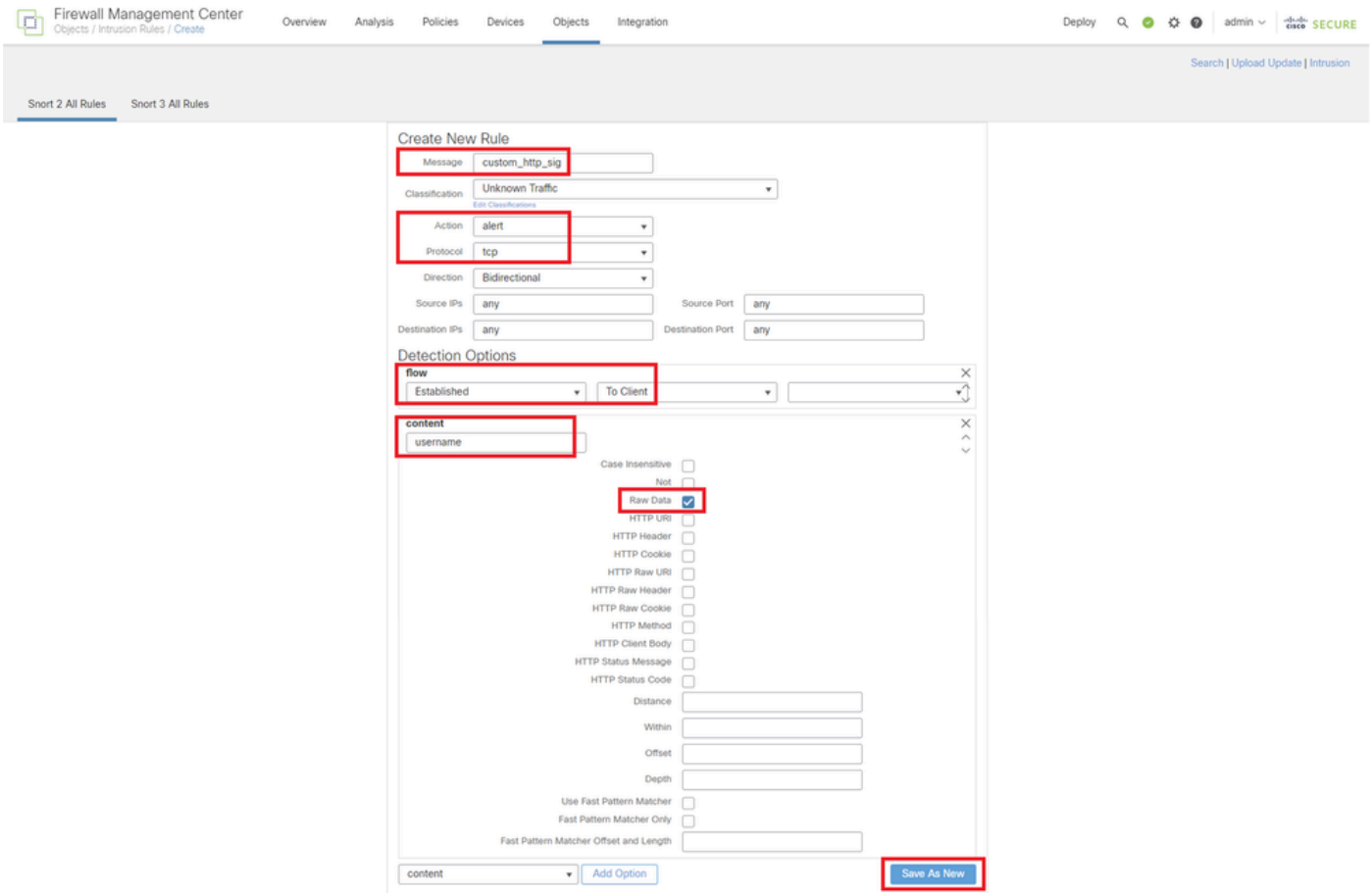


Aangepaste regel maken

Voer de benodigde informatie in voor Aangepaste lokale snelregel.

- Inbraak : custom_http_sig
- Actie : waarschuwing
- Protocol: TCP
- stroom : vastgesteld, naar de klant

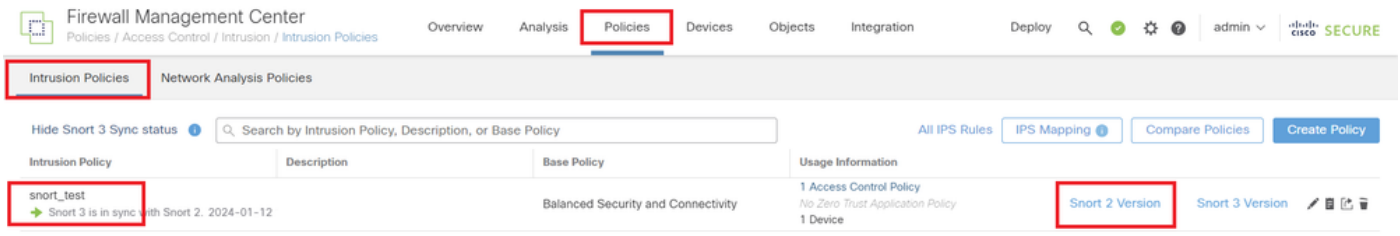
- inhoud: gebruikersnaam (ruwe gegevens)



Voer de benodigde informatie voor deze regel in

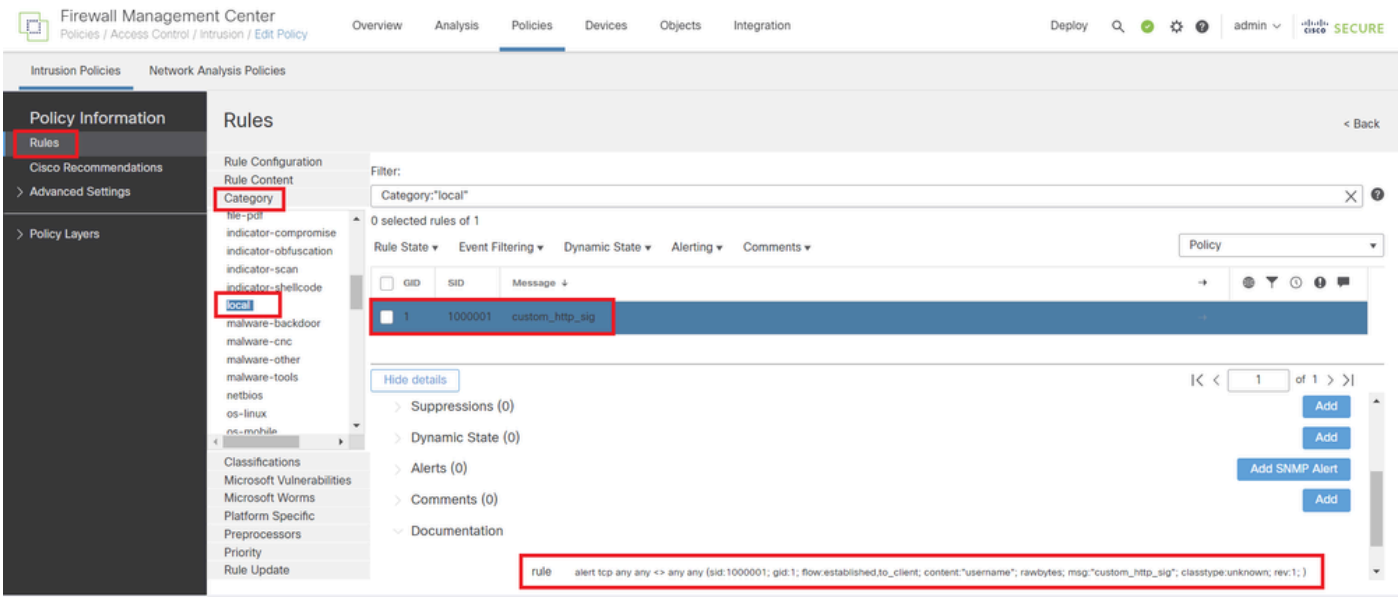
Stap 3. Aangepaste lokale snelregel bevestigen

Navigeren naar Beleid > Inbraakbeleid op FMC, klik op Sneltoets 2 Versie knop.



Aangepaste regel bevestigen

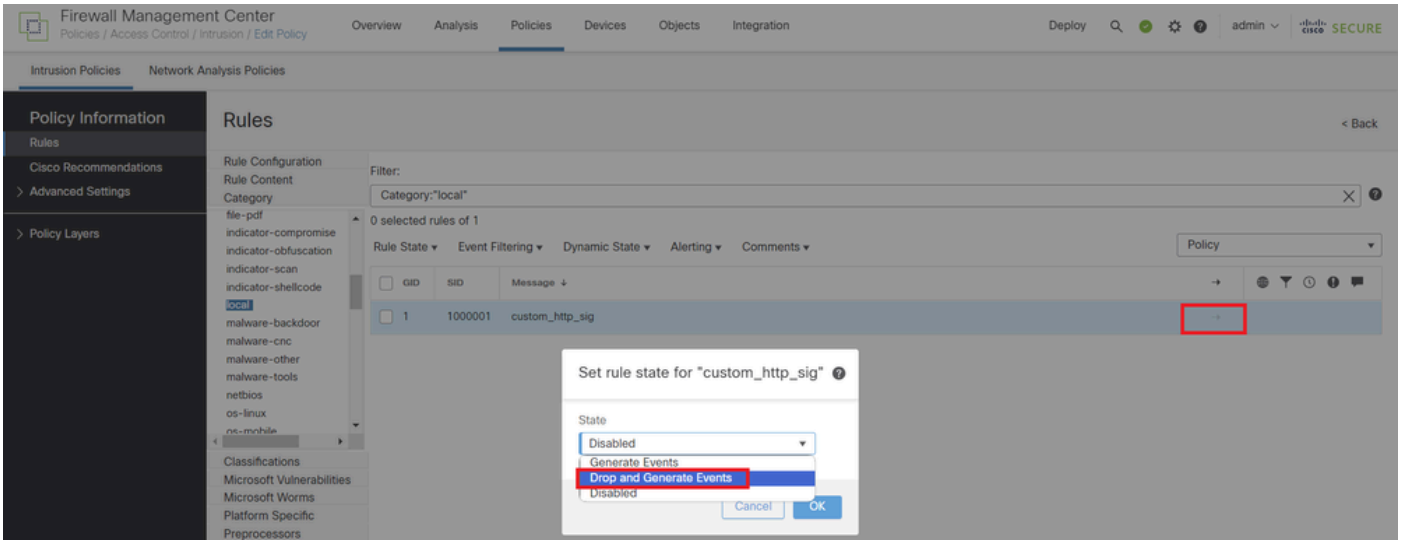
Ga naar Regels > Categorie > Lokaal op VCC, bevestig de details van de Aangepaste Lokale Snortregel.



Detail van aangepaste regel

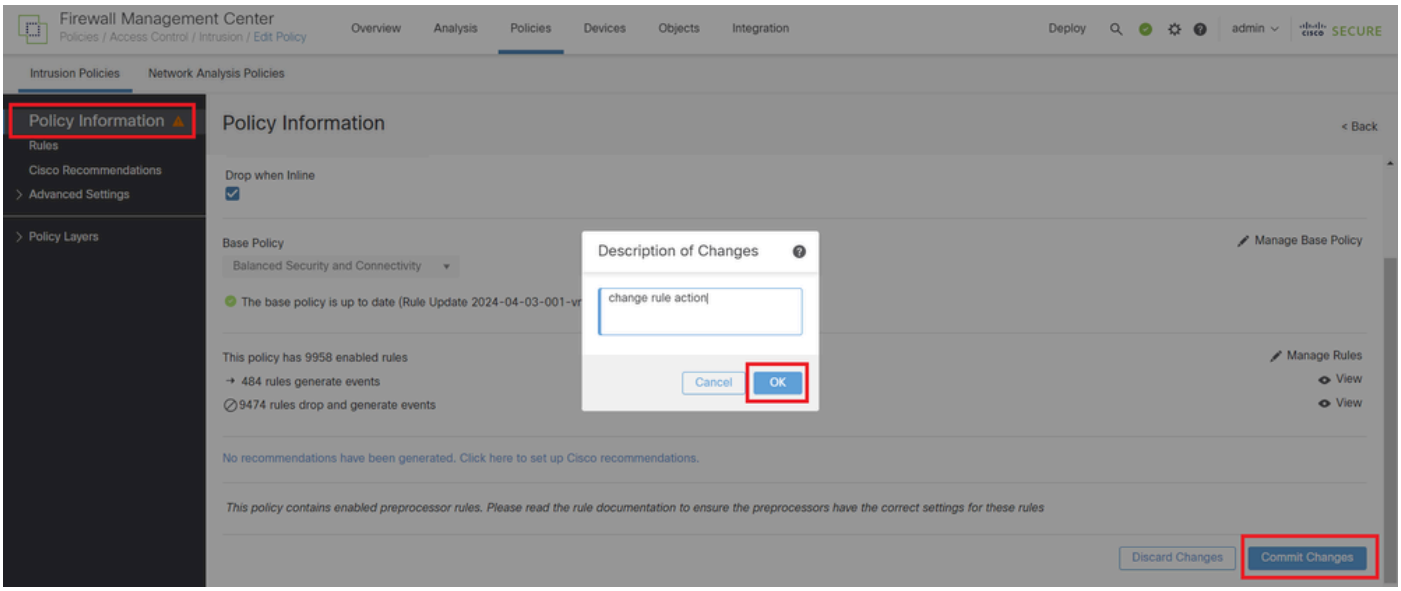
Stap 4. Handeling regels wijzigen

Klik op de knop Status, stel de status in om gebeurtenissen te laten vallen en te genereren en klik op de knop OK.



Verander de actie van de regel

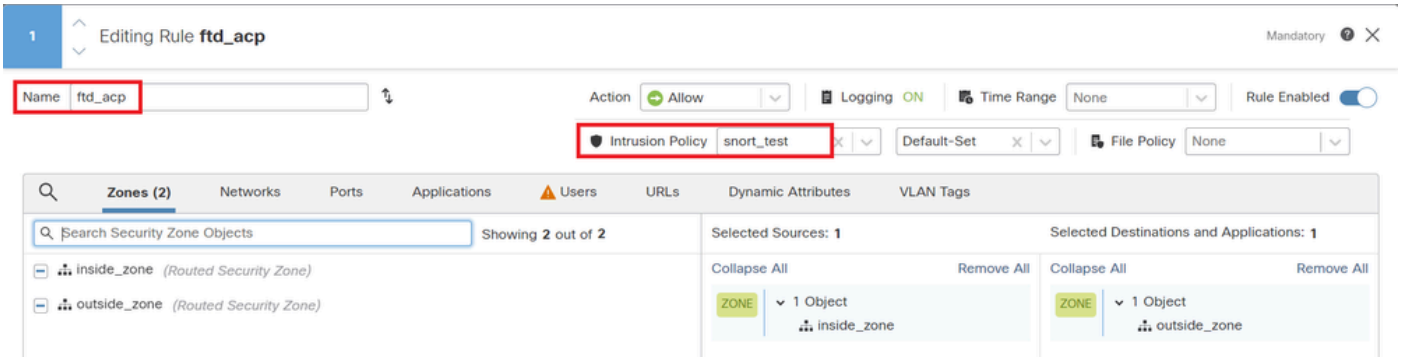
Klik op de knop Beleidsinformatie en klik op de knop Wijzigingen vastleggen om de wijzigingen op te slaan.



Wijzigingen vastleggen

Stap 5. Associate Inbraakbeleid met Access Control Policy (ACS)-regel

Ga naar Beleid > Toegangsbeheer bij VCC, associeer Inbraakbeleid met ACS.



Associatie met de ACS-regeling

Stap 6. Wijzigingen implementeren

Breng de wijzigingen in FTD aan.

Wijzigingen implementeren

Verifiëren

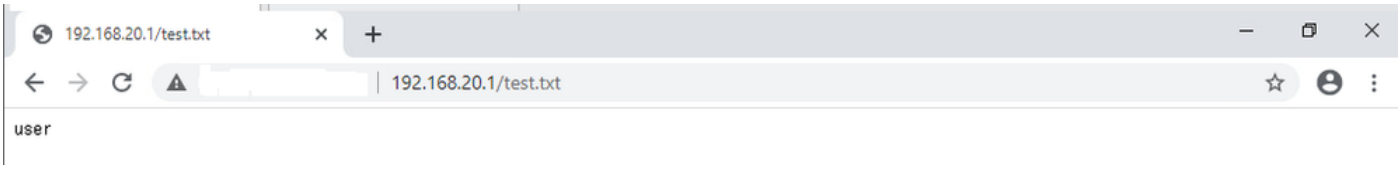
Aangepaste lokale snortregel wordt niet geactiveerd

Stap 1. Inhoud van bestand in HTTP-server instellen

Stel de inhoud van het test.txt bestand op de HTTP server kant in op gebruiker.

Stap 2. Eerste HTTP-aanvraag

Open de HTTP Server (192.168.20.1/test.txt) vanuit de browser van de client (192.168.10.1) en bevestig dat de HTTP-communicatie is toegestaan.



Eerste HTTP-aanvraag

Aangepaste lokale snortregel wordt geactiveerd

Stap 1. Inhoud van bestand in HTTP-server instellen

Stel de inhoud van het test.txt bestand op HTTP server kant in op gebruikersnaam.

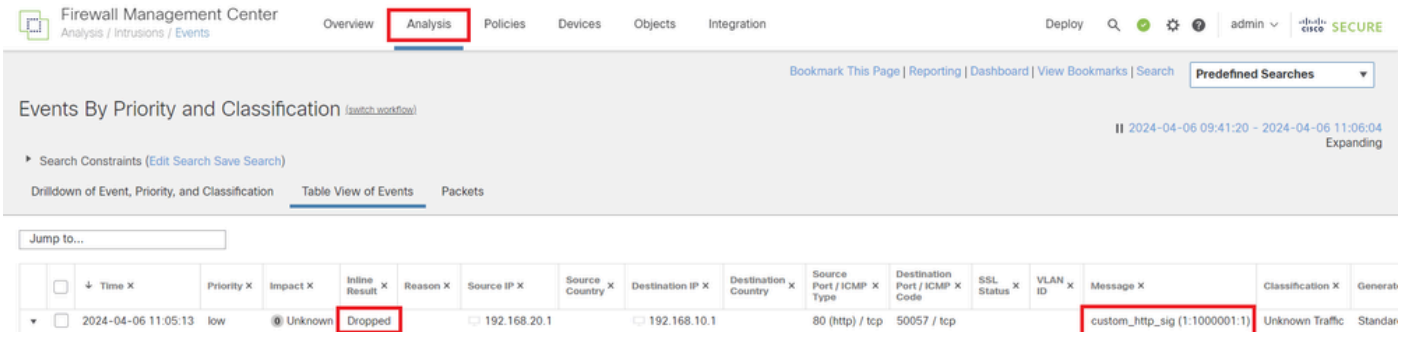
Stap 2. Eerste HTTP-aanvraag

Open de HTTP Server (192.168.20.1/test.txt) vanuit de browser van de client (192.168.10.1) en bevestig dat de HTTP-communicatie is geblokkeerd.

Eerste HTTP-aanvraag

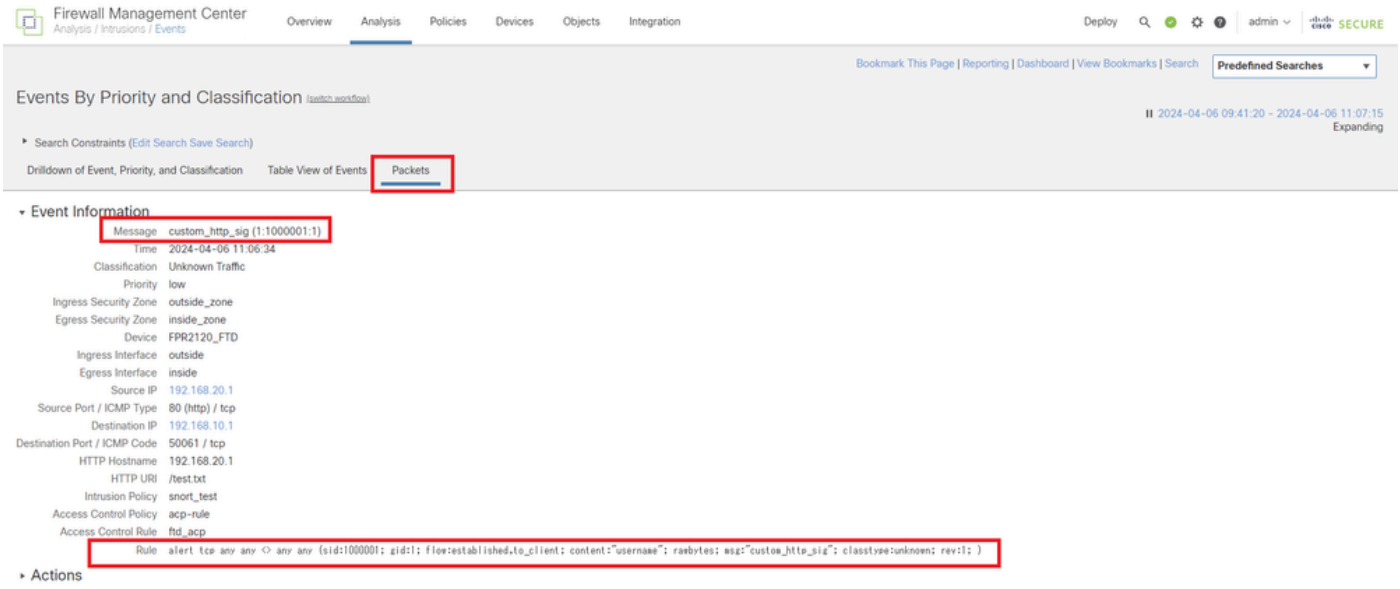
Stap 3. Inbraakgebeurtenis bevestigen

Navigeren naar Analyse > Inbraakacties > Evenementen op FMC, bevestigen dat de Inbraakgebeurtenis wordt gegenereerd door de Aangepaste lokale Snortregel.



Inbraakgebeurtenis

Klik op het tabblad Pakketten en bevestig de details van Inbraakgebeurtenis.



Detail van inbraakgebeurtenis

Problemen oplossen

Start de opdrachtsystem support trace om het gedrag op FTD te bevestigen. In dit voorbeeld wordt het HTTP-verkeer geblokkeerd door de IPS-regel (gid 1, SID 1000001).

<#root>

>

system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
```

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.