

# Configureer aangepaste lokale snortregels in Snort3 op FTD

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configuratie](#)

[Methode 1. Importeren van snort 2 naar snort 3](#)

[Stap 1. Snelversie bevestigen](#)

[Stap 2. Een aangepaste lokale snurkregel in kleur 2 maken of bewerken](#)

[Stap 3. Aangepaste lokale snortregels importeren van snort 2 naar snort 3](#)

[Stap 4. Handeling regels wijzigen](#)

[Stap 5. Bevestig geïmporteerde aangepaste lokale snelregel](#)

[Stap 6. Associate Inbraakbeleid met Access Control Policy \(ACS\)-regel](#)

[Stap 7. Wijzigingen implementeren](#)

[Methode 2. Een lokaal bestand uploaden](#)

[Stap 1. Snelversie bevestigen](#)

[Stap 2. Een aangepaste lokale snelregel maken](#)

[Stap 3. De aangepaste lokale snelregel uploaden](#)

[Stap 4. Handeling regels wijzigen](#)

[Stap 5. Bevestig geüploade aangepaste lokale snelregel](#)

[Stap 6. Associate Inbraakbeleid met Access Control Policy \(ACS\)-regel](#)

[Stap 7. Wijzigingen implementeren](#)

[Verifiëren](#)

[Stap 1. Inhoud van bestand in HTTP-server instellen](#)

[Stap 2. Eerste HTTP-aanvraag](#)

[Stap 3. Inbraakgebeurtenis bevestigen](#)

[Veelgestelde vragen \(FAQ\)](#)

[Problemen oplossen](#)

[Referentie](#)

---

## Inleiding

In dit document wordt de procedure beschreven om Aangepaste lokale snelregels te configureren in Snort3 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:

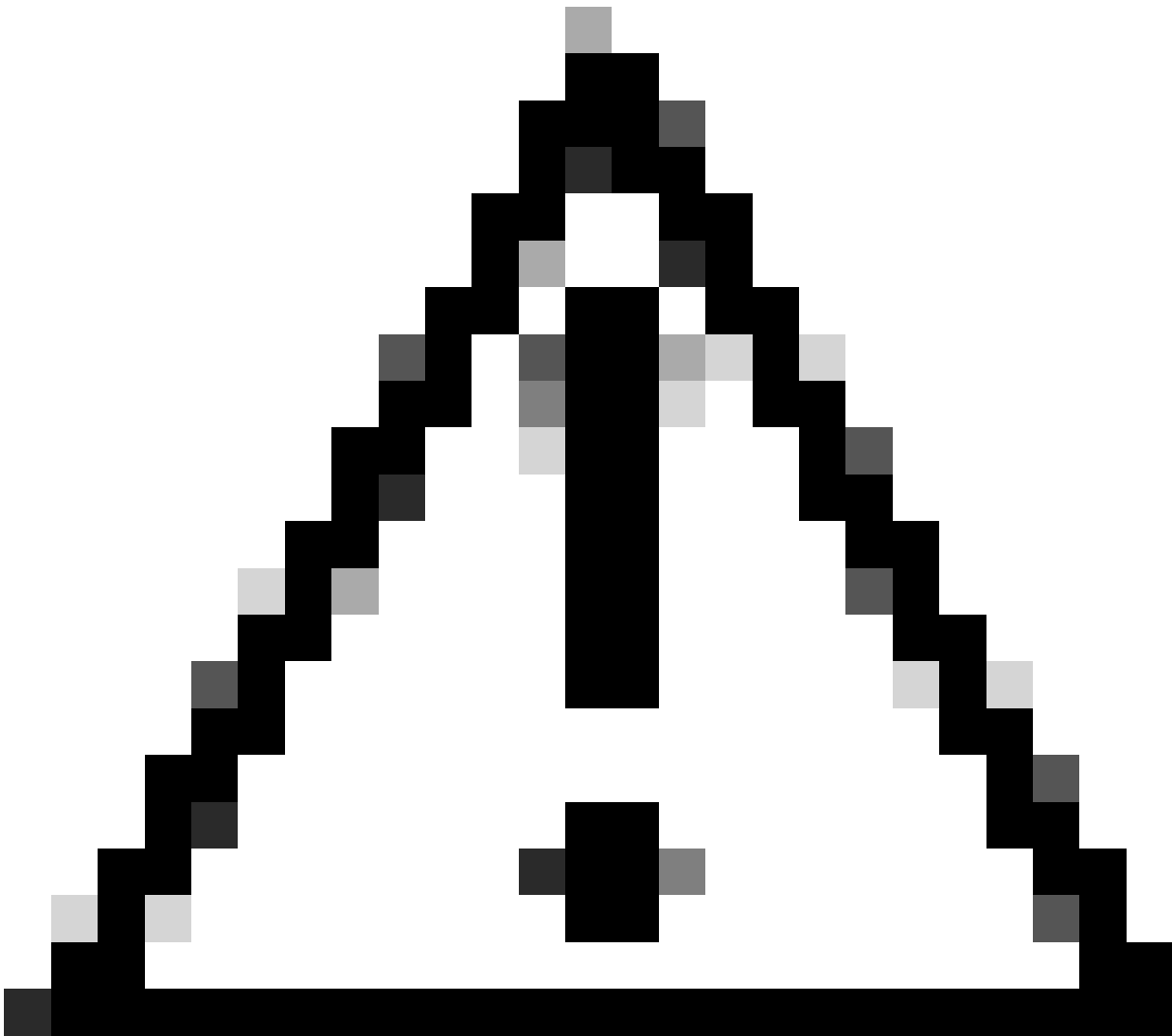
- Cisco Firepower Management Center voor VMware 7.4.1
- Cisco FirePOWER-applicatie 2120 7.4.1

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

Ondersteuning voor Snort 3 in bedreigingsverdediging met management center begint in versie 7.0. Voor nieuwe en opnieuw in beeld gebrachte apparaten van versie 7.0 en hoger, is Snort 3 de standaard inspectie-engine.

Dit document geeft een voorbeeld van hoe u de Snortregels voor Snort 3 kunt aanpassen, evenals een praktisch controlevoorbeeld. Met name wordt u geïntroduceerd hoe u een inbraakbeleid kunt configureren en verifiëren met een aangepaste snortregel om HTTP-pakketten die een bepaalde tekenreeks (gebruikersnaam) bevatten te laten vallen.

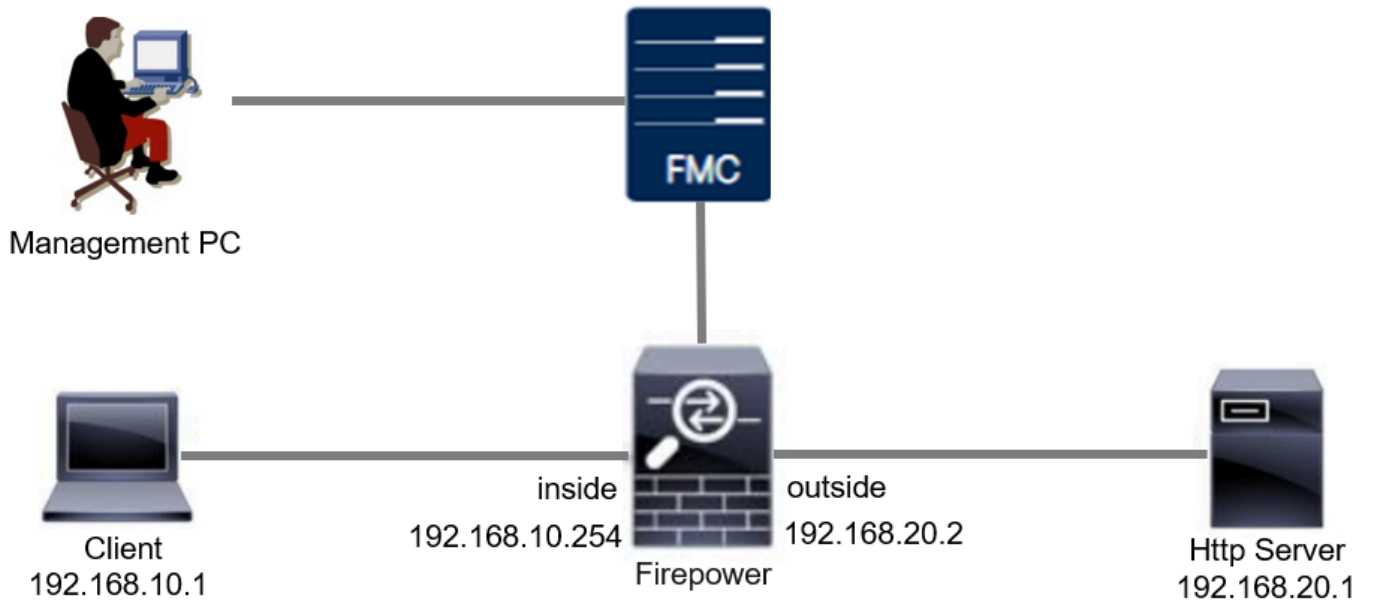


Waarschuwing: het maken van aangepaste lokale snelregels en het bieden van ondersteuning daarvoor valt buiten de TAC-ondersteuningsdekking. Daarom kan dit document alleen als referentie worden gebruikt en u vragen deze aangepaste regels naar eigen goeddunken en op eigen verantwoordelijkheid te maken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

---

## Netwerkdigram

Dit document introduceert de configuratie en verificatie voor Aangepaste lokale snortregel in Snort3 in dit diagram.



Netwerkdigram

## Configuratie

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



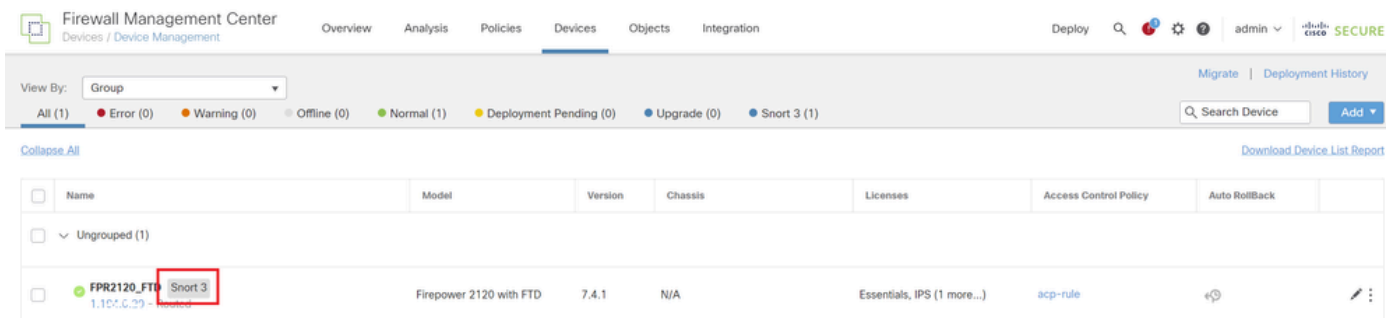
Opmerking: op dit moment is het niet mogelijk om aangepaste lokale snortregels toe te voegen vanaf de pagina Snort 3 All Rules (Alle regels) in de FMC GUI. U moet de methode gebruiken die in dit document is geïntroduceerd.

---

## Methode 1. Importeren van snort 2 naar snort 3

### Stap 1. Bevestig de snelversie

Navigeer naar Apparaten>Apparaatbeheer op FMC en klik op Devicetab. Bevestig dat de snortversie Snort3 is.



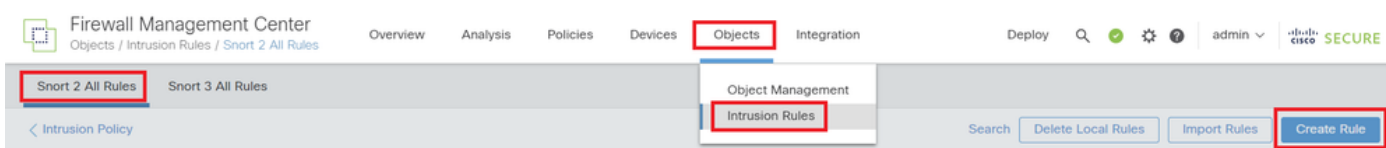
Snelversie

## Stap 2. Een aangepaste lokale snurkregel in kleur 2 maken of bewerken

Ga naar Objecten > Inbraakregels > Sneltoets 2 Alle regels op FMC. Klik op Regelknop maken om een aangepaste lokale snortregel toe te voegen of navigeer naar objecten > Inbraakregels > Sneltoets 2 Alle regels > Lokale regels op FMC, klik op knop Bewerken om een bestaande aangepaste lokale snortregel te bewerken.

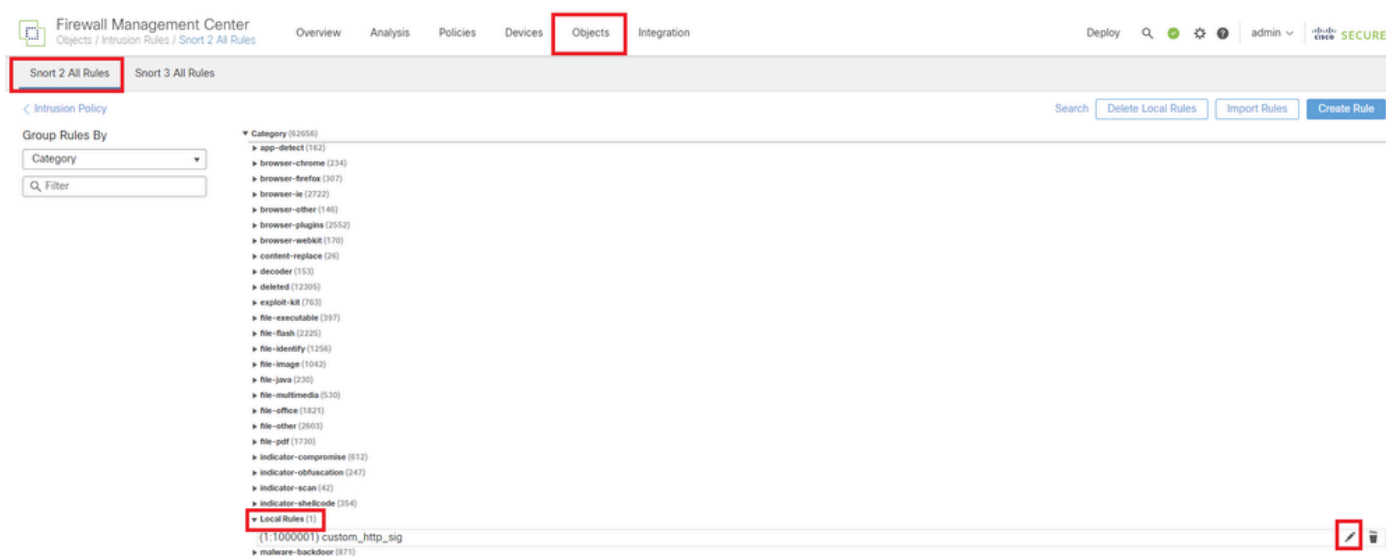
Voor instructies hoe u Aangepaste lokale snurrtregels kunt maken in Snort 2, raadpleegt u [Aangepaste lokale snurrtregels configureren in Snort2 op FTD](#).

Voeg een nieuwe Aangepaste lokale Snurregel toe zoals in de afbeelding wordt weergegeven.



Een nieuwe aangepaste regel toevoegen

Bewerk een bestaande Aangepaste lokale Snelregel zoals in de afbeelding. In dit voorbeeld wordt een bestaande douaneregel bewerkt.



Een bestaande aangepaste regel bewerken

Voer de handtekeninginformatie in om HTTP-pakketten te detecteren die een specifieke string

bevatten (gebruikersnaam).

- Bericht: custom\_http\_sig
- Actie : waarschuwing
- Protocol: TCP
- stroom : vastgesteld, naar de klant
- inhoud: gebruikersnaam (ruwe gegevens)

Firewall Management Center  
Objects / Intrusion Rules / Create

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Upload Update Intrusion

Snort 2 All Rules Snort 3 All Rules

Edit Rule 1:1000000:3 (Rule Comment)

Message: custom\_http\_sig

Classification: Unknown Traffic

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any Source Port: any

Destination IPs: any Destination Port: any

Detection Options

flow: Established To Client

content: username

Raw Data

Save Save As New

Voer de benodigde informatie voor deze regel in

### Stap 3. Aangepaste lokale snortregels importeren van snort 2 naar snort 3

Navigeer naar Objecten > Inbraakregels > Sneltoets 3 Alle regels > Alle regels op FMC, klik op Sneltoets 2 converteren en voer uit Tasks keuzelijst in.

Firewall Management Center  
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Upload Update Intrusion

Snort 2 All Rules Snort 3 All Rules

< Intrusion Policy Back To Top

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

50,094 rules

| Info  | Rule Action       | Assigned Groups |
|---|-------------------|-----------------|
| 148:2 (cip) CIP data is non-conforming to ODVA standard | Disable (Default) | Builtins        |
| 133:3 (dce_smb) SMB - bad SMB message type              | Disable (Default) | Builtins        |

Upload Snort 3 rules

Convert Snort 2 rules and Import

Convert Snort 2 rules and download

Add Rule Groups

Controleer het waarschuwingsbericht en klik op OK.

## Convert Snort 2 rules and import



The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.

Cancel

OK

Waarschuwingbericht

Navigeer naar Objecten > Inbraakregels > Sneltoets 3 Alle regels op FMC en klik op All Snort 2 Converted Global om de geïmporteerde aangepaste lokale snortregel te bevestigen.

The screenshot shows the Firewall Management Center interface. The left sidebar shows a tree view with 'Local Rules (1 group)' expanded, and 'All Snort 2 Converted Global' selected. The main area shows the details for this group, including a description and a table of rules. A red box highlights the 'All Snort 2 Converted Global' group in the sidebar and the '2000:1000000 custom\_http\_sig' rule in the table. A green notification box states 'The custom rules were successfully imported'.

| GID:SID      | Info            | Rule Action       | Assigned Groups              | Alert Configuration |
|--------------|-----------------|-------------------|------------------------------|---------------------|
| 2000:1000000 | custom_http_sig | Disable (Default) | All Snort 2 Converted Glo... | None                |

Bevestig geïmporteerde aangepaste regel

### Stap 4. Handeling regels wijzigen

Klik per Inbraakbeleid volgens de Handeling van de Regel van de doeldouaneregels.



**All Rules**

- Local Rules (1 group)
- All Snort 2 Converted Global
- MITRE (1 group)
- Rule Categories (9 groups)

**Local Rules / All Snort 2 Converted Global**

**Description** Group created for custom rules enabled in snort 2 version

Rule Actions  Tasks

1 rule

✔ The custom rules were successfully imported ✕

|   | GID:SID      | Info            | Rule Action   | Assigned Groups              | Alert Configuration |
|---|--------------|-----------------|---|------------------------------|---------------------|
| > | 2000:1000000 | custom_http_sig | <div style="border: 1px solid #ccc; padding: 2px;"> <span>⊗ Disable (Default) (Overridden)</span><br/> <span>🛑 Block</span><br/> <span>⚠ Alert</span><br/> <span>✍ Rewrite</span><br/> <span>⬇ Drop</span><br/> <span>🟢 Pass</span><br/> <span>🛑 Reject</span><br/> <span>⊗ Disable (Default)</span><br/> <span>↔ Revert to default</span><br/> <span style="border: 2px solid red; padding: 2px;">Per Intrusion Policy</span> </div> | All Snort 2 Converted Glo... | None                |

Handeling regels wijzigen

Voer in het scherm Handeling regels bewerken de informatie in voor de Handeling beleid en regels.

- Beleid: snort\_test
- Regel Actie: BLOK



Opmerking: Regelhandelingen zijn:

Blok— genereert gebeurtenis, blokkeert het huidige bijpassende pakket en alle daaropvolgende pakketten in deze verbinding.

Waarschuwing: genereert alleen gebeurtenissen voor bijpassend pakket en laat pakket of verbinding niet vallen.

Herschrijven— genereert gebeurtenis en overschrijft pakketinhoud op basis van de optie vervangen in de regel.

Pass— Er worden geen gebeurtenissen gegenereerd, zodat pakketverkeer zonder verdere evaluatie kan worden doorgegeven via alle volgende Snortregels.

Drop— genereert gebeurtenis, laat vallen overeenkomend pakket en blokkeert geen verder verkeer in deze verbinding.

Afwijzen— genereert gebeurtenis, laat vallen overeenkomend pakket, blokkeert verder verkeer in deze verbinding en stuurt TCP opnieuw instellen als het een TCP-protocol is

---

naar bron- en doelhosts.

Uitschakelen—Dit komt niet overeen met verkeer op basis van deze regel. Er worden geen gebeurtenissen gegenereerd.

Standaard—Hiermee wordt de standaardactie van het systeem hersteld.

2000:100... | custom\_http\_sig

All Policies  Per Intrusion Policy

Policy: snort\_test

Rule Action: BLOCK

Add Another

Comments (optional): Provide a reason to change if applicable

Cancel Save

Handeling regels bewerken

## Stap 5. Bevestig geïmporteerde aangepaste lokale snelregel

Blader naar **Beleid > Inbraakbeleid** op FMC en klik op **Snelheid 3** versie die overeenkomt met het inbraakbeleid in de rij.

| Intrusion Policy  | Description | Base Policy                        | Usage Information   |
|---|-------------|------------------------------------|---|
| snort_test<br>→ Snort 3 is in sync with Snort 2. 2024-01-12 |             | Balanced Security and Connectivity | 1 Access Control Policy<br>No Zero Trust Application Policy<br>1 Device |

Snort 2 Version Snort 3 Version

Bevestig geïmporteerde aangepaste regel

Klik op **Local Rules > All Snort 2 Converted Global** om de details van de aangepaste lokale snortregel te controleren.

Firewall Management Center  
Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects Integration Deploy

Used by: 1 Access Control Policy | No Zero Trust Application Policy | 1 Device

Base Policy: Balanced Security and Connectivity | Mode: Prevention

Active Rules 9811 | Alert 478 | Block 9333

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** → Summary

Rule Overrides

103 items | All

All Rules  
Overridden Rules  
MITRE (1 group)  
Local Rules (1 group)  
**All Snort 2 Converted Global**  
Rule Categories (9 groups)

Local Rules / All Snort 2 Converted Global

Description: Group created for custom rules enabled in snort 2 version

Rule Action: Search by CVE, SID, Reference Info, or Rule Message

1 rule | Presets: Alert (0) | Block (1) | Disabled (0) | Overridden (1) | Advanced Filters

| GID:SID    | Rule Details    | Rule Action | Set By        | Assigned Groups         |
|------------|-----------------|-------------|---------------|-------------------------|
| 2000:10... | custom_http_sig | Block       | Rule Override | All Snort 2 Converte... |

alert tcp any any <> any any { sid:1000000; gid:2000; flow:established,to\_client; raw\_data; content:"username"; msg:"custom\_http\_sig"; classtype:unknown; rev:3; }

Bevestig geïmporteerde aangepaste regel

## Stap 6. Associate Inbraakbeleid met Access Control Policy (ACS)-regel

Navigeren naar beleid > Access Control FMC, inbraakbeleid koppelen aan ACS.

1 Editing Rule **ftd\_acp** Mandatory

Name: ftd\_acp

Action: Allow | Logging: ON | Time Range: None | Rule Enabled: ON

Intrusion Policy: snort\_test | Default-Set: | File Policy: None

Zones (2): inside\_zone (Routed Security Zone), outside\_zone (Routed Security Zone)

Showing 2 out of 2

Selected Sources: 1 | Selected Destinations and Applications: 1

Collapse All | Remove All | Collapse All | Remove All

ZONE | 1 Object | inside\_zone

ZONE | 1 Object | outside\_zone

Associatie met de ACS-regeling

## Stap 7. Wijzigingen implementeren

Breng de wijzigingen in FTD aan.

Firewall Management Center  
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects Integration

Return to Access Control Policy Management

acp-rule

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More

Deploy

Advanced Deploy | Ignore warnings: | Deploy All

FPR2120\_FTD | Ready for Deployment | 1 device

Wijzigingen implementeren

## Methode 2. Een lokaal bestand uploaden

### Stap 1. Snelversie bevestigen

Zie stap 1 van methode 1.

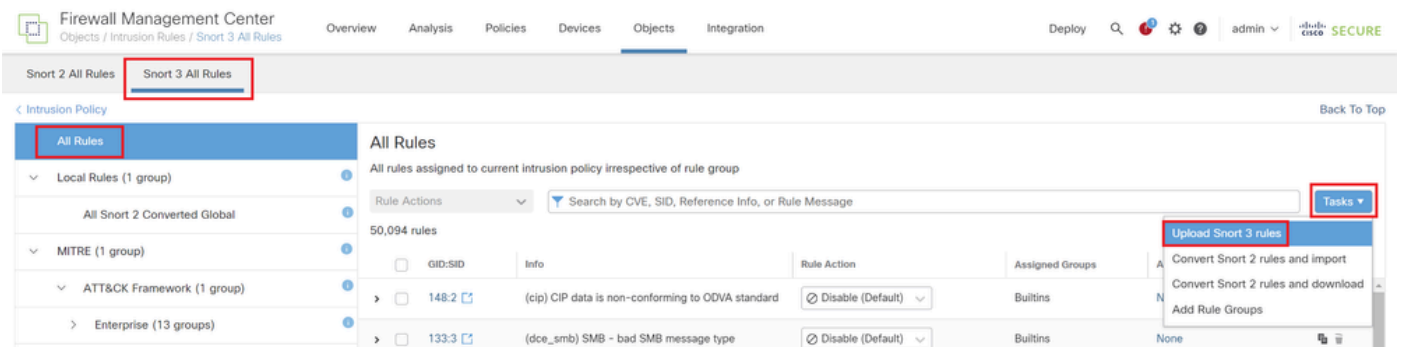
### Stap 2. Een aangepaste lokale snelregel maken

Maak handmatig een aangepaste lokale snurkregel en sla deze op in een lokaal bestand met de naam custom-rules.txt.

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

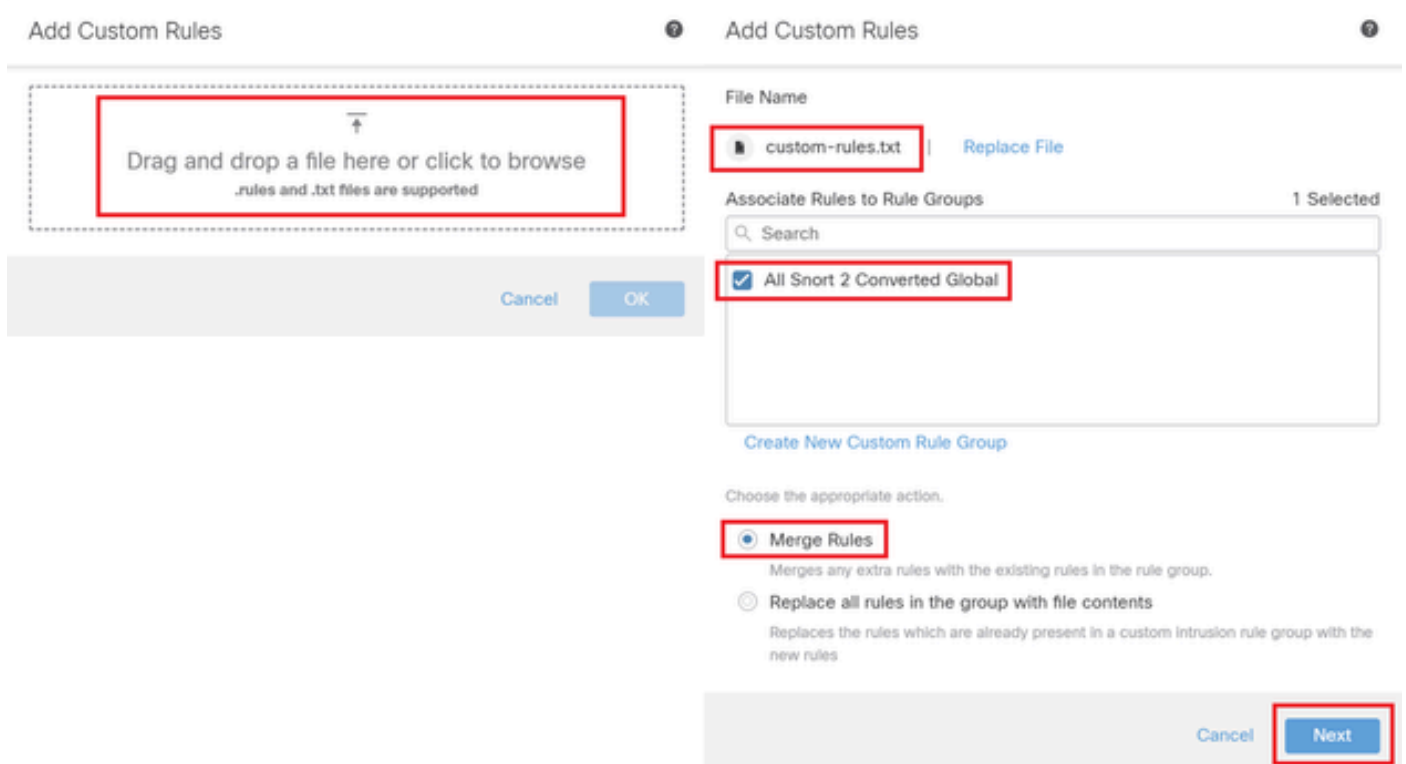
### Stap 3. De aangepaste lokale snelregel uploaden

Navigeer naar Objecten > Inbraakregels > Sneltoets 3 Alle regels > Alle regels op FMC, klik op Upload Sneltoets 3 regels uit de vervolgkeuzelijst Tasks.



Aangepaste regel uploaden

In het scherm Aangepaste regels toevoegen sleept u het lokale bestand custom-rules.txt, selecteert u de Regelgroepen en de juiste actie (regels samenvoegen in dit voorbeeld) en klikt u vervolgens op de knop Volgende.



Aangepaste regel toevoegen

Bevestig dat het lokale regelbestand is geüpload.

## Add Custom Rules



### Summary

✓ 1 new rule

2000:1000000

Download the summary file.

Back

Finish

Uploadresultaat bevestigen

Navigeer naar Objecten > Inbraakregels > Sneltoets 3 Alle regels op FMC en klik op All Snort 2 Converted Global om de geüploadde aangepaste lokale snortregel te bevestigen.

The screenshot shows the Firewall Management Center interface. The breadcrumb navigation is "Objects / Intrusion Rules / Snort 3 All Rules". The "Snort 3 All Rules" tab is selected. The "Local Rules / All Snort 2 Converted Global" group is expanded, showing a table with one rule:

| gid:SID                               | Info            | Rule Action  | Assigned Groups              | Alert Configuration |
|---------------------------------------|-----------------|--|------------------------------|---------------------|
| <input type="checkbox"/> 2000:1000000 | custom_http_sig | <input checked="" type="radio"/> Disable (Default) | All Snort 2 Converted Glo... | None                |

The rule's configuration details are shown below the table:

```
alert tcp any any <-> any any ( sid:1000000, gid:2000, flow:established,to_client, raw_data, content:"username"; msg:"custom_http_sig"; classtype:unknown; rev:3; )
```

Detail van aangepaste regel

### Stap 4. Handeling regels wijzigen

Zie stap 4 van methode 1.

Stap 5. Bevestig geüploadde aangepaste lokale snelregel

Zie stap 5 van methode 1.

Stap 6. Associate Inbraakbeleid met Access Control Policy (ACS)-regel

Dit is hetzelfde als in stap 6 van methode 1.

## Stap 7. Wijzigingen implementeren

Zie stap 7 van methode 1.

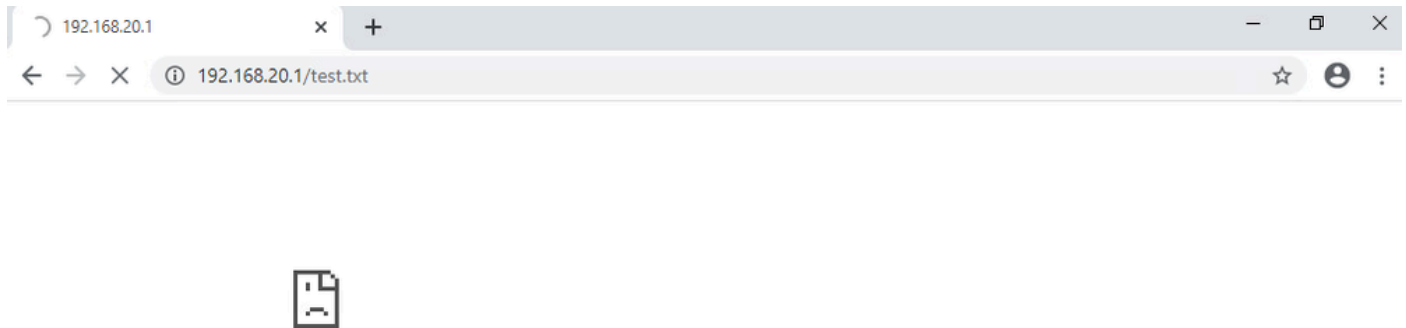
# Verifiëren

## 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

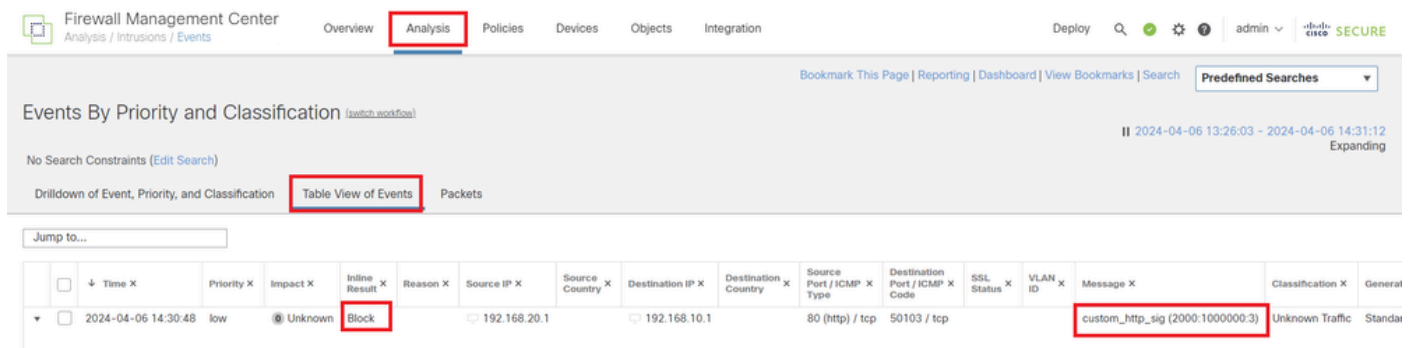
Open de HTTP Server (192.168.20.1/test.txt) vanuit de browser van de client (192.168.10.1) en bevestig dat de HTTP-communicatie is geblokkeerd.



Eerste HTTP-aanvraag

## Stap 3. Inbraakgebeurtenis bevestigen

Navigeer naar **Analysis > Intrusies > EventSons FMC**, bevestig dat de Inbraakgebeurtenis wordt genereerd door de Aangepaste Lokale Snelregel.

A screenshot of the Cisco Firewall Management Center (FMC) interface. The 'Analysis' tab is selected. The main area shows 'Events By Priority and Classification' for the period 2024-04-06 13:26:03 to 2024-04-06 14:31:12. A table of events is displayed, with one event highlighted. The event details are as follows:

| Time                | Priority | Impact  | Inline Result | Reason | Source IP    | Source Country | Destination IP | Destination Country | Source Port / ICMP Type | Destination Port / ICMP Code | SSL Status | VLAN ID | Message                          | Classification  | Generated |
|---------------------|----------|---------|---------------|--------|--------------|----------------|----------------|---------------------|-------------------------|------------------------------|------------|---------|----------------------------------|-----------------|-----------|
| 2024-04-06 14:30:48 | low      | Unknown | Block         |        | 192.168.20.1 |                | 192.168.10.1   |                     | 80 (http) / tcp         | 50103 / tcp                  |            |         | custom_http_sig (2000:1000000:3) | Unknown Traffic | Standar   |

Inbraakgebeurtenis

Klik op PacketStab, bevestig de details van Inbraakgebeurtenis.

The screenshot shows the 'Analysis' tab in the Firewall Management Center. The main heading is 'Events By Priority and Classification'. Below this, there are navigation options: 'Drilldown of Event, Priority, and Classification', 'Table View of Events', and 'Packets'. The 'Event Information' section is expanded, showing details for a message with ID 2000:1000000:3. The details include:

- Message: custom\_http\_sig (2000:1000000:3)
- Time: 2024-04-06 14:31:26
- Classification: Unknown Traffic
- Priority: low
- Ingress Security Zone: outside\_zone
- Egress Security Zone: inside\_zone
- Device: FPR2120\_FTD
- Ingress Interface: outside
- Egress Interface: inside
- Source IP: 192.168.20.1
- Source Port / ICMP Type: 80 (http) / tcp
- Destination IP: 192.168.10.1
- Destination Port / ICMP Code: 50105 / tcp
- HTTP Hostname: 192.168.20.1
- HTTP URI: /nest.txt
- Intrusion Policy: snort\_test
- Access Control Policy: acp-rule
- Access Control Rule: ftd\_acp

The rule definition is also visible: `Rule: alert tcp any any -> any any ( sid:1000000; gid:2000; flowestablished,to_client; rax_data; content:'username'; msg:'custom_http_sig'; classtype:unknown; rev:3; )`

Detail van inbraakgebeurtenis

## Veelgestelde vragen (FAQ)

Q: Wat wordt aanbevolen, Snort 2 of Snort 3?

A: Vergeleken met Snort 2, biedt Snort 3 verbeterde verwerkingsnelheden en nieuwe functies, waardoor het de meer aanbevolen optie.

Q: Na het upgraden van een versie van FTD voorafgaand aan 7.0 naar een versie 7.0 of later, wordt de kortere versie automatisch bijgewerkt aan Snort 3?

A: Nee, de inspectiemotor blijft op Snort 2. Als u Snort 3 na de upgrade wilt gebruiken, moet u deze expliciet inschakelen. Merk op dat Snort 2 is gepland om te worden afgekeurd in een toekomstige release en u wordt sterk aanbevolen om te stoppen met het nu gebruiken.

Q: In Snort 3, is het mogelijk om een bestaande douaneregel uit te geven?

A: Nee, je kunt het niet bewerken. Om een specifieke douaneregel uit te geven, moet u de relevante regel verwijderen en deze opnieuw genereren.

## Problemen oplossen

Start de opdracht `system support trace` om het gedrag op FTD te bevestigen. In dit voorbeeld wordt het HTTP-verkeer geblokkeerd door de IPS-regel (2000:1000000:3).

```
<#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:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '

ftd\_acp

', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1

Event

:

2000:1000000:3

, Action

block

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:

ips, block

Referentie

[Configuratiehandleiding voor Cisco Secure Firewall Management Center Snort 3](#)

## 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.