

# Filter snortregels op basis van SRU en LSP versie van Firepower Devices die door FMC worden beheerd

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Procedure om gesorteerde regels te filteren](#)

---

## Inleiding

Dit document beschrijft hoe u snurkregels kunt filteren op basis van de versie Cisco Secure Rule Update (SRU) en Link State Packet (LSP) van vuurkrachtapparaten die worden beheerd door het Firepower Management Center (FMC).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van opensource Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

### Gebruikte componenten

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

- Dit artikel is van toepassing op alle Firepower platforms
- Cisco Firepower Threat Defence (FTD), waarop softwareversie 7.0.0 wordt uitgevoerd
- Firepower Management Center Virtual (FMC) waarop softwareversie 7.0.0 wordt uitgevoerd

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

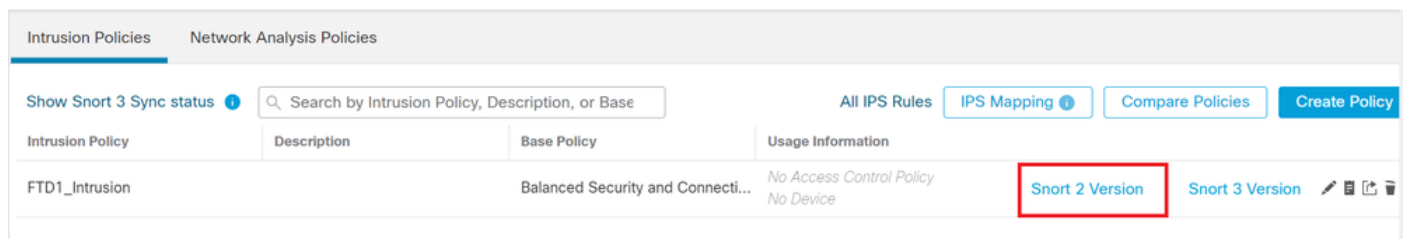
In de context van inbraakdetectiesystemen (IDS) en inbraakpreventiesystemen (IPS) staat "SID" voor "Signature ID" of "Snort Signature ID".

Een Sort Signature ID (SID) is een unieke identifier die aan elke regel of handtekening binnen de regelset is toegewezen. Deze regels worden gebruikt om specifieke patronen of gedragingen in netwerkverkeer te detecteren die kunnen duiden op kwaadaardige activiteit of beveiligingsbedreigingen. Elke regel is gekoppeld aan een SID om gemakkelijk referentie en beheer mogelijk te maken.

Bezoek de [SNORT](#)-website voor informatie over opensource Snort.

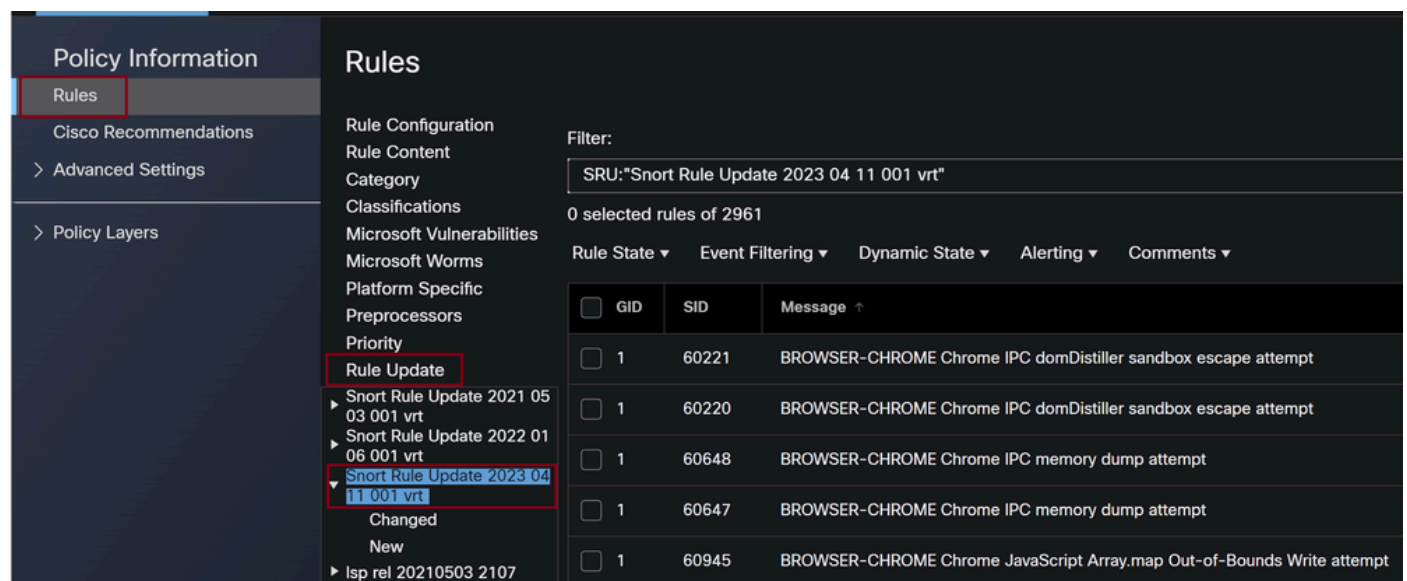
## Procedure om gesorteerde regels te filteren

Als u de SID's van de regel Sneltoets 2 wilt bekijken, navigeert u naar FMC Policies > Access Control > Intrusion, klik vervolgens op de SNORT2-optie in de rechterbovenhoek, zoals in de afbeelding:

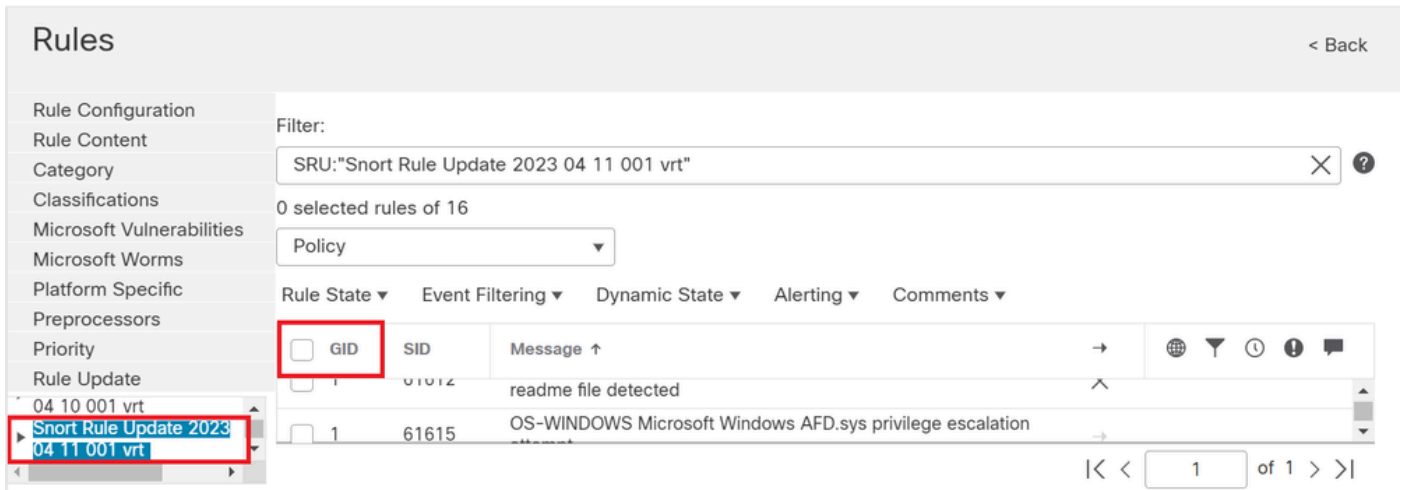


Sorteren 2

Naar navigeren Rules > Rule Update en selecteer de meest recente datum om de SID te filteren.

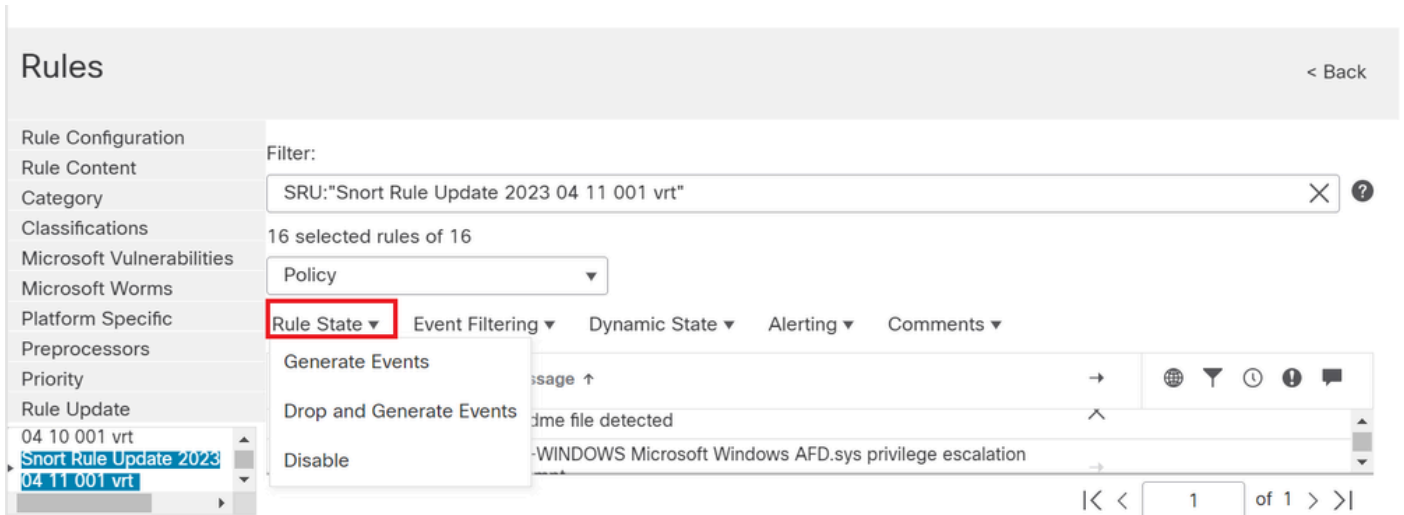


Regelupdate



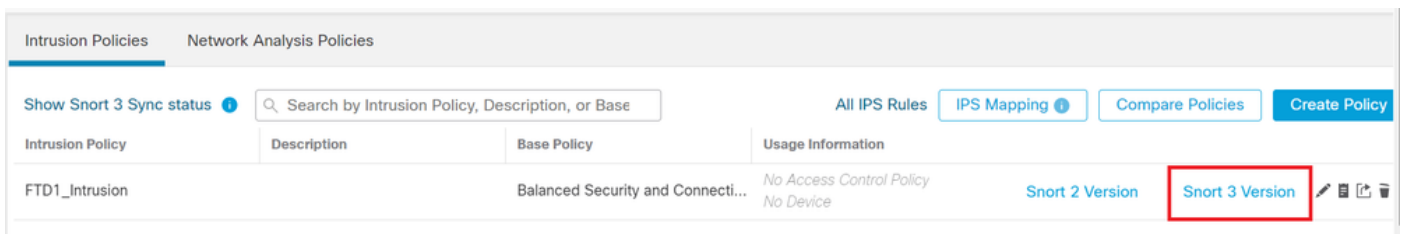
Beschikbare Sid's volgens snelregels

Selecteer een gewenste optie onder **Rule State** zoals in de afbeelding.



Regelstaten selecteren

Als u de SID's van de snort 3-regel wilt weergeven, navigeert u naar **FMC Policies > Access Control > Intrusion**. Klik vervolgens op de **SNORT3**-optie in de rechterbovenhoek, zoals in de afbeelding:



Sorteren 3

Naar navigeren **Advanced Filters** en selecteer de meest recente datum om de SID te filteren zoals in de afbeelding.

< Intrusion Policy

Policy Name  Used by: No Access Control Policy | No Device

Mode  Base Policy Balanced Security and Connectivity

Disabled 39249 | Alert 470 | Block 9151 | Overridden 0 | Rewrite 0 | Pass 0 | Drop 0 | Reject 0

Rule Groups Back To Top

50 items  Excluded | Included | Overridden

All Rules Reco

> Browser (6 groups)

> Server (8 groups)

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

48,870 rules

Preset Filters: 470 Alert rules | 9,151 Block rules | 39,249 Disabled rules | 0 Overridden rules

Advanced Filters

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
>	<input type="checkbox"/> 1:28496	<a href="#">BROWSER-IE Microsoft Internet Explore...</a>	<input type="text" value="Alert (Default)"/>	Browser/Internet Explo...

Sorteren op 3 filters

## Advanced Filters ?

LSP

Select...

Show Only \*  New  Changed

Classifications

Select...

Microsoft Vulnerabilities

Select...

Cancel

OK

LSP onder geavanceerd filter

## Advanced Filters ?

LSP

Show Only \*  New  Changed

Classifications

Microsoft Vulnerabilities

Cancel

LSP-versie

### All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 ▾ | 48,870 rules      Preset Filters: 0 Alert rules | **11 Block rules** | 11 Disabled rules | 0 Overridden rules | [Advanced Filters](#)

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

Vooraf ingestelde filter voor Sid's

Selecteer een gewenste optie onder **Rule state** zoals in de afbeelding.

### All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22  | 22 ▾ | 48,870 rules      Preset Filters: 0 Alert rules | 11 Block rules | 11 Disabled rules | 0 Overridden rules | [Advanced Filters](#)

<input checked="" type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input checked="" type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor



## 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.