

# Aanvullende maatregelen in het kader van snort 3-regels op het VCC configureren

## Inhoud

---

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Functiedetails](#)

[FMC-doortocht](#)

---

## Inleiding

In dit document wordt de ondersteuning van Firepower Management Center (FMC) beschreven voor extra handelingen volgens de regels in de versie van 7.1.

## Achtergrondinformatie

Hoewel de Firepower Threat Defence (FTD) Seven Inbraakbeleidsregels ondersteunt voor handelingen Waarschuwen/uitschakelen/blokkeren/afwijzen/herschrijven/doorgeven/neerzetten in 7.0, heeft het FMC slechts drie snort 3-regels ondersteund: "Waarschuwing", "uitschakelen" en "blokkeren".

Vanuit Firepower 7.1.0 ondersteunt het FMC de configuratie van nieuwe regelacties.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van opensource Snort
- Firepower Management Center (FMC) 7.1.0+
- Firepower Threat Defence (FTD) 7.0.0+

### Gebruikte componenten

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

- Dit document is van toepassing op alle Firepower platforms waarop Snort 3 wordt uitgevoerd
- Cisco Firepower Threat Defence Virtual (FTD), versie 7.4.2 van de software
- Firepower Management Center Virtual (FMC), waarop softwareversie 7.4.2 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.

## Functiedetails

De nieuwe snort 3 regel acties toegevoegd en hun beschrijvingen zijn als volgt:

Nummer paspoort: Geen gebeurtenis gegenereerd, maakt het mogelijk dat pakket zonder verdere evaluatie wordt doorgegeven via eventuele volgende Snortregels.

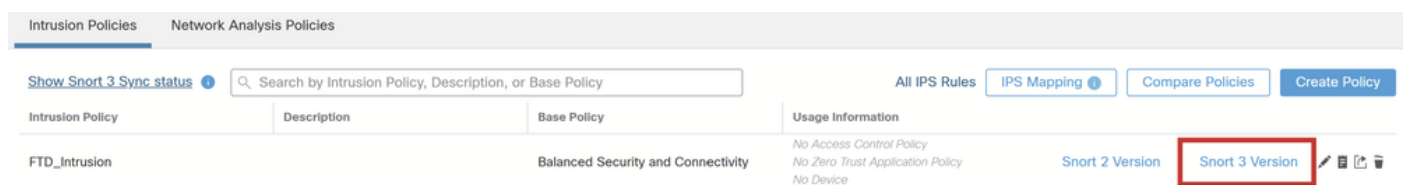
Afwijzing: Produceert gebeurtenis, laat vallen aanpassend pakket en blokkeert geen verder verkeer in deze verbinding.

Afwijzen: Produceert gebeurtenis, laat vallen aanpassend pakket, blokkeert verder verkeer in deze verbinding en verzendt TCP teruggesteld of de haven ICMP onbereikbaar naar bron en bestemmingsgastheren.

Herschrijven: Hiermee wordt een gebeurtenis gegenereerd en pakketinhoud overschreven op basis van de optie Vervangen in de regel.

## FMC-doortocht

Als u de regels voor snort 3 in een inbraakbeleid wilt weergeven, navigeert u FMC Policies > Access Control > Intrusion, vervolgens op de optie Snort 3 Version in de rechterbovenhoek van het beleid, zoals in de afbeelding:



Versie Snuit 3

Klik op Basisbeleid > Alle regels, u kunt de standaardhandelingen zien van alle systeem gedefinieerde Snort 3 regels.

< Policies / Intrusion / FTD\_Intrusion

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

Base Policy: Balanced Security and Connectivity Mode: Prevention

Active Rules 9693 Alert 474 Block 9219

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

### Balanced Security and Connectivity

50 items

All Rules

49,532 rules

Presets: Alert ( 474 ) | Block ( 9,219 ) | Disabled ( 39,839 ) | Overridden ( 0 ) | Advanced Filters

GID:SID	Rule Details	Rule Action	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet Explorer crea...	Alert (Default)	Malicious File,Drive-by Co...
1:32478	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File,Drive-by Co...
1:32479	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File,Drive-by Co...
1:26633	BROWSER-IE Microsoft Internet Explorer html...	Alert (Default)	Malicious File,Internet Expl...
1:31621	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File,Drive-by Co...
1:31622	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File,Drive-by Co...

Basisbeleid

Als u de regelactie in een van deze nieuwe regelacties wilt wijzigen, gaat u naar Regel Overschrijven > Alle regels en selecteert u de regelactie in de vervolgkeuzelijst voor de geselecteerde regel.

< Policies / Intrusion / FTD\_Intrusion

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

Base Policy: Balanced Security and Connectivity Mode: Prevention

Active Rules 9693 Alert 474 Block 9219

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

### Rule Overrides

102 items

All Rules

49,532 rules

Presets: Alert ( 474 ) | Block ( 9,219 ) | Disabled ( 39,839 ) | Overridden ( 0 ) | Advanced Filters

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive...
1:32478	BROWSER-IE Microsoft Internet ...	Block	Base Policy	Malicious File,Drive...
1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive...
1:26633	BROWSER-IE Microsoft Internet ...	Rewrite	Base Policy	Malicious File,Inter...
1:31621	BROWSER-IE Microsoft Internet ...	Drop	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Reject	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Disable	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Revert to default	Base Policy	Malicious File,Drive...

Aanvullende regelacties

< Policies / Intrusion / FTD\_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 474 Block 9219

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

**Rule Overrides** Back To Top

102 Items All x v Rule Action v Search by CVE, SID, Reference Info, or Rule Message

49,532 rules Presets: Alert ( 474 ) | Block ( 9,219 ) | Disabled ( 39,839 ) | Overridden ( 0 ) | Advanced Filters

✔ Rule action changed successfully x

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
<input type="checkbox"/>	1:28496 BROWSER-IE Microsoft Internet ...	<b>Reject</b>	Rule Override	Malicious File, Drive...
<input type="checkbox"/>	1:32478 BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
<input type="checkbox"/>	1:32479 BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
<input type="checkbox"/>	1:26633 BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Inter...

De regelhandeling wijzigen

De met voeten getreden regels zijn te vinden onder Regel met voeten treedt > Met voeten getreden Regels.

< Policies / Intrusion / FTD\_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 473 Block 9219 Others 1

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

**Rule Overrides** Back To Top

102 Items All x v Rule Action v Search by CVE, SID, Reference Info, or Rule Message

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

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
<input type="checkbox"/>	1:28496 BROWSER-IE Microsoft Internet ...	<b>Reject</b>	Rule Override	Malicious File, Drive...

Opheffing regels

## 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.