# Aangepaste lokale snelregels op een Cisco FireSIGHT-systeem

## Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Werken met de aangepaste lokale regels](#)
[Lokale regels importeren](#)
[Lokale regels bekijken](#)
[Lokale regels inschakelen](#)
[Bekijk de verwijderde lokale regels](#)
[Nummering van de plaatselijke regels](#)

## Inleiding

Een aangepaste lokale regel op een FireSIGHT System is een aangepaste standaard Snortregel die u importeert in een ASCII-tekstbestandsindeling vanuit een lokale machine. Met een FireSIGHT System kunt u lokale regels importeren via de webinterface. De stappen om lokale regels te importeren zijn heel eenvoudig. Om een optimale lokale regel te schrijven, heeft een gebruiker echter diepgaande kennis nodig over de Snort- en netwerkprotocollen.

Het doel van dit document is om u tips en hulp te bieden bij het schrijven van een aangepaste lokale regel. De instructies voor het maken van lokale regels zijn beschikbaar in de *Snort User Manual,* die beschikbaar is op snort.org. Cisco raadt u aan de gebruikershandleiding te downloaden en te lezen voordat u een aangepaste lokale regel schrijft.

> **Opmerking:** De regels die in een Sourcefire Rule Update (SRU) worden geleverd, worden aangemaakt en getest door de Cisco Talos Security Intelligence en Research Group, en ondersteund door het Cisco Technical Assistance Center (TAC). Cisco TAC biedt geen ondersteuning bij het schrijven of afstemmen van een aangepaste lokale regel. Als u echter problemen ondervindt met de functionaliteit voor het importeren van regels van uw FireSIGHT-systeem, neem dan contact op met Cisco TAC.

> **Waarschuwing**: Een slecht geschreven aangepaste lokale regel kan invloed hebben op de prestaties van een FireSIGHT-systeem, wat kan leiden tot prestatieverslechtering van het gehele netwerk. Als u problemen ondervindt met de prestaties in uw netwerk en er zijn aangepaste lokale snelregels ingeschakeld op uw FireSIGHT-systeem, raadt Cisco u aan die lokale regels uit te schakelen.

# Voorwaarden

## Vereisten

Cisco raadt u aan kennis te hebben van Snelregels en het FireSIGHT-systeem.

## Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Het FireSIGHT Management Center (ook bekend als Defense Center)
- Software versie 5.2 of hoger

# Werken met de aangepaste lokale regels

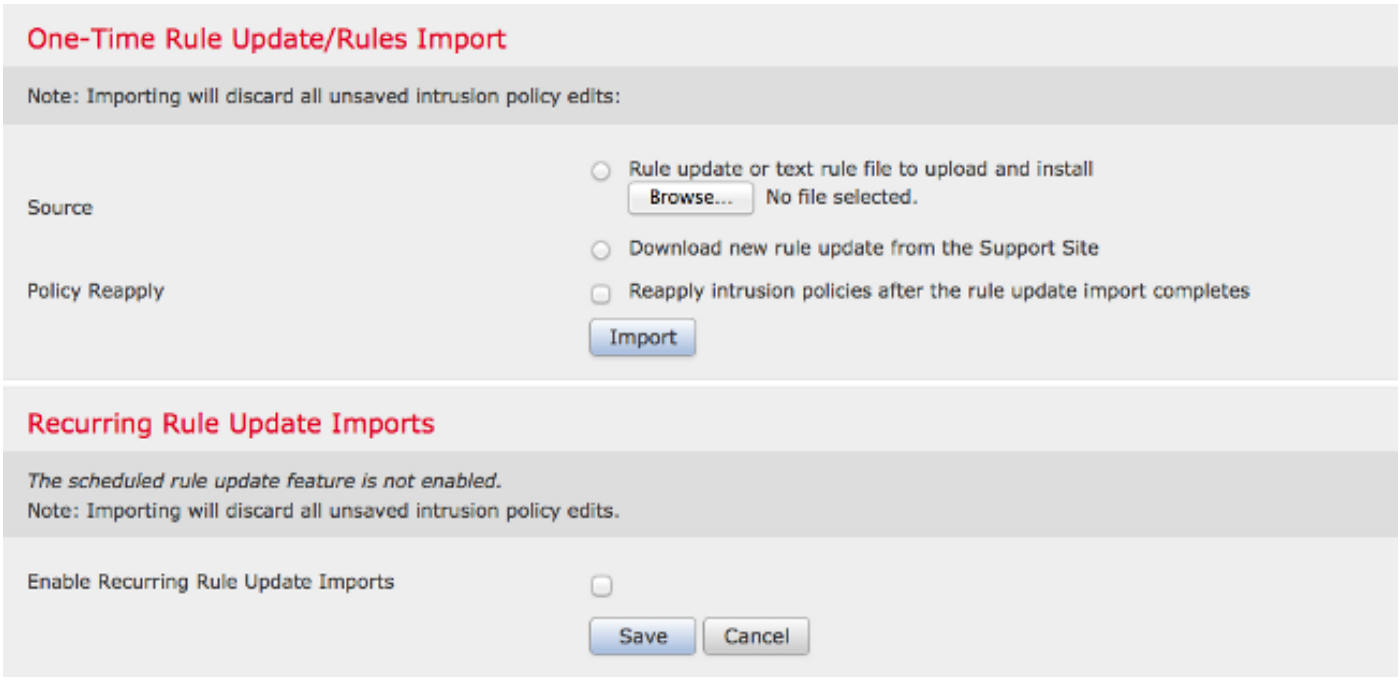
## Lokale regels importeren

Voordat u begint, moet u ervoor zorgen dat de regels in het bestand geen ontsnappingstekens bevatten. De regelimporteur vereist dat alle aangepaste regels worden geïmporteerd met ASCII- of UTF-8-codering.

De volgende procedure legt uit hoe u lokale standaardtekstregels kunt importeren van een lokale machine:

1. Ga naar de pagina **Regel editor** door te navigeren naar **Beleid > Inbraakproces > Regel-editor**.

2. Klik op **Regels importeren**. De pagina **Regel updates** verschijnt.




*Afbeelding: Een screenshot van de pagina Regel updates*

3. Selecteer **Regelupdate of tekstregelbestand om te uploaden en te installeren** en klik op **Bladeren** om het regelbestand te selecteren.

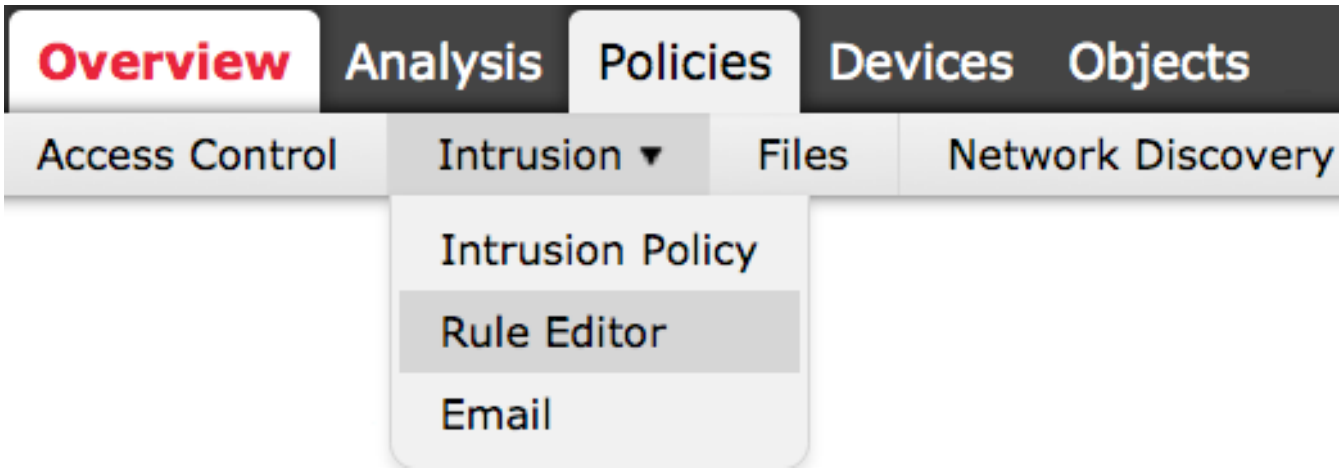
> **Opmerking:** Alle geüploade regels worden opgeslagen in de categorie **lokale regels**.

4. Klik op **Importeren**. Het regelbestand wordt geïmporteerd.

> **Voorzichtig:** De FireSIGHT-systemen maken geen gebruik van de nieuwe regel die voor inspectie is ingesteld. Om een lokale regel te activeren, moet u deze inschakelen in het inbraakbeleid en vervolgens het beleid toepassen.

## Lokale regels bekijken

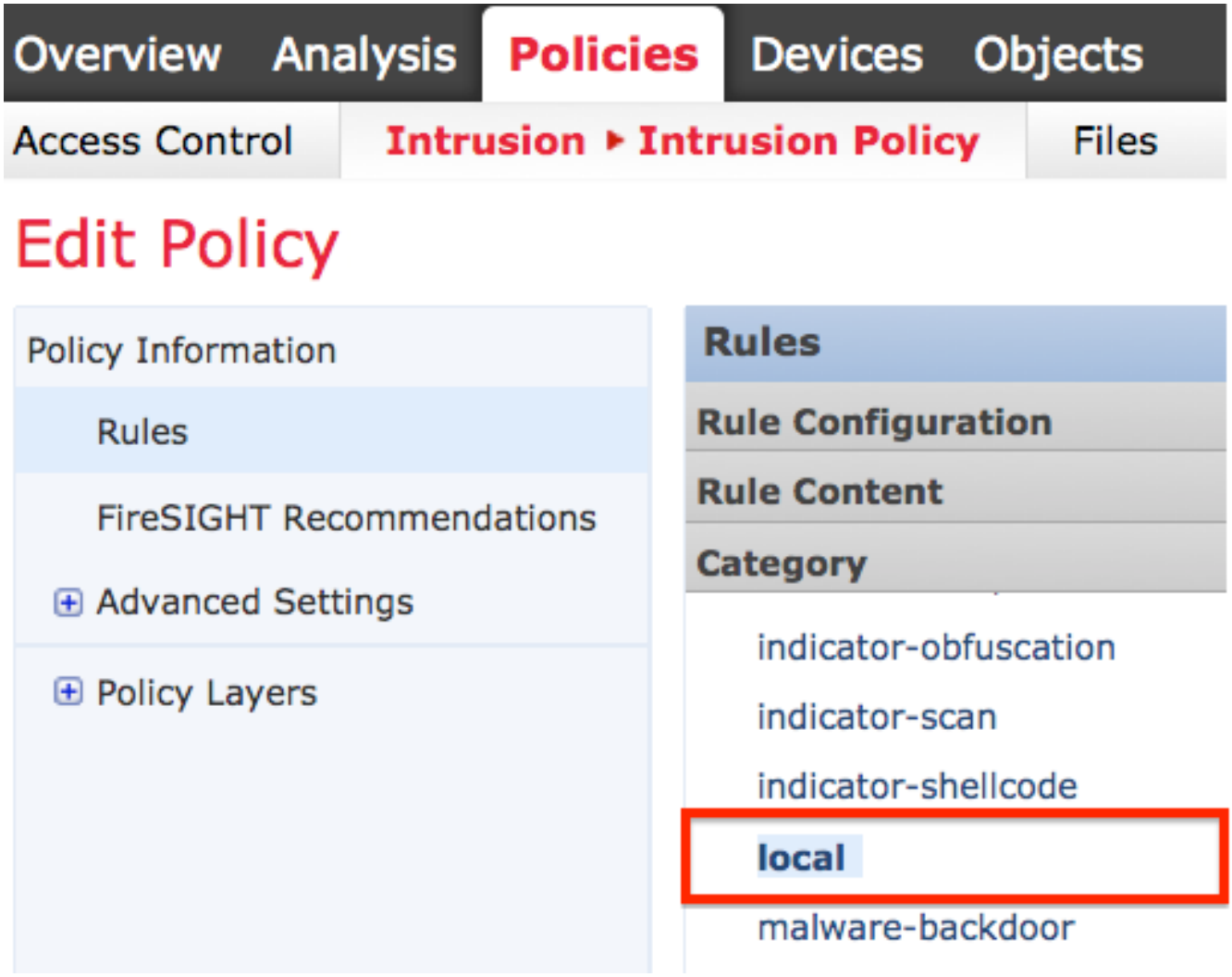
- Om het revisienummer voor een huidige lokale regel te bekijken, navigeer je naar de pagina **van de** regeleditor (**Beleid > Indringing > Regeleditor**).



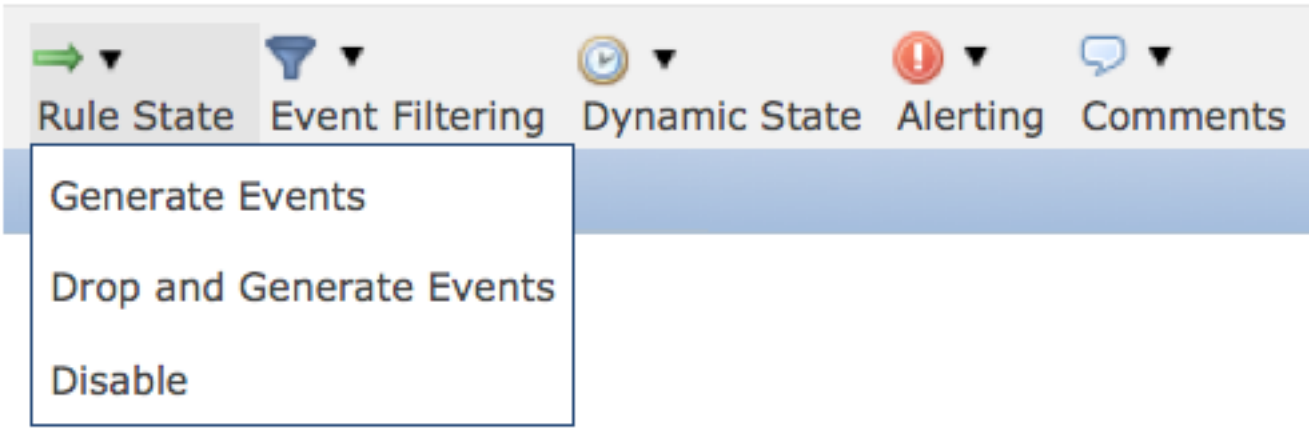

- Klik op de pagina Regel editor op de categorie **Lokale regel** om de map uit te vouwen en klik vervolgens op **Bewerken** naast de regel.
- Alle geïmporteerde lokale regels worden automatisch opgeslagen in de categorie **lokale regels**.

## Lokale regels inschakelen

- Standaard stelt het FireSIGHT-systeem de lokale regels in een uitgeschakelde toestand in. U moet de staat van lokale regels handmatig instellen voordat u ze kunt gebruiken in uw inbraakbeleid.
- Om een lokale regel mogelijk te maken, navigeer je naar de pagina Policy Editor (**Policy > Inbraakbeleid > Inbraakbeleid**). Selecteer **Regels** in het linkerdeelvenster. Selecteer onder de **categorie Lokaal**. Alle plaatselijke regels moeten worden vermeld, indien beschikbaar.




- Selecteer na het selecteren van de gewenste lokale regels een status voor de regels.




- Zodra de regelstatus is geselecteerd, klikt u op de optie **Beleidsinformatie** in het linkerpaneel. Selecteer de knop **Wijzigingen vastleggen**. Het inbraakbeleid wordt gevalideerd.

  **Opmerking:** De beleidsvalidatie mislukt als u een geïmporteerde lokale regel inschakelt die het afgekeurde trefwoord drempelwaarde in combinatie met de drempelwaarde voor inbraakgebeurtenissen in een inbraakbeleid gebruikt.

## Bekijk de verwijderde lokale regels

- Alle verwijderde lokale regels worden verplaatst van de categorie lokale regels naar de categorie verwijderde regels.
- Om het revisieaantal van een geschrapte lokale regel te bekijken, ga naar de pagina van de **Redacteur van de Regel**, klik op de **geschrapte** categorie om de map uit te breiden, dan klik het *potlood* pictogram om het detail van de regel in de **pagina van de Redacteur van de Regel** te bekijken.

## Nummering van de plaatselijke regels

- U hoeft geen generator (GID) op te geven. als u dit wel doet, kunt u alleen GID 1 voor een standaard tekstregel of 138 voor een gevoelige gegevensregel opgeven.
- Geef geen SID (snort ID) of revisienummer op wanneer u een regel voor het eerst importeert; dit voorkomt botsingen met SID's van andere regels, waaronder verwijderde regels.
- Het FireSIGHT Management Center wijst automatisch de volgende beschikbare aangepaste regel SID van 1000000 of hoger toe, en een herzieningsnummer van 1.
- Als u probeert een inbraakregel te importeren met een SID groter dan 2147483647, zal een validatiefout optreden.
- U moet de SID die is toegewezen door IPS en een revisienummer groter dan het huidige revisienummer opnemen wanneer u een bijgewerkte versie van een lokale regel importeert die u eerder hebt geïmporteerd.
- U kunt een lokale regel die u hebt verwijderd, herstellen door de regel te importeren met behulp van de SID die is toegewezen door IPS en een revisienummer dat groter is dan het huidige revisienummer. Merk op dat het FireSIGHT Management Center het revisienummer automatisch verhoogt wanneer u een lokale regel verwijdert; dit is een apparaat waarmee u lokale regels kunt herstellen.

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.