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

Inhoud

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.

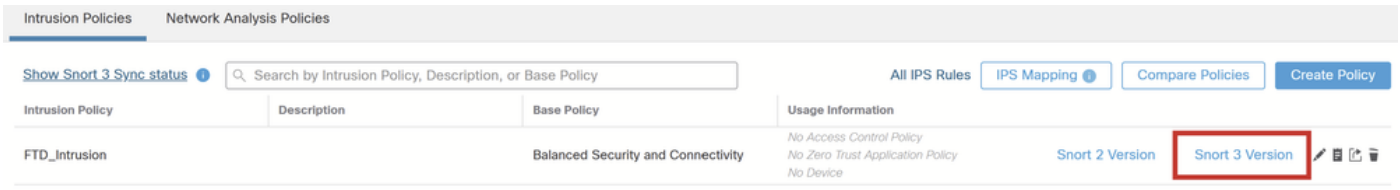
Afwijzing: Produceert gebeurtenis, laat vallen aanpassend pakket en blokkeert geen verder verkeer in deze verbinding.

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.

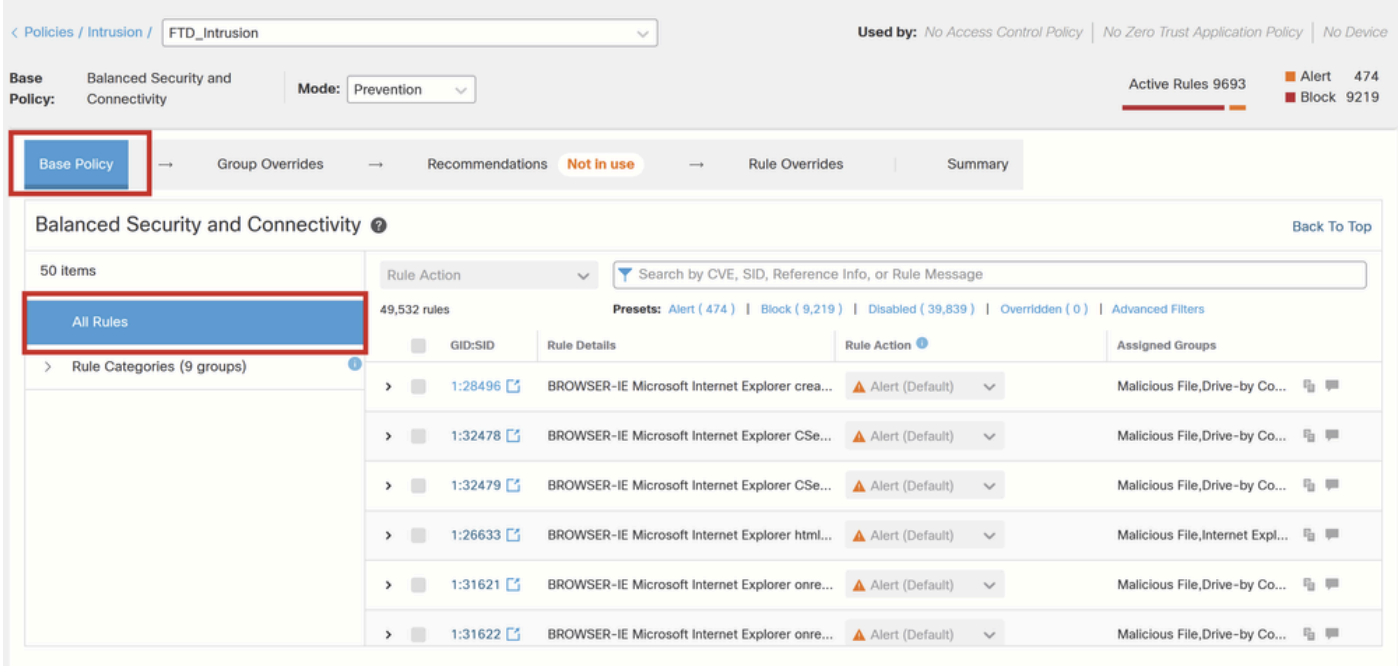
FMC-doortocht

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



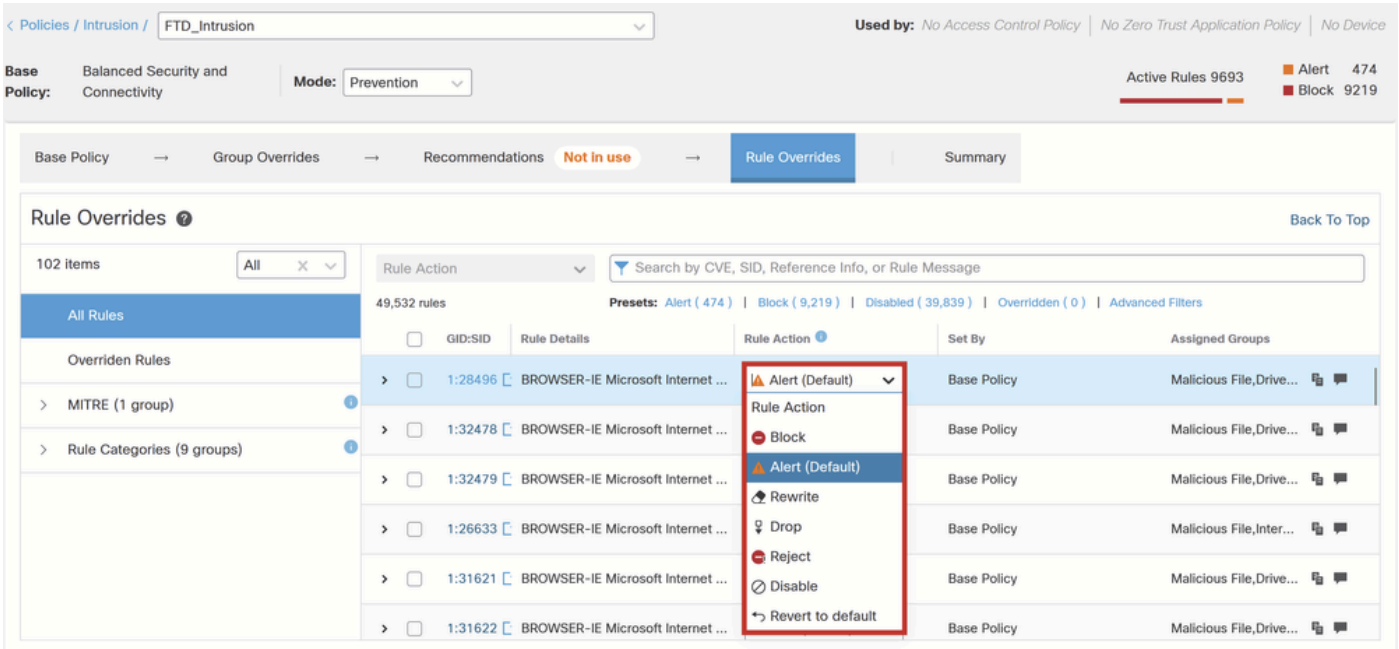
Versie Snuit 3

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

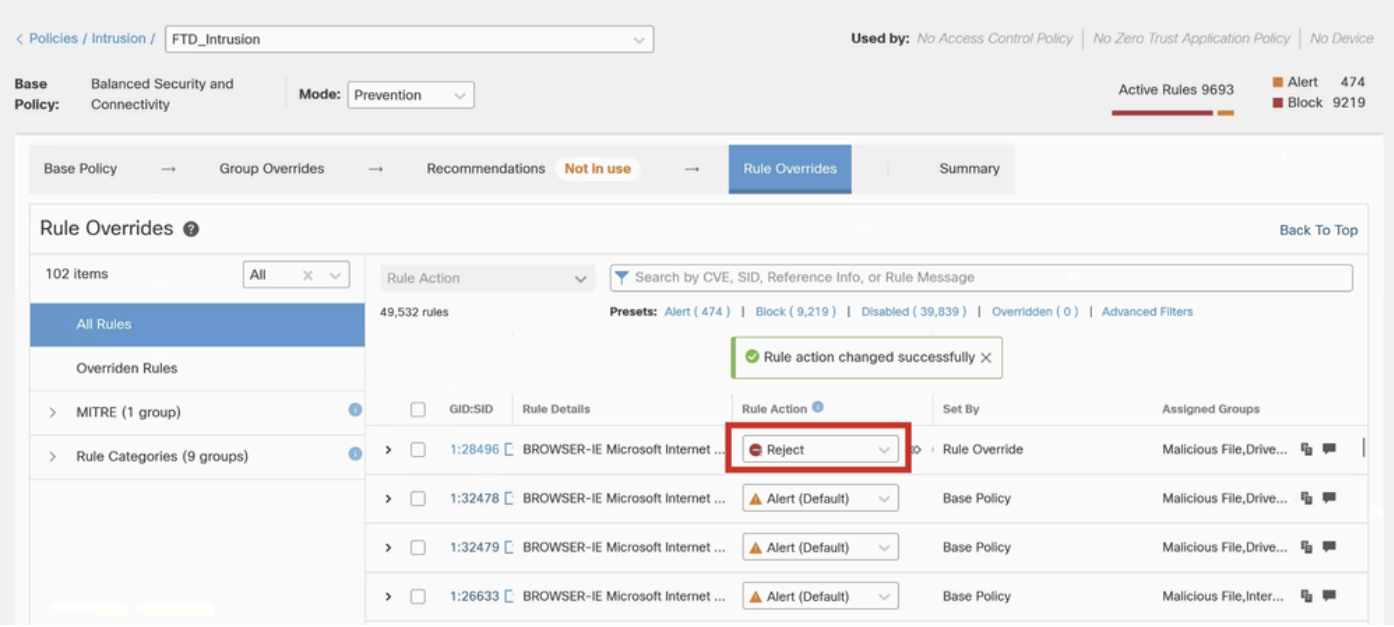


Basisbeleid

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.

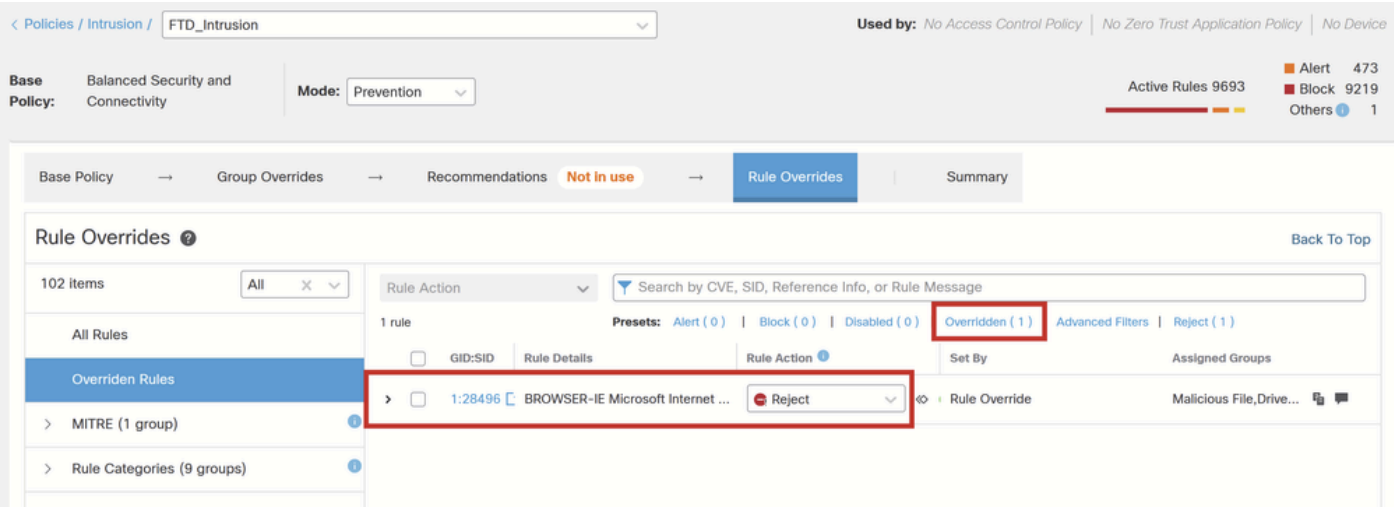


Aanvullende regelacties



De regelhandeling wijzigen

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



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.