Opties om foutieve positieve inbraakingen te verminderen

Inhoud

Inleiding

Een inbraakpreventiesysteem kan buitensporige waarschuwingen op een bepaalde kortingsregel opleveren. De waarschuwingen kunnen waar positief of fout-positief zijn. Als u veel valse positieve waarschuwingen ontvangt, zijn er verschillende opties beschikbaar om deze te beperken. Dit artikel geeft een overzicht van de voor- en nadelen van elke optie.

Opties om foutieve positieve meldingen te beperken

> Opmerking: Deze opties zijn gewoonlijk niet de beste keuze, maar kunnen onder bepaalde omstandigheden de enige oplossing zijn.

1. Rapport aan Cisco Technical Support

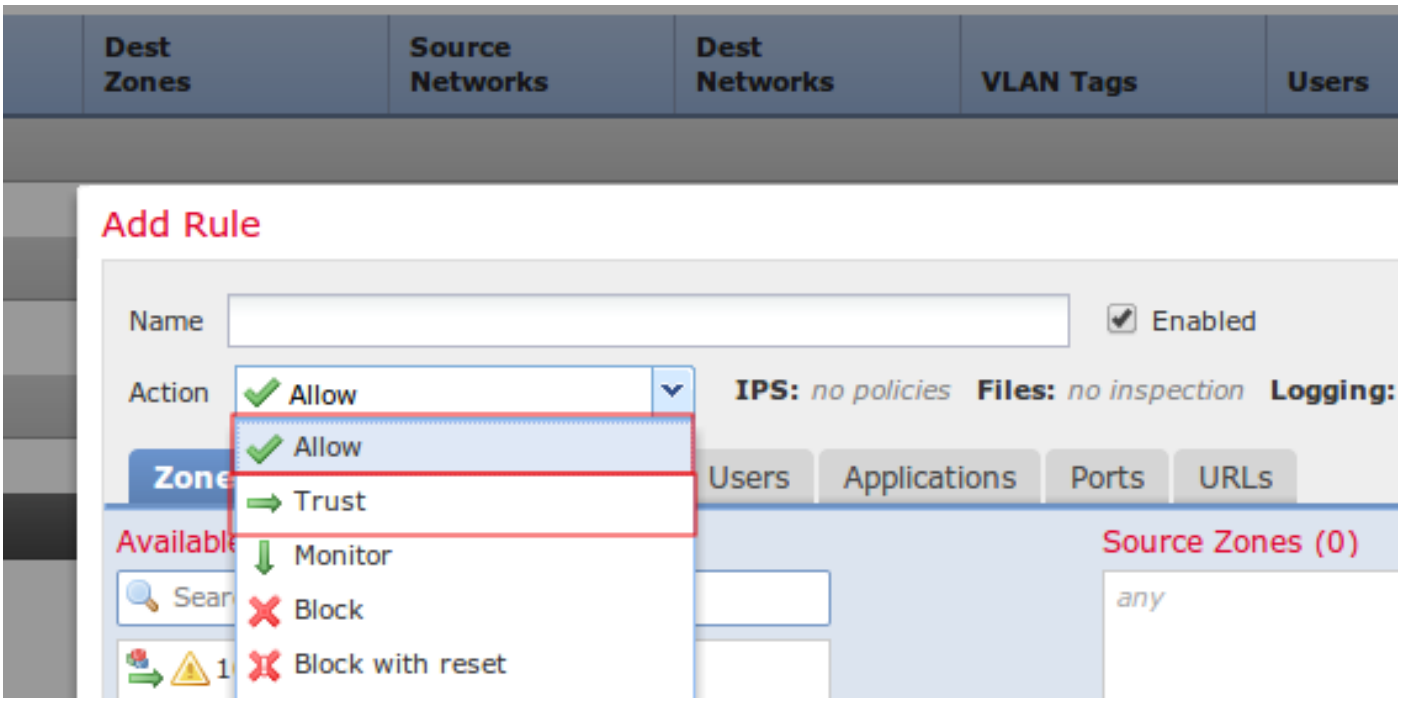
Als u een kortregel vindt die waarschuwingen op goedkoop verkeer instelt, moet u deze aan Cisco Technical Support melden. Als dit eenmaal is gemeld, escaleert een Customer Support Engineer het probleem tot kwetsbaarheids Research Team (VRT). VRT onderzoekt mogelijke verbeteringen van de regel. Betere regels zijn doorgaans beschikbaar voor de verslaggever zodra ze beschikbaar zijn, en worden ook toegevoegd aan de volgende officiële bijwerking.

2. Vertrouwen of toestaan van regels

De beste optie om een betrouwbaar verkeer toe te staan om zonder inspectie door een Sourcefire-apparaat te lopen is **vertrouwen** in **stellen** of actie **toestaan** zonder een gekoppeld inbraakbeleid. Om een trust te configureren of regel toe te staan, navigeer dan naar **beleid > Toegangsbeheer > Toevoegen regel**.

> Opmerking: Verkeersmatching Trust of laat regels toe die niet zijn ingesteld om gebruikers,

toepassingen of URL's aan elkaar te koppelen, zal minimale invloed hebben op de algehele prestaties van een Sourcefire-apparaat, omdat dergelijke regels in FirePOWER-hardware kunnen worden verwerkt.



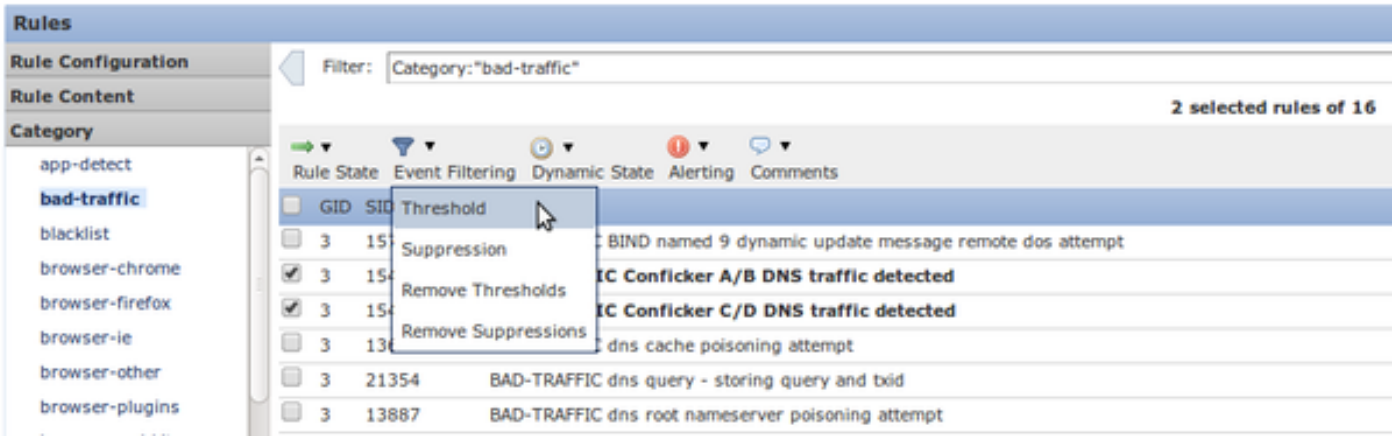
Afbeelding: Configuratie van een vertrouwensregel

3. Onnodige regels uitschakelen

U kunt regels van de Kort die oude en gepatcheerde kwetsbaarheden mikken. Het verbetert de prestaties en vermindert valse positieven. Met FireSIGHT-aanbevelingen kunt u deze taak ondersteunen. Daarnaast kunnen regels die veelvuldig signaleringen met een lage prioriteit opleveren of signaleringen die niet kunnen worden uitgevoerd, goede kandidaten zijn voor verwijdering uit een inbraakbeleid.

4. Drempel

U kunt **Drempel** gebruiken om het aantal inbraakgebeurtenissen te verminderen. Dit is een goede optie om te vormen wanneer van een regel wordt verwacht dat deze regelmatig een beperkt aantal gebeurtenissen op normaal verkeer teweegbrengt, maar zou een indicatie van een probleem kunnen zijn wanneer meer dan een bepaald aantal pakketten met de regel overeenkomt. U kunt deze optie gebruiken om het aantal gebeurtenissen te beperken dat wordt veroorzaakt door ruis.



Afbeelding: Configuratie van de drempel

5. Onderdrukking

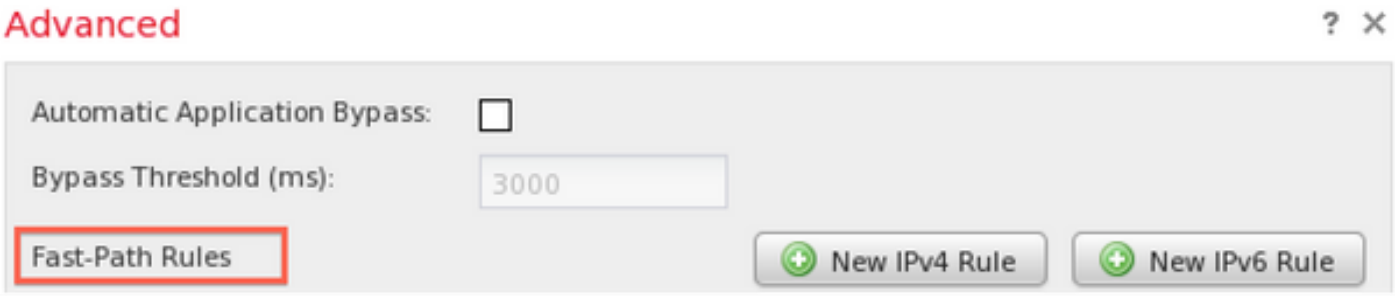
U kunt **Suppression** gebruiken om het bericht van gebeurtenissen volledig te elimineren. Deze is ingesteld op **Drempel**.

> **Voorzichtig:** De suppressie kan prestatiekwesties leiden, omdat, terwijl er geen gebeurtenissen worden gegenereerd, Snort nog het verkeer moet verwerken.

> Opmerking: De suppressie voorkomt niet dat regels afvallen en het verkeer daalt, dus het verkeer kan in stilte worden teruggedraaid wanneer het overeenkomt met de uitrolregel.

6. Regels voor Fast Path

Overeenkomstig met Vertrouwen en regels van het Toegangsbeleid toestaan kunnen Fast-Path-regels ook inspectie omzeilen. Technische ondersteuning van Cisco raadt het gebruik van Fast-Path-regels over het algemeen niet aan, omdat ze zijn geconfigureerd in het **Advanced** venster van de pagina van het **apparaat** en omdat de regels voor toegangscontrole vrijwel altijd voldoende zijn.



Afbeelding: De optie Fast-Path Rules in het venster Advanced.

Het enige voordeel om fast-path regels te gebruiken is dat ze een groter maximum volume verkeer kunnen verwerken. Fast-Path-regels verwerken verkeer op het hardwareniveau (bekend als NMSB) en kunnen theoretisch tot 200 Gbps verkeer verwerken. Daarentegen worden regels met **vertrouwen** en staan acties gepromoot naar de Network Flow Engine (NFE) en kunnen deze een maximum van 40 Gbps aan verkeer verwerken.

Opmerking: Fast-Path-regels zijn alleen beschikbaar voor 8000 Series apparaten en de 3D9900.

7. Voorschriften

Om te voorkomen dat een specifieke regel op verkeer van een bepaalde gastheer van start gaat (terwijl ander verkeer van die gastheer moet worden geïnspecteerd), gebruik een van *het* type *passeergewoonte* regel. In feite is dit de enige manier om het voor elkaar te krijgen. Hoewel regels doorgeven effectief is, kan het heel moeilijk zijn ze te onderhouden omdat regels handmatig worden geschreven. Daarnaast, als de oorspronkelijke regels van de passeerregels door een regelupdate worden gewijzigd, moeten alle bijbehorende passenregels handmatig worden bijgewerkt. Anders kunnen ze ineffectief worden.

8. SNORT_BPF variabele

De variabele Snort_BPF in een inbraakbeleid maakt bepaald verkeer in staat om inspectie te omzeilen. Terwijl deze variabele een van de eerste keuzes was op oudere softwareversies, adviseert Cisco Technical Support om een regel voor toegangscontrole te gebruiken om inspectie te omzeilen, omdat de variabele korter, zichtbaarder en veel gemakkelijker te configureren is.