Quality-of-Service (DoS) SYN-filtering op 300 Series Managed-switches

Doel

Een Denial of Service (DoS)-aanval treft overstromingen in een netwerk met vals verkeer. Hiermee worden netwerkserverbronnen niet bij legitieme gebruikers gebruikt. Een SYN-overstroming doelt in het bijzonder het TCP-protocol. TCP-protocol vereist drie stappen om te functioneren. Eerst stuurt een gebruiker hun IP-adres naar de server en vraagt hij om een verbinding. Daarna reageert de server op het verzoek en wacht de bevestiging af. Tenslotte erkent de gebruiker dat de server een verbinding heeft geopend. Een TCP SYN-aanval gebruikt meerdere IP-adressen om een verbinding aan te vragen, maar stuurt nooit een bevestiging terug naar de server nadat een verbinding is geopend. Een server kan slechts een beperkte hoeveelheid verbindingen openen alvorens het TCP verzoeken, zelfs van legitieme gebruikers begint te laten vallen.

TCP-verkeer wordt verzonden op verschillende virtuele poorten. Deze havens zijn een manier om netwerkverkeer in gemeenschappelijke groepen te verdelen. Het SYN-filter kan worden ingesteld om verkeer vanaf een bepaalde virtuele poort te blokkeren. Bovendien wordt het SYN-filteren ingesteld op een echte, fysieke poort of LAG op de schakelaar. Dit artikel legt uit hoe u SYN-filtering op de 300 Series Managed-switches moet configureren.

Opmerking: Syn-filters kunnen alleen worden gebruikt als DoS Prevention is ingeschakeld. Raadpleeg de *instellingen van* het artikel *Security Suite voor 300 Series Managed-switches* voor hulp.

Toepasselijke apparaten

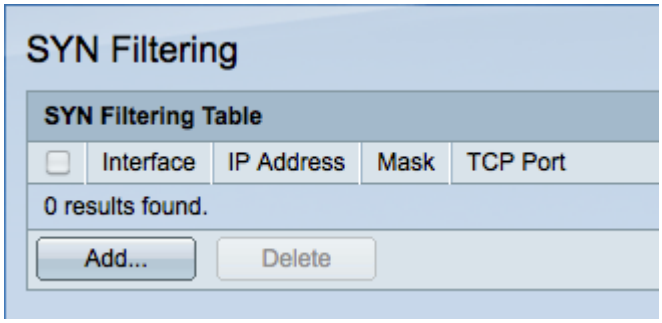
- SF/SG 300 Series Managed-switches

Softwareversie

- v1.2.7.76

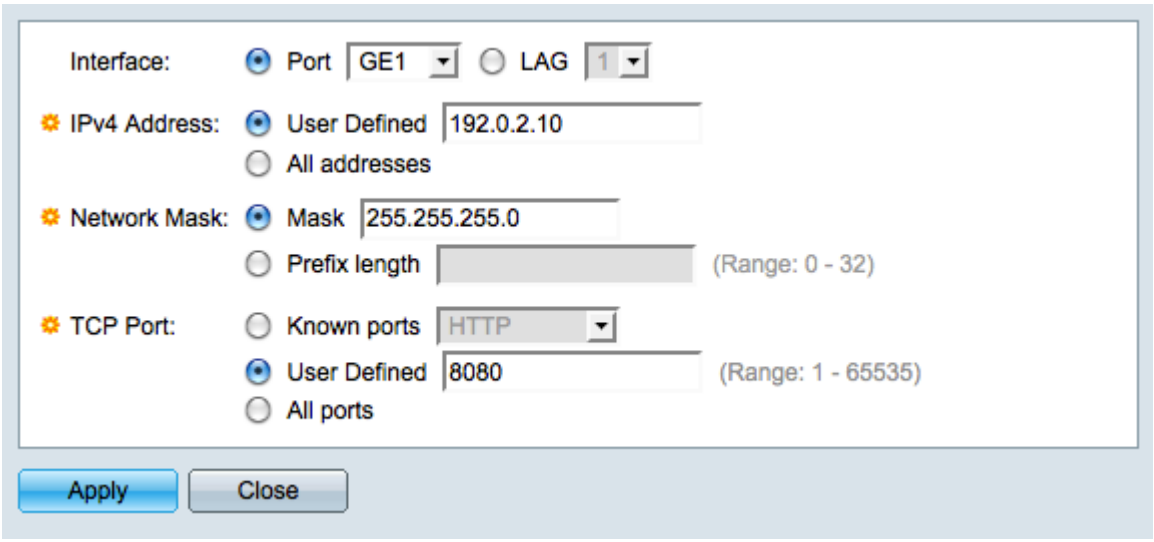
Configuratie SYN-filtering

Stap 1. Meld u aan bij het web-configuratieprogramma en kies **Security > Denial of Service Prevention > SYN Filtering**. De pagina *SYN-filtering* wordt geopend:



Stap 2. Klik op **Add** om een nieuw SYN-filter toe te voegen. Het venster *Syn Filtering*

toevoegen verschijnt.



Stap 3. Klik op de radioknop die overeenkomt met de gewenste interface in het interfaceveld. Dit is de fysieke locatie waaraan het filter zal worden toegewezen.

- Port - de fysieke poort op de schakelaar. Kies een specifieke poort in de vervolgkeuzelijst Port.
- LAG — Een groep havens die als één haven fungeren. Kies een specifiek LAG in de vervolgkeuzelijst LAG.

Stap 4. Klik op de radioknop die overeenkomt met het gewenste IPv4-adres in het veld IPv4-adres.

- Gebruiker gedefinieerd - Voer een IP-adres in dat voor TCP-verkeer moet worden gefilterd.
- Alle adressen - alle IPv4 adressen worden gefilterd voor TCP-verkeer. Naar Stap 6 indien Alle adressen zijn geselecteerd.

Stap 5. Klik op de radioknop die met de methode overeenkomt die wordt gebruikt om het subnetmasker van het IP-adres in het veld Netwerkmasker te definiëren.

- masker - Voer het netwerkmasker in het veld Netwerkmasker in.
- Lengte voorvoegsel — Voer de lengte van het prefix in (gehele getal in het bereik van 0 tot 32) in het veld Lengte Prefixeren.

Stap 6. Klik op de radioknop die overeenkomt met de gewenste TCP-poort die in het veld TCP-poort wordt gefilterd. Dit zijn de virtuele poorten waarin het netwerkverkeer is verdeeld.

- Bekende poorten — Kies een TCP poort die u kunt filteren in de vervolgkeuzelijst Bekende poorten.
- Gebruiker gedefinieerd - Voer een TCP-poort in om te filteren.
- Alle poorten — alle TCP-poorten worden gefilterd.

Stap 7. Klik op **Toepassen** om uw wijzigingen op te slaan en klik vervolgens op **Sluiten** om het venster *Syn Filtering toevoegen* te sluiten.