Synchronize (SYN) Filtering Configuration op de 300 Series Managed-switches

Doel

TCP is een protocol op de transportlaag dat betrouwbare, geordende levering van pakketten voorziet en ook voor detectie van fouten en voor verloren gegevens om terugzending te veroorzaken tot de gegevens correct en volledig ontvangen zijn. Voordat de client gegevens verstuurt, vraagt deze om een verbinding met een synchroon (SYN) pakket naar de server om de verbinding te starten. De server verstuurt dan een SYN- en erkenningspakket (ACK) naar de client en de client verstuurt een ACK-pakket om de serverrespons te erkennen. Na deze drierichtingsverbinding tussen de client en de server kunnen gegevens worden verzonden.

Een SYN-aanval op de overstromingen gebeurt wanneer deze TCP-handdruk wordt onderbroken. Een kwaadaardige client overspoelt de server met SYN-pakketten, reageert de server met SYN en ACK-pakketten voor alle kwaadaardige clientverzoeken, maar de kwaadaardige client stuurt geen ACK-pakketten terug. De server wacht op een ACK-pakket dat eenvoudigweg niet zal arriveren, dat de bronnen van de server voor legitieme gebruikers verbruikt en uiteindelijk het netwerk neerbrengt. SYN-filtering voorkomt deze aanvallen. Dit artikel legt uit hoe u SYN-filtering op de 300 Series Managed-switches moet configureren.

Toepasselijke apparaten

- SF/SG 300 Series Managed-switches

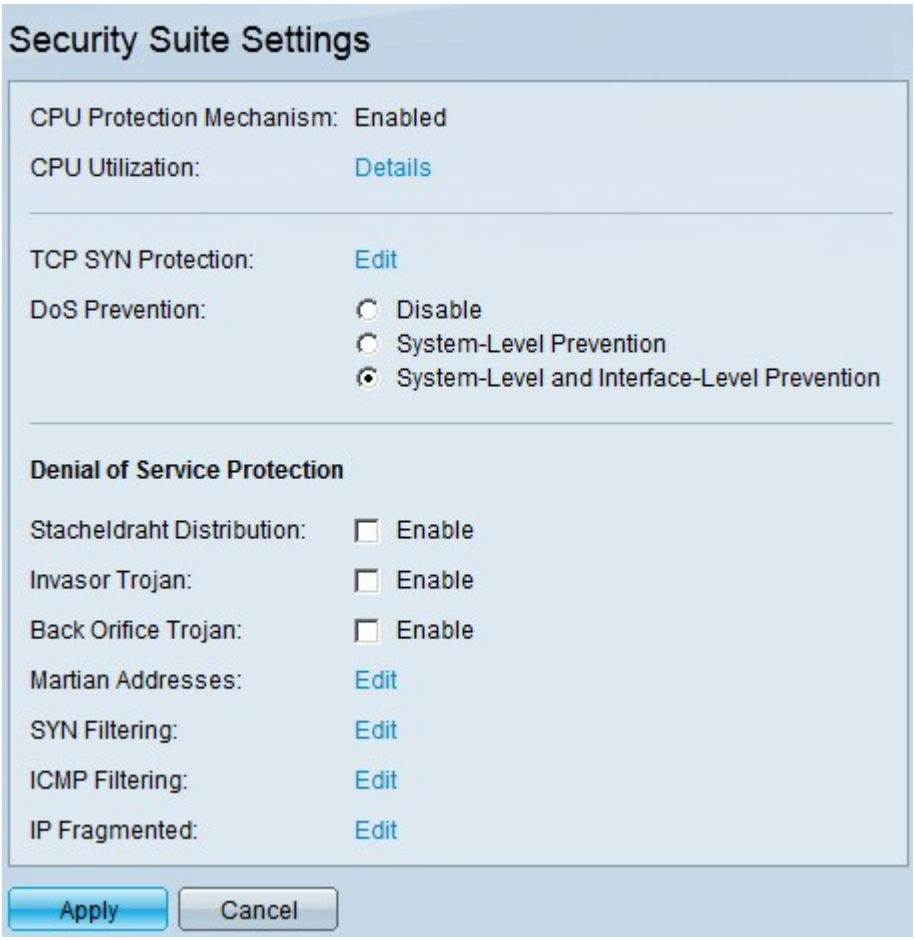
Softwareversie

- v1.2.7.76

voorkoming van serviceniveau inschakelen

Om SYN-filtering toe te passen, moet u eerst zorgen dat de switch in de juiste preventie van serviceniveau is voorzien. In dit gedeelte wordt uitgelegd hoe u het juiste preventieniveau op de 300 Series Managed-switches kunt instellen.

Stap 1. Meld u aan bij het programma voor webconfiguratie en kies **Security > Denial of Service Prevention > Security Suite-instellingen.** De pagina *Instellingen Security Suite* wordt geopend:



Stap 2. In het veld DoS Prevention zijn er drie niveaus van preventie. Klik op **systeemniveau en interfaceniveau-preventie**. Dit niveau laat u SYN-filtering configureren.

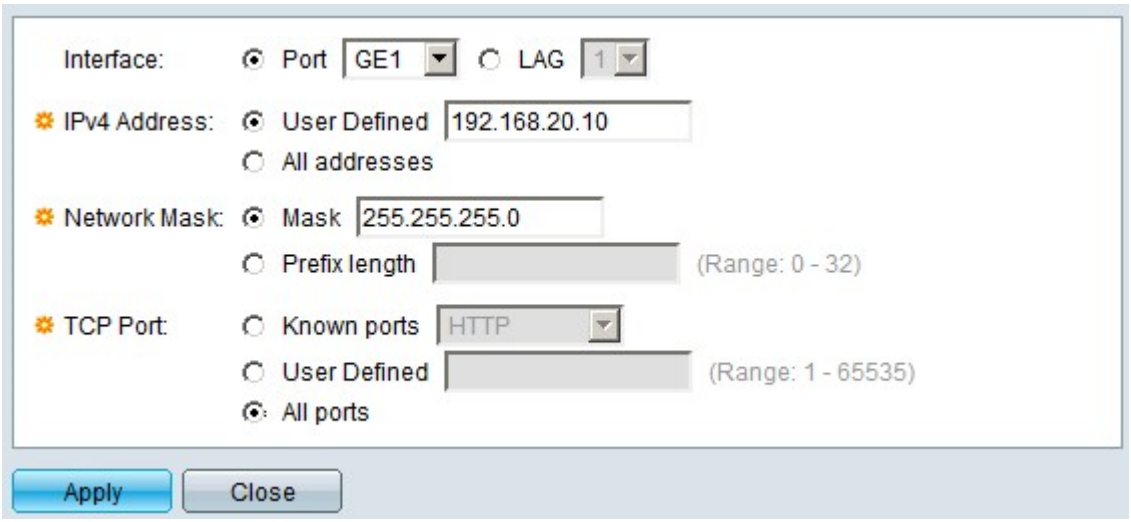
Stap 3. Klik op **Toepassen** om de configuratie op te slaan.

TCP SYN-pakketten filteren

In dit gedeelte wordt uitgelegd hoe u SYN-filtering op de 300 Series Managed-switches kunt configureren.

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**. Het venster *SYN-filtering* toevoegen verschijnt:



Stap 3. Klik in het veld Interface op de radioknop van een van de beschikbare interfaceopties:

- Port - Hiermee kunt u de poort selecteren waarvan u SYN-pakketten wilt filteren uit de vervolgkeuzelijst.
- LAG - Hiermee kunt u de LAG kiezen waaruit u SYN-pakketten wilt filteren in de vervolgkeuzelijst Link Aggregation Group (LAG). Een LAG groepeert meerdere poorten in één logische poort.

Stap 4. Klik in het veld IPv4-adres op de radioknop van een van de beschikbare opties om het IPv4-adres/adressen te definiëren om SYN-pakketten te filteren van:

- Gebruikershandleiding — Hiermee kunt u het IPv4-adres invoeren waarvoor het filter van de SYN-pakketten is gedefinieerd.
- Alle adressen - Deze optie filtert alle IPv4 adressen voor SYN-pakketten.

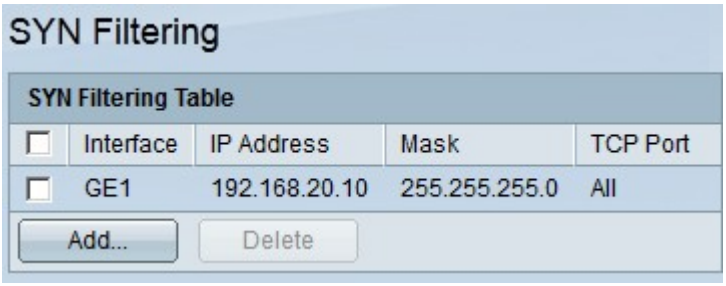
Stap 5 Klik in het veld Netwerkmasker op de radioknop van een van de beschikbare opties om het netwerkmasker van het IP-adres in Stap 4 in te voeren:

- masker - Met deze optie kunt u het subnetmasker van het IP-adres invoeren.
- Lengte prefixmasker - Met deze optie kunt u het IP-adres van het subnetmasker in het prefix-formaat invoeren.

Stap 5. Klik in het veld TCP-poort op een van de beschikbare opties om de TCP-poorten te bepalen om te filteren:

- Bekende poorten — Met deze optie kunt u poorten kiezen uit de vervolgkeuzelijst Bekende poorten. Bijvoorbeeld HTTP is 80 en TELNET is 23.
- Gebruikershandleiding — Met deze optie kunt u de TCP-poortnummers naar filter invoeren.
- Alle poorten — Deze optie filtert alle TCP-poorten.

Stap 6. Klik op **Toepassen** om de configuratie op te slaan. De wijzigingen worden aangebracht in de tabel SYN-filtering:



Stap 7. (Optioneel) om een SYN-filter te verwijderen in de tabel SYN-filtering, schakelt u het vakje in het SYN-filter dat u wilt verwijderen. Klik vervolgens op **Verwijderen**.