Internet Control Message Protocol (ICMP), Filtering Configuration voor de 300 Series Managed-switches

Doel

Internet Control Message Protocol (ICMP) is een protocol op de netwerklaag dat wordt gebruikt om fouten te melden en ter kennis te brengen, alsmede om fouten te ontdekken. Er zijn veel aanvallen die op een netwerk met ICMP kunnen worden uitgevoerd. Een ICMP flood Denial of Service (DoS)-aanval van de overstromingen is bijvoorbeeld een aanval die de kwetsbaarheden van het ICMP-protocol en de incorrecte netwerkconfiguratie exploiteert. ICMP-filtering is een oplossing om dit soort aanvallen op het netwerk te voorkomen. U kunt de schakelaar configureren om de IP-adressen of -poorten te filteren waarvan u ICMP-pakketten wilt blokkeren. Dit artikel legt uit hoe u ICMP-filtering op de 300 Series Managed-switches kunt configureren.

Toepasselijke apparaten

- SF/SG 300 Series Managed-switches

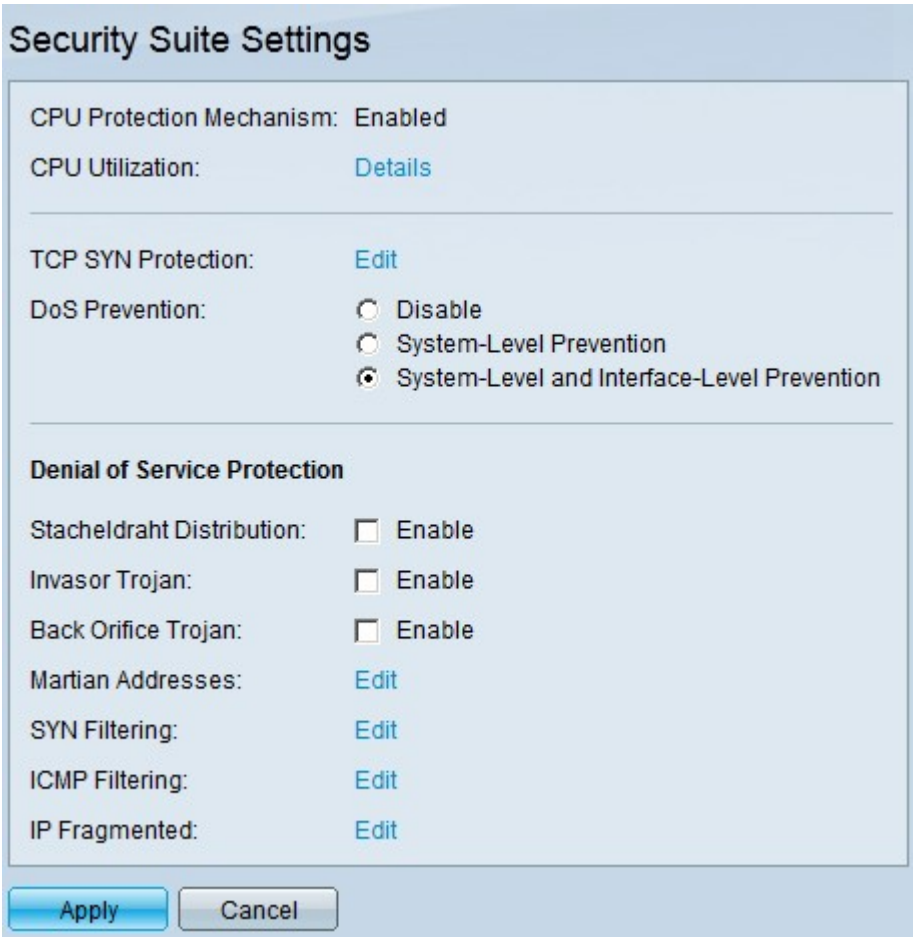
Softwareversie

•1.3.0.62

voorkoming van serviceniveau inschakelen

Om ICMP-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:



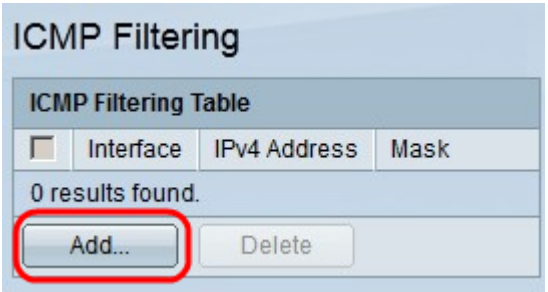
Stap 2. In het veld *DoS Prevention* zijn er drie niveaus van preventie. Klik op de radioknop **Systeem-Level en Interface-Level Prevention**. Op dit niveau kunt u ICMP-filtering configureren.

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

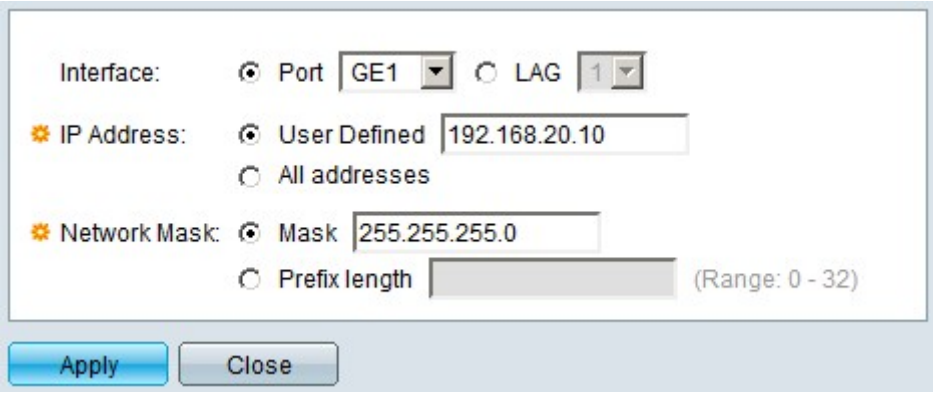
ICMP-filtering

Deze sectie legt uit hoe u ICMP-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 > ICMP Filtering**. De pagina *ICMP-filtering* wordt geopend:



Stap 2. Klik op **Add**. Het venster *ICMP-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 kiezen waarvan u ICMP-pakketten wilt filteren.
- LAG — Hiermee kunt u de LAG kiezen waarvan u ICMP-pakketten wilt filteren. LAG groepeert meerdere poorten in één logische poort.

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

- Gebruiker gedefinieerd - door gebruiker gedefinieerde ICMP-pakketbronnen.
- Alle adressen — Alle bereik van IP-adresbronnen in ICMP.

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 - Subnet masker in dot formaat, bijvoorbeeld 255.255.255.0.
- Lengte voorvoegsel — Subnetmasker in slaat formaat, bijvoorbeeld \24.

Stap 6. Klik op **Toepassen** om de configuratie op te slaan.

In het onderstaande beeld worden de wijzigingen na de configuratie weergegeven:

Stap 7. (Optioneel) Controleer om een ICMP-filter te verwijderen het aanvinkvakje van het ICMP-filter dat u wilt verwijderen in de tabel met ICMP-filtering en klik vervolgens op **Verwijderen**.