

IP Source Guard Configuration op SX500 Series Stackable-switches

Doel

IP Source Guard is een veiligheidsfunctie die kan worden gebruikt om verkeersaanvallen te voorkomen die worden veroorzaakt wanneer een host het IP-adres van een aangrenzende host probeert te gebruiken. Wanneer IP Source Guard is ingeschakeld, geeft de switch alleen het client-IP-verkeer naar IP-adressen door in de DHCP Snooping Binding-database. Als het pakket dat een host ontvangt, overeenkomt met een ingang in de database, geeft de switch het pakket door. Als het pakje niet overeenkomt met een ingang in de database, komt deze te vervallen.

In een real-time scenario, is één manier waarin IP Bron Guard wordt gebruikt om te helpen om man-in-het-midden aanvallen te voorkomen waar een onvertrouwde derde probeert om als echte gebruiker te maskeren. Gebaseerd op de adressen die in de IP bron Guard bindende databank worden gevormd, is alleen het verkeer van de cliënt met dat IP adres toegestaan en de rest van de pakketten worden ingetrokken.

Opmerking: DHCP-decodering dient ingeschakeld te worden zodat IP-bronbewaking kan functioneren. Raadpleeg het artikel *DHCP-configuratie van SX500 Series Stackable Switches* voor meer informatie over het inschakelen van DHCP-signalering. Het is ook nodig om de bindende databank aan te passen om aan te geven welke IP-adressen zijn toegestaan. Meer informatie hierover is te vinden in het artikel *Configuration of DHCP Snooping Binding Database op SX500 Series Stackable Switches*.

Dit artikel legt uit hoe u IP Source Guard op de SX500 Series Stackable Switches kunt configureren.

Toepasselijke apparaten

- SX500 Series Stackable-switches

Softwareversie

- v1.2.7.76

Instellingen IP-bronbewaking instellen

Instellingen IP-bronbewaking mondiaal inschakelen

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > IP Source Guard > Properties**. De pagina *Eigenschappen IP Source Guard* wordt geopend:

Properties

DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently enabled.

IP Source Guard Status: Enable

Apply Cancel

Stap 2. Controleer het aanvinkvakje **Enable** om IP-bronbewaking mondiaal in te schakelen.

Properties

DHCP Snooping must be enabled for IP Source Guard to operate. DHCP Snooping is currently enabled.

IP Source Guard Status: Enable

Apply Cancel

Stap 3. Klik op **Toepassen** om de instellingen toe te passen.

Interface-instellingen bewerken voor IP-bronbewaking

Als de IP Source Guard op een onvertrouwde poort of LAG is ingeschakeld, worden de DHCP-pakketten die worden verzonden toegestaan door de DHCP-oplossingsdatabase. Als het IP-adres met een filter is ingeschakeld, is pakkettransport als volgt toegestaan:

- IPv4-verkeer — Het IPv4-verkeer dat gekoppeld is aan het IP-bronadres van de poort is toegestaan.
- Niet IPv4-verkeer — al het niet-IPv4-verkeer is toegestaan.

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > IP Source Guard > Interface Settings**. De pagina *Interface-instellingen* wordt geopend:

Interface Settings

DHCP Snooping must be enabled for IP Source Guard to operate. IP

Interface Settings Table

Filter: *Interface Type* equals to

	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1	FE1	No	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Stap 2. Kies een interfacetype in de vervolgkeuzelijst Interfacetype en klik op **Go** in het veld Filter.

De tabel met interface-instellingen bestaat uit de volgende parameters.

- Interface — Toont de interface waarop de IP-bronbewaking wordt toegepast.
- IP Source Guard — laat zien of IP Source Guard is ingeschakeld of niet.
- DHCP Snooping Trusted Interface - toont of het een DHCP-vertrouwde interface is. Trusted interfaces kunnen alleen verkeer binnen het netwerk ontvangen. IP Source Guard wordt gewoonlijk op DHCP-interfaces geconfigureerd die niet worden vertrouwd. Een onvertrouwde interface is een interface die zodanig is geconfigureerd dat hij berichten van buiten het netwerk kan ontvangen.

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input checked="" type="radio"/>	1	FE1	No	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Stap 3. Klik op de radioknop die overeenkomt met de te bewerken interface en klik op **Bewerken** onder in de pagina. Het venster *Interface-instellingen bewerken* verschijnt.

Interface: Unit/Slot Port LAG

IP Source Guard: Enabled

Stap 4. Controleer het veld IP-bronbewaking in om IP-bronbewaking op de huidige interface in te schakelen.

Interface: Unit/Slot Port LAG

IP Source Guard: Enabled

Stap 5. Klik op **Toepassen**. De wijzigingen worden weergegeven.

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input checked="" type="radio"/>	1	FE1	Yes	No
<input type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Interface-instellingen voor IP-bronbewaking kopiëren

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > IP Source Guard > Interface Settings**. De pagina *Interface-instellingen* wordt geopend:

Interface Settings Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1/2"/> <input type="button" value="Go"/>				
	Entry No.	Interface	IP Source Guard	DHCP Snooping Trusted Interface
<input type="radio"/>	1	FE1	Yes	No
<input checked="" type="radio"/>	2	FE2	No	No
<input type="radio"/>	3	FE3	No	No
<input type="radio"/>	4	FE4	No	No
<input type="radio"/>	5	FE5	No	No
<input type="radio"/>	6	FE6	No	No
<input type="radio"/>	7	FE7	No	No
<input type="radio"/>	8	FE8	No	No
<input type="radio"/>	9	FE9	No	No
<input type="radio"/>	10	FE10	No	No

Stap 2. Klik op de radioknop voor de gewenste interface en klik op **Instellingen kopiëren**. Het venster *Instellingen kopiëren* verschijnt.

Copy configuration from entry 2 (FE2)

to: (Example: 1,3,5-10 or: FE1,FE3-FE5)

Stap 3. Voer de interface(s) of bereik(en) van interfaces in waarop de gekozen ingang moet

worden gekopieerd en klik op **Toepassen**. De instellingen worden toegepast.