IP Source Guard-Konfiguration auf Stackable Switches der Serie Sx500

Ziel

IP Source Guard ist eine Sicherheitsfunktion, mit der Datenverkehrsangriffe verhindert werden können, die entstehen, wenn ein Host versucht, die IP-Adresse eines benachbarten Hosts zu verwenden. Wenn IP Source Guard aktiviert ist, überträgt der Switch nur den Client-IP-Datenverkehr an IP-Adressen, die in der DHCP Snooping Binding-Datenbank enthalten sind. Wenn das Paket, das ein Host sendet, mit einem Eintrag in der Datenbank übereinstimmt, leitet der Switch das Paket weiter. Wenn das Paket nicht mit einem Eintrag in der Datenbank übereinstimmt, wird es verworfen.

In einem Echtzeit-Szenario kann IP Source Guard beispielsweise eingesetzt werden, um Man-in-the-Middle-Angriffe zu verhindern, bei denen ein nicht vertrauenswürdiger Dritter versucht, sich als legitimer Benutzer zu tarnen. Basierend auf den in der IP Source Guard-Bindungsdatenbank konfigurierten Adressen ist nur der Datenverkehr vom Client mit dieser IP-Adresse zulässig, und die restlichen Pakete werden verworfen.

Hinweis: DHCP-Snooping sollte aktiviert sein, damit IP Source Guard funktioniert. Weitere Informationen zur Aktivierung von DHCP Snooping finden Sie im Artikel *DHCP Snooping Configuration on SX500 Series Stackable Switches*. Außerdem muss die Bindungsdatenbank so konfiguriert werden, dass angegeben wird, welche IP-Adressen zulässig sind. Weitere Einzelheiten hierzu finden Sie im Artikel *Konfiguration der DHCP Snooping Binding Database auf Stackable Switches der Serie SX500.*

In diesem Artikel wird erläutert, wie IP Source Guard auf den Stackable Switches der Serie Sx500 konfiguriert wird.

Anwendbare Geräte

·Stackable Switches der Serie Sx500

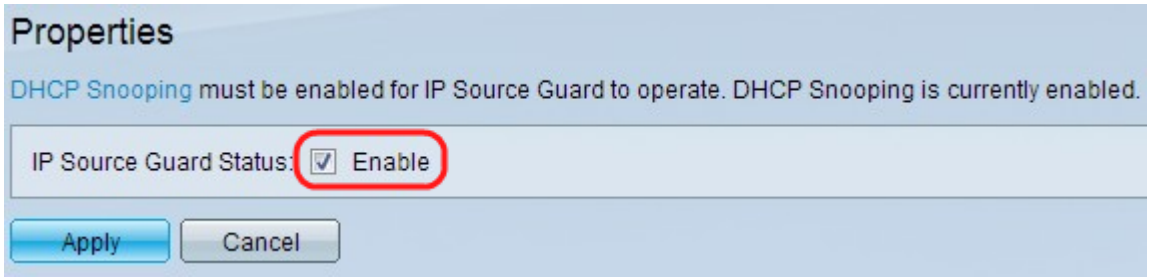
Softwareversion

·v1.2.7.76

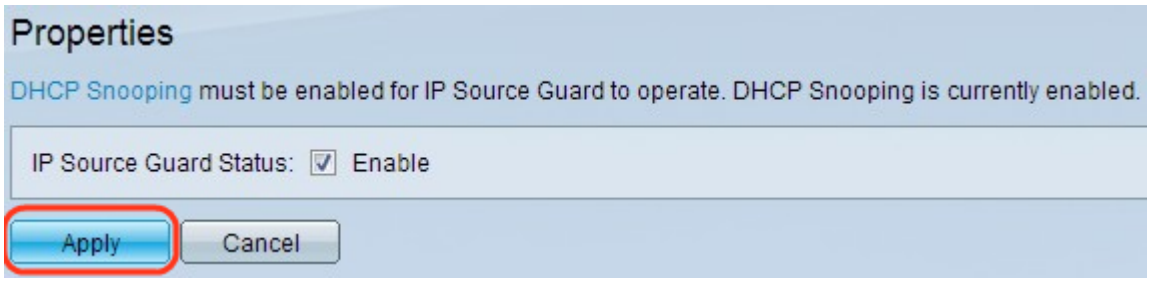
Konfigurieren der IP Source Guard-Einstellungen

IP Source Guard-Einstellungen global aktivieren

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > IP Source Guard > Properties aus**. Die Seite *Eigenschaften von IP Source Guard* wird geöffnet:



Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um IP Source Guard global zu aktivieren.



Schritt 3: Klicken Sie auf **Übernehmen**, um die Einstellungen zu übernehmen.

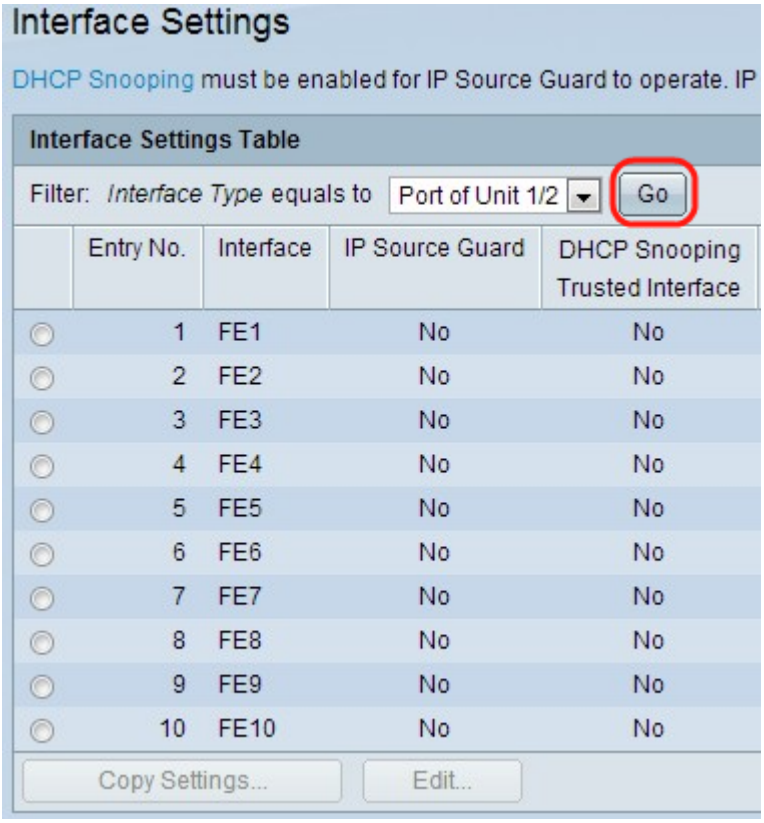
Schnittstelleneinstellungen für IP Source Guard bearbeiten

Wenn der IP Source Guard auf einem nicht vertrauenswürdigen Port oder einer LAG aktiviert ist, sind die übertragenen DHCP-Pakete von der DHCP Snooping-Datenbank zugelassen. Wenn die IP-Adresse mit einem Filter aktiviert ist, ist die Paketübertragung wie folgt zulässig:

·IPv4-Datenverkehr - Der IPv4-Datenverkehr, der der Quell-IP-Adresse des jeweiligen Ports zugeordnet ist, ist zulässig.

·Nicht-IPv4-Datenverkehr - Der gesamte Nicht-IPv4-Datenverkehr ist zulässig.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > IP Source Guard > Interface Settings (Sicherheit > IP-Quellschutz > Schnittstelleneinstellungen)**. Die Seite *Schnittstelleneinstellungen* wird geöffnet:



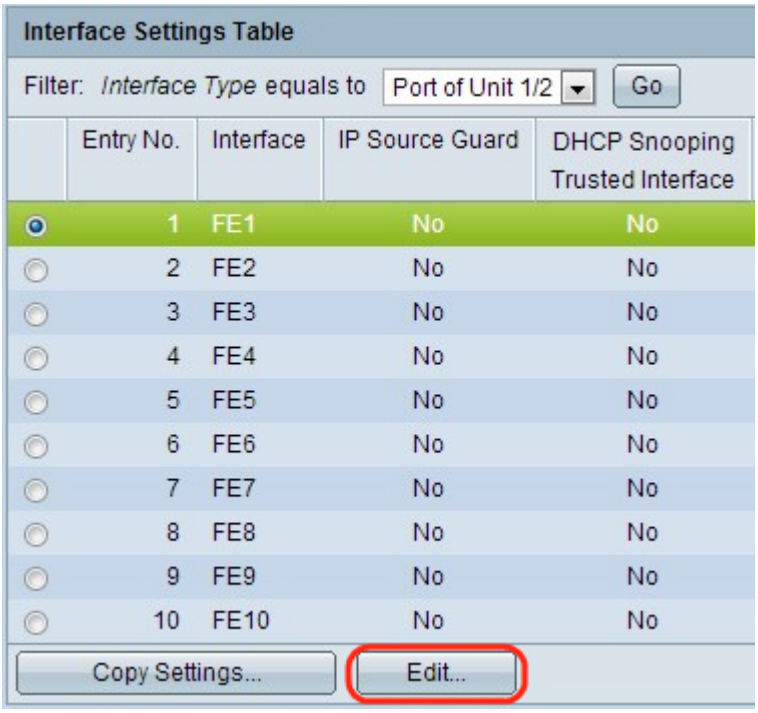
Schritt 2: Wählen Sie in der Dropdown-Liste Schnittstellentyp einen Schnittstellentyp aus, und klicken Sie im Feld Filter auf **Los**.

Die Tabelle für Schnittstelleneinstellungen besteht aus den folgenden Parametern.

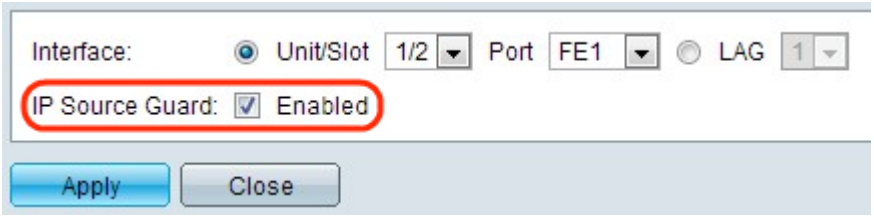
·Schnittstelle - Zeigt die Schnittstelle an, auf die der IP Source Guard angewendet wird.

·IP Source Guard - Zeigt an, ob IP Source Guard aktiviert ist.

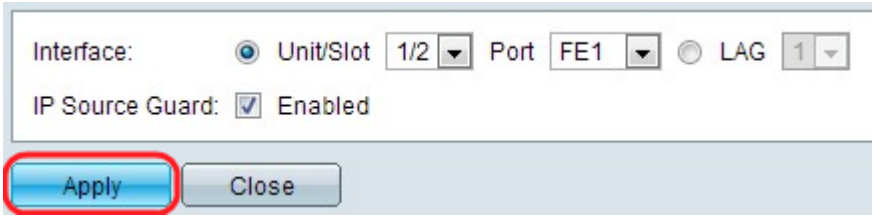
·Vertrauenswürdige DHCP Snooping-Schnittstelle - Zeigt an, ob es sich um eine DHCP-vertrauenswürdige Schnittstelle handelt. Vertrauenswürdige Schnittstellen können Datenverkehr nur von innerhalb des Netzwerks empfangen. IP Source Guard wird normalerweise auf DHCP-Schnittstellen konfiguriert, die nicht vertrauenswürdig sind. Eine nicht vertrauenswürdige Schnittstelle ist eine Schnittstelle, die so konfiguriert ist, dass sie Nachrichten von außerhalb des Netzwerks empfangen kann.



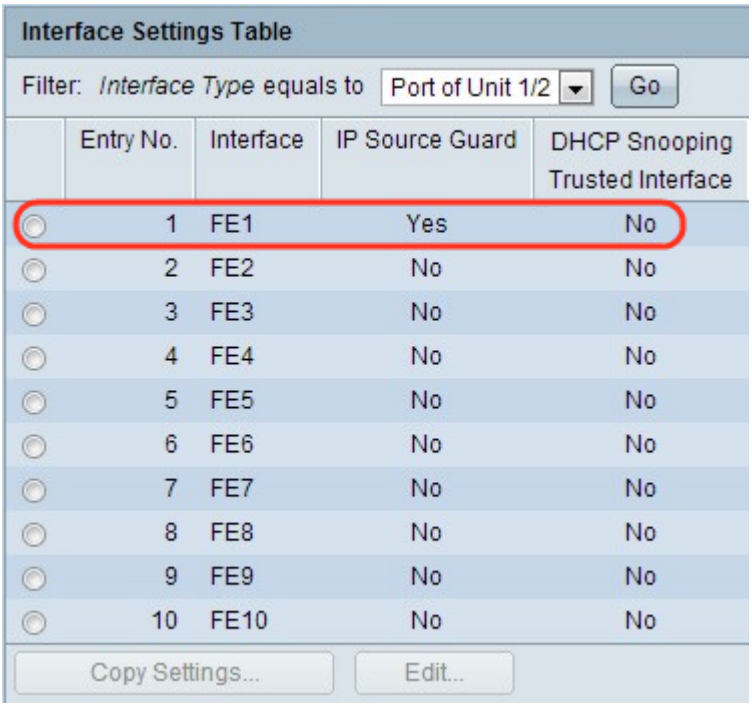
Schritt 3: Klicken Sie auf das Optionsfeld für die zu bearbeitende Schnittstelle, und klicken Sie unten auf der Seite auf **Bearbeiten**. Das Fenster *Schnittstelleneinstellungen bearbeiten* wird angezeigt.



Schritt 4: Aktivieren Sie im Feld IP Source Guard die Option Enable (Aktivieren), um IP Source Guard auf der aktuellen Schnittstelle zu aktivieren.

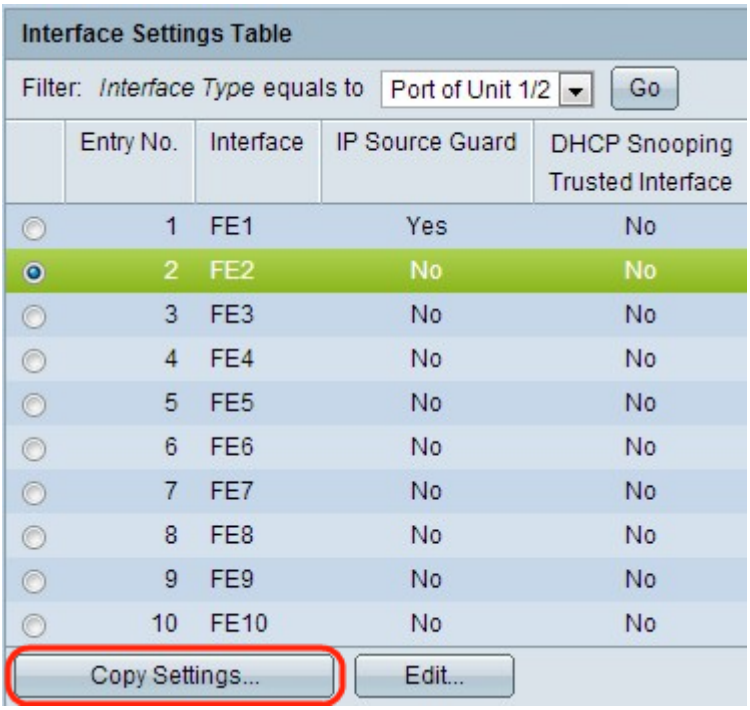


Schritt 5: Klicken Sie auf **Übernehmen**. Die Änderungen werden angezeigt.

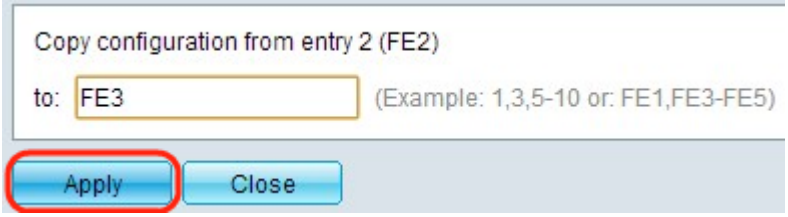


Schnittstelleneinstellungen für IP Source Guard kopieren

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > IP Source Guard > Interface Settings (Sicherheit > IP-Quellschutz > Schnittstelleneinstellungen)**. Die Seite *Schnittstelleneinstellungen* wird geöffnet:



Schritt 2: Klicken Sie auf das Optionsfeld für die gewünschte Schnittstelle, und klicken Sie auf **Copy Settings**. Das Fenster *Kopiereinstellungen* wird angezeigt.



Schritt 3: Geben Sie die Schnittstelle bzw. die Schnittstellen ein, auf die der ausgewählte Eintrag kopiert werden soll, und klicken Sie auf Apply. Die Einstellungen werden angewendet.