Konfiguration der Denial of Service (DoS) IP Fragments Filtering auf stapelbaren Switches der Serie Sx500

Ziel

Denial of Service (DoS) Prevention erhöht die Netzwerksicherheit und filtert Pakete mit bestimmten IP-Adressparametern, sodass sie nicht in das Netzwerk gelangen. Die maximale Größe des IP-Pakets beträgt standardmäßig 1.500 Byte, doch wenn das Paket diese Größe überschreitet, muss das Paket fragmentiert werden. Diese Pakete müssen gelegentlich blockiert werden, da sie Sicherheitsschwachstellen darstellen können, wie zum Beispiel zu viele unvollständige Datagramme, um eine Diensteverweigerung zu verursachen und Sicherheitsmaßnahmen zu umgehen.

Die DoS-IP-Fragmentfilterung wird verwendet, um die fragmentierten IP-Pakete zu blockieren. In diesem Dokument wird erläutert, wie Sie die Filtereinstellungen für DoS-IP-Fragmente auf den stapelbaren Switches der Serie Sx500 konfigurieren.

Anwendbare Geräte

·Stackable Switches der Serie Sx500

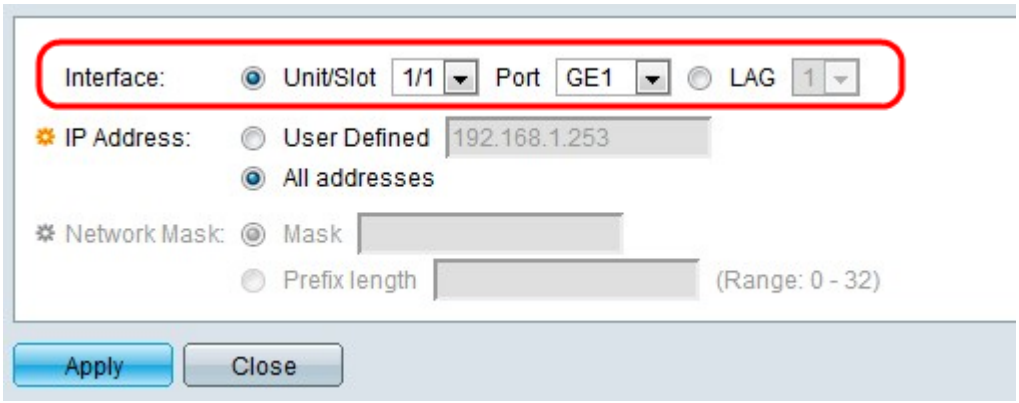
Softwareversion

·v1.2.7.76

IP-Fragmentfilter hinzufügen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Sicherheit > Denial of Service Prevention > IP Fragments Filtering (IP-Fragmentfilterung) aus.** Die Seite *IP Fragments Filtering* (IP-Fragmentfilterung) wird geöffnet:

Schritt 2: Klicken Sie in der Tabelle für die IP-Fragmentfilterung auf **Hinzufügen**. Das Fenster *IP-Fragmentfilterung hinzufügen* wird angezeigt.

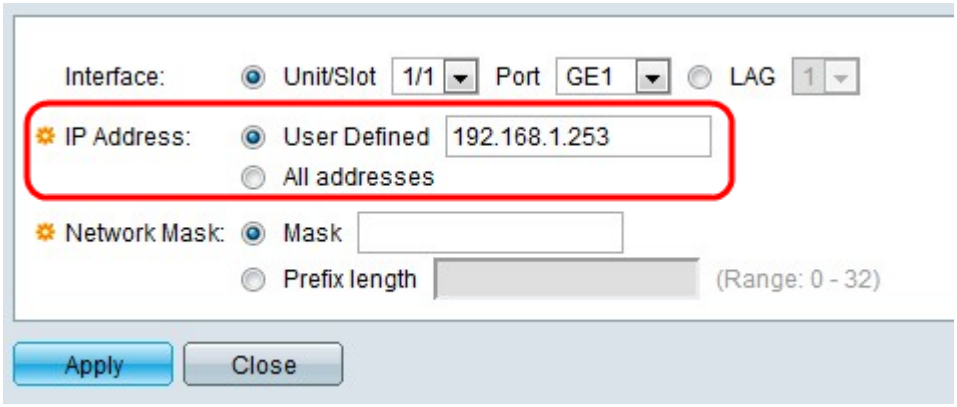


Schritt 3: Klicken Sie im Feld Schnittstelle auf das Optionsfeld für den gewünschten Schnittstellentyp.

·Einheit/Steckplatz - Wählen Sie aus den Dropdown-Listen Einheit/Steckplatz die entsprechende Einheit/Steckplatz aus. Die Einheit identifiziert, ob der Switch aktiv ist oder ein Stack-Element vorhanden ist. Der Steckplatz identifiziert, welcher Switch an welchen Steckplatz angeschlossen ist (Steckplatz 1 ist SF500 und Steckplatz 2 ist SG500). Wenn Sie mit den verwendeten Begriffen nicht vertraut sind, lesen Sie Cisco Business: Glossar neuer Begriffe.

- Port (Port) - Wählen Sie aus der Dropdown-Liste "Port" den gewünschten Port aus, den Sie konfigurieren möchten.

·LAG: Wählen Sie die gewünschte LAG aus der LAG-Dropdown-Liste aus. Eine Link Aggregate Group (LAG) dient zum Verbinden mehrerer Ports. LAGs vervielfachen die Bandbreite, erhöhen die Portflexibilität und bieten Verbindungsredundanz zwischen zwei Geräten, um die Port-Nutzung zu optimieren.

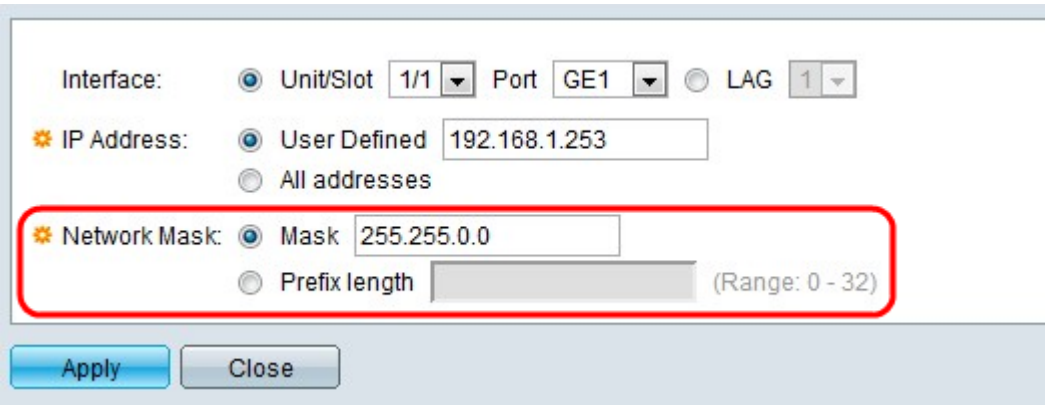


Schritt 4: Klicken Sie auf das Optionsfeld, das der IP-Adresse entspricht, aus der Pakete im Feld IP Address (IP-Adresse) gefiltert werden sollen.

·Benutzerdefiniert - Geben Sie eine IP-Adresse ein, von der die fragmentierten IP-Pakete gefiltert werden.

·Alle Adressen - Blockiert fragmentierte IP-Pakete von allen Adressen.

Hinweis: Wenn Sie in Schritt 4 die Option Alle Adressen ausgewählt haben, fahren Sie mit Schritt 6 fort.



Schritt 5: Klicken Sie auf das Optionsfeld für die gewünschte Netzwerkmaske im Feld Netzwerkmaske.

·Maske - Geben Sie die Netzwerkmaske im IP-Adressformat ein. Damit wird die Subnetzmaske für die IP-Adresse definiert.

·Präfixlänge - Geben Sie die Präfixlänge ein (ganze Zahl im Bereich von 0 bis 32). Damit wird die Subnetzmaske nach Präfixlänge für die IP-Adresse definiert.

Schritt 6: Klicken Sie auf **Übernehmen**.