

# Konfiguration der DoS-IP-Fragmentierungsfilterung für Managed Switches der Serie 300

## Ziel

Netzwerkverkehr wird über mehrere Pakete gesendet, die Datagramme genannt werden. Jede Transportmethode (Ethernet, Tokenring usw.) hat eine maximale Größe an Datagrammen, die sie verarbeiten kann. Wenn das Datagramm zu groß für die Übertragungsmethode ist, wird es in kleinere Fragmente aufgeteilt. Dieser Prozess wird als IP-Fragmentierung bezeichnet. Der Großteil des Netzwerkverkehrs muss nicht fragmentiert werden. Der fragmentierte Datenverkehr kann als Denial of Service (DoS)-Angriff verwendet werden. Ein DoS-Angriff überflutet ein Netzwerk mit falschem Datenverkehr und verlangsamt oder stoppt das Netzwerk. Managed Switches der Serie 300 können IP-Fragmente blockieren, wodurch die Netzwerkanfälligkeit für einen DoS-Angriff verringert wird. In diesem Artikel wird erläutert, wie Sie die Einstellungen für die *IP-Fragmentfilterung* auf Managed Switches der Serie 300 konfigurieren.

**Hinweis:** IP-Fragmentfilter können nur verwendet werden, wenn DoS Prevention aktiviert ist. Hilfe finden Sie im Artikel *Security Suite Settings on 300 Series Managed Switches*.

## Anwendbare Geräte

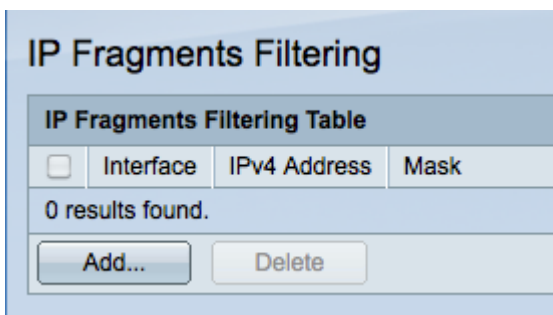
·Managed Switches der Serie SF/SG 300

## Softwareversion

·1.3.0.62

## 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:



IP Fragments Filtering Table			
<input type="checkbox"/>	Interface	IPv4 Address	Mask
0 results found.			
<input type="button" value="Add..."/>		<input type="button" value="Delete"/>	

Schritt 2: Klicken Sie auf **Hinzufügen**, um einen neuen IP-Fragmentfilter hinzuzufügen. Das Fenster *IP-Fragmentfilterung hinzufügen* wird angezeigt.

Interface:  Port  LAG

IP Address:  User Defined  All addresses

Network Mask:  Mask  Prefix length (Range: 0 - 32)

Apply Close

Schritt 3: Klicken Sie im Feld Schnittstelle auf das Optionsfeld für die gewünschte Schnittstelle. Dies ist der physische Speicherort, dem der Filter zugewiesen wird.

·Port - Der physische Port am Switch. Wählen Sie einen bestimmten Port aus der Dropdown-Liste Port aus.

·LAG - Eine Gruppe von Ports, die als ein Port fungieren. Wählen Sie aus der LAG-Dropdown-Liste eine bestimmte LAG aus.

Schritt 4: Klicken Sie auf das Optionsfeld für die gewünschte IPv4-Adresse, die im Feld IP Address (IP-Adresse) gefiltert werden soll.

·Benutzerdefiniert - Geben Sie eine IP-Adresse ein, die gefiltert werden soll.

·Alle Adressen - Alle IPv4-Adressen werden gefiltert.

**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, das der Methode entspricht, mit der die Subnetzmaske der IP-Adresse im Feld Netzwerkmaske definiert wird.

·Maske - Geben Sie die Netzwerkmaske in das Feld für die Netzwerkmaske ein.

·Präfixlänge - Geben Sie die Präfixlänge (ganze Zahl im Bereich von 0 bis 32) im Feld Präfixlänge ein.

Schritt 6: Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, und klicken Sie dann auf **Schließen**, um das Fenster *IP-Fragmentfilterung hinzufügen zu schließen*.