

Konfiguration der DoS-SYN-Filterung (Denial of Service) für Managed Switches der Serie 300

Ziel

Ein DoS-Angriff (Denial of Service) überflutet ein Netzwerk mit falschem Datenverkehr. Dadurch werden Netzwerkeserverressourcen von legitimen Benutzern abgezogen. Eine SYN-Flood zielt insbesondere auf das TCP-Protokoll ab. Für die Funktion des TCP-Protokolls sind drei Schritte erforderlich. Zunächst sendet ein Benutzer seine IP-Adresse an den Server und fordert eine Verbindung an. Anschließend antwortet der Server auf die Anfrage und wartet auf eine Bestätigung. Schließlich erkennt der Benutzer an, dass der Server eine Verbindung geöffnet hat. Bei einem TCP-SYN-Angriff werden mehrere IP-Adressen verwendet, um eine Verbindung anzufordern, jedoch niemals eine Bestätigung an den Server zurückgesendet, sobald eine Verbindung geöffnet ist. Ein Server kann nur eine begrenzte Anzahl von Verbindungen öffnen, bevor er beginnt, TCP-Anfragen selbst von legitimen Benutzern zu verwerfen.

TCP-Datenverkehr wird über mehrere virtuelle Ports gesendet. Über diese Ports kann der Netzwerkverkehr in gemeinsame Gruppen aufgeteilt werden. Der SYN-Filter kann so konfiguriert werden, dass Datenverkehr von einem bestimmten virtuellen Port blockiert wird. Darüber hinaus wird die SYN-Filterung auf einem physischen Port oder einer LAG am Switch konfiguriert. In diesem Artikel wird erläutert, wie Sie die SYN-Filterung für die Managed Switches der Serie 300 konfigurieren.

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

Anwendbare Geräte

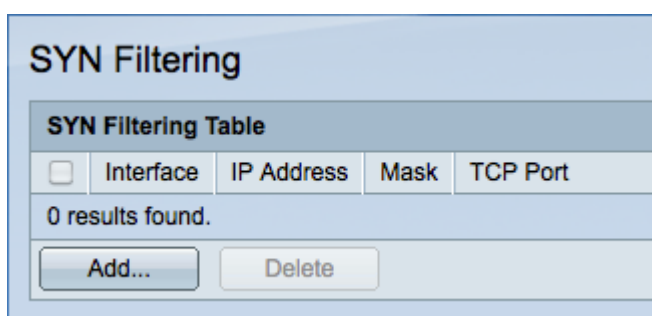
·Managed Switches der Serie SF/SG 300

Softwareversion

·v1.2.7.76

Konfiguration der SYN-Filterung

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Sicherheit** > **Denial of Service Prevention** > **SYN Filtering** aus. Die Seite *SYN-Filterung* wird geöffnet:



The screenshot shows the 'SYN Filtering' configuration page. At the top, there is a section titled 'SYN Filtering Table' with a table header containing columns for 'Interface', 'IP Address', 'Mask', and 'TCP Port'. Below the header, it states '0 results found.' At the bottom of the table area, there are two buttons: 'Add...' and 'Delete'.

Schritt 2: Klicken Sie auf **Hinzufügen**, um einen neuen SYN-Filter hinzuzufügen. Das Fenster *Syn-Filterung hinzufügen* wird angezeigt.

Interface: Port GE1 LAG 1

IPv4 Address: User Defined 192.0.2.10
 All addresses

Network Mask: Mask 255.255.255.0
 Prefix length (Range: 0 - 32)

TCP Port: Known ports HTTP
 User Defined 8080 (Range: 1 - 65535)
 All ports

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, das der gewünschten IPv4-Adresse im Feld IPv4-Adresse entspricht.

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

·Alle Adressen - Alle IPv4-Adressen werden für TCP-Datenverkehr gefiltert. Fahren Sie mit Schritt 6 fort, wenn Sie Alle Adressen ausgewählt haben.

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 das Optionsfeld für den gewünschten TCP-Port, der im Feld TCP-Port gefiltert werden soll. Dies sind die virtuellen Ports, in die der Netzwerkverkehr unterteilt ist.

·Bekannt Ports - Wählen Sie einen TCP-Port aus, der aus der Dropdown-Liste "Bekannt Ports" gefiltert werden soll.

·Benutzerdefiniert - Geben Sie einen TCP-Port ein, der gefiltert werden soll.

·Alle Ports - Alle TCP-Ports werden gefiltert.

Schritt 7: Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, und klicken Sie

dann auf **Schließen**, um das Fenster *Syn-Filterung hinzufügen* zu schließen.