Denial of Service (DoS) SYN Filtering Configuration on 300 Series Managed Switches

Objective

A Denial of Service (DoS) attack floods a network with false traffic. This draws network server resources away from legitimate users. A SYN flood targets TCP protocol in particular. TCP protocol requires three steps to function. First, a user sends their IP address to the server and requests a connection. Next, the server responds to the request and waits for a confirmation. Finally, the user acknowledges that the server has opened a connection. A TCP SYN attack uses multiple IP addresses to request a connection, but never send an acknowledgment back to the server once a connection is open. A server can only open a limited amount of connections before it starts to drop TCP requests, even from legitimate users.

TCP traffic is sent on several virtual ports. These ports are a way for network traffic to be split into common groups. The SYN filter can be configured to block traffic from a specific virtual port. In addition, SYN filtering is configured on an actual, physical port or LAG on the switch. This article explains how to configure SYN filtering on the 300 Series Managed Switches.

Note: Syn filters can only be used if DoS Prevention is enabled. Refer to the article *Security Suite Settings on 300 Series Managed Switches* for help.

Applicable Devices

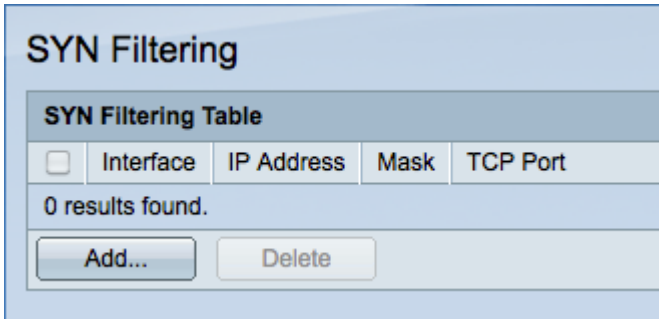
- SF/SG 300 Series Managed Switches

Software Version

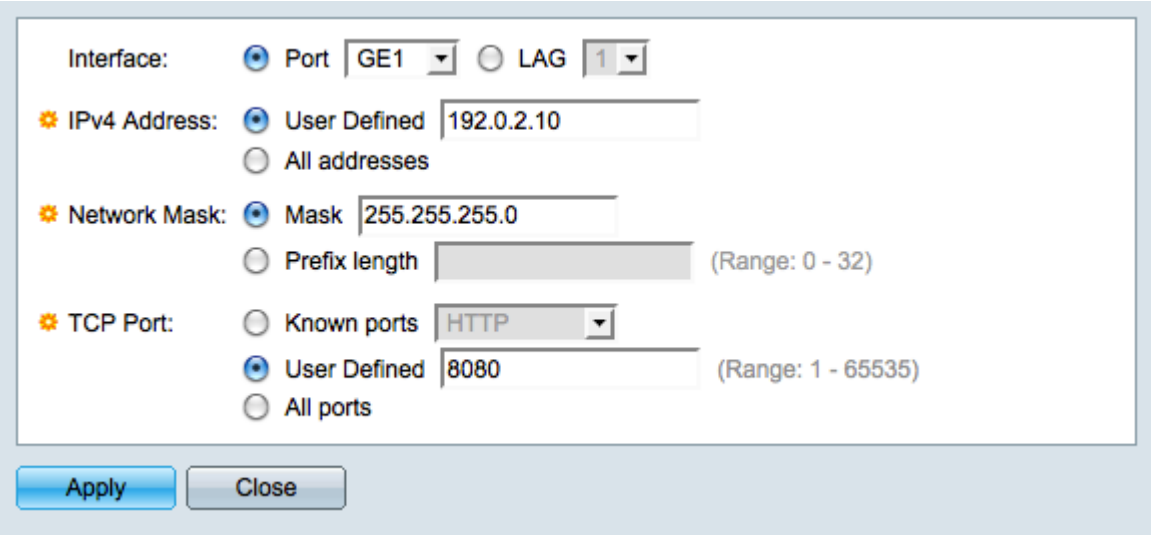
- v1.2.7.76

SYN Filtering Configuration

Step 1. Log in to the web configuration utility and choose **Security > Denial of Service Prevention > SYN Filtering**. The *SYN Filtering* page opens:



Step 2. Click **Add** to add a new SYN filter. The *Add Syn Filtering* window appears.



Step 3. Click the radio button that corresponds with the desired interface in the Interface field. This is the physical location that the filter will be assigned to.

- Port — The physical port on the switch. Choose a specific port from the Port drop-down list.
- LAG — A group of ports that act as a single port. Choose a specific LAG from the LAG drop-down list.

Step 4. Click the radio button that corresponds with the desired IPv4 address in the IPv4 Address field.

- User Defined — Enter an IP address to be filtered for TCP traffic.
- All addresses — All IPv4 addresses are filtered for TCP traffic. Skip to Step 6 if All addresses is chosen.

Step 5. Click the radio button that corresponds with the method used to define the subnet mask of the IP address in the Network Mask field.

- Mask — Enter the network mask in the Network mask field.
- Prefix Length — Enter the prefix length (integer in the range of 0 to 32) in the Prefix length field.

Step 6. Click the radio button that corresponds with the desired TCP port to be filtered in the TCP Port field. These are the virtual ports that network traffic is divided into.

- Known Ports — Choose a TCP port to be filtered from the Known ports drop-down list.
- User Defined — Enter a TCP port to be filtered.
- All Ports — All TCP ports are filtered.

Step 7. Click **Apply** to save your changes and then click **Close** to exit the *Add Syn Filtering* window.