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

Objective

Network traffic is sent by use of multiple packets called datagrams. Each transport method (ethernet, token ring, etc.) has a maximum size of datagram that it can handle. If the datagram is too large for the transmission method, it is split into smaller fragments. This process is known as IP fragmentation. Most network traffic does not have to be fragmented. In fact, traffic that has been fragmented can be used as in a Denial of Service (DoS) attack. A DoS attack floods a network with false traffic and slows or stops the network. 300 Series Managed switches can block IP fragments, which decreases the networks vulnerability to a DoS attack. This article explains how to configure the *IP Fragments Filtering* settings on 300 Series Managed Switches.

Note: IP fragment 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

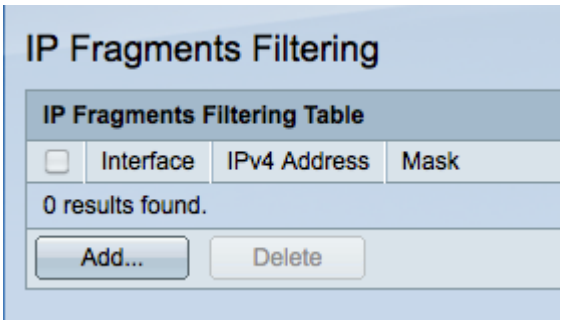
- SF/SG 300 Series Managed Switches

Software Version

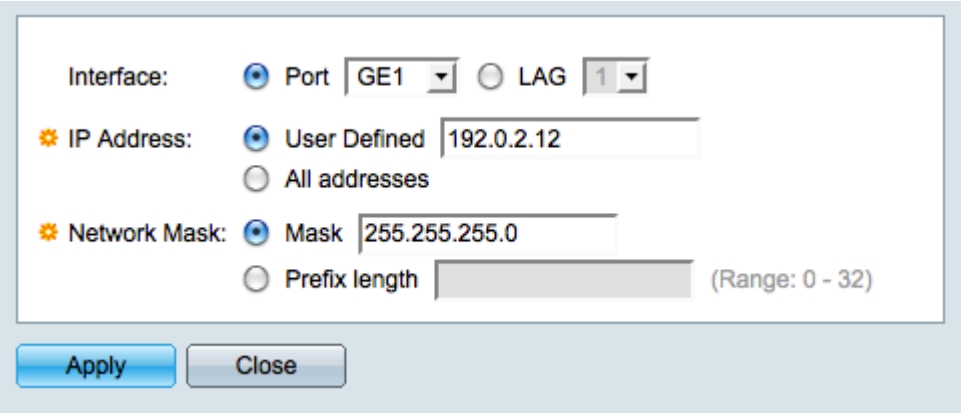
- 1.3.0.62

Add IP Fragments Filter

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



Step 2. Click **Add** to add a new IP fragments filter. The *Add IP Fragments 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 to be filtered in the IP Address field.

- User Defined — Enter an IP address to be filtered.
- All addresses — All IPv4 addresses are filtered.

Note: If you chose All addresses in Step 4, skip to Step 6.

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 **Apply** to save you changes and then click **Close** to close the *Add IP Fragments Filtering* window.