Denial of Service (DOS) SYN Filtering Configuration on Sx500 Series Stackable Switches

Objective

SYN filtering is one of the DOS prevention features. It is used to prevent TCP connections from a specific port or a LAG. This allows the switch administrator to block unwanted TCP ports. Packets that are destined for these blocked TCP ports will be filtered out of the system. This is mainly used to filter TCP packets that contain the SYN flag.

This article explains how to configure SYN filtering on the Sx500 Series Stackable Switches.

Applicable Devices

- Sx500 Series Stackable Switches

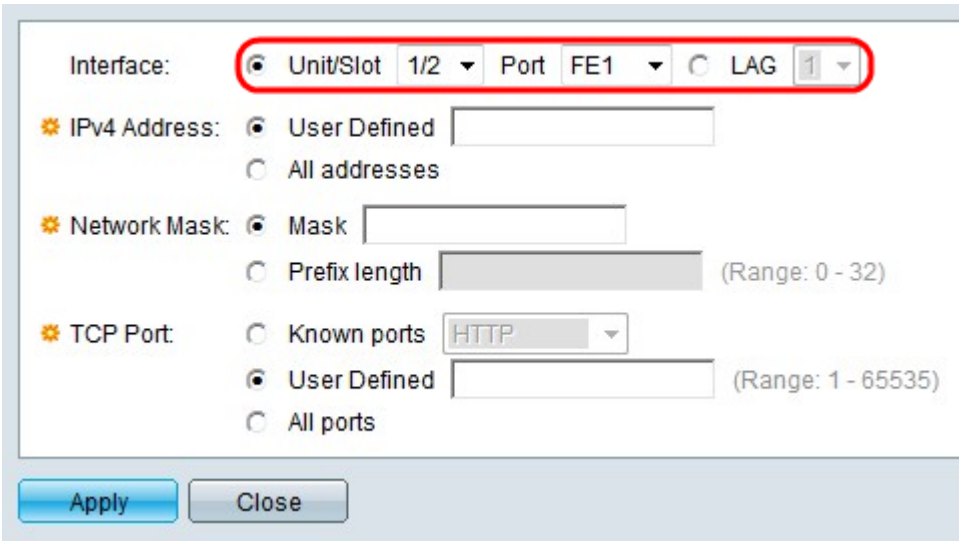
Software Version

- v1.2.7.76

SYN Filtering

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.

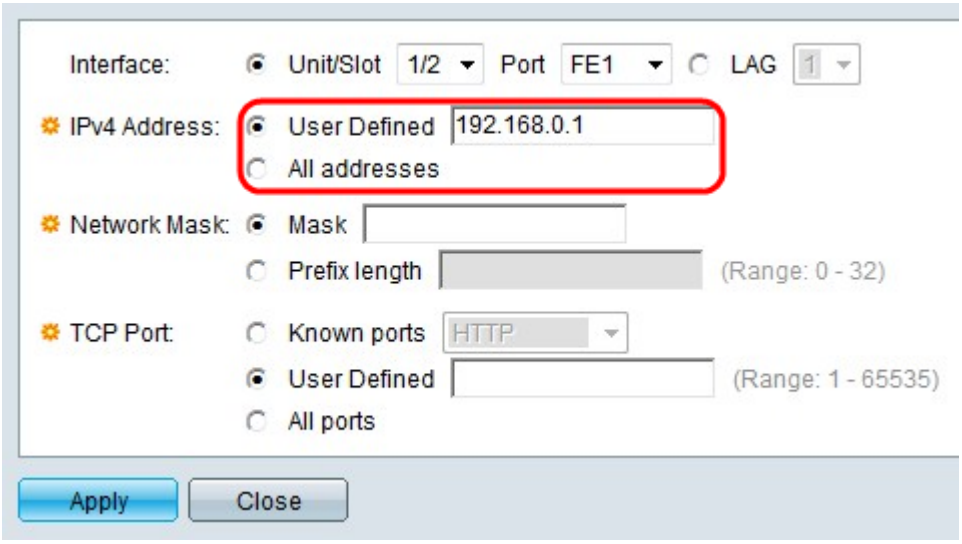


Step 3. Click the radio button that corresponds to the desired interface type in the Interface field.

- Unit/Slot — From the Unit/Slot drop-down lists choose the appropriate Unit/Slot. The unit identifies whether the switch is active or a member in the stack. The slot identifies which switch is connected to which slot (slot 1 is SF500 and slot 2 is SG500). If you are unfamiliar with the terms used, check out Cisco Business: Glossary of New Terms.

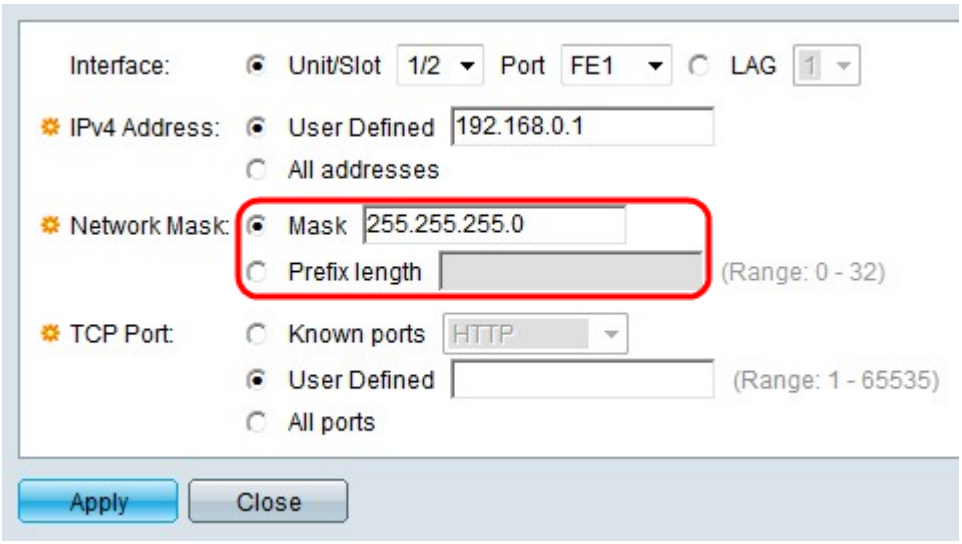
  – Port — From the Port drop-down list, choose the appropriate port to configure.

- LAG — Choose on which LAG the STP is advertised from the LAG drop-down list. A Link Aggregate Group (LAG) is used to link multiple ports together. LAGs multiply bandwidth, increase port flexibility, and provide link redundancy between two devices to optimize port usage.



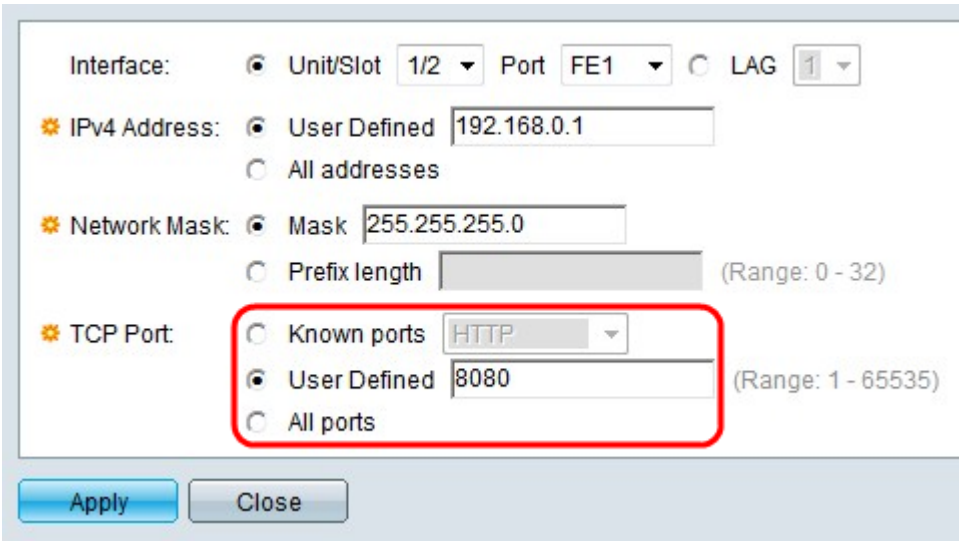
Step 4. Click the radio button that corresponds with the desired IPv4 address in the IPv4 Address field.

- User Defined — Filter is defined to the user defined IP address.
- All addresses — Filter is defined to all IP addresses.



Step 5. Click the radio button that corresponds with the desired network mask in the Network Mask field.

- Mask — Enter the network mask in IP address format. This will define the subnet mask for the IP address.
- Prefix length — Enter the prefix length (integer in the range of 0 to 32). This will define the subnet mask by prefix length for the IP address.



Step 6. Click the radio button that corresponds with the desired TCP port that is to be applied to the filter in the TCP Port field.

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

Step 7. Click **Apply**.