Configuration of Denial of Service Prevention Techniques (Security Suite) on Sx500 Series Stackable Switches

Objective

Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks restrict the valid users to use the network. The attacker performs a DOS attack by flooding a network with many unnecessary requests that take up all the bandwidth of the network. DoS attacks can either slow down a network, or completely take down a network for several hours. DoS protection is the main feature for improving network security; it detects the abnormal traffic and filters it.

This article explains the configuration of Denial of Service on Security Suite Settings and various techniques used for Denial of Service Prevention.

Note: If the DoS Prevention chosen is System-Level and Interface-Level Prevention, then the Martial Addresses, SYN Filtering, SYN Rate Protection, ICMP Filtering, and IP Fragment Filtering can be edited and configured. These configurations are also explained in this article.

Note: Before the DoS prevention is activated, it is necessary to unbind all Access Control Lists (ACLs) or any advanced QoS policies that are configured to the port. ACL and advanced QoS policies are not active once the DoS protection is enabled on the port.

Applicable Devices

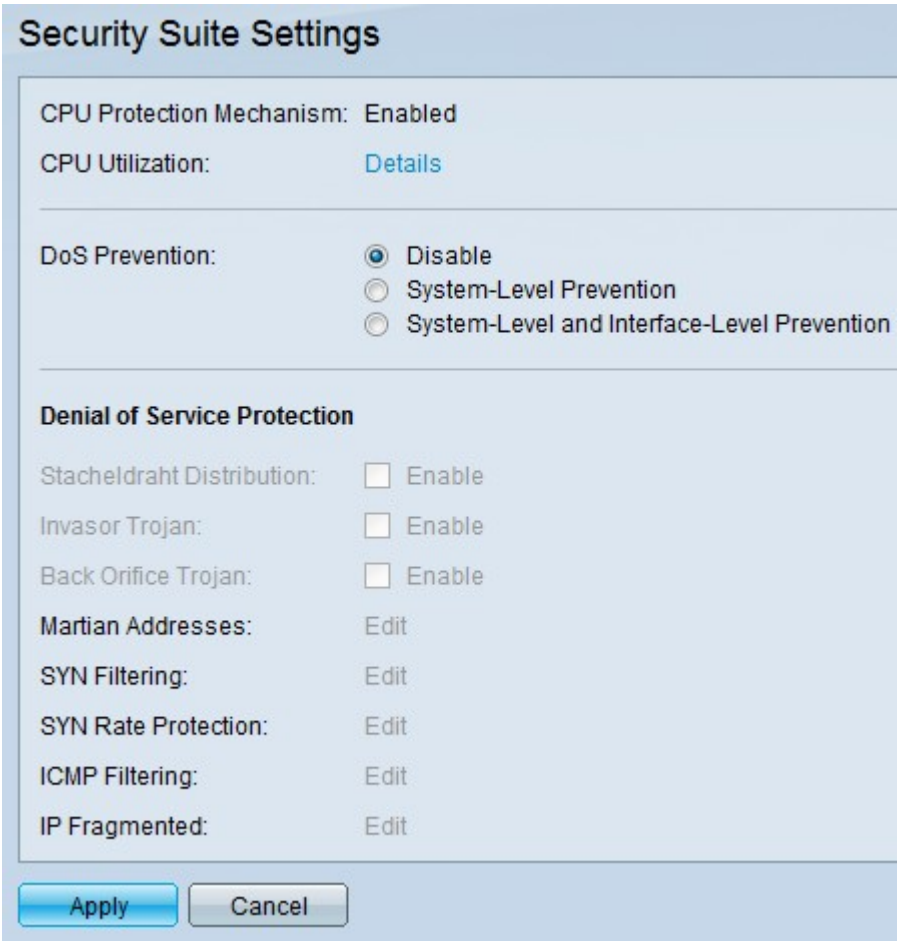
- Sx500 Series Stackable Switches

Software Version

- 1.3.0.62

Configuration of Denial of Service on Security Suite Settings

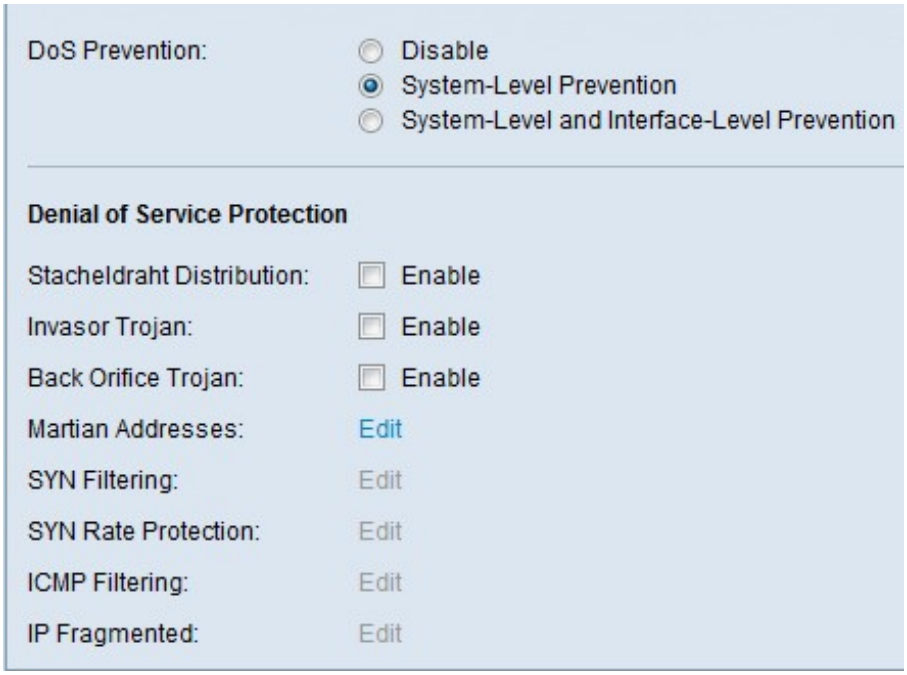
Step 1. Log in to the web configuration utility, and choose **Security > Denial of Service Prevention > Security Suite Settings**. The *Security Suite Settings* page opens:



- CPU Protection Mechanism — This is
- **Enabled**. This indicates that the Security Conversion Tool (SCT) is enabled.
- CPU Utilization — Click
- **Details** beside the CPU utilization to view the CPU resource utilization information.

Step 2. Click the appropriate radio button under DoS Prevention field.

- Disable — To disable DoS prevention.
- System-Level Prevention — This prevents attacks from Stacheldraht Distribution, Invasor Trojan and Back Orifice Trojan.
- System-Level and Interface-Level Prevention — This prevents attacks per interface on the switch.



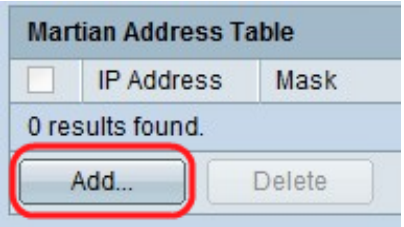
Step 3. These options can be chosen for Denial of Service Protection:

- Stacheldraht Distribution — This is an example of DDoS attack where the attacker uses a client program to connect to the computers inside the network. Those computers then sends out multiple login requests to the internal server and start a DDoS attack.
- Invasor Trojan — If the computer is infected by this attack, the TCP port 2140 is used for malicious activity. .
- Back Orifice Trojan — This discards UDP packets that are used to communicate with the server and client program for DoS attack.

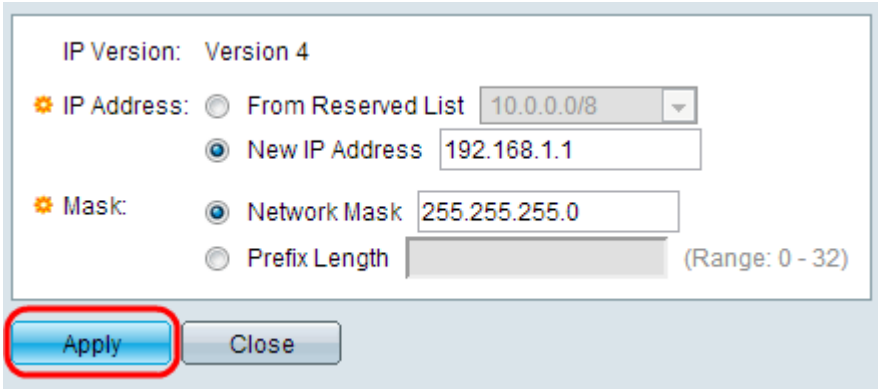
Configuration of Martian Addresses

Step 1. Click **Edit** in the Martian Addresses field then the *Martian Addresses* page opens. Martian Addresses indicate the IP address that can possibly be the cause of an attack on the network. Packets which come from these networks are dropped.

Step 2. Check **Include** in the Reserved Martian Addresses and click **Apply** to add the Reserved Martian Addresses in the System Level Prevention list.



Step 3. To add a Martian Address click **Add**. The *Add Martian Addresses* page is displayed. Enter these parameters:



Step 4. In the IP Address field enter the IP address which needs to be rejected.

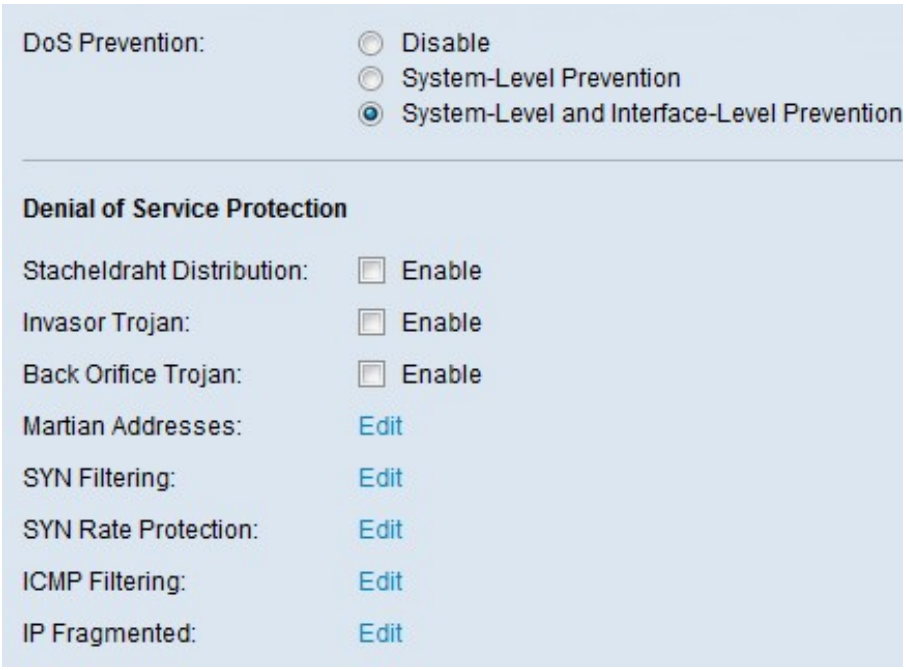
Step 5. The Mask of IP address to indicate the range of IP addresses which should be rejected.

- IP Version — The supported IP version. At present, only IPv4 is allowed.
- From reserved List — Choose a known IP address from reserved list.
- New IP address — Enter an IP address.
- Network Mask — Network Mask in the dotted decimal format.
- Prefix Length — Prefix of IP address to define the range of IP addresses for which the Denial of Service Prevention is enabled.

Step 6. Click **Apply** which makes the Martian Address to be written to the Running Configuration file.

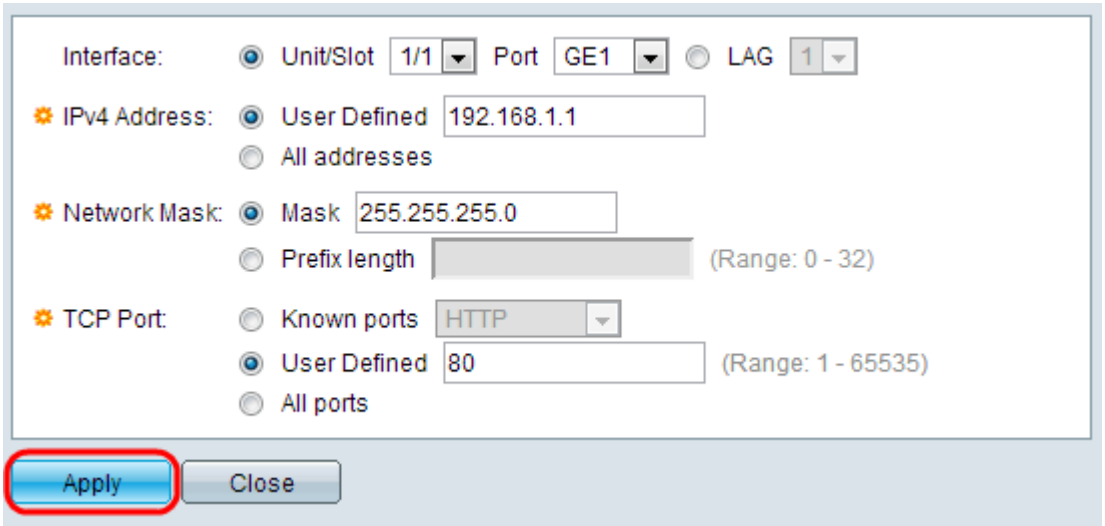
Configuration of SYN Filtering

SYN Filtering allows network administrators to drop illegal TCP packets with SYN flag. SYN port filtering is defined on a per-port basis.



Step 1. To configure SYN Filtering click **Edit** and the *SYN Filtering* page opens:

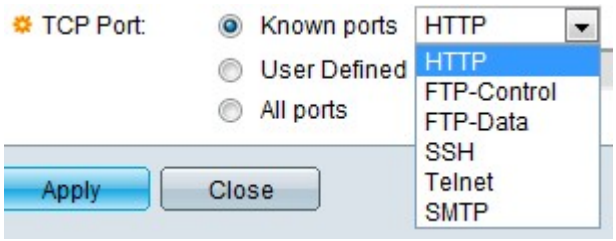
Step 2. Click **Add**. The *Add SYN filtering* page is shown. Enter these parameters in the displayed fields:



Step 3. Choose the interface on which the filter needs to be defined.

Step 4. Click **User Defined** to give an IP address for which the filter is defined or click **All Addresses**.

Step 5. The Network Mask for which the filter is enabled. Click **Prefix Length** in order to specify the length, its range is from 0 to 32, or click **Mask** to enter the subnet mask as in dotted decimal notation.



Step 6. Click the destination TCP port being filtered. They are of the types:

- Known Ports — Choose a port from the list.
- User Defined — Enter the port number.
- All Ports — Click to indicate that all ports are filtered.

Step 7. Click **Apply** which makes the SYN Filtering to be written to the running configuration file.

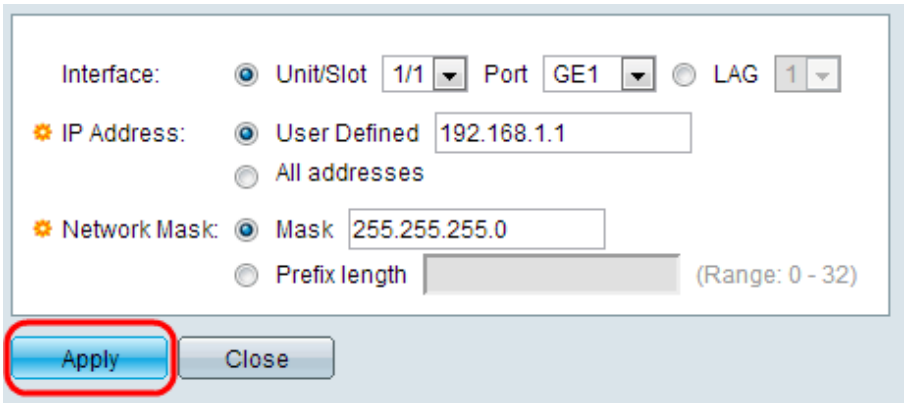
Configuration of ICMP Filtering

Internet Control Message Protocol (ICMP) is one of the most important Internet Protocols. It is a network layer protocol. ICMP is used by the operating systems to send error messages to tell that the service which was requested is not available or a particular host cannot be reached. It is also used to send diagnostic messages. ICMP cannot be used to exchange data between the systems. They are usually generated in response to some errors in the IP datagrams.

ICMP traffic is a very critical network traffic but it can also lead to many network issues if it is used against the network by a malicious attacker. This brings up the need for strictly filtering the ICMP traffic that comes from the Internet. The *ICMP Filtering* page enables the filtering of the ICMP packets from particular sources. This minimizes the load on the network in case if there is any ICMP attack.

Step 1. To configure ICMP Filtering click **Edit** and the *ICMP Filtering* page opens.

Step 2. Click **Add**. The *Add ICMP Filtering* page is shown. Enter these parameters in the displayed fields:



Step 3. Choose the interface on which the ICMP Filtering is defined.

Step 4. Enter the IPv4 Address for which the ICMP packet filtering is enabled or click **All Addresses** to block ICMP packets from all source addresses. If IP address is entered, enter either the mask or prefix length.

Step 5. The Network Mask for which the rate protection is enabled. Choose the format of the network mask for the source IP address and click one of the fields.

- Mask — Choose the subnet to which the source IP address belongs to and enter the subnet mask in dotted decimal format.
- Click **Prefix Length** in order to specify the length and enter the number of bits that consists of the source IP address prefix, its range is from 0 to 32.

Step 6. Click **Apply** which makes the ICMP Filtering to be written to the running configuration file.

Configuration of IP Fragments Filtering

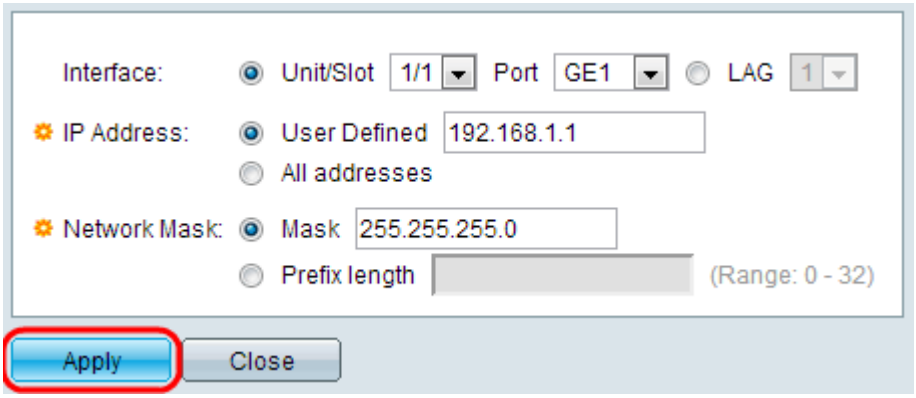
All the packets have a Maximum Transmission Unit (MTU) size. MTU being the size of the largest packet that a network can transmit. IP takes the advantage of fragmentation so that packets can be formed which can traverse through a link with a smaller MTU than the original packet size. Therefore, packets whose sizes are larger than the permissible MTU of the link must be divided into smaller packets to allow them to traverse through the link.

On the other hand, fragmentation can also pose many security problems. So it becomes necessary to block IP fragments as sometimes they can be a reason for system compromise.

Step 1. To configure IP Fragments Filtering click **Edit** and the *ICMP Fragments Filtering* page opens.

Step 2. Click **Add**. The *Add IP Fragment Filtering* page is shown. Enter these parameters in

the displayed fields:



Step 3. Interface — Choose the interface on which the IP fragmentation is defined.

Step 4. IP Address — Enter the IP Address for which the IP fragmentation is enabled or click **All Addresses** to block IP fragmented packets from all source addresses. If IP address is entered, enter either the mask or prefix length.

Step 5. Network Mask — The Network Mask for which the IP fragmentation is blocked. Choose the format of the network mask for the source IP address and click one of the fields.

- Mask — Choose the subnet to which the source IP address belongs to and enter the subnet mask in dotted decimal format.
- Click **Prefix Length** in order to specify the length and enter the number of bits that consists of the source IP address prefix, its range is from 0 to 32.

Step 6. Click **Apply** to make the IP Fragments Filtering to be written to the running configuration file.