

SYN Rate Protection on 300 Series Managed Switches

Objective

Denial of Service (DOS) prevention is a network technology that increases network security. SYN rate protection is a DOS prevention feature that limits the number of SYN packets that a port or LAG can receive. This is used to prevent SYN floods on a network. SYN floods are a type of DOS attack that occurs when an attacker sends multiple SYN request packets to a network. This overloads the resources of the network which makes the network unresponsive to actual traffic.

To utilize this feature, DoS Prevention must be enabled to System-Level and Interface-Level Prevention on the *Security Suite Settings* page. Refer to the article *Security Suite Settings on 300 Series Managed Switches* for more information.

This article explains how to configure and apply a SYN rate limit to an interface on the 300 Series Managed Switches.

Applicable Devices

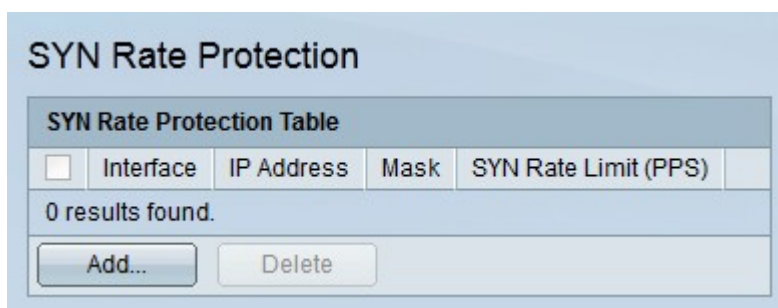
- SF/SG 300 Series Managed Switches

Software Version

- v1.2.7.76

SYN Rate Protection

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



SYN Rate Protection Table				
<input type="checkbox"/>	Interface	IP Address	Mask	SYN Rate Limit (PPS)
0 results found.				
<input type="button" value="Add..."/>		<input type="button" value="Delete"/>		

Step 2. Click **Add** to add SYN Rate Protection. The *Add SYN Rate Protection* window appears.

Interface: Port FE1 LAG 1

IP Address: User Defined 192.168.1.1 All addresses

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

SYN Rate Limit: 250 PPS (Range: 199 - 1000)

Apply Close

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

- Port — From the Port drop-down list choose the port that the SYN rate protection will apply to.
- LAG — From the LAG drop-down list choose the LAG that the SYN rate protection will apply to.

Step 4. Click the radio button that corresponds to the desired IPv4 address in the IP address field. Packets from these IP addresses will be limited by SYN rate protection.

- User Defined — Enter an IPv4 address.
- All addresses — All IPv4 addresses apply.

Step 5. Click the radio button that corresponds to 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. Enter a value in the SYN Rate Limit field. This is the maximum number of SYN packets the interface can receive per second.

Step 7. Click **Apply**. The SYN Rate Limit is applied to the interface.

SYN Rate Protection

SYN Rate Protection Table				
<input type="checkbox"/>	Interface	IP Address	Mask	SYN Rate Limit (PPS)
<input type="checkbox"/>	FE1	192.168.1.1	255.255.255.0	250

Add... Delete