IPv4 Firewall Rule configuration on Cisco SA540 Security Appliance

Objective

The objective of this document to explain how to configure IPv4 firewall rules on Cisco SA540 Security Appliance. Firewall provide network protection by blocking unwanted traffics or by denying unauthorized access to network. The Cisco SA500 Series has a powerful firewall feature which block unauthorized traffic and allow only authorized traffic.

Applicable Devices

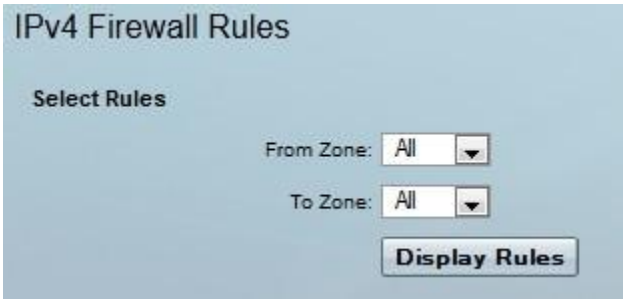
• SA540 Security Appliance

Software Version

• v2.1.21

Outbound Firewall Configuration

Step 1. Log in to the web configuration utility, choose **Firewall > IPv4 Rules**. The *IPv4 Firewall Rules* page opens:



Step 2. From the From Zone drop down list choose the desired option to indicate the source.

- LAN —Local Area Network (LAN) is the network that interconnects devices over a limited area.
- WAN — Wide Area Network (WAN) is the network that covers a broad area that links across regional or national boundaries.
- DMZ — Demilitarized Zone (DMZ) is the network that permits two LAN networks instead of the currently available single LAN network.

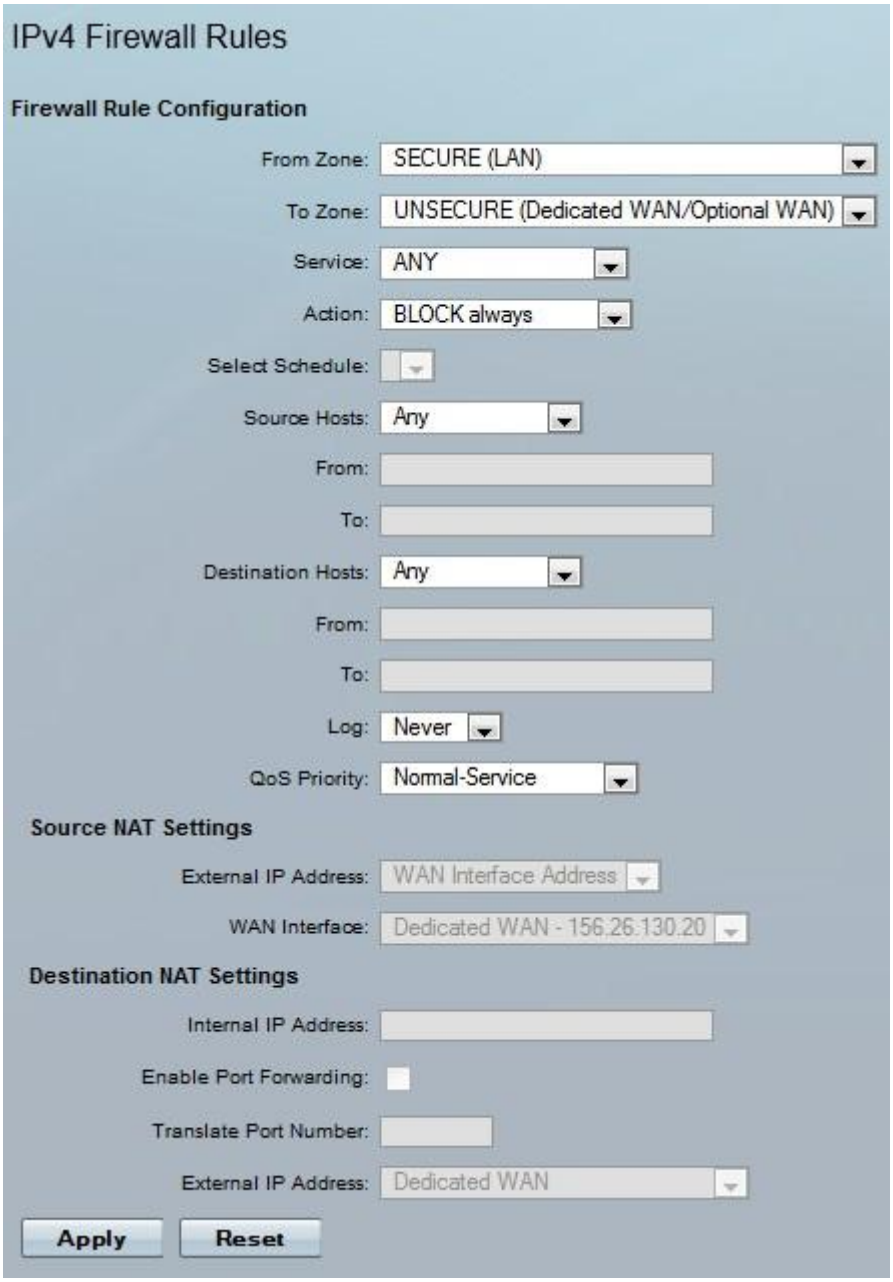
Step 3.From the To Zone drop down list choose the option to indicate the destination.

Step 4. Click **Display Rules** to display configured rules.

Add Firewall Rule

Step 1. Log in to the web configuration utility, choose **Firewall > IPv4 Rules**. The *IPv4 Firewall Rules* page opens:

Step 2. To create a new firewall rule click **Add.** The *IPv4 Firewall Rules* window appears:



Step 3. In the IPv4 Firewall Rules Window enter the parameters in the fields or choose the parameters from the drop-down lists.

• From Zone — The source of the outbound traffic. Outbound traffic originates from SECURE Local Area Network (LAN) - locally connected devices or DMZ (De Militarized Zone) - local servers which are logically separated from normal users.

• To Zone — The destination network for the outbound traffic, it can be Wide Area Network (WAN), DMZ or remote servers and hosts.

• Service — the security appliance comes with predefined service types which include range of protocols and applications such as Border Gateway router (BGP), (Transmission Control Protocol) TCP, or user customized services types created in the service menu.

• Action **—** defines firewall schedules .

– BLOCK always — blocks the outbound traffic always or choose ALLOW always to allow outbound traffic make the rule active all the time .

– BLOCK by schedule — blocks the outbound traffic by schedule.

– ALLOW by schedule — Allows outbound traffic by schedule. Choose the schedule created from the Select Schedule drop-down list.

• Source Hosts — users located on the SECURED LAN or DMZ which generate traffics to the outside network.

– Any — Chooses all users in the SECURED LAN or DMZ network .

– Single Address — For a single user. Enter the IP address in From field.

– Address Range — Define many users and enter the starting IP address in From field and the end IP address To field to

• Destination Hosts — Defines all the destination servers and users .

– Any — Defines all users and servers outside the local network .

– Single Address — Defines a single remote server and enter the IP address in From field.

– Address Range — Defines a range of users and enter the starting IP address in From field and the end IP address To field.

• Log — Choose the desired option from the drop down list.

– Always — To log every packet in the firewall rule .

– Never — Not to log the packets .

• Qos Priority — The firewall rule used to set packet priority for services.

– Normal-Service — Minimum priority. All the TOS bits are set to zero .

– Minimize-cost — Uses ToS equal to 1 to set the cost .

– Maximize-Reliability — ToS equal to 2. This will give the traffic the highest reliability.

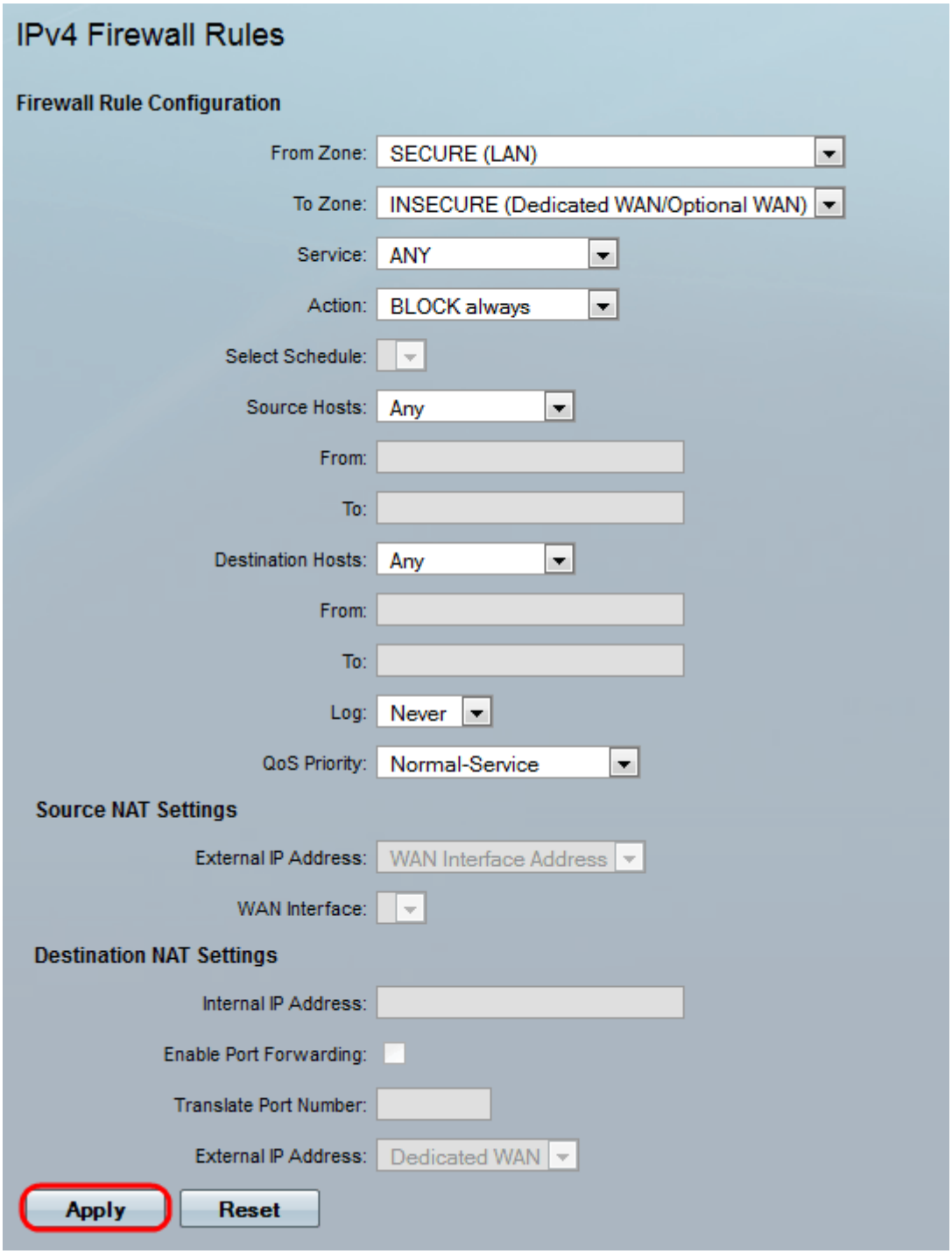
– Maximize-Throughput — ToS equal to 3.

– Minimize-Delay — Gives the highest priority to the packet .

Step 4. Click **Apply** to save.

Inbound Firewall Configuration

Step 1. Log in to the web configuration utility, choose **Firewall > IPv4 Rules**. The *IPv4 Firewall Rules* page opens:



Step 2. To create a new firewall rule click **Add** and Enter the parameters in the fields or choose the parameters from the drop-down lists.

• From Zone — The source of the traffic. Inbound traffic originates from INSECURE (Dedicated WAN/Optional WAN) - local connected devices, or DMZ (De Militarized Zone) Servers .

• To Zone — The destination network for the outbound traffic. The destination network can be SECURE(LAN)or DMZ .

• Service — Choose service type from the predefined services which include a range of protocols and applications or customized services types created. To create Customized rule, choose **Firewall > Services** from the navigation menu.

• Action **—** The action check box defines firewall schedules.

– Choose BLOCK always to block the outbound traffic always or choose ALLOW always to allow outbound traffic make the rule active all the time .

– Choose BLOCK by schedule to block the inbound traffic by schedule.

– ALLOW by schedule — Allows inbound traffic by schedule. Choose the schedule created from the Select Schedule drop-down list.

• Source Hosts — Users located on the SECURED LAN or DMZ, which generate traffic to the outside network.

– Any — All the users in the SECURED LAN or DMZ network.

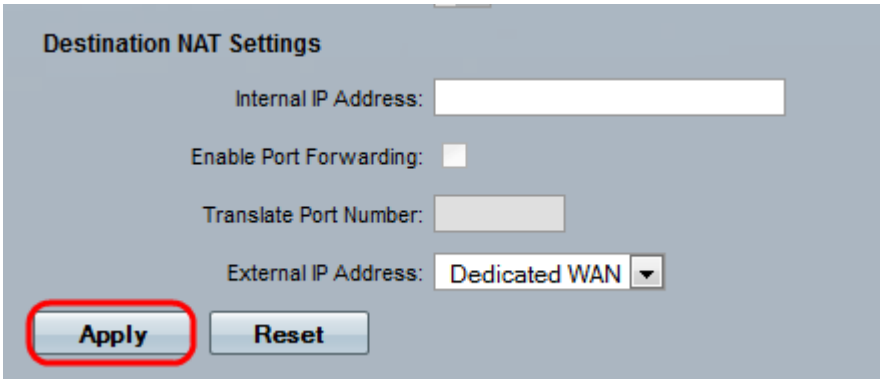
– Single Address — A single user. Enter the IP address in the From field.

– Address Range — Defines many users by starting IP address in the **From** field and the end IP address in the **To** field.

• Log — Choose **Always** to log every packet in the firewall rule or choose **never** not to log the packets .

Step 3. Set the destination network under the Destination NAT Settings section and Enter the IP address of the Internal IP address or check **Enable Port Forwarding** check box and enter the port number in Translate Port Number to forward the traffic to a specific port.

Step 4. Select the public interface to be used in the NAT translation by choosing **Dedicated WAN** or **Optional WAN** in the External IP Address drop-down menu.



Step 5.Click **Apply** to save.