Network Address Translation (NAT)

Network Address Translation (NAT) maps outbound IP addresses to prevent exposing internal IP addresses.

NAT allows you to:

- Conceal the internal IP address from external exposure or access.
- Reduce the demand for registered IP addresses because internal IP addresses are not revealed to the outside world.

Incoming IP addresses can be translated to correct internal IP addresses.

Source Network Address Translation (SNAT)

Source Network Address Translation (SNAT) maps internal IP (private IP) addresses to an external IP (public IP) address.Source Network Address Translation (SNAT) re-writes the IP address of the computer that originated the packet. SNAT is composed of two steps:

- The process of translating an internal IP address into an external IP address.
- The process of undoing the translation for returning traffic, that is, rewriting the IP address of the computer that originated the packet.

For example, consider an internal IP address 10.1.2.27 sends a packet to an external web server. The Barracuda Web Application Firewall translates the internal IP address 10.1.2.27 to an external IP address 209.165.201.10. When the external web server responds, the external IP address 209.165.201.10 receives the packet and sends it to the internal IP address 10.1.2.27.

Following are the SNAT Capabilities Provided by the Barracuda Web Application Firewall:

- **Dynamic NAT**: Sets up a sequential translation between internal IP addresses and external IP addresses. You can specify a range of external IP addresses, and the Barracuda Web Application Firewall dynamically maps the internal IP address to the available external IP address. For example, enter the internal IP address *10.1.2.0* in **Pre SNAT Source** with subnet mask *255.255.255.0* in **Pre SNAT Source Mask** and enter a range of external IP addresses (*209.165.201.11 - 209.065.201.16*) in **Post SNAT Source**. The Barracuda Web Application Firewall will translate internal source IP addresses to the available external IP address.
- **Static NAT**: Sets up a one to one translation between a single internal IP address and a single external IP address. For example, an internal IP address of 10.1.2.27 will always translate to 209.165.201.10.

A SNAT rule can be added in the **NETWORKS > NAT** page. In the **Add NAT** section, select **Source NAT** as **NAT Type** and specify values for the fields. For more information, click **Help** on the relevant web interface page.

Destination Network Address Translation (DNAT)

Destination Network Address Translation (DNAT) re-writes the destination IP address of incoming traffic. Consider you have a server inside your LAN, and you want users outside the network to access that server. This can be accomplished by configuring DNAT rule that directs all the traffic passing through the Barracuda Web Application Firewall to the internal network.

For example, users outside your network cannot access a mail server inside your LAN with the IP address 192.168.2.5 on port 25 through the Barracuda Web Application Firewall because routing to a private IP address is not possible. If you want to allow users to access that mail server, you need to configure the DNAT rule for port 25 so that traffic destined for port 25 on the WAN interface of the Barracuda Web Application Firewall is redirected to 192.168.2.5.

Ensure that you configure an ACL rule along with the DNAT rule to allow the traffic to pass through the Barracuda Web Application Firewall via port 25 or else the firewall will drop the incoming packets.

A DNAT rule can be added in the **NETWORKS > NAT** page. In the **Add NAT** section, select **Destination NAT** as **NAT Type** and specify values for the fields. For more information, click **Help** on the relevant web interface page..