Allowing Internet Access for the Back-end Servers in Two-Arm Proxy Mode - Version 9.0 and Earlier

When the Barracuda Web Application Firewall is deployed in Two-Arm Proxy Mode, all traffic originating from the LAN to the Internet is denied by default. NAT rules must be configured to map internal source IP addresses to routable IP addresses.

The Barracuda Web Application Firewall allows you to configure NAT rules on the **ADVANCED > Advanced Networking** page.

Configuring Source Network Address Translation Rule

Perform the following steps:

1. From the **ADVANCED > Network Firewall** page in the **Source Network Address Translation** section, specify values for the following:
    1. **Pre SNAT Source** - Specify the IP Address/Network of your back-end Web server that needs to be translated.
    2. **Pre SNAT Source Mask** - Specify the associated network mask for the source IP Address/Network.
    3. **Protocol** - Select TCP/UDP as the communication protocol to be used between the hosts.
    4. **Destination Port** - Specify the destination port/range of port numbers of the server to which the back-end server wants to connect.
    5. **Outgoing Interface** - Select WAN as the outgoing interface for the traffic to pass through.
    6. **Post SNAT Source** - Specify the IP Address to which your Web server IP Address should be mapped to access the Internet.
2. Click **Add**.

If the **Post SNAT Source** is different from the WAN IP address of the Barracuda Web Application Firewall, you need to add the new IP address in the **Custom Virtual Interfaces** section on the **ADVANCED > Advanced Networking** page to associate it to the WAN interface.

If the back-end server needs to connect to the Internet via Barracuda Web Application Firewall, the servers default gateway should be either:

- The LAN IP address of the Barracuda Web Application Firewall, OR
- Custom Virtual Interface configured on the LAN interface of the Barracuda Web Application Firewall. Custom Virtual Interface can be configured using **Interface** tab on the **ADVANCED > Advanced Networking** page.

NAT for LAN Servers (Auto SNAT)

You can configure auto SNAT for LAN servers to reach Internet directly without any NAT or ACL rule being configured. Use the **ADVANCED > Advanced Networking** page to configure NAT for LAN Servers.

Steps To Configure NAT for LAN Servers

Perform the following steps:

1. Go to the **ADVANCED > Advanced Networking** page.

2. In the **Network Configuration** section, select **System** as **Network Group** and then select the **Configuration** tab.
3. In the **NAT for LAN Servers** section, set **Enable SNAT for LAN Servers** to *Yes*.
4. Click **Save**.

When **Enable SNAT for LAN Servers** is set to *Yes*, all traffic originating from LAN to go out on the WAN is automatically NATted with the WAN interface IP address. The traffic originating from any subnet that belongs to LAN is also NATted. In this case, a user is not required to configure SNAT and ACL rule for the real servers, as the Barracuda Web Application Firewall automatically NATs and allows the LAN traffic to go out to the Internet.

If you want more granular access control on the traffic originating from the LAN going out to the Internet, set **Enable SNAT for LAN Servers** to *No* and manually configure the SNAT rule.