Allowing Internet Access for the Backend Servers in Two-Arm Proxy Mode - Version 9.0 or Later

https://campus.barracuda.com/doc/78152119/

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 **NETWORKS > NAT** page.

Configure the Source Network Address Translation Rule

1. From the **Add NAT** section, specify values for the following:
   - **NAT Type** - Select **Source NAT**.
   - **Network Group** - Specify the network group for which NAT rules need to be added.
   - **Outgoing Interface** - Select WAN as the outgoing interface for the traffic to pass through.
   - **Pre SNAT Source** - Specify the IP address/network of your backend web server that needs to be translated.
   - **Pre SNAT Source Mask** - Specify the associated network mask for the source IP address/network.
   - **Protocol** - Select TCP/UDP as the communication protocol to be used between the hosts.
   - **Destination Port** - Specify the destination port/range of port numbers of the server to which the backend server wants to connect.
   - **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 must add the new IP address in the **Custom Virtual Interfaces** section on the **NETWORKS> Interfaces** page to associate it to the WAN interface.

If the backend server must connect to the Internet via the Barracuda Web Application Firewall, the server's default gateway should be *one* of the following two:

- The LAN IP address of the Barracuda Web Application Firewall
- The custom virtual interface configured on the LAN interface of the Barracuda Web Application Firewall. The custom virtual interface can be configured on the **Interface** tab on the **NETWORKS> Interface** page.

NAT for LAN Servers (Auto SNAT)

You can configure auto-SNAT for LAN servers to reach the Internet directly without any NAT or ACL rule being configured. Go to the **NETWORKS> Network Configuration** page to configure NAT for LAN Servers.

Configure NAT for LAN Servers

1. Go to the **NETWORKS> Network Configuration** page.
2. In the **Network Configuration** section, set **Yes** for **Enable SNAT for LAN Servers** to allow all the servers in the LAN to reach Internet directly without even configuring any NAT or ACL rule.
3. 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 NATed with the WAN interface IP address. The traffic originating from any subnet that belongs to LAN is also NATed. In this case, a user is not required to configure SNAT and ACL rules for the Real servers because the Barracuda Web Application Firewall automatically NATs and allows the LAN traffic to go out to the Internet.

For 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.