How to Configure Layer 2 Bridging

https://campus.barracuda.com/doc/53248855/

When performing layer 2 bridging the Barracuda NextGen Firewall F-Series will be completely transparent to the user. The interface is not assigned an IP address and can not be directly contacted by the user in the bridged networks. Traffic passing through the layer 2 bridge will retain it's original MAC address with the bridge acting as a proxy ARP in the middle. Since the bridged network interface do not have an IP address you will need to use a separate interface to locally administer the Barracuda NextGen Firewall F-Series. You can define multiple bridging groups on one interface. Traffic between the interface groups is forwarded on layer 3. Define a pass and a broad-multicast access rule for each bridge interface group.

The bridge can only be used for IP based protocols.

Step 1. Configure Transparent Layer 2 Bridging

1. Go to CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Settings.
2. In the left menu, select Layer 2 Bridging.
3. Click Lock.
4. In the Bridged Interface Group table, click + to add an entry. For each interface group, you can edit the following settings:
   - Bridged Interfaces - Add all interfaces to be bridged together in this group. For each interface enter the following settings:
     - Name - The exact network interface label, as listed in the network configuration. E.g., eth1
     - Allowed Networks (ACL) - Networks that are allowed to communicate over the bridged interface. You can enter complete networks, individual client/server IP addresses, or network ranges.
     - Unrestricted MACs - List of MAC address for which the Allowed Networks (ACL) does not apply.
- **MAC Change Policy** – Select **Allow-MAC-Change** to permit the MAC address of the interface to be changed, otherwise select **Deny-MAC-Change**.
  - **Use IP BARP Entries** – Select **yes** if the Barracuda NextGen Firewall F-Series must learn the MAC addresses from IP and ARP traffic and record IP addresses that are assigned to a specific MAC address in a separate table. If there are a very large number of IP addresses in a specific network segment, select **no** to keep the ARP table from being overrun.

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

**Step 2. Create Access Rules for Layer 2 Bridging**

To allow network traffic to pass between the bridged interfaces, create **Pass** and **Broad-Multicast** access rule for every bridged interface group.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.

1. Click **Lock**.
2. Create a pass access rule with the following settings:
   - **Action** – Select **PASS**.
   - **Bi-Directional** – **Yes**.
   - **Source** – Select **Any (0.0.0.0/0)**
Service - Select Any
Destination - Select a network object containing all networks or IP addresses for the bridged interfaces. E.g., 10.0.8.0/24 and 172.31.1.25
Connection Method - Select Original Source IP

3. Create a Broad-Multicast access rule with the following settings:
   - Action - Select Broad-Multicast.
   - Source - Select a network object containing all networks or IP addresses for the bridged interfaces. E.g., 10.0.8.0/24 and 172.31.1.25
   - Service - Select Any
   - Connection Method - Select Original Source IP
   - Destination - Enter the destination networks/IP addresses. E.g., 10.0.8.25

   To use a DHCP server over the layer 2 bridge, also add 0.0.0.0 to the source and 255.255.255.255 to the destination IP addresses.

   - Propagation List - Enter the propagation interface or IP address(es). For more information, see How to Create a Broad-Multicast Access Rule.

4. Rearrange the order of the access rules so the new rules can match incoming traffic.
5. Click Send Changes and Activate.
Figures

1. fw_layer2_bridge.png
2. trans_l2_config.png