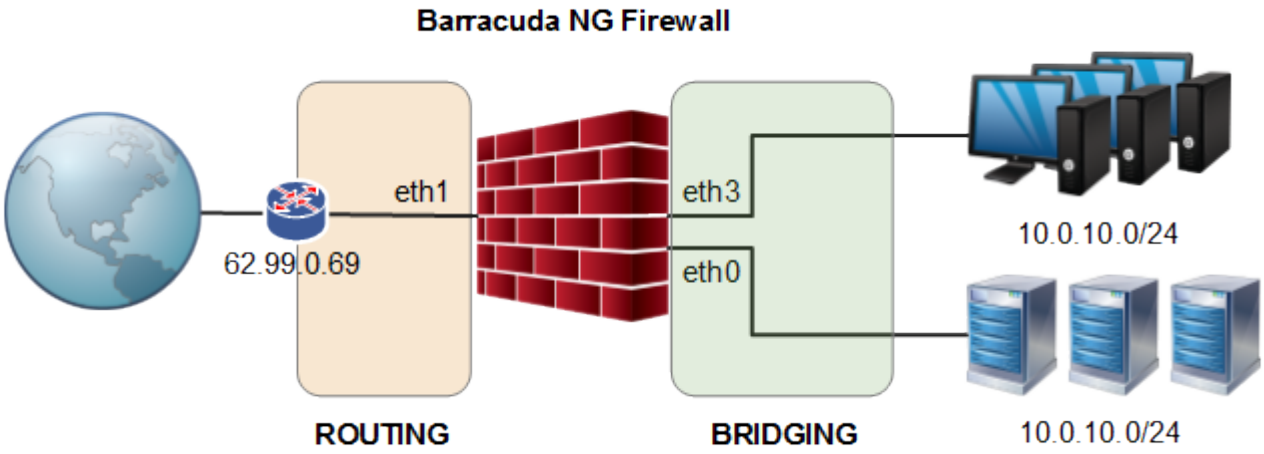
How to Configure Routed Layer 2 Bridging

https://campus.barracuda.com/doc/41115957/

Routed bridging is used when the firewall must act as a layer 2 bridging and layer 3 routing device simultaneously. This is needed when the clients and servers in the bridged network must send data into another network. The bridged interfaces are assigned local ip addresses so the clients in the bridged networks can directly address the Barracuda NG Firewall. Firewall rules forward traffic between the bridge interface groups and the external networks.

In this article



Step 1. Configure a Routed Layer 2 Bridge

Create a layer 2 bridge and add bridge IP addresses to allow the clients in the bridges networks to directly access the Barracuda NG Firewall.

1. Open the **Firewall Forwarding Settings** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall**).
2. In the left navigation, click on **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

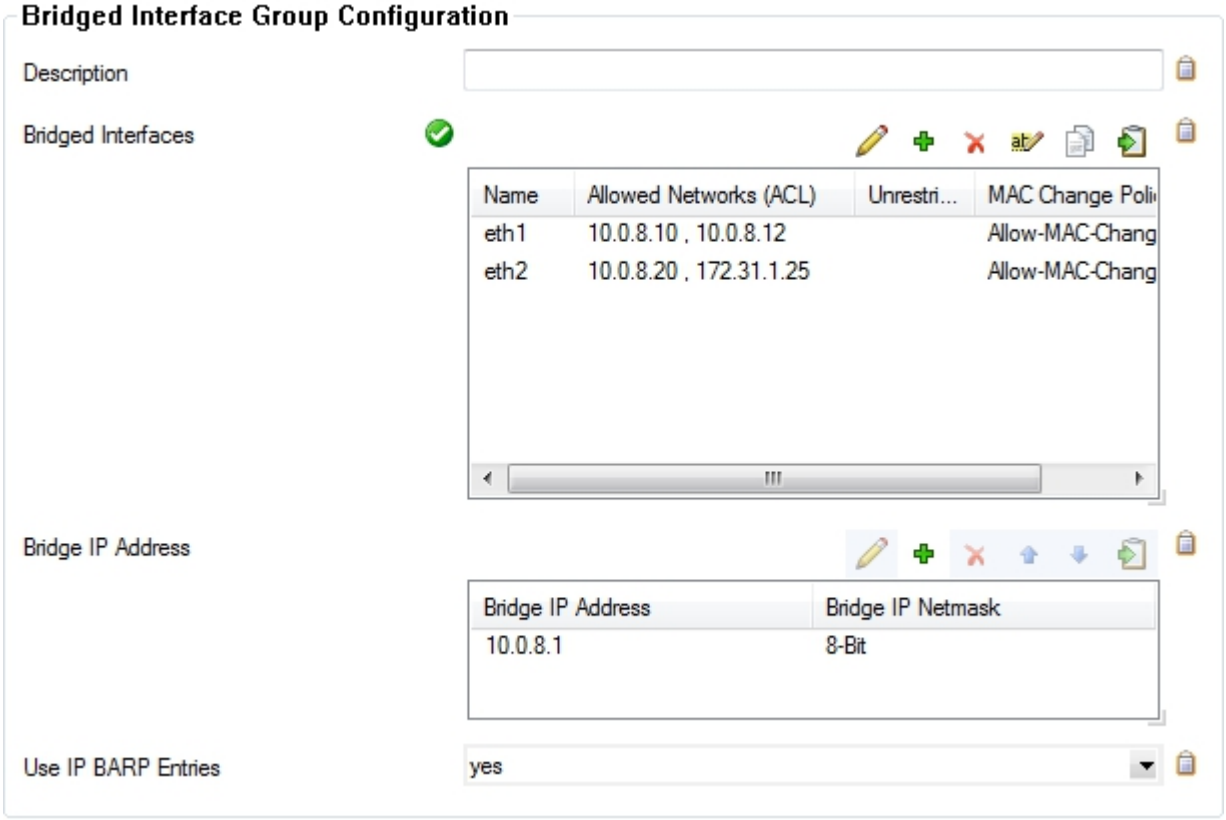
interface enter the following settings:

- **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**.

◦ **Bridge IP Address** – Add an entry or edit an existing entry for the gateway. In the entry, specify the following settings for the gateway:

- **Bridge IP Address** – IP address for the gateway. E.g., 62.99.0.254
- **Bridge IP Netmask** – Netmask for the gateway.

◦ **Use IP BARP Entries** – Select **yes** if the Barracuda NG Firewall 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 Firewall Rules

To allow network traffic to pass between the bridged interfaces, create Pass and Broad-Multicast firewall rules:

1. Open the **Forwarding Rules** page (**Config > Full Config > Box > Virtual Servers > *your virtual server*>Assigned Services > Firewall**).
2. Click **Lock**.
3. Create a **Pass** firewall rule with the following settings:
   - **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 **No SNAT**.
4. Create a **Broad-Multicast** firewall rule with the following settings:
   - **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 **No SNAT**.
   - **Destination** – Enter the destination networks/IP addresses. E.g., `10.0.8.255`

     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.
5. Rearrange the order of the firewall rules so the new rules can match incoming traffic.
6. Click **Send Changes** and **Activate**.

Figures

1. FW_Bridging_L2Bridge.png
2. route_trans_l2_2config.png