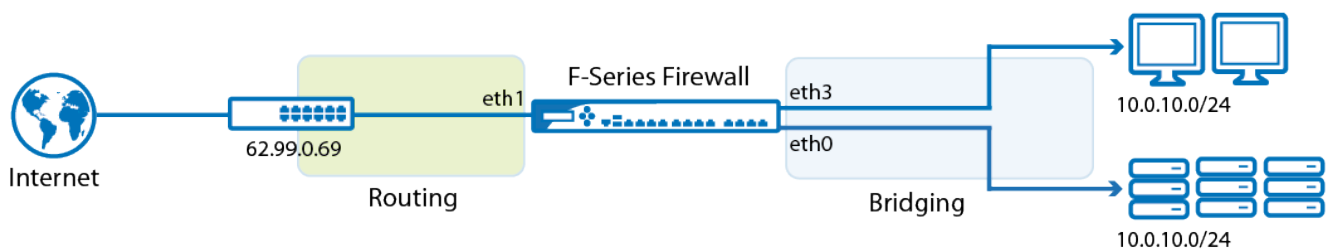


How to Configure Routed Layer 2 Bridging

<https://campus.barracuda.com/doc/48203318/>

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 NextGen Firewall F-Series. Firewall rules forward traffic between the bridge interface groups and the external networks.



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 NextGen Firewall F-Series.

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

Bridged Interface Group Configuration

Description

Bridged Interfaces      

Name	Allowed Networks (ACL)	Unrestr...	MAC Change Poli
eth1	10.0.8.10 , 10.0.8.12		Allow-MAC-Chang
eth2	10.0.8.20 , 172.31.1.25		Allow-MAC-Chang

Bridge IP Address      

Bridge IP Address	Bridge IP Netmask
10.0.8.1	8-Bit

Use IP BARP Entries

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

Step 2. Create access rules

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a **Pass** access 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 **Original Source IP**
4. Create a **Broad-Multicast** access 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 **Original Source IP**
 - **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.
 - **Propagation List** - Enter the network interfaces. E.g., eth0, eth0, brid01
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_routed_layer2_bridge.png
2. route_trans_l2_2config.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.