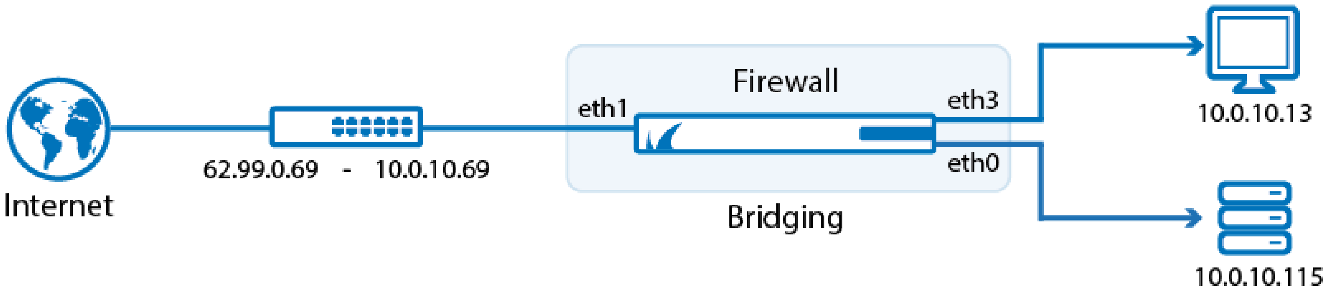
How to Configure Layer 2 Bridging

https://campus.barracuda.com/doc/73719336/

When performing layer 2 bridging the Barracuda CloudGen Firewall 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 CloudGen Firewall. 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.

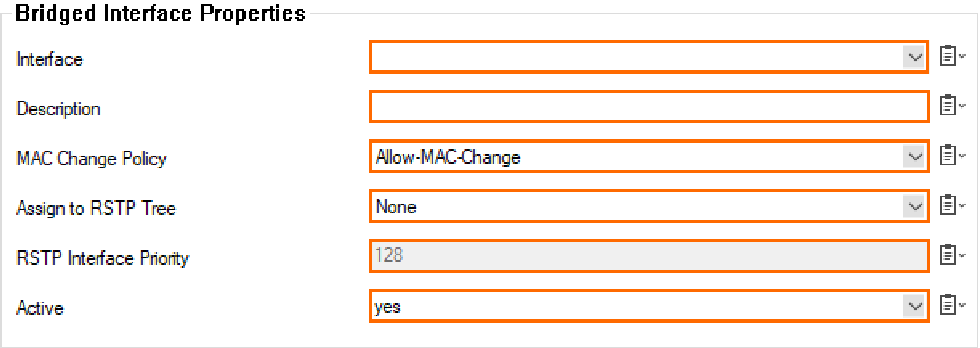
The bridge can only be used for IPv4 based protocols.



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:
        - **Interface** – Select the interface from the list.
        - **Description** – Enter an optional description of the interface.
        - **MAC Change Policy** – This option controls whether a MAC address that is bound to an IP address may change during an active session. If the policy allows a MAC to change, a previously assigned IP address is subsequently available at a different MAC address.
            - **Allow-MAC-Change** – MAC addresses may change during an active session.

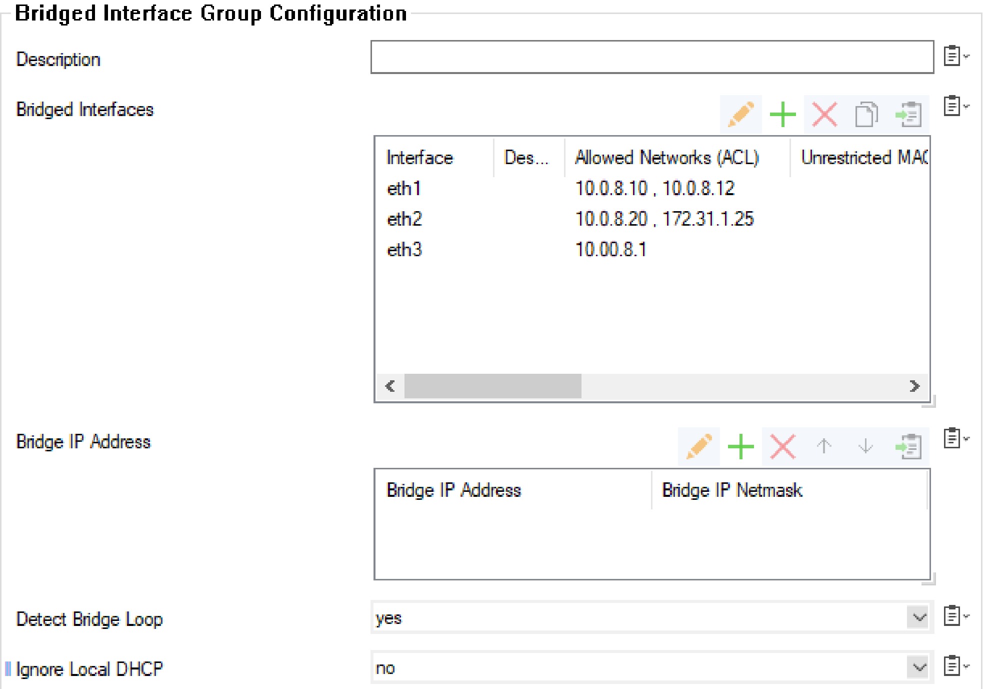
        - **Deny-MAC-Change** – MAC addresses must not change during an active session.
    - **Assign to RSTP Tree** – Assign the interface to an existing RSTP Tree by choosing it from the list.
    - **RSTP Interface Priority** – Assign a priority to the RSTP interface. This might affect the role the port will play in the calculated topology.
    - **Active** – Default is **yes**. Set to **no** to disable the setting to leave the interface within the configuration but prevent it from being used.



Bridged Interface Properties

Interface	
Description	
MAC Change Policy	Allow-MAC-Change
Assign to RSTP Tree	None
RSTP Interface Priority	128
Active	yes

  - **Detect Bridge Loop** – Detected layer 2 loops and disable ARP and broadcast propagation if required. Note that a bridge IP address must be preset for loop detection to work. Default is **yes**.



Bridged Interface Group Configuration

Description

Bridged Interfaces

Interface	Des...	Allowed Networks (ACL)	Unrestricted MA
eth1		10.0.8.10 , 10.0.8.12	
eth2		10.0.8.20 , 172.31.1.25	
eth3		10.00.8.1	

Bridge IP Address

Bridge IP Address	Bridge IP Netmask

Detect Bridge Loop	yes
Ignore Local DHCP	no

5. **RSTP Tree** – Add RSTP trees to the bridged interface group so that a subset of its interfaces can be assigned to them.
6. Click **OK**.
7. 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**.
2. Click **Lock**.
3. 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**
4. 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`

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

Figures