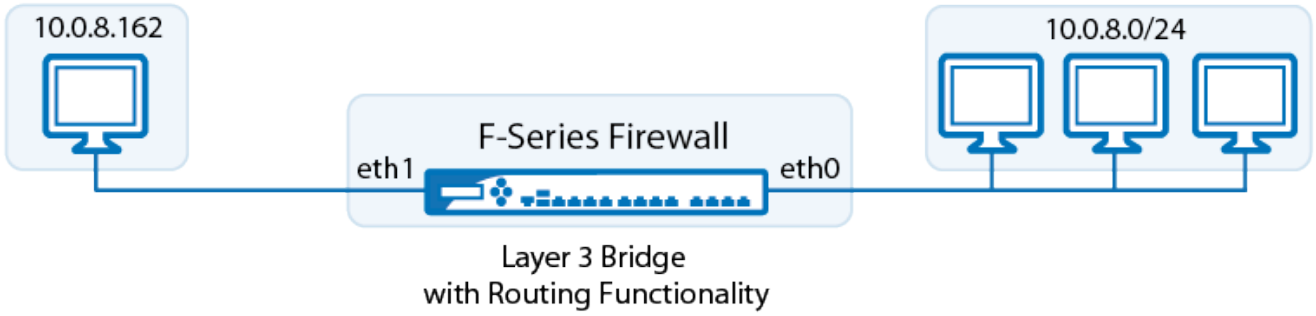
How to Configure Layer 3 Bridging

https://campus.barracuda.com/doc/46209396/

Layer 3 bridging is best used for client and server groups that include just a few clients that usually communicate with machines in their group. The bridge consists of two proxy ARPs and a firewall rule to pass traffic back and forth. If you want to bridge multiple clients, use a routed transparent Layer 2 bridge instead.

- All network traffic is delivered using Layer 3 (routing) lookups.
- All bridged network nodes must be entered into the configuration.
- Bridging is NOT Layer 2 transparent; the source MAC is not propagated in connection requests.
- Traffic between routed and bridged destinations is forwarded.
- Bridged network nodes may (if allowed) locally communicate with the interface.

An example setup that would be appropriate for layer 3 bridging would be if one PC in the network must be separated from the other clients and protected by the firewall. The PC that is to be singled out is placed in its own small network (e.g., 10.0.8.160/29) and the firewall acts as a non-transparent translational bridge between the 10.0.8.0/24 and the 10.0.8.0/29 networks. The Barracuda NextGen Firewall F-Series will answer all ARP requests that are transmitted between the networks.



In this article

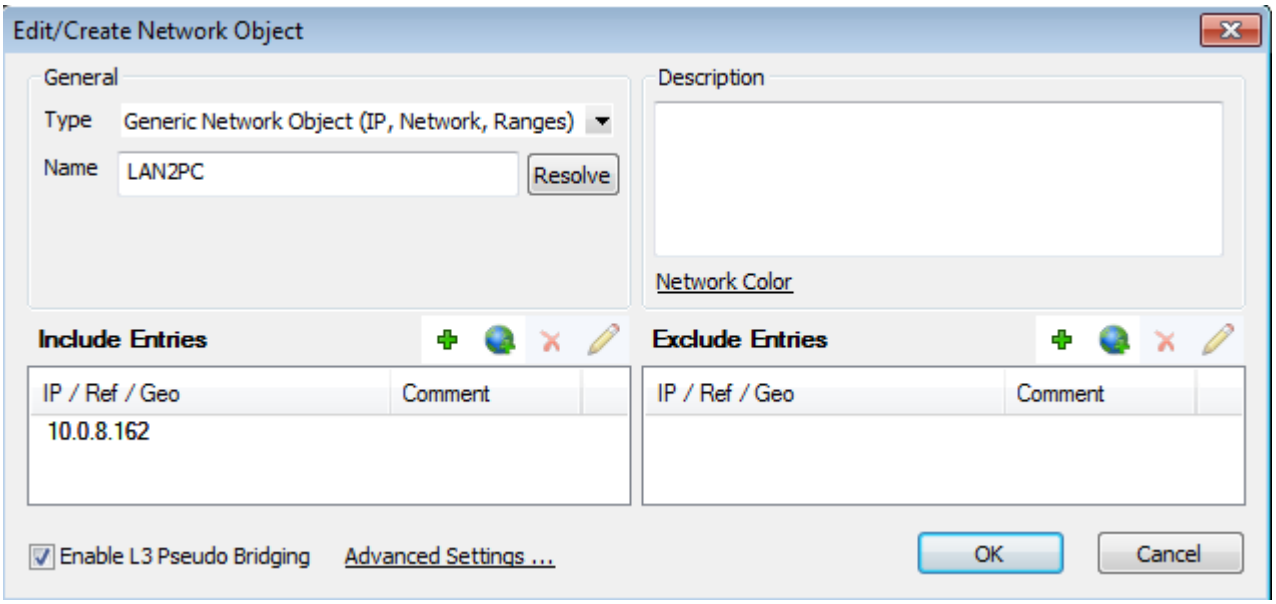
Before you Begin

Assign an IP addresses to each network interface of the Barracuda NextGen Firewall F-Series that you want to use for the bridge. (**CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Server Properties**).

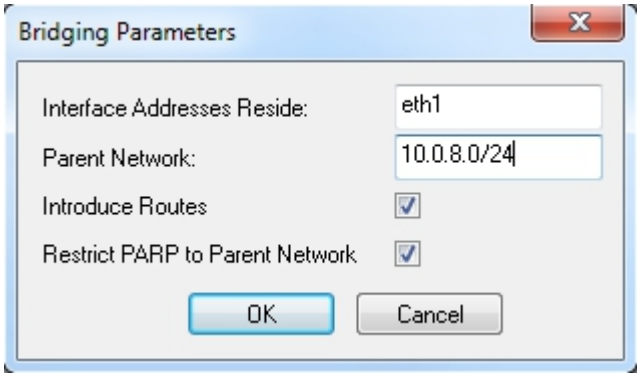
Step 1. Create a Network Object for the client PC

Create a network object for the clients that should be bridged:

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **Forwarding Rules**.
2. Click **Lock**.
3. Create a network object for the clients that must be bridged.
4. In the **IP/Ref** table, add the IP address of the client:



5. In the **Bridging Parameters** window, edit the following settings:
   - **Interface Addresses Reside** - Enter the network interface that points to the bridged clients. For example, enter *eth1*.
   - **Parent Network** - Enter the parent network address. E.g., `10.0.8.0/24`
   - Select the **Introduce Routes** and **Restrict PARP to Parent Network** check boxes.



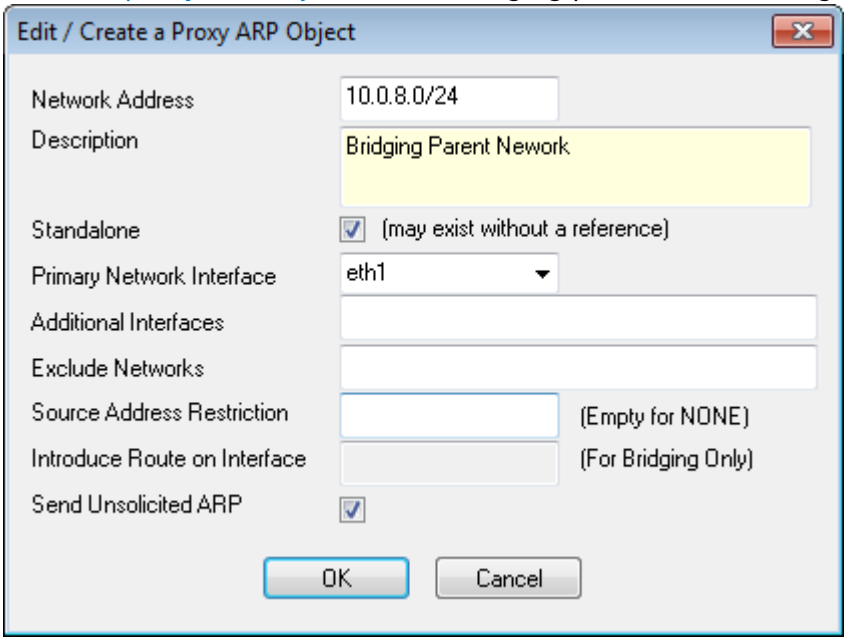
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

You now have a network object for the client that you can use when creating the layer 3 bridge.

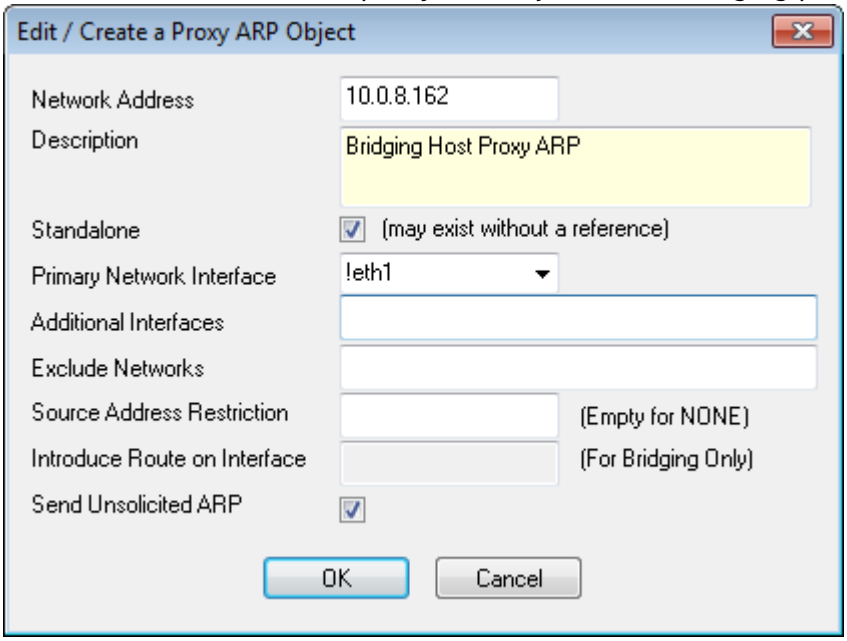
Step 2. Create Proxy ARP Objects

To make sure that ARP requests are answered on the interface for the new network, create a proxy ARP object for the bridging parent network and bridged clients.

1. Go to **CONFIGURATION > Configuration Tree > Box >Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a proxy ARP object for the bridging parent network. E.g., `10.0.8.0/24`



4. Create a proxy ARP object for the bridged client. E.g., `10.0.8.162.` (optional) Restrict the source IP addresses of the proxy ARP object to the bridging parent network.



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

Step 3. Create Access Rules for Layer 3 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** – Select the check box.
   - **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`
   - **Connection Method** – Select **No SNAT**.
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`
   - **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 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 access rules so the new rules can match incoming traffic.
6. Click **Send Changes** and **Activate**.

You can now use the separated PC as if it were on the same network with the exception that the MAC address of the PC will be replaced by the MAC of the Barracuda NextGen Firewall F-Series when traversing the bridge.

Figures

1. fw_layer3_bridge.png
2. FW_Layer3Bridge_01.png
3. parp.png
4. FW_Layer3Bridge_02.png
5. FW_Layer3Bridge_03.png