

This document provides information on how to configure a local bridge for use with your own workstation. The idea is to explore the Barracuda NG Firewall's advanced traffic inspection features by using traffic that your workstation generates on the LAN. For this you will need to connect your workstation across a local bridge on the Barracuda NG Firewall to the LAN.

The set of instructions will show how to configure a local bridge on port2 and port3 of the Barracuda NG Firewall. There are a few steps that are needed before the bridge configuration can be completed.

## Preconditions

### Firewall

For the default configuration it is assumed that port1 is going to be the management port. This means that the default management IP 192.168.200.200 will remain configured to this interface.

### WiFi

The Country must be selected. If this is not completed then no IP configurations will be possible when applicable. This only applies to WiFi capable models F101/F201/F301.

### DHCP Server

The DHCP Server and DHCP client should be disabled. These are disabled by default unless changes have been made previously.

## Required Information

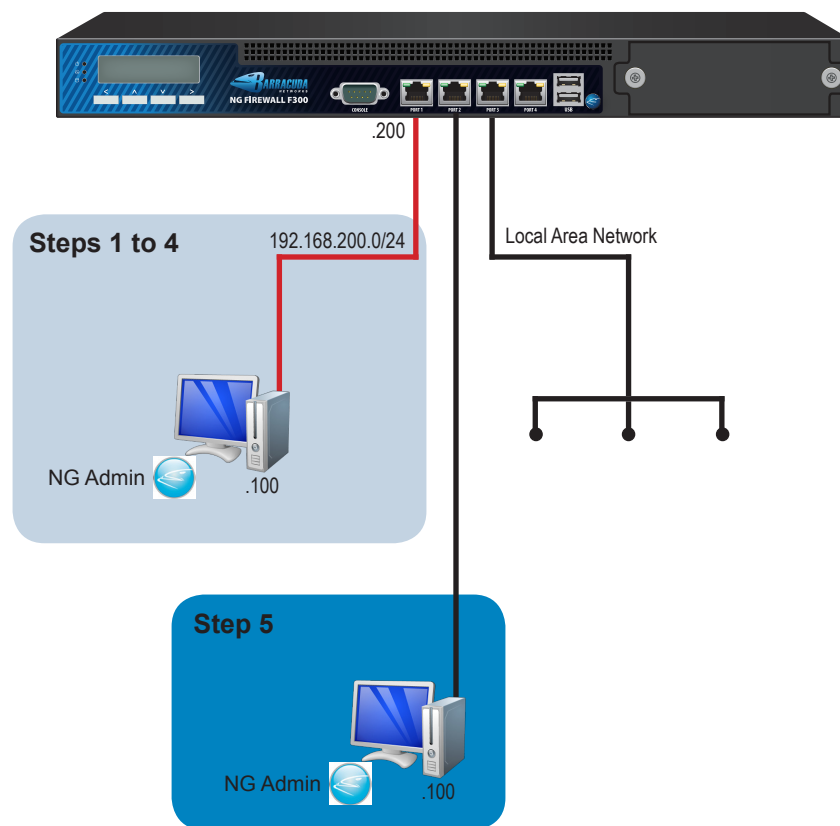
You will need the IP address that will be assigned to the bridge and the default route of the bridged network. You can obtain the gateway of the LAN before you disconnect your computer from the LAN. On your computer navigate to **Control Panel > Network and Sharing > Change adaptor settings**. Then select your LAN adaptor click on the **IPv4 properties** to open. If you have a static IP address you will see all the information in this window including the default route and DNS information. If you have a DHCP address, nothing will appear in this window.

For users that have a DHCP address you will need to access the MS Windows command line. To access the Windows command line click the Windows start button on the task bar. Now in the run/search bar type **cmd** to open the MS Windows command line window. Now type the command **ipconfig/all**. This will print all of the computers network configurations on the screen. Scroll to the top and search for the information pertaining to the **Ethernet Adaptor Local Area Connection**. This will provide you with the required information.

## Extra Information

You will be creating a bridge between port2 and port3. The initial configurations will be completed with your workstation connected to port1. This document will assume that the Quick Start Guide has been followed and the wireless country code is already set.

## Network Deployment

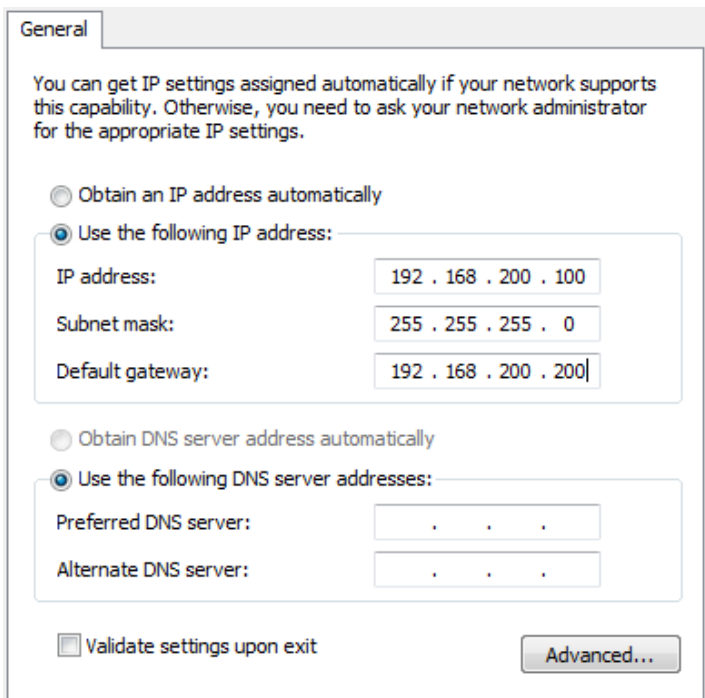


## 1. Connect

You will need to directly connect your firewall to port1 of your Barracuda NG Firewall. For this we will use a crossover cable. A red crossover cable is provided with the Barracuda NG Firewall. Connect port3 to the LAN you are going to bridge your workstation too. You will need a straight through cable to connect the firewall to the local LAN. A white straight through cable is provided with the Barracuda NG Firewall.

Now you will need to set your computers IP address manually.

- You can set your IP address by navigating to **Control Panel > Network and Sharing Center > Change adapter settings**.
- Double click your LAN adapter and select **Properties**.
- Double click on **Internet Protocol Version 4 (TCP/IPv4)** to open the window.
- Select **Use the following IP address** and enter an IP address. In our example we will use **192.168.200.100** but you can use any IP address on the **192.168.200.0/24** network other than **192.168.200.200** as this is the management IP address of the firewall.



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 200 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 200 . 200

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Validate settings upon exit

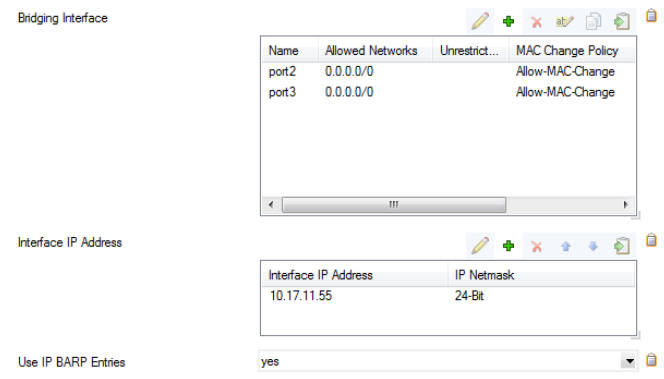
Advanced...

Now you can connect to the Barracuda NG Firewall with the NG Admin application using the default settings.

Management IP Address	Login	Password
192.168.200.200	root	ngf1r3wall

## 2. Bridging Configuration

- Open the Barracuda NG Admin application and connect to your Barracuda NG Firewall unit.
- Navigate to the **Config** tab and select **Full Config**.
- Open the **Network** configuration node and select **WiFi** in the left pane.
- Check that the appropriate **Location** is set. (Applies to WiFi enabled units F101/F201/F301). If you had to set the country code, click **Send Changes** followed by **Activate**.
- Next click **Config Tree**, select **Virtual Servers > S1 > Assigned Services > NGFW (Firewall) > Forwarding Settings**.
- Select **Layer 2 Bridging** in the left navigation pane. Click the **Lock** button on the navigation bar to enable changes to be made here.
- Click **+** to add a **Bridging Group** and name it appropriately. E.g: **br1**
- At this point you are now working within the **Bridging Group** window and you can enter the **Bridging Interfaces**.
- Click **+** to add the first bridged interface. **Naming is critical here! You MUST name the bridged interfaces to match the physical interface.**
- The first **Bridging Interface** will be named **port2**.
- The **Bridging Interface: port2** window is now open.
- Add **0.0.0.0/0** to the **Allowed Networks** table and click **OK**.
- Now add a second **Bridging Interface** named **port3**, add **0.0.0.0/0** to the **Allowed Networks** table and click **OK**.
- You are now back in the **Bridging Group: br1** window and need to assign an IP address to this bridging group.
- Click **+** and add **10.17.11.55** (or an IP relative to your network) to the **Interface IP Address** and click **OK**.
- To finish the Layer 2 Bridging configuration, click **Send Changes** followed by **Activate**.



Bridging Interface

Name	Allowed Networks	Unrestrict...	MAC Change Policy
port2	0.0.0.0/0		Allow-MAC-Change
port3	0.0.0.0/0		Allow-MAC-Change


Interface IP Address

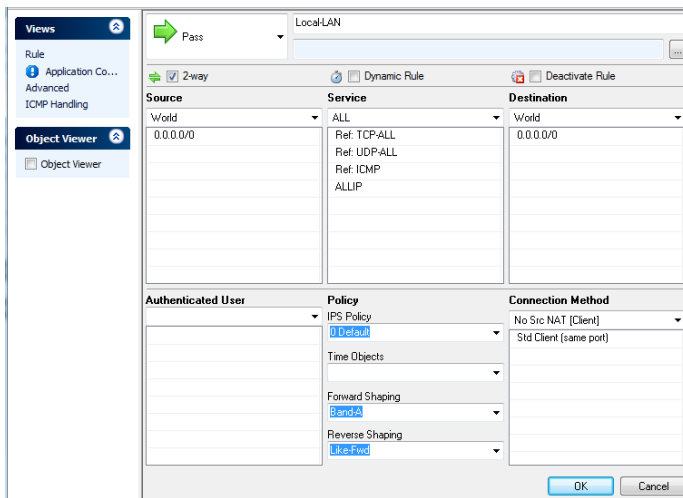
Interface IP Address	IP Netmask
10.17.11.55	24-Bit

Use IP BARP Entries: yes

## 3. Forwarding Firewall Configuration


You can now configure the forwarding rule necessary to allow traffic across the bridge and utilize the advanced traffic inspection features of the Barracuda NG Firewall.

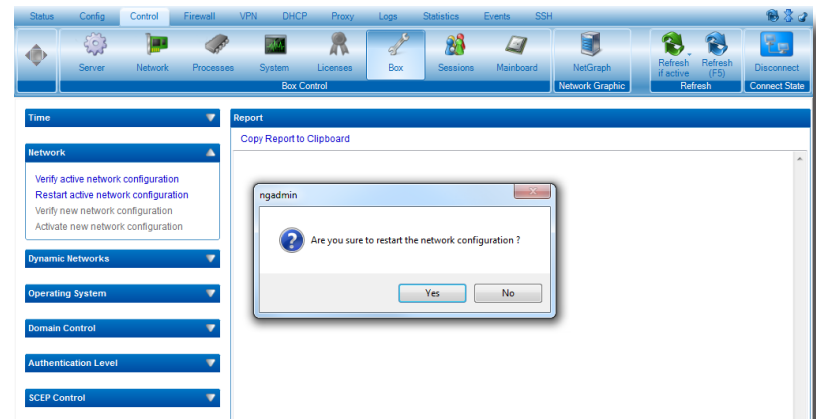
- Click on the **Config Tree** button on the navigation bar to bring you back to the config tree view.
- You will notice that the **Config Tree** is still open and **Forwarding Settings** is still highlighted.
- Click on **Forwarding Rules** just above Forwarding Settings.
- Click the **Lock** button on the navigation bar to enable changes to be made here.
- Right click in the rule window and select **New...** to create a new firewall rule.
- Provide an appropriate name for this firewall rule and Select  **Pass** as action.
- Enter a check mark in the **2-way** selection.
- **Source** is **World 0.0.0.0/0**.
- **Service** is **ALL**.
- **Destination** is **World 0.0.0.0/0**.
- **Connection Method** is **No Src NAT [Client]**.
- Click **Application Control** in the left navigation pane.
- Select the following options: **Generic Patterns: NONE, Port Protocol Protection Policy: Use Matching Service Settings, Application Detection: Detect Only, Application Selection: Explicitly Select Protocols**.
- In the **Explicit Application Selection** window, right click and choose **Select All**.
- Click **OK** to finish the firewall rule configuration.
- Click **Send Changes** followed by **Activate**.



## 4. Network Activation

In order for certain changes to take effect you will need to complete the following step.

- Navigate to: **Control >  Box > Network**.
- Click **Restart active network configuration**.
- You will be disconnected from the firewall. At this point you can connect your workstation to port2 and set your workstations IP appropriately to match your LAN using either DHCP or a statically assigned IP address of your choosing. Once this is complete you can reconnect to the firewall management IP **192.168.200.200**.



You have completed the configurations necessary explore the NG Firewall's advanced traffic inspection features by using traffic that your workstation generates on the LAN. At this point you will be able to generate traffic using your workstation.

## 5. Viewing Generated Traffic

To view the traffic that your workstation is generating you simply need to click on "Logs" on the navigation bar. Click on the drop down window and select **S1 > NGFW > NGFW**. This is a static view. To see the "Live" view simply click on **Live Update** on the top right side of the navigation bar. This view will provide you with the request, action, and the rule associated with the action as well as the source and destination addresses. It will also provide you with the protocol and port numbers.