

## How to Set Up a High Availability Cluster

<https://campus.barracuda.com/doc/41115836/>

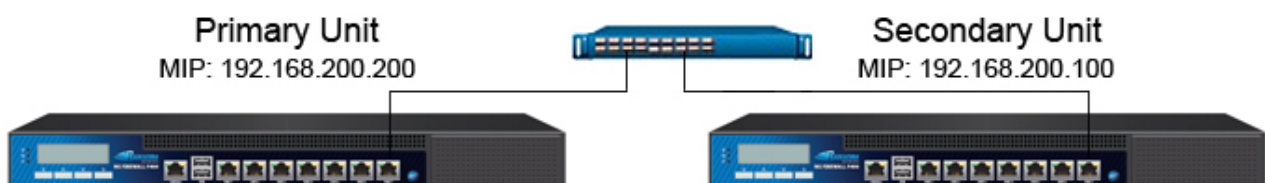
Both of the systems that you set up in a high availability (HA) cluster must be the same model and firmware version. For instructions on how to configure an HA cluster using different revisions of the same appliance model, see [How to Restore a Configuration on Appliances After an RMA](#).

A high availability (HA) cluster can transparently failover to the secondary unit if your primary unit goes down unexpectedly or requires maintenance. You can set up an HA cluster on a Barracuda NG Control Center or a standalone HA cluster. A standalone HA cluster includes two standalone Barracuda NG Firewalls or two Barracuda NG Control Centers.

To protect against failure of network components, you can use a dedicated private link as a secondary HA connection.

### In this article:

## Standalone Barracuda NG Firewall HA Cluster



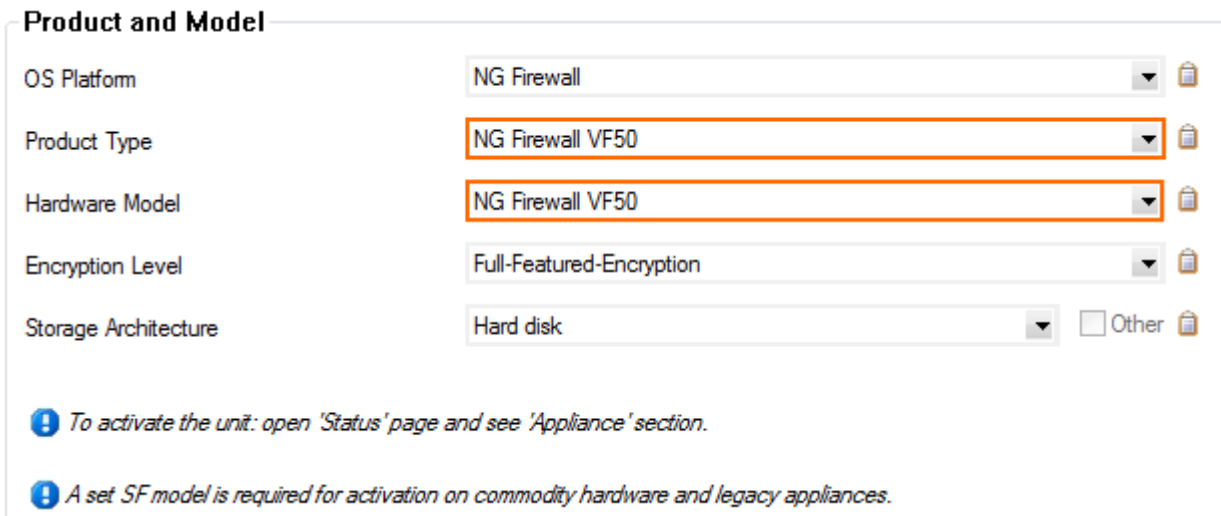
### Before you Begin

- Connect the primary unit and secondary unit to a network switch.
- Verify the **Product Type** in the **Box Properties** and **Server Properties** match your appliance.
- Verify that the **Product Name** of the primary NG Firewall is different from the **Product Name** of the secondary NG Firewall.

### Step 1. (Virtual NG Firewalls only) Verify the Product Type

Set the product type matching your license if you are using a virtual Barracuda NG Firewall. This is not necessary on hardware appliances.

1. Open the **Box Properties** page (**Configuration > Full Configuration > Box**).
2. Click **Lock**.
3. Select the Barracuda NG Firewall Model from the **Product Type** list. E.g., **NG Firewall VF50**
4. Select the Barracuda NG Firewall Model from the **Hardware Type** list.



**Product and Model**

OS Platform	NG Firewall	
Product Type	NG Firewall VF50	
Hardware Model	NG Firewall VF50	
Encryption Level	Full-Featured-Encryption	
Storage Architecture	Hard disk	<input type="checkbox"/> Other

**!** To activate the unit: open 'Status' page and see 'Appliance' section.

**!** A set SF model is required for activation on commodity hardware and legacy appliances.

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

### Step 2. Create the DHA Unit

On the primary unit, create DHA configuration for the secondary unit.

1. Open the **Configuration > Full Configuration** page.
2. Right-click **Box** and select **Create DHA box**. At the bottom of the **Config Tree**, the **HA Box** configuration node is added.
3. Open the **HA Network** page (**Configuration > Full Configuration > Box > HA Box**).
4. Enter the **Management IP (MIP)** for the secondary unit.
5. Click **Send Changes** and **Activate**.

### Step 3. Create the PAR File for the Secondary Unit

On the primary unit, export the PAR file for the secondary unit.

1. On the primary unit, create the PAR file:
2. Go to the **Config>Full Config** page.
3. From the **Config Tree**, right-click **Box** and select **Create PAR file for HA box**.
4. Save the PAR file to your local hard disk drive.

#### Step 4. Import the PAR File on the Secondary Unit

On the secondary unit, import the boxha.par PAR file created on the primary unit:

1. Open the **Configuration > Full Configuration** page.
2. From the **Config Tree**, right-click **Box** and select **Restore from PAR file**.
3. Click **OK**.
4. Select the boxha.par file created in Step3 and click **OK**.
5. Click **Activate**.

#### Step 5. Activate the New Network Configuration for the Secondary Unit

On the secondary unit, activate the network configuration.

1. Go to the **Control > Box** page.
2. In the left navigation pane, expand **Network** and click **Activate new network configuration**.
3. Select **Failsafe** as the activation mode.
4. In the left menu, expand **Operating System** and click **Reboot**.

#### Step 6. Select the Active and Backup Unit on the Primary Unit

In the virtual server settings of the primary unit, select where the virtual server should be running.

1. Open the **Server Properties** page (**Configuration > Full Configuration > Box > Virtual Server > your virtual server**).
2. Click **Lock**.
3. Verify that the **Product Type** matches your license.
4. To run the virtual server on the primary unit per default:
  1. **Active Box** – Select **This-Box**.
  2. **Backup Box** – Select **Other-Box**.
5. To run the virtual server on the secondary unit per default:
  - From the **Active Box** list, select **HA-Box**.
  - From the **Backup Box** list, select **Other-Box** or **No-Backup** if you do not want this virtual server to be part of the high availability cluster.

Consider the limitations described in [Best Practice - Service Dependencies and Multiple Services of the Same Type on one Virtual Server](#) before using multiple virtual servers on one NG Firewall.
6. Click **Send Changes** and **Activate**.

#### Step 7. Install Licenses

You must install licenses on both units. For instructions, see [How to Activate and License a Barracuda NG High Availability Cluster](#).

## Set Up an HA Cluster in the Barracuda NG Control Center

### Before you Begin

Select two Barracuda NG Firewalls in the same cluster.

### Set up an HA Cluster

1. Log into the Barracuda NG Control Center.
2. Open the **Config** page.
3. From the **Config Tree**, expand **Multi-Range** and navigate to the cluster that contains your HA units.
4. Create a virtual server.
5. Open the **Server Properties** page.
6. In the **Virtual Server Definition** section, define the primary unit and secondary unit.
  - **Primary Box** - The active system.
  - **Secondary Box** - The HA partner.
7. Click **Send Changes** and **Activate**.

The primary and secondary servers are created and configured as HA partners on both units.

### Figure 3. Virtual Server Settings for an HA Cluster on the Barracuda NG Control Center

Virtual Server Definition	
Server Name	<input type="text" value="borderS1"/>
Description	<input type="text"/>
Product Type	<input type="text" value="netfence-standard"/>
Encryption Level	<input type="text" value="Full-Featured-Encryption"/>
Unique Server ID	<input type="text" value="5bc5bcc8-c279-4d8c-1b12-36e9ab3ab4a0"/>
Primary Box	<input type="text" value="HQ-Perimeter-HA1"/>
Secondary Box	<input type="text" value="HQ-Perimeter-HA2"/>

### Configure a Private Uplink

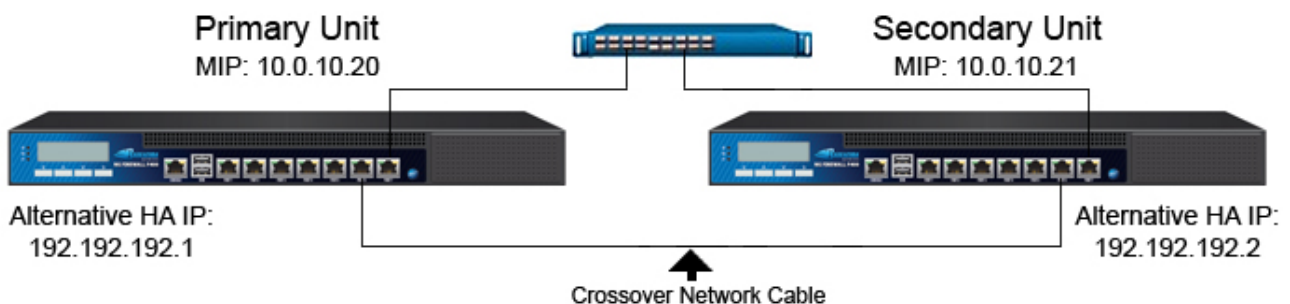
After setting up an HA cluster, you can also configure a private uplink for it. For the private uplink, you must configure a 2-bit network as a subnet and provide exclusive network devices for the private

uplink.

To configure a private uplink, complete the following steps on the primary unit:

These steps use the example IP addresses from the following figure:

**Figure 4. HA Cluster with Private Uplink**



### Before You Begin

To avoid any errors when you configure the private uplink, connect the primary unit and secondary unit with a crossover cable.

### Step 1. Define Alternative HA IP Addresses

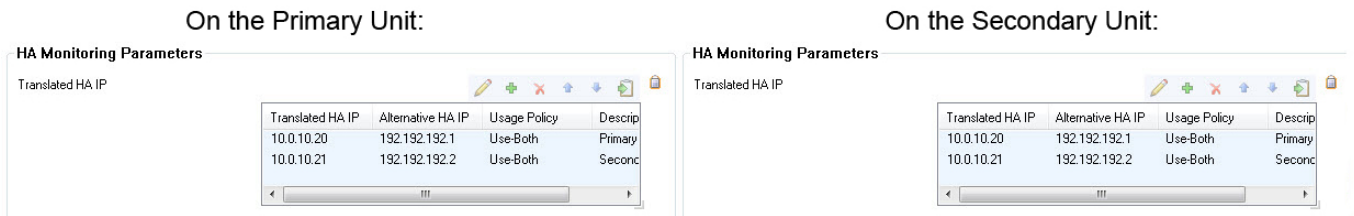
1. Open the **Network** page (**Config > Full Config > Box > Network**).
2. Click **Lock**.
3. From the **Configuration Mode** menu in the left navigation pane, click **Switch to Advanced View**.
4. In the **Additional Local IPs** section, add the IP address for the unit in the additional subnet. For example, *192.192.192.1*.
5. From the **Responds to Ping** and **Management IP** lists, select yes.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

### Step 2. Activate the Private Uplink

1. Open the **Control** page (**Config > Full Config > Box > Infrastructure Services**).
2. Click **Lock**.
3. In the **HA Monitoring Parameters** section, add entries for the primary unit and secondary unit. In each entry, specify these settings:
  - **Translated HA IP** – Enter the original management IP address (for example: 10.0.10.20).
  - **Alternative HA IP**– Enter the additional local network IP of the unit (for example: 192.192.192.1).

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

**Figure 5. HA Monitoring Settings on Both HA Units**



**Step 3. Add the Alternative HA IP to the ACL List**

To grant administrative access rights for alternative HA IP address usage, add the alternative HA IP address to the ACL list:

1. Open the **Administrative Settings** page (**Config > Full Config > Box > Administrative Settings**).
2. Click **Lock**.
3. In the **Access Control List** section, add the alternative HA IP address.
4. Click **Send Changes** and **Activate**.

**Check Virtual Server HA Status**

Check the server status on both HA units to verify that the virtual servers have been correctly assigned.

1. On the primary unit:
  - o Go to the **Control > Server** page.
  - o In the **Server Status** table, verify that the virtual server is correctly assigned. The **Status** column must display *primary*. The **Status HA Partner** column must display *standby*.
2. On the secondary unit:
  - o Go to the **Control > Server** page.
  - o In the **Server Status** table, verify that the virtual server is correctly assigned. The **Status** column must display *standby*. The **Status HA Partner** column must display *primary*.

When the primary unit goes down, the secondary unit changes its status to *primary* and replaces the primary unit with all its functionalities. Depending on whether your primary unit is running or down, the **Control > Server** page displays as follows:

Primary Unit State	Secondary Unit State
--------------------	----------------------

Server	Status	Status HA Partner	IP Addresses
VIRTCTRL	primary	standby	10.0.15.3,10.20.0.80,172.16.1.254,19...
Status	primary		
HA	primary	standby	
IP			
1			10.0.15.3
2			10.20.0.80
3			172.16.1.254
4			194.93.0.80
5			62.99.0.80

Block Server Start Server Stop Server Restart Server

**N/A - Primary unit down**

Server	Status	Status HA Partner	IP Addresses
VIRTCTRL	standby	primary	10.0.15.3(!),10.20.0.80(!),172.16.1.25...
Status	standby		
HA	standby	primary	
IP			
1			10.0.15.3(!)
2			10.20.0.80(!)
3			172.16.1.254(!)
4			194.93.0.80(!)
5			62.99.0.80(!)

Block Server Start Server Stop Server Restart Server

Server	Status	Status HA Partner	IP Addresses
VIRTCTRL	secondary	down	10.0.15.3,10.20.0.80,172.16.1.254,19...
Status	secondary		
HA	secondary	down	
IP			
1			10.0.15.3
2			10.20.0.80
3			172.16.1.254
4			194.93.0.80
5			62.99.0.80

Block Server Start Server Stop Server Restart Server

## Figures

1. HA-setup.png
2. HA\_set\_product\_type.png
3. cc\_adm1.jpg
4. HA-private\_uplink.png
5. ha\_monitor.jpg
6. HA\_state\_up\_primary.png
7. HA\_state\_up\_secondary.png
8. HA\_state\_down\_secondary.png

© Barracuda Networks Inc., 2019 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.