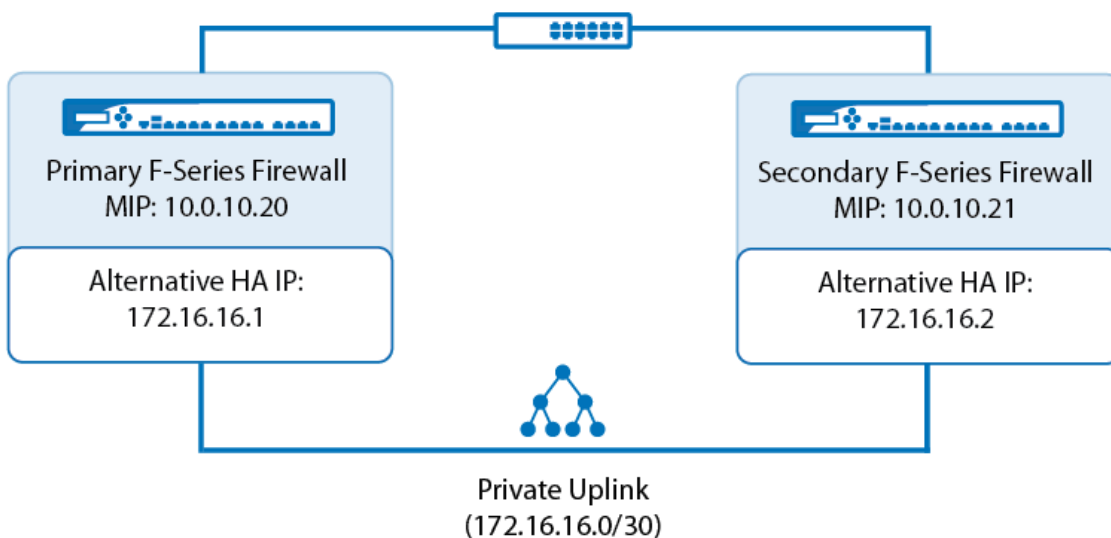


How to Configure a Private Uplink for a HA Cluster

<https://campus.barracuda.com/doc/48202854/>

After setting up an HA cluster, you can also configure a private uplink to safeguard against failure of the switch connecting the two HA firewalls. For the private uplink, you must configure a 2-bit network as a subnet and configure the NextGen Firewall F-Series to use this connection to send the HA sync packets.



Before you begin

- Barracuda Networks recommends directly connecting both firewalls with a crossover cable for the private uplink.
- A /30 network. E.g., 172.16.16.0/30

Step 1. Define the alternative HA IP address for the primary firewall

1. Log into the primary NextGen Firewall F-Series.
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. Click **Lock**.
4. In the left menu, expand the **Configuration Mode** section and click **Switch to Advanced View**.
5. Click **+** to add the private IP address as an **Additional Local IP**. The **IP Address Configuration** window opens.
 - **Interface Name** - Select the interface the crossover cable is connected to.
 - **IP Address** - Enter the Alternative HA IP address for the firewall. E.g., 172.16.16.1

- **Associated Netmask** – Select **/30**.
- **Responds to Ping** – Set to **yes**.
- **Management IP** – Set to **yes**.

IP Address Configuration

Interface Name	eth3	<input type="checkbox"/> Other
IP Address	172.16.16.1	
Associated Netmask	30-Bit	
Responds to Ping	yes	
Management IP	yes	

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

Step 2. Define the alternative HA IP address for the secondary firewall

1. Log into the primary NextGen Firewall F-Series.
2. Go to **CONFIGURATION > Configuration Tree > Box > HA Box > HA Network**.
3. Click **Lock**.
4. Click **+** to add the private IP as an **Additional Local IP**.
5. Enter a **Name** and click **OK**. The **IP Address Configuration** window opens.
 - **Interface Name** – Select the interface the crossover cable is connected to.
 - **IP Address** – Enter the Alternative HA IP address for the firewall. E.g., 172.16.16.2 for the secondary firewall.
 - **Associated Netmask** – Select **/30**.
 - **Responds to Ping** – Set to **yes**.
 - **Management IP** – Set to **yes**.

IP Address Configuration

Interface Name	eth3	<input type="checkbox"/> Other
IP Address	172.16.16.2	
Associated Netmask	30-Bit	
Responds to Ping	yes	
Management IP	yes	

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

Step 3. Activate the private uplink








For the HA sync to work over the private link, you must associate the private link IPs with the corresponding management IP addresses.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Control**.
2. Click **Lock**.
3. In the **HA Monitoring Parameters** section, add entries for the primary firewall and secondary firewall:
 - **Translated HA IP** - Enter the management IP address E.g., 10.0.10.20 for the primary firewall
 - **Alternative HA IP** - Enter the additional local network IP of the firewall. E.g., 172.16.16.1 for the primary firewall
 - **Usage Policy** - Select **Use Both** to send the HA sync and heartbeat over both the management IP link and the private uplink. Alternatively, select **Use Alternative only** to only use the private uplink.


Translated HA IP	<input type="text" value="10.0.10.20"/>	
Alternative HA IP	<input type="text" value="172.16.16.1"/>	
Usage Policy	<input type="text" value="Use-Both"/>	
Description	<input type="text" value="Primary NG"/>	
Translated HA IP	<input type="text" value="10.0.10.21"/>	
Alternative HA IP	<input type="text" value="172.16.16.2"/>	
Usage Policy	<input type="text" value="Use-Both"/>	
Description	<input type="text" value="Secondary NG"/>	

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

HA Monitoring Parameters

Translated HA IP ✔       

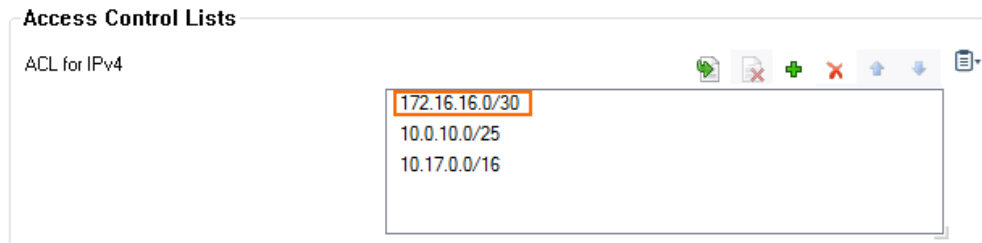
Translated HA IP	Alternative HA IP	Usage Policy	Description
10.0.10.20	172.16.16.1	Use-Both	Primary
10.0.10.21	172.16.16.2	Use-Both	Secondary

 Use this to establish HA heartbeat communication across an additional uplink.

Step 4. Add the alternative HA IP address 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. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. Click **Lock**.
3. In the **Access Control List** section, add the /30 network containing the alternative HA IP addresses.

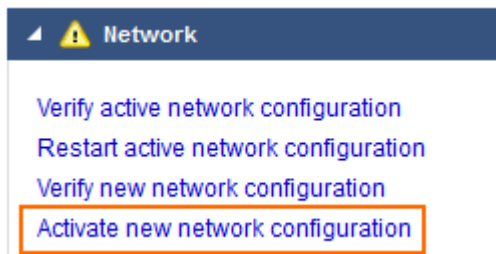


4. Click **Send Changes** and **Activate**.

Step 5. Activate the network configuration on the primary and secondary NextGen Firewall F-Series

Activate the network configuration on the primary and secondary NextGen Firewall F-Series.

1. Go to **CONTROL > Box**.
2. In the menu, expand **Network** and click **Activate new network configuration**.



3. Select **Failsafe** as the activation mode.

Figures

1. HA-private_uplink.png
2. Private_Uplink_01.png
3. Private_Uplink_02.png
4. Private_Uplink_02.png
5. Private_Uplink_03.png
6. Private_Uplink_04.png
7. Private_Uplink_05.png
8. Standalone_HA_06.png

© Barracuda Networks Inc., 2021 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.