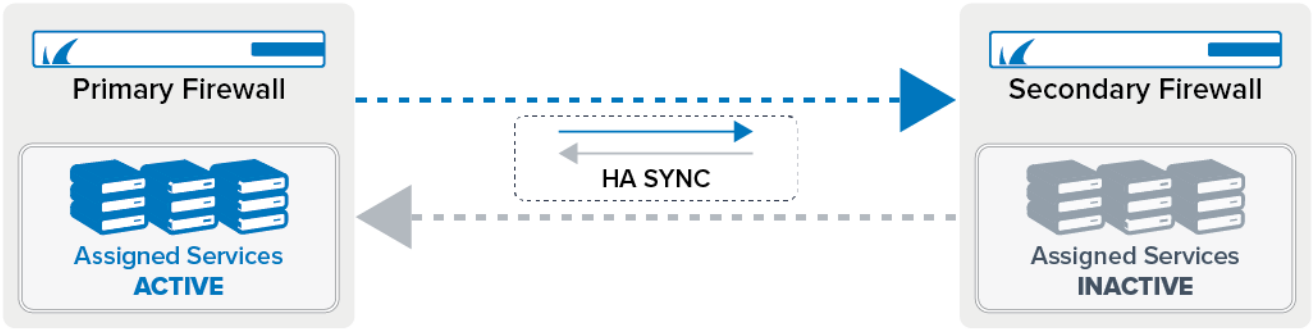
How to Set Up a High Availability Cluster

https://campus.barracuda.com/doc/96026367/

Both systems in a high availability (HA) cluster must be the same model and firmware version, but do not have to be the same hardware revision. For instructions on how to configure an HA cluster using different revisions of the same appliance model, see How to Restore the High Availability Cluster Configuration after an RMA.

The functionality of stand-alone and managed high availability clusters are the same. However, the configuration differs. For a stand-alone HA cluster, the primary firewall downloads the licenses for both firewalls, and when the secondary firewall is joined to the HA cluster, the license for the secondary firewall is transferred over. The licenses are bound to the MAC addresses of the primary and secondary firewall. The primary firewall is also the configuration master for all configurations, except for the Network page. All configurations and session information are synced from the primary firewall to the secondary firewall. To protect against failure of network components, you can use a dedicated private link as a secondary HA connection.

Stand-Alone HA Cluster



Before You Begin

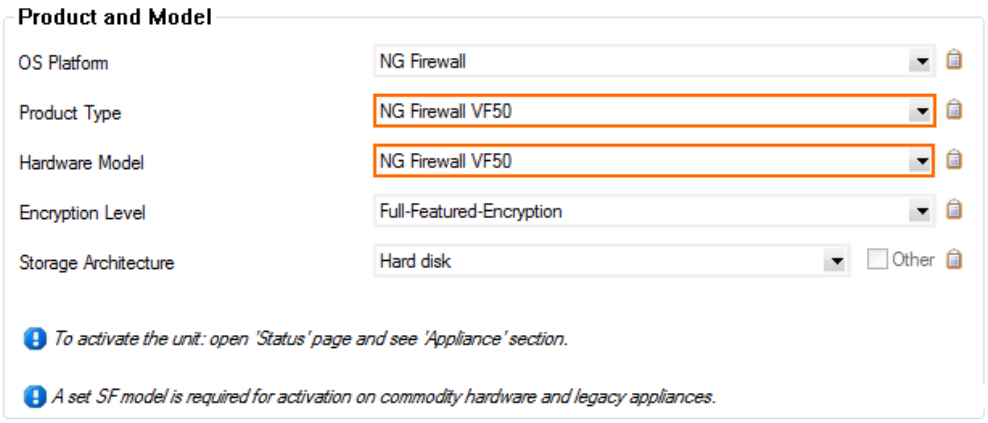
- Connect the primary firewall and secondary firewall to a network switch.

Step 1. (Virtual only) Verify the Product Type

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Box Properties**.
2. Click **Lock**.
3. Select the model from the **Product Type** list. E.g., **CloudGen Firewall VF50**

4. Select the model from the **Hardware Model** list.

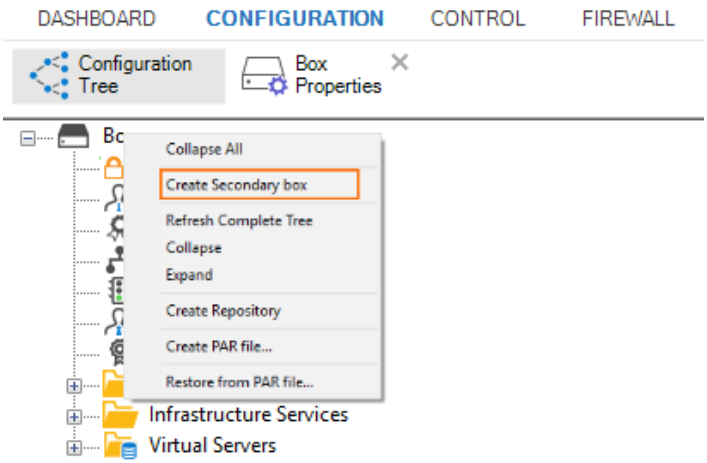


5. Click **Send Changes** and **Activate**.

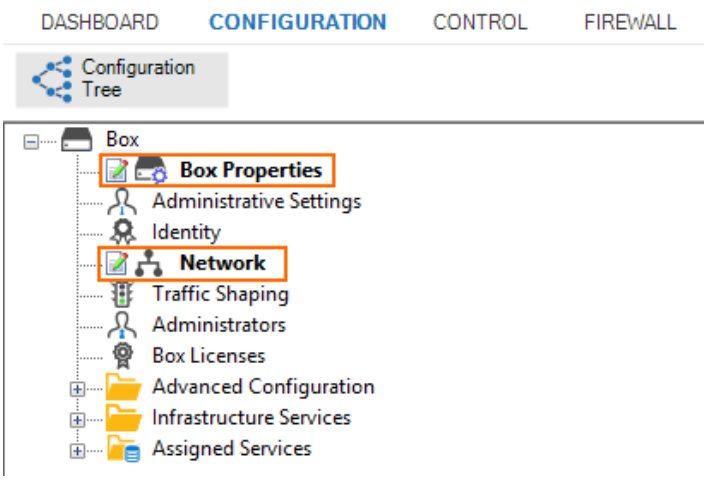
Step 2. Create the Secondary Firewall

On the primary firewall, create the configuration for the secondary HA firewall.

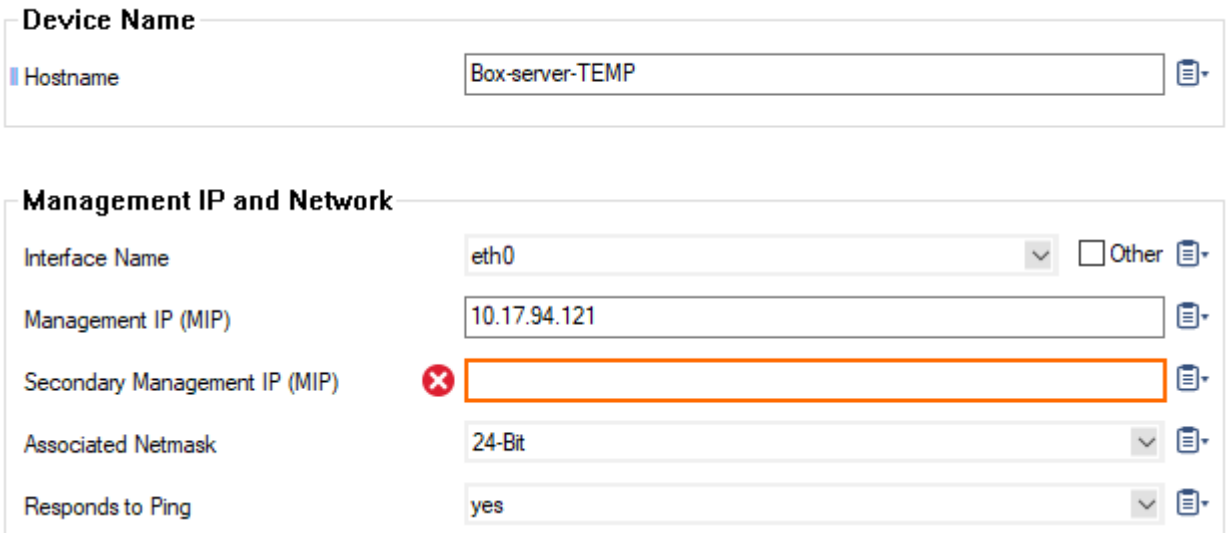
1. Go to **CONFIGURATION > Configuration Tree > Box**.
2. Right-click **Box** and select **Create Secondary box**.



3. The **Box Properties** and **Network** nodes are replaced by new a node, each suitable for an HA configuration.



4. Open the **Network** page.
5. Enter the **Management IP (MIP)** for the secondary firewall. The MIPs of the HA pair must be in the same subnet.



6. If you have configured networks using additional local IP addresses on the primary firewall,
   1. Expand the **Configuration Mode** menu and select **Switch to Advanced**.
   2. Scroll down to **Additional Local IPs** and edit each entry:
      - Enter an **IP Address** from the available network for the secondary firewall.
7. Click **Send Changes** and **Activate**.

Step 3. Create the PAR File for the Secondary Firewall

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

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

Step 4. Import the PAR File on the Secondary Firewall

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

1. Go to **CONFIGURATION > Configuration Tree > Box**.
2. From the **Config Tree**, right-click **Box** and select **Restore from PAR file**.
3. Click **OK**.
4. Select the **box_secondary.par** file created in Step 3 and click **OK**.
5. Click **Activate** .

Step 5. Activate the New Network Configuration for the Secondary Firewall

On the secondary firewall, activate the network configuration.

1. Go to **CONTROL > Box**.
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 Box**.

Step 6. Activate the New Network Configuration for the Primary Firewall

On the primary firewall, activate the network configuration.

1. Go to **CONTROL > Box**.
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 Box**.

Step 6. Install Licenses

You must install licenses on both firewalls. For instructions, see How to Activate and License a Standalone High Availability Cluster.

Next Steps

Configure a Private Uplink

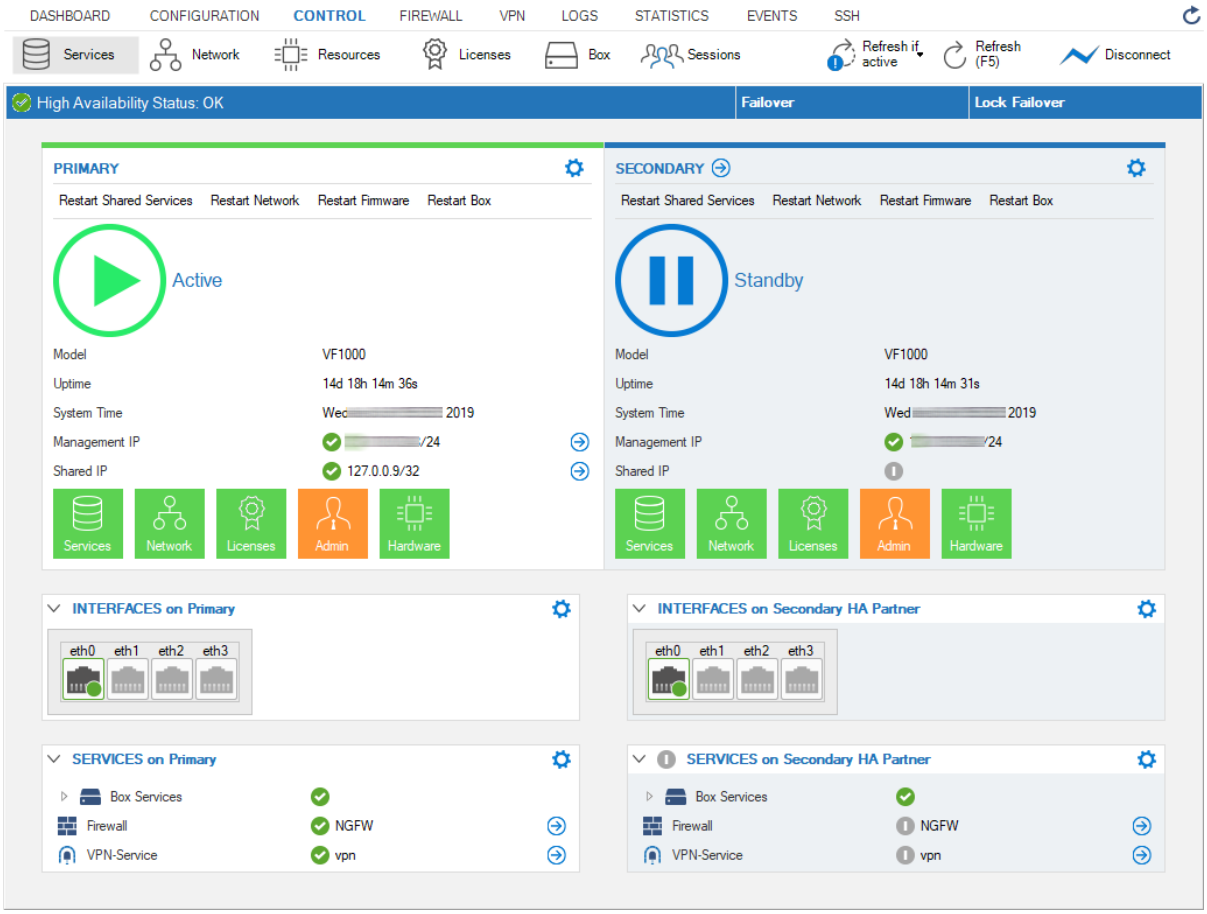
To avoid the switch connecting the primary and secondary firewall from becoming the single point of failure for the HA cluster, configure a private uplink for HA sync. Connect both firewalls with a crossover cable. Each firewall receives an additional management IP address in the /30 subnet used for the private uplink. The HA sync can use the private uplink as an alternative to the normal connection between the management IPs, or it can use both links simultaneously.

For more information, see How to Configure a Private Uplink for a High Availability Cluster.

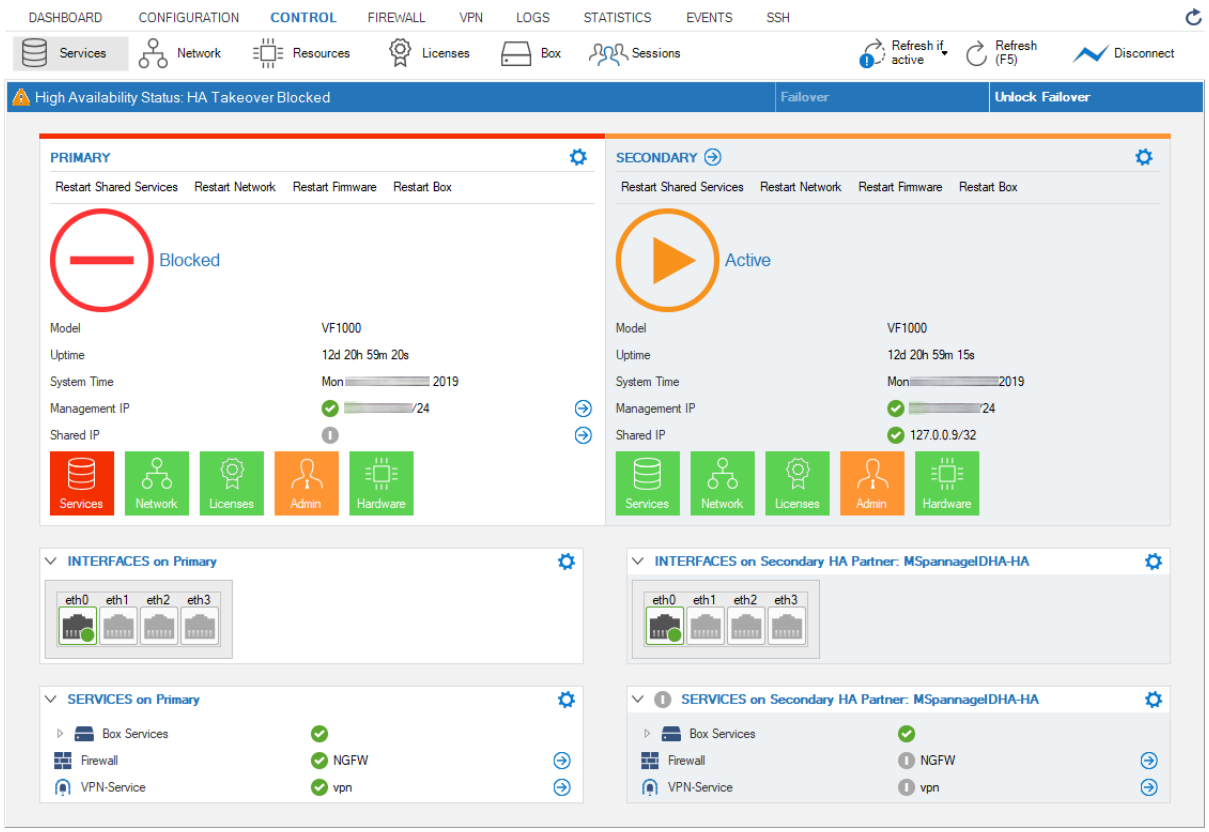
Check the Service HA Status

Check the services' status on both HA firewalls to verify that they have been correctly assigned.

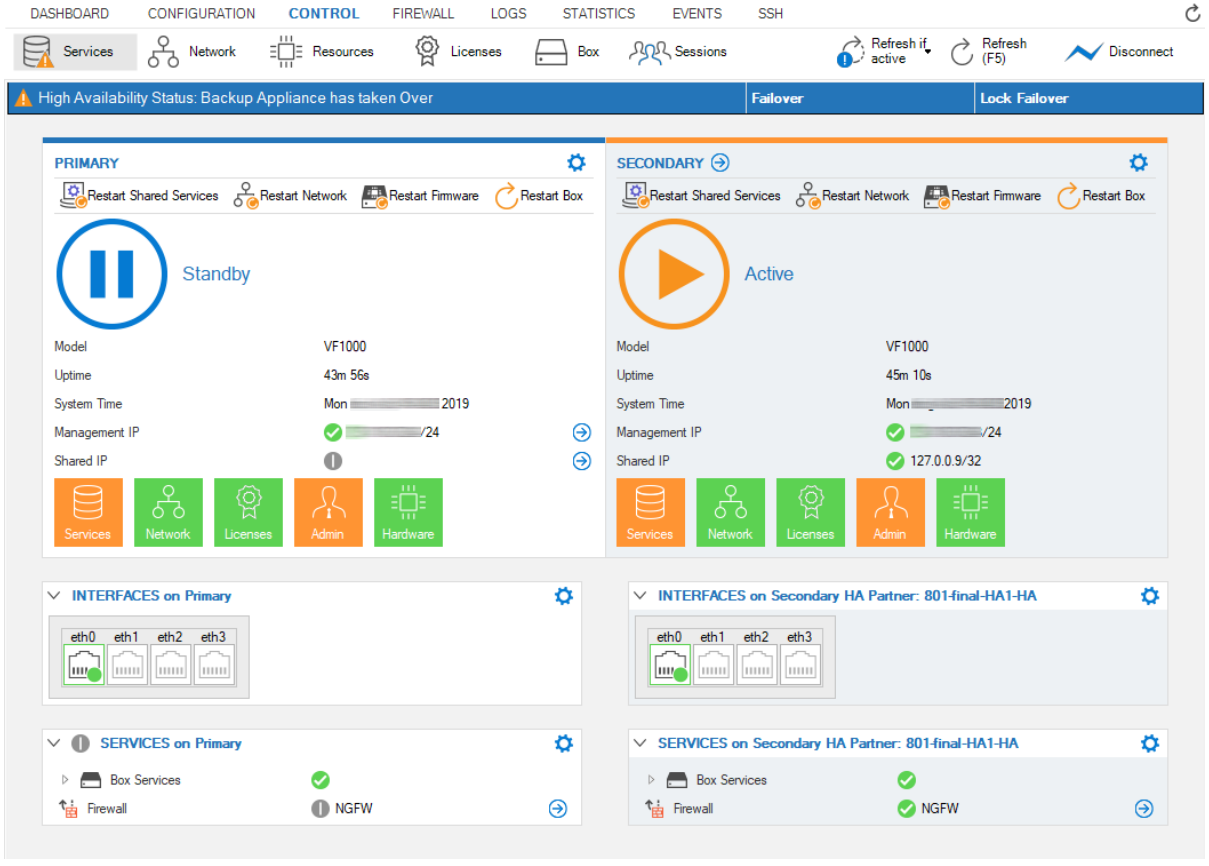
1. Go to **CONTROL > Services**.



When the primary firewall goes down, the secondary firewall changes its status to Primary and replaces the primary firewall with all its functionalities. Immediately after the failover, the services on the primary are blocked:



When clicking **Unlock Failover**, the services on the primary will be put into standby mode:



Figures

1. ha_sync_80.png
2. HA_set_product_type.png
3. HA_create_secondary_box.png
4. HA_nodes_for_secondary_created.png
5. HA_enter_management_IP_for_secondary.png
6. HA_in_default_state.png
7. HA_failover_to_secondary.png
8. HA_secondary_is_active.png