

How to Restore the Configuration on a HA Cluster after an RMA

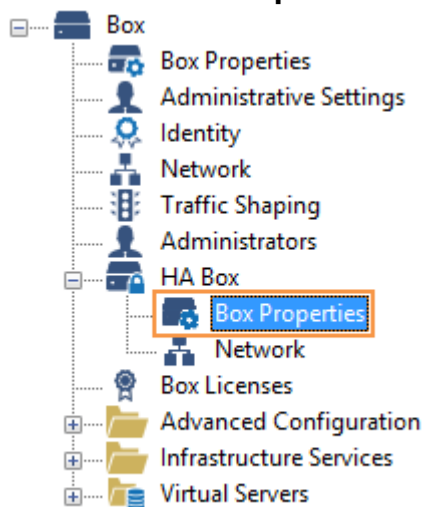
<https://campus.barracuda.com/doc/48202910/> If a NextGen Firewall residing in an HA cluster gets replaced with a newer revision model of the same product type (e.g., from F400 Rev. A to F400 Rev. B), you must create a configuration backup (PAR file) on the running HA partner and restore the configuration on the new appliance. This typically occurs in RMA cases, or if your appliance is replaced by Barracuda Networks' hardware refresh program.

Replacing the secondary HA firewall

If the primary NextGen F-Series Firewall is running, and the secondary firewall was replaced by a new model, restore the configuration from the primary one.

Step 1. Select the hardware model

1. Log into the primary NextGen F-Series Firewall.
2. Go to **CONFIGURATION > Configuration Tree > HA Box**.
3. Double-click **Box Properties**.



4. Click **Lock**.
5. In the **Product and Model** section, choose the correct **Hardware Model** for the replaced firewall (secondary), and edit the remaining entries according to the appliance model.
6. Click **Send Changes** and **Activate**.

Step 2. Configure the secondary firewall

1. Log into the primary NextGen F-Series Firewall.
2. Go to **CONFIGURATION > Configuration Tree > HA Box**.
3. Double-click **HA Network**.
4. Click **Lock**.
5. In the **Management IP and Network** section, set the **Management IP** of the new HA partner

(secondary).

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

Step 3. Create a PAR file

1. Log into the primary NextGen F-Series Firewall.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **Box** and select **Create PAR file for HA box** .

Step 4. Restore the secondary firewall

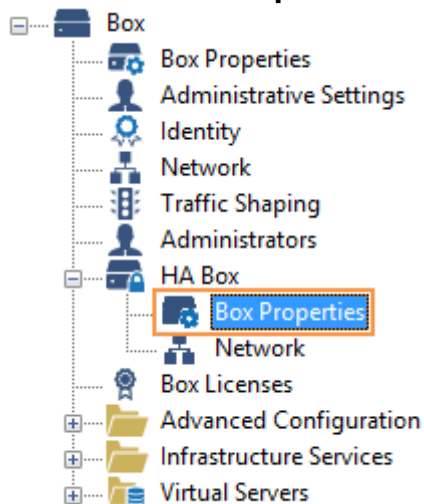
1. Log into the secondary NextGen F-Series Firewall.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **Box** and select **Restore from PAR file**.
4. Go to **CONTROL > Box**.
5. In the left menu, expand **Network** and click **Activate new network configuration**.
6. Select **Failsafe** as the activation mode.
7. In the left menu, expand **Operating System** and click **Reboot Box**.

Replacing the primary HA firewall

If the secondary firewall is running, and the primary firewall was replaced by a new model, restore the configuration from the secondary one.

Step 1: Select the hardware model

1. Log into the secondary firewall.
2. Go to **CONFIGURATION > Configuration Tree > HA Box**.
3. Double-click **Box Properties**.



4. Click **Lock**.

5. In the **Product and Model** section, choose the correct **Hardware Model** for the replaced firewall (primary), and edit the remaining entries according to the appliance model.
6. Click **Send Changes** and **Activate**.

Step 2. Configure the primary firewall

1. Log into the secondary firewall.
2. Go to **CONFIGURATION > Configuration Tree > HA Box > HA Network**.
3. Click **Lock**.
4. In the **Management IP and Network** section, set the **Management IP** of the new HA partner (primary).
5. Click **Send Changes** and **Activate**.

Step 3. Create a PAR File

1. Log into the secondary firewall.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **Box** and select **Create PAR file for HA box**.

Step 4. Restore the primary firewall

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **Box** and select **Restore from PAR file**.
4. Go to **CONTROL > Box**.
5. In the left menu, expand **Network** and click **Activate new network configuration**.
6. Select **Failsafe** as the activation mode.
7. In the left menu, expand **Operating System** and click **Reboot Box**.

Figures

1. HA-Config.png
2. HA-Config.png

© Barracuda Networks Inc., 2024 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.