

How to Enable HA Auto-Pairing for Two Managed Firewalls

<https://campus.barracuda.com/doc/96765709/>

HA auto-pairing lets you extend a managed firewall to an HA pair of managed boxes. As of firmware release 8.2.1, HA auto-pairing is enabled by default and now supports automated pairing of managed firewalls. If you are using an earlier firmware release, you should not use the auto-pairing feature. Instead, apply the PAR file.

Before You Begin

- Ensure you are familiar with the basic concept of HA auto-pairing. For more information, see [HA Auto-Pairing](#).
- Ensure your managed firewall has firmware 8.3.0 or higher and that the HA auto-pairing feature is enabled by default.
- Ensure that both firewalls are connected via the private uplink cable on the HA port. For more information, see [HA Auto-Pairing](#).

Enable HA Auto-Pairing for Two Managed Firewalls

Step 1 (Only for Virtual Appliances) Activate the HA Auto-Pairing Feature on Both Boxes

You can omit the following steps on hardware appliances because HA auto-pairing is already enabled.

1. Log into your primary/(secondary) firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. In the left menu bar, select **Automatic HA Pairing**.
4. Click **Lock**.
5. In the section **Automatic HA Pairing**, set **Enable Automatic HA Pairing** to **yes**.
6. Select the interface from the list **HA physical interface**.



Automatic HA Pairing	
Enable Automatic HA Pairing	Yes
HA physical interface	
Enable Serial Check	Yes

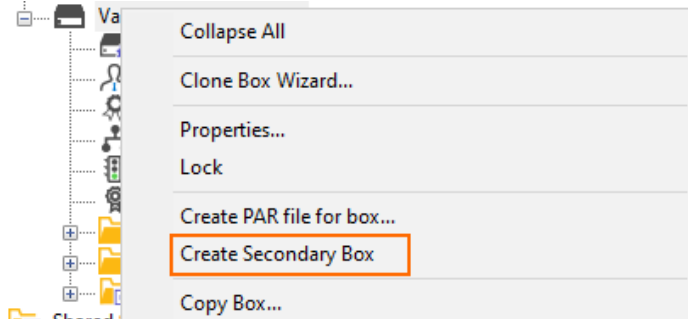
7. Click **Send Changes/Activate**.
8. Repeat the previous steps on the secondary firewall.

Step 2. Create a DHA Configuration on the Primary Firewall

1. On the primary firewall, go to **CONFIGURATION > Configuration Tree > Multi Range >**

your range > your cluster > Boxes > your primary box.

2. Right-click **Box** and select **Create Secondary Box**.



Step 3. Add the Secondary Serial Number on the Primary Firewall

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Properties > Identification**.
3. Click **Lock**.
4. In the section **Product and Model**, enter the serial number of the secondary firewall in the field **Secondary Serial Number**.
5. Click **Send Changes/Activate**.

Product and Model	
OS Platform	CloudGen Firewall
Product Type	VF1000
Firewall Model	VF1000
Software Firewall (SF) Model	None
Encryption Level	Full-Featured-Encryption
Storage Type	SSD/HDD <input type="checkbox"/> Other
Serial Number	
Secondary Serial Number	1234567

Step 4. On the Primary Firewall, Set the Management IP of the Secondary Firewall

1. On the primary firewall, go to **CONFIGURATION > Configuration Tree > Box > Network > IP Configuration**.
2. In the section **Management Network and IPs**, enter the management IP of the secondary firewall in the field **Secondary Management IP**.

Management Network and IPs

Interface: eth0 ☐ Other

Primary Management IP: 10.17.37.205

Secondary Management IP: 10.17.37.206

Associated Netmask: 24-Bit

Responds to Ping: yes

Use for NTPd: yes

Trust Level: Trusted (added to Trusted-LAN for Firewall)

MTU:

Advertise Route: no

Shared IPs in this Network

IP Address	Alias for this IP	Responds to
10.17.37.207	None	yes

Default Route via Shared IP: yes

3. Click **Send Changes/Activate**.

Step 5. Initiate a Network Activation on the Primary Firewall

1. Log into your primary firewall.
2. Go to **CONTROL > Box > Network** and click **Activate new network configuration** to initiate a network activation on the primary firewall.

Wait until the pairing is completed. You can also inspect the log-files `box_Config.log` and `box_Control_daemon.log` for details. You can identify all entries caused by HA auto-pairing by the prefix `[AutoPairing]`.

Figures

1. enable_auto_pairing.png
2. ha_auto_pairing_create_secondary_box.png
3. enter_serial_number.png
4. ha_auto_pairing_enter_secondary_mip.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.