How to Upgrade Licenses for a CloudGen Firewall HA Pair in Azure

https://campus.barracuda.com/doc/98207596/

In some cases, you may have to upgrade the licenses of an HA system to prevent the CloudGen Firewall HA pair in Azure from running into a limitation or when a business increase requires a larger CloudGen Firewall instance with more throughput. For this process to work, you will receive two license tokens.

License Token Requirement

In a high availability (HA) Barracuda CloudGen Firewall Vx cluster, each unit must have its own license token. Get the license tokens from Barracuda Networks Technical Support. You must install the license token for the secondary unit before installing the license token for the primary unit.

> Barracuda Firewall Admin must be connected to the Internet.

Before upgrading your licenses, make sure that the primary CloudGen Firewall is in active mode.

Upgrade the Licenses of the CloudGen Firewall HA Pair

Step 1. Introduce the License Tokens on Your High Availability Units

1. Introduce the license tokens on the secondary and primary unit and activate the boxes.
2. Go to the **Status > Licenses** page.
3. Verify that all purchased licenses are listed in the **Active Licenses** section.

- After the activation process successfully completes, you will receive a notification email from Barracuda Networks Technical Support.
- The licenses for both units in your HA cluster are downloaded and installed on the primary unit.
- After your licenses are successfully retrieved, a notification window opens.

Step 2. Resize the Instances in Azure

Shut down the the secondary and primary units, resize both the instances, and switch the units back on.

> You cannot change the model type in Firewall Admin before you shut down the appliance and

complete the following steps.

1. Log into the Azure portal: https://portal.azure.com
2. Shut down the secondary CloudGen Firewall unit.
3. Resize the instance.
4. Restart the secondary CloudGen Firewall unit.
5. As soon as the box is reachable, perform a failover to the secondary unit.
6. Shut down the primary CloudGen Firewall unit.
7. Resize the instance.
8. Start the primary primary CloudGen Firewall unit.
9. As soon as the box is reachable, perform a failover to the primary unit.

Step 3. Change the Instance Type in Barracuda Firewall Admin

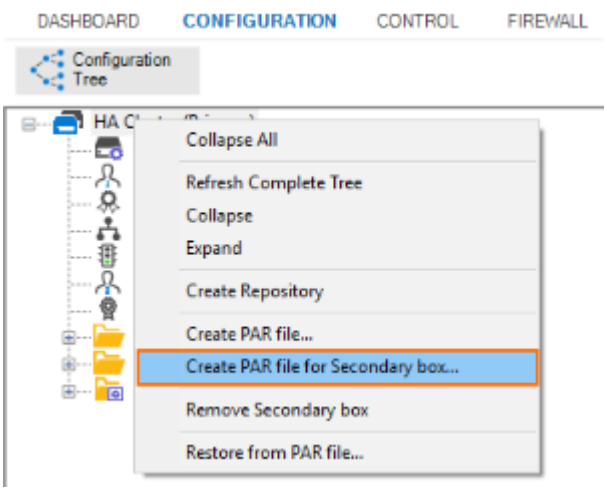
Adjust the instance type on the primary and secondary CloudGen Firewall.

Make sure to double-check the type because the system will fail back if this step takes too long.

1. Log into the CloudGen Firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Properties**.
3. Click **Lock**.
4. Adjust the appliance type and model.
5. Click **OK**.
6. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
7. Click **Lock**.
8. Adjust the network interface, if necessary.
9. Click **Send Changes** and **Activate**.
10. Go to **CONTROL > Box > Network**.
11. Activate the new network configuration.

Step 4. Create a PAR File on the Primary Firewall

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **HA-Cluster (Primary)**.
4. From the drop-down list, select **Create PAR file for Secondary box**.



5. Save the PAR file.

Step 5. Import the PAR File on the Secondary Firewall

1. Log into the secondary firewall.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **HA-Cluster (Secondary)**.
4. In the list, click **Restore from PAR file**.
5. Click **Activate**.
6. Go to **CONTROL > Box**.
7. In the left menu, expand **Network** and click **Activate new network configuration**.
8. Select **Failsafe** as the activation mode.
9. In the left menu, expand **Operating System** to expand the menu.
10. Click **Reboot Box**.

After 30 minutes, the new license should be downloaded. You can check the status under control licenses

Figures

1. HA_create_PAR_file_for_secondary.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.