How to Import an Existing Barracuda NG Firewall into a NG Control Center

https://campus.barracuda.com/doc/43846896/

If you want to manage a previously configured NG Firewall and not loose its configuration, import the PAR file. After importing the PAR file the NG Control Center automatically signs the box certificates. Deploy the PAR file to the NG Firewall to finish adding the NG Firewall to the NG Control Center. Since virtual server and service names must be unique per cluster, it is recommended to replace the default S1 virtual server with a new virtual server using an unique name. After moving and, if necessary renaming the services to the new virtual server, delete the old S1 virtual server.

In this article:

Before you Begin

- Verify that the name of the virtual server and all included service on the NG Firewall are not already used in the cluster.
- For NG Firewalls deployed in the same Azure VNET either a static internal IP address or a remote management tunnel is required to connect to the NG Control Center. For more information, see Best Practice - Switch to a Static Internal IP Address in Microsoft Azure.

Step 1. Export the PAR file on the NG Firewall

Create a PAR file on the NG Firewall. This file contains all your configuration settings.

1. Log into the NG Firewall
2. Go to **CONFIGURATION > Configuration Tree > Box**.
3. Right click on the **Box** node and select **Create PAR file**.
4. Choose the destination folder and click **Save**.
5. Click **OK**.

Step 2. Import the PAR file on the NG Control Center

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster***.
2. Right click on **Boxes** and select **Import Box from PAR file**.

3. Select the PAR file created in step 1 and click **Open**.
4. Enter a **Box Name** for the NG Firewall. The name can not be changed after importing the PAR file.
5. Click **Activate**.

Step 3. (optional) Configure Remote Management Tunnel

If your NG Firewall can not directly access the NG Control Center, configure a remote management tunnel. NG Firewalls in the Azure must use a remote management tunnel if a dynamic interface is used. For more information, see How to Configure a Remote Management Tunnel for Barracuda NG Firewalls.

Step 4. Enable the NG Firewall

Imported NG Firewalls are disabled per default. Disables NG Firewall are represented by a grey status icon.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > *your NG Firewall* > Box Properties**.
2. In the left menu, select **Operational**.
3. Set **Disable Box** to **no**.
4. Click **Send Changes** and **Activate**.

The status of the NG Firewall on the **Status Map** (**CONTROL > Status Map**) now changes from grey (offline) to red with dashes (unreachable).

Step 5. Deploy the PAR file to the NG Firewall

Deploy the PAR file to the NG Firewall.

Step 5.1 Create the PAR file on the NG Control Center

1. Log in to the NG Control Center.
2. Expand the node for the NG Firewall you imported in Step 2.
3. Right click on the box name and select **Create PAR file for box**.
4. Choose the destination folder and click **Save**.

Step 5.2. Import the PAR on the NG Firewall

1. Log in to you NG Firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box**.
3. Right click on the **Box** node and select **Restore from PAR file**.
4. Click **OK**.
5. Select the PAR file created in Step 5.1. and click **Open**.
6. Click **Activate**.
7. Go to **CONTROL > Box**.
8. In the left menu, expand **Operating Systems** and click **Firmware Restart**.
9. Click **YES**. The firmware of the NG Firewall restarts.

The status of the NG Firewall is now green, red or yellow. It can take a couple of minutes to for the NG Firewall to create a management tunnel.