How to Import an Existing F-Series Firewall into a Control Center

https://campus.barracuda.com/doc/46208937/

If you want to manage a previously configured NextGen Firewall F-Series and not lose its configuration, import the PAR file. After importing the PAR file, the NextGen Control Center automatically signs the box certificates. Deploy the PAR file to the firewall to finish adding the firewall to the 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 services on the NextGen Firewall F-Series are not already used in the cluster.
- For firewalls deployed in the same Azure VNET, either a static internal IP address or a remote management tunnel is required to connect to the Control Center.

Step 1. Export the PAR file on the NextGen Firewall F-Series

Create a PAR file on the NextGen Firewall F-Series. This file contains all your configuration settings.

1. Log into the NextGen Firewall F-Series
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 Control Center

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

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

Step 3. (optional) Configure Remote Management Tunnel

If your NextGen Firewall F-Series can not directly access the Control Center, configure a remote management tunnel. 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 an F-Series Firewall.

Step 4. Enable the NextGen Firewall F-Series

Imported Firewalls are disabled per default. Disabled NextGen Firewall F-Series are represented by a grey status icon.

1. Log in to the Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > *your NextGen Firewall F-Series* > Box Properties**.
3. In the left menu, select **Operational**.
4. Click **Lock**.
5. Set **Disable Box** to **no**.
6. Click **Send Changes** and **Activate**.

The status of the NextGen Firewall F-Series 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 NextGen Firewall F-Series

Deploy the PAR file to the NextGen Firewall F-Series.

Step 5.1 Create the PAR file on the Control Center

1. Log into the Control Center.
2. Expand the node for the NextGen Firewall F-Series 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 NextGen Firewall F-Series

1. Log in to you NextGen Firewall F-Series.
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**.

Step 5.3. Activate the Network Configuration

1. Go to **CONTROL > Box**.
2. In the left menu, expand the **Network** section and click **Activate new network configuration**.
3. Select **Failsafe**.

Step 5.4. Restart the Firmware

1. Go to **CONTROL > Box**.
2. In the left menu, expand **Operating Systems** and click **Firmware Restart**.
3. Click **YES**. The firmware of the firewall restarts.

On the Control Center go to **CONTROL > Status Map**. The status of the imported firewall is now green, red or yellow. It can take a couple of minutes to for the now managed firewall to create a management tunnel.