Migration from 8.0.1/8.0.2/8.0.3/8.0.4/8.0.5 to 8.0.6

https://campus.barracuda.com/doc/96768141/

This article assumes that you have already successfully upgraded to firmware version 8.0.1/8.0.2/8.0.3/8.0.4/8.0.5.

Before You Begin

Important Notes Before Migrating

Split Control Centers

If you are running split Control Centers (multiple Control Centers in a parent-to-child relation), you must perform a series of steps in order to use split Control Centers with a simplified configuration.

> The following instructions contain 2 sequences, where the first sequence (Steps 1-2) must be done before upgrading to 8.0.6 and the second sequence (Steps 3-5) afterward!
>
> The upgrade contains a new default rule set for the host firewall that contains all new settings for running a split CC with an optimized configuration procedure. If you have made changes to your host firewall rule set, you must create a backup of your individual rules before upgrading and then restore them after the upgrade.

Step 1. (optional)

If you have modified the host firewall rule set by adding individual rules, create a backup of all your individual rules on all Control Centers (parent and child).

Step 2.

Perform the upgrade to firmware 8.0.6. During the upgrade, the default rule set for the host firewall will be updated and include all entries for a split Control Center.

Step 3.

After upgrading to 8.0.6, perform these steps:

1. Log into the child Control Center(s).
2. Go to **CONFIGURATION > Configuration Tree > Multi Range > Global Settings > CC Parameters > Split Control Center**.
3. Click **Lock**.
4. Switch to **Advanced Configuration Mode**.
5. For **Parent Control Center IP**, enter the box level IP of the parent Control Center.
6. Click **Send Changes / Activate**.

Step 4.

Perform a **Copy from Default** for the host firewall rule set for every split Control Center (parent and child).

Step 5. (optional)

If you have created a backup of individual host firewall rules, restore the rules.

Proxy and URL Filters

If you are upgrading from firmware version 8.0.4 to 8.0.6 and **Default Access Control Policies** are allowed in **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP Proxy > HTTP Proxy Settings > Access Control > ACL Entries >** ***your entry for URL Filter Categories*** , you must check the categories that could be empty.

In any case, it is recommended to reconfigure them. If the list is not empty, perform a dummy change and re-enter the number for **Num Categorize Helpers**, and then confirm with **Send Changes / Activate**.

Header Reordering for VLANs and DHCP Relay Agent

Important

If you are using xDSL links on a VLAN interface, or if you are using the DHCP-server service or DHCP relay agent on your firewall, perform the steps below before applying the update:

1. Go to **Configuration Tree > Box > Network**.
2. On the left side, click **Virtual LANs**.
3. In the list, double-click the VLAN entry where the xDSL is attached to.
4. Enable **Header Reordering**.
5. Click **OK** and **Send Changes/Activate**.
6. Go to **CONTROL** > **Box** and click **Network** in the left navigation bar to expand the menu.
7. In the left navigation bar, click **Activate new network configuration**.

8. Click **Soft...** to trigger a network activation.

After completing these steps, it is safe to install update 8.0.6.

Within the reboot from the firmware update, the **Header Reordering** setting will be applied to your VLAN interface.

If these steps are not done before the update, be aware of the following:

- Your xDSL connection will no longer work after the update.
- Your DHCP server will no longer work as expected for VLANs after the update.
- Your DHCP relay agent will no longer work as expected.

For more information on the setting for header reordering, see also 8.0.6 Release Notes, paragraph "Usage of DHCP on a VLAN Interface".

Barracuda Firewall Admin

After updating a system, you must also download Firewall Admin with the same version. Firewall Admin is backward-compatible. That means you can manage 7.x and 8.x F-Series Firewalls and Control Centers with Firewall Admin 8.x.

Always use the latest version of Barracuda Firewall Admin.

Read the **Release Notes**, especially the **Known Issues** section, for the firmware version that you want to update to.

For more information, see 8.0.6 Release Notes.

Migration Path to 8.0.6

The following table lists all current firmware versions to which this article applies:

Current Version	Target Version 8.0.6
8.0.1	Yes
8.0.2	Yes
8.0.3	Yes

8.0.4	Yes
8.0.5	Yes

Review Upgrade Requirements

Verify that your CloudGen Firewall or Control Center meets the upgrade requirements, and read the release notes for the firmware version.

Supported Models for Firmware Version 8.0.6

The following models will be capable of running firmware version 8.0.6:

Barracuda CloudGen F-Series and Control Center Models	
Hardware Systems	F12 Rev A, F18 Rev A/B, F80 Rev A/B, F82 Rev A, F93 Rev A, F180 Rev A/B, F183 Rev A, F183R Rev A, F193 Rev A, F280 Rev B/C, F380 Rev A/B, F400 Rev B/C (8/12 ports), F600 Rev C/D, F800 Rev B/C, F900 Rev A (only fresh install), F900 Rev B, F1000 Rev A, F1000 Rev B, C400 Rev A, C610 Rev A
Virtual Systems	VF10, VF25, VF50, VF100, VF250, VF500, VF1000, VF2000, VF4000, VF8000, VC400, VC610, VC820, Proxmox running with KVM images
Public Cloud	AWS, Azure, Google Cloud

Standard Hardware Systems	
Standard Hardware	A standard hardware system is a Barracuda CloudGen Firewall F-Series running on 3rd-party server hardware using an SF license. Consult the Barracuda Networks Technical Support to find out if your specific standard hardware is supported.

Disk Space Requirements

Upgrading to version 8.0.6 requires your disk partitions to have enough free disk space.

Only a fresh install will repartition the firewall's disk drive for future requirements.

Firmware 8.0.6 will require the following partition spaces:

Hard Drive Partition	**Disk Space Requirements**
/	Minimum 6 GB, 2 GB free

/phion0	1.5 GB free
/boot	Minimum 180 MB

Migration Instructions for 8.0.6

When upgrading according to the migration path above, you must complete the migration steps listed below:

Step 1. (optional) Remove Virtual WAN Configuration

This step is necessary only if you have configured a connection to Microsoft Azure Virtual WAN.

In the following steps, you must remove the whole configuration for Azure Virtual WAN connections and re-enter all fields after the migration.

> It is recommended to save a copy of the edit fields for easing the input after the migration, e.g., by making a screenshot.

1. Log into the CloudGen Firewall with Firewall Admin.
2. Go to **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your Box* > Advanced Configuration > Cloud Integration.**
3. Select **Azure Virtual WAN** in the left menu.
4. Click **Lock**.
5. In the **Azure Virtual WAN Connections** section, click the entry of your Virtual WAN and click **x** to remove it.
6. Click **Send Change**s and **Activate**.

> After the update, you must reconnect to Microsoft Azure Virtual WAN and re-enter the previously deleted configuration.

How to Migrate to Version 8.0.6

Download the appropriate download file.

If You Migrate from Version 8.0.1/8.0.2/8.0.3/8.0.4/8.0.5 to 8.0.6.

1. Go to the download portal http://d.barracuda.com//ngfirewall/8.0.6/patch.GWAY-8.0.6-0211.tgz.
2. Download the **patch** package.

Start the Update

You can now update the CloudGen Firewall or Control Center.

For more information, see Updating CloudGen Firewalls and Control Centers.