Migration from 7.x - 8.0.0 to 8.0.6

https://campus.barracuda.com/doc/96768139/

Important Note for Users Operating Firmware 7.2.5 or 7.2.6

IMPORTANT NOTE
Ensure that the partition layout of your firewall/Control Center applies to the values in the table of paragraph "Disk Space Requirements" below.

1. If you operate a firewall that was shipped from the factory with firmware 7.2.6, or if you have already repartitioned the hard disk and performed a fresh install of firmware 7.2.6, then the hard disk already has a partition layout that is suitable for firmware 8.x.
   In this case you can upgrade directly to firmware 8.x without repartitioning the hard disk.
2. If you operate a firewall with firmware version 7.2.5 or earlier, you must repartition the hard disk with the layout listed below and fresh install firmware 7.2.6. After that, you can update to 8.x without repartitioning.

Before You Begin

Important Notes Before Migrating

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.

1. After upgrading to 8.0.6, perform these steps:
2. Log into the child Control Center(s).
3. Go to **CONFIGURATION > Configuration Tree > Multi Range > Global Settings > CC Parameters > Split Control Center**.
4. Click **Lock**.
5. Switch to **Advanced Configuration Mode**.
6. For **Parent Control Center IP**, enter the box level IP of the parent Control Center.
7. 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.

Disk Space Requirements

Upgrading to version 8.0.2 or higher 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 if not already done:

Disk Space Requirements **FIREWALL**:

Hard Drive Partition	Disk Space Required
Swap	2 GB
Boot	1 GB
/	8 GB
/phion0	4 GB
/art	3 GB

Disk Space Requirements **CONTROL CENTER**:

Hard Drive Partition	Disk Space Required
Swap	2 GB
Boot	1 GB
/	10 GB
/phion0	4 GB
/art	10 GB

Header Reordering for VLANs

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
7.0.0 - 7.0.4	Yes
7.1.0 EA - 7.1.5	Yes
7.2.0 - 7.2.6	Yes
8.0.0	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.

Migrating vs. Clean Install

Firmware version 8.0.6 supports both migrating from 7.x to 8.0.6 and a clean install of 8.0.6.

Barracuda Networks recommends that you do a fresh install due to the following reasons:

- Firmware 8.0.2 and higher has been refactored to meet increasing storage demands, also for upcoming releases. For this, the internal disk of the firewall must be repartitioned to provide enough space at the startup of the firewall. This is the ideal opportunity to prepare your firewall for future firmware releases with increasing storage demands.
- For more information on how to do a fresh install, see "How to Do a Fresh Install of Firmware 8.0.6" at the end of this article.

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.

Legacy Services with Release of Firmware 8.0.6

With firmware release 8.0.2 and higher, the following services are no longer available:

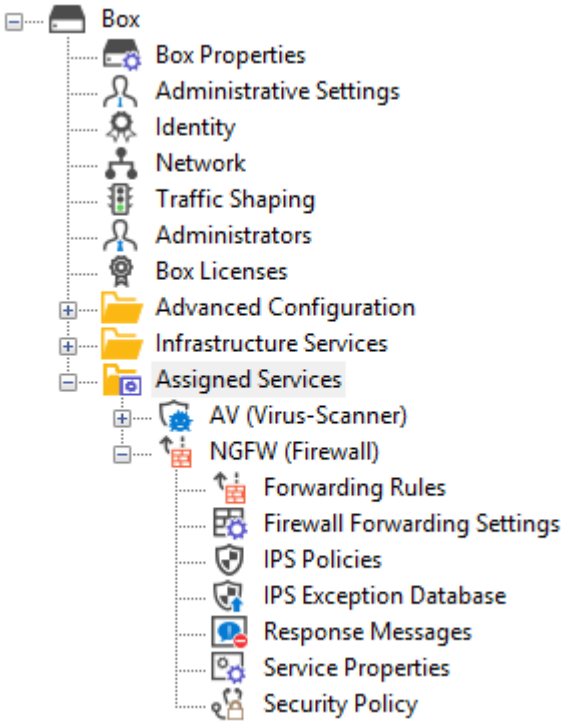
Legacy Services no longer available in firmware release 8.0.2 and higher

- SSH Proxy
- FTP Gateway
- Mail Gateway
- SPAM Filter
- Public Key Infrastructure Service
- NG Web Filter (IBM/ISS)

Before migrating your firewall to release 8.0.6, you must remove these services on your current release, e.g., firmware release 7.2. This applies both to stand-alone and managed firewalls in cluster versions lower than 8.x.

Replacement of Virtual Servers by a New 2-Layer Architecture

The former 3-layer server-service architecture has been replaced by a 2-layer architecture where services are now operated on top of the box layer. With firmware 8.0.2 and higher, services are subordinated to the **Assigned Services** node and allow a simpler administration of services and reduce error-prone issues by limiting services to run only on the box where they are initially created on.



If you are migrating from a firmware version earlier than 8.0.2 to the new firmware 8.0.6, the old 3-layer architecture will still be active and you still can make changes to the respective server-service nodes.

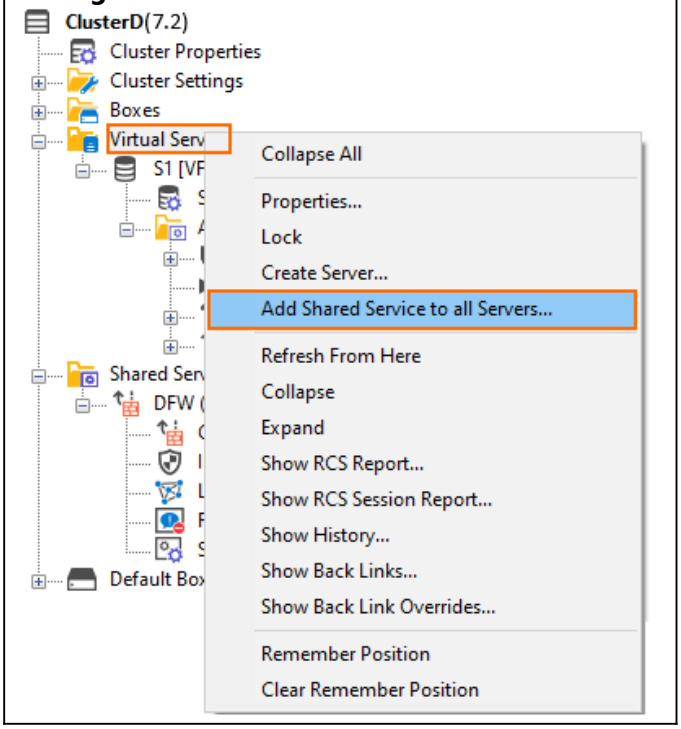
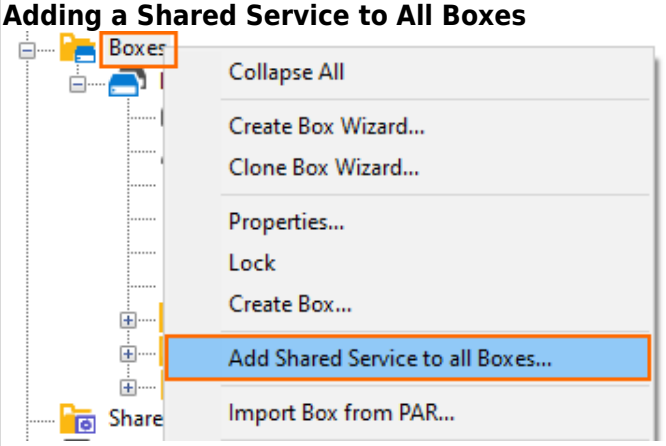
However, if you want to create a new node for services, firmware 8.0.6 only supports the creation of the 2-layer-based **Assigned Services** node.

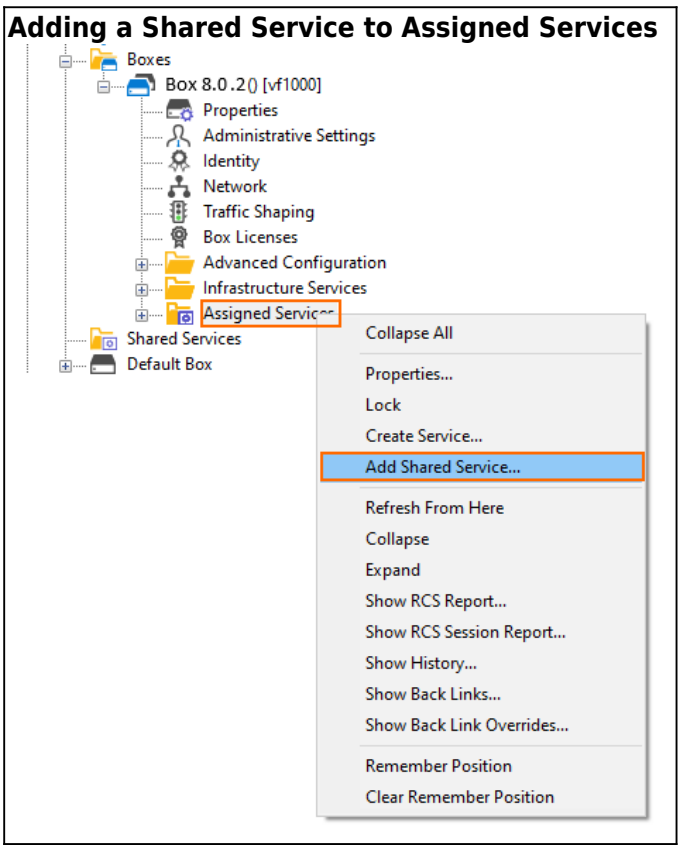
For more information, see 8.0.6 Release Notes, Assigned Services, and Understanding Assigned Services.

Shared Services

If you manage multiple cluster versions on your Control Center, note that a shared service for an 8.x cluster must be configured differently than for a 7.x cluster.

Unlike for 7.x clusters, a shared service for an 8.x cluster can no longer be assigned to the **Server** node, but rather must be assigned to the **Assigned Services** node.

Box in a Cluster for Firmware 7.2 (3-layer server-service architecture)	Box in a Cluster for Firmware 8.0 (2-layer assigned-service architecture)
Adding a Shared Service to All Servers 	**Adding a Shared Service to All Boxes** 



Naming of Bridges

The name of bridge devices `phbr-<name>` has been replaced by the new `name br.<name>`.

Migration Instructions for 8.0.6

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

Step 1. Replace Legacy Services (Where Applicable)

Legacy services that provided antivirus integration can be substituted to preserve the level of security. The substitutions for the following services can be configured by following these links:

Legacy Service	Substitutions, e.g., Firmware Release 7.2
Mail Gateway	• Mail Security in the Firewall • How to Configure Mail Security in the Firewall

FTP Gateway	• How to Configure Virus Scanning in the Firewall for FTP Traffic • How to Configure the FTP Gateway

After substituting, it is safe to remove the respective legacy services.

Step 2. Remove All Legacy Services from the Virtual Server

The following steps must be executed for all legacy services listed at the beginning of this paragraph if they are running on top of your virtual server.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services**.
2. Right-click the legacy service.
3. In the list, select **Lock**.
4. Right-click the legacy service.
5. In the list, select **Remove Service**.
6. In the notification window, click **Yes** to remove the service.
7. Click **Activate**.

Step 3. (optional) Disconnect Your CloudGen Firewall from Azure OMS Log Analytics Workspace

This step is necessary only for CloudGen Firewalls that are connected to an Azure OMS Log Analytics workspace if you migrate from firmware 7.x to 8.0.6.

1. Log into the Azure portal: https://portal.azure.com.
2. In the left menu, click **All services** and go to **Log Analytics workspaces**.
3. Select the workspace that your CloudGen Firewall is attached to.
4. Click **Virtual machines** to show a list of all virtual machines.
5. Click on the entry of the virtual machine of your CloudGen Firewall.
6. Click **Disconnect** to disconnect the CloudGen Firewall from the Log Analytics workspace.
7. To confirm that you want to disconnect the virtual machine, click the **Yes** button.
8. Wait until you are informed that it is successfully disconnected.

After the update, you must reconnect your Log Analytics workspace again.

VPN IPsec Tunnels with IKEv2 DH-Groups for Phase 1 & 2

Some DH groups with a smaller length are no longer suited to provide state of the art security for IKEv2 in phase 1 and phase 2.

If you have VPN IPsec tunnels configured that use IKEv2 DH groups, you must check the setting with a version of Firewall Admin that applies to a firewall firmware version earlier than or equal

to 8.0 before migrating!

To check the settings, do not use Firewall Admin for CloudGen Firewall 8.0.3 at this point unless you want to break your VPN tunnels!

Elliptic Curves for Diffie Hellman Groups with a bit-length smaller than 256 bit are no longer supported because they are not secure.

To check the settings, use Firewall Admin for a CloudGen firmware version 8.0 or earlier:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN > Site to Site > IPsec IKEv2 Tunnels > *your IPsec IKEv2 Tunnel***, section **Phase 1, DH Group**.
2. If you have configured a red marked **DH-Group** 25, 26, 27, 28, 29, or 30 for **Phase 1 & 2**, replace this value by a **DH-Group** marked as green in the following table:

Keyword	DH Group	Modulus
ecp192	25	192 bits
ecp224	26	224 bits
ecp256	19	256 bits
ecp384	20	384 bits
ecp512	21	512 bits
ecp224bp	27	224 bits
ecp256bp	28	256 bits
ecp384bp	29	384 bits
ecp512bp	30	512 bits

After this point, it is safe to use Firewall Admin for firmware release 8.0.6.

DNS

Firmware 8.0.2 includes a new DNS implementation with a redesigned user interface to provide a better user experience. If you are running a DNS server, all DNS zones and records will be migrated to the 8.0.2 firmware version. Also, if the DNS server is active on 7.x and when migrating from 7.2 to 8.0.2, all migrated IP addresses will be assigned to the ALL listener category. This only refers to the **Listener Name** parameter in the DNS records, *not* the **DNS Listener Classification. The DNS Listener Classification** is not changed (or created) upon migration but can be configured afterward for additional answer conditions (*INTERNAL*/*EXTERNAL*) on the DNS records.

1. Please read the DNS documentation DNS before migrating. Depending on your current

configuration, additional configuration steps may be necessary after migration.
After the migration, an implicit listener will only be available for direct-attached networks. For recursive lookups from remote networks, you must create a listener for the IP address where DNS queries will be received on. These listeners must be associated with their corresponding zone entries.

2. If you have configured/modified special BIND parameters on file system level in firmware releases earlier than 8.0.3, only those parameters will be migrated that are directly available through the new user interface.

Zones

Zones will be migrated depending on their zone type:

Zone Type of DNS < 8.0.2	Migration	Target Zone Type of DNS 8.0.3/8.0.4/8.0.5/8.0.6
Master zone	Yes	Primary zone
Master zone that contains in-addr.arpa / ipv6.arpa	Yes	Reverse zone
Slave zone	Yes	Secondary zone
Forward zone	No	-
Hint zone	No	-

Record Types

All records will be migrated. However, there will be a differentiation:

- Standardized record types will be migrated to standardized record types, e.g., A, AAAA, NS, MX
- Non-standardized record types will be migrated to OTHER record type

DNS Configuration Options

Configuration parameters that are not explicitly mentioned here will not be migrated!

Configuration parameters that will be migrated are listed in the following table.

Configuration value	Where to find in old DNS < 8.0.2	Where to find in new DNS 8.0.3 / 8.0.4 / 8.0.5 / 8.0.6
forwarders	DNS Configuration > right-click on root node → Properties...	DNS Forwarders
masters	DNS Configuration > right-click on zone node → Properties... > type "Slave" > Masters	Primary DNS Servers

allow-transfer	DNS Configuration > right-click on zone node → Properties... > advanced...	Zone Transfer ACL
TTL of the SOA record	DNS Configuration > right-click on zone node → Properties... > Start of authority (SOA) > Expire (TTL)	Edit Hosted Zone > TTL
SOA MNAME	DNS Configuration > right-click on zone node → Properties... > Start of authority (SOA) > Primary Server	Edit Hosted Zone > Primary Name Server
SOA RNAME	DNS Configuration > right-click on zone node → Properties... > Start of authority (SOA) > Responsible person	Edit Hosted Zone > Responsible Person Email
$TTL	DNS Configuration > right-click on zone node → Properties... > Start of authority (SOA) > Standard TTL	Edit Hosted Zone > TTL

Usage of DNS Command Line Tool 'dig'

Because the new DNS implementation in the firmware release 8.0.2 or higher is based on BIND V9.11, the usage of DNS cookies is now allowed as a default. DNS cookies increase the security during the communication between a BIND-based DNS server and a BIND-based client, e.g., a CloudGen Firewall acting as a client and sending resolving requests to another CloudGen Firewall running as a primary DNS.

The BIND V9.11 command line tool 'dig' uses DNS cookies when queries are sent. However, this can lead to problems if a resolving query with a DNS cookie is received by a Microsoft DNS server because cookies are not handled there. User scripts that execute the command 'dig' will therefore fail in case the answering DNS server is from Microsoft.

To avoid problems, you must modify your scripts that use the 'dig' command so that DNS cookies are not used when the command 'dig' is executed. For this, add the option '+nocookie' to the end of the line, e.g., `dig ..... +nocookie`.

For more information on how to use 'dig', log into the shell and type '`man dig`'.

First-Generation ATP to Second-Generation Barracuda ATP Cloud Migration

As of January 31, 2019, the first-generation ATP cloud services used by default with firmware versions 7.0.x, 7.1.0, 7.1.1, and 7.2.0 will be discontinued. Firewalls using ATP must switch to the second-generation ATP cloud service, which is known as Barracuda Advanced Threat Protection (BATP).

The following table gives an overview of the options you have when you run a special firmware

version:

Product	Your Current Firmware Version	Migrating Option
Stand-alone Box	7.1.0, 7.1.1, 7.2.0	Update to the latest 7.1.x or 7.2.x releases, which are using BATP, without the need for further changes. For more information, see **How to Install Updates via NextGen Admin** on *campus.barracuda.com* . If you cannot update your stand-alone box(es) to the latest releases, you can also migrate manually. For more information, see **How to Migrate Boxes with 7.1.0, 7.1.1 and 7.2.0 to BATP** below.
Control Center with Managed Box	CC: 7.1.0, 7.1.1, 7.2.0 and Box: 7.1.0, 7.1.1, 7.2.0	Update your managed boxes via the Control Center to the latest firmware release. For more information, see How to Update Control Center-Managed CloudGen Firewalls. If you cannot update your managed box(es) to the latest releases, you can also migrate manually. For more information, see **How to Migrate Boxes with 7.1.0, 7.1.1 and 7.2.0 to BATP** below.
Control Center with Managed Box	CC: 7.1.2, 7.2.1 or newer and Box: 7.1.0, 7.1.1, 7.2.0	If you cannot update your managed box(es) to the latest release, contact the Barracuda Networks Support Team.
Stand-alone Box Managed Box	7.1.2 or newer 7.2.1 or newer	These firmware versions already support BATP. No changes are necessary.

How to Migrate Box with 7.1.0, 7.1.1 and 7.2.0 to BATP

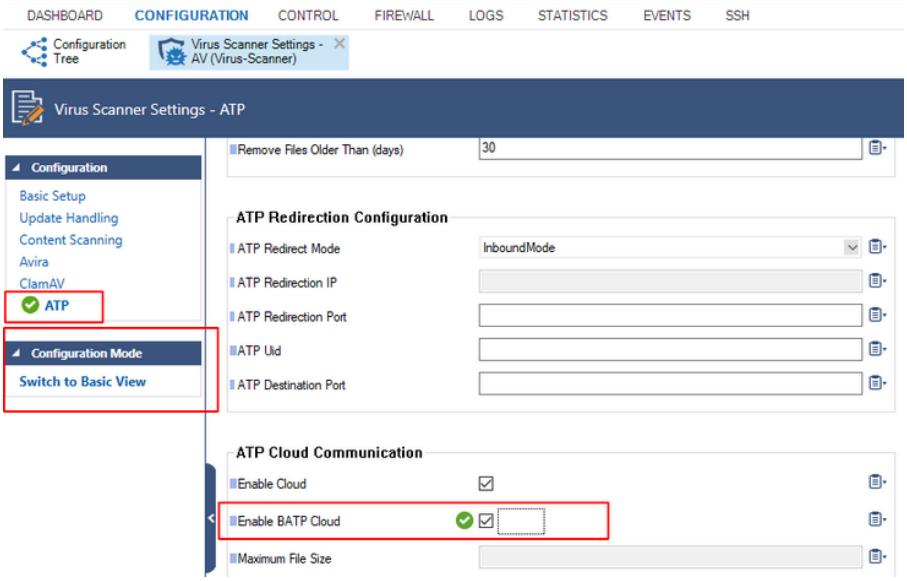
Step 1. Enable Expert Settings in Barracuda Firewall Admin

For more information, see Barracuda Firewall Admin Settings.

Step 2. Enable the BATP Cloud Service

Enabling the BATP cloud service disconnects your firewall from the first-generation ATP service and connects it to the second-generation Barracuda ATP Cloud.

1. Log into your firewall.
2. Go to **CONFIGURATION > Configuration Tree > *your virtual server* > Assigned Services > AV (Virus Scanner) > Virus Scanner Settings**.
3. In the left menu, click **ATP**.
4. Click **Lock**.
5. In the **ATP Cloud Communication** section, select the check box **Enable BATP Cloud**.



6. Click **Send Changes**.
7. Click **Activate**.

Your firewall now is connected to the second-generation Barracuda ATP Cloud service.

SSL VPN

If you are upgrading from 7.x, you will need to enable the TOTP service in order to continue allowing your users to self-enroll in the time-based one-time password authentication scheme.

Change to List of Available Ports for Barracuda Download Servers

Barracuda Networks download servers no longer provide downloads on port 8000. Instead, downloads are delivered only through ports 80 and 443.

For more information, see Best Practice - Hostname List for Barracuda Online Services.

Source-Based VPN Routing Table Entries

If you are using source-based VPN routing tables, you have the option of moving the entries to the main routing table. For this, you must set the switch **Add VPN Routes to Main Routing Table (Single Routing Table)** to **yes** in **CONFIGURATION > Configuration Tree > *your virtual server* > VPN > VPN Settings > Server Settings**.

Unlike before, entries with identical destination addresses in the main routing table are now aggregated regardless of their source address to save valuable memory for even more routing entries. You must be aware that when moving source-based VPN routing entries to the main routing table, the source address of a VPN routing entry will be ignored. Therefore, if you want to route VPN traffic based on a special source address, it is recommended not to use the option as described above.

Firewall Activity Log

When updating a box to 8.0.6, logging of the actions Drop/Remove is disabled by default.

In case the log policy **Activity Log Data** is set to **Log-Info-Text**, the setting must be reconfigured after the update to 8.0.6. The update will introduce the default value **Log-Info-Code**.

Update for SNMP, PHION-MIB.txt File

A new PHION-MIB.txt file is provided that solves an issue where throughput data can now exceed the limit of a 32-bit integer. If your CloudGen Firewall is also part of your SNMP, you should download this new file version. For more information, see PHION-MIB Field Descriptions.

Transfer and Reassign Certificates

In case you are running a stand-alone firewall and want to manage it in a Control Center, all certificates stored in the local Certificate Store must be saved on the stand-alone firewall, imported to the Certificate Store on the Control Center, and reassigned at their appropriate location of usage. For more information, see How to Import an Existing CloudGen Firewall into a Control Center.

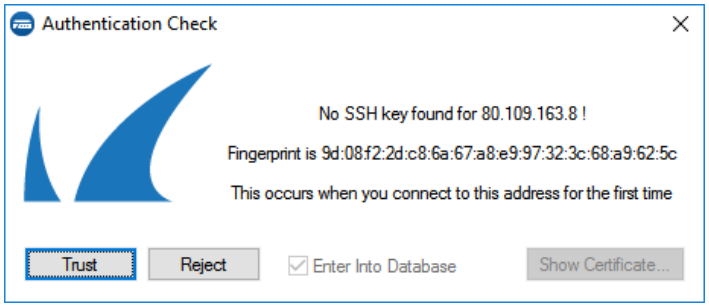
SSL VPN, NAC, and SSL VPN Authentication

SSL VPN authentication and NAC are automatically migrated into the default access control policy.

For more information, see How to Configure Access Control Policies for Multi-Factor and Multi-Policy Authentication.

ECDSA SSH Key

Depending on the cipher preferred by the SSH client, you may be prompted to accept the new ECSDA key.



Initial Grace Period for Default Password

When licensing a hardware appliance or a virtual firewall, the initial default password must be immediately changed to a new password after logging in. The new password will be valid even after the license has expired.

How to Do a Fresh Install of Firmware 8.0.6

For a fresh install, it is recommended to first back up your firewall configuration. After installing the new firmware 8.0.6, the configuration must be restored.

1. Create a backup of your firewall configuration. For more information, see How to Back Up and Restore Firewall, Secure Access Controller and Control Center Configurations.
2. Install the new firmware 8.0.6. For more information, see How to Recover a CloudGen Firewall or Control Center Appliance with a USB Flash Drive.
3. Restore the previously created backup of your firewall configuration. For more information, see How to Back Up and Restore Firewall, Secure Access Controller and Control Center Configurations.

How to Migrate to Version 8.0.6

Download the appropriate download file.

If You Migrate from Version 8.0 or 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.

If You Migrate from Versions 7.x to 8.0.6

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

Start the Update

You can now update the CloudGen Firewall or Control Center.

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

Figures

1. assigned_services_tree.png
2. shared_services_7.png
3. add_shared_services_to_all_boxes_802.png
4. shared_services_8.0.2.png
5. migrate_to_batp_enable_batp_cloud.png
6. authentication_check.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.