7.2.5 Migration Notes

https://campus.barracuda.com/doc/90442541/

Migration Path to 7.2.5

You can upgrade to firmware 7.2.5 from the following firmware versions:

Current Version	Target Version 7.2.5
6.0.0 - 6.0.7	Yes
6.1.0 - 6.1.3	Yes
6.2.0 - 6.2.4	Yes
7.0.0 - 7.0.4	Yes
7.1.0 EA - 7.1.5	Yes
7.2.0 EA1	Yes
7.2.1 EA2	Yes
7.2.2 - 7.2.4	Yes

Direct updating from firmware 5.x to 7.2.x is not possible. For more information, see Migrating from 5.4.x to 6.0.x .

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

For more information, see 7.2.5 Release Notes .

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

You can upgrade the following CloudGen Firewall models to 7.2.5:

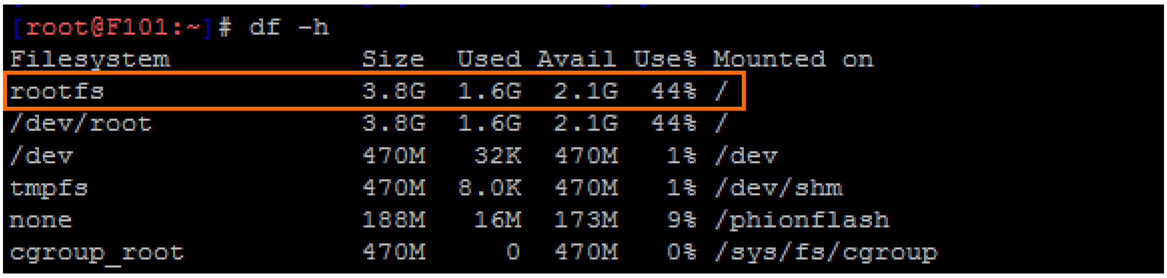
Barracuda CloudGen F-Series and Control Center Models

Hardware Systems	F10 Rev B, F12 Rev A, F15 Rev A/B, F18 Rev A, F80 Rev A/B, F82 Rev A, F100 Rev B, F101 Rev B, F180 Rev A, F183 Rev A, F183R Rev A, F200 Rev C, F201 Rev C, F280 Rev A/B, F300 Rev B, F301 Rev B, F380 Rev A, F400 Rev B, F600 Rev C/D, F800 Rev B/C, F900 Rev A/B, F1000 Rev A, C400, C610
Virtual Systems	VF10, VF25, VF50, VF100, VF250, VF500, VF1000, VF2000, VF4000, VF8000, VC400, VC610, VC820, VFAC400, VFAC610, VFAC820
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

To upgrade a system to version 7.2.5, you must have at least 50 MB of free space in the **/boot/** partition and at least 2.1 GB in the / (root) partition. If you are upgrading an F10 Rev B, F100 Rev B, F101 Rev B, verify that enough disk space is available:



```
[root@F101:~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
rootfs                  3.8G  1.6G  2.1G  44% /
/dev/root               3.8G  1.6G  2.1G  44% /
/dev                    470M   32K  470M   1% /dev
tmpfs                   470M  8.0K  470M   1% /dev/shm
none                    188M   16M  173M   9% /phionflash
cgroup_root             470M     0  470M   0% /sys/fs/cgroup
```

To free up disk space, download the following cleanup script, and apply it via remote execution to centrally managed firewalls. For standalone firewalls, the script can be executed locally on firewall.

- Block the Virus Scanner service.
- Download the Barracuda Cleanup Script for F10, F15, F100 models. Deploy it via remote execution to centrally managed firewalls. Alternatively run the commands manually in the command line interface.

  > If you still do not have enough free disk space to update, contact Barracuda Technical Support.

Upgrading One Firewall in a High Availability Cluster

If you are upgrading a firewall in a high availability (HA) cluster without upgrading its partner, you must re-synchronize the firewalls:

1. Go to **FIREWALL > Live > Show Proc**.
2. Select the **Sync Handler** process and select **Kill Selected**.

The process is automatically restarted after a couple of seconds, and the primary and secondary firewalls automatically synchronize their sessions.

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 5.2.x, 5.4.x, 6.x and 7.x F-Series Firewalls and Control Centers with Firewall Admin 7.2.5.

Always use the latest version of Barracuda Firewall Admin.

Migration Instructions for 7.2.5

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

Change to List of Available Ports for Barracuda Download Servers

Barracuda 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 7.2.5, 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 needs to re-configured after the update to 7.2.5. 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 now can 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 standalone firewall and want to manage it in a Control Center, all certificates stored in the local Certificate Store must be saved on the standalone 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.

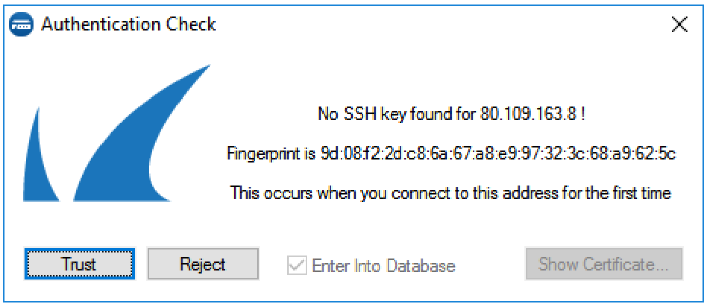
SSL VPN, NAC, and SSL VPN Authentication

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.



Authentication Check

No SSH key found for 80.109.163.8 !

Fingerprint is 9d:08:f2:2d:c8:6a:67:a8:e9:97:32:3c:68:a9:62:5c

This occurs when you connect to this address for the first time

Rename SSL Interception

SSL Interception has been renamed to SSL Inspection.

Initial Grace Period for Default Password

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

Start the Update

You can now update the CloudGen Firewall or Control Center.

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

Figures