Migrating to 6.1

https://campus.barracuda.com/doc/43846929/

Before migrating your Barracuda NG Firewall to 6.1.x, review the requirements and changes listed in the following sections. Some changes applied during the migration might require you to make preparations before the update or extra configurations after the update.

Migration Path to 6.1.x

You can upgrade to firmware 6.1 from the following firmware versions:

Current Version	Target Version			
	6.1.0	6.1.1	6.1.2	6.1.3
6.0.0	Yes	Yes	Yes	Yes
6.0.1	Yes	Yes	Yes	Yes
6.0.2	No	Yes	Yes	Yes
6.0.3	No	No	Yes	Yes
6.0.4	No	No	No	Yes
6.0.5 and higher	No	No	No	No

- Direct updating from versions 4.2.x or 5.x to version 6.1.x is not possible.
- Barracuda NG Firewall F100 and F101 models must follow special migration instructions. See **F100.**
- The migration path for Barracuda NG Firewalls or NG Control Centers using Citrix Xen HVM images is 5.4 > 6.0.2 > 6.1.1 (or higher).

For more information on migrating to 6.0, 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.

Review Upgrade Requirements

Verify that your Barracuda NG Firewall or Barracuda NG Control Center meets the upgrade requirements.

Supported Models

You can upgrade the following Barracuda NG Firewall models to major version 6.

Barracuda NG Firewall Systems	
Hardware Systems	F10 Rev A/B, F15, F100 Rev A/B, F101 Rev A/B, F200 Rev A/B/C, F201 Rev A/B/C, F280 Rev A, F300 Rev A/B, F301 Rev A/B, F380 Rev A , F400 Rev A/B, F600 Rev A/B/C , F800 Rev A/B, F900 Rev A, F1000 Rev A, C 400, C610
Virtual Systems	VF25, VF50, VF100, VF250, VF500, VF1000, VF2000, VF4000, VF8000, VC400, VC610, VC820, AWS, Azure, vCloudAir
Legacy and Standard Hardware Systems	
Legacy	Legacy phion appliances are not supported for version 6.x or higher.
Standard Hardware	A standard hardware system is a Barracuda NG Firewall running on 3rd party server hardware using an SF license. Consult the Barracuda Networks Technical Support in order to find out if your specific standard hardware is supported.

Disk Space Requirements

You must have at least 50 MB of free space in the **/boot/** partition and twice the size of the update package in the **/** (root) partition.

Barracuda NG Firewall F100 / F101

The Barracuda NG Firewall F100 and F101 added support for virus scanning in the firewall for firmware 6.1.0 and higher. To improve performance and conserve disk space, the following additional changes were made:

- Avira is used as the virus scanner engine for the F100/F101. The ClamAV virus scanning engine is no longer available.

Complete the following steps to verify whether enough disk space is available:

```
[root@f100:~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
rootfs                3.8G  1.8G  1.9G  49% /
/dev/root             3.8G  1.8G  1.9G  49% /
/dev                  470M   32K  470M   1% /dev
tmpfs                 470M  8.0K  470M   1% /dev/shm
none                  188M  944K  188M   1% /phionflash
cgroup_root           470M     0  470M   0% /sys/fs/cgroup
none                   32M     0   32M   0% /phionflash/var/phion/run/virscan/S1_AV/cas/storage-tmpfs
```

If you do not have at least twice the size of the update package disk space available, complete the following steps before updating:

- Block the Virus Scanner service.
- On the command line, delete unnecessary files by executing the following commands:
  ```
  rm -rf /var/phion/mcdownload/clam/files/* rm -rf
  /var/phion/mcdownload/avira/files/* rm -rf
  /var/phion/preserve/boxupdate/updateStatus.db rm -rf
  /var/phion/preserve/boxupdate/clam/*
  ```
  If you still do not have enough free disk space to update your F100 or F101, contact Barracuda Technical Support.

Upgrade Barracuda NG Control Center C400 / C610

If you are updating by reinstalling via a USB stick, change the boot device order in the BIOS. Contact Barracuda Networks Technical Support if you need the BIOS password.

Upgrading a High Availability (HA) Unit without Upgrading its HA Partner Unit

If you are upgrading a unit in a high availability (HA) cluster without upgrading its partner, you must re-synchronize both units:

1. Go to the **FIREWALL > Live > Show Proc** page.
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 unit automatically synchronize their sessions.

Barracuda NG Admin

After updating a system, you must also download the Barracuda NG Admin with the same version. Barracuda NG Admin is backward-compatible. This means you can manage 5.x NG Firewalls and NG Control Centers with Barracuda NG Admin 6.1.3.

Do not use versions of Barracuda NG Admin below 6.1.3.

Migration Instructions for 6.1.3

When upgrading from 6.0.x to 6.1.3, you must complete the migration steps listed below and also perform the migration steps for 6.1.0, 6.1.1, and 6.1.2 to complete the upgrade:

Secure Web Proxy

- The Secure Web Proxy is no longer supported with firmware version 6.1.3. Remove the service before updating to 6.1.3. Use SSL Interception and URL Filtering in the Firewall or HTTP Proxy

instead.
For more information, see How to Configure SSL Interception in the Firewall, URL Filtering in the Firewall, or How to Set Up and Configure the HTTP Proxy.

Migration Instructions for 6.1.2

When upgrading from 6.0.x to 6.1.2, you must complete the migration steps for 6.1.0 and 6.1.3 listed below and also perform the migration steps for 6.1.1 to complete the upgrade:

SSH Proxy

- Remove /phion0/run/sshprx/YOUR_VIRTUAL_SERVER_YOUR_SSH_PROXY_SERVICE_NAME/USERNAME_ssh_config for the SSH proxy configuration to be modified to use the new ciphers added to the SSH Proxy service in 6.1.2.

Migration Instructions for 6.1.1

When upgrading from 6.0.x to 6.1.1, you must complete the migration steps for 6.1.0 listed below and also perform the migration steps for 6.1.1 to complete the upgrade:

NG Firewall and NG Control Center Firmware Update Element

- Add the IP addresses for the Barracuda Download portal (**64.235.151.85** and **95.172.71.5**) to the **Barracuda Update Servers** network object on the Barracuda NG Control Center and stand-alone NG Firewalls.

Citrix HVM Images

- Barracuda NG Firewalls and NG Control Centers running on a Citrix hypervisor using the HVM images now use the **xen-netfront** network driver instead of the **8139cp** driver. Upgrade your Citrix XenServer to version 6.2 or higher to take advantage of the PVHVM support.

Azure

- Updating to 6.1.1 replaces your existing SSH key on the Barracuda OS level. Go to **CONFIGURATION > Configuration Tree > Box > Identity** and generate a new **SSH Private Key** for the SSH key in NG Admin and the SSH key on the box level to match up.

Product Tips

- Go to **CONTROL > File Updates** page, select **Product Tips** from the drop-down list, and click

Set Area Config. Do a dummy change to active the configuration. This will enable or disable Product Tips for the NG Control Center and all its managed NG Firewalls.

Migration Instructions for 6.0.x to 6.1.0

When upgrading from 6.0.x to 6.1.0, you must complete the following migration steps to complete the upgrade:

Managed NG Firewalls

- You must install Hotfixes 670 and 681 on the NG Control Center running 6.0.X before upgrading managed NG Firewalls to 6.1.

Barracuda NG Firewall F100 and F101 Virus Scanning Changes

- To improve performance, Barracuda Networks recommends to use virus scanning in the firewall instead of malware scanning in the HTTP Proxy.
- The ClamAV virus scanning engine is no longer available for F100/F101 - the Avira virus scanning engine is automatically started as a replacement. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Virus Scanner > Virus Scanner Settings** to configure the Avira virus scanning engine settings.

Dynamic Routing

- A dummy change to the **Access Lists** in the **Filter Setup IPv4** and **IPv6** of the **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > OSPF/RIP/BGP Settings** page is required after the update for changes to the access lists order to take effect.
- All **Route Maps** in the **Filter Setup IPv4** and **IPv6** of the **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > OSPF/RIP/BGP Settings** page must be deleted and, after a **Send Changes** and **Activate,** re-entered.

SSL VPN

- Existing Outlook Web Access configurations are automatically migrated to use the new OWA 2007 Web Forward Template. If you are using OWA 2003 or 2010, go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > VPN > SSL VPN**, edit the Outlook Web Access Web Forward, and select the correct OWA version from the **Web Forward Template** drop-down list.

Events

- The default Event configuration has been improved for firmware 6.1.0. A new notification type was added. Events using the default settings are automatically migrated to the new default values. Events with non-default settings are not changed. For more information, see Events.

Step 3. Start the Update

Now you can update the Barracuda NG Firewall or Barracuda NG Control Center.

For more information, see Updating Barracuda NG Firewalls and NG Control Centers.

Figures