Release Notes

https://campus.barracuda.com/doc/43847272/

Before installing or upgrading to the new firmware version, back up your configuration and read the release and migration notes. If you are updating from a version earlier than 6.0.x, all migration instructions for 5.x and 6.0 also apply.

Do not manually reboot your system at any time while the update is in process, unless otherwise instructed by Barracuda Networks Technical Support. Upgrading can take up to 60 minutes, depending on your current firmware version and other system factors. If the process takes longer, please contact Barracuda Networks Technical Support for further assistance.

In these Release Notes:

General

If you want to update an existing system:

- When updating from an earlier version to 6.1, the following update path applies: **4.2 > 5.0 > 5.2 > 5.4 > 6.0 > 6.1.**
- Barracuda NG Firewall F100 and F101 models using the ClamAV Virus Scanner may not have enough free disk space for updating. For more information, see Migrating to 6.1.
- Do not upgrade Barracuda NG Firewalls or NG Control Centers using Xen HVM images to 6.1.0.

For more information, see Migrating to 6.1.

GPL Compliance Statement

This product is in part Linux-based and contains both Barracuda Networks proprietary software components and open source components in modified and unmodified form. Some of the open source components included underlie either the GPL or LGPL, or other similar licensing, which requires all modified or unmodified source code to be made freely available to the public. This source code is available at http://source.barracuda.com.

Hotfixes Included with Barracuda NG Firewall Version 6.1.3

- Hotfix **736**: DNS Server
- Hotfix **731**: Dynamic Routing
- Hotfix **727**: VPN Configurations in CudaLaunch
- Hotfix **724**: Firewall
- Hotfix **722**: Boxconfig

Improvements Included in Barracuda NG Firewall Version 6.1.3

Barracuda NG Admin

- NG Admin now works as expected for Windows usernames in all languages. (BNNGF-34773)
- The Firewall Audit user interface now also processes and displays purged data that was moved to a custom directory. (BNNGF-23820)
- In the GTI Editor service list, external VPN servers are now listed in the service list. (BNNGF-26754)
- FAN rpm values are now displayed in integral numbers. (BNNGF-35773)
- On the **VPN > Client to Site** page, you can now enable a **CN Name** column to show the **CN Name** of the client certificate. (BNNGF-29310)
- Input validation for DKIM records has been updated to allow periods FQDNs. (BNNGF-27546)
- On stand-alone NG Firewalls, the HTTP Proxy tab is now accessible for all admins with the necessary permissions. (BNNGF-22710)
- On stand-alone NG Firewalls, the ATD tab is now accessible for all admins with the necessary permissions. (BNNGF-35888)
- Entering multiple comma-separated DNS Server IP addresses in the client-to-site template now works as expected. (BNNGF-35864)

Barracuda OS

- Updated BIND to version 9.9.8P2 to fix security vulnerability CVE-2015-8000. (BNNGF-35608)
- Updated libuser to fix the following security vulnerabilities: CVE-2015-3245 and CVE-2015-3246 (BNNGF-32316)
- Updated NTP to fix several security vulnerabilities. (BNNGF-35032)
- Improved log message for model-specific performance script to: Applying model-specific performance settings

Firewall

- SSL Interception domain exceptions now works as expected. (BNNGF-31886)
- Increased default certificate size generated by SSL Interception to 2048 for non-export restricted firewalls. (BNNGF-33024)

- Logging for ICMP connections now works as expected. (BNNGF-28753)
- ICMP replies without ECHO sent to the management IP address are now dropped. (BNNGF-28557)
- Traffic Shaping now works expected for synced sessions after an HA failover. (BNNGF-28870)
- If **Log Session State Changed** is enabled for an access rule matching an ICMP echo request to the management IP address, it is now logged as expected to the firewall log.
- Blocked ICMP packets are no longer logged twice if **Log ICMP Packets** is set to **Log-All**. (BNNGF-30357)
- The client-to-site **Group Policy** configuration now displays correctly when setting the screen resolution to **medium-125%**. (BNNGF-35150)
- Application Control now works as expected to for SSL-encrypted connections when SSL Interception is disabled. (BNNGF-34855)

OSPF/RIP/BGP

- The OSPF service can now listen correctly on interfaces that were down when the service started. (BNNGF-35732)

NG Control Center

- **Create a box wizard** now configures Wi-Fi correctly for Barracuda NextGen Firewall F280b, F180, and F80. (BNNGF-35348)

HTTP Proxy

- Activating configuration changes no longer causes the HTTP Proxy to fail in rare cases. (BNNGF-25238)
- Flushing selected proxy cache entries now works as expected. (BNNGF-23118)

VPN

- Added option to bind the dynamic tunnels to an explicit IP address. (BNNGF-34544)

Azure

- Changing the password of the NG Firewall VM via the Azure web interface now works as expected. (BNNGF-33675)

SSL VPN

- VPN profiles are now imported correctly. (BNNGS-1596)
- Updated certificates used for provisioning resources. (BNNGS-1505)

Known Issues

6.1.3

- HA session sync between NG Firewalls using firmware 6.1.3 and 6.2.0 does not work.

Miscellaneous

- NG Control Center: Network > Azure Advanced Networking is displayed in a 6.1 cluster even if the managed NG Firewall is running version 6.1.1 or 6.1.0 that does not support this feature.
- HTTP Proxy: Custom block pages do not work for the HTTP Proxy when running on the same NG Firewall as the Firewall service. This issue does not occur when running the HTTP proxy service on a second NG Firewall behind the NG Firewall running the Firewall service.
- SSL VPN: Favorites are not included in the PAR file.
- SSL VPN: Text fields do not accept the # character.
- SSL VPN: The mobile navigation bar is missing from servers entered in the **Allowed Hosts**.
- SSL VPN: User Attributes do not support UTF-8.
- SSL VPN: The allowed host filter path must be unique.
- Safe Search: In some cases, YouTube safety mode does not work when logged in with a Google account.
- Safe Search: If Safe Search is enabled, it is not possible to log into YouTube when cookies are disabled.
- Safe Search: Safe Search is not enforced by Bing when using HTTP.
- VPN Routing: When a duplicate route to an already existing VPN route in the main routing table is announced to the NG Firewall via RIP, OSPF, or BGP, a duplicate routing entry is created and the route that was added last is used.
- VPN Routing: Creating a direct or gateway route with the same metric and destination as a VPN route in the main routing table results in duplicate routes. The route added last is used.
- HTTP Proxy: **Custom Cipher String** and **Allow SSLv3** settings only apply to reverse proxy configurations.
- CC Wizard: The CC Wizard is currently not supported for NG Control Centers deployed using NG Install.
- ATD: Only the first URL in the Quarantine Tab that leads to a quarantine entry is displayed, even if the User and/or IP address downloaded more than one infected file.This can be dangerous if the first downloaded file is a false-positive.
- Firewall: It is not possible to join a **join.me** session if SSL Interception and Virus Scanning is enabled in the matching access rule.
- Firewall: Using SSL Interception in combination with URL Filtering and category exemptions may result in degraded performance.
- NG Admin: SPoE does not work if an IPv6 virtual server IP address is used.
- Barracuda OS: **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually.
- Terminal Server Agent: It is not currently possible to assign connections to Windows networks shares to the actual user.
- Firmware Update: Log messages similar to `WARNING: /lib/modules/2.6.38.7-9ph5.4.3.06.x86_64/kernel/drivers/net/wireless/zd1211rw/zd1211rw.ko needs unknown symbol ieee80211_free_hw` may appear while updating, but can be ignored.

- **Attention**: Amazon AWS/Microsoft Azure: Performing **Copy from Default** of Forwarding Firewall rules currently locks out administrators from the unit and requires a fresh installation of the system.
- Application Control 2.0 and Virus Scanning: Data Trickling is done only while the file is downloaded, but not during the virus scan. This may result in browser timeouts while downloading very large files.
- Application Control 2.0 and Virus Scanning: If the Content-Length field in HTTP headers is missing or invalid, the **Large File Policy** may be ignored.
- Application Control 2.0 and Virus Scanning: It is not currently possible to perform virus scanning for chunked transfer encoded HTTP sessions such as media content streaming. Barracuda Networks recommends excluding such traffic from being scanned.
- Application Control 2.0 and Virus Scanning: In very rare cases, if the SSL Interception process is not running, but the option **Action if Virus Scanner is unavailable** is set to **Fail Close**, a small amount of traffic may already have passed through the firewall.
- Application Control 2.0 and Virus Scanning: In rare cases, Google Play updates are sometimes delivered as partial updates. These partial updates cannot be extracted and are blocked by the virus scanning engine. The engine reports **The archive couldn't be scanned completely**. Either create a dedicated firewall rule that does not scan Google Play traffic, or set **Block on Other Error** in **Avira Archive Scanning** to **No.**
- Barracuda OS: Restoring units in default configuration with par files created on an NG Control Center may result in a corrupt virtual server. Instead, copy the par file to *opt/phion/update/box.par* and reboot the unit.
- VPN: Rekeying does not currently work for IPsec Xauth VPN connections. The VPN tunnel terminates after the configured rekeying time and needs to be re-initiated.
- High Availability: IPv6 network sessions might not be established correctly after an HA failover.