Release Notes 6.0.7

https://campus.barracuda.com/doc/56656400/

This firmware version is affected by a critical security issue resolved by installing Hotfix 837. For more information, see Hotfix 837 - Security Issue.

Before installing the new firmware version, back up your configuration and read all of the release notes that apply to the versions that are more current than the version that is running on your system.

Do not manually reboot your system at any time while the update is in process, unless otherwise instructed by Barracuda Networks Technical Support. Depending on your current firmware version and other system factors, upgrading can take up to 60 minutes. 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:

- Direct updating from versions 5.0.x or 5.2.x to version 6.0.7 is not possible, and no countermanding is possible.
- The following update path applies: **5.0 > 5.2 > 5.4 > 6.0.**
- Legacy phion appliances are not supported for version 6.0 or higher.
- Barracuda NG Control Centers with clusters version 4.0 or earlier cannot be updated. Upgrade the clusters to version 4.2 before installing the update.
- 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 from 5.4.x to 6.0.x.

As of Barracuda NG Admin version 6.0.x, Microsoft Windows Vista, Windows XP, Windows Server 2003 and 2003 R2 are no longer supported.

Hotfixes included with Barracuda NG Firewall version 6.0.7

The following previously released public hotfixes are included with this release:

- Hotfix **801** – OpenSSL
- Hotfix **814** – DNS Server

What´s new in Barracuda NG Firewall version 6.0.7

Barracuda NG Firewall firmware 6.0.7 is a maintenance release. No new features were added.

Improvements included in Barracuda NG Firewall version 6.0.7

Barracuda NG Admin

- NG Admin is no longer supported on Windows Vista. (BNNGF-41630)
- In the TINA VPN tunnel configuration dialog, the drop-down menu for the **Compression** parameter is now displayed correctly. (BNNGF-41793)
- The throughput of the network interfaces on **CONTROL > Network** is now shown in MBit instead of bps10. (BNNGF-42329)
- Editing application rules with a large number of applications no longer causes NextGen Admin to crash. (BNNGF-41417)
- IPv6 ICMP traffic no longer shows the ICMP identifier as the port on the **FIREWALL > Live** and **FIREWALL > History** pages. (BNNGF-31417)
- It is now possible to use numbers in the name of a **Trusted Root Certificate** in the **SSL Interception** configuration. (BNNGF-32428)
- NextGen Admin dashboard stability improvements. (BNNGF-42232)
- **Max Entries** on the **FIREWALL > History** page are now honored immediately without a manual refresh. (BNNGF-41383)
- The timestamp for the last successful IPS update is now displayed correctly. (BNNGF-42374)
- **Networks** in the **GTI Editor** are no longer shown in phion notation. (BNNGF-41357)

Barracuda OS

- Firewalls and Control Centers using legacy phion licenses no longer receive IPS patterns.(BNNGF-42195)
- It is no longer required to restart the authentication service when configuring DC agent / DC client authentication. (BNNGF-41689)

VPN

- It is now possible to use the following DH Groups for IKEv1 IPsec: 1,2,5,14-18. (BNNGF-32748)
- Mitigated a hardware-related bug resulting in soft lockups on Barracuda Control Center C400. (BNNGF-41683)
- Updated OpenSSL to version 1.0.1u due to security vulnerability CVE-2016-6304. (BNNGF-41828)

Firewall

- **Broad-Multicast** rules no longer use Application Control. (BNNGF-29188)

DNS Server

- Updated BIND to version 9.9.9-P4 due to security vulnerability CVE-2016-8864. (BNNGF-43010)

HTTP Proxy

- Updated HTTP Proxy to fix connection error handling. (BNNGF-41946)

Control Center

- Updating patterns and definitions for a large number of managed firewalls no longer overloads the Control Center. (BNNGF-42828)
- Improved error handling for file and pattern updates of managed firewalls. (BNNGF-42756)
- Pattern updates for ranges where all managed firewalls use the distributed firewall service now work as expected. (BNNGF-42907)

Known Issues

6.0.7

No new known issues have been found in 6.0.7.

Miscellaneous

- NG Admin: Opening the Activation dialog on Windows 10 may cause NG Admin to be unresponsive for up to 20 seconds. Use NextGen Admin 7.0.0 or higher instead.
- IPsec: IPsec VPN tunnels using SHA512 between two F-Series Firewalls running firmware versions 6.0.5 and 6.0.6 fail.
- NG Admin: The IPsec **ID-type** parameter is displayed in the client-to-site VPN configuration dialog, even if it is not supported by the firmware running on the NG Firewall.
- NG Control Center: **Peer IP Restrictions** must include management IP address, Control Center

IP address, VIP IP addresses or networks, client IP address, and MIP for local managed NG Firewalls.

- HTTP Proxy: It is not possible to use ClamAV in combination with the HTTP Proxy service on Barracuda NG Firewall F100 and F101 models.
- CC Wizard: The CC Wizard is currently not supported for NG Control Centers deployed using NG Install.
- Firewall: Using SSL Interception in combination with URL filtering and category exemptions may result in degraded performance.
- 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 are enabled in the matching access rule.
- SSL VPN Mobile Portal: Mobile Portal configurations and settings are currently not included in PAR files.
- Virus Scanner: On small firewall models with insufficient free memory, the virus scanning service may stall during virus pattern updates.
- 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 currently not 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 currently not 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.**