Release Notes 6.0.4

https://campus.barracuda.com/doc/46894554/

Barracuda Networks recommends to always install the latest firmware release of the major version to benefit from the latest security and stability improvements.

This firmware version includes 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 4.2.x, 5.0.x or 5.2.x to version 6.0.4 is not possible and no countermanding is possible.
- The following update path applies: **4.2 > 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.

For more information, see Migrating from 5.4.x to 6.0.x.

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

Hotfixes Included with Barracuda NG Firewall Version 6.0.4

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

- Hotfix **715**: DC Client Authentication
- Hotfix **723**: Firewall
- Hotfix **732**: Dynamic Routing

What´s New in Barracuda NG Firewall Version 6.0.4

Barracuda NG Firewall firmware 6.0.4 is a maintenance release only. No new features were added.

Improvements Included in Barracuda NG Firewall Version 6.0.4

Barracuda NG Admin

- Configuration files for the dashboard and Firewall monitor are now written to the correct folder. (BNNGF-33185)
- Importing certificate chains with intermediate certificates now works as expected. (BNNGF-31539)
- When updating, the success message is no longer displayed before the unit reboots after an update. (BNNGF-34469)
- Deleting multiple public or SSH keys in the NG Admin settings now works as expected. (BNNGF-33108)
- Updated **DNS Blacklisting** help text to include instructions for including subdomains. (BNNGF-32827)
- Exporting, Importing, and Merging HTTP Proxy ACL entries from and to the clipboard now works as expected. (BNNGF-23121)
- The **Accepted Identification** column in the GTI Editor **Groups** tab is now displayed correctly. (BNNGF-34112)
- Restoring from a PAR file no longer causes NG Admin to freeze. (BNNGF-33988)
- Reputation search for IP addresses in **FIREWALL > Live** and **FIREWALL > History** now works as expected. (BNNGF-33440)
- Clicking **Clear** for the **Forwarding Settings > Authentication > Operational Settings** now works as expected. (BNNGF-24004)
- On the Status Map of the Control Center setting, **Use MIP instead of Access IP** now works as

expected. Selecting this option is now saved on the client computer running NG Admin. (BNNGF-34280)
- Changed error message when a user without permission to view the Status Map on the Control Center logs into the Control Center. (BNNGF-34562, BNNGF-34381)
- A scroll bar is now added to the client-to-site configuration if necessary. (BNNGF-33446)
- Fixed typo in Application based provider selection error message if the **connection list** is invalid. (BNNGF-34105)
- Removed **FIREWALL > Trace** page. (BNNGF-34382)

Barracuda OS

- HA sync no longer causes soft lockups if the HA partner is unavailable. (BNNGF-31427)
- DHCP with multiple encapsulated options now works as expected. (BNNGF-32890)
- The DC Client now correctly interprets user group information sent by the DC Agent. (BNNGF-33146)
- IPFIX log streaming with intermediary reports no longer causes high system load. (BNNGF-34016)
- Updated default cipher strings. (BNNGF-30772)
- Updated OpenSSH to fix security vulnerability CVE-2015-5600. (BNNGF-34260)
- Updated default values for **Max Session Slots** and **Max Routing Cache Entries** for Barracuda NG Firewall F18. F80, F180, F280, F380, F600, F800, F900, and F1000. (BNNGF-34268)
- Added support for /31 bit networks. (BNNGF-34175)
- The virtual server monitoring state is no longer listed on the **CONTROL > Server** page if **IP Monitoring Policy** is set to **No**. (BNNGF-24160)
- Group information is no longer logged when **Log Settings > Log Groups** is set to **no**. (BNNGF-33012)
- Fixed rare issue preventing controld from restarting services. (BNNGF-26689)
- Added option to import certificates for syslog streaming. (BNNGF-33447)
- Disabled **URL Filter** check box for **App Redirect** access rules. (BNNGF-26064)
- **Remove DHA box** is no longer visible in the context menu of the configuration tree if the configuration is not locked. (BNNGF-26421)
- Changed default settings for Netflow/IPFIX collectors. (BNNGF-34020)
- IPFIX logs are no longer filled up with **Decoding element LogOP failed** messages. (BNNGF-33444)
- Added source and destination IP address to the box level eventS.log logfile. (BNNGF-32438)

VPN

- Added **MD160**, **SHA256**, and **SHA512** to the supported hash algorithms for IPsec VPNs. (BNNGF-30520)
- IPsec ID Type is now configurable for IPsec Site-to-Site VPN tunnels. (BNNGF-32639, BNNGF-17248, BNNGF-32661)

Firewall

- HA session sync now works as expected. (BNNGF-33810, BNNGF-33715)
- The DCERPC firewall plugin no longer silently drops packets. (BNNGF-26756)
- Fix for several issues potentially causing kernel panics. (BNNGF-33174)
- Parsing compressed HTML pages by IPS now works as expected. (BNNGF-25552)
- The Firewall Activity log now logs the correct port for HTTP traffic when cumulative logging is enabled. (BNNGF-34784)
- When logging forwarding firewall traffic to an **own logfile**, **log session state change**, data is now written to the correct log file. (BNNGF-33658)
- Ruleset reevaluation no longer terminates active sessions not affected by changes to the ruleset. (BNNGF-32343)
- Using a **hostname (DNS resolvable)** type network object in a Host Firewall rule now works as expected. (BNNGF-31042)

SIP Proxy

- SIP connections using a different connection IP address than the connecting IP address are now handled correctly. (BNNGF-33448)

NG Control Center

- Linking and creating repository entries for the **Network** configuration now works as expected. (BNNGF-33037)
- CC Admins using peer IP restrictions and SPoE can now successfully authenticate. (BNNGF-27515)

HTTP Proxy

- Updated squid to version 3.5.10 to address multiple security vulnerabilities. (BNNGF-31849)
- Counting of files blocked by ATD now works as expected. (BNNGF-34400)

Wi-Fi

- The Wi-Fi UI process now listens on the correct management IP address after a management IP address change. (BNNGF-25082)

Access Control Service

- The access control UI process now listens on the correct management IP address after a management IP address change. (BNNGF-33049)

Known Issues

6.0.4

No new known issues have been found in firmware 6.0.4.

Miscellaneous

- 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: **Custom Cipher String** and **Allow SSLv3** settings only apply to reverse proxy configurations.
- 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 is enabled in the matching access rule.
- SSL VPN Mobile Portal: Mobile Portal configurations and settings are currently not included in PAR files.
- Virus Scanner: The virus scanning service stalls 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.**
- 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 currently does not work for IPsec Xauth VPN connections. The VPN tunnel terminates after the configured rekeying time and needs to be re-initiated.