Release Notes 6.0.5

https://campus.barracuda.com/doc/49057063/

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 5.0.x or 5.2.x to version 6.0.5 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.

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 6.0.5

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

- Hotfix **757** – SSLv2

What´s new in Barracuda NG Firewall version 6.0.5

Barracuda NG Firewall firmware 6.0.5 is a maintenance release only. No new features were added.

Improvements included in Barracuda NG Firewall version 6.0.5

Barracuda NG Admin

- NG Admin now works as expected for Windows usernames in all languages. (BNNGF-34773)
- The **Settings** section is now visible when editing firewall objects. (BNNGF-36918)
- In the GTI Editor service list, external VPN servers are now listed in the service list. (BNNGF-26754)
- 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)
- FAN rpm values are now rounded to the next integer. (BNNGF-35773)
- The help text for **Enable Cache Manager** in the HTTP Proxy is now displayed correctly. (BNNGF-27177)
- 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)
- Saving a filter on the **Firewall > History** page now also saves the **Max Entries** value. (BNNGF-34211)
- Help text for **TI-ID** and **TI Classification** are now displayed correctly in the GTI Editor. (BNNGF-35445)
- The client-to-site **Group Policy** configuration now displays correctly when setting the screen resolution to **medium-125%**. (BNNGF-35150)
- Input validation for DKIM records has been updated to allow periods FQDNs. (BNNGF-27546)

Barracuda OS

- Updated BIND to fix the following security vulnerabilities: CVE-2015-8000, CVE-2015-8704, CVE-2015-8705, CVE-2015-8704, and CVE-2015-8705. (BNNGF-35608, BNNGF-36213)
- ppp and bond interfaces no longer cause crashes. (BNNGF-36189)
- Updated libuser to fix the following security vulnerabilities: CVE-2015-3245 and CVE-2015-3246 (BNNGF-32316)
- Fixed hardware detection for devices using Realtek network chips. (BNNGF-35992)
- RCS no longer shows an error when using **Show Differences** in the forwarding firewall ruleset. (BNNGF-35844)
- Added i40e driver to support the Intel Ethernet Controller XL710 family. (BNNGF-33357)
- Updated NTP to fix several security vulnerabilities. (BNNGF-35032)
- Updated OpenSSL to version 1.0.1q to fix several security vulnerabilities. (BNNGF-31109)
- Added IPFIX uniflow and biflow basic templates without Barracuda-specific information. (BNNGF-35904)
- Changed log message of the applperf script to **Applying model-specific performance settings**. (BNNGF-34766)

VPN

- The VPN device index is now used for all transports for a VPN tunnel configured via the GTI Editor. (BNNGF-35913)
- Exceeding the maximum number of VPN tunnels now generates **Resource Limit Exceeded** event (136). (BNNGF-36272)
- Client-to-site VPN traffic is no longer blocked if a MAC address-based block rule is used. (BNNGF-32662)
- IKEv1 IPsec site-to-site tunnels now use the negotiated NAT-T proposal from phase 1 in phase 2. (BNNGF-36933)

Firewall

- Disabling SSLv2 for the firewall authentication web interface now disables the SSLv2 protocol, not just SSLv2 ciphers. (BNNGF-36979)
- Renamed **Inline Authentication** to **Inline Authentication for HTTP and HTTPS** in the advanced access rule settings. (BNNGF-36589)
- Increased default certificate size generated by SSL Interception to 2048 for non-export restricted firewalls. (BNNGF-33024)
- SSL Interception domain exceptions now work as expected. (BNNGF-31886)
- Traffic Shaping now works expected for synced sessions after an HA failover. (BNNGF-22870),
- Blocked ICMP packets are no longer logged twice if **Log ICMP Packets** is set to **Log-All**. (BNNGF-30357)
- Application Control now works as expected 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)

Mail Gateway

- Virus scanning with the Avira virus scanning engine now works as expected. (BNNGF-29910)
- Domain check now works as expected. (BNNGF-36139)

NG Control Center

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

HTTP Proxy

- Flushing selected proxy cache entries now works as expected. (BNNGF-23118)

Distributed Firewall

- The distributed firewall now loads the SSL Interception configuration correctly. (BNNGF-35561)

Known Issues

6.0.5

No new known issues have been found in firmware 6.0.5.

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 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: 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.