6.2.1 Release Notes

https://campus.barracuda.com/doc/71862721/

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 836. For more information, see Hotfix 836 - Security Issue.

Changelog

To keep our customers informed, the known issues list and the release of hotfixes resolving these known issues are now updated regularly.

- 19.10.2017 – Release Hotfix 849 KRACK Attack.

Before installing or upgrading to the new firmware version,

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. For assistance contact Barracuda Networks Technical Support.

In these Release Notes:

- Back up your configuration.
- The following upgrade path applies: **5.0 > 5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2.1**
- Before updating, read and complete the migration instructions.

For more information, see Migrating to 6.2.

As of January 31, 2019, the first-generation ATP cloud services used by default with firmware versions 6.2.x, 7.0.x, 7.1.0, 7.1.1, and 7.2.0 will be discontinued. Firewalls using ATP must switch to the second-generation ATP cloud service, which is known as Barracuda Advanced Threat Protection (BATP).

For more information, see 6.2 Migration Notes.

Hotfixes Included with Version 6.2.1

- Hotfix **729**: Cumulative Application Control Hotfix
- Hotfix **730**: Dynamic Routing
- Hotfix **734**: Client Application
- Hotfix **735**: DNS
- Hotfix **741**: Mail Gateway Virus Scanning
- Hotfix **742**: DNS Server

What´s New in Version 6.2.1

6.2.1 is a maintenance release. No new features were added.

Improvements Included in Version 6.2.1

Barracuda NextGen Admin

- The firmware update element now shows the correct update packages. (BNNGF-35093)
- NextGen 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)
- Removed client-to-site group policy popup if IKEv1 or IKEv2 IPsec profiles are not configured. (BNNGF-34997)
- Flushing the **Threat Scan** cache no longer flushes the Firewall history cache. (BNNGF-34039)
- The **Accepted Identification** column in the GTI Editor **Groups** tab is now displayed correctly. (BNNGF-34112)
- Restoring from a PAR file no longer causes NextGen Admin to freeze. (BNNGF-33988)
- 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)
- On the File Content Policy configuration page, the **QoS** column now displays policy rules with **No Change** correctly. (BNNGF-34763)
- Admins logging in with a RSA key only are no longer prompted to enter a password when logging in. (BNNGF-24921)
- Editing the hostname of a **Network** configuration node in the Repository while in Advanced View now works as expected. (BNNGF-16011)
- Firewall Monitor now displays user data when filtering for a username. (BNNGF-35915)
- On stand-alone NextGen Firewalls, the HTTP Proxy tab is now accessible for all admins with the

necessary permissions. (BNNGF-22710)

- On stand-alone NextGen Firewalls, the ATD tab is now accessible for all admins with the necessary permissions. (BNNGF-35888)
- 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)
- 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 NextGen Admin. (BNNGF-34280)
- Removed **FIREWALL > Trace** page. (BNNGF-34382)
- A scroll bar is now added to the client-to-site configuration if necessary. (BNNGF-33446)
- Input validation for DKIM records has been updated to allow periods in FQDNs. (BNNGF-27546)
- Entering multiple comma-separated DNS Server IP addresses in the client-to-site template now works as expected. (BNNGF-35864)
- The **Product Tips** pop-up is no longer displayed after the **Status Map** of the Control Center has timed out. (BNNGF-33914)

Barracuda OS

- Updated BIND to fix the following security vulnerabilities: CVE-2015-8000, CVE-2015-8704, and CVE-2015-8705. (BNNGF-35608)
- 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)
- Updated time zones for Russia. (BNNGF-26258)
- Added i40e driver to support the Intel Ethernet Controller XL710 Family. (BNNGF-33357)
- Hardware pool licenses can now be applied to cold spares. (BNNGF-20758)
- Fixed hardware detection for devices using Realtek network chips. (BNNGF-35992)
- Cooking statistics no longer produces occasional **Corrupted Data File** errors. (BNNGF-22400)
- Updated NTP to fix security vulnerabilities CVE-2015-7704 and CVE-2015-7705. (BNNGF-35032)
- Fixed rare issue preventing controld from restarting services. (BNNGF-26689)
- Added IPFIX uniflow and biflow basic templates without Barracuda-specific information. (BNNGF-35904)
- Allow FQDNs as NTP servers. (BNNGF-26482)
- Updated OpenSSL to version 1.0.1q to fix several security vulnerabilities. (BNNGF-31109)
- Added uniflow support for IPFIX log collectors. (BNNGF-34653)
- Lifetime for protected IP addresses is now displayed correctly. (BNNGF-33206)
- The **build ART tree** option now works as expected when restoring the configuration from a PAR file. (BNNGF-34687)
- Added error message if **Save current config for ART** is triggered without root permissions. (BNNGF-33998)
- On the **Administration** page, added an option to the **Advanced View** to bind the ntp daemon to an IP address or interface. (BNNGF-34756)
- Counting protected IP addresses after an upgrade now works as expected. (BNNGF-35281)

Firewall

- IPv6 session state changes are now logged as expected. (BNNGF-32925)
- Custom block pages no longer cause package flooding when blocking services that reuse the same source and port for multiple destinations. (BNNGF-32831)
- 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)
- SSL Interception improvements to properly load some HTTPS sites. (BNNGF-35183)
- Active ONC-RPC now works as expected. (BNNGF-36162)
- IPv6 session sync now works as expected for HA clusters. (BNNGF-20271)
- Application detection now works as expected for Dropbox. (BNNGF-36366)
- Safe Search for Bing now works as expected. (BNNGF-35141)
- Improved application Detection without SSL Interception for HTTPS Applications. (BNNGF-29714)
- Virus scanning file transfers using active FTP now works as expected. (BNNGF-35476)
- DNS Blacklist checks now use the correct IP address for reputation lookups. (BNNGF-35977)
- 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)
- Shaping is now applied to synced sessions after a failover. (BNNGF22870).
- The Firewall Activity log now logs the correct port for HTTP traffic when cumulative logging is enabled. (BNNGF-34784)
- The Host Firewall now handles DNS objects as expected. (BNNGF-31042)
- URL Filtering in the Firewall is no longer selectable for Application Redirect access rules. (BNNGF-26064)
- Blocked ICMP packets are no longer logged twice if **Log ICMP Packets** is set to **Log-All**. (BNNGF-30357)

VPN

- The VPN device index is now used for all transports for a VPN tunnel configured via the GTI Editor. (BNNGF-35913)
- Added **Next Hop Routing** option for IPsec tunnels configured via the GTI Editor. (BNNGF-35432)
- IKEv2 tunnels no longer create multiple Security Associations. (BNNGF-34466)
- 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)
- Support for X.509 authentication for multiple, concurrent client-to-site VPN sessions by the same user. Note that this feature requires Barracuda Network Access Client 3.7 or higher and a valid Premium Remote Access subscription. (BNNGF-35671)

HTTP Proxy

- Updated SQUID to version 3.5.10 to fix several security vulnerabilities. (BNNGF-31849)

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

OSPF/RIP/BGP

- The OSPF service can now listen correctly on interfaces that were down when the service started. (BNNGF-35732)
- Advertising and learning multipath routes via OSPF now works as expected. (BNNGF-33355)
- Added option to send default route via BGP. (BNNGF-34823)
- Added option to configure **point-to-mulitpoint** OSPF connections. (BNNGF-34814)

Control Center

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

Mail Gateway

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

Azure

- Changing the password of the NextGen Firewall VM via the Azure web interface for Azure Service Manager (ASM) now works as expected. (BNNGF-33675)

Issues resolved by hotfixes

The following hotfixes have been released for firmware version 6.2.1

Hotfix 849 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Known Issues

6.2.1

- Azure: If the MAC Address of the network interface changes between the time the firewall is deployed until it is licensed via Barracuda Activation in a Control Center, the wrong MAC address is used to activate the license.

Miscellaneous

- VMware: Network interfaces using the VMXNET3 driver do not send IPsec keep alive packets unless TX checksumming is disabled for the interface (ethtool -K INTERFACE tx off).
- URL Filter: F-Series Firewalls running 6.2.0 or higher that are managed by a Control Center using firmware 6.0.X or 6.1.X must complete a dummy change in the security policy whenever enabling/disabling the URL Filter in the **General Firewall Settings**.
- Azure: After updating a firewall using Azure UDR via Azure Service Manager, the **Deployment Type** may be displayed incorrectly as **y**. This does not affect updating Azure UDR routes.
- SSL VPN: Some modern browsers such as Chrome and Firefox no longer support Java applets. Instead, use browsers with Java applet support, such as Internet Explorer or Safari.
- IKEv2: Disabling a site-to-site tunnel on the **VPN > Site-to-Site** page is not possible.
- IKEv2: Changing a setting for an IKEv2 tunnel disabled in the configuration causes all active IKEv2 tunnels to initiate a re-keying.
- IKEv2: Client certificate authentication for client-to-site IKEv2 IPsec VPNs requires **X509 Certificate** to be enabled in the **VPN Settings**. Enabling this setting requires all VPN group policies to use client certificate authentication.
- IKEv2: After a restart, the **Last Access** and **Last Duration** time displayed for site-to-site IKEv2 IPsec tunnels is not reset.
- IKEv2: Using a hostname or subnets as **Remote Gateway** is currently not possible.
- IKEv2: Using pre-shared keys with IKEv2 client-to-site VPNs is not possible.
- IKEv2: Using X509 Subject Policy in a client-to-site **Group VPN Settings** is not possible.
- IKEv2: Changing client-to-site minimum and maximum lifetime values has no effect.
- IKEv2: Connecting to an IKEv2 IPsec client-to-site VPN using iOS or Android devices is not possible.
- IKEv2: You can only use MSAD authentication schemes for client-to-site IKEv2 IPsec VPNs.
- Azure Control Center: On first boot "fatal" log messages may occur because master.conf is missing. These log messages can be ignored.
- IKEv1 IPsec: When using 0.0.0.0 as a local IKE Gateway, you must enable **Use IPsec Dynamic IPs** and restart the VPN service before a listener on 0.0.0.0 is created.
- HTTP Proxy: Custom block pages do not work for the HTTP Proxy when running on the same NextGen F-Series Firewall as the Firewall service. This issue does not occur when running the HTTP Proxy service on a second NextGen F-Series Firewall behind the NextGen F-Series 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.
- VPN Routing: When a duplicate route to an already existing VPN route in the main routing table is announced to the NextGen Firewall F-Series 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 Control Centers deployed using Barracuda F-Series 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.
- Barracuda NextGen 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 and Virus Scanning: Data Trickling is only done while the file is downloaded, but not during the virus scan. This may result in browser timeouts while downloading very large files.
- Application Control and Virus Scanning: If the Content-Length field in HTTP headers is missing or invalid, the **Large File Policy** may be ignored.
- Application Control 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 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 a 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.
- Global File Content, User Agent, and Schedules objects are not available as cluster and range objects.