6.2.4 Release Notes

https://campus.barracuda.com/doc/73701241/

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.

Changelog

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

- 2017-11-29 – Release Hotfix 858 – Firewall service stability improvements.
- 2018-05-16 – Release Hotfix 873 – Fixes the security vulnerability CVE-2018-10115 in 7zip

In These Release Notes:

- Back up your configuration.
- The following upgrade path applies: **5.0 > 5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2.4**
- Before updating, read and complete the migration instructions.

For more information, see Migrating to 6.2.4.

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 6.2.4 Migration Notes.

What´s New in Version 6.2.4

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

Improvements Included in Version 6.2.4

Barracuda NextGen Admin

- NextGen Admin now supports virtual DPI scaling for high-resolution displays. BNNGF-48005
- Copy from default with a **Send Changes** and **Activate now** writes the default values correctly into the configuration file without requiring an additional configuration change. BNNGF-46249
- NextGen Admin now shows IPsec local / remote network settings as expected. BNNGF-45097
- Admins can now delete an entire cluster regardless of existing server references. BNNGF-45322
- NextGen Admin now shows more informative error messages if the files for the **Firmware Update** element could not be downloaded. BNNGF-44095
- Very long TXT DNS record entries are no longer truncated in NextGen Admin. BNNGF-43417
- Adding or removing interfaces that are part of a bridged interface now works as expected. BNNGF-43407
- The certificate dialog in NextGen Admin now displays the correct expiration date and fingerprint. BNNGF-39201
- Using the Im/Export certificate button in NextGen Admin now works for certificate chains. BNNGF-32287
- When a **Range Properties** or **Cluster Properties** node is locked, selecting **Copy From Default** is no longer possible. BNNGF-41375
- Connection loss during PAR file creation no longer results in an empty PAR file. BNNGF-43909
- Cluster and range firewall objects are now automatically refreshed when opening the configuration dialog. BNNGF-46288
- Using link override for repository-linked default boxes in a cluster now keeps this information when firewall configuration are created from the default box. BNNGF-40444
- Resolved issue causing NextGen Admin to fail when managing multiple firewalls and Control Centers. BNNGF-44892
- Changed the label of the **Listening IP** drop-down list to **Use Transport Source** instead of **default-from-My-IP**. BNNGF-44618
- On the **FIREWALL > Users** page, double-clicking on a user now displays a formatted list of groups. BNNGF-45817
- The option **Copy From Default** is no longer available for **Server Properties** or **Service Properties** nodes. BNNGF-22790
- Access Control Service Allowed Client Versions can now also match on NAC 4.0 clients. BNNGF-45220
- On the **DASHBOARD** page in the **Recent Severe Events** element, events with invalid dates no longer cause NextGen Admin to crash. BNNGF-44234
- Changing password on first login in NextGen Admin now works as expected. BNNGF-44771
- The textbox in the network activation window is wide enough for data entry. BNNGF-44426

Barracuda OS

- Setting the **Max Session Source Accounting Objects** in the **General Firewall Settings** to a

non-zero value no longer causes errors when loading the ACPF kernel module. BNNGF-47622
- Updated Linux kernel to fix security vulnerabilities CVE-2016-10229 and CVE-2017-6214. BNNGF-45808
- Resolved logic error in the configuration process that could allow an attacker to gain unauthorized, low-privilege access to the NextGen Firewall via the management IP addresses. BNNGF-48134
- Local out (LOUT) IPv6 sessions on port 636 are now terminated correctly. BNNGF-46877
- The firewall no longer crashes if more than 250 VLANs are configured. BNNGF-46702
- Logging into ART via SSH now works as expected for firewall models with more than one network card. BNNGF-47275
- ART rescue installation now works as expected for F800 and F900. BNNGF-43060
- Changed the maximum number of concurrent connections to the firewall authentication daemon to 1020 connections. BNNGF-47067
- ONCRPC Firewall plugin stability improvements. BNNGF-46256
- Adding multiple pool licenses to an Access Concentrator now works as expected. BNNGF-42774
- Hardware firewalls using flash storage no longer write core files, because these would fill up the limited storage on the firewall. BNNGF-44597
- 2-factor authentication with OTP now works as expected. BNNGF-44128
- The values for maximum session slots for some hardware models have been adjusted. BNNGF-43667
- Authentication from Aerohive Wi-Fi appliances now works as expected. BNNGF-43384
- TCP window size for syslog streaming is now set correctly. BNNGF-45814
- Corrected time zone for Europe/Istanbul. BNNGF-44151
- Updated e1000e driver to version 3.3.5.3 to solve issue causing the interface to become unresponsive after a reset. BNNGF-44205
- Retransmissions from the server no longer cause some websites to not load when virus scanning is enabled. BNNGF-44273
- Update **Root DNS** network object to include the the current DNS root servers. BNNGF-38070
- Memory management improvements have been added for the **Access Control** service. BNNGF-36173
- Resolved issues where a **Login master from X.X.X.X: unkown user** event was triggered every hour on the passive firewall in a high availability cluster. BNNGF-35824
- The list of available time zones is now identical for all firewall service configurations. BNNGF-44482
- In some cases, Report Creator reports filtering for exactly one destination are empty. BNNGF-43852
- Interface names are now mapped correctly from the Defaults file for port names. BNNGF-49478
- Traffic shaping no longer fills up when bandwidth limit is not reached. BNNGF-44340

Firewall

- File scanning results from the Avira virus scanning engine that contain multiple result messages are now interpreted correctly. BNNGF-42674
- Files in the Virus Scanner quarantine are now purged on a hourly and size basis.

BNNGF-45303

- Skype Audio is now detected without a preceding SSL dummy handshake. BNNGF-43091
- It is now possible to detect the TOR browser 6.5 using Application Control. BNNGF-44075
- SSL Interception now handles connections where the MTU/MSS size is smaller than the default correctly. BNNGF-48135
- Internal IPS rules are now included in the IPS signature list. BNNGF-43544
- Risk-level overrides for applications now work as expected. BNNGF-24640
- Using IPS in **Report Only** mode for IPv6 traffic now works as expected. BNNGF-23520
- Application Provider Selection improvements for applications using SNI in the TLS 1.2 handshake. BNNGF-45975
- Copying MAP access rules between different rule lists no longer changes the connection object. BNNGF-46090
- Configuring weights between 1 and 100 for source-based multi-path routes now work as expected. BNNGF-46324
- Rules with Firewall History Entry set to No in the Advanced Settings are no longer displayed in the **FIREWALL > History** page. BNNGF-45900
- Trend Micro AV updates are now detected correctly by Application Control. BNNGF-41169
- Multiple stability improvements for the URL Filter service. BNNGF-48972
- Firewall service stability improvements. BNNGF-48225

ATP

- Scanning large archives via ATP no longer causes a high CPU load. BNNGF-45761
- ATP email notifications are now sent via plain-text emails. BNNGF-44080

SMTP

- The SMTP for sending email notifications can now handle multiple responses. BNNGF-45798

VPN

- Resolved issue causing the second column of the VPN Server Settings to be invisible. BNNGF-46515
- Fast reconnect for TINA VPN tunnels now works as expected. BNNGF-45741
- Solved issue with the IKEv1 daemon causing the VPN service to fail. BNNGF-40960
- In **VPN > Site-to-Site**, a Dynamic Mesh does not display a VPN tunnel to itself any more. BNNGF-45073
- Performance improvements for VPN tunnels on Ethernet bundles (bond) interfaces running on NextGen Firewall hardware models using the igb driver. BNNGF-42808
- The GTI Editor no longer allows VPN tunnels to have both Dyn Mesh and WAN Optimization enabled. BNNGF-44805
- Upgrading to 7.1.0 no longer causes VPN traffic to be missing from the IPFIX flow. BNNGF-44308
- It is now possible to use network mapping for the S-Series VIP networks. BNNGF-41924
- Client-to-site VPN connections using SHA2 certificates in combination with password authentication now work as expected. BNNGF-42586

- Memory handling improvements for IPsec IKEv1 tunnels in the VPN service. BNNGF-44360
- A fast reconnect now works as expected for routed VPN tunnels. BNNGF-44931

Control Center

- Control Center license updates for managed firewalls no longer fails due to a failed lock on the license configuration node. BNNGF-40233
- Upgrading a pool license no longer requires a manual reassignment of the pool licenses. BNNGF-44277
- The CC Syslog service now works as expected when UDP is configured as the **Supported Protocol**. BNNGF-44632
- In the Control Center, performance improvements have been made to display status maps. BNNGF-45011
- Updating pool licenses no longer deletes the license comment. BNNGF-42442
- Entering email addresses in the CC Wizard now works as expected. BNNGF-44288
- Using an Explicit CC IP address in **Box Properties** no longer breaks syslog streaming to the Control Center. BNNGF-34556
- In the **Activate** tab, Secure Access Concentrators are now displayed correctly after adding VACC licenses. BNNGF-45749

DHCP Server

- DHCP requests are now passed to the DHCP server if a bridge is configured. BNNGF-31658
- Setting the Max, Min, and Default lease times in the DHCP lease configuration is now mandatory. BNNGF-46098

DNS

- Creating DNS SRV records containing an underscore character now works as expected. BNNGF-44193
- DNS slave zones are now processed correctly even if multiple DNS masters are configured. BNNGF-44937
- Using underscores in DNS zones now works as expected. BNNGF-44153
- The DNS suffix parameter no longer accepts multiple comma-separated values. BNNGF-43488

WiFi

- The security issue to protect against the WPA2 vulnerability (KRACK attack) has been resolved. BNNGF-49766

Issues Resolved by Hotfixes

Hotfix 858 – Firewall service stability improvements

- Stability improvments to the Firewall service, to fix an issue causing a kernel panic when the traffic stream matches the Viber messaging platform pattern.

Known Issues

6.2.4

- Transferring data over configured VLAN interfaces of a NextGen Firewall F180 or F280b can fail even if the MTU size is changed. BNNGF-46289

Miscellaneous

- Web Security Gateway authentication schemes are currently not working. (BNNGF-45113)
- NextGen Firewall F10 Rev A: It is currently not possible to install a Barracuda NextGen Firewall F10 Rev A via F-Series Install. Install 6.2.2 and upgrade to 6.2.4 instead. (BNNGF-43579)
- In some cases, Report Creator reports filtering for exactly one destination are empty.
- NextGen Admin: Activating a license can take up to 30 seconds, during which time the window seems unresponsive before the activation is completed. Use NextGen Admin version 7.0.0 or higher instead. (BNNGF-41343)
- NextGen Admin: It is possible to configure IPsec site-to-site tunnels on firewalls running 6.2.0 to use the ID type IPV4_ADDR_SUBNET (explicit), even though this is not supported. The IPsec tunnel cannot be established.
- IKEv2: When using a subnet as the remote gateway, you must configure an ID type.
- 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.
- VMware: Network interfaces using the VMXNET3 driver do not send IPsec keepalive 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 **X.509 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 X.509 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.
- SafeSearch: In some cases, YouTube safety mode does not work when logged in with a Google account.
- SafeSearch: If SafeSearch 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.
- ATP: 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.