6.2.3 Release Notes

https://campus.barracuda.com/doc/71862714/

This firmware version is affected by 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) > 6.2.3**
- Before updating, read and complete the migration instructions.

For more information, see 6.2 Migration Notes.

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 6.2.3

- Hotfix **818** – Control Center
- Hotfix **813** – DNS Server
- Hotfix **810** – SSL VPN
- Hotfix **805** – Cumulative Hotfix
- Hotfix **802** – HTTP Proxy
- Hotfix **800** – OpenSSL

What´s new in Version 6.2.3

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

Improvements included in Version 6.2.3

Barracuda NextGen Admin

- The **FIREWALL > Monitor** page now no longer crashes if an element is selected that is not supported by the firmware. BNNGF-40884
- Editing application rules with a large number of applications no longer causes NextGen Admin to crash. BNNGF-41417
- Firewall throughput exceeding 30 Gbps is now displayed correctly on the **FIREWALL > Live** page. BNNGF-36450
- Filtering IPv6 connections by their destination interface on the **Firewall > Live** and **Firewall > History** pages now works as expected. BNNGF-37137
- NextGen Admin is no longer supported for Windows Vista. BNNGF-41630
- NextGen Admin automatic session reconnection improvements. BNNGF-43601
- **Available IPs** in the **Service Properties** are now displayed correctly if the **Secondary IP** in the **Server Properties** is left empty. BNNGF-22643
- Full-screen command line apps are now displayed correctly in the NextGen Admin SSH tab. BNNGF-11234
- A warning is shown when connecting to a firewall running a newer firmware than is supported by this version of NextGen Admin. BNNGF-39095
- NextGen Admin dashboard stability improvements. BNNGF-42232
- IPv6 ICMP traffic no longer shows the ICMP identifier as the port on the **FIREWALL > Live** and **FIREWALL > History** pages. BNNGF-31417
- It is no longer possible to create or edit connection objects in the Host Firewall object viewer. BNNGF-29380
- Copying application rules using a custom application object to another ruleset now works as expected. BNNGF-39965
- The **Max Entries** setting on the **FIREWALL > History** page is now honored immediately without a manual refresh. BNNGF-41383

- The status icon of the **CONTROL > Network** page no longer displays an incorrect status after dynamic routing changes. BNNGF-30769
- NextGen Admin no longer cuts off the **Phase 2 lifetimes** in the site-to-site IPsec configuration dialog. BNNGF-42321
- **Networks** in the GTI Editor are no longer shown in phion (reverse CIDR) notation. BNNGF-41357
- The time stamp for the last successful IPS update is now displayed correctly. BNNGF-42374
- RDP clients using the Touch API to emulate the right-click now work as expected for NextGen Admin. BNNGF-27845
- When a service is restarted, the name of the service is now included in the log message. BNNGF-40650
- 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
- Updated the icon for the URL Filter policy action alert. BNNGF-43320
- IPS exception attributes are no longer replaced by wildcards when the IPS pattern for the exception has been removed by an IPS signature update. BNNGF-40600
- Sorting the user column in Grouped By User mode on the **FIREWALL > User** page now works as expected. BNNGF-39618
- Sorting the applications browser by risk now works as expected. BNNGF-42377
- If the user information is available, usernames are now displayed for firewall connection cache entries on the **FIREWALL > History** page. BNNGF-39617
- The error dialog warning stating that local changes have not been sent now includes the relevant configuration nodes. BNNGF-40010

Barracuda OS

- 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
- Updated Wi-Fi kernel module to fix security vulnerability CVE-2014-2672. BNNGF-40703
- Firewalls and Control Centers using legacy phion licenses no longer receive IPS pattern updates. BNNGF-42195
- Firewall session sync between firewalls running 5.4 and 6.0 now works as expected. BNNGF-40900
- IPv6 router advertisements and link local address computation now work as expected. BNNGF-38442
- Updated libCURL to fix several security vulnerabilities. BNNGF-42747
- A rare case where the authentication service causes system crashes is fixed. BNNGF-43285
- Updated BIND to version 9.9.9-P4 due to security vulnerability CVE-2016-8864. BNNGF-43010
- Event 2045 Entering Grace mode is now triggered correctly when the license enters Grace mode. BNNGF-41064
- Web Log streaming now works as expected for HTTPS sessions when no additional Application Control features are enabled in the access rule. BNNGF-41274
- Kernel memory management improvements. BNNGF-39854

- Session sync in a high availability cluster no longer blocks services starting after a failover. BNNGF-40050
- F-Series Install can now use encrypted PAR (PCA) files. BNNGF-40064
- It is no longer required to restart the authentication service when configuring DC agent / DC client authentication. BNNGF-41689
- It is now possible to enter a hostname as the NTP server. BNNGF-38950
- The default ruleset now includes a service object and rule for Barracuda ScreenConnect. BNNGF-40180
- Added support for the **Aruba Instant** Wi-Fi access points to the Wi-Fi authentication scheme. BNNGF-37349
- Corrected the portmapping for the Barracuda NextGen Firewall F1000. BNNGF-42285
- Changed naming for RSA ACE authentication prompts to match official naming for SecurID. BNNGF-36838
- Logging into the ART menu via SSH key now works as expected. BNNGF-30782
- Modified help text to state that user authentication objects using NTLM/ MS-CHAP authentication must enter the username as follows – **DOMAIN\user**. BNNGF-41070
- The trust level for the **Additional IPs** is added to the respective network objects as expected. BNNGF-30560

Firewall

- Application Control statistics now work as expected when the **Maximum sessions** in the **General Firewall Settings** are set to a high value. BNNGF-39474
- Improved session handling of the firewall service to fix random system crash. BNNGF-38163
- In rare cases, virus scanning FTP traffic caused a firewall lockup. This no longer occurs. BNNGF-41082
- Schedule objects with a large number of objects (>128) now work as expected. BNNGF-40857
- Inline firewall authentication now uses a browser authentication pop-up window by sending 401 unauthorized, and no longer redirects to the login page. BNNGF-40979
- Firewall ruleset re-evaluations no longer terminate sessions matching rules using hostname network objects. BNNGF-40353
- SSL Interception now works as expected for clients using the TLS certificate status request extension (OCSP stapling). BNNGF-41451, BNNGF-41093, BNNGF-41413
- Memory consumption improvements in the Firewall service request handler. BNNGF-36793
- A system crash caused while evaluating a session in the Firewall service no longer occurs. BNNGF-32923
- SSL Interception now works as expected when a TCP window update is sent after the TCP handshake. BNNGF-37275
- Using the skinny firewall plugin in a high availability cluster no longer causes a system crash. BNNGF-42090
- Custom block pages no longer cause package flooding when blocking services that reuse the same source and port for multiple destinations. BNNGF-42472
- DHCP requests are no longer intermittently dropped when sent over a bridged interface. BNNGF-40262
- Improved user agent detection for browsers on Android devices. BNNGF-40067
- It is now possible to use transparent redirect in combination with Application Control features.

BNNGF-40384

- The firewall no longer crashes when manually terminating sessions using WAN Optimization via command line interface. BNNGF-39730
- Unusual HTTP trailing header fields are now handled correctly. BNNGF-40200
- For layer2 bridges it is now possible to disable decrementing the ICMP TTL in the advanced access rule settings. By default, the ICMP TTL is decremented when passing through the layer2 bridge and a ICMP type 11 reply sent if the TTL equals zero. BNNGF-41220
- Using same port in a connection object using the translated source IP from the DHCP interface now works as expected. BNNGF-38814
- Handling and matching for user objects containing users in many different groups is improved. This no longer causes the access rule to not match. BNNGF-43511
- Internet Explorer 11 on Windows 10 is now detected by User Agent Filtering. BNNGF-40690
- A leading **/** (forward slash) in the URL path of a custom application object no longer causes the URL to not match. BNNGF-40052
- The **Portmapper** service object now uses the ONRPC firewall plugin. BNNGF-36160
- It is now possible to use numbers in the name of a **Trusted root certificate** in the SSL Interception configuration. BNNGF-32428
- The default connection object names are renamed to match the **Translated IP** policy names. BNNGF-39803
- It is now possible to edit the **IPS** or **Traffic Shaping** settings of multiple access rules at once. BNNGF-38788
- Cloned custom application objects now have a unique name. BNNGF-40051
- Block page delivery improvements. BNNGF-41440
- The firewall loopback traffic on port 9023 is no longer sent out on a different interface. BNNGF-40381
- Application Control HTTP parses improvements to be able to detect Facebook file transfers. BNNGF-38975
- Broad-Multicast rules no longer use Application Control. BNNGF-29188
- Hostname network objects not using an FQDN are now resolved correctly. BNNGF-35815
- Traffic Shaping for bi-directional access rules using QoS Band (Reply) set to Like-Fwd now works as expected. BNNGF-36372
- Firewall statistics for UDP traffic now work as expected. BNNGF-42153
- Custom connection objects can now use the same port in combination with load balancing or failover settings. BNNGF-32672
- Local networks configured as direct attached routes and with a virtual server IP address are now added to the **local network** network object. BNNGF-36290
- Updated list of DCERPC codes. BNNGF-39881
- For access rules matching on the VPN username, the user is now displayed in the **FIREWALL > Live** and **History** pages as well as in the firewall logs. BNNGF-29581
- Kaspersky Endpoint Security pattern updates are now detected correctly by Application Control. BNNGF-41071

URL Filter

- **Time stamps** in URL Filter log messages now use the configured time zone. BNNGF-40183

Virus Scanner and ATD

- Improved ATD file queue handling. BNNGF-40831
- Renaming executable files to file types not scanned by ATD no longer allows you to bypass the ATD scan. BNNGF-40350
- ClamAV freshclam fallback update method is now disabled by default. **Legacy licensed firewalls must enable freshclam updates manually.** BNNGF-42234
- Executable archives are now detected and handled correctly when scanned by ATD. BNNGF-41024
- It is now possible to add exceptions to the virus-scanned MIME types by entering the exempted MIME type with a prepended "!" in the **Scanned MIME Types on the Security Policy** page. E.g., !application/mapi-http BNNGF-43070
- The **<factory-default-mime-types>** now include all **application/*** MIME types. BNNGF-41376
- It is now possible to run the HTTP Proxy as a reverse proxy on a non-standard port in combination with the **scan first, then deliver** ATD policy. BNNGF-39655
- Manually deleting ATD files from the **Scanned Files** or **Malicious Files** tabs now marks them as deleted in the **Top Threats** dashboard element. BNNGF-39915
- It is no longer possible to manually quarantine mail attachments scanned by ATD to avoid the mail server IP address from being placed in quarantine. BNNGF-39476

SNMP

- IPsec tunnel states are now correct in the box level SNMP service. BNNGF-40965

VPN

- Mitigated a hardware-related bug resulting in soft lockups on Barracuda Control Center C400. BNNGF-41683
- The WAN Optimization deduplication process no longer crashes if a large number of sessions are using WAN Optimization. BNNGF-39729
- Increased the maximum number of sessions for WAN Optimization. BNNGF-40787
- Added option to disable Replay Protection for IPsec IKEv1 site-to-site VPN tunnels by setting the Replay Window Size to -1. BNNGF-38991
- IKEv2 VPN tunnels configured on an older firmware version no longer break when the firmware is updated. BNNGF-40611
- Client-to-site VPN connections with the native Android IPsec VPN client now work as expected. BNNGF-36486
- Client-to-site certificate policies OID matching improvements. BNNGF-38545
- Renamed **Server Key** to **Service key** in the client-to-site personal license configuration dialog. BNNGF-42419
- The label of the **Name** column in the client-to-site **VPN Clients Downloads** section is now changed to **Description** to match the **Upload** dialog. BNNGF-43206
- It is now possible to click **Send Changes** without a dummy change when importing client-to-site profiles. BNNGF-42278

SSL VPN

- Authenticating multiple users via NTLM for web forwards now works as expected. BNNGS-2356
- POST requests now work on WebApps that use SSO NTLM authentication. BNNGS-2609

HTTP Proxy

- Updated HTTP Proxy to fix connection error handling. BNNGF-41846
- Kerberos authentication now works as expected with the HTTP Proxy service. BNNGF-41625
- It is no longer possible to enter the **Visible Hostname** as an **Additional Backend domains** entry. BNNGF-39874
- Protected IP addresses for the HTTP Proxy in Reverse Proxy mode are now counted correctly. BNNGF-31773
- **ssl_bump server-first** is now replaced by **peek-n-splice** in the HTTP Proxy. BNNGF-37732

OSPF/RIP/BGP

- Multipath BGP routes handling improvements. BNNGF-43378
- The **split-horizon** parameter is now written to the RIP configuration file correctly. BNNGF-42843
- Routes learned via OSPF or BGP are now removed immediately if the associated interface goes down. BNNGF-40927
- Allow other interfaces in RIP filter configuration. BNNGF-35502

Control Center

- Improved error handling for file and pattern updates of managed firewalls. BNNGF-42756
- Updating patterns and definitions for a large number of managed firewalls no longer overloads the Control Center. BNNGF-42828
- Deleting a managed firewall on the Control Center while it is still referenced by a virtual server now displays an error message. BNNGF-40378
- CC VPN service memory consumption improvements. BNNGF-43392
- CC Admins can no longer see file updates for firewalls out of their administrative scope. BNNGF-38799
- Non-local references for global, range, and cluster network objects are no longer removed when the object is renamed. BNNGF-40370
- Site-specific single IP address network objects now work as expected in the distributed firewall service. BNNGF-39118
- CC-Data-Receiver (mdist2) service stability improvements. BNNGF-37964
- Pattern updates for ranges where all managed firewalls use the distributed firewall service now work as expected. BNNGF-42907
- Enabling the URL Filter is now shown correctly in RCS. BNNGF-40534
- A new range is now displayed immediately in the configuration tree before activating the changes. BNNGF-26668
- Deleting an **Update Task** after the transfer has been completed now also removes the file from the firewall. BNNGF-38906
- File content, user agent, and schedule objects can now be configured as global, range, and

cluster objects. BNNGF-36850
- It is no longer possible to select **NG Control Center** as the platform when creating a new managed firewall on the Control Center. BNNGF-32353
- A new cluster is now displayed immediately in the configuration tree when creating a new cluster with an activation template. BNNGF-38703
- For Control Center high availability clusters, the syslog format no longer differs when the virtual server fails over the the secondary Control Center. BNNGF-39917
- Corrected the UI text to be displayed when no product tips are available. BNNGF-42129
- The Wi-Fi configuration is now included in the **Box Network Repository** entry. BNNGF-39824

Wi-Fi

- Running multiple Wi-Fi services on Wi-Fi-enabled firewall models now works as expected. BNNGF-40173

DHCP Server

- The **BOOTP lease time** is now handled correctly in the DHCP server configuration files. BNNGF-33394
- DHCP reservations can now use any IP address in the **Used Subnet** and no longer have to be outside of the DHCP pool range. BNNGF-40352

Public Cloud (AWS/ Azure)

- XML parsing errors for **IP Forward protection** in Azure no longer occur. BNNGF-42117

FSC-Series

- It is no longer possible to change the S-Series VIP network on the Secure Access Concentrator VPN service. BNNGF-39936
- After deleting and re-creating an S-Series VIP network, the correct CIDR network is used. BNNGF-40348
- It is no longer possible to unlock the SC Editor before activating changes. BNNGF-39910
- Removed **DES** and **NONE**, and set the default encryption to AES256 for SC VPN. BNNGF-40435
- Deleting a cluster now also removes the configuration for the SCs in the cluster. BNNGF-40654
- It is now possible to explicitly set the Wi-Fi channel used by the SC. BNNGF-40062
- Attempting to create an invalid S-Series VIP network no longer results in a disconnect. BNNGF-41208
- **Copy from Default** now works as expected for S-Series VIP Networks and SC Editor configuration nodes. BNNGF-41048
- Removed the **VPN** column from the SC Editor. BNNGF-40502
- SCs created from a template now have default values. BNNGF-39776
- It is now possible to use network mapping for the S-Series VIP networks. BNNGF-41924

Issues resolved by hotfixes

The following hotfixes have been released for firmware version 6.2.3

Hotfix 849 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Known Issues

6.2.3

- 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 6.2.3 instead. (BNNGF-43579)
- In some cases Report Creator reports filtering for exactly one destination are empty.

Miscellaneous

- 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 **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.