6.2.2 Release Notes

https://campus.barracuda.com/doc/71862717/

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) > 6.2.2**
- 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 6.2.2

- Hotfix **784** – CC Database
- Hotfix **779** – Secure Access Concentrator and Control Center
- Hotfix **777** – Cumulative Hotfix
- Hotfix **771** – Wi-Fi Service
- Hotfix **770** – Dynamic Routing
- Hotfix **773** – SSL VPN
- Hotfix **765** – DNS Server
- Hotfix **762** – HTTP Proxy
- Hotfix **753** – SSLv2
- Hotfix **752** – Realtek Network Interfaces
- Hotfix **748** – glibc

What´s new in Version 6.2.2

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

Improvements included in Version 6.2.2

Barracuda NextGen Admin

- Configuring VPN Firewall rulesets now works as expected. (BNNGF-38858)
- The **Message Board** is no longer missing an entry. (BNNGF-36584)
- Added **Shared Secret** input validation to check for invalid characters in the IPsec site-to-site configuration dialog. (BNNGF-37984)
- Added input validation to disallow pound signs ('#') in password fields. (BNNGF-37737)
- The **Settings** section is now visible when editing firewall objects. (BNNGF-36918)
- Improved the port speed indicator in the DASHBOARD > Port element, that, in some cases, showed incorrect information. (BNNGF-36663)
- You can now edit the LDAP request timeout by editing the Windows registry setting **DWORD SessionLoginTimeout** in **HKEY_CURRENT_USER\Software\Barracuda\ngadmin\Settings**. (BNNGF-36559)
- Invalid IP addresses in the source and destination are no longer dropped silently when creating an IPS exception. (BNNGF-36509)
- Filtering for **IPS Severity** in the **FIREWALL > Monitor** now works as expected. (BNNGF-36469)
- NextGen Admin no longer crashes when logging in to a Control Center and the CC Admin has no permission for **CC Configuration Module** > **Access to CC Config**. (BNNGF-36038)
- Cloning a connection object with a reference to a network object now works as expected.

(BNNGF-38459)

Barracuda OS

- Hardware pool licenses are now also valid for the direct predecessor of the model they are issued for. E.g., F80 pool licenses are also valid on F100/101. (BNNGF-37618)
- Update glibc library to version 2.9-5 to mitigate potentially remote code execution via specially crafted DNS response messages: CVE-2015-7547. (BNNGF-36717)
- Improvements to the IPFIX uniflow templates. (BNNGF-37086)
- IPFIX intermediate reports are now sent reliably. (BNNGF-36887)
- Updates BIND to version 9.9.8-p4 to fix the following security vulnerabilities: CVE-2016-1285, CVE-2016-1286, and CVE-2016-2088.(BNNGF-37217)
- Forcing network interfaces using 8169.ko module to manually set speed and duplex settings now works as expected.(BNNGF-28066)
- Corrected help text for DNS Interception. Wildcards are not supported. (BNNGF-36230)
- Updated 7zip to be able to extract v5 RAR files. (BNNGF-37391)
- The primary firewall in a high availability cluster now successfully downloads the licenses for the secondary firewall. (BNNGF-24200)
- Update packages are now detected correctly by the **Firmware Update** element. (BNNGF-36299)
- CC admins can now log in via SSH when TACPLUS authentication is used. (BNNGF-37442)
- IPFIX log streaming with intermediary reports no longer causes high system load. (BNNGF-34016)
- The license state is no longer invalid when one firewall in an HA cluster is replaced with its direct successor. (BNNGF-37136)
- Monitoring routes with **Reachable IPs** now works as expected. (BNNGF-37128)
- Importing AES configuration from RSA version 8.1. P5 or higher now works as expected. (BNNGF-34621)
- IP addresses where all four segments use 3 digits can now be entered via LCD. (BNNGF-29888)
- VMware images now use **dynmod** as the default networking driver. (BNNGF-35781)
- Default keyboard layout for NextGen Install F installations set to **us**. (BNNGF-37159)
- Updated ixgbe.ko to version 4.3.13 module to fix issue after reboot. (BNNGF-38080)
- Activating pool licenses no longer overwrites the serial number of the Control Center. (BNNGF-36485)

Firewall

- Creating a self-signed certificate in the Security Policy now works as expected. (BNNGF-38006)
- Sessions now sync correctly in an HA cluster between firewalls. (BNNGF-37024)
- MIME headers containing digits are now parsed correctly. (BNNGF-37724)
- Fixed race condition between the traffic shaping and routing subsystems. (BNNGF-38048)
- The IPS now works as expected when scanning SSL Intercepted traffic. (BNNGF-35440)
- Renamed **Inline Authentication** to **Inline Authentication for HTTP and HTTPS** in the advanced access rule settings. (BNNGF-36589)
- Disabling SSLv2 for the firewall authentication web interface now disables the SSLv2 protocol, not just SSLv2 ciphers. (BNNGF-36979)

- Added support to scan HTTP and HTTPS connections using chunked transfer encoding. The **Stream Scanning Buffer** can be configured in the **Advanced Virus Scanner Settings** on the **Security Policy** page. (BNNGF-37938)
- SMTPS on port 465 is no longer scanned if virus scanning for SMTP/SMTPS is disabled. (BNNGF-36953)
- The feature level of the firewall service is now limited to the cluster version instead of the firmware version of the Control Center. (BNNGF-38254)
- URL Filter block pages are no longer partially delivered. (BNNGF-35578)
- In rare cases, **Block Other Session Limit Exceeded** would occur for non-TCP traffic without having exceeded the limit. This is now handled correctly. (BNNGF-36808)
- The firewall no longer freezes in rare cases and requires a manual reboot. (BNNGF-36816)
- Improved URL categorization for SSL-intercepted hosts. (BNNGF-35450)
- Configuring Traffic Shaping in the GTI Editor with the **shape on output interface** option now works as expected.(BNNGF-36548)
- SSL Interception with certificates chains now works as expected. (BNNGF-38655)
- SMTPS added to **Any-Email** service object. (BNNGF-34998)
- The default **DNSBL** server is now set to **b.barracudacentral.org**. (BNNGF-36773)
- The skinny plugin now works with Cisco Call Manager. (BNNGF-32217)
- FWD Firewall statistics now work as expected. (BNNGF-36005)
- IPS now logs the correct **action state** in the threat log. (BNNGF-34323)
- IPv6 rulesets using network objects with references now work as expected. (BNNGF-37111)
- File Content policy now detects HTML5 video content. (BNNGF-37277)
- Guest ticketing now supports setting a maximum time limit for guest tickets. Ticketing admins cannot create tickets exceeding this limit. (BNNGF-35797)
- Resolving a large number of hostname network objects now works as expected. (BNNGF-35963)
- acpfctrl monitoring now works as expected. (BNNGF-36754)

URL Filter

- Added **Learning Management Systems** category to the URL Filter. (BNNGF-37457)

Virus Scanner and ATD

- The **FIREWALL > ATD** page now shows the recipient and subject of the email containing the malicious mail attachment. (BNNGF-36959, BNNGF-37148)
- Added support to scan RTF files with ATD. (BNNGF-38150)
- ATD can now use a configured system proxy for the upload to the Barracuda ATD Cloud. (BNNGF-36738)
- Infected mail attachments are now stored in the quarantine folder on the firewall. (BNNGF-37336)
- Updated ClamAV to version 0.99 to fix several security vulnerabilities. (BNNGF-35441)
- Files using HTTP content type of chunked encoding are now scanned by the virus scanner and ATD. (BNNGF-37692)
- Added PUA configuration option for ClamAV virus scanning engine with exceptions for win32packer and Block OLE2 Macros. (BNNGF-37177)

VPN

- Creating IPsec tunnels with two different ID types where one of them is IPV4_ADDR now works as expected. (BNNGF-37020)
- IPsec tunnels with explicit IPV4_ADDR_SUBNET ID types are now handled correctly. (BNNGF-35720)
- The VPN hub now correctly detects if the remote VPN service is restarted and automatically removes the dynamic tunnels. (BNNGF-35968)
- Terminating and initiating a TINA tunnel using **Null** cipher with **PFS** now works as expected. (BNNGF-38310)
- VPN service no longer crashes if the IPsec key length is not set correctly. (BNNGF-37133)
- IKEv1 IPsec site-to-site tunnels now use the negotiated NAT-T proposal from phase 1 in phase 2. (BNNGF-36933)

HTTP Proxy

- Update squid to version 3.5.19 due to the following security vulnerabilities: CVE-2016-4555, CVE-2016-4556, CVE-2016-4554, CVE-2016-4553 and SQUID-2016:3+4+5+6 (BNNGF-37828, BNNGF-38384, BNNGF-36855)
- The default deny-all ACL is now also applied to the reverse proxy. (BNNGF-30773)
- The reverse proxy now works as expected. (BNNGF-36818)
- Statistics for HTTP Proxy now use correct destination entries. (BNNGF-36962)
- Using **Partial Search** in **Group ACL** no longer causes the HTTP proxy to crash on startup. (BNNGF-36638)
- The virus scanning block page now shows correct URL for FTP over HTTP Proxy connections. (BNNGF-38910)
- URL Filtering in the HTTP Proxy now works as expected. (BNNGF-36963)
- Added **no-digest** to the backend configuration for the reverse proxy. (BNNGF-36566)
- **URL Fetching** in the HTTP Proxy neighbor settings now works as expected. (BNNGF-37278)

OSPF/RIP/BGP

- Improved interface state changes detection. (BNNGF-37510)
- OSPF routes that are denied by the area import filter are no longer learned. (BNNGF-36992)

Azure / AWS

- The Azure UDR daemon no longer crashes on system shutdown. (BNNGF-36856)
- Setting a root password using extended ASCII characters during deployment now works as expected. (BNNGF-35994)

Access Control Service

- Added Windows 10 to the Access Control Service trustzone. (BNNGF-36691)

Control Center

- Configuration timeout for configuration updates is now configurable. (BNNGF-36975)
- Changed **Range Name** to **Range Number** when creating a new range. (BNNGF-36662)
- Creating a new box certificate for managed firewalls no longer causes the remote management tunnel to fail. (BNNGF-27846)
- The configurations in the Set area config on the **File Updates** configurations are now included in the archive.PAR file. (BNNGF-29061)
- It is no longer possible to create a CC admin using local authentication with an empty password. (BNNGF-37040)
- RCS changelog messages now allow the "-" character. (BNNGF-37119)
- It is no longer possible to add blank entries to the **Additional CC IP addresses** list. (BNNGF-37952)

Wi-Fi

- Setting the **Wi-Fi bit rate** manually no longer results in poor throughput. (BNNGF-38395)
- Enabled **802.11n** and removed **Super G channel bonding** for F80, F180, and F280 revision B. (BNNGF-35877)

DHCP-Relay

- The **Relay Interface** list now shows the correct port names. (BNNGF-37057)

DHCP Server

- Added options for PXE boot in **Basic View** mode. (BNNGF-37516)

S-Series

- Deleting a range containing a Secure Access Concentrator no longer causes the S-Series VIP network editor to fail. (BNNGF-38563)
- SCs no longer disappear from the CONTROL > Status Map when the SC is removed from a template using the box description. (BNNGF-37616)
- Added support for Barracuda M11 3G modem for SC. (BNNGF-36630)

Issues resolved by hotfixes

The following hotfixes have been released for firmware version 6.2.2

Hotfix 849 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Known Issues

6.2.2

- NextGen Admin: Activating a license can take up to 30 seconds in which 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.

Miscellaneous

- 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 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.