7.0.3 Release Notes

https://campus.barracuda.com/doc/71862314/

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.

- 31.07.2017 – Firmware version 7.0.3 released.
- 20.09.2017 – Added known issue für Web Security Gateway authentication
- 26.09.2017 – Hotfix 841 for the Firewall service released.
- 3.10.2017 – Hotfix 845 for Google Cloud released
- 19.10.2017 – Release Hotfix 848 KRACK Attack.
- 10.11.2017 – Release Hotfix 853 – Firewall service stability improvements.
- 23.11.2017 – Release Hotfix 855 – Resolves issue causing network interruptions after a soft network activation.

- Back up your configuration.
- The following upgrade path applies – **5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2 (optional) > 7.0.3**
- Before updating, read and complete the migration instructions.

For more information, see Migrating to 7.0.

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 7.0 Migration Notes.

What´s New in Version 7.0.3

NextGen Firewall firmware 7.0.3 is a maintenance release. No new features were added.

Improvements Included in Version 7.0.3

Barracuda NextGen Admin

- Security associations for IKEv2 IPsec tunnels are now grouped on the **VPN > Site-to-Site** page. BNNGF-44319
- DSL Modem status is now displayed as expected. BNNGF-44078
- 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
- Resolved issue causing the second column of the VPN Server Settings to be invisible. BNNGF-46515
- On the **Control Center > Firmware Updates** page, the Product Tips now show the full firmware version number the hotfix applies to. BNNGF-46584
- Admins can now delete an entire cluster regardless of existing server references. BNNGF-45322
- NextGen Admin now shows IPsec local / remote network settings as expected. BNNGF-45097
- Several changes have been made in NextGen Admin to improve user experience on the VPN page. BNNGF-19036
- On the **VPN > Site-to-Site** page, a Dynamic Mesh tunnel connecting to itself is no longer displayed. BNNGF-45073
- NextGen Admin dialogs after a **Send Changes** are now always displayed on a valid monitor. BNNGF-47238
- The **VPN Client-to-Site** page now shows correct information regarding the 'Last status' in the column of a user. BNNGF-23879
- It is now possible to use the mouse wheel to scroll through the list of recent logins in the **Administrators logged in** element on the Dashboard. BNNGF-45363
- In **NextGen Admin > OPTIONS** in the **Client Settings** section, an option has been added that enables users to switch between in-place editing and opening the Rule Editor when double-clicking inside a cell in the rule list. BNNGF-45402
- Resolved issue causing NextGen Admin to fail when managing multiple firewalls and Control Centers. BNNGF-44892
- In NextGen Admin, the user interface for tunnel settings for IKEv2 tunnels is now displayed correctly. BNNGF-44403
- Cluster and range firewall objects are now automatically refreshed when opening the configuration dialog. BNNGF-46288
- Copying MAP access rules between different rule lists no longer changes the connection object. BNNGF-46090
- On the **FIREWALL > Users** page, double-clicking on a user now displays a formatted list of groups. BNNGF-45817
- It is now possible to include references to other network objects when importing a list of

network objects from a CSV file. BNNGF-45490

Barracuda OS

- Updated Linux kernel to fix security vulnerabilities CVE-2016-10229 and CVE-2017-6214. BNNGF-45808
- Added an option so that when updating a firewall in a high availability cluster, the virtual server is now automatically failed over to the other firewall. BNNGF-44423
- Adding or removing interfaces that are part of a bridged interface now works as expected. BNNGF-43407
- ART rescue installation now works as expected for F800 and F900. BNNGF-43060
- Box layer HA sync for the NextGen Control Center now works as expected. BNNGF-45796
- It is now possible to get the interface alias via SNMP. BNNGF-44543
- Enrollment of Simple Certificates (SCEP) now works as expected. BNNGF-44266
- Increased the timeout for OCSP/CRL validation responses. BNNGF-47017
- Changed the maximum number of concurrent connections to the firewall authentication daemon to 1020 connections. BNNGF-47067
- Updated net-snmp to version 6.7.3 due to security vulnerability CVE-2015-5621. BNNGF-44944
- Logging into ART via SSH now works as expected for firewall models with more than one network card. BNNGF-47275
- The firewall no longer crashes if more than 250 VLANs are configured. BNNGF-46702
- Upgrading no longer causes VPN traffic to be missing from the IPFIX flow. BNNGF-44308
- The SMTP for sending email notifications can now handle multiple responses. BNNGF-45798
- Web Security Gateway authentication scheme now works as expected. BNNGF-45113
- For F82 hardware firewalls, the network activation timeout has been increased to 180 seconds. BNNGF-44959
- Updated e1000e driver to version 3.3.5.3 to solve issue causing the interface to become unresponsive after a reset. BNNGF-44205
- Updated ntpd to version 4.2.6p5 to fix several security vulnerabilities. BNNGF-36184
- TCP window size for syslog streaming is now set correctly. BNNGF-45814
- When using health checks for gateway routes, a state change no longer enables previously disabled routes. BNNGF-44821
- Configuring weights between 1 and 100 for source-based multipath routes now work as expected. BNNGF-46324
- Resolved issues where a "Login master from X.X.X.X: unknown user" event was triggered every hour on the passive firewall in a high availability cluster. BNNGF-35824

Access Control Service

- Memory management improvements have been added for the Access Control service. BNNGF-36173
- Access Control Service Allowed Client Versions can now also match on NAC 4.0 clients. BNNGF-45220

DHCP

- 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

- DNS slave zones are now processed correctly even if multiple DNS masters are configured. BNNGF-44937

FSC-Series

- It is now possible to use network mapping for the FSC-Series VIP networks. BNNGF-41924

Firewall

- 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
- Local out (LOUT) IPv6 sessions on port 636 are now terminated correctly. BNNGF-46877
- ONCRPC Firewall plugin stability improvements. BNNGF-46256
- Firewall service stability improvements. BNNGF-41729
- Firewall stability improvements for handling FTP traffic. BNNGF-45899
- Skype Audio is now detected without a preceding SSL dummy handshake. BNNGF-43091
- The values for maximum session slots for some hardware models have been adjusted. BNNGF-43667
- IPS no longer scans traffic on the loopback interface. BNNGF-42855
- Risk level overrides for applications now work as expected. BNNGF-24640
- Internal IPS rules are now included in the IPS signature list. BNNGF-43544
- Rules with **Firewall History Entry** set to **No** in the **Advanced Settings** are no longer displayed in the **FIREWALL > History** page. BNNGF-45900

URL Filter

- Setting **Action if online URL database is unavailable** to block traffic to all websites in the **Advanced Settings** of the URL Filter policy objects now works as expected. BNNGF-47206

HTTP Proxy

- When setting the config option **Front End HTTPS header** to **On** or **Auto** on a reverse proxy, a backend server redirects requests to HTTPS instead of HTTP if the backend server supports squid-specific HTTP headers. BNNGF-45534
- The HTTP Proxy no longer crashes if the Virus Scanner worker process reaches its limit. BNNGF-44542
- HTTP Proxy no longer blocks all traffic when MIME type ACLs are configured. BNNGF-43340
- Explicit IPv6 service listener IP addresses no longer cause the HTTP Proxy service to crash during the configuration activation. BNNGF-46808
- Downloading files with a ftp:// URL through an HTTP Proxy service using Scan First, Then Deliver ATP scan mode now works as expected. BNNGF-44990

RIP/OSPF/BGP

- For BGP over IKEv1 VPN tunnels, the BGP daemon is now only notified if the VPN tunnel status changes. BNNGF-45984
- For dynamic routing over VPN, it is now possible to rewrite the next hop to a reachable IP. BNNGF-44604

Virus Scanner and ATP

- File scanning results from the Avira virus scanning engine that contain multiple result messages are now interpreted correctly. BNNGF-42674
- Virus scanning in the firewall now works as expected if the virus scanning service is on a different virtual server. BNNGF-46675
- Files in the Virus Scanner quarantine are now purged on a hourly and size basis. BNNGF-45303
- File downloads using HTTP POST requests no longer fail with the ATP policy Scan First, Then Deliver. BNNGF-42269
- Only files uploaded to the ATP cloud are now counted toward the monthly ATP limit; files previously scanned or manually uploaded are no longer counted. BNNGF-47148
- The file queue waiting to be scanned by ATP is now sorted based on the start time. BNNGF-47595

VPN

- Simultaneous client-to-site VPN connection attempts of multiple clients no longer leads to invalid cookie errors. BNNGF-46589
- Running a large number of IKEv1 IPsec VPN tunnels in conjunction with frequent DNS lookups now works as expected. BNNGF-46461
- Fast reconnect for TINA VPN tunnels now works as expected. BNNGF-45741
- Added parameters to IKEv2 IPsec tunnel configuration dialog for routed VPN setups. BNNGF-43616
- Memory handling improvements for IPsec IKEv1 tunnels in the VPN service. BNNGF-44360

Control Center

- Upgrading a pool license no longer requires a manual reassignment of the pool licenses. BNNGF-44277
- New columns have been added and improvements have been made to the Floating Pool Licenses tab. BNNGF-44074
- Transferring multiple updates via the Control Center now shows all processed updates on the hardware firewall. BNNGF-46244
- Increased timeout for submitting the CC Wizard configuration settings to 120 seconds. BNNGF-45136
- 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
- A corresponding message is shown if no product tips are available in **CC > Control > Firmware Update**. BNNGF-42129

- Changed the label of the **Listening IP** drop-down list in the GTI Editor to **Use Transport Source** instead of **default-from-My-IP**. BNNGF-44618

Issues Resolved by Hotfixes

Hotfix 855 – Control: Network Activation

- A soft network activation now only removes changed virtual server IP addresses and no longer causes a network interruption.

Hotfix 853 - Firewall Service Stability Improvements

- Firewall plugin stability improvments, resolving issues with failed FTP data sessions when handling a large number of FTP sessions.
- Resolved issue where in some cases application rules did not match for HTTPS sessions. This also caused URL Filter and File Content policies configured in the application rule to not be evaluated.

Hotfix 848 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Hotfix 845 – Google Cloud

- Generic Segmentation Offloading (GSO) is now disabled in the KVM networking drivers used for firewalls running in the Google Cloud.
  Note: After installing this package you cannot upgrade to 7.1.1.

Hotfix 841 – Firewall

- Resolves issues with some firewall plugins.

Current Known Issues

- **Nov 2017: URL Filter** – URL Filtering currently does not work with PAYG images.
- **Nov 2017: VLANs** – Transferring data over configured VLAN interfaces of a NextGen Firewall F180 or F280b can fail even if the MTU size is changed. BNNGF-46289
- **Sep 2017: Authentication** – Web Security Gateway authentication schemes are currently not working. (BNNGF-45113)
- **Feb 2017: NextGen Firewall F10 Rev A** – It is not currently possible to install a Barracuda NextGen Firewall F10 Rev A via F-Series Install. Install 6.2.2 and upgrade to 7.0.3 instead. (BNNGF-43579)
- **Oct 2016: Application Based Routing** – Streaming web applications such as WebEx,

GoToMeeting or bit torrent always use the default connection configured in the application-based provider selection object. (BNNGF-42261)

- **Sept 2016 IPsec IKEv1 IPv6** – It is not possible to use hostnames as the remote gateway.
- **Sept 2016: IPsec IKEv1 IPv6** – It is not possible to use a dynamic local gateway.
- **Sept 2016: TINA IPv6** – It is not possible to use proxies for TINA VPN tunnels using IPv6.
- **Sept 2016: OSPF** – Enabling OSPF through the **Run OSPF Router** setting currently has no effect on freshly installed 7.0.0 firewalls. Enable OSPF by entering a dummy IP address in the **Summary Range IP/ Mask** list of the **OSPF Area Setup**.
- **Sept 2016: 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). (BNNGF-38823)
- **Sept 2016: URL Filter** – 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**.
- **Sept 2016: Azure** – After updating a firewall using Azure UDR via Azure Service Manager, the **Deployment Type** might be displayed incorrectly as **y**. This does not affect updating Azure UDR routes.
- **Sept 2016: 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.
- **Sept 2016: 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.
- **Sept 2016: Terminal Server Agent** – It is not currently possible to assign connections to Windows network shares to the actual user.
- **Aug 2016: IKEv2** – Disabling a site-to-site tunnel on the **VPN > Site-to-Site** page is not possible. (BNNGF-40827)
- **Mar 2016:SSH** – There is no sshd listener for IPv6 management IP addresses. (BNNGF-37403)
- **Feb 2016: Azure Control Center** – On first boot, "fatal" log messages may occur because master.conf is missing. These log messages can be ignored. (BNNGF-36537)
- **Feb 2015: CC Wizard** – The CC Wizard is not currently supported for Control Centers deployed using Barracuda F-Series Install. (BNNGF-28210)
- **Nov 2015: IKEv2** – Using a hostname or subnet as **Remote Gateway** is not currently possible. (BNNGF-41471)
- **Nov 2015: IKEv2** – Using pre-shared keys with IKEv2 client-to-site VPNs is not possible. (BNNGF-34874)
- **Nov 2014: Barracuda OS** – **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually. (BNNGF-26880)
- **Oct 2014: SSL VPN** – Favorites are not included in the PAR file. (BNNGS-199)
- **Oct 2014: SSL VPN** – User Attributes do not support UTF-8. (BNNGS-435)