7.1.5 Release Notes

https://campus.barracuda.com/doc/79467118/

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.

- Back up your configuration.
- The following upgrade path applies – 5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2 (optional) > 7.0. (optional) > 7.1.5
- Before updating, read and complete the migration instructions.

For more information and a list of supported NextGen Firewall models, see 7.1.5 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 7.1.5 Migration Notes.

What´s New in Version 7.1.5

NextGen Firewall firmware 7.1.5 is a maintenance release. No new features were added.

Improvements Included in Version 7.1.5

Barracuda Firewall Admin

- When creating a GTI IPsec site-to-site tunnel in Barracuda Firewall Admin, the **IPsec ID** is now correctly set and no longer causes GTI flapping in the GUI. [BNNGF-48208]
- On the Control Center in **CONTROL -> Firmware Updates**, deleted files are no longer displayed in the list of the tab **Files on Control Center** after their removal. [BNNGF-54013]
- When configuring a **Connection Object** in **CONFIGURATION > Configuration Tree > your virtual server > Forwarding Rules**, the **Create Proxy Arp** check box is no longer available if **Single IP Network Object** is selected for **Translated Source IP**. [BNNGF-55724]
- VPN status for HA paired boxes no longer is flapping in CC **Status Map**. [BNNGF-56936]

Barracuda OS

- The firewall no longer crashes when syncing authentication information from a large number DC agents. [BNNGF-52805]
- License handling has been improved for managed boxes. [BNNGF-53512]
- The firewall no longer crashes in certain situations when validating certificates. [BNNGF-53868]
- General stability improvements. [BNNGF-54502]
- User information in the firewall and in the authentication database are now in sync. [BNNGF-54683]
- TS agent logons are now propagated to the firewall as expected. [BNNGF-54711]
- Barracuda update servers now only communicate on ports 80/443. Port 8000 is now disabled by default and only available for optional use. [BNNGF-54833]
- The firewall's internal hard disk partitions (boot, swap) have been resized to fit new requirements. [BNNGF-54925]
- General stability improvements. [BNNGF-55042]
- Firewalls in grace mode now keep the same features licensed as before. [BNNGF-55155]
- On multi-processor firewalls, traffic workload is now processed by multiple cores as expected. [BNNGF-55255]
- The F380 firewall no longer freezes due to a permanently rising CPU usage. [BNNGF-55270]
- Access rules now match with multiple references to GEO objects. [BNNGF-55517]
- Update processes for monitoring VPN tunnel connections are now terminated correctly. [BNNGF-55612]
- Firewall appliances no longer finishes installation via USB stick with wrong LED status (red), if the installation was successful but no hotfixes were installed. [BNNGF-55706]
- Group information is now processed correctly by the firewall if special delimiters are used between fields (e.g., name, surname) on an Active Directory. [BNNGF-55718]
- The required RAM for virtual images has been increased to 4 GB for all virtual appliances. [BNNGF-55748]
- The firewall now includes a command line tool for speed tests (/usr/bin/speedtest). [BNNGF-55921]
- LDAP CRL validation for certificates now work as expected for certificates using blank CRL Urls in the certificate. [BNNGF-56401]
- SNMP no longer causes memory leaks when initializing plugins. [BNNGF-56448]

Control Center

- Control Center managed firewall now exchange their HA-sync via the MIP instead of the VIP. [BNNGF-42227]
- Reassigning pool licenses to a larger quantity of boxes in the Control Center now works as expected. [BNNGF-53178]
- License activation on the Control Center has been improved in case the MAC address for a box is not available. [BNNGF-53854]
- CC authentication sync zones now work as expected. [BNNGF-54561]
- In the Control Center, download workers no longer stop in certain situations. [BNNGF-54808]
- In **Control Center -> NETWORK ACCESS CLIENT -> Status VPN**, the table is now restricted to display only entries for admins with respective access rights for range/cluster. [BNNGF-54873]
- When migrating a cluster in the Control Center, links to **Site Specific Network Objects** are no longer broken if they are referenced inside of a connection object. [BNNGF-55853]

DHCP

- The DHCP service no longer causes memory leaks when discovering interfaces. [BNNGF-56410]

Firewall

- HTTPs requests for blocked URLs now work as expected. [BNNGF-40237]
- Link protection now correctly re-writes certain hyperlinks. [BNNGF-53144]
- Port protocol protection now drops all packets for unallowed protocols as expected. [BNNGF-53593]
- Forwarding rulesets now match as expected in case DNS network objects are referenced in a generic network object. [BNNGF-54613]
- The creation of a self-signed certificate without CN, O, and OU works as expected with OpenSSL. [BNNGF-55425]
- The host firewall ruleset for inbound connections now allows exclusive SNMP access for addresses within the ACL. [BNNGF-55446]
- When accessing a blocked URL on the Internet via the HTTP Proxy with Application Control, **Access Block** pages are now displayed correctly by the firewall. [BNNGF-55949]
- Firewalls in an HA cluster no longer crash after enabling session balancing on a tunnel. [BNNGF-56497]
- The firewall no longer keeps rebooting in certain situations. [BNNGF-56603]
- MSAD authentication with TLS1.2 now works as expected. [BNNGF-56717]

HTTP Proxy

- The HTTP forward proxy no longer crashes on high loads while accessing MS-CHAP for authentication. [BNNGF-54503]

Virus Scanner and ATP

- The Virus Scanner no longer crashes in certain situations when HA sync is active. [BNNGF-55588]

VPN

- Dyn-Mesh tunnels now generate the correct event ID (3003, 3004) when starting or stopping. [BNNGF-43170]
- The firewall now provides the correct information to SNMP for the VPN state of IKEv2 tunnels. [BNNGF-54762]
- When querying the VPN tunnel status via SNMP, the maximum length of the tunnel name has been increased from 64 to 255 characters. [BNNGF-54997]
- Packages in VPN IKE tunnels are no longer dropped in case phase 1 keys are re-keyed before their end of lifetime. [BNNGF-55388]

Current Known Issues

- **July 2019**: Phion Legacy Pool Licenses are no longer shown on a Control Center in the Floating Licenses / Pool Licenses tab. [BNNGF- 52971]
- **Feb 2018:** The ZTD daemon on the NGF Control Center rarely runs into a condition, where it continuously polls the ZTD service for new access tokens. This may leave ZTD unusable and can be recognized in the ZTD map's feedback area, where tokens become invalid and immediately get renewed. Restarting the ZTD process via *kill -9 ztd* on the console temporarily resolves this issue. Alternatively log into the **ZTD web UI** > **Settings** page and delete the authentication token.
- **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
- **June 2017: Traffic Intelligence** – Dynamic Bandwidth and Latency Detection currently does not work on VPN transports using an IPv6 envelope. BNNGF-47114
- **June 2017: Control Center** – Importing an archive.par that does not contain a CC database dump fails if the CC database is enabled. BNNGF-46601
- **Oct 2016: Application Based Routing** – Streaming web applications such as WebEx, GoToMeeting, or BitTorrent always use the default connection configured in the application-based provider selection object. BNNGF-42261
- **Sept 2016: Terminal Server Agent** – It is not currently possible to assign connections to Windows network shares to the actual user.
- **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
- **Dec 2015: URL Filter** – It is not possible to establish WebEx sessions when the URL Filter is enabled on the matching access rule. BNNGF-35693
- **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-51388