7.1.4 Release Notes

https://campus.barracuda.com/doc/78808202/

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.

- 2018-09-19 – **Firmware version 7.1.4** released.
- 2018-11-21 – **Hotfix 890** - Virus Scanner (CloudGen Firewall) – By installing this hotfix, the Avira scanning engine will be updated to version 4 and update virus definitions even after September 30th 2019. For more information, see Hotfix 890.

- Back up your configuration.
- The following upgrade path applies – **5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2 (optional) > 7.0**. **(optional) > 7.1.4**
- Before updating, read and complete the migration instructions.

For more information and a list of supported NextGen Firewall models, see 7.1.4 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 7.1.4 Migration Notes.

What´s New in Version 7.1.4

NextGen Firewall firmware 7.1.4 is a maintenance release. No new features were added.

Improvements Included in Version 7.1.4

Azure Cloud

- Firewalls deployed in Microsoft Azure no longer lose connections at random intervals. [BNNGF-53269]

Barracuda NextGen Admin

- When managing a Control Center, entries in **Administrative Roles** are now sorted on role name.   [BNNGF-45524]
- Working on multiple **Network** nodes in NextGen Admin no longer causes a deformed window when trying to add or change a network route.   [BNNGF-49826]
- Adding new entries to the list in the section **Multi Subnet Configuration** of the **DHCP** service now works as expected.   [BNNGF-52735]
- On an F1000, the **Dashboard** no longer shows an incorrect interface layout.   [BNNGF-52780]
- In the **DHCP** tab of NextGen Admin, the correct number of subnets is now displayed for IPv6 addresses.   [BNNGF-53103]
- The column 'Expiration Date' for Control Center licenses in the **CONTROL > Barracuda Activation** tab now displays the license expiration based on the regional settings to avoid the incorrect interpretation of days and months.   [BNNGF-53371]
- Activating single licenses for hardware appliances on the Control Center no longer fails. [BNNGF-54197]
- When configuring the **Details** for the **Preauthentication Scheme** in the **Group VPN Settings** with NextGen Admin in **Client to Site Settings** (tab External CA, tab Goup Policy > Click here for options), the characters '-', '_' and '=', ' ', ',' may now be entered in the **Value Pattern** field.   [BNNGF-54876] and [BNNGF-54902]

Barracuda OS

- IPv6 now binds sockets after an HA failover as expected.   [BNNGF-47215]
- Gateway routes will come up again after the were temporarily not reachable.   [BNNGF-47345]
- Interfaces are now set up correctly when performing a Soft Network Activation. [BNNGF-50842]
- The Control Center no longer displays incorrect information for failed activations of Vx boxes. [BNNGF-52052]
- The application Twitch TV is now correctly identified by Application Filter objects. The application's risk level was erroneously detected as 2 by the Application Filter. [BNNGF-52857]
- The firewall no longer crashe in certain situations.   [BNNGF-52962]
- It is now possible to add add-Range licenses as unified cloud licenses to that they can be installed on cloud Control Centers.   [BNNGF-53203]

- IPFIX traffic is now forwarded correctly from the firewall in case a route is changed to another destination server.   [BNNGF-53143]
- Idle time calculations for the session idle timer are now working as expected.   [BNNGF-53398]
- Default route is available again after not being temporarily reachable.   [BNNGF-53533]
- DCERPC and ONCRPC now support wildcard matching.   [BNNGF-53541]
- The firewall no longer crashes in certain situations.   [BNNGF-53590]
- TCP sessions via dynmesh are no longer switched to RAWTCP.   [BNNGF-53675]
- Entering "View" and "Peers" is now mandatory when configuring SNMP.   [BNNGF-53702]
- The firewall no longer crashes in certain situations.   [BNNGF-53797]
- Starting with firmware release 7.2.2, all new F800/900 firewalls will support the three management ports in the order CONSOLE/MGMT/IPMI.   [BNNGF-54020]
- Source-based routing for WWAN now uses the correct source addresses as expected. [BNNGF-54085]
- PAP/CHAP authentication has been activated for the USB modem M40 and an edit field is provided for testing IP connections at **CONFIGURATION > Configuration Tree > Network > Wireless WAN** in the **Connection Monitoring** section.   [BNNGF-54221]
- Id 'Scanning for SSL intercepted traffic' is turned off, traffic is now handled correctly by the Intrusion Prevention System (IPS).   [BNNGF-54222]
- The system report in the **STATISTICS** page of the firewall now also contains statistics about the memory usage of the firewall.   [BNNGF-54290]
- When executing the commands `acpfctrl slot` or `cat /proc/nk_resource` in a command line shell, the firewall no longer displays orphaned slots or open IPS sessions in certain situations.   [BNNGF-54303]
- The specified port range 9000 to 14000 can now be correctly added when creating a service object.   [BNNGF-54392]
- When configuring the firewall's system proxy for the **HTTP/S connection type**, it is now necessary to configure an IP address in the corresponding field for the **System HTTP Proxy Settings** section.   [BNNGF-54490]
- The IPS decoder no longer causes null pointer dereferences.   [BNNGF-54562]
- Multiple IPv6 routes are now processed correctly and no longer cause 'wild' route entries in **CONTROL > Network** in the **TABLES** table.   [BNNGF-54674]

Control Center

- TF-Firewall syncs are displayed correctly.   [BNNGF-36748]
- Zero Touch boxes no longer show issues during firmware upgrades.   [BNNGF-51005]
- Repositories are now correctly linked when migrating a cluster on a Control Center. [BNNGF-51508]
- On a Control Center, only boxes are displayed in the **CONTROL > Geo Maps** view, which are also shown on the **CONTROL > Status Map**.   [BNNGF-53051]
- Manual override values are no longer lost after a cluster migration.   [BNNGF-53528]
- Checking the activation status no longer reports error messages for loading the certificate store.   [BNNGF-53650]
- In the Control Center, pool licenses are no longer displayed as expired if any additional

subscription was no longer extended.   [BNNGF-53662]

- On a Control Center terms of agreement are now displayed correctly when using a proxy. [BNNGF-53756]
- Using 'Link overrides' for repositories in connection with SSLVPN no longer causes problems. [BNNGF-53901]
- In **CONFIGURATION > Firmware Updates**, the status is now always updated after a firewall update has been initiated from a Control Center.   [BNNGF-54497]

DHCP

- The DHCP server now starts as expected for configured VLAN interfaces.   [BNNGF-52991]
- In NextGen Admin, text-based DHCP configuration is no longer limited to 30000 characters. [BNNGF-54209]
- The **Time Offset** option in **CONFIGURATION > Configuration Tree > DHCP Service > DHCP Option Templates** now allows you to enter negative values.   [BNNGF-54548]

Firewall

- TF-Firewall syncs are displayed correctly.   [BNNGF-36748]
- Sessions with certain invalid combinations of TCP flags are dropped to avoid false-positive security scans.   [BNNGF-50150]
- Properties under Application Filter are now correctly associated with a logical AND. [BNNGF-52855]
- Offline authentication no longer fails if passwords are used with special characters and umlauts.   [BNNGF-53543]
- Using an explicit service object with custom IP protocol in an access rule no longer stops dynamic source NAT from working.   [BNNGF-54203]
- The **Dynamic Network Object** 'Auth-RSASecureID' now displays configured IP addresses correctly in the list for **Host Rules** and is also processed as expected in predefined host access rules.   [BNNGF-54893]

Virus Scanner and ATP

- File scanning results from the Avira virus scanning engine that contain multiple result messages are now interpreted correctly.   [BNNGF-45597]
- The clamAV virus scanner has been updated.   [BNNGF-54556]
- The pattern version of ClamAV is now displayed correctly in **CONTROL > Server > Security Subscription** in the **Barracuda NG Malware Protection** section.   [BNNGF-54583]

VPN

- VPN connections no longer fail due to incorrect time calculations when checking certificate validity periods.   [BNNGF-48827]
- The firewall no longer crashes due to a race condition in cipher initialization.   [BNNGF-52291]
- The reverse routing check no longer fails in case that the B0 dynmesh transport is not active. [BNNGF-53773]
- Unneeded TCP connections for VPN are closed properly and no longer refuse establishing new

TCP connections with the error message 'no slot available'.   [BNNGF-54742]

Current Known Issues

- **Jun 2018: Firewall** – Copying access rules with enabled SSL Inspection from firewalls running firmware version 7.2.x to firewalls running firmware version 7.1.0 - 7.1.4, can have negative impact on SSL Inspection on the destination system.
- **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