7.1.3 Release Notes

https://campus.barracuda.com/doc/78152481/

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.

- 2018-06-14 – **Firmware version 7.1.3** released.
- 2018-08-22 – **Hotfix 882** - Azure Connectivity – The hotfix solves random Microsoft Azure network connectivity issues caused by the Hyper-V drivers (LIS). For more information, see Hotfix 882.
- 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) > 7.1.3**
- Before updating, read and complete the migration instructions.

For more information and a list of supported NextGen Firewall models, see 7.1.3 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 7.1.3 Migration Notes.

What´s New in Version 7.1.3

NextGen Firewall firmware 7.1.3 is a maintenance release. No new features were added.

Improvements Included in Version 7.1.3

Barracuda NextGen Admin

- The **Output-IF** column in the **History** page now also shows data of application rules. BNNGF-29499
- The meta data of an update package are now correctly displayed on the Control Center after the package has been installed on a centrally managed firewall unit. BNNGF-39235
- Barracuda NextGen Admin now supports wildcards as sub alt name to support iOS wildcard certificates. BNNGF-43124
- NextGen Admin now shows the completion of firmware download as expected. BNNGF-44064
- The IPsec IKEv2 window now fits into workspaces with a smaller resolution. BNNGF-45223
- Changing the order of referenced net objects no longer deletes the reference name. BNNGF-48440
- Schedule Objects are correctly disabled in Global-, Range-, and Cluster Firewall Objects. BNNGF-49512
- Client-to-site group policies are now correctly limited to support a maximum of 64 routes. BNNGF-50604
- IPsec IKEv1 VPN tunnels no longer show up multiple times on the VPN Status page. BNNGF-50916
- Having multiple configuration windows active in the Control Center configuration view, no correctly allows access to all active configurations. BNNGF-50927
- When creating a new rule, no application policies and no shaping are preset in the rule editor. BNNGF-51977
- Dashboard widgets are now disabled for the F10/F15/F100 models. BNNGF-52926
- NextGen Admin tabs can now be closed with the Ctrl-W shortcut. BNNGF-53008
- SCADA parameters have been renamed in General Firewall Configuration > Application Detection. BNNGF-53033
- UMTS links have been renamed to WWAN in the entire NG Admin configuration. BNNGF-53246
- It is now possible to enforce globally unique server and service names in a Control Center environment. BNNGF-53510

Barracuda OS

- Firmware support for appliance model F12.
- DHCP client connection attempts no longer produce connection issues. BNNGF-32801
- Application Based Link Selection now works as expected for Office 365. BNNGF-40234
- The firewall now also provides native VLAN support to allow untagged traffic over tagged interfaces. BNNGF-40337

- Infinite lifetime for IPv6 prefixes is now configurable. BNNGF-42733
- Excluding networks from PROXY ARPs now works as expected. BNNGF-48299
- Attachments with .eml extensions are now scanned regardless of specified content type. BNNGF-48677
- SSL Interception with RPC over HTTPS now works as expected. BNNGF-49600
- When handling FTP data, the firewall no longer produces a segmentation fault in certain situations. BNNGF-49676
- Barracuda Firewall now supports USB M40/41 LTE Modem. BNNGF-50451
- Flapping routes no longer occur in case a routed bridge is configured between your LAN and Wi-Fi. BNNGF-51087
- The firewall authentication daemon now correctly switches to the next available authentication server if the primary server replies to be unavailable. BNNGF-51637
- On hardware boxes, acquiring an IPv6 address from the ISP after setting up a DHCPv6 link now works as expected. BNNGF-51708
- The firewall now checks for the FTP plugin in the access rule's service object to decide whether Application Control is required. BNNGF-52054
- LDAP authentication timeout can now be configured. BNNGF-52123
- The default policy for the Proxy Web Filter is now allow-all-except. BNNGF-52175
- The statistics for disk reads and writes are now calculated correctly. BNNGF-52203
- Self-referencing network objects are no longer allowed. BNNGF-52282
- The SNMP box service now shows the correct IPsec tunnel state. BNNGF-52453
- Certain IP addresses are no longer re-evaluated in environments where DC Agent and Auth Sync are enabled through multiple locations. BNNGF-52550
- Custom MTU sizes now work as expected. BNNGF-52644
- FTPS can now be blocked on non-standard ports. BNNGF-53010
- The size limitations for the forwarding ruleset have been increased. BNNGF-53076
- The limitation for TINA routes has been raised to 50k. BNNGF-53146

Control Center

- CC administrators can no longer access or view licenses in **CONTROL** > **Licenses** in case they are not allowed to. BNNGF-36306
- After deleting a GTI group configuration, the configuration files now are removed. BNNGF-37491
- On the Control Center, the Unit description is no longer missing after a firmware update. BNNGF-51660
- SSL VPN configuration nodes can now be linked to a repository. BNNGF-51661
- Migrating a cluster no longer causes repository-linked C-Firewall rules to be renamed to "Default". BNNGF-52748
- The settings for VPN AC are now updated as expected when using a template. BNNGF-40464

Firewall

- The firewall no longer ignores TCP option MSS if Anti Virus detection is enabled for a firewall rule. BNNGF-46737
- The 64 character limitation of DNS network objects has been removed. BNNGF-48702

- With Application Based Link Selection enabled, access to services like Office Portal now work as expected. BNNGF-51619
- Opening www.mediamarkt.pl with SSL Interception now works as expected. BNNGF-52245
- Disabling outbound QoS, while inbound QoS is still active, no longer negatively affects network traffic. BNNGF-52281
- The Firewall Activity Log now contains correct messages for DROP/BLOCK actions. BNNGF-52434
- Outlook can again connect to the Exchange server when SSL Interception and Virus Scanning are enabled. BNNGF-52519
- The Last column of the VPN Access Cache now displays correct values. BNNGF-52610
- Passive PUT and active GET file transfers are now virus scanned if the FTP plugin is active. BNNGF-52650
- OCSP validation with HTTP 1.0 now also works if validation peers require the host field. BNNGF-52692

Virus Scanner and ATP

- Operational performance of the Virus Scanner has been improved. BNNGF-52126
- The file size limit has been increased to 10 MB for ATP. BNNGF-52467

VPN

- Exports of VPN Group Policies now correctly contain first and secondary IP addresses of the respective VPN service. BNNGF-47655
- IKEv2 does not trigger events when tunnel is terminated. BNNGF-52338
- iOS IPsec connections now work as expected. BNNGF-52557
- The VPN session handler no longer crashes when using certificate based authentication in Combination with network Access Client 5.0. BNNGF-53619

Web UI

- Creating a cascaded rule list now works as expected. BNNGF-51178
- The Application Monitor no longer displays pop-over errors for unknown data. BNNGF-52017

ZTD

- The status after a ZTD no longer is inconsistent in certain situations. BNNGF-51408

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 - 7.1.3, 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
- **September 2017: Azure ASM** – NextGen Firewalls deployed using Azure Service Manager now show the status **running** after deployment in the Azure portal. This does not affect the firewall VM's functionality. BNNGF-48296
- **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: 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: 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 Firewall as the Firewall service. This issue does not occur when running the HTTP Proxy service on a second NextGen Firewall behind the NextGen Firewall running the Firewall service.
- **Sept 2016: VPN Routing** – When a duplicate route to an existing VPN route in the main routing table is announced to the NextGen Firewall via RIP, OSPF, or BGP, a duplicate routing entry is created and the route that was added last is used.
- **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-26880