7.1.2 Release Notes

https://campus.barracuda.com/doc/74548110/

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.

- 2018-02-28 – **Firmware version 7.1.2** released.
- 2018-04-19 – **Hotfix 867** – 4G USB Modem M40/M41 Support – The hotfix adds support for Barracuda 4G USB Modem models M40/M41. For more information, see Hotfix 867.
- 2018-04-19 – **Hotfix 868** – Virus Scanner – The hotfix covers 5 important issues. For more information, see Hotfix 868.
- 2018-05-15 – **Hotfix 875** – Fixes the security vulnerability CVE-2018-10115 in 7zip. For more information, see Hotfix 875.
- 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) > 7.1.2**
- Before updating, read and complete the migration instructions.

For more information and a list of supported NextGen Firewall models, see 7.1.2 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 7.1.2 Migration Notes.

What´s New in Version 7.1.2

NextGen Firewall firmware 7.1.2 is a maintenance release. No new features were added.

Improvements Included in Version 7.1.2

Barracuda NextGen Admin

- UPNP broad-/multicasts now show the correct output interface in Live/History view. [BNNGF-29347]
- In the access rule editor, when using network objects for the destination, the "Create Proxy ARP" check box is available only for single IPv4 addresses. [BNNGF-37764]
- Disabling an IPsec IKEv2 tunnel via the VPN site-to-site tab now works as expected. [BNNGF-40827]
- In NextGen Admin, the DNS User Interface has been updated for configurations with "Negative Cache TTL" values. [BNNGF-45414]
- The reverse proxy now delivers root certificates only once per request. [BNNGF-46029]
- The firewall dashboard now correctly displays content older than 7 days. [BNNGF-46908]
- IPv6 addresses are now shown correctly in the GTI Editor. [BNNGF-47295]
- When connecting to a NextGen Firewall with an old version of NextGen Admin, a warning is displayed. [BNNGF-47333]
- ICMP policies are now copied together with a related access rule. [BNNGF-48046]
- In case a redirection target list reference is selected in a firewall rule, the fallback and cycle combo element is disabled. [BNNGF-48185]
- GTI configurations for IPsec tunnels now work as expected. [BNNGF-48342]
- Uploading a local package to the Control Center firmware update UI no longer causes timeouts. [BNNGF-48552]
- Adding entries for DNS zones now works as expected. [BNNGF-48703]
- When downloading terms of service during an activation with the wizard, the proxy settings are now used as expected. [BNNGF-49151]
- Up/Lifetime information for VPN tunnels is now displayed correctly. [BNNGF-49261]
- License tokens now may be entered case insensitive. [BNNGF-49166]
- The RECENT SEVERE EVENTS element in the DASHBOARD now displays the correct time. [BNNGF-49393]
- The entry Toggle Trace in the pop-up menu of the Firewall Live View is no longer available. [BNNGF-49574]
- Firewall stability improvements. [BNNGF-49639]
- QoS configuration is only available for IPv4. [BNNGF-50067]
- In the Virtual IP column of the **VPN > Client-to-Site** table, virtual IPs are now displayed correctly when accessing a box running 7.0.3 from NextGen Admin 7.1.1 [BNNGF-50094]
- For IPsec tunnels, the option Encaps. Mode Auto Detect has been renamed to NAT-T

Autodetect. [BNNGF-50158]
- Firewall Monitor in NextGen Admin now correctly evaluates time information. [BNNGF-50449]
- Copying serial numbers to the clipboard now works as expected in the Control Center activation tab. [BNNGF-50512]
- Peer and local addresses are now displayed correctly in the NextGen Admin VPN status pages. [BNNGF-50699]
- Display of firewall users in grouped view is no longer rendered unreadable with long group text. [BNNGF-50826]
- The firewall history no longer shows old entries as current hits. [BNNGF-51025]
- Firewall statistics now also display the port number in addition to the port name. [BNNGF-51083]
- Barracuda NextGen Admin no longer crashes after a Windows update. [BNNGF-51256]
- Loading the firewall history no longer causes errors on F10/F100 models. [BNNGF-51649]
- IPv6 Autoconfig now allows you to add a DNS server. [BNNGF-51665]

Barracuda OS

- Events for expiring Energize Update licenses are now created as expected. [BNNGF-41720]
- The firewall no longer crashes in an VMWARE ESXI 6.0.0 environment. [BNNGF-43656]
- Contacting license update servers through a proxy network now works as expected. [BNNGF-45037]
- Adding new PTR entries to the forward lookup zone now works as expected if both the forward AND reverse lookup zone is locked before the change. [BNNGF-46055]
- F800 Rev. B models with module M801 no longer experience port flapping with higher load. [BNNGF-46304]
- Client to server communication for segmented FTP commands no longer causes problems in certain situations. [BNNGF-46513]
- DSL now works as expected after an import of a PAR file. [BNNGF-47907]
- VLAN references are no longer displayed after the deletion of the VLAN. [BNNGF-48054]
- On certain models like the M30, an active modem is now found after activating a GMS channel. [BNNGF-48431]
- The firewall no longer drops packets that are larger than the MTU. [BNNGF-48521]
- IPv6 TCP sessions that do IPS scanning no longer cause memory leaks. [BNNGF-48698]
- Using the NTLM protocol for authentication over a forward proxy now works as expected. [BNNGF-48709]
- Soft Activation no longer causes a network interruption. [BNNGF-48862]
- The internal QoS shaping tree for Bandwidth and Latency Detection is now created on firewalls deployed in the Google and Azure Cloud. [BNNGF-49292]
- Interface names are now mapped correctly from the Defaults file for port names. [BNNGF-49478]
- TCP sessions now terminate after being idle for 24 hours. [BNNGF-49525]
- Auto-created source-based routing now works as expected. [BNNGF-49726]
- The security issue to protect against the WPA2 vulnerability (KRACK attack) has been resolved. [BNNGF-49766]
- TCPDump no longer disables a bundled interface in promiscuous mode. [BNNGF-49793]
- The threshold for lower fan speeds has been adjusted to accept cooler ambient temperatures.

[BNNGF-49795]
- Initial NTP synchronization now works as expected. [BNNGF-49860]
- On an F183R, start of bridging no longer causes the box to freeze. [BNNGF-49987]
- Multiple SMTP and FTP protocol handling improvements. [BNNGF-49866]
- FTP plugin now works with SynFlood Protection both for inbound and outbound connections. [BNNGF-50047]
- Validating licenses for long license names with long box names in a long cluster name no longer fails. [BNNGF-50253]
- FSC-2.0 boxes now accept SC 1.1 configurations. [BNNGF-50397]
- On the F82, **Control > Resources** now displays the RPM for the fan. [BNNGF-50653]
- HA takeover now works in acceptable times as expected. [BNNGF-50887]
- Running a bridging setup under heavy load for several hours now works as expected. [BNNGF-51044]
- The 40 Gbps module is now supported for the F1000 model. [BNNGF-49485]
- IPsec now triggers event ID 3000 as expected. [BNNGF-50824]
- Network activation no longer fails due to empty MTU parameter on VLAN interface. [BNNGF-51022]
- Logging into the firewall via SSH no longer displays error messages if no ECDSA key has been configured. [BNNGF-47059]

DHCP

- DHCP now sends IPv6 DHCP reply packets as expected. [BNNGF-41604]

Firewall

- Application Rules and URL categories now match correctly. [BNNGF-24209]
- Global firewall objects are now immediately activated by the firewall engine after a configuration on the Control Center. [BNNGF-38201]
- FTP data sessions are no longer evaluated against application rules if the FTP plugin is active and if Application Control is disabled. [BNNGF-51059]
- Application Based Provider Selection now handles traffic from YouTube and media streaming services. [BNNGF-50503]
- Client-to-site access rules no longer enable site-to-site tunnels. [BNNGF-50132]
- The firewall now delivers mails correctly to a client after STMP mail scanning is finished. [BNNGF-49850]
- FTP sessions are now handled correctly and no longer cause different errors. [BNNGF-49507, BNNGF-49304, BNNGF-48996]
- Multiple stability improvements for the URL Filter service. [BNNGF-48972]
- The trans7 process no longer produces a segmentation fault in certain situations. [BNNGF-49135]
- Interfaces for local traffic are now reported correctly. [BNNGF-48975]
- The firewall no longer crashes in certain situations with SCADA support enabled. [BNNGF-48844]
- Local-in SSH connections to the box are no longer unexpectedly blocked. [BNNGF-48439]
- The REST firewall plugin for /live and /history endpoints now works as expected. [BNNGF-49656]
- The firewall no longer crashes because of internally unreferenced DST entries. [BNNGF-50572]

- The passive unit of an HA cluster no longer writes *unhandled exception* error messages to the fatal log. [BNNGF-50747]
- Multipart emails with blanks in the boundary are now correctly scanned for malware. [BNNGF-50989]
- Sessions to a "slow" receiver no longer result in high CPU load of the tap3 process. [BNNGF-51090]
- The firewall no longer crashes based on an internal deep recursion. [BNNGF-51120]

Control Center

- Repository overrides are not lost when moving a server or a box to another cluster / range. [BNNGF-41785]
- In the GTI Editor, settings for Phase 1 Mode for an IPsec tunnel are now written correctly to the corresponding configuration file. [BNNGF-43874]
- Status colors in the Control Center status map are displayed correctly if an AV license is still valid and less than 90 days. [BNNGF-45530]
- On a Control Center, deleting a global repository now works as expected. [BNNGF-47325]
- If the serial gets changed on a virtual firewall, the activation daemon now downloads new licenses. [BNNGF-47608]
- SCA setups are no longer broken after an upgrade of a Control Center. [BNNGF-48187]
- The NextGen Firewall now creates correct events on boxes when external admins authenticate without a password on the Control Center. [BNNGF-48738]
- In rare cases, the Control Center Configuration Service ran out of resources. This issue has been resolved. [BNNGF-49488]
- Firmware update view is now displayed correctly on a Control Center and no longer causes an error message. [BNNGF-50102]
- Importing a 7.0 PAR file to a 7.1 Control Center no longer triggers a migration. [BNNGF-50137]
- Replacing/merging configurations using the clipboard in NextGen Admin now works as expected in the SCA editor. [BNNGF-50872]
- In the Control Center, floating licenses no longer will be removed due to differing hash. [BNNGF-50654]
- Migrating an SC from version 1.0 to 1.1 no longer triggers a verification check. [BNNGF-51159]
- Configuring SCA/AC settings on a newly deployed Control Center now works as expected. [BNNGF-49302]

HTTP Proxy

- For the HTTP proxy, identical names for visible hostname and backend hostnames are not allowed. [BNNGF-48550]
- URL Filtering now works as expected with PAYG images. [BNNGF-50579]

Public Cloud

- In the cloud, provisioning now successfully finishes even if the creation of datacenter network objects fails. [BNNGF-49455]

- On an MS Hyper V 2012 & 2016 server, VLAN traffic is now handled correctly. [BNNGF-49703]
- On a Hyper-V, the firewall now boots even with more than 4 interfaces configured. [BNNGF-49791]
- Resetting a password in an Azure Portal no longer causes memory leaks. [BNNGF-50721]

REST API

- The REST API no longer listens on the management IP per default. [BNNGF-48407]
- On a Control Center, REST API post requests no longer cause error 500 if RCS with forced message is enabled. [BNNGF-48475]

Virus Scanner and ATP

- A reload of the ATP page no longer causes an "FW Potential Spoofing Attempt" event [BNNGF-26793]
- The setting Block Encrypted Archives now works as expected. [BNNGF-48082]
- Configuring the RAM cache for the Virus Scanner no longer causes it to crash. [BNNGF-49323]
- Setting the Max. Archive size in the advanced ATP options is limited to the maximum value of 2047 and no longer causes the Virus Scanner to crash. [BNNGF-49413]
- Scanning emails with Clam AV now works as expected. [BNNGF-50194]
- The Virus Scanner and ATP no longer cause a crash when using OpenSSL. [BNNGF-50871]
- Processing and scanning mails now works as expected after an install of hotfix 852. [BNNGF-50609]
- Null byte reverse proxy attacks no longer result in high load of the virus scanning engine. [BNNGF-49628]
- The Virus Scanner no longer produces core dumps in certain situations. [BNNGF-50851]

VPN

- VPN routing in combination with BGP, TINA, and IPsec using main routing tables now works as expected. [BNNGF-49698]
- IKEv1 site-to-site settings no longer let client-to-site connections fail for iOS. [BNNGF-50014]
- Certificate-based authentication for Site-to-Site IPSEC with multiple altSubjectNames now works as expected. [BNNGF-50418]
- Establishing an IKEv1 site-to-site VPN tunnel in aggressive mode now works as expected. [BNNGF-50597]

Zero Touch

- Zero Touch Deployment now supports all NGF appliances. [BNNGF-49324]

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 - 7.1.2, 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