7.2.3 Release Notes

https://campus.barracuda.com/doc/79465061/

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.

- 2018-12-12 – **Firmware version 7.2.3** released.
- 2019-01-10 – **Hotfix 895** released. Firewall stability improvements. For more information, see Hotfix 895.
- 2019-01-23 – **Hotfix 897** released. VPN service improvements. For more information, see Hotfix 897 .
- 2019-01-29 – **Hotfix 896** and **Barracuda Firewall Admin 7.2.3 - 207** released. Azure Virtual WAN O365 policy support. For more information, see Hotfix 896 and Firewall Admin 7.2.3 - 207.
- 2019-02-18 – **Hotfix 898** released. This hotfix adds additional WAN probing- , LAN mode- , and Link Selection options for Barracuda Secure Connectors. For more information, see Hotfix 898.
- 2019-02-27 – **Hotfix 1001** released. This hotfix removes memory leaks from the DHCP, DHCP Relay, and SNMP service. For more information, see Hotfix 1001.
- 2019-04-11 – **Hotfix 1004** released. This hotfix ensures that pattern updates will be available for firewalls with firmware 7.2.3 after end of June 2019. For more information, see Hotfix 1004.

Before You Begin

- 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 (optional) > 7.2
- Before updating, read and complete the migration instructions.

For more information and a list of supported CloudGen Firewall models, see 7.2.3 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 7.2.3 Migration Notes.

What´s New in Version 7.2.3

Automated Connectivity for Azure Virtual WAN

Barracuda CloudGen Firewalls support Microsoft's Azure Virtual WAN technology to allow fast, secure, and uninterrupted network availability with your cloud-hosted or hybrid datacenter and your branch offices through Microsoft's global network. The CloudGen Firewall in combination with Virtual WAN fully enables automated large-scale branch connectivity, unified networks and policy management, and optimized routing using the Microsoft global network.

For more information, see Azure Virtual WAN.

New Behaviour of Refresh always / Refresh when active Button

When starting (over), Barracuda Firewall Admin now recalls the last state of the **Refresh always** / **Refresh when active** button set individually for the service bars **CONTROL, FIREWALL > LIVE**, **FIREWALL > SHAPING**, **VPN > Site-to-Site**, **VPN Client-to-Site**.

Multiple Ticket Administrators

With Barracuda Firewall Admin you can now configure mulitple ticketing administrators.

For more information, see How to Configure Guest Access with the Ticketing System.

Administrator Roles with New Option

The Control Center now provides a new option for permitting administrators to install already uploaded box firmware updates.

For more information, see How to Configure Administrative Roles.

New Subscription Element for Dashboard

The display area for subscriptions formerly reachable in **CONTROL > Server** has been replaced by a new element that is now located in the Dashboard in Barracuda Firewall Admin.

For more information, see DASHBOARD General Page and Server Page.

Integration of Notification Solution for Macmon

macmon Endpoint Security and Network Access Control is capable of collecting threat notifications from other systems in order to protect a network infrastructure from malicious clients. The CloudGen Firewall can be configured to send notifications to the macmon system as soon as ATP detects a threat.

For more information, see macmonEventNotification and How to Configure macmon Event Notifications to Report an ATP Incident to the macmon System.

Improvements Included in Version 7.2.3

Azure Cloud

- Updated network drivers to fix intermittent connectivity issues for firewalls deployed in Microsoft Azure. [BNNGF-53269]

Barracuda Firewall Admin

- The new event viewer now works as expected for a Control Center and allows connections without communication errors. [BNNGF-45396]
- When managing a Control Center, entries in **Administrative Roles** are now sorted on role name. [BNNGF-45524]
- 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]
- Working on multiple network nodes in Barracuda Firewall 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]
- Barracuda Firewall Admin no longer crashes when terminating the creation of an RCS report by pressing the ESC key. [BNNGF-52858]
- In the **DHCP** tab of NextGen Admin, the correct number of subnets is now displayed for IPv6 addresses. [BNNGF-53103]
- In Barracuda Firewall Admin, the list in **FIREWALL > Users** now displays user entries with the correct line height. [BNNGF-53351]
- The column **Expiration Date** for Control Center licenses in the **CONTROL > Barracuda Activation** tab now displays the license expiration based on the regional settings of the operating system to avoid the incorrect interpretation of days and months. [BNNGF-53371]
- In Barracuda Firewall Admin, **CONFIGURATION > Configuration Tree > Virtual Servers > your server > Assigned Services > Firewall > Rule Tester** no longer fails on a rule check

after changing back from an IPv6 check to an IPv4 check. [BNNGF-54041]
- When resetting the **Traffic Shaping** GUI in **Barracuda Firewall Admin > FIREWALL > Shaping**, the **ND** column is now reset. [BNNGF-54114]
- Changes to the description of a severity entry in **CONFIGURATION > Configuration Tree > Eventing** will now be displayed correctly in the **Severity** column in the **EVENTS** tab. [BNNGF-54201]
- On a Control Center in **Multi-Range > Global Settings**, service IPs are now displayed correctly in the VPN GTI editor. [BNNGF-54473]
- Barracuda Firewall Admin no longer creates an error if the timeout value in **Firewall Admin > OPTIONS > Settings > Client Settings > Log and Statistics Timeout** is greater than or equal to the time the log daemon takes to load log entries. [BNNGF-54479]
- Barracuda Firewall Admin no longer crashes after adding a scheduled block rule with large unusual timeframes. [BNNGF-54513]
- Barracuda Firewall Admin now encodes welcome messages in UTF-8 format for VPN client-to-site connections. [BNNGF-54733]
- Barracuda Firewall Admin no longer crashes when deleting the last line on the bottom of the list inside the **EVENTS** tab. [BNNGF-55142]
- Barracuda Firewall Admin no longer crashes when the last event in the list is clicked in the **EVENTS** tab. [BNNGF-55142]
- The event viewer in Barracuda Firewall Admin now displays event properties correctly on Microsoft Windows 7. [BNNGF-55143]
- In Barracuda Firewall Admin, **OPTIONS > Admin and CC Settings** is no longer limited to display only one trusted CC entry. [BNNGF-54860]
- 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 Firewall Admin no longer shows the version used of Firewall Admin as available download in the **DASHBOARD > UPDATES** widget. [BNNGF-54880]
- Network references can now be configured correctly on 6.2 and 7.1 Control Centers when being administrated with Barracuda Firewall Admin 7.2. [BNNGF-55324]
- Access Control Service ruleset versions have been updated to their newest client version. [BNNGF-55393]
- Host firewall rules are no longer capable of using geo-locations in the network objects dialog to prevent a firewall rule mismatch. Geo-locations are in general not available in host firewall rules. [BNNGF-55434]
- 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]
- Barracuda Firewall Admin no longer displays firewalls on the Control Center status map that have been removed from the configuration tree. [BNNGF-55815]
- Adding a new **Service or Server (SRV)** record in the DNS service now works as expected. [BNNGF-55967]

Barracuda OS

- Information about SNMP throughput, disk space and traffic shaping groups is now displayed correctly due to calculations with 64-bit integer data types. [BNNGF-52449]
- Multiple IPv6 routes are now processed correctly and no longer cause 'wild' route entries in **CONTROL > Network** in the **TABLES** table. [BNNGF-52751], [BNNGF-54674]
- The firewall no longer crashes when syncing authentication information from a large number DC agents. [BNNGF-52805]
- IPFIX traffic is now forwarded correctly from the firewall in case a route is changed to another destination server. [BNNGF-53143]
- Accessing **Network Objects** through the REST API is now enabled without the need to enable range- or cluster-Level Firewall Objects. [BNNGF-53161]
- MSAD offline group synchronization no longer fails over SSL. [BNNGF-53486]
- The firewall no longer crashes in certain situations when validating certificates. [BNNGF-53868]
- 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]
- The IPS decoder no longer causes null pointer dereferences. [BNNGF-54562]
- 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]
- Multi Range Repositories for SNMP now work as expected when a box is linked to the repository. [BNNGF-54745]
- Certificate authority (CA) cleanups are now done as expected when working with the Syslog service. [BNNGF-54788]
- 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]
- When configuring a virtual link for OSPF with Digest-MD5 encryption in **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > OSPF-RIP-BGP-Service > OSPF Area Setup > OSPF Area Configuration**, the authentication key input now accepts up to 16 characters. [BNNGF-54842]
- IPv6 with prefix delegation now works as expected on DHCP interfaces. [BNNGF-54856]
- MSAD is no longer having problems when key entries are present in the config file without any assigned value. [BNNGF-54897]
- The firewall's internal hard disk partitions (boot, swap) have been resized to fit new requirements. [BNNGF-54925]
- Access rules with MAC address match criteria no longer drop traffic mistakenly for forwarding rules. [BNNGF-54933]
- The CC Wizard in Barracuda Firewall Admin now accepts Hyper-V-based Control Centers as expected. [BNNGF-54941]
- Firewalls in grace mode now keep the same features licensed as before. [BNNGF-55155]
- The firewall now connects to the Barracuda Reporting Server through the remote management tunnel using the VIP. [BNNGF-55980]

- The firewall no longer crashes in certain situations. [BNNGF-55042]
- 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]
- The firewall now "Replies to Pings" for additional IPs as expected. [BNNGF-55289]
- The firewall now creates route change events after an ISP outage as expected. [BNNGF-55510]
- Update processes for monitoring VPN tunnel connections are now terminated correctly. [BNNGF-55612]
- macmon endpoint security and Network Access Control (NAC) has been integrated into the eventing system of the firewall. [BNNGF-55643], [BNNGF-55644]
- 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]
- Devices with WLAN can now connect as expected if multiple access points are configured. [BNNGF-55802]
- The firewall now includes a command line tool for speed tests (/usr/bin/speedtest). [BNNGF-55921]
- The IP address of the M40 modem is now written into the dynamic network objects. [BNNGF-55931]
- Improvements have been made to HA sync. [BNNGF-55932]
- The firewall now connects to the Barracuda Reporting Server through the remote management tunnel. [BNNGF-55980]

Control Center

- Control Center-managed firewalls now exchange their HA-sync via the MIP instead of the VIP. [BNNGF-42227]
- Encrypting the root password now uses the SHA256 instead of the MD5 algorithm. [BNNGF-51547]
- Access to the Control Center database has been improved. [BNNGF-52998]
- 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]
- 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]
- When adding a new administrative role in the Control Center in **CONFIGURATION > Configuration Tree > Administrative Roles**, administrator roles can now be configured to **Install uploaded Box Firmware Updates** in the section **CC Control**. [BNNGF-54275]
- In **CONFIGURATION > Firmware Updates**, the status is now always updated after a firewall update has been initiated from a Control Center. [BNNGF-54497]
- CC authentication sync zones now work as expected. [BNNGF-54561]

- In Barracuda Firewall Admin, the **Box Clone Wizard** now clones virtual servers with cleared server IPs. [BNNGF-54801]
- In the Control Center, download workers no longer stop in certain situations. [BNNGF-54808]
- 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]
- After reinstalling a Control Center, SC boxes show up as expected in the Status Map. [BNNGF-56019]
- When creating a virtual managed box in the Control Center, the Web UI is now disabled. [BNNGF-56187]

DHCP

- The DHCP server now starts as expected for configured VLAN interfaces. [BNNGF-52991]
- In Barracuda Firewall Admin, text-based DHCP configuration is no longer limited to 30,000 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]
- The firewall now sends router advertisements as expected if a working DHCP relay is configured. [BNNGF-55113]

Firewall

- HTTPs requests for blocked URLs now work as expected. [BNNGF-40237]
- Sessions with certain invalid combinations of TCP flags are dropped to avoid false-positive security scans. [BNNGF-50150]
- 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]
- Forwarding rulesets now match as expected in case DNS network objects are referenced in a generic network object. [BNNGF-54613]
- 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]
- 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]
- Access rules now match with multiple references to GEO objects. [BNNGF-55517]
- The firewall no longer keeps rebooting in certain situations. [BNNGF-56603]

HTTP Proxy

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

Virus Scanner and ATP

- File scanning results from the Avira virus scanning engine that contain multiple result messages are now interpreted correctly. [BNNGF-45597]
- ATP with **Scan first, then deliver** is no longer restricted to port 443. [BNNGF-53694]
- The Virus Scanner service no longer crashes during a shutdown of the firewall. [BNNGF-54049]
- The ClamAV virus scanner has been updated. [BNNGF-54556]
- The pattern version of ClamAV is now displayed correctly in the **DASHBOARD** element **SUBSCRIPTION STATUS**. [BNNGF-54583]
- The Virus Scanner no longer crashes in certain situations when HA sync is active. [BNNGF-55588]

VPN

- The source address of source-based routing entries for VPN traffic will be ignored if they are moved to the main routing table by setting **Add VPN Routes to Main Routing Table (Single Routing Table)** to **yes** in **CONFIGURATION > Configuration Tree > your virtual server > VPN > VPN Settings > Server Settings**. [BNNGF-40962]
- Dynamic mesh tunnels now generate the correct event ID (3003, 3004) when starting or stopping. [BNNGF-43170]
- Dynamic mesh tunnel no longer fails after spoke HA failover. [BNNGF-53416]
- In the L2TP settings section of **VPN > L2TP/IPSEC**, the **Pool Size** now can exceed the size of a class C subnet. [BNNGF-54568]
- 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]
- 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]
- For Multi-Factor-Authentication-related client-to-site connections, tunnel probing has been set to silent mode. [BNNGF-55653]

Current Known Issues - General

- **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 a negative impact on SSL Inspection on the destination system.
- **ATP** – The "Scan first, then Deliver" option and SMTP-AUTH is not yet supported. [BNNGF-52992]
- **ATP** – The "Scan first, then Deliver" option and using an MUA (eMail client) - NGFW - MTA is

currently not supported. [BNNGF-52992]
- **ATP** – The "Scan first, then Deliver" option and using BDAT (e.g., Microsoft Exchange servers may use that) is not yet supported. [BNNGF-52992]
- **ATP** – The "Scan first, then Deliver" option with SMTP and VRF is not yet supported. [BNNGF-52992]
- **AWS-Cloud** – Deploying AWS Auto Scaling clusters in the US-East-1 region currently fails to create an S3 bucket automatically. Create the bucket manually instead.
- **Certificate Store** – When referencing certificates in the **Certificate Store** from services like **SSL Inspection**, the reference counter in the **Ref By** column still shows 0. [BNNGF-50666]
- **Control Center** – When a tunnel is deleted on a CC, the GTI tunnel is not automatically removed from the configuration. To work around this issue, perform a change in the VPN configuration on the affected firewall unit and activate the changes. The tunnel will then be removed along with the change. [BNNGF-54752]
- **Network** – Transferring data over VLAN interfaces configured on the switch port of CloudGen Firewall F180a or F280b fails due to inability of changing the MTU size. [BNNGF-46289]
- **Network** – OSPFv3 is currently not working as expected.
- **Firewall Admin** – Copy and paste of an access rule with explicit Named Network does not copy the Named Network structure. [BNNGF-48588]
- **Virtual Routing and Forwarding (VRF)** – Actively sending unsolicited ARP messages does not work with VRF. [BNNGF-52654]
- **Virtual Routing and Forwarding (VRF)** – Changing the ID of an active virtual router instance to another ID is currently not supported. Instead, see How to Delete a Virtual Router Instance and How to Configure and Activate a Virtual Router Instance with Hardware, Virtual, VLAN, or Bundled Interfaces.
- **Virtual Routing and Forwarding (VRF)** – Changing the MTU size for VR instances is currently not working as expected. [BNNGF-53385]
- **Virtual Routing and Forwarding (VRF)** – Configuration files for VR instances are currently not considered when moving PAR files between boxes. [BNNGF-53390]

Current Known Issues Related to the Web Interface for Cloud

- **Azure Cloud** – In Azure, after switching from Firewall Admin to the web interface, the connection can become very slow or even time out. [BNNGF-49960]
- **Backup/Restore** – For cloud instances, restoring configuration backups only works on model VFC8 model with BYOL.
- **SSL VPN** – SSL VPN on public cloud instances is currently not supported.