7.2.2 Release Notes

https://campus.barracuda.com/doc/78154642/

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.

First-Generation ATP to Second-Generation Barracuda ATP Cloud Migration

Changelog

To keep our customers informed, the Known Issues list and the release of hotfixes resolving these known issues are now updated regularly.

- 2018-08-16 – **Firmware version 7.2.2** released.
- 2018-08-23 – **Hotfix 881** - Azure Connectivity – The hotfix solves random Microsoft Azure network connectivity issues caused by the Hyper-V drivers (LIS). For more information, see Hotfix 881.
- 2018-08-23 – **Hotfix 883** - Curl-OpenSSL-Update – The hotfix provides a new curl binary and libcurl library which are linked against a newer OpenSSL version supporting newer algorithms. For more information, see Hotfix 883.
- 2018-08-23 – **Hotfix 884** - Azure-OMS-upgrade – The hotfix adds support for the latest versions of the Microsoft Azure OMS agent. For more information, see Hotfix 884.
- 2018-09-07 – **Hotfix 886** - Azure VWAN Connectivity – The hotfix provides automated connectivity to Azure Virtual WAN Preview. For more information, see Hotfix 886 and Barracuda Firewall Admin 7.2.2.
- 2018-11-21 – **Hotfix 889** - 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 889.

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 7.2.2 Migration Notes.

First-Generation ATP to Second-Generation Barracuda ATP Cloud Migration

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 7.2.2 Migration Notes.

What´s New in Version 7.2.2

Globally Configured Unique Server/Service Names

On a Control Center, server and service names can now be configured also globally as unique.

For more information, see How to Configure Virtual Servers.

Network Objects now Accepts IP Addresses and Hostnames

Network objects now accept IP addresses as well as hostnames and dresses or resolves a given hostname to its associated IP address.

For more information, see IP or Hostname Network Objects.

The use is limited to the CC and currently covers:

- Configuration of destination hosts for syslog streaming.
- Configuration of hostnames as proxy destination.

Event Notification for Unused Access Rules

The CloudGen Firewall now creates an event in case that an access rule has not been used for a given number of minutes. In case a network routing was configured wrong or network cables were patched wrong, this event will inform about traffic bypassing the firewall unexpectedly.

For more information, see Advanced Access Rule Settings and Security Events .

BRS

The Barracuda Reporting Server (BRS) is a hardware appliance purpose-built for rapidly generating reports while maintaining or improving the accuracy of reporting data. It also provides an aggregate view of data for customers with multiple connected devices.

For more information, see Barracuda Reporting Server (BRS) Integration.

Commandline PAR File Restore with CCDB

A command line tool called *cctool* has been implemented for backing up and restoring Control Center configurations including setups for FSCs.

For more information, see How to Backup and Restore CC Archive Par Files on the Command Line.

CloudGen Firewall and RSTP

RSTP on a CloudGen now creates events in case that the state of an RSTP link changes. This is useful for notifying administrators in case that links on the bridge change their state.

For more information, see Security Events .

Cloning Wizard

In the Control Center, cloning a box is now possible using a wizard.

For more information, see How to Add a New CloudGen Firewall to the Control Center.

Dynamic Firewall Rules

Administrators now can restrict enabling of dynamic firewall rules with time conditions.

For more information, see How to Restrict Enabling of Dynamic Firewall Rules.

Control Center Clustering

Control Centers can now be organized in a master to slave hierarchy.

For more information, see Control Centers in Master-to-Slave Relation

LED Status Improvements for Hotfixes

When installing a hotfix via USB during recovery, the firewall now indicates the status after the hotfix installation via its LEDs on the front panel.

Renaming of Clusters in the Control Center

It is now possible to add an individual description to the name of a cluster which will be displayed in the configuration tree of the Control Center.

Web UI for Virtual Appliances

The Web user interface is now also available for virtual appliances.

ATP on Small Appliances

Advanced Threat Protection (ATP) is now enabled on the F12 model where local virus scan is not possible due to resource restrictions. ATP provides full protection against viruses.

Active Bridging despite of Inactive Firewall

If configured, the bridge will now stay active even if the forwarding service is down.

Pool License Validity Improvement

Running release 7.2.2 or higher, services keep running with an additional grace of 24 hours after the pool license grace period has expired. The license keeps working, but configuration and updates are blocked.

Improvements Included in Version 7.2.2

Barracuda Firewall Admin

- In History View information about the output interface is now available. [BNNGF-29499]
- In Firewall Admin it is now possible to use wildcards for certificates in the subject alternative name. [BNNGF-43124]
- User interface improvements have been made in Firewall Admin for the SCA connector editor. [BNNGF-49796]
- In Firewall Admin group patterns are now selected correctly when double clicking a user entry. [BNNGF-50021]
- Firewall Admin now detects the F12 model. [BNNGF-50450]
- The VPN status page no longer displays IKEv2 tunnels multiple times in Firewall Admin. [BNNGF-50916]
- ATP entries in TOP THREATS now link correctly to the ATP tab in Firewall Admin. [BNNGF-51252]
- It is now possible to import network object as a CSV file that may also contain comments. [BNNGF-51982]
- Functionality for YouTube for Schools has been completely removed. [BNNGF-52011]
- Firewall Admin no longer shows wrong time values when accessing the VPN cache. [BNNGF-52610]
- Validation check for generic edit fields now accepts checking for allowed and forbidden characters. [BNNGF-52875]
- Tabs with the exception of the SSH tab can now be closed by typing CTRL-W on the keyboard.

[BNNGF-53008]
- In Firewall Admin the Status Map now allows to use the management IP address to get access to the CloudGen Firewall. [BNNGF-53154]
- VPN tunnels are now displayed in ascending or descending order depending on their Local IP and the sort order selection. [BNNGF-53168]
- In the IP view in Control > Network the modem interface has been renamed to be displayed as WWAN[ppp5]. [BNNGF-53246]
- In the SSL Policies table it is now possible to see which rules are using a policy. [BNNGF-53491]
- When configuring TI the transport selection no longer shows double entries. [BNNGF-53529]
- For propagation list, input is now limited to 64 characters. [BNNGF-53881]
- Enabling the CC database is now possible if a user opens the SCA editor for the first time. [BNNGF-53979]
- Barracuda Threatclass as the IP lookup tool in Firewall Admin has been replaced by https://db-ip.com/. [BNNGF-54223]
- Rule lists that are restricted to a certain VRI can now be updated. [BNNGF-54515]

Barracuda OS

- The firewall now supports untagged VLANs in combination with tagged ones. [BNNGF-40337]
- 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]
- The firewall no longer crashes in certain situations. [BNNGF-52464]
- A change of the log level to DEBUG for DC Client authentication information now reduces the size of the log file. [BNNGF-52590]
- Referencing from Generic Network Objects to IPv6 Network Objects is now allowed for explicit Src/Dst fields in access rule editor. [BNNGF-52722]
- Properties under Application Filter are now correctly associated with a logical AND. [BNNGF-52855]
- 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 crashes in certain situations. [BNNGF-52962]
- Changing the ID of an existing Virtual Router instance now works as expected. [BNNGF-52979]
- The captive portal detection to present the CP splash screen now works as expected. [BNNGF-53136]
- 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]
- The table umts1 with a default router has been added to the M40 model. [BNNGF-53231]
- In Firewall Admin all text labels with the name UMTS haven been renamed to WWAN. [BNNGF-53247]
- Redirections to the Landing Page are now working as expected for HTTPS. [BNNGF-53361]
- Idle time calculations for the session idle timer are now working as expected. [BNNGF-53398]
- MPEG elementary streams are now detected as a streaming content. [BNNGF-53412]
- License handling has been improved for managed boxes. [BNNGF-53512]
- Access rules with MAC based source addresses now pass traffic as expected. [BNNGF-53515]

- SMTP no longer causes problems with reddoxx mail servers. [BNNGF-53530]
- 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]
- In a HA setup hostname and boxname are now consistent. [BNNGF-53634]
- IPv6 rules sets now load as expected with more than one objects as destination. [BNNGF-53638]
- TCP sessions via dynmesh are no longer switched to RAWTCP. [BNNGF-53675]
- Entering "View" and "Peers" is now mandatory when configuring SNMP. [BNNGF-53702]
- Changing the ID of an existing Virtual Router instance no longer causes an inconsistency in forwarding rules. [BNNGF-53961]
- 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]
- HA session synchronization is now visualised in Firewall Admin under DASHBOARD > Firewall > NETWORKING SERVICES. [BNNGF-54206]
- In the GTI editor, the option 'Like-System-Settings' is now available as Proxy type. [BNNGF-54213]
- If 'Scanning for SSL intercepted traffic' is turned off, traffic is now handled correctly by the Intrusion Prevention System (IPS). [BNNGF-54222]
- The VPNAC service can now be used as expected after its creation. [BNNGF-54314]
- The firewall now sends unsolicited ARPs in VRFs after server starts. [BNNGF-54416]
- During an HA takeover duplicate IPs no longer show up in an additional VRI. [BNNGF-54417]

Control Center

- Repositories are now correctly linked when migrating a cluster on a Control Center. [BNNGF-51508]
- The Control Center no longer displays incorrect information for failed activations of Vx boxes. [BNNGF-52052]
- Access to the Control Center database has been improved. [BNNGF-52998]
- It is no longer possible to use the same name for Global and Cluster settings when configuring Secure Connector Networks. [BNNGF-53022]
- DHCP configuration for SCAs now uses the same settings as on CloudGen firewalls. [BNNGF-53395]
- Creating S-Series boxes in a scripted manner now works as expected. [BNNGF-53434]
- In the Control Center is is now possible to enforce unique server and services names. [BNNGF-53510]
- 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]
- In the SCA editor, IP ranges are now checked correctly for DHCP. [BNNGF-53679]
- /30, /31 and /32 hostmasks are now allowed for SCAs as data networks. [BNNGF-53738]
- On a Control Center terms of agreement are now displayed correctly when using a proxy. [BNNGF-53756]

- Renaming of SACs no longer causes errors when creating SAC boxes. [BNNGF-53841]
- Using 'Link overrides' for repositories in connection with SSLVPN no longer causes problems. [BNNGF-53901]

Firewall

- TF-Firewall syncs are displayed correctly. [BNNGF-36748]
- IPv6 ICMP 'Destination unreachable' messages are now forwarded as expected. [BNNGF-39029]
- If AV is active in an access rule, the TCP option for maximum segment size is no longer ignored. [BNNGF-46737]
- Network objects now accept longer DNS names up to a length of 96 characters. [BNNGF-48702]

Virus Scanner and ATP

- The Asia Pacific region has been added to the Barracuda ATP region selection. [BNNGF-51900]
- ATP status in ATP tab is updated every 30 seconds. [BNNGF-52727]
- ATP is now enabled on the F12 model where local virus scan is not possible due to resource restrictions. [BNNGF-53338]

VPN

- The First + Second IP addresses are now included in the export file when exporting a VPN Group Policy. [BNNGF-47655]
- The firewall no longer crashes due to a race condition in cipher initialization. [BNNGF-52291]
- The firewall no longer crashes in certain situations. [BNNGF-53116]
- C2S certificate authentication no longer fails. [BNNGF-53619]
- L2TP no longer prevents proper restart of the VPN service due to high loads. [BNNGF-53710]
- The reverse routing check no longer fails in case that the B0 dynmesh transport is not active. [BNNGF-53773]

Web UI

- The Web based user interface has been added to virtual appliances. [BNNGF-53155]

ZTD

- Units deployed with the Zero Touch feature no longer show issues during firmware upgrades. [BNNGF-51005]

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 Delivery" option and SMTP-AUTH is not yet supported. [BNNGF-52992]
- **ATP** – The "Scan first, then Delivery" option and using an MUA (eMail client) - NGFW - MTA is currently not supported. [BNNGF-52992]
- **ATP** – The "Scan first, then Delivery" option and using BDAT (e.g. Microsoft Exchange servers may use that) is not yet supported. [BNNGF-52992]
- **ATP** – The "Scan first, then Delivery" 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 does not work on models except VFC8 model with BYOL.
- **SSL VPN** – SSL VPN on public cloud instances is currently not supported.