

7.2.5 Release Notes

<https://campus.barracuda.com/doc/90442534/>

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.

- 22.10.2019 - **Firmware version 7.2.5** released.

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 [7.2.5 Migration Notes](#).

What's New in Version 7.2.5

CloudGen Firewall firmware 7.2.5 is a maintenance release. No new features were added.

Improvements Included in Version 7.2.5

Barracuda Firewall Admin

- SPAM tag/headers can now be configured individually. [BNNGF-55785]
- External administrators can now access the ATP tab as expected. [BNNGF-59652]
- The Firmware Update page no longer shows unallowed appliances from different ranges.

[BNNGF-59757]

- The list that is displayed when right-clicking an entry in the list of **FIREWALL > History** now shows **Clear History** as one of its entries. [BNNGF-60129]
- On an F600D, connected interfaces are now shown correctly on the **Dashboard**. [BNNGF-60240]
- A rendering issue in the Access Control Service view has been fixed. [BNNGF-60404]
- The SNMP service ACL input field in **CONFIGURATION > Configuration Tree > SNMP Service Settings > Access Groups > Peers** now accepts IPv6 addresses correctly. [BNNGF-61517]

Barracuda OS

- The firewall establishes connections via SAC as expected. [BNNGF-43766]
- When QoS is enabled, GRE tunnels now work as expected. [BNNGF-54027]
- Changing the LAN mode from **Manual** to **DHCP Server** for an SC now works as expected. [BNNGF-55676]
- Configurations from other models imported on F183 are now correctly migrated. [BNNGF-56850]
- Allow adding BCC credentials for automatic license download. [BNNGF-58428]
- Firewall Insights is now fully supported by firmware release 7.2.5. [BNNGF-59104]
- Network routes are now correctly introduced when using the M40 modem. [BNNGF-59579]
- Users can now authenticate and access the VPN if more than 10 MSAD servers are in the list. [BNNGF-59643]
- Multi-path routes with two gateways on different interfaces now work correctly. [BNNGF-59892]
- HA synchronization now works as expected both with and without a trustzone. [BNNGF-60053]
- Kernel has been updated and now covers CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479. [BNNGF-60349]
- In the SC editor, it is now possible to enter LTE user credentials. [BNNGF-60423]
- BIND has been updated to version 9.11.8 [BNNGF-60667]
- The access denied error message is now correctly displayed every time the block page is reloaded. [BNNGF-61188]
- Authentication using DC agent now works as expected. [BNNGF-61510]
- HTTP requests are no longer blocked by the URL filter unless the session counter does not exceed the configured limit. [BNNGF-61778]

Control Center

- Control Center administrators can no longer see pool licenses they are not allowed to see. [BNNGF-51704]
- Phion legacy pool licenses are now correctly displayed in **CONTROL > Pool Licenses**. [BNNGF-52971]
- Pool licenses of SC1 are now displayed correctly in **CONTROL > Barracuda Activation > Pool Licenses**. [BNNGF-53805]
- When migrating clusters, protocol entries are no longer broken in an application rule. [BNNGF-56252]

- VPN Access Control service now works correctly when migrating clusters from 7.0 to 7.2. [BNNGF-59208]
- In the Control Center, in **CONFIGURATION > Configuration Tree**, in the **Boxes** tab of the **Quick File Access** area, it is now possible to bulk enable/disable boxes for editing. [BNNGF-60532]
- Firewall Insights licenses are now shown correctly. [BNNGF-60536]
- Cloning a box using the Clone Wizard now sets the status of the cloned box to **enabled**. [BNNGF-60601]
- The **Create Box Wizard** now configures network interfaces correctly. [BNNGF-60738]

Firewall

- Dynamic rules are now terminated correctly if the user tries to **Disable & Terminate** it. [BNNGF-48333]
- The firewall no longer crashes in certain situations. [BNNGF-60612]
- Transparent redirect now works as expected. [BNNGF-60951]

Virus Scanner and ATP

- In case ATP has blocked a mail attachment, the replaced mail attachment has a valid filename extension and can now be opened as expected. [BNNGF-60949]

VPN

- IKEv2 now binds to all network interfaces if **Use IPsec dynamic IPs** is set to **yes**. [BNNGF-58259]
- Terminating IPsec VPN tunnels now works as expected. [BNNGF-59647]
- DYNMESH is now established correctly on multiple transports. [BNNGF-59773]
- IPsec tunnels no longer crash in rare situations. [BNNGF-60371]
- Client-to-site authentication scheme **Extract from Username** now also works for IPsec tunnels. [BNNGF-60397]
- Fixed an authenticated path traversal vulnerability in the VPN service. [BNNGF-60817]

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]
- **Create-dha** - In the Google Cloud, if the devices of a high availability cluster are in two different subnets, the create-dha tool cannot be used. [BNNGF-62445]
- **Firewall Admin** - Copy and paste of an access rule with explicit Named Network does not copy the Named Network structure. [BNNGF-48588]
- **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.
- **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-53208]
- **Virtual Routing and Forwarding (VRF)** - Configuration files for VR instances are currently not considered when moving PAR files between boxes. [BNNGF-53390]
- **VPN** - The IKE3 daemon crashes when establishing an IPsec C2S connection. [BNNGF-63401]

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.

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.