7.2.6 Release Notes

https://campus.barracuda.com/doc/90445688/

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.

- 12.3.2020 – **Firmware version 7.2.6** 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 7.2.6 Migration Notes.

Support for Firewall Admin

Barracuda Networks drops support for Firewall Admin running on Windows 7 and 8.0.

What´s New in Version 7.2.6

CloudGen Firewall firmware 7.2.6 is a maintenance release. No new features were added.

Improvements Included in Version 7.2.6

Barracuda Firewall Admin

- The set of hyphening characters for the naming of authentication schemes in **CONFIGURATION > Configuration Tree > Assigned Services > VPN > Client to Site**, tab **Group Policy**, window **Group VPN Settings**, section **Preauthentication**, window **Preauthentication Details > New Name/Scheme Mapping**, now also supports the '-' character. [BNNGF-61804]
- The geo-ip field in **Box > Properties > Geo Location** can now be manually overridden to store locations for SD-WAN and Firewall Insights. [BNNGF-62911]
- Firewall Admin now displays the correct number of sessions in **Firewall > Live**. [BNNGF-63675]
- Firewall Admin now displays a warning message when configuring .PAR files to be the default for creating backup archives. [BNNGF-64122]

Barracuda OS

- In case the modem access to a provider becomes invalid due to a misconfigured SIM-PIN, the credentials can now be reset using a command line tool. [BNNGF-52796]
- The firewall sends ARP requests for configured networks as expected. [BNNGF-56888]
- In case of an HA failover with IPv6 addresses, the MAC addresses are now advertised as expected. [BNNGF-58404]
- The edit fields for configuring the geolocation have been updated both for stand-alone boxes in **CONFIGURATION > Configuration Tree > Box > Properties > Geo Location** and on the Control Center in **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > *your range* > *your cluster* > Boxes > *your box* > Properties > Geo Location**. [BNNGF-60433]
- Local administrators no longer can log on after their accounts have been deleted. [BNNGF-60995]
- URL categories are now written into the firewall activity log as expected. [BNNGF-61101]
- LOUT traffic is now terminated as expected when the respective session is killed via the GUI. [BNNGF-61204]
- The user interface in Firewall Admin now works as expected if Weblog Streaming in **CONFIGURATION > Configuration Tree > Syslog Streaming** is deactivated. [BNNGF-61941]
- The Apple Push Notification certificate has been renewed. [BNNGF-62257]
- The default bootload delay has been set to 0. [BNNGF-62442]
- During a nested SSH connection from Firewall Admin via a Control Center to a managed box, file uploads from Firewall Admin will be done to the first SSH-connected device in the SSH chain. [BNNGF-62605]
- The M40 modem no longer loses its connection unexpectedly. [BNNGF-62916]
- The method for downloading lists of Azure IPs has been improved. [BNNGF-63160]
- Processing X.509 certificates no longer fails when special characters are contained in the certificate. [BNNGF-63277]
- The correct time is now displayed for logged-in users. [BNNGF-63359]

- The firewall no longer crashes in certain situations. [BNNGF-63905]
- When logging into a firewall, the **Installation Wizard** no longer asks a second time for the password in case the default password has already been changed. [BNNGF-63921]
- OSPFv3 for IPv6 is now working as expected. [BNNGF-64101]
- Granting shell level access to CC administrators now works as expected. [BNNGF-64102]
- The parameter **Bandwidth** in **CONFIGURATION > Configuration Tree > Virtual Servers > *my virtual server* > Assigned Services > OSPF/RIP/BGP > OSPF/RIP/BGP Settings**, left navigation bar, **Network Interfaces**, window **Interfaces**, section **OSPF Specific Parameters**, now accepts values with up to 10 digits. [BNNGF-64430]
- Migrating an F400B firewall to any F600D model now works as expected. [BNNGF-64524]
- CC Admin authentication with Yubikey + TACACS now works as expected. [BNNGF-64608]

Control Center

- In **Control Center > NETWORK ACCESS CLIENT > Status VPN**, the table is now restricted to display only entries for admins with respective access rights for range/cluster. [BNNGF-54873]
- The CC syslog now handles certificate chains. [BNNGF-61963]
- In **Control Center -> NETWORK ACCESS CLIENT -> Status VPN**, the table is now restricted to display only entries for admins with respective access rights for range/cluster. [BNNGF-62922]
- Firewall Admin no longer crashes if pasted strings contain tabulators for the cluster description. [BNNGF-63310]
- VIP networks for VPN offloading can now be configured as expected and are available in the **VPN Setting** of the VPNAC service. [BNNGF-64137]

Firewall

- X.509 certificates are now correctly handled for firewall/users. [BNNGF-62907]
- URL detection in HTML mails has been improved. [BNNGF-63255]

HTTP Proxy

- The proxy cache is now created correctly and no longer causes failures if a configuration is reloaded by the firewall. [BNNGF-61836]
- The HTTP proxy detects the eicar virus as expected. [BNNGF-62443]
- Several security issues for the HTTP proxy have been fixed. [BNNGF-63634, BNNGF-64604]

Virus Scanner and ATP

- Scanning antivirus content now honors all entries in the HTTP exception list. [BNNGF-62136]
- ATP for SMTP with scan-first now delivers mail to the correct port using PAT. [BNNGF-62252]

VPN

- When establishing an IPsec tunnel, the IPsec responder now checks for all configured proposals in phase2 and matches the configuration as expected. [BNNGF-56385]

- The firewall now removes unneeded listening sockets in case a connection cannot be established via a tunnel. [BNNGF-58575]
- When working with DYNMESH, the status DB is now correctly updated after a spoke failover. [BNNGF-62929]
- Disabling and re-enabling a VPN TINA tunnel no longer causes a routing problem. [BNNGF-62958]
- DynMesh log entries are now created only if the respective service is activated. [BNNGF-63230]
- IPsec client-to-site connections no longer fail in certain situations. [BNNGF-63401]
- IKEv1 AWS tunnels are now rekeying as expected. [BNNGF-64498]

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]
- **Google Cloud** – If the devices of a high availability cluster are in two different subnets, the create-dha tool cannot be used. [BNNGF-62445]
- **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]
- **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]
- **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** – On clients using NAC to connect to a VPN, direct access does not pick up stored credentials from the Windows credential vault. [BNNGF-64306]

Current Known Issues Related to the Web Interface for Cloud

- **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.
- **Firewall** – If application-based provider selection is activated, low data rates can occur in rare situations.
  Workaround: consider upgrading to firmware version 8.0 or higher.

© 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.