7.2.1 EA2 Release Notes

https://campus.barracuda.com/doc/75695679/

Early Release

EA firmware is available to early adopters who wish to test the latest features from Barracuda Networks, or who have a specific need for early access to a new feature or fix that would be beneficial to your environment.

The 7.2.1 EA2 release will not be displayed in the dashboard element of CloudGen Admin and will not be listed in the Control Center as a firmware update.

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.

- 2018-05-28 – Firmware version 7.2.1 EA2 released.
- 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 7.2.1 EA2 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).

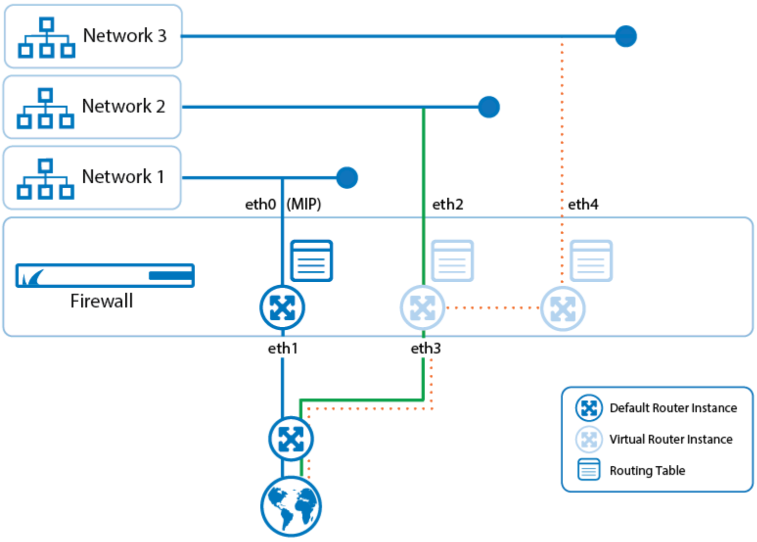
For more information, see 7.2.1 EA2 Migration Notes.

What´s New in Version 7.2.1 EA2

CloudGen Firewall and Virtual Routing and Forwarding (VRF)

Virtual routing and forwarding (VRF) is a technology based on the operating principle of a physical router. Unlike a single router, virtual routers (VR) can be run simultaneously as multiple instances where each uses its own routing table. Virtual routing can be used to segment network paths without using additional devices. The concept of keeping traffic on multiple network paths separated offers a huge variety of applications.

For more information, see Virtual Routing and Forwarding (VRF).



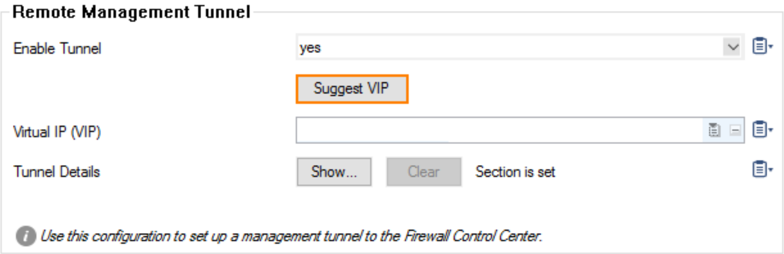
CloudGen Firewall and RSTP

The CloudGen Firewall now supports Layer 2 bridging with RSTP. The configuration of RSTP is fully integrated into the configuration window of Layer 2 bridging.

For more information, see How to Activate RSTP.

Improved UI support for Configuration of Virtual IPs for Remote Management Tunnels

Splitting network addresses into subnets and preserving them for future use always leads to fragmentation, often at the cost of a good overview. Knowing which private address is already used and which addresses are still available is essential for the configuration of remote management tunnels. Configuring a remote management tunnel now is supported by a button that helps to find free private IP addresses quickly that are available for VIP addresses.



Remote Management Tunnel

Enable Tunnel: yes

Virtual IP (VIP):

Tunnel Details: Section is set

Use this configuration to set up a management tunnel to the Firewall Control Center.

For more information, see [How to Configure a Remote Management Tunnel for a CloudGen Firewall.]()

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.]()

Improvements Included in Version 7.2.1 EA2

Barracuda CloudGen Admin

- UPNP broadcasts/multicasts now show the correct output interface in Live/History view. [BNNGF-29347]
- CC administrators can no longer access or view licenses in **CONTROL > Licenses** in case they are not allowed to. [BNNGF-36306]
- 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]
- CloudGen Admin now shows the completion of firmware download as expected. [BNNGF-44064]
- The IPsec IKEv2 window now fits into workspaces with a smaller resolution. [BNNGF-45223]
- In CloudGen Admin, the DNS user interface has been updated for configurations with "Negative Cache TTL" values. [BNNGF-45414]
- In CloudGen Admin and the web UI, Wi-Fi configurations are now created correctly by the box wizard. [BNNGF-47294]
- Changing the order of referenced network objects no longer deletes the reference name. [BNNGF-48440]
- 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]
- Server and service names can now be up to a length of 30 characters. [BNNGF-49121]
- The **RECENT SEVERE EVENTS** element in the **DASHBOARD** now displays the correct time. [BNNGF-49393]
- QoS configuration is available only for IPv4. [BNNGF-50067]
- Copying serial numbers to the clipboard now works as expected in the Control Center activation tab. [BNNGF-50512]
- When switching from firewall rule types supporting SSL Inspection to rule types not supporting it, SSL Interception is now correctly disabled. [BNNGF-50534]
- A **BLOCK** rule cloned from a **PASS** rule no longer contains the original references to SSL Inspection Policies. [BNNGF-50561]
- Client-to-site group policies are now correctly limited to support a maximum of 64 routes. [BNNGF-50604]
- Peer and local addresses are now displayed correctly in the CloudGen Admin VPN status pages. [BNNGF-50699]
- The connection status for a Barracuda Reporting Server is now displayed as expected. [BNNGF-50818]
- Display of firewall users in grouped view is no longer rendered unreadable with long group text. [BNNGF-50826]
- The certificate editor has been improved. [BNNGF-50930]
- 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]
- Blocking search strings and search results via the custom app Google Search now also correctly blocks Google autocomplete results. [BNNGF-51079]
- Merging logs is now allowed by default. [BNNGF-51244]
- Barracuda CloudGen Admin no longer crashes after a Windows update. [BNNGF-51256]
- The UI for site-to-site VPN connections now includes an edit field for changing the port for the TINA tunnel. [BNNGF-51415]
- The ATP status is displayed in the ATP element of the Dashboard and the ATP tab. [BNNGF-51585]
- 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]
- When creating a new rule, no application policies and no shaping are preset in the rule editor. [BNNGF-51977]
- For CloudGen Admin, a combined column for Geo Location, Named Networks, and the IP Address is available for Live and History view. [BNNGF-52536]
- Named Networks now work with configured IP addresses as expected. [BNNGF-52560]
- Refreshing tabs in **CONTROL > Network** now works as expected. [BNNGF-52678]
- Dashboard widgets are now disabled for the F10/F15/F100 models. [BNNGF-52926]
- SCADA Detection/Inspection has been renamed to **SCADA Protocol Detection**. [BNNGF-53033]

Barracuda OS

- DHCP client connection attempts no longer produce connection issues. [BNNGF-32801]

- Bonding interfaces no longer have to be named with a sequential name. [BNNGF-38352]
- Application Based Link Selection now works as expected for Office 365. [BNNGF-40234]
- Infinite lifetime for IPv6 prefixes is now configurable. [BNNGF-42733]
- The firewall no longer crashes in a VMWARE ESXI 6.0.0 environment. [BNNGF-43656]
- Excluding networks from PROXY ARPs now works as expected. [BNNGF-48299]
- Attachments with .eml extensions are now scanned regardless of specified content type. [BNNGF-48677]
- Using the NTLM protocol for authentication over a forward proxy now works as expected. [BNNGF-48709]
- TCP sessions now terminate after being idle for 24 hours. [BNNGF-49525]
- SSL Interception with RPC over HTTPS now works as expected. [BNNGF-49600]
- When handling FTP data, the firewall no longer produces a segmentation fault in certain situations. [BNNGF-49676]
- Tcpdump no longer disables a bundled interface in promiscuous mode. [BNNGF-49793]
- The IPv4 address of the B-root DNS server has been updated. [BNNGF-49948]
- Firewall activity log changes has been improved. [BNNGF-50169]
- Barracuda Firewall now supports USB M40/41 LTE Modem. [BNNGF-50451]
- On an F183R, the LED now shows the correct color after the installation. [BNNGF-50598]
- In case a network interface goes down the event ID 50 (Device Down) is now correctly triggered. [BNNGF-50608]
- On the F82, **Control > Resources** now displays the RPM for the fan. [BNNGF-50653]
- Event ID 3000 (VPN Service Tunnel Terminated) is now correctly triggered if VPN tunnels get terminated. [BNNGF-50824]
- Interfaces are now set up correctly when performing a soft network activation. [BNNGF-50842]
- HA takeover now works in acceptable time as expected. [BNNGF-50887]
- Overriding a URL category now works as expected. [BNNGF-50948]
- Network activation no longer fails due to empty MTU parameter on the VLAN interface. [BNNGF-51022]
- Running a bridging setup under heavy load for several hours now works as expected. [BNNGF-51044]
- Flapping routes no longer occur in case a routed bridge is configured between your LAN and Wi-Fi. [BNNGF-51087]
- FTP handling now works as expected if the FTP plugin is configured correctly. [BNNGF-51116]
- Port mapping has been adapted for F1000 with 40 Gbps. [BNNGF-51144]
- Silently dropped packets occuring if no firewall rule set is loaded, now also create a firewall History entry. [BNNGF-51272]
- The firewall and authentication service correctly synchronize login events to prevent users from being displayed as logged in. [BNNGF-51420]
- Memory leaks no longer occur in certain cases. [BNNGF-51353]
- The ClamAV virus scanner has been updated. [BNNGF-51576]
- The firewall no longer crashes in certain situations. [BNNGF-51667]
- On hardware boxes, acquiring an IPv6 address from the ISP after setting up a DHCPv6 link now works as expected. [BNNGF-51708]
- When an activation of a configuration fails, error messages are now displayed. [BNNGF-51867]
- The firewall now checks for the FTP plugin in the access rule's service object to decide whether Application Control is required. [BNNGF-52054]

- LDAP authentication timeout can now be configured. [BNNGF-52123]
- VLANs now work in ART mode. [BNNGF-52168]
- The default policy for the Proxy Web Filter is now **allow-all-except**. [BNNGF-52175]
- The statistics for disk reads and writes are now calculated correctly. [BNNGF-52203]
- Self-referencing network objects are no longer allowed. [BNNGF-52282]
- The SNMP box service now shows the correct IPsec tunnel state. [BNNGF-52453]
- Certain IP addresses are no longer re-evaluated in environments where DC Agent and Auth Sync are enabled through multiple locations. [BNNGF-52550]
- Interface statistics for VPN now work as expected. [BNNGF-52594]
- Custom MTU sizes now work as expected. [BNNGF-52644]
- External admin login now accepts the underscore character in the login name. [BNNGF-52791]
- FTPS can now be blocked on non-standard ports. [BNNGF-53010]
- The firewall no longer performs interface checks after setting Session Creation to "disabled" in **Forwarding Firewall -> Rule -> Advanced -> Interface Checks**. [BNNGF-53052]
- The size limitations for the forwarding ruleset have been increased. [BNNGF-53076]
- The firewall no longer produces misleading log entries in certain situations. [BNNGF-53131]
- The limitation for TINA routes has been raised to 50kB. [BNNGF-53146]
- The check box for "Allow SSLv2" has been removed for all firmware versions that no longer support it. [BNNGF-53170]
- Interface checks can now be disabled after a session creation. [BNNGF-53347]

Control Center

- After deleting a GTI group configuration, the configuration files now are removed. [BNNGF-37491]
- The settings for VPN AC are now updated as expected when using a template. [BNNGF-40464]
- Repository overrides are not lost when moving a server or a box to another cluster / range. [BNNGF-41785]
- Cloud units are now also displayed with different icons. [BNNGF-49956]
- In the Control Center, floating licenses are no longer removed due to differing hash. [BNNGF-50654]
- In the Control Center, pushing an SC to Zero Touch no longer fails when the model version is inherited from a template. [BNNGF-50762]
- Replacing/merging configurations using the clipboard in CloudGen Admin now works as expected in the SCA editor. [BNNGF-50872]
- CloudGen Admin now also displays SC2 boxes during Zero Touch deployment. [BNNGF-50954]
- Migrating an SC from version 1.0 to 1.1 no longer triggers a verification check. [BNNGF-51159]
- A manually defined LAN for the SC now gets introduced into the routing table of the SAC. [BNNGF-51323]
- SCA models are now being regarded in configurations and templates. [BNNGF-51412]
- On the Control Center, the Unit description is no longer missing after a firmware update. [BNNGF-51660]
- SSL VPN configuration nodes can now be linked to a repository. [BNNGF-51661]
- The M40 LTE modem has been integrated into the SCA2 user interface on the Control Center. [BNNGF-52029]
- Migrating a cluster no longer causes repository-linked C-Firewall rules to be renamed to

"Default". [BNNGF-52748]

DNS

- The B-Root DNS server has been updated on the firewall. [BNNGF-50390]

Firewall

- ISO files are now blocked from downloading when a file content policy has been configured. [BNNGF-48292]
- Local-in SSH connections to the box are no longer unexpectedly blocked. [BNNGF-48439]
- SSL Inspection policies are now able to download Intermediate CA Certificates automatically. [BNNGF-48865]
- Application Based Provider Selection now handles traffic from YouTube and media streaming services. [BNNGF-50503]
- 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]
- The time limit for checking revocations can now be increased during configuration. [BNNGF-51031]
- FTP data sessions are no longer evaluated against application rules if the FTP plugin is active and if Application Control is disabled. [BNNGF-51059]
- 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]
- With Application Based Link Selection enabled, access to services like Office Portal now work as expected. [BNNGF-51619]
- Opening www.mediamarkt.pl with SSL Interception now works as expected. [BNNGF-52245]
- Disabling outbound QoS, while inbound QoS is still active, no longer negatively affects network traffic. [BNNGF-52281
- The Firewall Activity Log now contains correct messages for **DROP/BLOCK** actions. [BNNGF-52434]
- Outlook can again connect to the Exchange server when SSL Interception and Virus Scanning are enabled. [BNNGF-52519]
- Passive PUT and active GET file transfers are now virus scanned if the FTP plugin is active. [BNNGF-52650]
- In **Live** and **History** view, POP3/S and SMTP/S entries are now displayed correctly. [BNNGF-50878]

FSC

- DHCP relay functionality for LAN and WAN has been added to the FSC. [BNNGF-51340]

HTTP Proxy

- For the HTTP proxy, identical names for visible hostname and backend hostnames are not allowed. [BNNGF-48550]

Public Cloud

- On a Hyper-V 2012 and 2016 server, VLAN traffic is now handled correctly. [BNNGF-49703]
- On Hyper-V, the firewall boots again if you have more than 4 interfaces configured. [BNNGF-49791]
- Resetting the password or SSH key now works as expected when the web UI is activated. [BNNGF-50299]
- Resetting a password in an Azure Portal no longer causes memory leaks. [BNNGF-50721]
- Identifying VMs in Azure now creates paginated output to display found resources. [BNNGF-50778]
- Creating a PAR file via the web UI and re-importing it now works as expected. [BNNGF-51253]
- PAYG licenses are now pushed to the Control Center when the PAR file retrieval is done. [BNNGF-51320]
- After a successful PAR file import, the one-time token is now successfully cleared. [BNNGF-51321]
- A new cloud utility for setting up multiple static NICs during provisioning has been created. [BNNGF-51396]
- Configuration support has been added for the new model VFC1. [BNNGF-51403]

REST API

- REST calls to the Status Map endpoint no longer cause timeout problems. [BNNGF-52450, BNNGF-52452]
- The REST-API now provides an interface for license activation. [BNNGF-45141]

SSL-VPN

- SSL VPN now allows to enable all protocol versions for a web forward. [BNNGS-3252]
- SMBv2/v3 support for Network places is now provided. [BNNGS-3228]
- Module help text for SSL-VPN has been improved. [BNNGS-3203]
- Devices are now allowed to retrieve custom VPN profiles. [BNNGS-3199]
- After an update from 7.0.x to 7.1.1, Radius authentication with Group Attribute now works as expected. [BNNGS-3208]
- Drive redirection now works on RDP connections. [BNNGS-3266]
- Using `${session:username}` with Network Places now works as expected. [BNNGS-3196]
- It is now possible to enable firewall rules for 1041d, 7h and 38m. [BNNGS-3250]

Virus Scanner and ATP

- Reloading of ATD pages no longer causes a potential IP spoofing attempt on the firewall. [BNNGF-26793]
- Null-byte reverse-proxy attacks no longer result in a high load of the virus scanning engine.

[BNNGF-49628]
- The Virus Scanner no longer produces core dumps in certain situations. [BNNGF-50851]
- The Virus Scanner and ATP no longer cause a crash when using OpenSSL. [BNNGF-50871]
- Operational performance of the Virus Scanner has been improved. [BNNGF-52126]
- The file size limit has been increased to 10 MB for ATP. [BNNGF-52467]

VPN

- IKEv1 site-to-site settings no longer let client-to-site connections fail for iOS. [BNNGF-50014]
- The port number for TINA tunnels can now be assigned for site-to-site connections. [BNNGF-50069]
- 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]
- A VPN client connection via CudaLaunch no longer fails from an iOS device. [BNNGF-50849]
- Syncing HA tunnels to the HA partner is now activated by default. [BNNGF-51153]
- CloudGen Admin no longer proposes pure ESP in phase 2 if NAT has been detected in phase 1. [BNNGF-51228]
- The X.509 explicit authentication method for a site-to-site tunnel now works as expected. [BNNGF-51237]
- IKEv2 does not trigger events when tunnel is terminated. [BNNGF-52338]
- iOS IPsec connections now work as expected. [BNNGF-52557]

Web UI

- When configuring a TINA tunnel, local and remote network objects are added to the network objects. [BNNGF-50637]
- After restoring a backup, IPsec tunnels now have the correct custom policy. [BNNGF-50652]
- DynDNS settings are now restored correctly from a backup. [BNNGF-50668]
- Creating a cascaded rule list now works as expected. [BNNGF-51178]
- The Application Monitor no longer displays pop-over errors for unknown data. [BNNGF-52017]

Zero Touch Deployment

- The ZTD notification view no longer resets when a new event is created. [BNNGF-48452]
- Units deployed with ZTD no longer show issues during firmware upgrades. [BNNGF-51005]
- The status of a firewall deployed with ZTD is no longer is inconsistent in some situations. [BNNGF-51408]
- The ZTD feedback message on S-Series units was updated to be more clear. [BNNGF-51409]

Current Known Issues - General

- **Firewall** – Pasting firewall rules that are using SLL Inspection Policies can cause problems if the target firewall rule set runs with feature level < 7.2. [BNNGF-53952]
- **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** – Time objects/schedule objects that are created in the global, range, or cluster firewall objects do not show up in the firewall rulesets. [BNNGF-49512]
- **Control Center** – S-Series boxes can not be created anymore in the Control Center after ZTD token has been issued. [BNNGF-53434]
- **Firewall** – Access rules with MAC-based source addresses may fail in certain situations. [BNNGF-53515]
- **Mail Security** – Retrieving messages POP3 may result in the first character of the mail body to be missing. [BNNGF-50969]
- **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.
- **CloudGen Admin** – Copy and paste of an access rule with explicit Named Network does not copy the Named Network structure. [BNNGF-48588]
- **CloudGen Admin** – When connecting with CloudGen Admin 7.2.x to a Control Center 7.2.x, the **Open Box Firewall** icon is not displayed for a firewall in the **Status Map** window. [BNNGF-50198]
- **URL-Filtering** – The mechanism for overriding URL categories does not work as expected. [BNNGF-50948]
- **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]
- **Virus Scanner** – The POP3 protocol currently only works on port 110. [BNNGF-50767]

Current Known Issues Related to the Web Interface for Cloud

- **Azure Cloud** – In Azure, after switching from CloudGen Admin to the web interface, the connection can become very slow or even time out. [BNNGF-49960]

- **Azure Cloud** – Resetting the password or an SSH key does not work when the web interface is activated. [BNNGF-50299]
- **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.

Figures