8.0.4 Release Notes

https://campus.barracuda.com/doc/93200022/

After updating to firmware release 8.0.4, Barracuda Networks highly recommends you to install hotfix-1037, which resolves stability issues.
For more information and to download the hotfix, see Hotfix-1037 in the download portal.

Changelog

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

- **10.12.2020 Hotfix 1039** – This is a cumulative hotfix with CloudGen Access Proxy support. It also contains hotfix 1037 for VPN tunnels and stability improvements for the application detection engine, and hotfix 1038, which covers firmware functionality for desktop appliances F180b and F280c.
  For more information, see Hotfix-1039-8.0.4.
  Note: The IPv6 implementation for the CloudGen Access Proxy will be part of an upcoming release.
- **17.2.2021 Hotfix 1041** – This hotfix solves several issues for the CloudGen Access proxy and ties the CGA service to the EU licensing policy.
  For more information, see Hotfix-1041-8.0.4.
- **25.3.2021 Hotfix 1045** - This cumulative hotfix includes hotfix #1041 (CGA/EU licensing policy), hotfix #1039 (Barracuda CloudGen Access Proxy service), hotfix #1038 (firmware functionality for desktop appliances F180b, F280c) and hotfix #1037 (VPN tunnels).
  For more information, see Hotfix-1045-8.0.4.

If you are using...

- xDSL links on a VLAN interface OR
- the DHCP-server service or DHCP relay agent on your firewall OR
- VLAN trunks and/or bond interfaces with VLAN (even without any DHCP service in use)

...perform the steps below before applying the update:

- Go to **Configuration Tree > Box > Network**.
- On the left side, click **Virtual LANs**.
- In the list, double-click the VLAN entry where the xDSL is attached to.
- Enable **Header Reordering**.
- Click **OK** and **Send Changes/Activate**.

- Go to **CONTROL** > **Box** and click **Network** in the left navigation bar to expand the menu.
- In the left navigation bar, click **Activate new network configuration**.
- Click **Soft...** to trigger a network activation.

After completing these steps, install the update to 8.0.4.

Within the reboot from the firmware update, the **Header Reordering** setting will be applied to your VLAN interface.

If these steps are not done before the update, be aware of the following:

- Your xDSL connection will no longer work after the update.
- Your DHCP server will no longer work as expected for VLANs after the update.
- Your DHCP relay agent no longer works as expected.

Before installing 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.

Legacy Services Announcement

Services and features eventually reach their natural end of life for various reasons, including replacements by new and improved technologies and changes to the marketplace. Not continuing to maintain legacy features in our software allows us to concentrate on more important aspects of our products. The following services are no longer available in releases 8.0.1 or higher.

- SSH Proxy
- FTP Gateway
- Mail Gateway
- SPAM Filter
- Public Key Infrastructure Service
- NG Web Filter (IBM/ISS)
- Distributed DNS

Legacy Items Announcement

The following items will no longer be available:

- SIP-Plugin

- Inventory tree-node
- Generic IPS Patterns
- Firewall Service SOCKS
- H.323 Gatekeeper
- Flex

What's new in Version 8.0.4

Version 8.0.4 is generally a maintenance release.

For customers running firmware 8.0.3, no new features have been added.

For customers running firmware 7.x, see the following list of features that also apply to the new firmware 8.0.2/8.0.3/8.0.4.

The section for Improvements Included in Version 8.0.4 applies to all.

Migrating the Old 3-Layer Server-Service Architecture to the New 2-Layer Assigned Services Architecture

This applies only to firewalls that are currently operating firmware 8.0.1 and upgrading to firmware 8.0.2/8.0.3/8.0.4.

With firmware version 8.0.4, you have the option to migrate the former 3-layer server-service architecture to the new 2-layer Assigned Services architecture. While this is optional in all 8.0.x releases, it will be mandatory in the next upcoming major release.

AutoVPN

For Barracuda-only environments, setting up a site-to-site VPN tunnel has been greatly improved. The new AutoVPN feature provides robust VPN connections through TINA tunnels that are automatically set up with dynamic routing between local networks. AutoVPN is suited for creating multiple boxes in the cloud and connecting them with a TINA site-to-site VPN tunnel.

The automatic setup of VPN tunnels is initiated via the command-line interface (CLI) and REST API.

For more information, see AutoVPN for CloudGen Firewall Devices 8.0.1 or Higher.

Barracuda Control Center License Activation

When a Control Center is started for the first time, the CC Wizard will prompt you to enter a username

and a password that will be used to automatically download licenses.

For more information, see Getting Started - Control Center.

Barracuda Firewall Insights

The Barracuda Reporting Server has been replaced by Barracuda Firewall Insights. Barracuda Firewall Insights is an advanced reporting and analytics platform that ingests, aggregates, and analyzes data automatically from any CloudGen Firewall deployed across your organizational network, including public cloud deployments. Analytics by Firewall Insights provide actionable information for the entire WAN, including dynamic availability information on SD-WAN connections, transport data, security, and web and network traffic details.

For more information, see Firewall Insights.

IPv6 for Client-to-Site Payload

Client-to-Site VPN TINA tunnels now support the configuration of IPv6 client networks.

> On the firewall, the use of IPv6 networks requires at least firmware version 8.0.1.
>
> In order to connect to the firewall, the client requires at least NAC version 5.1.0 or higher. For more information, see Release Notes - Barracuda NAC/VPN Client 5.1 for Windows.

Microsoft Azure Market Place Improvements

The Microsoft Azure Marketplace supports the deployment of High Availability clusters. High Availability ensures that the services running on the CloudGen Firewall are always available even if one unit is unavailable. It is therefore highly recommended. The deployment of a CloudGen Firewall in Microsoft Azure is easy thanks to the web interface that guides you through the process.

Microsoft Azure Virtual WAN

The Barracuda CloudGen Firewall supports up to four Internet Service Provider (ISP) links to Microsoft Azure Virtual WAN. You must have a static IPv4 public IP address with similar bandwidth and latency. For each link, two active-active IPsec IKEv2 VPN tunnels are automatically created if you use automated connectivity. BGP multi-path routing is used to route the traffic, and the configuration of BGP multi-path routing is likewise set up automatically when using automated connectivity. The firewall learns path information as set by the Virtual WAN hub, which results in better path affinity. In addition, BGP-based load balancing and automatic path failover are used for the best connection results.

For more information, see Azure Virtual WAN.

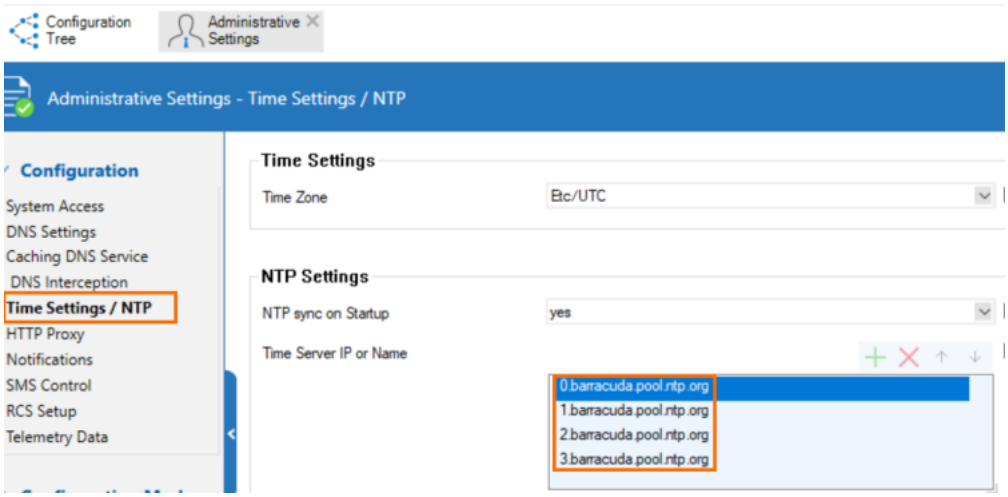
Multi-Factor Authentication with Time-Based One-Time Password (TOTP)

With the release of firmware version 8.0.1, the Barracuda CloudGen Firewall supports multi-factor authentication for user accounts on an individual basis, using a Time-based One-time Password (TOTP) as a secondary authentication method. Multi-factor authentication can be enabled for client-to-site VPN (TINA protocol only), SSL VPN, CudaLaunch, and the Barracuda VPN Client for Windows. Multi-factor authentication using TOTP requires an Advanced Remote Access subscription.

For more information, see How to Configure Multi-Factor Authentication Using Time-based One-time Password (TOTP).

NTP Servers for the Barracuda Zones

The NTP default configuration now displays 4 NTP servers for the Barracuda zone in **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.



New DNS User Interface and Advanced DNS Features

The DNS service has been refactored and now offers a new user interface. This user interface is now tightly incorporated into new features that extend the DNS by various advanced options. The feature set of the new DNS service now includes:

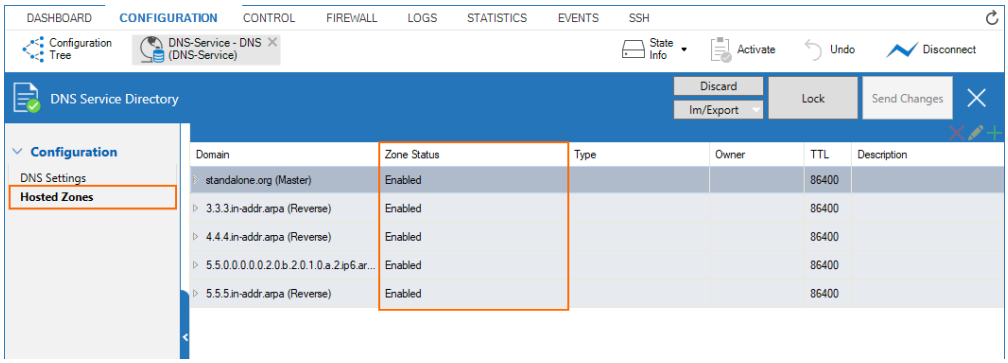
- Stand-alone and distributed DNS service
- Master / Slave / Forward DNS zones
- Split DNS
- Health probing

The new DNS service is based on the commonly known BIND standard. In case a recursive DNS server is configured, the DNS service automatically configures empty zones. This prevents the firewall from sending meaningless queries to Internet servers that cannot handle them.

Note that this option cannot be disabled when the firewall is configured to operate in recursive mode.

For more information, see DNS. Also, see the paragraph **DNS** in the section **Improvements Included in Version 8.0.4** further below.

Zone records in the list of DNS zones can now be selectively enabled/disabled. The list window in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DNS-Service > Hosted Zones** displays the new status field in an additional column.



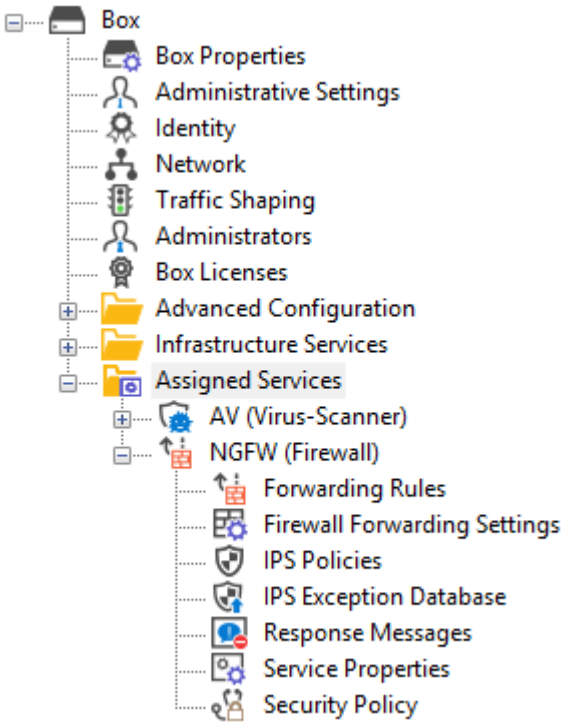
Because this option is available only for stand-alone firewalls and Control Centers with a firmware version higher than or equal to version 8.0.4, this option will also show up in a mixed environment of 8.0.4 and 8.0.3 appliances, but the option will not work on a device running firmware version 8.0.3.

Wildcards (*) are now allowed for the field **Owner** in case of CNAME, DNAME, and TXT records.

Also, zone names in the list may now contain the underscore character (_) if the firewall's firmware is higher than or equal to 8.0.4 or 8.1.1.

Replacement of Virtual Servers by a New 2-Layer Architecture

The former 3-layer server-service architecture has been replaced by a 2-layer architecture in which services are now operated on top of the box layer. With firmware 8.0.1, services are subordinated to the **Assigned Services** node and allow a simpler administration of services and reduce error-prone issues by limiting services to run only on the box they are initially created on.



Virtual servers will no longer be supported in firmware releases > 8.0.x. When migrating a cluster, it will no longer be possible to create cluster servers.

For more information, see Assigned Services and Understanding Assigned Services.

Optimized Command-Line Tool for Configuring an HA Pair of Firewalls in the Cloud

The command-line tool `create-dha` for creating an HA pair of firewalls in the cloud has been optimized. The command no longer requires you to configure the parameter of a netmask because both firewalls must be configured in a subnet of the same size.

REST API Extensions

- REST calls for logins, logout, and authentication for endpoints
- REST for all common access rule operations: create / delete / list / change
- REST calls for network objects (stand-alone + CC (global cluster firewall objects))
- REST calls for service objects (CC + stand-alone)
- REST calls for enabling and activating IPS
- REST calls to allow you to manage box administrators
- REST calls to allow you to manage tokens
- CLI tool to enable REST by default on cloud firewalls (place in user data)

For more information, see https://campus.barracuda.com/product/cloudgenfirewall/api/8.0

SNMP

SNMP now provides the option to monitor license status, the number of days until a license expires, and the current number of protected IPs.

Also, there is now the option to monitor certificates and their expiration date.

SSL VPN

The new TOTP portal provides self-enrollment and self-service of the TOTP authentication scheme.

SSL VPN resources can now be configured as dynamic apps. If configured as a dynamic app, Super Users can enable, disable, or time-enable a resource. Dynamic access can be configured for web apps, native apps, generic tunnels, and network places.

For more information, see SSL VPN.

Usage of DHCP on a VLAN Interface

Requesting an IP address from a DHCP server for a VLAN interface is supported by a feature called **Header Reordering** and can be found in the **VLANs Window** accessible in **CONFIGURATION > Configuration Tree > Network > Virtual LANs**.

> With firmware versions 8.0.0 and 8.0.1, due to a misleading interpretation of the related visual control item in the user interface, the DHCP address assignment sometimes caused issues or failed. Users were forced to select the check box inadvertently.
>
> With firmware version 8.0.2, this misleading interpretation has been fixed.
>
> Because header reordering now works as expected, the usage must now be re-adapted.

For correct usage of the user interface item **Header Reordering**, see the following table:

User Action	User Interface Item	Description
Default state: header reordering is off.	Header Reordering ☐	No header reordering is done for DHCP on a VLAN interface.
Select the check box in case the assignment of an IP address from a DHCP server fails.	Header Reordering ☑	Header reordering for DHCP on a VLAN interface is now activated.

VPN IPv6 Payloads

With the exception of SD-WAN, IPv6 payloads in VPN tunnels are supported and now work for TINA site-to-site and client-to-site tunnels.

Improvements Included in Version 8.0.4

Authentication

- Firewalls can now be configured to send authentication requests for admin accounts to a Control Center that then acts as an authentication proxy forwarding these requests to another centralized authentication service, e.g., MSAD. [BNNGF-63916] [BNNGF-63916]
- Authentication to the firewall no longer stops randomly in certain situations. [BNNGF-63940]
- When moving user data out of the base DN path to another location, the MSAD group cache is now updated as expected. [BNNGF-64379]
- MSAD and LDAP authentication now work as expected with the offline group cache in case the base DN contains blanks. [BNNGF-64736]
- When activating cache MSAD groups, logon events are counted as expected. [BNNGF-65083]
- The calculation of the requestor ID for RADIUS with MFA authentication now works as expected. [BNNGF-65095]
- RADIUS authentication no longer fails in certain situations. [BNNGF-65505]
- RADIUS authentication now works as expected for configured CC Template Admins. [BNNGF-65881]

Barracuda Firewall Admin

- In case an interface is running in half-duplex mode, its state is displayed in the color orange in **DASHBOARD > INTERFACES**. [BNNGF-23923]
- The term "realm" has been replaced by the term "trust level" at all relevant points in the user interface. [BNNGF-63852]
- After enabling header reordering, the list **Reference** in **CONFIGURATION > Box > Configuration Tree > Network > Interfaces** now displays correct values. [BNNGF-63950]
- Firewall Admin displays interfaces correctly in **Firewall > Live** for an IPv6 session sync for an HA setup. [BNNGF-64685]
- Failover and balance options for connections in host firewall rules have been removed. [BNNGF-65255]
- Firewall **STATISTICS** for sessions are now displayed correctly. [BNNGF-65436]
- On firewalls with the 3-layer architecture (server-service layer), it is no longer possible to move Secure Access Controllers (SAC400, VACC400, SAC610, VACC610, SAC820, VACC820) to a different cluster. [BNNGF-65531]
- The defaults for MTU have been updated in the **VPN Settings**. [BNNGF-65561]
- When logging off from SSH during a file upload/download, the file transfer is stopped and Firewall Admin no longer crashes. [BNNGF-65802]
- Bulk transformation of firewalls from the old 3-layer to the new 2-layer architecture now works

as expected. [BNNGF-65979]
- In some certificates, it is no longer necessary to enter the country code if it is not essentially required. [BNNGF-66132]
- The Network Object pop-up in the access rule list now displays its content correctly. [BNNGF-66166]
- In case the firewall's firmware is higher than or equal to 8.0.4 or 8.1.1, it is now possible to use the '_' character in zone names. [BNNGF-66253]
- After deploying an AWS firewall via PAR file, the network integrity check now works as expected after the VIP network is configured. [BNNGF-66269]
- The dialog for **VPN Settings** no longer crashes when double-clicking on the **Root Certificates** table. [BNNGF-66760]
- DNS record data for the TXT record type are now correctly displayed in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DNS > DNS Service > Hosted Zones**. [BNNGF-67107]
- After a 7.2 to 8.0.1 migration, server IP addresses are no longer displayed multiple times in the **Edit Hosted Zone** window in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DNS > DNS Settings > Hosted Zones**. [BNNGF-67113]
- The user interface has been updated at various places to reflect inclusive terminologies. [BNNGF-67545], [BNNGF-67571], [BNNGF-67572]

Barracuda OS

- Certain devices using an older TCP stack implementation no longer experience session drops in combination with IPS and Application Detection. [BNNGF-29095]
- CC admins can now log into SSH-managed boxes as expected in case **Force Key Authentication** in the **SSH** settings is set to **Yes**. [BNNGF-46990]
- The FTP plugin now works with correct ports in PASV mode. [BNNGF-53016]
- Configuring IPv6 subnets for IPv6 DHCP addresses in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DHCP > Operation Setup IPv6**, in the configuration window **Subnets > Network Address Field**, now works as expected. [BNNGF-56665]
- The name of the log file is now correctly set in the activation script/applications for the OSPF service. [BNNGF-59974]
- After establishing a dynamic mesh tunnel, shaping tree information is now correctly displayed. [BNNGF-60069]
- Wi-Fi is no longer broken after an activation of a new network configuration or a restart of the firewall. [BNNGF-62806]
- If a firewall is enabled to use an IPv6 management IP address, unwarranted warnings no longer occur when logging into the firewall with Firewall Admin for the first time. [BNNGF-64160]
- SNMP now provides the option to monitor license status, the number of days until a license expires, and the current number of protected IPs. [BNNGF-64162]
- SNMP now provides the option to monitor certificates and their expiration date. [BNNGF-64163]
- When installing a CloudGen Firewall image via a USB drive, importing PAR or PCA files now works as expected. [BNNGF-64201]
- IPFIX intermediate reports for long-running sessions now work as expected. [BNNGF-64291]
- Because Windows Server 2008 R2 has already reached EoS, the TS Agent support has been

dropped for this operating system. [BNNGF-64300]
- Restoring a standby PAR file on a virtual appliance now works even if the secondary box is a different model. [BNNGF-64423]
- GRE tunnels are now possible with a dynamic default route. [BNNGF-64497]
- The NTP default configuration now displays 4 NTP servers for the Barracuda zone in **CONFIGURATION > Configuration Tree > Box > Administrative Settings**. [BNNGF-64707]
- Users authenticated via the DC Agent are no longer logged out after 12 hours if meanwhile an HA failover occurs on an HA pair of firewalls. [BNNGF-64730]
- Migrating firewalls with different port names (e.g., port1, p1) using PAR files no longer results in errors but now shows warnings. [BNNGF-64921]
- The telemetry system has been completely revamped. [BNNGF-64964]
- On managed firewalls, virtual router (VR) instances can be created using **Emergency override**. [BNNGF-64999]
- Restoring a configuration from a PAR file no longer fails in certain situations. [BNNGF-65039]
- SLACK notifications work as expected. [BNNGF-65132]
- Firewalls with only layer-3 bridges no longer crash in certain situations. [BNNGF-65135]
- The creation of empty dynamic placeholder network objects is now allowed. [BNNGF-65141]
- On firewalls hosted in a Hyper-V(2019) platform, routes with reachable IP addresses are no longer taken down accidentally in certain situations. [BNNGF-65247]
- A line of output is added to the log if CC-activate is not able to access a server IP on port 810. [BNNGF-65296]
- GoToMeeting no longer fails when SSL interception is activated. [BNNGF-65465]
- In cases of a third-party HTTPS proxy, proxy connects from the firewall to that HTTP proxy are now correctly intercepted. [BNNGF-65491]
- Logging into SSH on a managed firewall as a CC admin with either a key or a key and a password now works as expected. [BNNGF-65512]
- Additional local IP addresses no longer appear in the list of Management IP addresses. [BNNGF-65522]
- Application Detection now honors URLs as expected. [BNNGF-65556]
- During an ATP file scan, the wait page is now displayed as expected. [BNNGF-65580]
- The firewall no longer crashes accidentally in certain situations after updating to firmware version higher than or equal to 7.2.6. [BNNGF-65636]
- Reporting the SD-WAN status for a huge number of tunnels no longer causes memory issues. [BNNGF-65682]
- The firewall no longer produces memory leaks in certain situations. [BNNGF-65804]
- The firewall model F280b now displays the correct sensor values in Firewall Admin. [BNNGF-65843]
- After changing the **GPS Coordinates** in **CONFIGURATION > Box Properties > Geo Location**, the firewall now transmits the correct values to Barracuda Firewall Insights. [BNNGF-65877]
- Migrating a firewall from a 3-layer to a 2-layer architecture no longer fails in case the firewall is missing the server before the migration. [BNNGF-65895]
- Installing a firewall using a PCA file with the correct password and a different serial number now works as expected, whereas an incorrect password sets the firewall to the default configuration. [BNNGF-65904]

- L2TP is now working as expected with a Honeywell Dolphin 99x. [BNNGF-65939]
- IPS is now working as expected. [BNNGF-65946]
- Downloading licenses on stand-alone HA clusters will download the licenses of both partners again at the same time. [BNNGF-66065]
- Routing entries are now removed from the routing table as expected. [BNNGF-66101]
- A firewall as part of an HA pair no longer remains occasionally blocked after a failover. [BNNGF-66240]
- IPsec connections between CGFW in AWS and AWS VPG are now working as expected. [BNNGF-66248]
- The configuration has been set to download intermediate certificates per default. [BNNGF-66282]
- The login for xDSL is now working as expected. [BNNGF-66294]
- When Geo IP information is entered manually in **CONFIGURATION > Configuration Tree > Box > Properties**, the associated file under /opt/phion/run will no longer be reset after a box reboot. [BNNGF-66359]
- In HA clusters of hardware firewalls, the MTU size for interfaces can now be adjusted as expected in **Box > Network > Physical Interfaces**. [BNNGF-66556]
- OSPF no longer prevents the firewall from learning the default IPv6 route. [BNNGF-66630]
- The F800c/F900b firewall now displays correct sensor values. [BNNGF-66745], [BNNGF-67528]
- The installation progress is now correctly displayed in the LCD display on the models F380b, F400c, and F600d. [BNNGF-66791]
- **Prefix List Filters** for OSPF no longer cause errors in certain situations when **Send Changes** is clicked. [BNNGF-66838]
- A BGP route is now correctly removed in case the related network connection becomes unavailable. [BNNGF-67136]
- Forwarding SMTP data in conjunction with AV scanning no longer is blocked if AV scanning takes longer. [BNNGF-67176]
- Mixing corporate-site pool licenses and single-instance licenses works now as expected. [BNNGF-67396]
- If the LTE connection is broken, the new status is displayed as **Unknown** in **CONTROL > NETWORK**. [BNNGF-67454]
- The LEDs now work as expected when deploying an F93/F193 with a USB installation stick. [BNNGF-68591]

CloudGen Firewall Install

- When importing an ISO file for installation, it is deleted after the installation. [BNNGF-66295]

Control Center

- Pool-licence timestamp requests now work as expected. [BNNGF-63215]
- Updating multiple firewalls via the Control Center with different schedules now works as expected. [BNNGF-64141]
- Authentication Sync Zone now works as expected. [BNNGF-64409]
- GTI tunnels are no longer deleted from appliances in certain situations for 2-layer boxes. [BNNGF-64754]

- The **Status Map** in the Control Center now correctly displays information about VPN tunnels on inactive firewalls. [BNNGF-65059]
- When creating a new box in an 8.0 cluster, the settings are now correctly copied from the default box node in the configuration tree. [BNNGF-65204]
- When cloning a firewall with a 3-layer architecture in the Control Center, the box-clone wizard now works as expected. [BNNGF-65631]
- The Control Center no longer accidentally generates new box keys for firewalls that were originally deployed via ZTD. [BNNGF-65807]
- The Control Center firmware update page shows firmware updates as expected. [BNNGF-65892]
- When hundreds of CGF firewalls are created in the Control Center, the **Config Tree** is now displayed correctly. [BNNGF-65912]
- Installed hotfixes are no longer displayed as installable. [BNNGF-66176]
- The SC models SC2.8 and SC2.9 are now part of the SC2 submodel list. [BNNGF-67268]

DHCP

- The interface option for DHCPv6 Interface in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DHCP > DHCP Enterprise Configuration > Operational Setup IPv6** can now be configured as expected in case the DHCPv6 service is enabled. [BNNGF-55707]
- Input values for the IPv6 **Network Address** and **Interface** fields in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DHCP > Operation Setup IPv6**, in the configuration window **Subnets > Network Address Field**, are now validated to accept only correct values. [BNNGF-56800]
- The input field for DHCP address reservations in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DHCP > DHCP Enterprise Configuration > Operational Setup**, in the window **Subnets**, in the section **Pool Properties > Reservations**, only accepts alphanumeric characters and digits when entering the value. [BNNGF-57643]
- The conversion method for the **Vendor ID** can now be selected in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DHCP > DHCP Enterprise Configuration > Operational Setup**, in the window **Subnets**, in the field **Vendor ID Conversion**. [BNNGF-61945]
- The **DHCPv6 Server Identifier** field in **CONFIGURATION > Configuration Tree > Box > Assigned Servcies > DHCP > DHCP Enterprise Configuration > Operational Setup IPv6**, in the section **Service Availability**, now accepts hostnames and IPv6 IP addresses. [BNNGF-62910]

DNS

- The DNS service now accepts dynamic DNS updates for a given zone from the local subnet. [BNNGF-61373]
- For the DNS service, wildcards (*) are now allowed for the field **Owner** in case of CNAME, DNAME, and TXT records. [BNNGF-63925]
- DNS known hosts configured in **CONFIGURATION > Configuration Tree > Box > Administrative Settings > DNS Setting**, in the section **Advanced DNS Settings**, in the

list **Know Hosts**, are now considered for mail event notification. [BNNGF-64036]
- In case of single firewalls and Control Centers with a firmware version higher than or equal to 8.0.4, a check box for enabling/disabling DNS record entries will be displayed in multiple DNS configuration windows. [BNNGF-64675]
- "@" A-Records with health probe now work as expected. [BNNGF-65600]
- The BIND subsystem has been updated to cover recent CVEs. [BNNGF-66339]
- When creating an A record for a certain DNS zone, the hostname is now correctly generated based on the field **Name/Owner**. [BNNGF-66422]
- The user interface for DNS has been updated and now displays technically correct terms. [BNNGF-67544]

Firewall

- The connection object for **Round Robin / Failover** in a host firewall rule now works as expected. [BNNGF-55008]
- Deny application rules with a URL Filter Match Object no longer block DNS traffic. [BNNGF-65803]

HTTP Proxy

- Improvements have been made for the interaction of the HTTP proxy and the virus scanner under high loads. [BNNGF-64106]
- After updating to firmware version 7.2.6 or higher, the HTTP proxy now starts as expected if ACLs are configured for MIME-type / user authentication **Deny**. [BNNGF-65659]
- Several improvements to the HTTP proxy have been made. [BNNGF-66036]
- ECDH key exchange ciphers are now correctly enabled for the reverse proxy mode in conjunction with SSL interception. [BNNGF-66826]

REST

- The REST daemon no longer produces memory leaks in certain situations. [BNNGF-63465]

Virus Scanner

- Correct timestamp values are now displayed for scanned ATP files. [BNNGF-65894]

VPN

- Errors no longer occur in case of an HA failover with VPNR interfaces. [BNNGF-64609]
- High memory loads for TINA tunnels no longer occur in certain situations. [BNNGF-65122]
- In site-to-site VPN TINA tunnels, DHCP relay packets are now correctly forwarded to the DHCP server. [BNNGF-65811]
- The VPN transport mode **routing** now works as expected in HA pairs with different firmware versions. [BNNGF-65903]
- Memory leaks no longer occur if the VPN configuration is reloaded. [BNNGF-66204]
- When authenticating a user with **Primary Scheme** against MSAD for a client-to-site VPN connection, the **Firewall Objects** on User/Group now work as expected for the logged-in

user. [BNNGF-66357]
- The IKE daemon now works as expected if more than 1 network is added to an existing VPN tunnel. [BNNGF-66621]
- Azure vWAN no longer causes the VPN service to crash. [BNNGF-66649]
- IKEv2 tunnels are no longer terminated and restarted accidentally in certain situations. [BNNGF-66887]

WEB UI

- Changing the system time using the Web UI now works as expected. [BNNGF-64958]
- The firewalls X50, X51, X100, X101, and X200 can now also be migrated to their respective F-type firewalls. [BNNGF-65896]
- When restoring a backup file, the file selection dialog window now enables the **Save** button correctly. [BNNGF-66412]
- In the Web UI, the firmware version of the firewall is now the same as the version that can be queried in the console. [BNNGF-66573]

Known Issues

- **Azure** – OMS is currently not supported on CC-managed boxes.
- Currently, no RCS information is logged for **Named Networks**. [BNNGF-47097]
- **Barracuda Firewall Admin** – Copying and pasting an access rule with explicit named network does not copy named network structure. [BNNGF-48588]
- The learn-only mode for OSPF is not working as expected. [BNNGF-65299]
- **If you do not have hotfix-1045 installed**, migrating a firewall from the former 3-layer to the new 2-layer architecture cannot be done for firewalls with repository links to the nodes **Properties**, **Network**, and **Control** in the **Configuration Tree**. [BNNGF-67675]
- "vmxnet" driver version 2 is no longer supported. Before updating, you must change to, for example, vmxnet3.
- The migration wizard to 2-layer architecture for a managed box on a CC does not update the status map accordingly. A workaround using conftool is available.
- **DNS** – After the migration, SOA TTL values are set to 0. [BNNGF-69221]
- PAR files that have been exported with the cctool and with a size larger than 2 GB are broken. [BNNGF-71814]

Figures

1. ntp_servers_for_barracuda_zones.png
2. dns_zones_overview_window.png
3. assigned_services_tree.png
4. header_reordering_off.png
5. header_reordering_on.png