8.0.1 Release Notes

https://campus.barracuda.com/doc/84313441/

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.

Changelog

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

- **19.09.2019 Hotfix 1015** – Hotfix 1015 is a cumulative package for CGF 8.0.1 that fixes several known issues. For more information, see Hotfix 1015.
- **23.09.2019 Hotfix 1016** – Hotfix 1016 solves an issue that prevented logs from being sent to Azure OMS. For more information, see Hotfix 1016.
- **01.10.2019 Hotfix 1017** – Hotfix 1017 solves an issue with the synchronisation of the CC database between two CCs in a CC-HA cluster. For more information, see Hotfix 1017.

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 8.0.1

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.

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 for entering 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 usage of IPv6 networks requires at least firmware version 8.0.1.

In order to be able to connect to the firewall, the client requires at least NAC version 5.1.0 or greater. For more information, see Release Notes - Barracuda NAC/VPN Client 5.1 for Windows.

Multi-Factor Authentication with Time-based One-time Password (TOTP)

With release 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).

New DNS User Interface and Advanced DNS Features

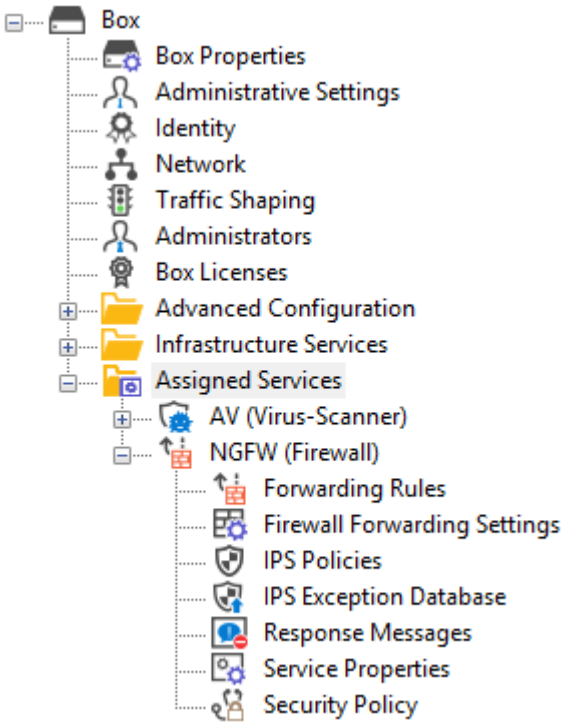
The DNS service has been refactored and now presents a new user interface. This user interface is now tightly incorporated into new features that extend the DNS by various advanced options. The feature set of the new DNS service now includes:

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

For more information, see DNS.

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 where 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 where they are initially created on.



Virtual servers will no longer be supported in upcoming firmware releases.

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 to optionally configure the parameter of a netmask because both firewalls must be configured in a subnet of the same size.

REST API Extensions

- 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

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.

vWAN

The connection to Microsoft Azure vWAN has been greatly improved. Azure Virtual WAN can be used both on CC managed and standalone CloudGen Firewall devices and is configured in the **Cloud Integration**. The new configuration path is **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your Box* > Advanced Configuration > Cloud Integration.** In addition, specific vWAN logs have been added and can be found in **LOGS > Box > Cloud > azurevwan**. If you are using automated connectivity the association of the hub is done automatically.

For more information, see Azure Virtual WAN.

SSL VPN

The new TOTP portal provides self enrolment 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.

Improvements Included in Version 8.0.1

ATP & Antivirus

- Virus scanning now covers also SMBv2 & SMBv3. [BNNGF-56423]
- The ATP Scan-First option now works also for file downloads from Cloud storages. [BNNGF-58570]

Barracuda Firewall Admin

- When opening an SSH session in Firewall Admin, the initial screen now has the correct size. [BNNGF-40761]
- In the Control Center, the status of pending SCA configuration updates is now displayed correctly. [BNNGF-47124]
- The help-text explanation for the address notation in the user interface has been exchanged in order to use the CIDR notation in the **Network Prefix** edit field. [BNNGF-50048]
- SPAM tag/headers can now be configured individually. [BNNGF-55785]
- Adding a new **Service or Server (SRV)** record in the DNS service now works as expected.

[BNNGF-55967]
- Test mails can now be sent when configuring Email Notifications in Administrative Settings and in the AV/ATP section. [BNNGF-56291]
- In Firewall Admin, it is again possible to add more than 10 Named Networks. [BNNGF-56496]
- A checkbox for activating SMB virus scanning has been added to CONFIGURATION > Security Policy Settings, section Virus Scanner Configuration. [BNNGF-56426]
- The **Server Action** list in **CONFIGURATION > Configuration Tree > Eventing**, tab **Notification**, window **Notification**, tab **Server Action**, is now displayed as expected. [BNNGF-56622]
- The display color for access rules can now be adjusted interactively to be better perceived in the window **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**. [BNNGF-56630]
- The display color for access rules has been adjusted for easier viewing in the window **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**. [BNNGF-56631]
- Firewall Admin no longer crashes in certain situations after configuring a hostname as a global network object. [BNNGF-56782]
- Cloning a template in the SC editor no longer causes problems if a dash character is part of the template name. [BNNGF-56836]
- When configuring the VPN Client in **VPN-service > Client-to-Site > External > Group Policy > VPN Client Network** and setting the parameter **Always on** to **Yes**, users are no longer able to disconnect from the VPN. [BNNGF-56851]
- The VPN status for HA paired boxes no longer flaps in CC **Status Map**. [BNNGF-56936]
- **Import Private Key from Clipboard/File** in **Firewall Admin > Configuration > Configuration Tree > Assigned Services > VPN-Service > VPN settings > Server Certificates** now works as expected.. [BNNGF-57387]
- If **User: Not set** for filter settings is selected in the **USER** element of the **Firewall** tab, information is now correctly displayed. [BNNGF-57670]
- With firmware release 8.0.1, Geo Maps are replaced by a new CC-SDWAN Dashboard labeled SD-WAN. [BNNGF-57773]
- When applying a user filter in Firewall Admin, **FIREWALL > History** now works as expected. [BNNGF-58007]
- Firewall Admin no longer displays 'mip' for the **Access IP** in the **Status Map** of a managing Control Center for a subordinated Control Center. [BNNGF-58013]
- The **Refresh** button in the **Activation** tab is displayed as expected. [BNNGF-58073]
- Firewall Admin no longer crashes during the migration of cluster configurations. [BNNGF-58113]
- On firewalls that support LTE, the LTE provider is now correctly shown at the bottom of the main display area in **CONTROL > Network**. [BNNGF-58277]
- When exporting VPN profiles for a VPN client, Firewall Admin no longer uses default ciphers. [BNNGF-59018]
- The Log Viewer's focus now sticks to the last selected line after a filter is deactivated. [BNNGF-59251]
- The rule editor now supports selective blocking of IPv6 extension headers. [BNNGF-59479]
- In the Control Center, the columns **File Transfer Status**, **Transfer Time** and **Transfer Info** are now correctly filled if more than 1 firmware update file is transferred to a firewall.

[BNNGF-59530]
- In Firewall Admin, when using **Deliver First, then Scan** as a global policy, scanned files now show the correct policy name in the list. [BNNGF-59584]
- External administrators can now access the ATP tab as expected. [BNNGF-59652]
- Right-clicking a **Geo Location** in the **Source** list of the Rule Editor and selecting **Remove** in the list now removes the entry from the **Source** list as expected. [BNNGF-59754]
- 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 TCP Stream Reassembly option has been moved to **CONFIGURATION > Configuration Tree > General Firewall Configuration > Operation**, section **Default TCP Policy**. [BNNGF-61173]
- The SNMP service ACL input field in **CONFIGURATION > Configuration Tree > SNMPOP Service Settings > Access Groups > Peers** now accepts IPv6 addresses correctly. [BNNGF-61517]

Barracuda OS

- When the power button is pushed on the F100, the shutdown command is now executed. [BNNGF-29311]
- The Authentication Client for windows no longer steals the focus from an active running program and now works as expected. [BNNGF-47656]
- The position of the Time-Zone column for firewall stored logs is now the same as on the Control Center. [BNNGF-53478]
- Disabling or deleting neighbors no longer restarts the BGP service. [BNNGF-54547]
- The MSAD authentication scheme now supports User Principal Names. [BNNGF-54606]
- User information in the firewall and in the authentication database are now in sync. [BNNGF-54683]
- x.509 client authentication is now provided for weblog streaming. [BNNGF-54725]
- The firewall now provides the correct information to SNMP for the VPN state of IKEv2 tunnels. [BNNGF-54762]
- When configuring a virtual link for OSPF with Digest-MD5 encryption in **CONFIGURATION > Configuration Tree > Box > Assigned Services > OSPF-RIP-BGP-Service > OSPF Area Setup > OSPF Area Configuration**, the authentication key input now accepts up to 16 characters. [BNNGF-54842]
- IPv6 with delegation now works as expected on DHCP interfaces. [BNNGF-54856]
- The **CC Wizard** in Barracuda Firewall Admin now accepts Hyper-V-based Control Centers as expected. [BNNGF-54941]
- On multi-processor firewalls, traffic workload is now processed by multiple cores as expected. [BNNGF-55255]
- Firewall history in system report now also works for VRF-enabled boxes. [BNNGF-55658]
- Changing the LAN mode from **Manual** to **DHCP Server** for an SC now works as expected. [BNNGF-55676]

- Archive scanning now supports scanning of SMTP, POP3 and FTP. [BNNGF-55696]
- Firewall appliances no longer finish installation via USB stick with incorrect LED status (red) if the installation was successful but no hotfixes were installed. [BNNGF-55706]
- Group information is now processed correctly by the firewall if special delimiters are used between fields (e.g., name, surname) on an Active Directory. [BNNGF-55718]
- DNS now supports multiple and extra long values (> 255 characters) in the TXT record. [BNNGF-55782]
- In **CONFIGURATION > Configuration Tree > Box > Virtual Servers > Assigned Services > OSPF-RIP-BGP Service > OSPF-RIP-BGP Settings > BGP Router Setup**, the edit-field for BGP AS numbers now accepts 32-bit numbers in the private range (4200000000 - 4294967294). [BNNGF-55796]
- Devices with WLAN can now connect as expected if multiple access points are configured. [BNNGF-55802]
- Improvements have been made to HA sync. [BNNGF-55932]
- The firewall now connects to the Barracuda Reporting Server through the remote management tunnel using the VIP. [BNNGF-55980]
- IPv6 box ACLs now work as expected with netmasks smaller than 64 bit. [BNNGF-56060]
- The Firewall is now able to process SAML assertions [BNNGF-56147]
- The throughput on an F900 now works as expected due to a network driver update. [BNNGF-56293]
- In Firewall Admin, **Firewall > Live**, the bandwidth indicator now shows correct values if there are no display filters for traffic summary set. [BNNGF-56299]
- Exporting IPFIX flow information for long-running sessions no longer terminates unexpectedly. [BNNGF-56330]
- If the watchdog is enabled in the configuration, it is now started correctly after an update. [BNNGF-56438]
- SNMP no longer causes memory leaks when initializing plugins. [BNNGF-56448]
- WIFI AP Authentication with Aruba access points now works again. [BNNGF-56574]
- The firewall no longer crashes in certain situations. [BNNGF-56589]
- The M40 modem no longer becomes unstable on the F12 firewall with USB3. [BNNGF-56595]
- The firewall no longer keeps rebooting in certain situations. [BNNGF-56603]
- On the Control Center, a new service object has been added for SC default ports in the host firewall ruleset. [BNNGF-56610]
- Reinstallation using ART now works as expected. [BNNGF-56731]
- Configurations from other models imported on F183 are now correctly migrated. [BNNGF-56850]
- The CloudGen Firewall no longer produces memory leaks due to unreleased resources during the handling of rulesets. [BNNGF-56999]
- CPU statistics time (per CPU and percentage) is now calculated correctly on the firewall. [BNNGF-57549]
- The firewall no longer crashes in certain situations. [BNNGF-57597]
- It is now possible to send notifications via Slack. [BNNGF-57640]
- Fixed an error using a DC/TS client not synchronizing to a trustzone in an HA configuration. [BNNGF-57732]
- SNMP configuration changes are now followed by an update of the ruleset for dynamic IPs, which are then immediately used. [BNNGF-57960]

- In case of an SSL inbound connection, the firewall now correctly uses the server's cipher preferences. [BNNGF-58014]
- Fixed an error using pipe symbols in server-start and server-stop scripts. [BNNGF-58356]
- Allow adding BCC credentials for automatic license download. [BNNGF-58428]
- Obsolete modems are no longer displayed for selection in the section **Connection Details** in **Network > Wireless WAN**. Only Barracuda modems are available. [BNNGF-58568]
- Mellanox interfaces now work as expected. [BNNGF-58914]
- Services no longer go down in certain situation during pool license updates. [BNNGF-59000]
- After an installation of a firmware on an F800C/F900b Firewall from a .PAR file, the configuration is now correctly set on the IPMI module. [BNNGF-59114]
- On PAYG cloud firewalls, the WCS service now uses the correct license base. [BNNGF-59148]
- (Re-)Starting the VPN service no longer causes errors in the fatal log due to unclosed file descriptors. [BNNGF-59192]
- Reaching the Azure gateway via ARP no longer fails due to a kernel update. [BNNGF-59236]
- The firewall models F12, F18, F80, F180, F183, F183R, and F280 now support up to 10 VRF instances. [BNNGF-59396]
- When using SMTP scanning, the connection to the client mail server no longer runs into a timeout. [BNNGF-59397]
- HA takeovers no longer occur due to low memory situations with high data throughput. [BNNGF-59553]
- 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]
- The firewall no longer crashes in certain situations. [BNNGF-59653]
- If communication fails with Barracuda DC agent, the event "DC Agent Communication Failure" with ID=4113 is created. [BNNGF-59741]
- On a CGF with a M40 modem, registration in a roaming network now works as expected. [BNNGF-59769]
- Multi-path routes with two gateways on different interfaces are now working correctly. [BNNGF-59892]
- The firewall no longer crashes in certain situations. [BNNGF-60095]
- In the SC editor it is now possible to enter LTE user credentials. [BNNGF-60423]
- BIND has been updated to 9.11.8 [BNNGF-60667]
- After a importing the PAR files for an HA-pair, licensing the boxes and C2S VPN connections now work as expected. [BNNGF-60155]
- Kernel has been updated and now covers CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479. [BNNGF-60349]
- OSPF filters work correctly after a manual restart of the routing service and then do not cause a fail of HA-failover. [BNNGF-60824]
- Authentication using DC agent now works as expected. [BNNGF-61510]

Cloud

- Endpoint routing attributes for Office 365 are now treated according to the priorities Default, Allow, and Optimize. [BNNGF-56203]

- A HA secondary is no longer stuck in certain situations. [BNNGF-56297]
- The CloudGen Firewall VCC400 now supports migrating firewall between firmware versions. [BNNGF-56698]
- The create-dha tool has been updated and now supports soft boxnet activation on the primary firewall. [BNNGF-59038]
- Accessing the online Barracuda cloud services such as the URL Filter service now works as expected. [BNNGF-60732]

Control Center

- On a Control Center, importing an archive.par without a CCDB dump no longer fails if the CCDB is active. [BNNGF-46601]
- Control Center administrators no longer can 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]
- Reassigning pool licenses to a larger quantity of boxes in the Control Center now works as expected. [BNNGF-53178]
- Pool licenses of SC1 are now displayed correctly in **CONTROL > Barracuda Activation > Pool Licenses**. [BNNGF-53805]
- On the Control Center in **CONTROL -> Firmware Updates**, deleted files are no longer displayed in the list of the tab **Files on Control Center** after their removal. [BNNGF-54013]
- If an administrator makes changes on a box via "Emergency Override", the difference between the configurations on the box and on the Control Center is now visible in the **Status Map**. [BNNGF-54496]
- CC authentication sync zones now work as expected. [BNNGF-54561]
- Expired Control Center admin users are now correctly reset. [BNNGF-54765]
- When migrating a cluster in the Control Center, links to **Site Specific Network Objects** are no longer broken if they are referenced inside of a connection object. [BNNGF-55853]
- A warning message is now displayed before disabling **Own Firewall Objects** on range or cluster level in the **Range/Cluster Properties > General in the Specific Settings** section. [BNNGF-55943]
- After reinstalling a Control Center, SC boxes show up as expected in the Status Map. [BNNGF-56019]
- When creating a repository for **CONFIGURATION > Configuration Tree > Box > Network** on an F82 firewall, the section for Barracuda DSL Modem is now displayed as expected. [BNNGF-56069]
- Configuration changes in the Control Center on range level no longer freeze and are now processed as expected. [BNNGF-56170]
- When creating a virtual managed box in the Control Center, the Web UI is now disabled. [BNNGF-56187]
- When migrating clusters, protocol entries are no longer broken in an application rule. [BNNGF-56252]
- On a Control Center, authentication synchronization over trustzone sync now works as expected. [BNNGF-56365]

- If the configuration of a managed box differs from the respective configuration on the Control Center, the difference is now displayed to be out of sync in the Status Map. [BNNGF-56430]
- IPS pattern updates are now sent only to boxes which have IPS enabled. [BNNGF-56806]
- In the Control Center, the firewall icon is now displayed as expected in the column **Access IP** of the **Status Map** in case a distributed firewall service is running on the corresponding firewall. [BNNGF-57970]
- Fixed an issue where connecting to a Control Center status map did not work. [BNNGF-58021]
- On a Control Center, repository settings for **Firewall > Firewall Forwarding Settings** can now be modified as expected. [BNNGF-58060]
- Migrating SC setups from firmware version 6.2 to 7.2 now works as expected. [BNNGF-58135]
- It is now possible to re-deploy configurations for ZTD. [BNNGF-58293]
- The list of external administrators can now be sorted individually by using a numerical value in the field 'Priority' in CONFIGURATION > Administrators > External Admins. [BNNGF-58345]
- When configuration updates for an SC are blocked due to a version mismatch, a warning is now displayed in **Configuration Updates**. [BNNGF-58495]
- On a split-CC environment accessing boxes using MIP or VIP now works as expected. [BNNGF-58616]
- SC REST now supports the configuration and control of the usage of management and data networks. [BNNGF-59041]
- Zero Touch Deployments now signal the result for a successful and failed operation with an audio signal. [BNNGF-59456]
- If multiple VIP networks are available, the corresponding name for the networks are now displayed. [BNNGF-59774]
- 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]

DHCP

- The firewall now sends router advertisements as expected if a working DHCP relay is configured. [BNNGF-55113]
- The DHCP service no longer causes memory leaks when discovering interfaces. [BNNGF-56410]

Firewall

- Application based link selection now works as expected for "Web Browsing" applications. [BNNGF-28138]
- NTP traffic is now sent via VIP if the option **Start NTPd** is set to **Yes**. [BNNGF-32753]
- Traffic shaping is now working as expected when AV scan is enabled in Application Control. [BNNGF-41356]
- Application Based Provider Selection now works as expected for more applications [BNNGF-42261]
- Dynamic rules are now terminated correctly if the user tries to "Disable & Terminate" it. [BNNGF-48333]

- Link protection now correctly rewrites certain hyperlinks. [BNNGF-53144]
- If an active session is terminated by Firewall Admin, it no longer causes stalled sessions on clients but resets the session as expected. [BNNGF-54500]
- DNS now handles hostnames with a maximum length of 256 characters. [BNNGF-54572]
- The kernel no longer crashes in certain situations. [BNNGF-55971]
- IPS events are now correctly sent via syslog streaming. [BNNGF-56332]
- When accessing a virus file on an SSL web server running on non-standard ports, the ATP block page now shows the correct URL. [BNNGF-56383]
- MSAD authentication with TLS1.2 now works as expected. [BNNGF-56717]
- When using traffic shaping (QoS), traffic is now correctly forwarded between different priority classes on virtual machines after priority adjustments. [BNNGF-56790]
- The Host Firewall no longer generates its own log files when the corresponding setting in **Access Rule -> Advanced -> Own Log File** is set to **No**. [BNNGF-56825]
- When HTTP headers are parsed by the firewall, the response header is now forwarded completely. [BNNGF-58314]
- Fixed a problem with CRL checks where all HTTPs traffic was blocked. [BNNGF-58506]
- Fixed incorrect URLs on the download page when using ATP with **Scan-First Deliver-Later**. [BNNGF-58543]
- The firewall no longer crashes in certain situations. [BNNGF-58573]
- The firewall no longer reboots unexpectedly due to high loads. [BNNGF-58593]
- URLs for onedrive.live.com are now correctly categorized by the URL filter. [BNNGF-58642]
- The firewall no longer crashes in certain situations. [BNNGF-60612]
- Transparent Redirect now works as expected. [BNNGF-60951]

FSC/SC

- Changing the LAN interface IP address from an FSC is now updated on an SC as expected. [BNNGF-55333]
- Disabling LAN interface settings for an SCA now works as expected. [BNNGF-55343]

HTTP Proxy

- The HTTP forward proxy no longer crashes on high loads while accessing MS-CHAP for authentication. [BNNGF-54503]
- The reverse proxy for HTTPS now offers TLS 1.1/1.2 [BNNGF-56116]
- Service interruption time has been decreased when a proxy rule is changed. [BNNGF-56184]

Report Creator

- Report Creator now correctly displays ATP results when Meiryo Regular or MS Gothic Regular fonts are used. [BNNGF-54354]

REST API

- New endpoints have been added to extend the scope of Zero Touch related REST API.

[BNNGF-59274]

SSL VPN

- All cookies returned from the SSL VPN are now marked as secure. [BNNGS-3632]
- **RDP** – Redirect Printers option now works on macOS. [BNNGS-3436]
- **Web Apps** – Added validation to custom headers. [BNNGS-3537]
- **Web Apps** – The HTTP Post limit has been increased and made configurable. [BNNGS-3527]

REST API

- Newly generated tokens in the REST config plugin can now be used immediately after the generation. [BNNGF-56113]
- A REST API connection is no longer reset after a configuration has been reloaded. [BNNGF-56119]

Virus Scanner

- In Firewall Admin, ATP now accepts Excel macro files for file scanning. [BNNGF-56466]
- Block on error no longer blocks encrypted archives. [BNNGF-56495]
- An issue where the Virus Scanner stopped processing scan requests when certain types of archives were scanned with ATP has been solved. [BNNGF-58370]
- Fixed fail-open and fail-close policy issues for SMTP scanning in combination with clamAV. [BNNGF-58523]

VPN

- Multi-Factor Authentication for client-to-site VPN tunnels can now be done with MSAD user + MSAD password + RSA token. [BNNGF-26260]
- CudaLaunch VPN connections now work as expected on iOS 9.3. [BNNGF-38029]
- The source address of source-based routing entries for VPN traffic will be ignored if they are moved to the main routing table by setting **Add VPN Routes to Main Routing Table (Single Routing Table)** to **yes** in **CONFIGURATION > Configuration Tree > Assigned Services > VPN > VPN Settings > Server Settings**. [BNNGF-40962]
- Dyn-Mesh tunnels now generate the correct event ID (3003, 3004) when starting or stopping. [BNNGF-43170]
- The **Encryption** field in the window **Change Ipsec Phase I** now shows the correct type of encryption. [BNNGF-42083]
- IPsec IKEv2 VPN tunnels now support **RADIUS** authentication scheme. [BNNGF-49976]
- Dynamic mesh tunnels no longer fail after spoke HA failover. [BNNGF-53416]
- Client-to-site connections with IKEv2 tunnels now work as expected when the network type is set to **Local (Proxy ARP)** [BNNGF-54813]
- Client-to-site TINA tunnels now support the configuration of IPv6 adresses for the payload. [BNNGF-54846]
- At logon with NAC 5.0.1, the VPN log now reports the correct error message if no more data is

received. [BNNGF-55389]
- The firewall no longer crashes during re-keying phase 1 for a IKEv2 client-to-site VPN tunnel. [BNNGF-55899]
- Establishing a site-to-site TINA tunnel after an HA failover no longer causes crypto errors and now works as expected. [BNNGF-56143]
- In Firewall Admin, entries in **LOGS > VPN** now show correct duration time in the correct format. [BNNGF-56282]
- Traffic from a managed box is sent correctly to the CC through the management tunnel. [BNNGF-56309]
- Disabling IPsec VPN tunnel now works as expected. [BNNGF-56688]
- Fixed a Linux / MacOS VPN client local priviledge escalation. [BNNGF-57654]
- Administrators can now enforce the usage of TOTP in the Group Policy settings. [BNNGF-57689]
- A script now changes the MTU size for every VPN service to 1300. [BNNGF-57998]
- Enabling the option **Use IPsec dynamic IPS** in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings > Server Settings**, section **IKE Parameters**, will establish a listening port on 0.0.0.0 as expected. [BNNGF-58146]
- The process **ike3** now binds to all network interfaces if **Use IPsec dynamic IPs** is set to **yes**. [BNNGF-58259]
- Boxes using an M40 modem for dial-in now successfully re-establish an IKEv2 tunnel connection after a temporary tunnel shutdown due to 4G restarts or bad signals. [BNNGF-58513]
- The execution of the 'getcrl' command no longer fails in certain situations. [BNNGF-58683]
- Terminating IPsec VPN tunnels now works as expected. [BNNGF-59647]
- The Web UI now accepts entering 0.0.0.0/0 for the remote peer. [BNNGF-59784]
- When establishing an IPsec site-to-site tunnel with multiple intermediate CA certificates, the correct certificates are now used. [BNNGF-59803]
- 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]
- Transferring files via a client-to-site connection to a network share no longer causes the VPN client to crash if compression is enabled. [BNNGF-61103]
- The default encryption for AutoVPN has been changed to use AES256. [BNNGF-60941]
- Auditing of SSLVPN Dynamic Firewall Rules has been improved. [BNNGS-3593]
- In SSLVPN Network Places, a **Show Hidden Files** option has been added. [BNNGS-3510]

Web UI

- Deleting predefined networks objects no longer cause an error message. [BNNGF-53580]
- On the Web UI in the section **Security Subscription Status**, the firewall no longer displays the status **Licensed : disabled** for the malware protection subscription status if malware protection is licensed and running. [BNNGF-56586]
- In the Web UI, the subscription status now looks consistent for license-based services. [BNNGF-59268]

Known Issues

- **Azure Cloud** – Network activation on a CloudGen Firewall with Azure-accelerated network interfaces can fail and put the firewall into an unusable state in certain situations. [BNNGF-62926]
  Rebooting will solve the problem.
- 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]
- **Barracuda OS** – After a reboot of the partner box via **Control > Service > Restart Box**, **Control > Service**, the firewall is not able to reconnect to the rebooted box automatically. As workaround, use **Reconnect Session to Unit** to reconnect and restore the status. [BNNGF-61773]
- **DNS** – DHCP is broken on VLAN interfaces. As workaround, disable header reordering in the Virtual LAN configuration for every VLAN. [BNNGF-61859]
  As a workaround, disable header reordering on the Virtual LAN Configuration for every VLAN.
- **DNS** – The migration of the DNS service fails when importing a 7.x PAR file on a 8.x box. [BNNGF-61953]
- **Firewall** – Transparent redirects are not working as expected. Workaround: Configure a next hop that is not in a local network. [BNNGF-61912]
  For more information, see How to Configure a Transparent Redirect.
- **VPN** – VPN transport type "Routing" for TINA tunnels is broken. [BNNGF-61912]
- **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]

Figures