8.2.0 Release Notes

https://campus.barracuda.com/doc/95256618/

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.

Due to a known issue concerning VPN, users with several hundred VPN tunnels should not install this release.

For details, see the **Known Issues** section below: VPN, BNNGF-73584.

Changelog

To keep our customers informed, the "Known Issues" list and the release of hotfixes resolving these known issues are now updated regularly. If there are intermediate updates to this release, the corresponding notes will be found in this info box.

- **9.9.2021 – Release of Hotfix 1058**.
  For more information on Hotfix-1058, see https://dlportal.barracudanetworks.com/#/packages/5288/firewall-1058-8.2.0-131102200.tgz.

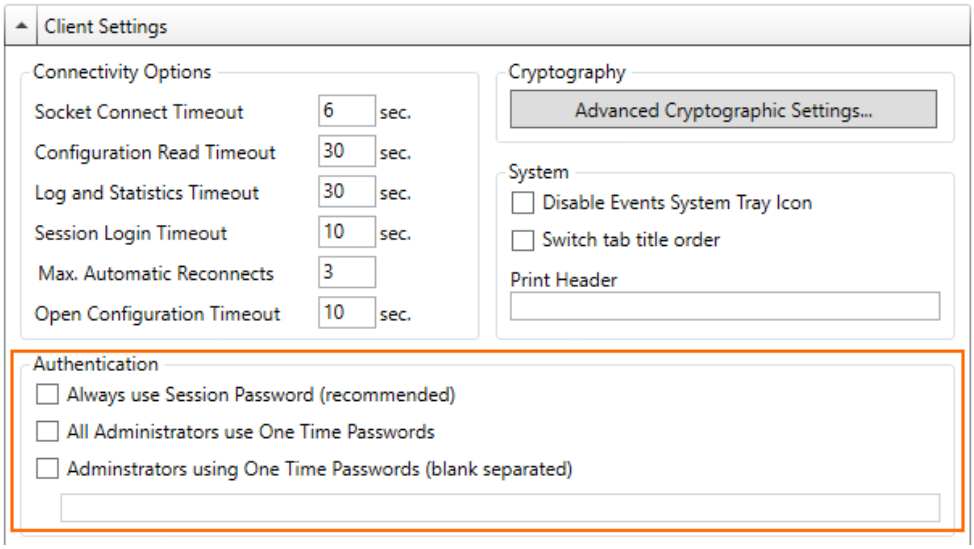
Version 8.2.0 is a major update firmware release including numerous valuable features and improvements.

What's new in version 8.2.0

Firewall Admin

The usage of session and one-time passwords in **Firewall Admin > Settings > Client Settings** can now be configured in the section **Authentication**.

Barracuda Firewall Admin 8.2 Settings:

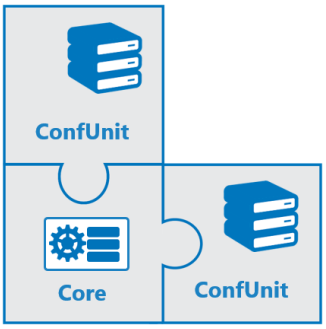


For more information on how to use OTP, see

- How to Configure Multi-Factor Authentication Using Time-based One-time Password (TOTP)
- How to Self-Enroll for Time-Based One-Time Passwords (TOTP) using the Simple TOTP Web Portal

Configuration Template Manager

Configuration Templates are a new Control Center tool for creating and maintaining configurations for firewalls and SCs, with a special focus on scalability and automation. The tool is available for the Control Center and CG firewalls starting with release 8.2.



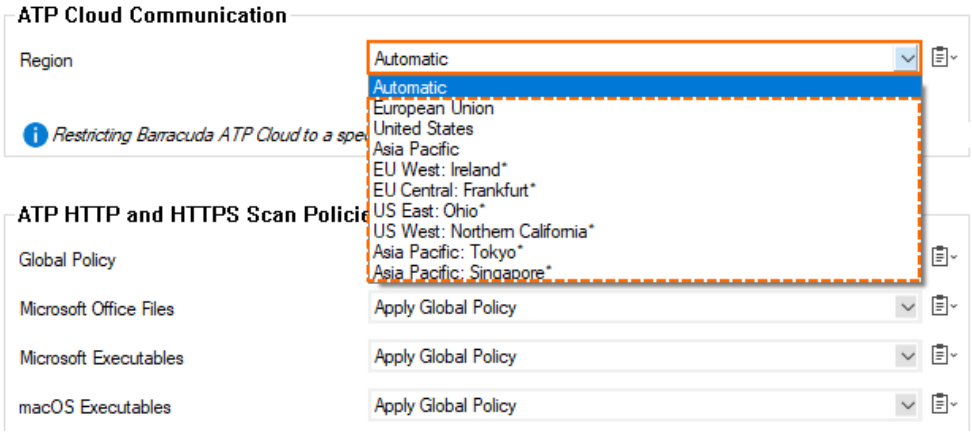
Configuration Templates allow you to do the following:

- Manage common configuration information for deploying and managing large-scale configurations while providing maximum freedom to individually configure parameters. This makes it easy to distinguish similar configurations from each other.

For more information on the Configuration Template Manager, see Configuration Template Manager.

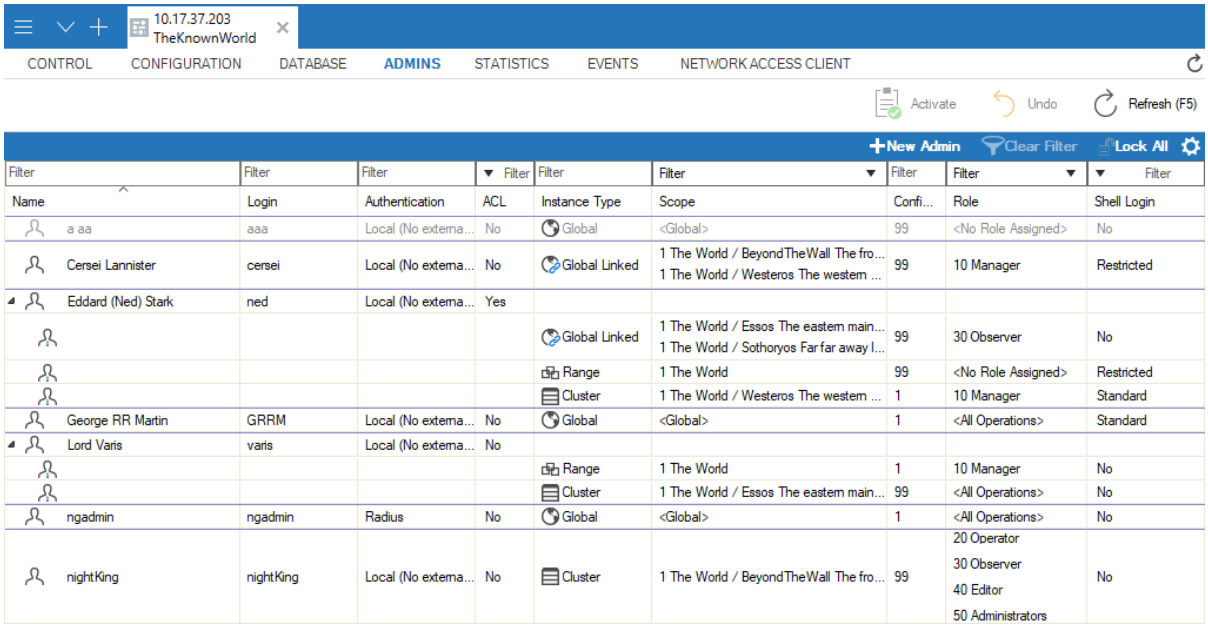
Barracuda ATP

When configuring ATP Cloud Communication in **CONFIGURATION > Configuration Tree > Box > Assigned Services > Virus Scanner > Virus Scanner Settings > ATP**, the list for **Region** in the section **ATP Cloud Communication** now contains entries that offer a greater range of options for the region.



Control Center Admins

The user interface for Control Center administrators has been redesigned to provide a better overview.



Google Cloud

If you experience transfer rate issues when connecting from an on-premises CloudGen firewall to the Google Cloud via a VPN TINA tunnel, please read the following to potentially resolve the problem:

1. Because Google Cloud VPN does not support fragmenting of packets after the encapsulation, the maximal MTU size for VPN gateways must be set to 1460 bytes. Therefore, if you want to connect from an on-premises CloudGen Firewall to the Google Cloud via a VPN TINA tunnel, you must ensure that the standard MTU size on your firewall is set to 1390 Bytes, e.g., in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings > Routed VPN**.
2. Some Internet providers regard port #691 as a 'lower port number' (because the port number is lower than 1024) and limit the maximal transfer speed on that port. Because Barracuda CloudGen Firewalls use port #691 for VPN TINA tunnels, connecting to the Google Cloud may result in a limited transfer speed, which negatively influences the flow of traffic through port #691.

   Because this is not a generic problem caused by the firewall, Barracuda recommends as a workaround to shift traffic from such a speed-limited connection port to a port range above 1024, which is usually not limited in speed. For this, you must do the following:
   1. On the active side of the VPN tunnel, which is the CloudGen Firewall, create an access rule with a DstNAT for the host firewall that redirects traffic from port #691 to any valid/free port number above 1024 that provides higher speed transfers. For more information on how to create a DstNAT access rule, see How to Create a Destination NAT Access Rule.
   2. On the passive side of the VPN tunnel, create an access rule with an AppRedirect to shift traffic from your selected high-speed port back to the original port #691. For more information on how to create an AppRedirect access rule, see How to Create an App Redirect Access Rule.

Hostname List for Barracuda Services

Access to hosts and domains in the Barracuda Cloud is required for the proper operation of a Barracuda CloudGen Firewall or Control Center. The hostname list has been updated to reflect the newest values for domains and their associated IP addresses and port numbers.

For more information on the updated hostname list, see Best Practice - Hostname List for Barracuda Online Services.

New Barracuda Health Monitoring System Goes Live

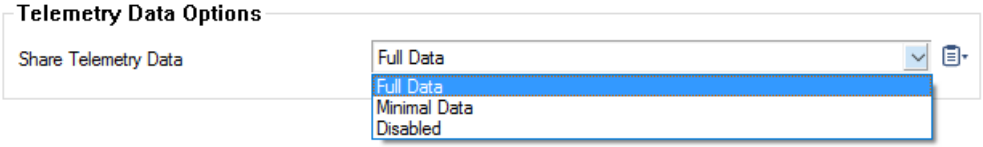
Think Customer and Drive Innovation are core values of Barracuda Networks. The better we understand how our solutions are used, the better we can enhance our services and proactively improve product quality. A big step in this direction is provided by the analysis of appliance health data and associated contextual telemetry information that the newer Barracuda CloudGen Firewall appliances can provide. With the current firmware release this is now active by default.

Please be advised that upgrading to firmware version 8.2.0 will automatically enable appliance health monitoring and contextual telemetry to send telemetry data in **full data** mode. Barracuda health monitoring includes the transmission of a predefined set of telemetry data to speed up support

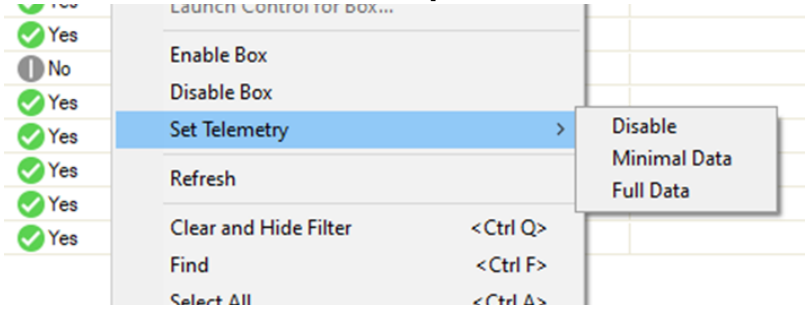
diagnostics and enable proactive maintenance. In case system components subject to wear and tear degrade over time, or configuration settings are sub-optimal, our support team will be able to anticipate issues long before they actually materialize, and to recommend optimized system settings to reduce unnecessary system loads. During normal support operations, the Barracuda support team will also be able to react to problems and troubleshoot much faster with up-to-date health data - and without the need to always arrange for a maintenance window.

The configuration change is automatically applied to all new installations and upgrades of previous firmware versions. The status of Barracuda health monitoring is displayed in the Dashboard view in the **Status** window for stand-alone firewalls and on the Firewall Control Center under **Control > Status Map**.
Transmitted data does not include sensitive information, nor does the scheme itself allow Barracuda to access any appliance remotely in any way. A complete list of predefined telemetry parameters is published in Barracuda Campus.
For more information, see
https://campus.barracuda.com/product/cloudgenfirewall/doc/79463312/telemetry-data/.
The status of the telemetry system will be indicated at different places in the user interface. In the STATUS element of the DASHBOARD, you will see the status of the telemetry system indicated by this entry:

In case your firewall cannot connect to our health monitoring servers, or you want to reduce the data amount to a minimum, you can change telemetry data settings under **Configuration > Configuration Tree > Box > Administrative Settings > Telemetry Data**.



For Control Center-managed firewalls, administrative settings can be linked via the repository feature, or you can change settings for multiple firewalls in **Configuration > on right table/register "Boxes" > select all or multiple boxes > context menu > Set Telemetry > Full Data**.



REST API Enhancements

The REST API has been updated and is now in sync with the newest features of firmware release 8.2.0.

Tufin Integration

Tufin SecureTrack is a firewall management solution that enables security, compliance, and connectivity visualization of Enterprise IT across multi-vendor firewall environments and cloud platforms. SecureTrack provides insights into network connectivity and security policy changes and can also alert for potential new security risks.

With the start of firmware release 8.2, the CloudGen Firewall supports integration with Tufin SecureTrack.

For more information on how the Barracuda CloudGen Firewall integrates with Tufin SecureTrack, see TUFIN Integration API Service.

VPN

VPN Forward Error Correction

The transmission of interactive and streaming content can sometimes lead to data loss during transmission. If sufficient bandwidth is present, additional forward-error-correction (FEC) packets can be sent so that lost payload can be recovered.

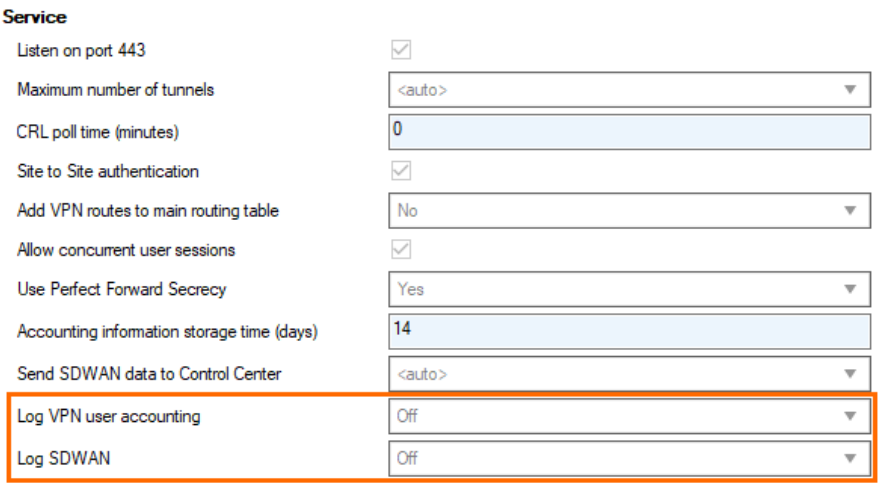
Because FEC requires a special CPU command set, known as the SSSE3 extension, virtual hardware also depends on the availability of this extension. Therefore, it is necessary to upgrade the virtual hardware to make use of this special feature on ESXi hypervisors.

For more information on upgrading virtual hardware, see the migration instructions for 8.2.0 in the 8.2.0 Migration Notes.

Switches for Logging Special VPN Information

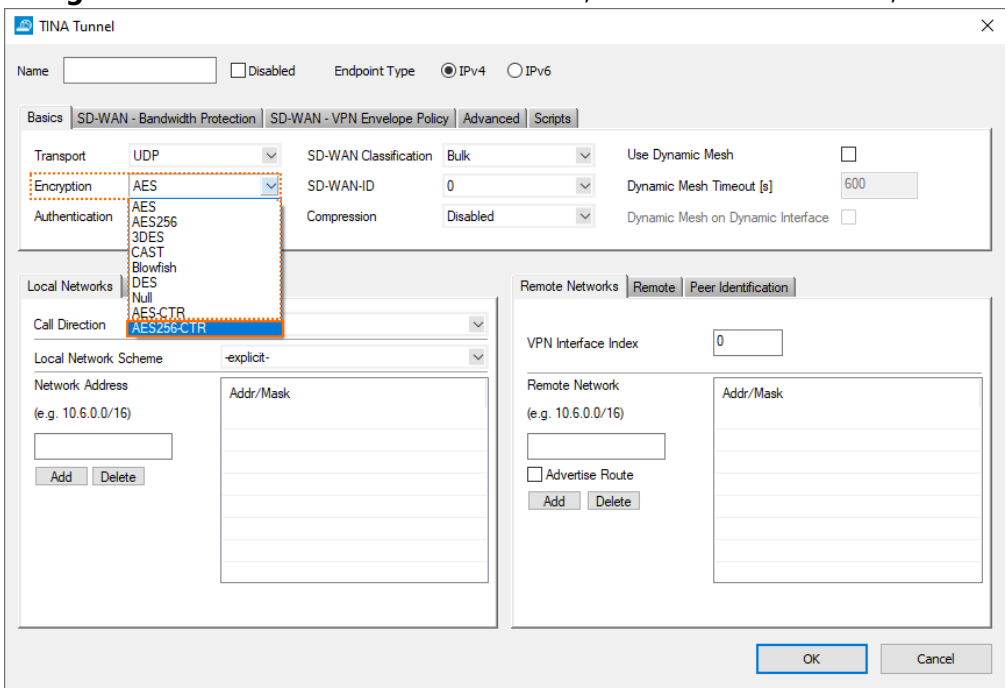
Two new switches have been added to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings**:

1. **Log VPN** user accounting: If set to **On**, this option creates a log entry for every user log-in and log-off for a client-to-site connection.
2. **Log SDWAN**: If set to **On**, the firewall stores the Min/Avg/Max value of the throughput every 5 minutes.



New Encryption Option for TINA Tunnels

The new option **AES256-CTR** has been added to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Site to Site**, window **TINA Tunnel**, tab **Basics**, list **Encryption**.



Improvements Included in Version 8.2.0

Authentication

- In case of a group of RADIUS servers, authentication requests are no longer sent to other RADIUS servers if the first server has rejected the request. [BNNGF-67177]

- Authentication with TACACS+ now works as expected. [BNNGF-67386]
- TS agent authentication now works reliably with more than 1024 terminal servers. [BNNGF-67667]
- The SSH service no longer unexpectedly dies when updating configurations. [BNNGF-68109]
- The TACACS+ authentication no longer crashes after an update. [BNNGF-68147]
- Authenticating with an OTP on the CPN client no longer reports errors on the first login. [BNNGF-69229]
- Authentication redirect now works as expected. [BNNGF-69280]
- The menu list in **CC > Config > Global Settings > Administrative Roles > External Admins** now includes an entry for redirecting authentication. [BNNGF-69312]
- RADIUS authentication now works as expected. [BNNGF-70048]
- TOTP usernames with underscore are now correctly displayed in **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Time-based OTP Bulk Enrollment**, section **User Bulk Enrollment**. [BNNGF-70094]
- The firewall authentication screen and the ticketing page have been updated. [BNNGF-70608]
- TOTP users no longer show up after being deleted. [BNNGF-70741]
- Changes to authentication configurations now work as expected. [BNNGF-70775]
- Radius authentication now accepts up to 99 simultaneous authentications. [BNNGF-70953]
- The firewall authentication daemon no longer needs to be killed manually when doing changes to Inline Authentication settings. [BNNGF-71363]
- After exceeding the maximum permitted login attempts, no AD server within the same group gets queried within the configured timeout period. [BNNGF-71966]

Barracuda Firewall Admin

- Administrator accounts can now be cloned for CC Admins. [BNNGF-55604]
- The user interface for ADMINS has a new design. [BNNGF-56755]
- The SNMP service ACL input field in **CONFIGURATION > Configuration Tree > SNMPOP Service Settings > Access Groups > Peers** now accepts IPv6 addresses correctly. [BNNGF-61517]
- When executing an **Emergency Override**, notification dialog windows will also be displayed to inform the user. [BNNGF-63969]
- In Firewall Admin, logging can now be restricted to the selected VPN IKEv1 tunnel. [BNNGF-64420]
- The usage of session and one-time passwords in **Firewall Admin > Settings > Client Settings** can now be configured in the section **Authentication**. [BNNGF-64612]
- Statistic entries for managed boxes running with the new 2-layer service architecture now contain the appropriate **Assigned Services** name. [BNNGF-65765]
- The user interface for **CC Administrators** has a new design. [BNNGF-66104]
- The CRL issuer of root certificates at **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings > Root Certificates** can now be selected in the **Certificate revocation** tab. [BNNGF-66252] [BNNGF-71701]
- BGP route map entries no longer accept '0' as a sequence number in **CONFIGURATION > Configuration Tree > Box > Assigned Services > OSPF/RIP/BGP Routing > Filter Setup IPv4**, section **BGP Specific Conditions**, window **Route Map Entry**, edit field **Sequence Number**. [BNNGF-66293]

- The '#' character is now allowed in the SMTP password field. [BNNGF-69024]
- In case of a network activation in **CONTROL > Box > Network > Activate new network configuration**, the firewall checks and highlights the "Soft" button in case a soft activation is adequate for the preceding changes. [BNNGF-69235]
- The two columns **Authentication Level** and **Last Password Change** have been added to be selectable for the **CC Admin** view. [BNNGF-69527]
- Two new switches have been added to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings**: 1. Log VPN user accounting. 2. Log SDWAN. [BNNGF-69961]
- When importing an invalid certificate chain, Firewall Admin now reports this with an error message. [BNNGF-70093]
- Firewall Admin no longer sets the values of SOA records to zero. [BNNGF-70320]
- Firewall Admin now displays all licenses correctly on a Control Center in **CONTROL > Barracuda Activation**. [BNNGF-70793]
- The user interface for the new CC Admin dialog now contains the help information. [BNNGF-70922]
- The new option **AES256-CTR** has been added to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Site to Site**, window **TINA Tunnel**, tab **Basics**, list **Encryption**. [BNNGF-71136]
- An icon has been added to **CONTROL** to indicate the status of the CloudGen Access service. [BNNGF-71394]
- Filtering options have been added for the Control Center in **CONTROL > Pool Licenses**. [BNNGF-71555]
- The Control Center tab **Barracuda Activation** has been relocated and can now be found as part of **Control Center > Licensing**. [BNNGF-71559]
- A graph for the past usage of pool licenses has been added to the **Barracuda Activation** dashboard. [BNNGF-71560]
- The Control Center tab **Pool Licenses** has been relocated and can now be found as part of **Control Center > Licensing**. [BNNGF-71561]
- The list view at **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings > Root Certificates** now displays the issuer of the certificate in the column **Issued By**. [BNNGF-71701]
- In case of a bulk server migration from the older 3-layer to the new 2-layer service architecture on a Control Center, hotfixes are now announced in an information window to let the user chose whether to install the hotfix. [BNNGF-71718]
- A doughnut chart has been added to display the subscription usage of pool licenses. [BNNGF-71822]
- The dashboard for licensing has been completely reworked, can now be accessed on the Control Center at **CONTROL > Licensing**, and also contains customizable filters for adding and removing date from the list. [BNNGF-72108]
- Configuration fields have been added for Forward Error Correction for VPN TINA tunnels at **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Site to Site**, tab **TINA Tunnels**, window **TINA Tunnel**, tab **SD-WAN - Bandwidth Protection**. [BNNGF-72161]
- Firewall Admin now correctly displays the value for **Ipsec Timeout** in **VPN Settings**. [BNNGF-72815]

- CloudGen Access icons are now correctly displayed in the tab bar. [BNNGF-72848]
- TLS v1.3 can now be selected in case Feature Level is greater than or equal to 8.0. [BNNGF-73200]
- Starting with release 8.2.0, Firewall Admin only offers RSA keys with sizes that are greater than 1024 bit in length. [BNNGF-73202]
- On the Control Center, the tabs **Barracuda Activation** and **Pool licenses** tabs have been replaced by the new common tab **Licensing**. [BNNGF-73399]
- The ACL edit field in the edit window for CC Admins in **CC > ADMINS**, tab **General** now processes the IP addresses in CIDR notation. [BNNGF-73700]
- A new column **Pool License Type** for displaying the license type has been added to **CC > CONTROL > Licensing > POOL LICENSES** and **CC > CONTROL > Licensing > FLOATING LICENSES**. [BNNGF-73705]
- A new information field **Firmware Version** has been added to the **CONTROL** view in Firewall Admin. [BNNGF-74324]
- Forwarding Zones now store the value for **Forwarders** in the correct field. [BNNGF-74365]
- The new licensing tab in the Control Center no longer displays licenses for versions lower than 7.1 and informs with a notification message in the corresponding window. [BNNGF-74432]
- Firewall Admin uses the last chosen zoom level to display all pool licenses. [BNNGF-74497]
- Session reconnects are now much more responsive. [BNNGF-74644]
- Firewall Admin no longer displays 3-layer server-service nodes for boxes running with the 2-layer assigned services node in certain situations. [BNNGF-75611]

Barracuda OS

- The connection statistics for application rules have been completely removed. [BNNGF-27651]
- The agent string limit has been increased to now accept 192 characters. [BNNGF-35986]
- Telemetry data generation for IKEv2 tunnels has been fixed and now reports the correct number of tunnels. [BNNGF-45302]
- The retrieval of metadata for the firmware update of managed boxes now works as expected. [BNNGF-54555]
- HA repository links are now supported. [BNNGF-68143]
- Non-managed HA clusters can now be migrated in a single step. [BNNGF-69060]
- Migration of boxes no longer fails if the box name is identical to the server name when uniqueness is set to global. [BNNGF-69199]
- DNS-based network objects are now supported by the personal firewall. [BNNGF-55320]
- Archive scanning is now also available for SMTP, POP3, and FTP. [BNNGF-55696]
- Configuring IPv6 subnets for IPv6 DHCP addresses in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DHCP > Operation Setup IPv6**, configuration window **Subnets > Network Address Field**, now works as expected. [BNNGF-56665]
- A complete update no longer leads to two secondary boxes. [BNNGF-70328]
- When migrating a bridge, a warning will be displayed to inform the user about a necessary boxnet activation. [BNNGF-72003]
- References to certificates in the **Certificate Store** are now created as expected. [BNNGF-71691]
- KVM-based CG firewalls can now be shutdown via Proxmox UI. [BNNGF-60594]
- The S7 protocol support has been updated. [BNNGF-60637]

- Browser agent Opera will now be blocked on request as expected. [BNNGF-60719]
- The firewall operates at its maximum throughput when offloading is disabled. [BNNGF-61644]
- The 2-layer service architecture is now supported by repositories. [BNNGF-61779]
- When applying a 'BLOCK' rule, erroneous events no longer occur in certain cases. [BNNGF-63275]
- 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]
- SSL VPN now supports TLSv1.3. [BNNGF-63985]
- Policy routes can now be enabled via **Soft Activation**. [BNNGF-64221]
- The status of pool licenses no longer gets corrupted in certain situations. [BNNGF-64716]
- An automatically generated RCS report now contains the RCS message field/info. [BNNGF-65509]
- WAagent now creates the swap partition as expected and no longer takes away storage space from the root partition. [BNNGF-66051]
- CC event notifications are now sent correctly if the StartTLS option is activated in **CC > Box > Administrative Settings > Notifications**, section **Email Notifications**. [BNNGF-66456]
- If a VLAN is configured for the first time on the firewall, the option for **Header Reordering** is by default set to **On** in **CONFIGURATION > Configuration Tree > Network > Virtual VLAN**. [BNNGF-66582]
- The dot character (' . ') is no longer allowed to be used in bridge names. [BNNGF-66666]
- A successful installation with NGInstall is now also indicated with a sound on F380b, F400c, and T400. [BNNGF-66777]
- The SNMPd no longer crashes after a failover. [BNNGF-66792]
- The SNMP trap uses the correct IP as agent address and correctly handles the event. [BNNGF-66793]
- File uploads from on-premises boxes to GCP via a TINA tunnel now works as expected due to a fix for the VirtIO driver. [BNNGF-66954]
- Host names may now be used for explicit IP addresses in the VPN GTI editor. [BNNGF-67163]
- Certificates with empty subject but with valid subject alternative names are now supported according to RFC5280, section 4.1.2.6. [BNNGF-67778]
- Authenticating via DC Agent if a large number of user accounts is configured now works as expected. [BNNGF-67861]
- If connections to an external bind IP on LTE- and XDSL-equipped firewalls breaks, active sessions for TINA tunnels are now actively terminated and therefore no longer cause trouble for other types of traffic. [BNNGF-68021]
- The archive scanner no longer freezes in certain situations, and archives can be downloaded again. [BNNGF-68051]
- When configuring a remote management tunnel on a Control Center in **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > your managed CloudGen firewall > Network**, the **Suggest VIP** button now also works in conjunction with repositories. [BNNGF-68056]
- Recovering a CC using a box.par file now works as expected. [BNNGF-68097]
- Local authentication is now enabled for the command line tool cctool. [BNNGF-68548]
- Update from 7.2.6 to 8.0.3 or 8.0.4 now works as expected. [BNNGF-68689]
- Client-to-site VPN networks are now announced by OSPF. [BNNGF-68731]

- The REST API for handling a virtual server on a firewall has been removed from stand-alone boxes. [BNNGF-68801]
- Moving an interface to another namespace no longer requires a network activation. [BNNGF-69189]
- Downloading a PAR file with cctool to HA firewalls operating the 2-level service architecture now works as expected. [BNNGF-69232]
- When configuring routing tables in **CONFIGURATION > Configuration Tree > Box > Network > Advanced Routing**, and **Configuration Mode** is set to **Advanced**, it is now possible to configure a source IP address for source-based routing. [BNNGF-69345]
- Soft activation now removes all vlans as expected. [BNNGF-69348]
- OID for BGP now works as expected. [BNNGF-69558]
- After logging into SSH as an Admin on box level of a CC, the command **ulimit** now runs under the correct permissions. [BNNGF-69603]
- The firewall no longer crashes in conjunction with TFTP. [BNNGF-69849]
- DNS objects now work as expected on F900 units after upgrading from 7.2.6 to 8.0.4. [BNNGF-69994]
- When blocking a service from Firewall Admin, the CloudGen Access proxy service is stopped as expected. [BNNGF-70000]
- Intensive configuration updates on an HA pair with configured DNS Server service no longer run into a timeout when the changes are synced to the secondary firewall. [BNNGF-70089]
- On an 8.2.0 Control Center, 8.0 box network nodes can no longer be created. [BNNGF-68952]
- The configuration of autonegotiation, speed, and duplex now works as expected for the SFP slots. [BNNGF-70146]
- When migrating from the former 3-layer server-service architecture to the new 2-layer service architecture, the secondary box is not created if it was already configured before the migration. [BNNGF-70197]
- When using an additional private HA uplink, the correct HA partner status is displayed for both boxes in Firewall Admin. [BNNGF-70198]
- Hardware detection for port-labeling now works as expected and creates an appropriate log entry. [BNNGF-70223]
- After migrating from 7.2.6 to 8.0.4, syslog streaming now works as expected. [BNNGF-70432]
- The GEO IP database has been updated. [BNNGF-70442]
- The URL Filter no longer looks up categories for private IP addresses. [BNNGF-70465]
- The firewall now always boots and correctly honors the configured external log storage location. [BNNGF-70493]
- The firewall no longer terminates sessions after receiving an RST with sequence numbers that are too old. [BNNGF-70685]
- Unsupported offloading settings are automatically disabled on the interfaces. [BNNGF-70739]
- Expired QuoVadis trusted CA intermediate certificates have been updated and no longer break SSL Interception. [BNNGF-70864]
- It is now possible to configure more than 16 bridge groups. [BNNGF-70894]
- The Linux command 'sudo' has been updated to cover CVE-2021-3156. [BNNGF-70994]
- Log lines are now displayed correctly in the Web UI. [BNNGF-71011]
- IPMI for HA can now be configured, and config entries are stored accordingly. [BNNGF-71087]
- The system-wide limit of open files has been increased for certain appliances. [BNNGF-71114]
- The SNMP path is now available for the PHION-MIB OID for hardware sensors on F280 boxes as

expected. [BNNGF-71159]
- Host names are now consistent in version 8. [BNNGF-71190]
- Changes made on the firewall by external users with a login name containing the '@' character are now shown in RCS with '(at)'. [BNNGF-71191]
- SNI SSL now works with the correct certificate. [BNNGF-71422]
- The GEO IP database has been updated. [BNNGF-71808]
- Non-TOR applications no longer get flagged as false-positive TOR application by the firewall. [BNNGF-71962]
- It is now possible to use certificates from the Certificate Store in the HTTP proxy. [BNNGF-71998]
- After the migration from the 3-layer server-service architecture to the new 2-layer service architecture, the secondary HA firewall now realizes that there was a migration and works as expected. [BNNGF-72196]
- Offline bridges now receive configuration updates as expected. [BNNGF-72266]
- The GEO IP database has been updated. [BNNGF-72503]
- The firewall plugins for SQLNet, ICABrowser, and RSH have been removed. [BNNGF-72524]
- The UI check box for the option **Use Same Port** like in the Web UI window **Firewall > Connection Objects > Connection Objects > Add Connection Object** now works as expected. [BNNGF-72703]
- On firewalls operating under KVM, packets are now evenly distributed between all available CPUs. [BNNGF-72844]
- Apple authentication is not intercepted. [BNNGF-72857]
- When setting **Enable BFD** to **yes** in **CONFIGURATION > Configuration Tree > Box > Services > OSPF/RIP/BGP Settings > Neighbor Setup IPv4**, window **Neigbhbors**, section **BGP Parameters** (in advanced mode), the settings are available immediately after confirming the configuration. [BNNGF-73069]
- The speed test works as expected. [BNNGF-73131]
- Service objects with port ranges containing only 2 ports no longer cause the firewall to crash. [BNNGF-73649]
- Importing of boxes with a virtual server into 8.0 cluster is allowed. [BNNGF-73755]
- On an HA cluster the session sync now works as expected [BNNGF-73831]
- The term 'serverIP' has been replaced by 'sharedIP' in the host firewall ruleset. [BNNGF-74310]

Cloud General

- All the ports listed in the NGF-VPN service object will be allowed to the DHCP interfaces. The rule OP-SRV-VPN-DHCP is part of the new default ruleset. [BNNGF-70218]

Cloud Azure

- The deployment no longer breaks in conjunction with the Microsoft Azure Linux Agent. [BNNGF-68889]

Cloud Google

- When performing an HA failover in Google Cloud, the HA box no longer runs out of memory. [BNNGF-69915]

Control Center

- The command line tool cctool now supports ConfTemplate-based boxes (CGF and SC) and encrypted PAR files. [BNNGF-68552]
- Archive PAR file creation now works as expected for larger PAR files. [BNNGF-71743]
- PAR files greater than 2 GB are no longer broken when exported with the command line tool cctool. [BNNGF-71814]

DHCP

- Pool ranges for **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > Assigned Services > DHCP** now work as expected for network masks larger than /24. [BNNGF-69115]

DNS

- After migrating to 8.0.4, the default values in SOA records are no longer set to zero. [BNNGF-69221]
- It is now possible to select a **Forwarding** zone as **Hosted Zone Type** in **CONFIGURATION > Configuration Tree > Box > Assigned Services > DNS > DNS Settings > Hosted Zones**, window **Add Hosted Zone / Domain**. [BNNGF-71553]
- The BIND system has been updated to fix CVE-2021-25215. [BNNGF-74781]

High Availability

- There are now 2 fields for the primary and the secondary HA box to enter/save an RSA-server-key. [BNNGF-32212]

HTTP Proxy

- The HTTP proxy has been updated and no longer leaks information. [BNNGF-64698]
- The HTTP proxy has been updated to version 4.15. [BNNGF-74727]

REST

- Deprecated REST API endpoints have been removed. [BNNGF-63305]
- The REST API now supports configuration for Management IP, Management Access Tunnel, and Shared IPs for the 2-layer service architecture. [BNNGF-70925]
- The REST API now supports configuration for DHCP under **Box configuration** and **CC Configuration**. [BNNGF-72090]
- The REST API now supports assigning a pool license. [BNNGF-72887]

Virus Scanner

- When configuring ATP Cloud Communication in **CONFIGURATION > Configuration Tree >**

Box > Assigned Services > Virus Scanner > Virus Scanner Settings > ATP, the list for **Region** in the section **ATP Cloud Communication** now contains entries that offer a greater range of options for the region. [BNNGF-67209]

VPN

- Support for SAML authentication has been added to the client-to-site VPN. [BNNGF-63047]
- Traffic is now routed correctly to the corresponding VPN tunnels. [BNNGF-63242]
- Radius authentication with a OTP no longer creates multiple SMSs to be sent. [BNNGF-63328]
- SD-WAN bandwidth measurement now works as expected. [BNNGF-63703]
- The AES-CTR encryption has been implemented for VPN TINA tunnels. [BNNGF-64151]
- IPSEC IKEv1 now enforces configured DH group in phase 2 SA negotiation. [BNNGF-64739]
- Dynmesh tunnel configuration is synced to the HA partner as expected. [BNNGF-65023]
- Dynmesh transports now recover as expected after an Internet outage [BNNGF-65026]
- The VPN service no longer experiences memory issues in certain situations. [BNNGF-65639]
- Active channel probing in SD-WAN now works as expected. [BNNGF-66121]
- Performance testing of any encryption method now works as expected. [BNNGF-67031]
- The AES256 cipher key length for VPN TINA tunnels is now logged. [BNNGF-68600]
- UDP transports now works as expected after an update to 8.0.4. [BNNGF-68988]
- With this release, you can now use VPN services on CGF Firewalls as an endpoint for FSCs. This option can be configured for every FSC management or data network and is available for FSCs configured with the new Configuration Templates feature. [BNNGF-69360]
- BGP routing over IKEv2 tunnels now works again as expected [BNNGF-69418]
- When establishing an IPsec tunnel, the IPsec responder now checks for all configured proposals in phase 2 and matches the configuration as expected. [BNNGF-69485]
- The import of PFX files into VPN settings now works as expected. [BNNGF-69741]
- The NAC clients 5.1.2 and 5.2.0 now connect to the VPN server as expected. [BNNGF-70145]
- VPN IPsec IKEv1 client-to-site tunnels are no longer crash in certain situations. [BNNGF-70309]
- Several improvements have been made to stabilize TINA tunnels and to prevent connections from unexpectedly closing. [BNNGF-70363]
- VPN log no longer shows C2S cleartext passwords. [BNNGF-70438]
- L2TP tunnels behind a NAT device now work as expected. [BNNGF-70676]
- TINA VPN tunnels running under firmware 8.0.4 no longer experience drop-outs due to memory issues in certain situations. [BNNGF-70825]
- The feature 'Temporary enable Tunnel' for IPsec IKEv1 tunnels has been completely disabled. [BNNGF-71403]
- After migrating from the 3-layer server-service architecture to the new 2-layer service architecture, IKE tunnels work as expected. [BNNGF-71419]
- The VPN client for NAC 5.2.1 no longer crashes if tunnel compression is active. [BNNGF-71648]
- IPsec tunnels are now stable and work as expected. [BNNGF-72561]
- The triple-DES encryption will no longer be available if VPN is operating in FIPS 140-2 mode. [BNNGF-73018]
- IKEv1 tunnels are now stable and work as expected. [BNNGF-73187]
- DynMesh tunnels are now completely removed when no longer needed. [BNNGF-73356]
- The signal handler of the VPN server now works as expected and is no longer terminated

unexpectedly in certain situations. [BNNGF-73384]

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 an explicitly named network does not copy the named network structure. [BNNGF-48588]
- **Barracuda Firewall Admin** – FW Admin 8.x fails to configure DNS 7.x correctly. [BNNGF-77636]
- **Barracuda OS** – Event Mail Notification is not working after the update to 8.2.0. [BNNGF-76327]
- The learn-only mode for OSPF is not working as expected. [BNNGF-65299]
- **Control Center** – After configuration and activation of the SAML/ADFS authentication, the SP metadata is not set on the Control Center. [BNNGF-76521]
  As a workaround, complete the following steps: 1. Connect to the box. 2. Configure SAML doing an **Emergency Override**.
- **DNS** – Although the underscore character ('_') may be used for DNS domain names in the CGF user interface, the character is not processed correctly by the underlying BIND system. [BNNGF-69225]
  It is not recommended to use the underscore character ('_').
- **Firewall** – Inspecting traffic for QUIC / UDP 443 is currently not supported. [BNNGF-74540]
- **Firewall** – If there are multiple custom objects filtering for the same content, matching will fail. [BNNGF-76562]
- "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.
- Installing a box with box.pca and/or re-deploying config via /opt/phion/update/box.pca does not work. [BNNGF-77829]
- **SSLVPN** – RDP connections can terminate after an unspecified amount of time and need to be re-established by the user. In some cases, connections cannot be re-established at all.
  For a workaround, manually restart the service on the CLI via `killall sslvpnsrv` To periodically restart via a cron job and/or script, use `/usr/bin/killall sslvpnsrv` For questions on how to implement automatic restart procedures, contact Barracuda Technical Support for assistance. [BNNGS-3761]
- **VPN** - If the firewall has hundreds of VPN tunnels established and the tunnels are either operating via a routed VPN or are "TCP and/or hybrid and/or IPsec tunnels", re-establishing these tunnels after a provider outage does not work. [BNNGF-73584]

Figures

1. firewall_admin_client_settings_authentication.png
2. puzzle_01.png
3. atp_fine_grained_selection_options.png
4. new_cc_admin_overview.png
5. telemetry_status_element_dashboard.png
6. t_data.png
7. t_data_CC.png
8. vpn_settings_2_new_switches.png
9. vpn_tina_new_aes-ctr_setting.png