8.0.3 Release Notes

https://campus.barracuda.com/doc/91982249/

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 8.0.3.

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.

Changelog

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

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 8.0.3

Version 8.0.3 is generally a maintenance release.

For customers running firmware 8.0.2, 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.

The section for Improvements Included in Version 8.0.3 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.

With firmware version 8.0.3, 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).

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

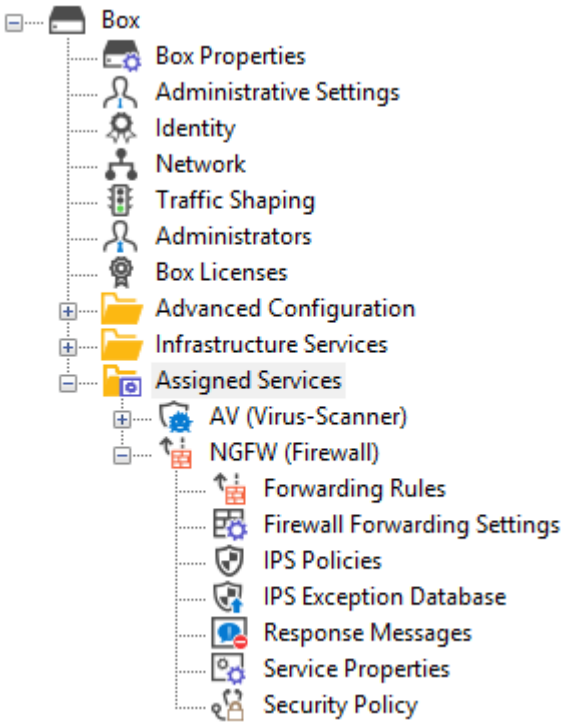
The new DNS service is based on the commonly known BIND standard. In case a recursive DNS server is configured, the DNS service automatically configures empty zones. This prevents the firewall from sending meaningless queries to Internet servers that cannot handle them.

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 8.0.3** further below.

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

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 8.0.3

Authentication

- Changing the initial/default password is now enforced and covers all login use cases. [BNNGF-63422]
- Authenticating with TOTP and a QR code now works as expected. [BNNGF-63965]

Barracuda Firewall Admin

- When switching to the view **CC > File Updates**, the list restores the last selected type of download. [BNNGF-56639]
- Copying to clipboard from various lists no longer fails in certain situations. [BNNGF-61669]
- The set of hyphening characters for the naming of authentication schemes in **CONFIGURATION > Configuration Tree > Assigned Services > VPN > Client to Site**, tab **Group Policy**, window **Group VPN Settings**, section **Preauthentication**, window **Preauthentication Details > New Name/Scheme Mapping**, now also supports the "-" character. [BNNGF-61804]
- The label of the DHCP tab now indicates the pool usage by the term "usage". [BNNGF-63400]
- In **Firewall > Live**, the list of filters now displays **Source** and **Destination** as expected. [BNNGF-63660]
- When using GTI in clusters, Firewall Admin now supports feature level 8.0 and 8.1 for VPN servers. [BNNGF-63779]

- Restarting dynamic networks in **Control -> Services** now works as expected. [BNNGF-63807]
- AV pattern updates can now be enabled/disabled in the **Subscription Status** element on the DASHBOARD. [BNNGF-63886]
- vWAN configurations are now correctly exported from Firewall Admin in **Config >Advanced Configuration > Cloud Integration**. [BNNGF-63907]
- When logging into a firewall, the **Installation Wizard** no longer asks a second time for the password in case the default password has already been changed. [BNNGF-63921]
- Invalid characters are purged in the data pasted into configuration fields. [BNNGF-63967]
- Firewall Admin now displays a warning message when configuring PAR files to be the default for creating backup archives. [BNNGF-64122]
- Pasting an access rule in Personal Firewall Rules in **CONFIGURATION > Assigned Services > VPN > Client to Site-VPN**, in the tab **Offline Firewall Rules**, now displays the correct number of pasted rules. [BNNGF-64182]
- In Firewall Admin it is now possible to push zero-touch configurations to a box-server HA pair of firewalls. [BNNGF-64727]
- The edit field for adding/deleting network routes for a list entry in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Client-to-Site**, tab **External CA > Common** accepts entering IPv4/v6 addresses with masks. [BNNGF-65033]
- Firewall Admin now handles caches for negative DNS responses as expected. [BNNGF-65602

Barracuda OS

- The trans7 process no longer produces a segmentation fault in certain situations. [BNNGF-49135]
- In case the modem access to a provider becomes invalid due to a misconfigured SIM-PIN, the credentials can now be reset using a command-line tool. [BNNGF-52796]
- DHCPv6 links use a provider's DNS only if configured. [BNNGF-54807]
- Information for network resources is now processed case-insensitive. [BNNGF-54972]
- The firewall sends ARP requests for configured networks as expected. [BNNGF-56888]
- In case of an HA failover with IPv6 addresses, the MAC addresses are now advertised as expected. [BNNGF-58404]
- URL categories are now written into the firewall activity log as expected. [BNNGF-61101]
- LOUT traffic is now terminated as expected when the respective session is killed via the GUI. [BNNGF-61204]
- Authentication key input now allows you to enter up to 16 characters. [BNNGF-61830]
- The user interface in Firewall Admin now works as expected if weblog streaming in **CONFIGURATION > Configuration Tree > Syslog Streaming** is deactivated. [BNNGF-61941]
- The method for downloading lists of Azure IPs has been improved. [BNNGF-63160]
- If search string logging is enabled in **CONFIGURATION > Configuration Tree > General Firewall Configuration > Global Search Engine** (in advanced configuration mode), detected search strings are now logged. [BNNGF-63286]
- Clicking **Notification Test** in **Administrative Settings > Notifications** now creates and sends test notifications as expected. [BNNGF-63336]
- Several visualization issues for the **SD-WAN Monitor** and the **DASHBOARD** have been fixed.

[BNNGF-63455]
- The firewall no longer causes memory leaks in certain situations. [BNNGF-63689]
- The firewall no longer crashes in certain situations. [BNNGF-63905]
- If TCP window scaling is disabled on an HTTP server, the firewall now correctly processes traffic if inbound synflood protection is enabled. [BNNGF-63936]
- IPv6 prefix delegation for DHCP clients now works as expected. [BNNGF-63948]
- The firewall now passes correct information to the **Update** element in **Firewall Admin > DASHBOARD** for displaying the update status. [BNNGF-63949]
- Migrating from the server-service to the assigned services structure (box-server migration) with multiple loopback IPs now works as expected. [BNNGF-63953]
- Syslog streaming over SSL now works as expected. [BNNGF-63977]
- The event for interface mismatch no longer shows incorrect information in its message. [BNNGF-64034]
- SFP modules are now recognized correctly and network activation no longer fails. [BNNGF-64048]
- Slave interfaces spawned by the accelerated network interfaces in Azure VMS now use the naming `mlx<index>` where `index` stands for the number of the interface. [BNNGF-64076]
- Granting shell level access to CC administrators now works as expected. [BNNGF-64102]
- An HA pair of firewalls is now correctly configured with the same network cards. [BNNGF-64257]
- TLSv1.2 is now the default preset protocol used for syslog encryption. [BNNGF-64259]
- Triggering a soft activation no longer disables header reordering on VLAN interfaces. [BNNGF-64265]
- The parameter **Bandwidth** in **CONFIGURATION > Configuration Tree > Virtual Servers > *my virtual server* > Assigned Services > OSPF/RIP/BGP > OSPF/RIP/BGP Settings**, left navigation bar, **Network Interfaces**, window **Interfaces**, section **OSPF Specific Parameters**, now accepts values with up to 10 digits. [BNNGF-64430]
- Migrating an F400B Firewall to any F600D model now works as expected. [BNNGF-64524]
- Firewall tunnels (GRE / IP in IP) are treated as interfaces as well. [BNNGF-64566]
- When connecting with OTP to an HA cluster, the status of the primary and secondary firewall in **CONTROL > Services** is displayed correctly. [BNNGF-64579]
- CC Admin authentication with Yubikey + TACACS now works as expected. [BNNGF-64608]
- Valid pool licenses are no longer removed from managed boxes during a pool license renewal. [BNNGF-65056]
- IP address ranges are now correctly resolved into their geolocation. [BNNGF-65062]
- The host firewall ruleset has been updated to allow BFD ports. [BNNGF-65098]
- The default size for the /root/ partition is now 30 GB. [BNNGF-65153]
- After a box-server migration, previously created auto-policy routes work as expected. [BNNGF-65244]
- Firewalls operating firmware version 7.x will be able to securely stream syslogs to Control Centers updated from 7.2.x to 8.0.x. [BNNGF-65653]

Cloud (general)

- Error messages have been improved to be more human readable. [BNNGF-64050]
- If vWAN is activated, its state is now also part of telemetry information. [BNNGF-64219]

- Soft migration for vWAN3 now works as expected. [BNNGF-64329]

Cloud Azure

- If RCS messages are enabled, the agent for Azure Operations Management Suite (OMS) can now complete its tasks as expected. [BNNGF-63986]
- Azure VPN sites created without active BGP no longer break the deployment. [BNNGF-64061]
- If DHCP is disabled globally, ISP links that have been set as DHCP links are ignored. [BNNGF-64605]
- Configured ADSL links are now supported as VPN site links. [BNNGF-64983]
- Dead Peer Detection (DPD) no longer causes failures in certain situations. [BNNGF-65035]

Control Center

- Box-server to service migration now migrates GTI tunnel configurations. [BNNGF-63899]
- The command-line tool cctool now supports creating PAR files for CC-managed boxes and HA boxes. [BNNGF-63904]
- It is now possible to deploy a pair of box-server HA boxes via zero-touch. [BNNGF-64591]

Firewall

- URL detection in HTML mails has been improved. [BNNGF-63255]
- Some enhancements for the S7+ protocol have been made. [BNNGF-63415]
- Search engines can now be selectively disabled for SafeSearch in **CONFIGURATION > Configuration Tree > Infrastructure Services > General Firewall Configuration > Global Search Engine**. [BNNGF-63825]
- The factory default ruleset of the CGF has been updated to reflect the latest executables used by the Network Access Client. [BNNGF-64511]
- The Application "Mendeley" is now categorized as a Learning Management System. [BNNGF-65205]

HTTP Proxy

- Several CVEs have been fixed for the HTTP proxy. [BNNGF-63633]
- The HTTP proxy no longer fails combined with certificate chains. [BNNGF-63854]
- When using the reverse proxy, SLL/TLS for backends now works as expected. [BNNGF-63861]

REST

- New REST plugins for authentication requests are now available. [BNNGF-63150]

VPN

- Up- and life-times are now correctly displayed for VPN tunnels. [BNNGF-54549]
- VPN transports working in 'routing' mode now forward traffic as expected. [BNNGF-61912]
- **VPN Name** and **Used by** are now considered for filtering in **FIREWALL > Live** and **FIREWALL > History** view. [BNNGF-63144]

- IKE reauthentication has been disabled to prevent the firewall from losing tunnels to Azure. [BNNGF-63701]
- IKEv2 VPN client-to-site connections now support split tunneling. [BNNGF-64436]
- IKEv1 AWS tunnels now rekey as expected. [BNNGF-64498]
- Tunnels shown on the SD-WAN dashboard for administrators now comply with their corresponding administration scope. [BNNGF-64600]
- Creating a certificate on the Web UI in the Certificate Manager no longer produces a corrupt key. [BNNGF-64638]

WEB UI

- A check box for header reordering has been added to the Web UI. [BNNGF-64055]

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]
- **Barracuda Firewall Admin** – Firewall Admin does not work with OTP or two-factor authentication. [BNNGF-59761]
- The learn-only mode for OSPF is not working as expected. [BNNGF-65299]
- "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.
- **VPN** – Remembered credentials may not be retrieved properly from Windows Credential Vault if using Direct Access. [BNNGF-64306]
- **VPN** – The DHCP relay setup via an S2S tunnel is currently not working. [BNNGF-65811]
  As a workaround, run the CLI command: `acpfctrl perf disable reducememcpyopt`. The command's effect is non-persistent. If you must restart your firewall often, embed the command into a server start-script.
- **Firewall Admin** – The list box **Explicit Transport Listening IP** in **CONFIGURATION > Configuration Tree > Box > Virtual Servers > My Server > Assigned Services > VPN > VPN GTI Settings** does not accept input of DNS names. [BNNGF-67163]
- If an install stick was created with 8.0.3 and an F93/F193 firewall is deployed, the LEDs will not work. [BNNGF-68591]

Figures

1. assigned_services_tree.png
2. header_reordering_off.png
3. header_reordering_on.png