# 8.0.2 Release Notes

https://campus.barracuda.com/doc/90445593/

If you are using...

- xDSL links on a VLAN interface OR
- the DHCP-server service 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 8.0.2.

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.

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 8.0.2

#### 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.

With firmware version 8.0.2, 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.

IMPORTANT NOTE

If you are using the SCA Editor for your SCs and also operate VPN tunnels via GTI, DO NOT MIGRATE the server-service node to the new Assigned Services node!

This is because of a known issue that will be fixed in the next upcoming firmware release.

For more information on how to migrate the server-service node to the new Assigned Services node, see Migrating the Server Node to the Assigned Services Node (optional).

Version 8.0.2 is generally a maintenance release.

For customers running firmware 8.0.1, 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.

The section for Improvements Included in Version 8.0.2 applies to all.

**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

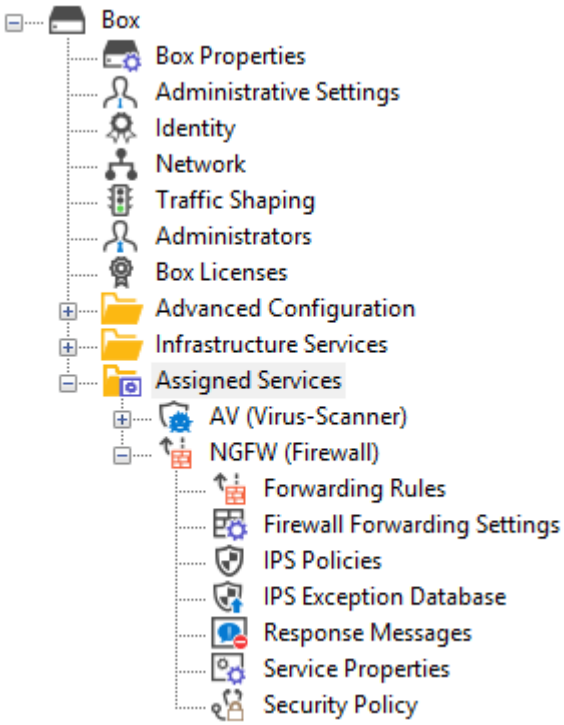
The DNS service has been refactored and now offers a new user interface. This user interface is now tightly incorporated into new features that extend the DNS by various advanced options. The feature set of the new DNS service now includes:

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

For more information, see DNS. Also, see the paragraph **DNS** in the section **Improvements Included in Version 8.0.2** 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 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 8.0.2

#### Barracuda Firewall Admin

- When launching Firewall Admin, the application now has preset filters in **FIREWALL > Live / History / Threat Scan**. [BNNGF-58448]
- If the maximum limit for NAT table entries is reached, a warning is now displayed. [BNNGF-60345]
- In the Control Center, in **CONFIGURATION > Configuration Tree**, in the **Boxes** tab of the **Quick File Access** area, it is now possible to bulk enable/disable boxes for editing. [BNNGF-60532]
- On an HA pair of firewalls, the state of the secondary firewall is now displayed correctly in **Firewall Admin > CONTROL**. [BNNGF-61773]
- The migration wizard now also supports single boxes. [BNNGF-62714]
- The geo-ip field in **Box > Properties > Geo Location** can now be manually overridden to store locations for SD-WAN and Firewall Insights. [BNNGF-62911]

#### Barracuda Firewall Admin Rel. 802-104, Feb. 2020

- When switching to the view **CC > CONTROL > Remote Execution**, the last selection in the list view is now correctly restored. [BNNGF-55593]
- The default Dashboard and its elements are now displayed according to a new default layout on managed and unmanaged boxes. [BNNGF-55906; BNNGF-64086]
- When switching to the view **CC > File Updates**, the list restores the last selected type of download. [BNNGF-56639]
- Firewall Admin no longer crashes in certain situations. [BNNGF-58375; BNNGF-59609; BNNGF-63871; BNNGF-64131; BNNGF-64414; BNNGF-64429]
- 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 view for the box listing next to the CC configuration tree has been improved. [BNNGF-61898; BNNGF-64407]
- Several visualization issues for the **SD-WAN Monitor** and the **DASHBOARD** have been fixed. [BNNGF-62215; BNNGF-63455; BNNGF-63677; BNNGF-63762]
- It is now possible to import certificate chains for the **CC Syslog Service**. [BNNGF-62424]
- Invalid characters are purged in the data pasted into configuration fields. [BNNGF-62438; BNNGF-63967]
- The icon for a firewall now correctly displays the status after a patch installation. [BNNGF-63636]
- In **Firewall > Live**, the list of filters now displays **Source** and **Destination** as expected. [BNNGF-63660]
- Session related OTP issues no longer occur in certain situations. [BNNGF-63771; BNNGF-63775]
- When using GTI in clusters, Firewall Admin now supports feature level 8.0 and 8.1 for VPN servers. [BNNGF-63779]

- Selecting an IKEv2 VPN tunnel in **VPN > Status** with activated **Access Cache** and **Drop Cache** areas now correctly displays its tunnel details. [BNNGF-63826]
- AV pattern updates can now be enabled/disabled in the **Subscription Status** element on the DASHBOARD. [BNNGF-63886]
- 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]
- List entries for the migration of the Server-Service to the new Assigned-Services architecture have been improved. [BNNGF-64010; BNNGF-64119]
- The configuration for **VPN Settings** is now working as expected. [BNNGF-64071]
- 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]
- The option for **VPN File Download** is no longer supported and has been removed from the VPN overview window. [BNNGF-64198]
- For the DNS service it is now possible to create DKIM TXT records with a '_' character in the records name/owner. [BNNGF-64513]

#### Barracuda OS

- When blocking IPv6 packets for certain Extension Headers for an IPv6 Access Rule in **CONFIGURATION > Configuration Tree > Assigned Services > Firewall > Forwarding Rules > Access Rule Editor > (View) IPv6 Extension Header**, the name of the blocked type will be displayed in the **Firewall History**. [BNNGF-59834]
- High traffic load over a bond interface is now distributed as expected. [BNNGF-59916]
- Validation of certificates no longer causes memory issues in case OCSP checks fail. [BNNGF-59922]
- The edit fields for configuring the **Geo Location** have been updated both for stand-alone boxes in **CONFIGURATION > Configuration Tree > Box > Properties > Geo Location** and on the Control Center in **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > your range > your cluster > Boxes > your box > Properties > Geo Location**. [BNNGF-60433]
- Available Server IPs are now correctly displayed in **Create Service Wizard**. [BNNGF-60924]
- Local administrators can no longer log on after their accounts have been deleted. [BNNGF-60995]
- After a fresh installation via a USB stick, the status LEDs on the firewall now show the correct colors, and time-jumps of the clock no longer occur. [BNNGF-61163]
- DHCP on a VLAN now works as expected. [BNNGF-61859]
- In **CONFIGURATION > Configuration Tree > Network > IP Configuration**, in the window **Shared Networks and IPs**, reachable IPs are now correctly propagated to automatically create default routes. [BNNGF-62126]
- For DNS, a certain IP address may be assigned only to a single listener. [BNNGF-62189]
- The default bootload delay has been set to 0. [BNNGF-62442]
- Layer 2 monitoring now works as expected. [BNNGF-62599]
- During a nested SSH connection from Firewall Admin via a Control Center to a managed box, file uploads from Firewall Admin will be done to the first SSH-connected device in the SSH chain. [BNNGF-62605]

**Cloud**

- Network activations no longer fail on Azure Accelerated Network interfaces when switching from dynamic to static networking or when setting up an HA pair using create-dha. [BNNGF-62926]

**Control Center**

- VPN Access Control service now works correctly when migrating clusters from 7.0 to 7.2. [BNNGF-59208]
- The Firmware Update page no longer shows unallowed appliances from different ranges. [BNNGF-59757]
- It is now possible to add a custom script to the configuration of a Secure Connector, which will be executed at network activation. [BNNGF-61803]
- When new firewalls are created in a Control Center, the default firewall ruleset is no longer broken. [BNNGF-61852]
- The CC syslog now handles certificate chains. [BNNGF-61963]
- **Send Changes** no longer fails for 32-bit appliances in 7.x clusters on 8.0.x CCs for the boxnet node. [BNNGF-63145]

**DNS**

- If the DNS service is active and when migrating from 7.2 to 8.0.2, all migrated IPs will be assigned to the **ALL** listener category. [BNNGF-61817]
- Importing a 7.2 PAR file on an 8.x firmware based firewall no longer destroys the DNS configuration. [BNNGF-61953]

**Firewall**

- When QoS is enabled, GRE tunnels now work as expected. [BNNGF-54027]
- HTTP requests are no longer blocked by the URL Filter unless the session counter does not exceed the configured limit. [BNNGF-61778]
- Serving DHCP leases over a bridge interface now works as expected. [BNNGF-61809]
- When migrating from 7.x to 8.0.2 or when deploying a new 8.0.2 firewall, the routing tables are now configured correctly if multiple default routes with at least one DHCP interface are present. [BNNGF-61828]

**HTTP Proxy**

- The access denied error message is now correctly displayed every time the block page is reloaded. [BNNGF-61188]
- The proxy cache is now created correctly and no longer causes failures if a configuration is reloaded by the firewall. [BNNGF-61836]
- The HTTP proxy detects the eicar virus as expected. [BNNGF-62443]

**Virus Scanner**

- Scanning antivirus content now honors all entries in the HTTP exception list. [BNNGF-62136]

- ATP for SMTP with scan-first now delivers mail to the correct port using PAT. [BNNGF-62252]

**VPN**

- When selecting **Preauthentication Scheme** under **Group VPN Settings**, the feature now works as expected. [BNNGF-57963]
- DYNMESH is now established correctly on multiple transports. [BNNGF-59773]
- VPN connection attempts no longer crash when entering very long passwords. [BNNGF-61951]
- It is now possible to set an interface name in the local IP field for an IKEv2 VPN tunnel. [BNNGF-62115]
- Client-to-Site connections no longer crash in certain situations. [BNNGF-62918]
- The VPN service no longer produces memory leaks in certain situations. [BNNGF-62923]
- Disabling and re-enabling a VPN TINA tunnel no longer causes a routing problem. [BNNGF-62958]
- The firewall now sends the status of all transports in the logstream to Firewall Insights. [BNNGF-63312]

## Known Issues

- Currently, no RSC 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]
- "vmxnet" driver version 2 is not supported any longer. 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.
- GTI and the SCA Editor are not handled correctly by the migration wizard to 2-layer architecture. [BNNGF-63899]
- **VPN** – On clients using NAC to connect to a VPN, direct access does not pick up stored credentials from the Windows credential vault. [BNNGF-64306]

## Figures

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