8.0.6 Release Notes

https://campus.barracuda.com/doc/96768149/

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.

- **23.3.2022 – Hotfix 1076** - DNS - Bind update to 9.16.27 has been released. For more information, see https://dlportal.barracudanetworks.com/#/packages/5430/dns-1076-8.0.6-147541920.tgz.
- **9.2.2023 – Hotfix 1090** - OpenSSL - For more information, see https://dlportal.barracudanetworks.com/#/packages/5575/openssl-1090-8.0.6-175839239.tgz.

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, it is safe to install update 8.0.6.

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 will no longer work as expected.

Before installing the new firmware version:

Do not manually reboot your system at any time while the update is in process unless otherwise instructed by Barracuda Networks Technical Support. Upgrading can take up to 60 minutes. For assistance contact Barracuda Networks Technical Support.

Legacy Services Announcement

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

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

Legacy Items Announcement

The following items will no longer be available:

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

Version 8.0.6 is a maintenance release.

For customers running firmware 8.0.5, a new feature has been added. See the section *What's new in version 8.0.6* below. Further improvements - besides resolved bugs - can be found in the section *Improvements Included in Version 8.0.6* below.

For customers running firmware 7.x, see the following list of features that also apply to the new firmware 8.0.2/8.0.3/8.0.4/8.0.5/8.0.6.

The section for *Improvements Included in Version 8.0.6* applies to all.

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

This applies only to firewalls that are currently operating firmware 8.0.1 and upgrading to firmware 8.0.2/8.0.3/8.0.4/8.0.5/8.0.6.

With firmware version 8.0.6, you have the option to migrate the former 3-layer server-service architecture to the new 2-layer Assigned Services architecture. Although 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.

Control Centers Operating in a Parent-to-Child Relation

In the past, the configuration of Control Centers operating in a parent-to-child relation required modifying the host firewall rule set of the firewall. As of release 8.0.6, this is no longer necessary. Firmware release 8.0.6 now covers all necessary steps that require the user to perform a minimum of configuration steps to set up split Control Centers without having to modify the host firewall rule set.

In case you are already running split Control Centers, some steps must be performed before upgrading to firmware 8.0.6.

For more information, see 8.0.6 Migration Notes and its subordinated migration articles that relate to your running firmware versions, specifically the paragraph *Important Notes Before Migrating*.

Custom Box Descriptors

When managing a large number of firewalls in the Control Center, the naming scheme of the CloudGen Firewall proved to be insufficient. The Control Center now has an additional functionality to extend the standard naming scheme for CloudGen Firewalls. This functionality includes the option to enter additional fields for a more distinctive naming scheme of managed CloudGen Firewalls.

For more information, see How to Configure Custom Box Descriptors and Filter Managed Firewalls in Different Data Views.

Disk Encryption

To achieve higher protection for your data on your firewall, you can encrypt the hard disk. To do so, you must set a parameter in the corresponding configuration window of **NGInstall** and then re-install your firewall from scratch.

For more information, see How to Deploy a CloudGen Firewall Vx using Firewall Install on a VMware Hypervisor.

To download the newest version of NGInstall that includes the updates, go to https://dlportal.barracudanetworks.com/#/packages/5238/NGInstall_8.0.5-10.exe.

KTINA FIPS Crypto Module

FIPS 140-2 revalidation with Barracuda KTINA FIPS Crypto Module is in progress.

For more information, see https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List.

Along with the Barracuda Cryptographic Software Module, the VPN server will be FIPS 140-2 compliant again.

For more information, see https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/2458.

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 multipath routing is used to route the traffic, and the configuration of BGP multipath routing is likewise set up automatically when using automated connectivity. The firewall learns path information as set by the Virtual WAN hub, which results in better path affinity. In addition, BGP-based load balancing and automatic path failover are used for the best connection results.

For more information, see Azure Virtual WAN.

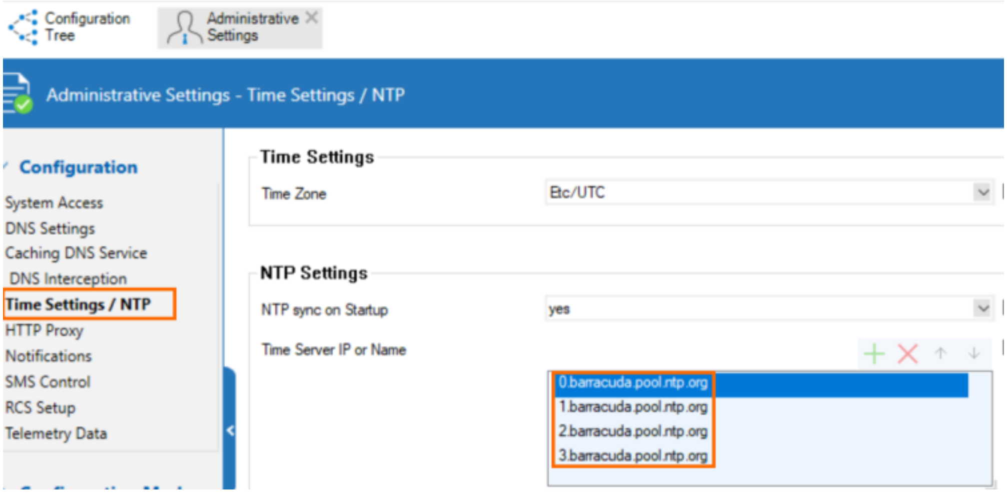
Multi-Factor Authentication with Time-Based One-Time Password (TOTP)

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

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

NTP Servers for the Barracuda Zones

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



Time Settings

Time Zone: Etc/UTC

NTP Settings

NTP sync on Startup: yes

Time Server IP or Name:
0.barracuda.pool.ntp.org
1.barracuda.pool.ntp.org
2.barracuda.pool.ntp.org
3.barracuda.pool.ntp.org

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:

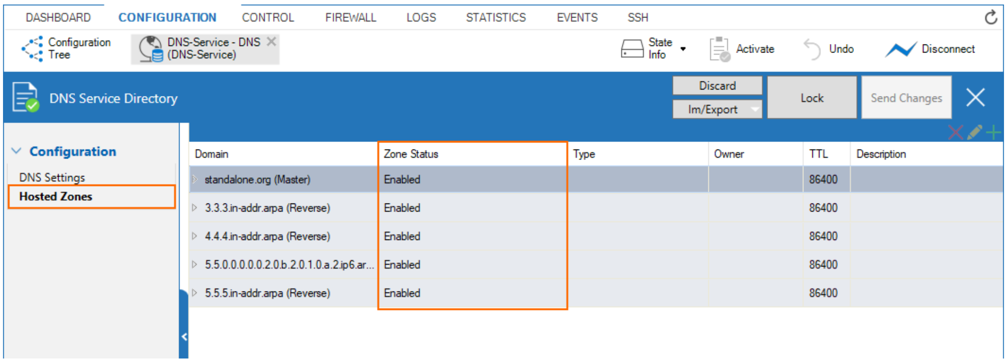
- Stand-alone and distributed DNS service
- Primary / Secondary / Forward DNS zones
- Split DNS
- Health probing

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 8.0.6" below.

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



Domain	Zone Status	Type	Owner	TTL	Description
standalone.org (Master)	Enabled			86400	
3.3.3.in-addr.arpa (Reverse)	Enabled			86400	
4.4.4.in-addr.arpa (Reverse)	Enabled			86400	
5.5.0.0.0.0.0.2.0.b.2.0.1.0.a.2.ip6.ar...	Enabled			86400	
5.5.5.in-addr.arpa (Reverse)	Enabled			86400	

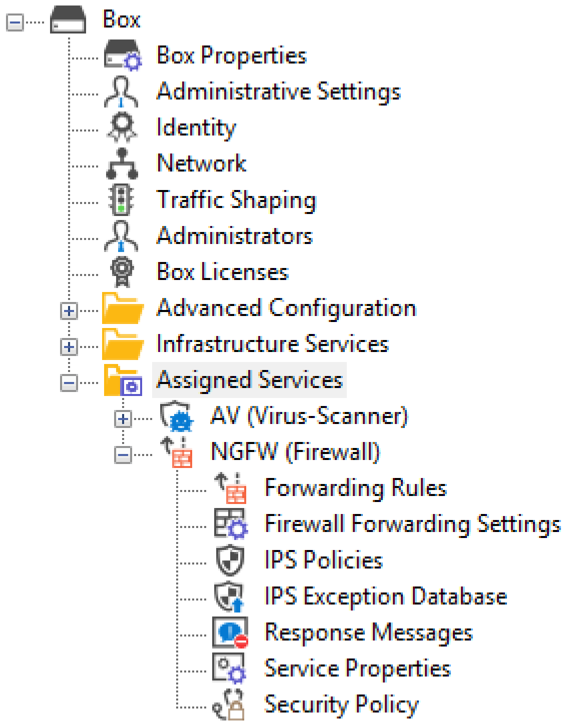
Because this option is available only for stand-alone firewalls and Control Centers with a firmware version 8.0.4 or higher, this option will also show up in a mixed environment of 8.0.4 and 8.0.3 appliances, but the option will not work on a device running firmware version 8.0.3.

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

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

Replacement of Virtual Servers by a New 2-Layer Architecture

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



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

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

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

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

REST API Extensions

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

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

SNMP

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

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

SSL VPN

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

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

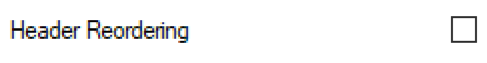
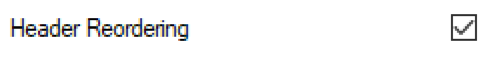
For more information, see SSL VPN.

Usage of DHCP on a VLAN Interface

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

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

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

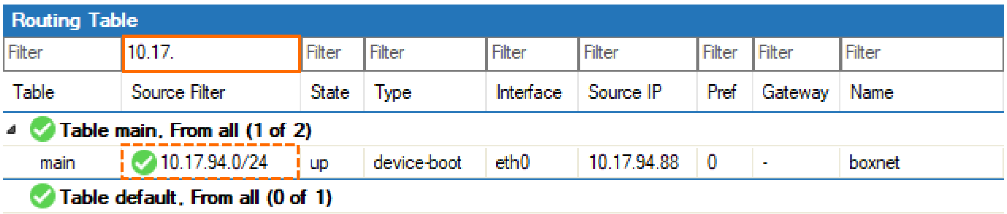
User Action	User Interface Item	Description
Default state: header reordering is off.	 Header Reordering ☐	No header reordering is done for DHCP on a VLAN interface.
Select the check box in case the assignment of an IP address from a DHCP server fails.	 Header Reordering ☑	Header reordering for DHCP on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

VPN IPv6 Payloads

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

What's New in Version 8.0.6

A filter and search function has been added to the list view for routing tables in **CONTROL > Network**.



Routing Table

Table	Source Filter	State	Type	Interface	Source IP	Pref	Gateway	Name
Filter	10.17.	Filter	Filter	Filter	Filter	Filter	Filter	Filter
✓ Table main, From all (1 of 2)								
main	✓ 10.17.94.0/24	up	device-boot	eth0	10.17.94.88	0	-	boxnet
✓ Table default, From all (0 of 1)								

See the next section for further improvements included in version 8.0.6.

Improvements Included in Version 8.0.6

Appliances

- The LCD now works as expected on the F1000B. [BNNGF-83659]

Authentication

- SAML authentication metadata is now generated correctly for a managed box. [BNNGF-76521]
- RADIUS no longer gets spammed with authentication requests when C2S/NAC has UDP chosen as transport. [BNNGF-80365]

Barracuda Firewall Admin

- IP addresses can now be filtered for the display of routing tables at **CONTROL > Network**, table **Routing Tables**. [BNNGF-55577]
- Creating certificates in Firewall Admin now forces the key length to be a multiple of 8 characters and ensures the creation process to succeed. [BNNGF-65515]
- The UI option for importing a certificate has been consolidated and is now displayed with the

text **Import Certificate from File...** at its current places in the UI. [BNNGF-76877]
- On a Control Center it is possible to enter pattern-based entries for cluster links in **ADMINS > my admin > Administrator Scopes > Global linked >Administrative Scope > Links**. [BNNGF-76899]
- Creating certificates with PCs located in the US no longer causes issues. [BNNGF-76958]
- When creating a certificate, it is now possible to enter an asterisk character (*) into the CF field. [BNNGF-78483]
- Pasting data from the clipboard into txt record now works as expected. [BNNGF-78797]
- When switching from the **FIREWALL > Forwarding Rules** tab to the **Firewall > local** tab, the **Refresh** button no longer vanishes. [BNNGF-79937]

Barracuda OS

- The default behavior for WWAN-capable CGF boxes with an attached M40/M41 modem is now set to perform SIM autoconfiguration. [BNNGF-69443]
- Connecting to a box via GUI no longer fails in certain situations. [BNNGF-70271]
- Firewalls running in an HA cluster now also support pool licenses even if there is only one license in the pool available. [BNNGF-70645]
- Importing a PEM file now writes the certificate chain correctly to the related configuration file. [BNNGF-70649]
- The boot status LED now works as expected. [BNNGF-71629]
- The Control Center no longer crashes in certain situations after reporting the error message "skb_warn_bad_offload". [BNNGF-73804]
- Default routes are now provided to DHCP clients as expected. [BNNGF-75691]
- Event notification now works as expected. [BNNGF-76327]
- Filebeat clients now report through the management tunnel as expected. [BNNGF-78034]
- Two boxes as part of an HA pair no longer crash simultaneously in certain situations. [BNNGF-78380]
- The `cstatd` log files no longer get flooded and the `phion0` partition no longer runs out of space. [BNNGF-78865]
- Outdated **Let's Encrypt** certificates no longer cause problems in certain situations. [BNNGF-79158]
- After moving the FTP plugin into the kernel space, a pair of HA firewalls no longer crashes in certain situations. [BNNGF-80493]
- The firewall no longer freezes in certain situations. [BNNGF-80576]

Control Center

- Discontinued/outdated licenses are ignored when a valid license subscription is activated in the Control Center. [BNNGF-71216]
- Pool licenses can now also be removed during an update of other pool licenses. [BNNGF-72989]
- If the auto-reassignment of an updated pool license to the managed firewalls fails at the first attempt, it will be retried. [BNNGF-73301]
- The CC clone wizard now adds the correct name to the new target box. [BNNGF-76336]

- On a Control Center, it is possible to enter pattern-based entries for cluster links in **ADMINS > my admin > Administrator Scopes > Global linked > Administrative Scope > Links**. [BNNGF-76870]
- Box descriptor fields now accept strings with a maximum length of 100 characters. [BNNGF-78146]
- Repository nodes can now contain the '-' character. [BNNGF-78196]
- A bug has been fixed where locking the FSC editor in **Cluster Settings** caused the FSC communication daemon to crash. [BNNGF-79090]

DHCP

- After a firmware update, DHCP now starts up as expected. [BNNGF-78040]

DNS

- The option to enter the **forward source-ip** for outgoing DNS queries has been added to the DNS settings. [BNNGF-71995]
- The BIND system has been updated to version 9.16.x. [BNNGF-74788]

Firewall

- The categorization of URLs for URL filters now works as expected. [BNNGF-78381]

HTTP Proxy

- URL filter categories now work as expected in the settings for the HTTP proxy access control. See also the red note in the article [https://campus.barracuda.com/product/cloudgenfirewall/doc/96768141/migration-from-8-0-1-8-0-2-8-0-3-8-0-4-8-0-5-to-8-0-6/] . [BNNGF-74895]

NGInstall

- NGInstall now provides the option to activate disk encryption. [BNNGF-76887]

REST

- The REST API call for determining the usage of memory now considers disk space usage in a dedicated **diskState** field. [BNNGF-76335]

SSL-VPN

- RDP connections no longer crash under high loads. [BNNGS-3761]
- OpenSSL no longer experiences infinite loops when parsing certificates. [BNNGF-83054]
- HTTP connections are cleaned up as expected. [BNNGS-3894]
- SSL VPN now provides information for "VPN profile OTP" to CudaLaunch. [BNNGS-3896]

- Clean-ups of VPN SSL sessions now work as expected and Firewall Admin no longer displays empty sessions in the **VPN** tab under **Client-to-Site**. [BNNGS-3897]
- Uncompleted connection attempts to SSL VPN no longer occur in certain situations. [BNNGS-3913]
- Web apps now open as expected for SSL VPN after an update to firmware version 8.2.1. [BNNGS-3917]
- If a tunnel's forwarding partner temporarily goes down, traffic is no longer blocked. [BNNGS-3920]
- Clean-up of orphaned sessions no longer causes tunneled web apps to drop. [BNNGS-3925]
- Terminated session sockets no longer are re-activated in certain situations. [BNNGS-3926]

VPN

- The VPN status page now correctly displays IKEv2 tunnels. [BNNGF-56468]
- VPN client-to-site connections no longer experience dropouts when an HA pair of boxes performs a failover. [BNNGF-74302]
- Logging enhancements have been made for the IKEv1/v2 log. [BNNGF-75690]
- Using MSAD + RSAACE for personal licenses no longer causes authentication errors. [BNNGF-76332]
- A VPN tunnel with DNS now starts as expected. [BNNGF-79154]
- IKEv2 memory leaks no longer occur when establishing VPN tunnels/transports. [BNNGF-81077]

Known Issues

- Currently, no RCS information is logged for **Named Networks**. [BNNGF-47097]
- The learn-only mode for OSPF is not working as expected. [BNNGF-65299]
- **Barracuda Firewall Admin** – FW Admin 8.x fails to configure DNS 7.x correctly. [BNNGF-77636]

Uncompleted connection attempts to SSL VPN no longer occur in certain situations. [BNNGS-3913]

Figures