8.3.0 Release Notes

https://campus.barracuda.com/doc/17169/

Important Announcements and Notes

Read this section before you continue with the Release Notes below.

Outdated technical features are subject to removal to keep the CloudGen Firewall up to date and performing properly. See the following two paragraphs for the features that will be removed in this release and the features that are subject to removal in upcoming releases.

Certain features will be removed completely because they have become technically obsolete; other features have become outdated and will be replaced by improved technology.

Features No Longer Supported as of the 8.3.0 Release

- **Generic Forwarder**
  As of 8.3.0, networks that were entered in **General Firewall Configuration -> Operational -> Generically Forwarded Networks** are no longer supported and will be removed. Networks that are configured in this list will no longer be forwarded by the firewall after updating to release 8.3.0. You must configure a forwarding firewall service with corresponding rules to have this functionality.
- **Protocol 254/FW compression**
  Firewall-to-Firewall compression has been discontinued and is no longer configurable. Traffic that was previously configured to use FW-2-FW compression will now be transported uncompressed.

Features that Will Become Obsolete in an Upcoming Release

- FWAudit
- WAN Optimization
- CloudGen Firewall Web UI

Precautionary Security Measures for Control Centers

If you have a Control Center deployed with the CC wizard and there is no ECDSA CC SSH key configured at **CC Identity**, Barracuda Networks recommends the following to avoid possible

security risks:

1. Manually create a new ECDSA "CC SSH key"
2. Create a legacy CC SSH key with more than 512 bits

Known Issue for IPS

If you are using IPS and want to continue to do so in firmware 8.3.0, you must deactivate any traffic for UDP.

This is a known issue and will be solved in the upcoming firmware release 8.3.1.

Release Notes

Before installing the new firmware version:

Do not manually reboot your system at any time during the update unless otherwise instructed by Barracuda Networks Technical Support. Upgrading can take up to 60 minutes.

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 1075** - OPEN SSL - has been released. For more information, see https://dlportal.barracudanetworks.com/#/packages/5432/openssl-1075-8.3.0-147513915.tgz.
- **23.3.2022 – Hotfix 1078** - DNS bind update to 9.16.27 - has been released. For more information, see https://dlportal.barracudanetworks.com/#/packages/5429/dns-1078-8.3.0-147541960.tgz.
- **29.5.2024 – Hotfix 1116** - Virus scanner engine update. This hotfix updates the virus scanner engine and fixes a license expiration issue.
  Note: After installing the hotfix, you can only update from 8.3.0 to 9.0.2!
  For more information, see https://dlportal.barracudanetworks.com/#/packages/5848/virscan-1116-8.3.2-216814708.tgz
- **8.7.2024 – Hotfix 1122** - OpenSSH. The hotfixes fix the CVE-2024-6387 "regreSSHion" vulnerability. For more information, see

https://dlportal.barracudanetworks.com/#/packages/5918/openssh-1122-8.3.3-220099653.tgz.

All NAC VPN improvements/features require the latest Barracuda Network Access Client version 5.3.x for Windows. For more information, see Release Notes - Barracuda NAC/VPN Client 5.3 for Windows.

Devices No Longer Supported

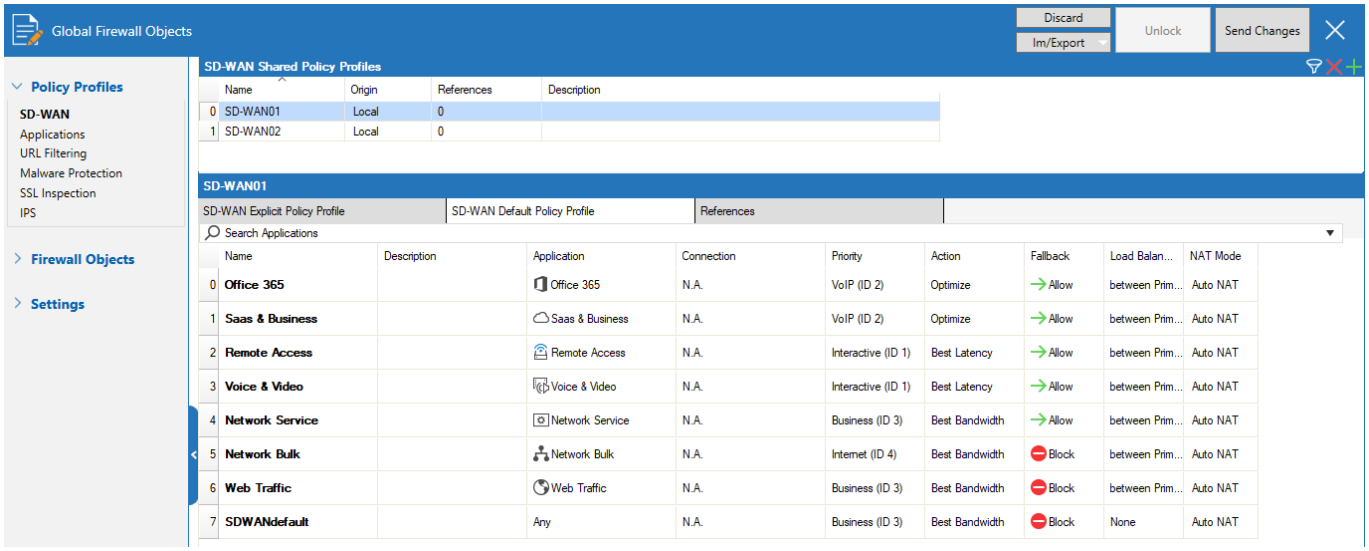
The following devices have reached EoL status:

Device Type	Model	EoL Date
CloudGen Firewall	F800 Rev. B	2022-03-01
CloudGen Firewall	F900 Rev. A	2021-11-31
Control Center	C400	2022-02-28
Control Center	C610	2022-02-28
Modem	M10 (3G/UMTS)	2019-03-31
Modem	M11 (3G UMTS)	2021-09-30

What's New in Version 8.3.0

CGF Policy Profiles

On Barracuda CloudGen Firewall version 8.3.0, a new feature has been implemented that allows central management of SD-WAN policies as well as policies for handling different network scenarios and applications. Policy profiles are predefined rules that can be applied to access rules on Control Center-managed or stand-alone firewall units. The Barracuda CloudGen Firewall allows administrators to manage, create, and customize general policies on global, range, cluster, or box level that can then be applied to access rules instead of configuring firewall objects. You can customize default profiles by adding or modifying policies, or create new profiles with explicit policies. This new feature is specifically designed to simplify the handling of policies, especially on a global scale. For more information, see Policy Profiles.



The Barracuda CloudGen Firewall provides the following policies:

SD-WAN Policies

SD-WAN provides multipath VPN tunnels across all providers with redundant, reliable, and fail-safe network connections. The Barracuda CloudGen Firewall provides a predefined default configuration of SD-WAN policies that allows you to use the advantages of SD-WAN immediately, without even having to set up your own configuration. For more information, see How to Create SD-WAN Policies.

Application Policies

Application policies allow administrators to block, allow, or customize traffic for detected applications on a global and local level. Create explicit profiles and policies on the Control Center and assign them to access rules on managed firewalls. For more information, see How to Create Application Policies.

URL Filtering Policies

Barracuda Networks provides a large database for URL filtering. The default action of a policy can be either to block all and define exceptions that are allowed, or to allow all and define exceptions that are blocked. You can customize a URL filtering policy profile to match individual requirements, or you can create explicit policies. For more information, see How to Create URL Filtering Policies.

Malware Protection Policies

Malware protection offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Intrusion Prevention System. Scanning is done according to the virus scanner configuration and, if an Advanced Threat Protection (ATP) license is present, also by the ATP engine. For more information, see How to Create Malware Protection Policies.

SSL Inspection Policies

SSL Inspection decrypts inbound and outbound SSL and TLS connections so the Barracuda CloudGen Firewall appliance can allow features, such as Malware Protection and the Intrusion Prevention System (IPS), to scan traffic that would otherwise not be visible to the firewall service. For more information, see How to Create TLS Inspection Policies.

IPS Scanning Policies

The Intrusion Prevention System (IPS) monitors local and forwarding traffic for malicious activities and provides various countermeasures to avert possible network attacks. Create explicit IPS policies to match individual network requirements. For more information, see How to Create IPS Policies.

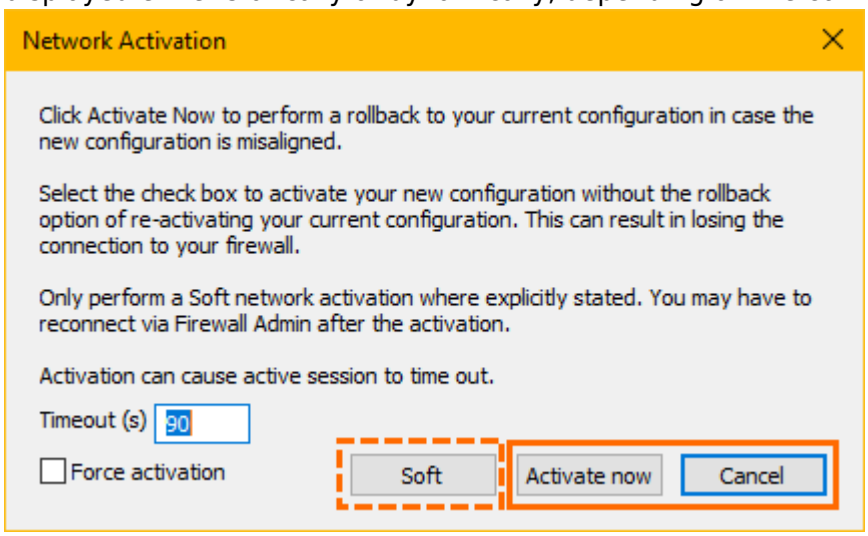
It is recommended to read the Known Issues section at the bottom of this 8.3.0 Release Notes article (**Known Issues related to CGF Policy Profiles**) before using CGF Policy Profiles.

Barracuda Firewall Admin

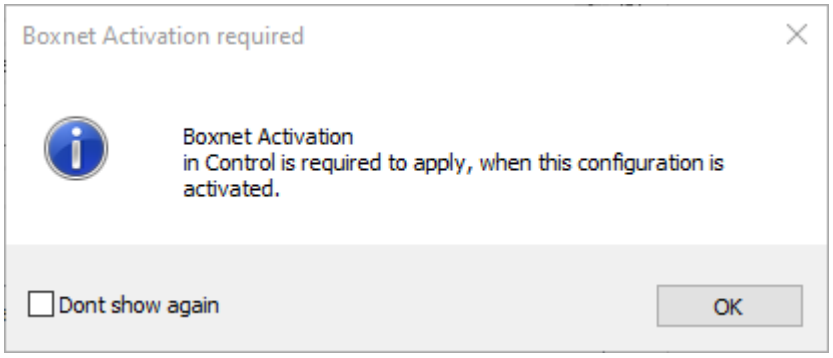
Barracuda Firewall Admin has undergone many changes, including those related to the new implementations listed below. The most salient improvements are as follows:

New Network Activation

Activating the network is now supported by two new dialog windows that include user-interface items displayed either statically or dynamically, depending on the context in which the window is displayed:



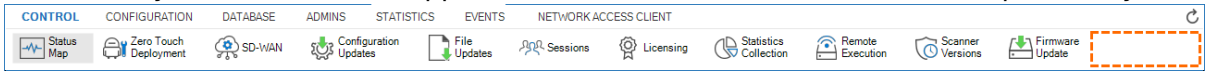
The **Soft** option will be displayed only in certain required contexts.



For more information, see How to Activate Network Changes.

Automated Session Reconnect

In the Control Center, the **Connect** button for reconnecting to a lost session has been removed. Reconnecting is now done permanently in the background. Firewall Admin checks the availability and immediately reconnects to an appliance when it becomes available after a previously lost session.



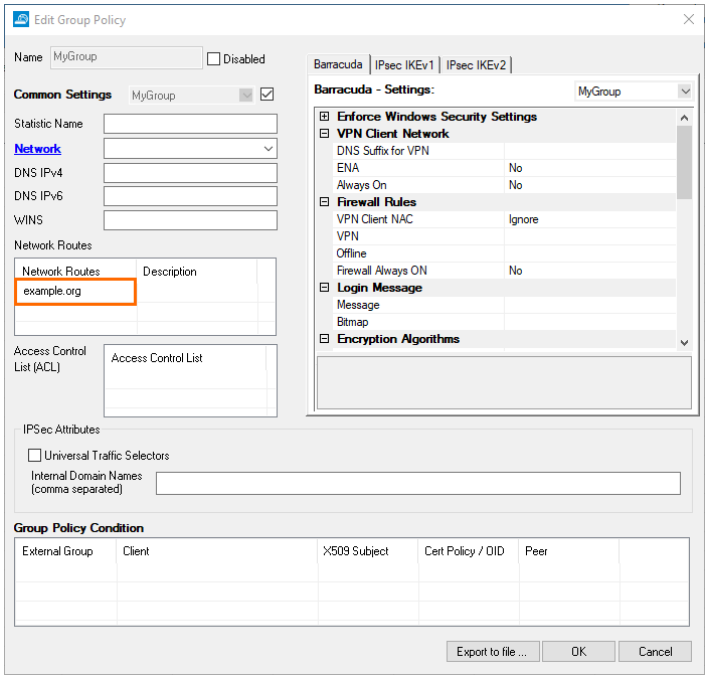
Automated HA Auto Pairing

The HA Auto-Pairing feature has been improved and now supports automated pairing of two Control Centers as well as the automated pairing of managed firewalls.

For more information, see HA Auto-Pairing and How to Enable HA Auto-Pairing for Two Managed Firewalls.

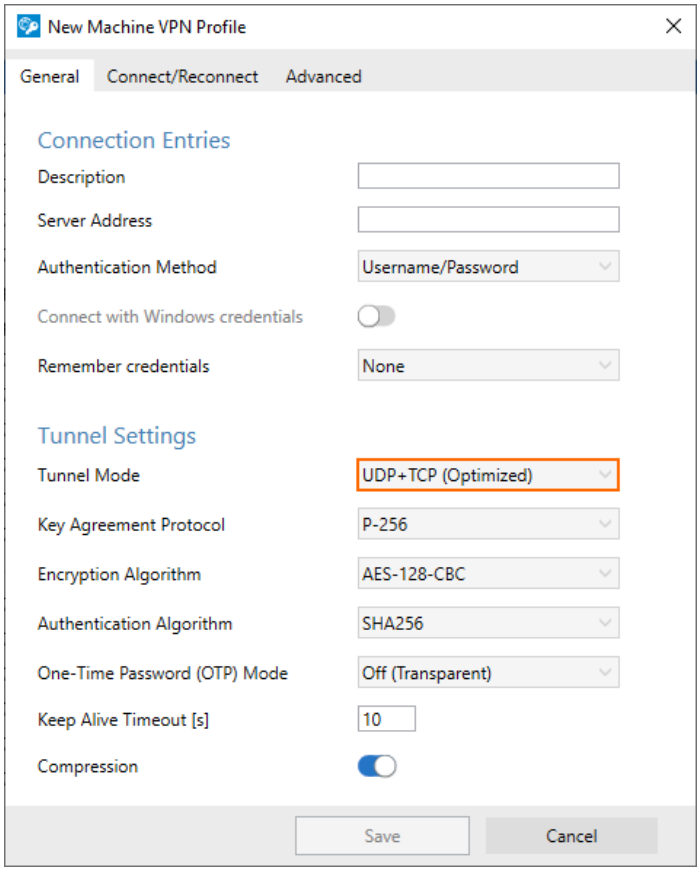
C2S TINA VPN Improvements

Unlike before, when network routes could only be entered as an IP address, they can now be entered as a domain in the group policies. These domains will be resolved by the CloudGen Firewall when a client connection to the firewall is established using Barracuda Network Access Client. In addition, a description can now be added to the domain names. This feature also is available when creating licenses for VPN users or when creating network routes for a template.

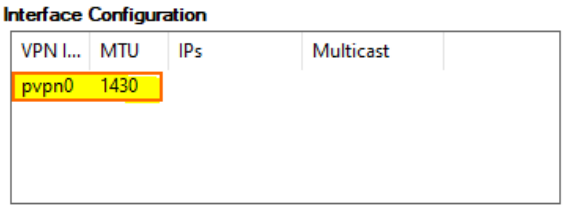


On the NAC Client site, these added domains will be introduced to Windows machines as routes using their related IP addresses. In order to log the DNS calls to resolve the introduced routes, some new logs have been added to the NAC Client.

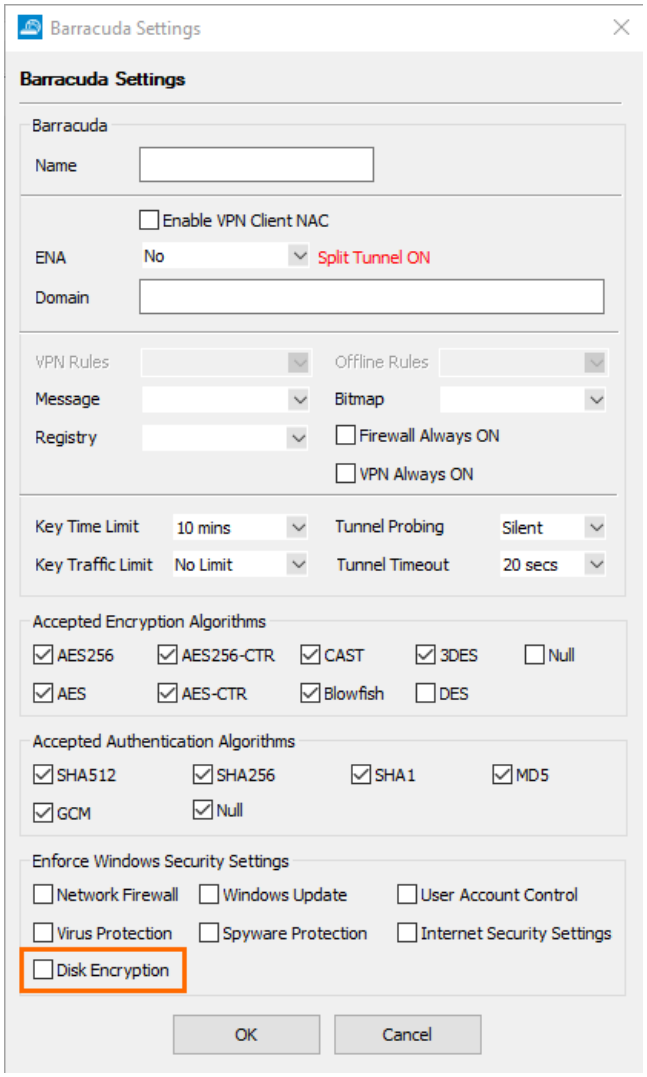
In order to avoid fragmented IP packets, a new transport mode has been added to the **Barracuda Network Access Client > Machine VPN Profile**, tab **General, Tunnel Settings > Tunnel Mode**. This mode starts the authentication and authorization messaging using the TCP protocol and then switches to the UDP protocol for exchanging data streams. For more information, see How to Create VPN Profiles.



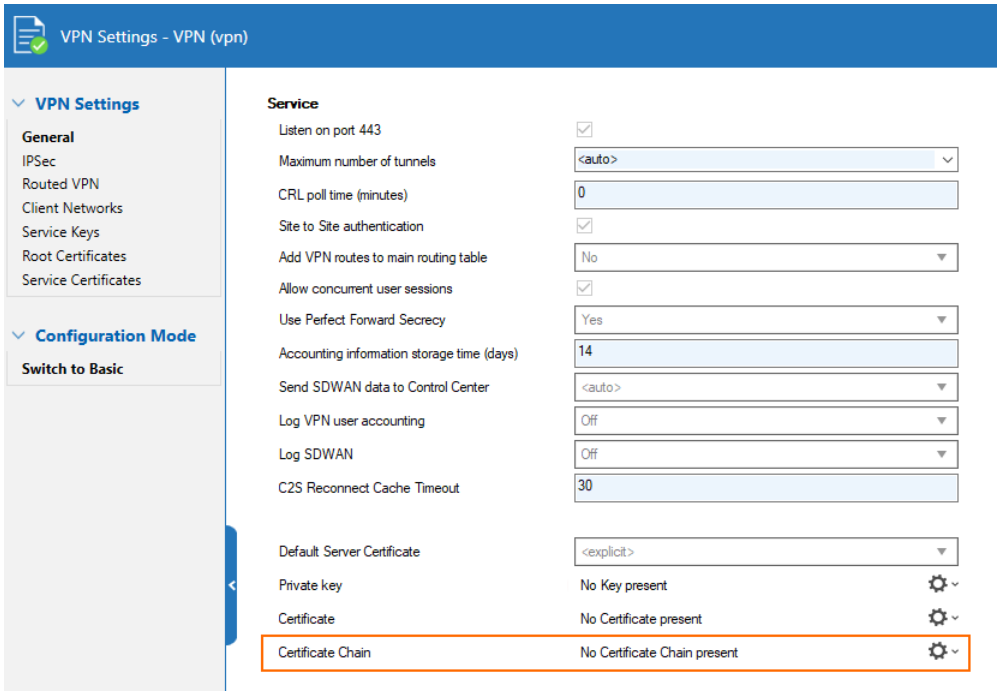
The MTU size can now be managed centrally in the **VPN Settings**. Unlike before, when the MTU size had to be configured individually on each client, clients will now receive the centrally managed MTU value when connecting to the VPN server.



In the Barracuda encryption settings at **CONFIGURATION > Configuration Tree > Box > Assigned Service > VPN Service > Client to Site-VPN**, tab **External CA > Barracuda**, window **Barracuda Settings**, a check box has been added that limits connections to the VPN server only for Windows clients that have disk encryption enabled.

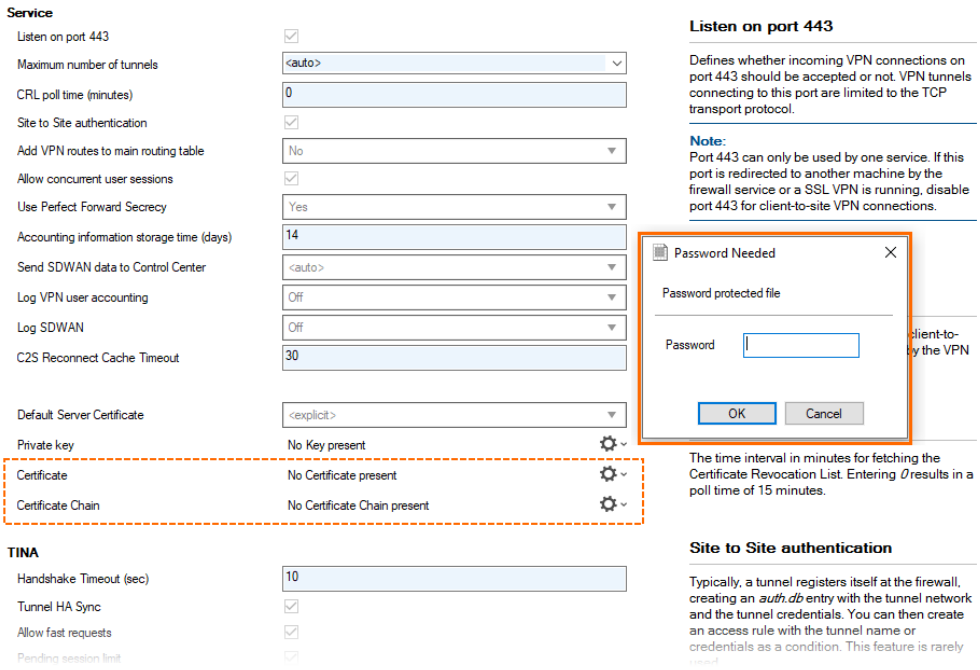


For the VPN server certificate, you can now configure a certificate chain.



For importing a certificate or a certificate chain, a password query has been implemented that displays a dialog window in the following three cases:

1. When the file to be imported is encrypted.
2. When parsing the file is not possible, e.g., due to faulty file content.
3. When the file to be imported has a different file extension, e.g., 'p12', ...



And finally, two new encryption methods, AES-GCM and AES-CTR, can now be configured in the client-

to-site **VPN Settings**.

ConfTemplate Editor

The ConfTemplate Editor has been improved and now also includes an area for displaying help information for ConfUnits. This area is located to the right of the edit area and includes a drop-down list to select the requested information. Example code snippets are also part of the help menu and can be copied and pasted into the editor. For a better overview, disabled instances are now displayed in gray in the ConfTemplate Manager. When editing is completed, clicking the OK button verifies the data in the editor and closes the window if no errors are found.

ConfUnits

ConfUnits have been updated, whereby some ConfUnits have been replaced and other units have been extended. There are two groups of ConfUnits:

- CGF ConfUnits currently include: `cgfCore, cgfDhcpSubnet, cgfDns, cgfFirewall, cgfGtiTunnel, cgfIpv4Route, cgfIpv6AdditionalAddress, cgfIpv6Route, cgfIpv6SharedNetwork, cgfRemoteManagementTunnel, cgfRepositoryLink, cgfSharedNetwork, cgfSiteSpecificObject`.
- FSC ConfUnits currently include: `fscAdvanced, fscConfEntry, fscContainer, fscCore, fscDhcpAdvanced, fscFirewall, fscLan, fscVpn, fscWan, fscWifi, fscWwan`.

IPS

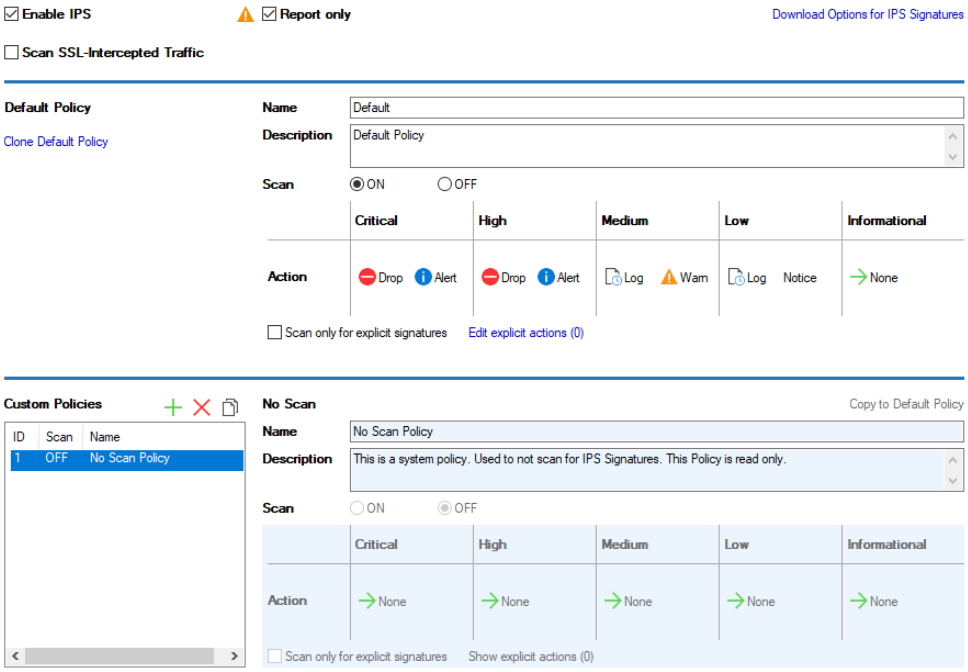
As of firmware 8.3, the CloudGen Firewall includes a new IPS system. The replacement of the former IPS system with the new implementation is fully transparent to the user. Any differences will appear at unobtrusive locations in the user interface when configuring the IPS system.

The new IPS system will operate using new IPS signatures. For this reason, the signature IDs (which are synonymous with the IPS rule sets) of the former IPS system (prior to firmware release 8.3.0) are no longer valid and will be dropped when updating to firmware release 8.3.0. For more information, see also 8.3.0 Migration Notes.

The signature database contains two rule sets:

- Performance Optimized
- Coverage Optimized

These two rule sets are essentially the same; however, the **Performance Optimized** rule set only contains signatures with priority "Critical" and "High".



Details on the operation of the IPS in case problems arise can be inspected in the log file `box_Firewall.log`.

IPv6 Enhancements

In order to fully support firewalling for IPv6 addresses, the range of functions was ported from IPv4 to IPv6 on the CloudGen Firewall. All configuration options - except IPv6 WINS, which has no relevance on IPv6 - are covered in the user interface in Firewall Admin, where applicable, and can be used transparently as with IPv4.

There are certain features that do not yet work for IPv6 and will be addressed in the upcoming firmware release 8.3.1:

- Functionality related to authentication, e.g., user matching in IPv6 rules, IPv6 address/port-based authentication, ATP quarantine.
- ProxyARP-like functionality for IPv6, e.g., neighbor discovery proxy.
- Application-based provider selection.
- Multicast firewall rules.
- Source-based routing.
- Certain services do not yet fully support IPv6, e.g., HTTP-proxy, DHCP, NTP, IPFIX, SIP-proxy, and more.
- Application Rules: while there are still two separate access rule sets for IPv4 and IPv6, there is only one application rule set that covers both IPv4 and IPv6 addresses. This means that application rules can match both IP versions, depending on the rule's source and destination.

OpenSSL 3 Update - FIPS

Because OpenSSL 1.0 is no longer supported, it has been replaced by OpenSSL 3. OpenSSL 3 supports running FIPS and non-FIPS sessions simultaneously but can also operate in only FIPS or non-FIPS mode. OpenSSL 3 is fully transparent to the user.

With the update of OpenSSH to version 8.8 in CGF firmware 8.3.1, RSA signatures using SHA1 have been disabled by default. When using an up-to-date client, this should not be an issue because it will automatically use another hashing algorithm. However, when using older clients, SSH logins might suddenly no longer work after the update. If this happens, it is recommended to first try with Firewall Admin and, if that still works, to check if updates to the SSH client being used are available.

REST API

The REST API has been updated and now includes the latest implementations.

The endpoints referencing an explicit virtual server were marked as deprecated in 8.2.0 and have been removed in the 8.3.0 release. Using deprecated endpoint messages are logged in the `restd` log file. The new service container API can be used with `/rest/control/v1/service-container/...`

You can now configure policies used by firewall rules via REST.

Configuration endpoints are now available:

- CC - create new managed box (with or without ConfTemplate)
  `/rest/cc/v1/ranges/{range}/clusters/{cluster}/boxes`
- CC - Site-specific objects
  `/rest/cc/v1/config/ranges/{range}/clusters/{cluster}/boxes/{box}/service-container/{service}/site-specific-objects/{name}`
- CC - Repository Links
  `/rest/cc/v1/config/ranges/{range}/clusters/{cluster}/boxes/{box}/repository/link`
- CC - Remote Management Tunnel
  `/rest/cc/v1/config/ranges/{range}/clusters/{cluster}/boxes/{box}/network/management-tunnel`
- CC/Box - Authentication - Local/LDAP
- CC/Box - Create/Update/Remove Service
  `/rest/cc/v1/ranges/{range}/clusters/{cluster}/boxes/{box}/service-container`
  `/rest/config/v1/service-container`
- CC/Box - IPv4/IPv6 Route Config
  `/rest/cc/v1/config/ranges/{range}/clusters/{cluster}/boxes/{box}/network`

```
/route/v4
/rest/cc/v1/config/ranges/{range}/clusters/{cluster}/boxes/{box}/network
/route/v6
```

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

VPN IKEv2

The VPN settings now contain a new configuration setting called IKEv2 Suppress Network Change Events. When the check box for this parameter is selected, network/interface changes that may cause an automatic reconnect of the VPN tunnel will be ignored. For more information, see IPsec Settings.

Improvements Included in Version 8.3.0

Authentication

- HA clusters in conjunction with RSA servers are now working as expected in case of a failover. [BNNGF-32212]
- The authentication service no longer causes issues in certain situations. [BNNGF-72944]
- Group caching for authentication now works as expected. [BNNGF-73209]
- The confirmation page is now forwarding as expected. [BNNGF-80885]

Barracuda Firewall Admin

- Blocking message boxes have been replaced by a notification bar. [BNNGF-14911]
- When enabling/disabling a B0 transport, the user is asked whether all associated transports should be enabled/disabled as well. [BNNGF-20482]
- Dump files are now written as expected in Firewall Admin. [BNNGF-31921]
- When creating an offline VPN firewall rule set, Firewall Admin no longer displays error messages about "**not enough memory available**" in Windows 10. [BNNGF-50103]
- VPN site-to-site tunnels via port 443 or other ports can now be configured in the GTI Editor. [BNNGF-52150]
- IP addresses can now be filtered to display routing tables at **CONTROL > Network**, table **Routing Tables**. [BNNGF-55577]
- By using a username and a key, it is now possible to log into a cloud box from Firewall Admin and also to connect to SSH without first connecting to the firewall. [BNNGF-55828]
- The configuration to add a default gateway for shared IPv6 addresses now follows the same user interface model as for IPv6 addresses. [BNNGF-58663]
- It is now possible to configure up to 128 networks in the settings for IPsec tunnels. [BNNGF-59686]
- The configuration field **High Performance settings** in the GTI Editor can be selected only for TINA UDP transports. [BNNGF-62477]
- It is now possible to open the configuration of a firewall from the parent Control Center that has been set on a child Control Center. [BNNGF-63289]

- Creating certificates in Firewall Admin now forces the key length to be a multiple of 8 characters and ensures the creation process succeeds. [BNNGF-65515]
- Entries for the record type **other** are now handled correctly. [BNNGF-67112]
- The asterisk character is no longer displayed in red when it is actually allowed. [BNNGF-69228]
- The routing table now also displays the name for a VPN tunnel in **CONTROL > Network > Routing Table**, column **Name**. [BNNGF-69599]
- 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]
- The licenses status for SD-WAN is now displayed in the DASHBOARD. [BNNGF-73118]
- An option for adding a CRL Issuer Certificate has been added to the VPN GTI Editor at **VPN Settings > Root Certificates**. [BNNGF-73473]
- It is now possible to enable bulk assignment for pool licenses. [BNNGF-74287]
- Session reconnects are now much more responsive. [BNNGF-74644]
- Migrating clusters to 8.2 only works for clusters greater than 8.0. [BNNGF-74729]
- In Firewall Admin, filtering strings in columns now also works with strings in quotation marks. [BNNGF-74785]
- It is now possible to change the telemetry setting with bulk configuration. [BNNGF-74967]
- Telemetry settings are now displayed in a list to the right of the configuration tree. [BNNGF-74998]
- The maximum number of tunnels is now displayed as expected in the VPN settings. [BNNGF-75379]
- 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]
- Status maps for the CC are now updated asynchronously. [BNNGF-75734]
- The **High Performance** setting is also available in the group configuration for TINA tunnels. [BNNGF-75736]
- Firewall Admin now works as expected if a large rule set contains large network objects. [BNNGF-75803]
- Firewall Admin no longer reports **Energize Update is missing** or an unknown license status on CCs for newly issued licenses. [BNNGF-76090]
- When entering matching criteria in the new list view for licenses, the view will scroll to the matching entry. [BNNGF-76209]
- Bulk operations for pool licenses now work as expected for revision models. [BNNGF-76287]
- In Firewall Live, <ctrl>-double-clicking a session now opens details for big sessions. [BNNGF-76302]
- The UI option for importing a certificate has been consolidated and is now displayed with the text **Import Certificate from File** at its 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 clicking on the button **Send Changes/Activate** for a boxnet activation, an extra info-message box is displayed including a check box for optionally selecting **Don't show again**. [BNNGF-77142]

- Tabs in Firewall Admin can now be closed with the middle mouse button. [BNNGF-77143]
- Before re-assigning licenses, a warning will be displayed. [BNNGF-77652]
- Repository nodes can now contain the '-' character. [BNNGF-78196]
- 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 a "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]
- It is now possible to find, edit, and replace information in the **ConfTemplate Editor**. [BNNGF-79966]
- While a subnode is open and modified in the configuration tree, a cluster migration is not possible. [BNNGF-80277]
- For importing a certificate or a certificate chain, a password query has been implemented that displays a dialog window in the following three cases: 1. When the file to be imported is encrypted. 2. When parsing the file is not possible, e.g., due to faulty file content. 3. When the file to be imported has a different file extension, e.g., 'p12'. [BNNGF-80435]
- IPv6 network objects can now be selected for application rules [BNNGF-80591]
- The table view for IPv6 access rules now displays a column for SSL Inspection for feature level 8.3. [BNNGF-80632]
- A new entry for ICMP-v6 is now part of the list of service objects. [BNNGF-80899]

Barracuda OS

- sshd listens in IPv6 address as expected. [BNNGF-37403]
- Connection issues no longer occur for a MIP interface with an IPv4 address if an IPv6 address is newly configured on the same interface. [BNNGF-55227]
- The control daemon now correctly monitors link-local IPv6 gateway routes. [BNNGF-59923]
- Unused box services are deactivated to save resources. [BNNGF-65148]
- 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]
- Bond interfaces can now be selected to be assigned to VLANs. [BNNGF-70440]
- The kernel has been updated to version 5.10.x. [BNNGF-70536]
- The F93 and F193 now support dual PSUs. [BNNGF-70644]
- 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 firewall now collects load statistics per CPU. [BNNGF-71137]
- The boot status LED now works as expected. [BNNGF-71629]
- Admin templates that contain the underscore ('_') character no longer cause issues with AD users. [BNNGF-72146]
- SNMP walk for determining the percentage of disk fill now works as expected. [BNNGF-73290]
- The Control Center no longer crashes in certain situations after reporting the error message "skb_warn_bad_offload". [BNNGF-73804]
- The release check on the firewall no longer fails in certain situations. [BNNGF-73812]

- Enabling `acpfctrl` to monitor portX on the firewall no longer eats up memory. [BNNGF-74046]
- The command '`/opt/phion/bin/external-netobj-tool create -s parameter`' now works as expected. [BNNGF-74047]
- SLACK notifications for eventing now work as expected. [BNNGF-74358]
- After updating from firmware version 7.2.6 to 8.0.5/8.2.1 or higher, routes are introduced as expected for GRE tunnels. [BNNGF-74692]
- The DHCP client now also requests and installs static routes. [BNNGF-75146]
- When upgrading a box to the new 2-layer service architecture, correct warnings will be displayed for all cases where server IPs are configured without routes. [BNNGF-75453]
- It is now possible to mark certificates as **trusted** in the certificate store. [BNNGF-75492]
- Default routes are now provided to DHCP clients as expected. [BNNGF-75691]
- Creating a new private key now updates the hash of the box certificate as expected. [BNNGF-76206]
- Event notification now works as expected. [BNNGF-76327]
- The firewall no longer experiences high CPU loads in certain situations due to optimizations of the `systemd` process. [BNNGF-76401]
- It is now possible for Firewall Insights to stream data to Logstash. [BNNGF-76503]
- The `acpf` TCP sequence check is now correct for packets following syn/fin. [BNNGF-77003]
- Switching to the 'dedicated HA config mode' no longer causes network errors depending on the configuration order of the primary and secondary box. [BNNGF-77407]
- When changing the MTU size of interfaces part of a bond interface, the MTU size for the bond interface is now set correctly. [BNNGF-77905]
- Filebeat clients now report through the management tunnel as expected. [BNNGF-78034]
- The back end now reports correct values to the UI for the state of /phion0 volumes on firewalls with very large disks. [BNNGF-78086]
- A memory leak has been fixed upon HA failover when using ISP links with DHCP. [BNNGF-78135]
- 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]
- The LTE modem is now enabled by default to be used by zero-touch via the mobile network. [BNNGF-79206]
- The DHCP client now introduces the default gateway route as expected. [BNNGF-79948]
- Disabling of ping responses for IPv6 server IP addresses now works as expected. [BNNGF-80015]
- 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 crashes in certain situations. [BNNGF-80562]
- The firewall no longer freezes in certain situations. [BNNGF-80576]
- HTTPS sites now load at expected speeds when certificates are validated. [BNNGF-80589]
- VLANs / Interfaces with the name "vlan" do not affect the activation or functionality of the unit. [BNNGF-81075]

Firewall Control Center

- The Control Center no longer sends a complete update after a preceding update is successfully finished. [BNNGF-48636]
- When a box with a GTI service tunnel is moved in the Control Center, the GTI tunnel is now moved together with the box as expected. [BNNGF-65484]
- Handling of locks during minimal PAR-file generation works as expected for zero-touch deployments (ZTD). [BNNGF-68061]
- Discontinued/outdated licenses are ignored when a valid license subscription is activated in the Control Center. [BNNGF-71216]
- The Control Center creates an event entry **File or Pattern Update Failed** if a file update to a box fails. [BNNGF-72198]
- Pool licenses can now also be removed during an update of other pool licenses. [BNNGF-72989]
- The CLI command '`cctool`' has been extended to support functionality for importing managed boxes on the CC and enabling/disabling managed boxes. [BNNGF-73098]
- 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 event service now sends emails to multiple recipients as expected. [BNNGF-73745]
- Control Centers operating firmware 8.3.0 or higher display only supported cluster versions higher or equal to 7.2. [BNNGF-74486]
- In case of an HA failover, the Control Center now sends correct PAR files to the firewall. [BNNGF-74628]
- SSH login for CC administrators works as expected. [BNNGF-74737]
- A dynamic network object is present in the host firewall for parent-to-child Control Centers (split CC). [BNNGF-75153]
- A CC admin for a new range will no longer see other ranges in the SD-WAN tab. [BNNGF-75190]
- Migrating distributed firewalls with similar server names to the 2-layer service architecture no longer leads to incorrect allocations of the rule sets in the firewalls. [BNNGF-76328]
- The CC clone wizard now adds the correct name to the new target box. [BNNGF-76336]
- Dynamic loading of the CC configuration tree has been improved. [BNNGF-76495], [BNNGF-76612]
- 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]
- A bug has been fixed where locking the FSC editor in **Cluster Settings** caused the FSC communication daemon to crash. [BNNGF-79090]
- In the Control Center, the SC editor now updates the VPN configuration as expected. [BNNGF-80407]

DHCP

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

DNS

- When a new record is opened for DNS, the value of 3600 is inserted into the TTL field by default. If records are changed, the TTL field remains untouched if it was empty before. [BNNGF-67109]
- When changing a value for a domain, the related serial is updated only for the affected domain, and serials for all other domains remain untouched. [BNNGF-68137]
- At **CONFIGURATION > Configuration Tree > Administrative Settings > Caching DNS Service**, the label for forwarders for DNS zones has been renamed to **Forwarders for DNS Zones**. [BNNGF-69590]
- Conditional forwarding for DNS now works as expected. [BNNGF-69838]
- 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 fix CVE-2021-25215. [BNNGF-74781]
- The BIND system has been updated to version 9.16.x. [BNNGF-74788]

Firewall

- The minimum version for TLS has been set to 1.2. [BNNGF-73183]
- Firewall authentication is now restricted to groups instead of individual users. [BNNGF-73708]
- HTTPS is now included again in the **All HTTP** protocol object. [BNNGF-74942]
- TCP resets are no longer dropped and sessions are now terminated correctly on ports 443 and 445. [BNNGF-76268]
- Improvements have been made to reduce waiting time in sessions when receiving resets in the TCP protocol. [BNNGF-76724]
- The categorization of URLs for URL filters now works as expected. [BNNGF-78381]
- The **From Client** and **From Server** categories have been removed from the configuration area at **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > IPS Policies**. [BNNGF-80017]
- The **Firewall Authentication Client** no longer logs out automatically after approximately 30 seconds. [BNNGF-80694]
- New configuration fields (**Redirection URL, Explicit Redirection URL**) have been added to the **Guest Access** configuration screen. [BNNGF-80897]

HTTP Proxy

- The HTTP proxy has been updated to version 4.15. [BNNGF-74727]
- URL filter categories now work as expected in the settings for the HTTP proxy access control. [BNNGF-74895]

REST

- As of release 8.2.1, SC confunits are now prefixed with 'fsc', and CGF confunits are prefixed with 'cgf'. [BNNGF-74599], [BNNGF-78506]
- Replacing large network objects no longer fails in certain situations. [BNNGF-75758]
- The REST API call for determining the usage of memory now considers disk space usage in a dedicated **diskState** field. [BNNGF-76335]

- The minimum value for "time to live" at **CONFIGURATION > Configuration Tree > Infrastructure Service > REST API Service > Access Tokens** is limited to 1. [BNNGF-76647]

SSL-VPN

- When configuring a launch path for SSLVPN, the path may now also contain the '#' character. [BNNGF-70950]
- RDP tunnels no longer crash under high load. [BNNGS-3761]
- 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

- In **Control Center > Configuration Tree > VPN GTI Editor > Tunnel Properties > Advanced**, it is now possible to configure the lifetime value for the 'Phase 2' of IKEv1 tunnels (Phase 2 Lifetime Adjust [sec]). [BNNGF-54150]
- The import of PFX files into VPN settings now works as expected. [BNNGF-69741]
- The VPN pre-handshake no longer cuts off parts of the username. [BNNGF-70815]
- After an ISP outage, VPN tunnels are re-established and now work as expected. [BNNGF-73584]
- 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]
- If the CPU is not supported, an entry will be created in the VPN log. [BNNGF-75760]
- New CRL settings are now enabled in the GTI Editor. [BNNGF-76253]
- Using MSAD + RSAACE for personal licenses no longer causes authentication errors. [BNNGF-76332]
- A new check box now enables the user to select whether to ignore routing/network changes for IKEv2. [BNNGF-77956]
- A VPN tunnel with DNS now starts as expected. [BNNGF-79154]
- For FIPS mode, a minimum of 2048-bit RSA box key will be required when connecting to the VPN server with FirewallAdmin (the VPN tab). [BNNGF-80686]

Known Issues

Known Issues Related to CGF Policy Profiles

- **IMPORTANT** – Policy profiles cannot be used on a VPN concentrator or Secure Access Controller!
- **Firewall** – If a VPN TINA tunnel transport over a specific ISP goes down, the Internet traffic over the same ISP link will not work either. [BNNGF-81749]
- Provider class in boxnet must not be changed "afterwards", unless existing VPN tunnels are reconfigured accordingly.
- There is currently no VRF support for policies in 8.3.0.
- Fallback (on-demand) does not always work in combination with explicit SD-WAN policy. [BNNGF-81805]

Known Issues Related to Other Topics

- **Azure** – OMS is currently not supported on CC-managed boxes.
- Currently, no RCS information is logged for **Named Networks**. [BNNGF-47097]
- **Barracuda Firewall Admin** – FW Admin 8.x fails to configure DNS 7.x correctly. [BNNGF-77636]
- **Barracuda OS** – Gateway probing continues after route got removed. [BNNGF81668]
- **Barracuda OS** – The IPv6 route management of `controld` interferes with SLAAC. [BNNGF-81574]
- 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 by doing an **Emergency Override**.
- F183R – The F183R freezes when starting the telemetry process if an M40 modem is connected. Workaround: if you disconnect the modem or disable telemetry, the problem will not occur.
- **Firewall** – A **Connection Object** is not applied if it uses network interfaces. [BNNGF-83146]
  As a workaround, also add the interface to the **Failover and Load Balancing** section and remove it again as soon as a fix is available.
  This issue affects release 8.3.0 and will be fixed in the upcoming firmware release 8.3.1.
- If you enable WanOPT on a tunnel, TCP traffic is no longer forwarded. However, ping works as expected. [BNNGF-82256]
- **IPS** – Using IPS for UDP in firmware 8.3.0 will break the firewall. [BNNGF-83189]

Figures

1. global_pols.png
2. network_activation_window_new.png
3. fwa_dialog_boxnet_activation_required_after_mip_change.png
4. fwa_no_connect_session_button.png
5. C2S_FQDN_for_network_routes.png
6. C2S_tunnel_mode_hybrid_tcp_udp.png
7. C2S_MTU_size_for_clients_02.png
8. C2S_disk_encryption.png
9. C2S_certificate_chain.png
10. vpn_settings_password_for_certs.png
11. IPS_conf_screen.png