

## 8.3.1 Release Notes

<https://campus.barracuda.com/doc/96772103/>

### Important Announcements and Notes

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

Outdated technical features are subject to removal in order to keep the CloudGen Firewall up to date and performing properly.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Certain features will be removed completely because they have become technically obsolete; other features have become outdated and will be replaced by improved technology.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 8.3.0/8.3.1 Release

- **Generic Forwarder**

As of 8.3.0/8.3.1, 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 or higher. 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

## Important Note for Users Wanting to Upgrade from Firmware Release 8.2.2

As of February 6, 2023, you can now upgrade from firmware release 8.2.2 to firmware release 8.3.1. This upgrade can be installed both on CloudGen Firewalls and on Control Centers. However, as this is a special upgrade, there are two different methods of how you must perform it depending on the type of your appliance.

For more information on how to upgrade from firmware release 8.2.2 to 8.3.1, see [8.3.1 Migration Notes](#).

## Use the Appropriate Firewall Admin Release

Generally, Barracuda Networks recommends using the latest version of Firewall Admin for a new firmware release.

As of the public availability of this firmware 8.3.1, Barracuda Networks recommends using at least Firewall Admin version 8.3.1-64. You can download this version here:  
[https://dlportal.barracudanetworks.com/#/packages/5466/FirewallAdmin\\_8.3.1-64.exe](https://dlportal.barracudanetworks.com/#/packages/5466/FirewallAdmin_8.3.1-64.exe).

In case of upcoming hotfixes that solve known issues for Barracuda Firewall Admin, you can find the respective notes for the updated version(s) in this info box:

- **9.6.2022 - Hotfix for Firewall Admin 8.3.1-202:**  
[https://dlportal.barracudanetworks.com/#/packages/5478/FirewallAdmin\\_8.3.1-202.exe](https://dlportal.barracudanetworks.com/#/packages/5478/FirewallAdmin_8.3.1-202.exe).
- **29.3.2022 - Hotfix 1094 for CloudGen Firewall 8.3.1:** This hotfix updates the Microsoft Open Management Infrastructure package to version 1.7.0-0. This fixes a security vulnerability (CVE-2022-29149) and adds stability and functionality improvements.  
For more information, see  
<https://dlportal.barracudanetworks.com/#/packages/5583/OMI-1.7.0-0-1094-8.3.1-180009149.tgz>

## Release Notes

Firmware version 8.3.1 is a minor release.

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.

### IMPORTANT Note for Hotfix-1083

**SAML/ADFS Authentication** also relies on the parameter **Session Cookie Lifetime** and can be configured at **Box > Infrastructure Service > Authentication Service > SAML/ADFS Authentication**, in section **SAML Configuration**. Switch to **Advanced Mode** in the left menu area, and click **CONFIGURATION MODE** to get access to this parameter.

If you have **SAML/ADFS Authentication** enabled and the value for the parameter **Session Cookie Lifetime** is not 0, you must set the value to 0 after installing hotfix-1083.

### 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.

- **6.7.2022 - Hotfix-1083:** Cumulative hotfix. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5519/cumulative-1083-8.3.1-157033585.tgz>.  
See also the following IMPORTANT note in the yellow info box.
- **3.11.2022 - Hotfix-1086:** OpenSSL 3.0.7. For more information, see: <https://dlportal.barracudanetworks.com/#/packages/5554/openssl-1086-8.3.1-167387414.tgz> AND <https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/>
- **13.12.2022 - Hotfix-1087:** Cumulative Hotfix 8.3.1. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5559/cumulative-1087-8.3.1-170933727.tgz>.
- **19.12.2022 - Hotfix-1088:** Reporting Service. For more information, see: <https://dlportal.barracudanetworks.com/#/packages/5557/reporting-1088-8.3.1-170832995.tgz> AND <https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/>
- **26.1.2023 - Hotfix-1089:** Security update. Fixes a security vulnerability (reported by SEC Consult) in the local Web UI. For more information, see: <https://dlportal.barracudanetworks.com/#/packages/5560/webui-sdwan-1089-8.3.1-17414>

[1891.tgz](#) AND

<https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/>

- **9.2.2023 - Hotfix-1092:** OpenSSL - For more information, see <https://dlportal.barracudanetworks.com/#/packages/5577/openssl-1092-8.3.1-175869362.tgz>.
- **15.2.2023 - Update package:** Update package for Barracuda CloudGen Firewall, Barracuda CloudGen WAN, and Barracuda Firewall Control Center from 8.x to 8.3.1 with hotfixes. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5580/update.GWAY-8.3.1-0086+5hotfixes.tgz>
- **15.2.2023 - Patch package:** Patch package for Barracuda CloudGen Firewall, Barracuda CloudGen WAN, and Barracuda Firewall Control Center from 8.3.x to 8.3.1 with hotfixes. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5580/update.GWAY-8.3.1-0086+5hotfixes.tgz>

The following devices have reached EoL status:

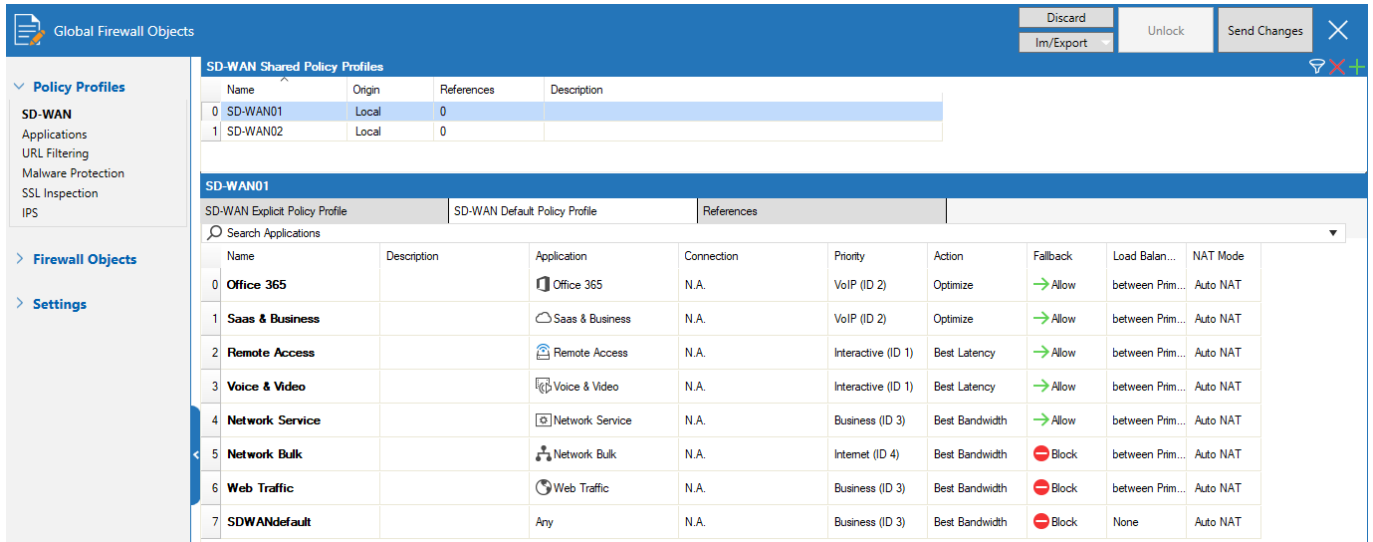
Device Type	Model	EoL Date
CloudGen Firewall	F800 Rev. B	2022-03-01
CloudGen Firewall	F900 Rev. A	2021-11-31
Control Center	C400	2022-02-28
Control Center	C610	2022-02-28
Modem	M10 (3G/UMTS)	2019-03-31
Modem	M11 (3G UMTS)	2021-09-30

## What's New in Version 8.3.1

### CGF Policy Profiles

On Barracuda CloudGen Firewall version 8.3.1, 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 creating 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 screenshot shows the 'Global Firewall Objects' configuration page. On the left, a sidebar lists 'Policy Profiles' and 'Firewall Objects'. The main area displays 'SD-WAN Shared Policy Profiles' with a table listing two profiles: SD-WAN01 and SD-WAN02. Below this, the 'SD-WAN01' configuration is shown, including a search bar for applications and a detailed table of policies.

Name	Origin	References	Description
0 SD-WAN01	Local	0	
1 SD-WAN02	Local	0	

SD-WAN01									
SD-WAN Explicit Policy Profile		SD-WAN Default Policy Profile		References					
Search Applications									
Name	Description	Application	Connection	Priority	Action	Fallback	Load Balan...	NAT Mode	
0 Office 365		Office 365	N.A.	VoIP (ID 2)	Optimize	→ Allow	between Prim...	Auto NAT	
1 Saas & Business		SaaS & Business	N.A.	VoIP (ID 2)	Optimize	→ Allow	between Prim...	Auto NAT	
2 Remote Access		Remote Access	N.A.	Interactive (ID 1)	Best Latency	→ Allow	between Prim...	Auto NAT	
3 Voice & Video		Voice & Video	N.A.	Interactive (ID 1)	Best Latency	→ Allow	between Prim...	Auto NAT	
4 Network Service		Network Service	N.A.	Business (ID 3)	Best Bandwidth	→ Allow	between Prim...	Auto NAT	
5 Network Bulk		Network Bulk	N.A.	Internet (ID 4)	Best Bandwidth	⊘ Block	between Prim...	Auto NAT	
6 Web Traffic		Web Traffic	N.A.	Business (ID 3)	Best Bandwidth	⊘ Block	between Prim...	Auto NAT	
7 SDWANdefault		Any	N.A.	Business (ID 3)	Best Bandwidth	⊘ Block	None	Auto NAT	

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 SSL 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](#).

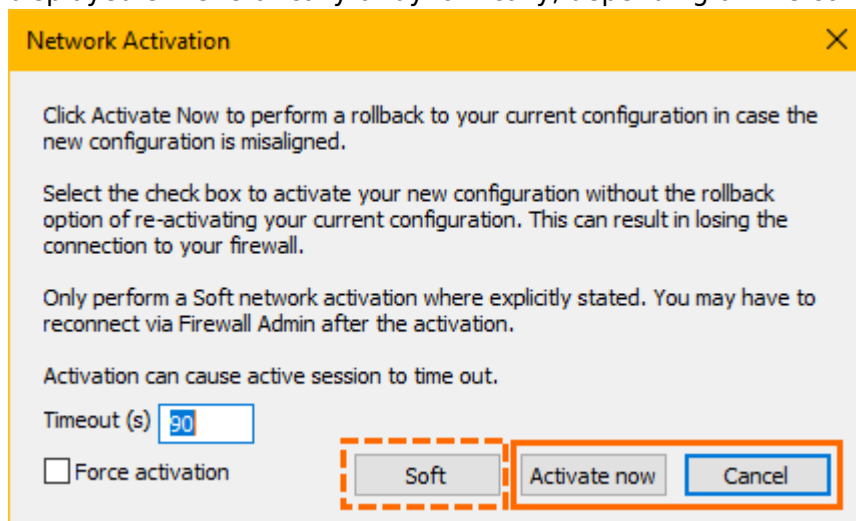
It is recommended to read the Known Issues section at the bottom of this 8.3.1 Release Notes article ( [Known Issues related to CGF Policy Profiles](#) ) before using CGF Policy Profiles.

### 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

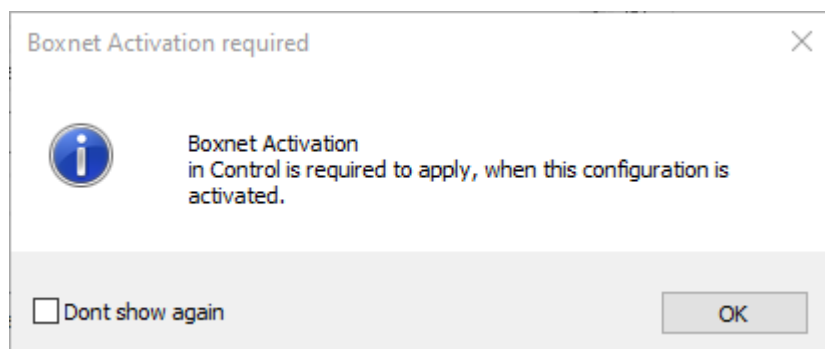
Activating the network is now supported by two new dialog windows that include user-interface items displayed either statically or dynamically, depending on the context in which the window is displayed:



The image shows a 'Network Activation' dialog box with a yellow title bar and a close button. The dialog contains the following text and controls:

- Click Activate Now to perform a rollback to your current configuration in case the new configuration is misaligned.
- Select the check box to activate your new configuration without the rollback option of re-activating your current configuration. This can result in losing the connection to your firewall.
- Only perform a Soft network activation where explicitly stated. You may have to reconnect via Firewall Admin after the activation.
- Activation can cause active session to time out.
- Timeout (s)
- ☐ Force activation
- Buttons: **Soft**, **Activate now**, and **Cancel**. The **Soft** button is highlighted with a dashed orange border, and the **Activate now** and **Cancel** buttons are grouped with a solid orange border.

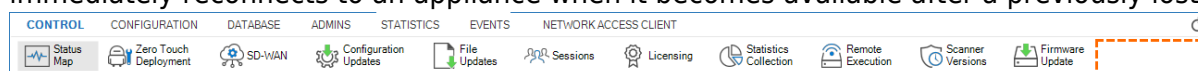
The **Soft** option will be displayed only in certain required contexts.



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.



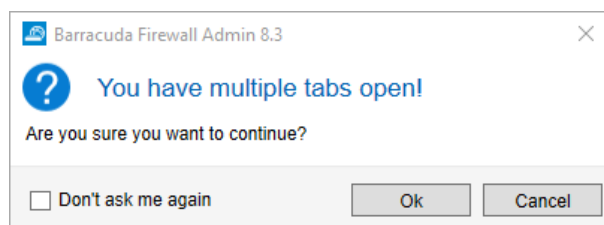
### Automated HA Auto Pairing

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](#).

### Barracuda Firewall Admin

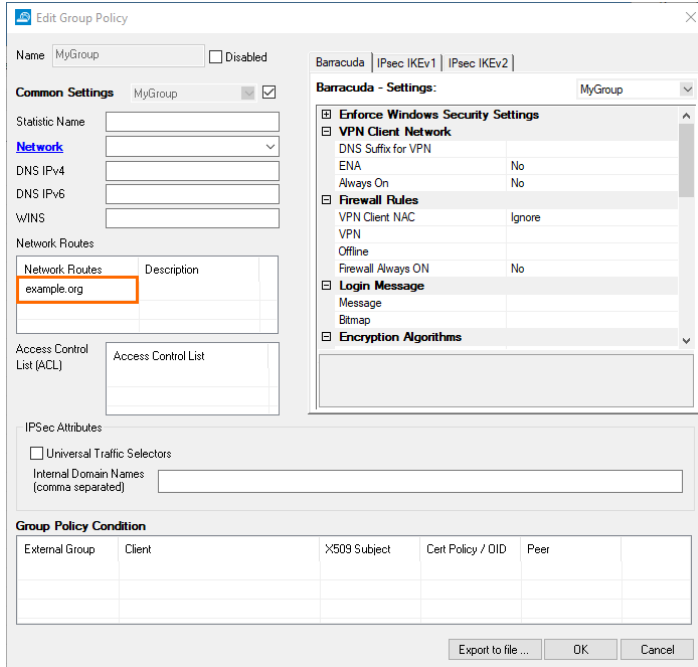
If multiple tabs are open in Barracuda Firewall Admin and the main window will be closed by clicking the 'X' symbol in the upper right corner of the window, a dialog will be displayed giving the user the choice to cancel the closing of all tabs or to keep Firewall Admin's window open. The option of displaying the dialog window can be turned off via a checkbox.



### 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.



**Edit Group Policy**

Name: MyGroup ☐ Disabled

**Common Settings** MyGroup ☒

Statistic Name:

**Network**

DNS IPv4:

DNS IPv6:

WINS:

**Network Routes**

Network Routes	Description
example.org	

**Access Control List (ACL)**

Access Control List

**IPSec Attributes**

☐ Universal Traffic Selectors

Internal Domain Names (comma separated):

**Group Policy Condition**

External Group	Client	X509 Subject	Cert Policy / OID	Peer

Export to file ... OK Cancel

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.

This feature requires Barracuda Network Access Client version 5.3 for Windows. For more information, see [Release Notes - Barracuda NAC/VPN Client 5.3 for Windows](#).

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](#).

New Machine VPN Profile

General

Connect/Reconnect

Advanced

Connection Entries

Description

Server Address

Authentication Method

Connect with Windows credentials

Remember credentials

Tunnel Settings

Tunnel Mode

Key Agreement Protocol

Encryption Algorithm

Authentication Algorithm

One-Time Password (OTP) Mode

Keep Alive Timeout [s]

Compression

Save

Cancel

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.

Interface Configuration

VPN I...	MTU	IPs	Multicast
pvpn0	1430		

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.

**Barracuda Settings**

**Barracuda**

Name

☐ Enable VPN Client NAC

ENA  Split Tunnel ON

Domain

VPN Rules  Offline Rules

Message  Bitmap

Registry  ☐ Firewall Always ON

☐ VPN Always ON

Key Time Limit  Tunnel Probing

Key Traffic Limit  Tunnel Timeout

**Accepted Encryption Algorithms**

☒ AES256 ☒ AES256-CTR ☒ CAST ☒ 3DES ☐ Null

☒ AES ☒ AES-CTR ☒ Blowfish ☐ DES

**Accepted Authentication Algorithms**

☒ SHA512 ☒ SHA256 ☒ SHA1 ☒ MD5

☒ GCM ☒ Null

**Enforce Windows Security Settings**

☐ Network Firewall ☐ Windows Update ☐ User Account Control

☐ Virus Protection ☐ Spyware Protection ☐ Internet Security Settings

☐ Disk Encryption

OK Cancel

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

VPN Settings - VPN (vpn)

**VPN Settings**  
 General  
 IPSec  
 Routed VPN  
 Client Networks  
 Service Keys  
 Root Certificates  
 Service Certificates  
  
**Configuration Mode**  
 Switch to Basic

**Service**

Listen on port 443 ☒

Maximum number of tunnels <auto>

CRL poll time (minutes) 0

Site to Site authentication ☒

Add VPN routes to main routing table No

Allow concurrent user sessions ☒

Use Perfect Forward Secrecy Yes

Accounting information storage time (days) 14

Send SDWAN data to Control Center <auto>

Log VPN user accounting Off

Log SDWAN Off

C2S Reconnect Cache Timeout 30

Default Server Certificate <explicit>

Private key No Key present

Certificate No Certificate present

Certificate Chain No Certificate Chain present

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', ...

**Service**

Listen on port 443 ☒

Maximum number of tunnels <auto>

CRL poll time (minutes) 0

Site to Site authentication ☒

Add VPN routes to main routing table No

Allow concurrent user sessions ☒

Use Perfect Forward Secrecy Yes

Accounting information storage time (days) 14

Send SDWAN data to Control Center <auto>

Log VPN user accounting Off

Log SDWAN Off

C2S Reconnect Cache Timeout 30

Default Server Certificate <explicit>

Private key No Key present

Certificate No Certificate present

Certificate Chain No Certificate Chain present

**Listen on port 443**

Defines whether incoming VPN connections on port 443 should be accepted or not. VPN tunnels connecting to this port are limited to the TCP transport protocol.

**Note:**  
Port 443 can only be used by one service. If this port is redirected to another machine by the firewall service or a SSL VPN is running, disable port 443 for client-to-site VPN connections.

**TINA**

Handshake Timeout (sec) 10

Tunnel HA Sync ☒

Allow fast requests ☒

Pending session limit ☒

**Site to Site authentication**

Typically, a tunnel registers itself at the firewall, creating an *auth.db* entry with the tunnel network and the tunnel credentials. You can then create an access rule with the tunnel name or credentials as a condition. This feature is rarely used.

**Password Needed**

Password protected file

Password

OK Cancel

And finally, two new encryption methods, AES-GCM and AES-CTR, can now be configured in the client-to-site **VPN Settings**.

## ConfTemplates

The ConfTemplate Editor has been improved. It now contains three areas for managing templates and instances:

- **Edit** – Clicking **Edit** brings the editing area for interactively configuring the template through edit fields to the front.
- **Script** – Clicking **Script** brings the script editor for configuring the template in text mode to the front and displays the ConfTemplate in the script language TDL.
- **Show Reference Library** – Clicking **Reference Library** opens the window for configuring parameters and variables.

For more information on ConfTemplates, see [Configuration Templates](#).

For more information on the ConfTemplate Manager, see [Configuration Template Manager](#).

For more information on the TDL script language, see [Template Definition Language - TDL](#).

## 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.
- SC 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.x. For more information, see also [8.3.1 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".

☒ Enable IPS
 ⚠ ☒ Report only
[Download Options for IPS Signatures](#)

☐ Scan SSL-Intercepted Traffic

---

**Default Policy**

[Clone Default Policy](#)

<b>Name</b>	Default				
<b>Description</b>	Default Policy				
<b>Scan</b>	<input checked="" type="radio"/> ON <input type="radio"/> OFF				
	<b>Critical</b>	<b>High</b>	<b>Medium</b>	<b>Low</b>	<b>Informational</b>
<b>Action</b>	Drop          Alert	Drop          Alert	Log          Warn	Log         Notice	None
<input type="checkbox"/> Scan only for explicit signatures <a href="#">Edit explicit actions (0)</a>					

---

**Custom Policies** [Copy to Default Policy](#)

ID	Scan	Name
1	OFF	No Scan Policy

<b>Name</b>	No Scan Policy				
<b>Description</b>	This is a system policy. Used to not scan for IPS Signatures. This Policy is read only.				
<b>Scan</b>	<input type="radio"/> ON <input checked="" type="radio"/> OFF				
	<b>Critical</b>	<b>High</b>	<b>Medium</b>	<b>Low</b>	<b>Informational</b>
<b>Action</b>	None	None	None	None	None
<input type="checkbox"/> Scan only for explicit signatures <a href="#">Show explicit actions (0)</a>					

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 to 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:

- 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](#).

## VPN Port Number

As of firmware release 8.3.1, the port number for the VPN server can now be configured individually in **CONFIGURATION > Configuration Tree > your box > Assigned Services > VPN > VPN Settings**, edit field **Local VPN listen port**.

Service	
Listen on port 443	<input checked="" type="checkbox"/>
Local VPN listen port	<input type="text" value="791"/>
Maximum number of tunnels	<input type="text" value="auto"/>

## Improvements Included in Version 8.3.1

### 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]

- When group caching is enabled, authentication now works as expected. [BNNGF-81127]

#### Barracuda Firewall Admin

- The length of the service name has been increased to 40 characters. [BNNGF-79461]
- The port number for a VPN server is no longer bound to port 691 and can now be configured individually both for UDP and TCP. [BNNGF-79836]
- Tabs in the ribbon bar now also display the name of the firewall and its associated MIP. [BNNGF-79931]
- If multiple tabs are present in the ribbon bar, clicking on the 'X' symbol of Firewall Admin's window in the upper-right corner causes a dialog window to be displayed that must be confirmed by the user. [BNNGF-80811]
- If a connection is made to an external VPN server in GTI, the transport source-IP can now be chosen in the user interface, as expected. [BNNGF-81074]
- In order to avoid interrupting the loading of extremely large numbers of boxes in a Control Center, refreshing session tabs can now be disabled with the **Refresh Always** button on the **CONTROL > Sessions** page. [BNNGF-81213]
- Limiting traffic in the default shaping tree now works as expected when a PC is located in the US. [BNNGF-81245]
- When enabling or disabling tunnels directly in the balloon dialog window of the GTI editor, the **Send Changes** button is now activated as expected. [BNNGF-82276]
- The list for additional VPN transport networks no longer displays additional GTI networks. [BNNGF-82939]
- Cluster names are now displayed as expected in a Control Center on the **CONTROL > Status Map > All** page. [BNNGF-82989]
- Connecting to the SSH now works as expected when connecting to the configuration with a public key and without entering the username into the AltName field. [BNNGF-83119]
- When using IPsec settings for client-to-site configurations, Firewall Admin no longer crashes in certain situations. [BNNGF-83373]
- The option **Transform virtual server into assigned service node** is now displayed as expected when clicking the appropriate configuration tree node. [BNNGF-83492]

#### Barracuda OS

- Connection failover for UDP and ESP traffic has been improved. [BNNGF-76131]
- 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]
- The **Model** label on the **CONTROL > Services** page is now displayed as expected. [BNNGF-78300]
- When SCADA detection is enabled and PLC is accessed via client-to-site VPN, the connection to PLC S7 now works as expected. [BNNGF-79273]
- In rare cases, calculations caused blocked sessions that now no longer occur. [BNNGF-80007]
- Application Control for AnyDesk now works as expected. [BNNGF-80329]
- TLS Inspection now works as expected in the HTTP proxy. [BNNGF-80500]
- Host routes with MTU 1500 now work as expected on interfaces with MTU 9000. [BNNGF-80501]

- Block pages are now also injected into plaintext HTTP sessions that are routed between VRF instances. [BNNGF-81198]
- The handling of IPv6 routes that are obtained through SLAAC has been improved. [BNNGF-81574]
- RIP now works as expected. [BNNGF-81977]
- The server node is now correctly removed from the configuration tree after migrating the old 3-layer service architecture to the new 2-layer one. [BNNGF-82070]
- An update of the Firewall Insight license now works as expected if the license name was previously changed. [BNNGF-82088]
- Fan speeds are now displayed correctly. [BNNGF-82702]
- Security measures have been taken for CVE-2022-0847. [BNNGF-82852]
- **Connection Objects** that reference a **Single IP Network Object** can now be configured again. [BNNGF-82977]
- Security measures have been taken for CVE-2022-0778. [BNNGF-83054]
- **Connection Objects** are applied as expected when using network interfaces. [BNNGF-83146]

## Cloud Azure

- A managed box now connects to an Azure VWAN as expected. [BNNGF-80901]
- Service IPs of additional IPs are now used in an HA pair as expected. [BNNGF-81951]
- Azure Load Balancer probes are now handled properly. [BNNGF-82114]

## Control Center

- On an 8.2.0 Control Center, the update package for 8.x to 8.2.0 now appears as expected. [BNNGF-77667]
- Control Centers with IPv4 and IPv6 enabled now work as expected after an update. [BNNGF-79934]
- After configuration changes, a bogus "defaultbox" is no longer displayed in the CC status map. [BNNGF-81019]

## DHCP

- **BOOTREPLY** messages are now processed as expected after the DHCP relay service is restarted following a complete configuration update. [BNNGF-81966]

## DNS

- If multiple DNS services are configured, DNS no longer causes issues with using incorrect source-IP addresses. [BNNGF-78289]
- The TTL value for DNS is now updated as expected. [BNNGF-82180]
- The DNS system BIND has been updated to version 9.16.27. [BNNGF-83078]

## Firewall

- The firewall no longer freezes when using IPS for UDP. [BNNGF-83189]

## HTTP Proxy

- The HTTP proxy no longer experiences memory leaks in certain situations. [BNNGF-80387]
- The proxy service no longer causes segmentation faults after transforming a box to operate the new 2-layer service architecture (Assigned Services). [BNNGF-83509]

## REST

- CC Admins with ACL no longer get 403 errors on certain REST API paths in certain situations. [BNNGF-80340]

## VPN

- Using special characters in the **Group Pattern** field of the **Group Policy Condition** no longer causes an issue when logging in. [BNNGF-76804]
- The port number for a VPN server is no longer bound to port 691 and can now be configured individually both for UDP and TCP. [BNNGF-79836]
- Downloading the CRL file now works as expected. [BNNGF-80823]
- IKEv2 memory leaks no longer occur when establishing VPN tunnels/transport. [BNNGF-81077]
- Default route and DNS server (IKEv1 C2S with IOS 15.2) now work as expected. [BNNGF-81513]
- Bandwidth probing for SD-WAN now displays the effective throughput between the two endpoints of the connection. [BNNGF-82160]
- TCP traffic on WanOPT tunnels is now forwarded as expected. [BNNGF-82256]
- Creating VPN connections using L2TP now works as expected. [BNNGF-82346]

## 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 8.3.1.

### 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]
- The learn-only mode for OSPF is not working as expected. [BNNGF-65299]
- **Barracuda OS** - The IPMI log shows errors after updating the IPMI firmware to 1911-R4-3.2.5.ima. However, these error log entries do not affect the normal function of the IPMI. [BNNGF-88127]
- **Firewall** - Inspecting traffic for QUIC / UDP 443 is currently not supported. [BNNGF-74540]
- **Firewall** - SSL inspection breaks on office 365 admin page with TLS 1.3. [BNNGF-83026]  
NOTE: If a contacted server does not support at least the configured minimum TLS version, then no connections to that server will be possible. Connections will be reset. This can especially have an impact on embedded frames or Cross-Origin Resource Sharing (CORS) when those servers do not support the same TLS version as the main site.  
For troubleshooting:  
Turn **Box > Infrastructure Services > General Firewall Configuration > Advanced Log Settings > SSL/TLS loglevel** to **debug**.  
Look out for "alert protocol version" in SSL logs (Assigned Services > NGFW > SSL), e.g.:  
11.04.2022 15:36:46 Info firewall: [TAP3Worker] Worker 1: Session 1271:  
SSL handshake to server failed: ID 2400 192.168.100.95:54525 <=>  
104.103.84.247:443 assets.onestore.ms: error in OpenSSL library:  
error:0A00042E:SSL routines::tlsv1 **alert protocol version**
- **Firewall Live** - The device filter **Any Interface** does not work. [BNNGF-85689]
- **VPN (SCA)** - With a fresh installation of 8.3.1 the SC Networks are no longer introduced into VPN table 5. [BNNGF-84737]

## 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. dialog\_window\_multiple\_tabs\_open.png
6. C2S\_FQDN\_for\_network\_routes.png
7. C2S\_tunnel\_mode\_hybrid\_tcp\_udp.png
8. C2S\_MTU\_size\_for\_clients\_02.png
9. C2S\_disk\_encryption.png
10. C2S\_certificate\_chain.png
11. vpn\_settings\_password\_for\_certs.png
12. IPS\_conf\_screen.png
13. vpn\_settings\_edit\_field\_for\_vpn\_port\_number.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.