
Release Notes 8.3.1

<https://campus.barracuda.com/doc/96024723/>

What's New in Version 8.3.1

Private Service Edge

Barracuda CloudGen WAN now provides private service edge for hybrid deployments. Private service edge is ideal for organizations that need to follow certain geopolitical requirements or need full control over the data plane. Private service edge devices provide the same scope of security and networking functionality as the cloud service and are administrated and maintained via a central management platform.

For more information, see [How to Create a Private Edge Gateway in Barracuda CloudGen WAN](#).

Secure Connector

The Barracuda Secure Connector is now available for Barracuda CloudGen WAN. The Secure Connector offers large-scale remote access capabilities. It enables the ever-growing number of IoT devices and micro-networks to securely connect to a central or distributed corporate datacenter. In such a scenario, a large number of small Secure Connector appliances connect via TINA VPN to the Barracuda CloudGen WAN Gateway.

Currently available Secure Connector hardware:

- [Secure Connector 2 Revision A](#)

The Secure Connector can be claimed and deployed in the same way as other CloudGen WAN hardware.

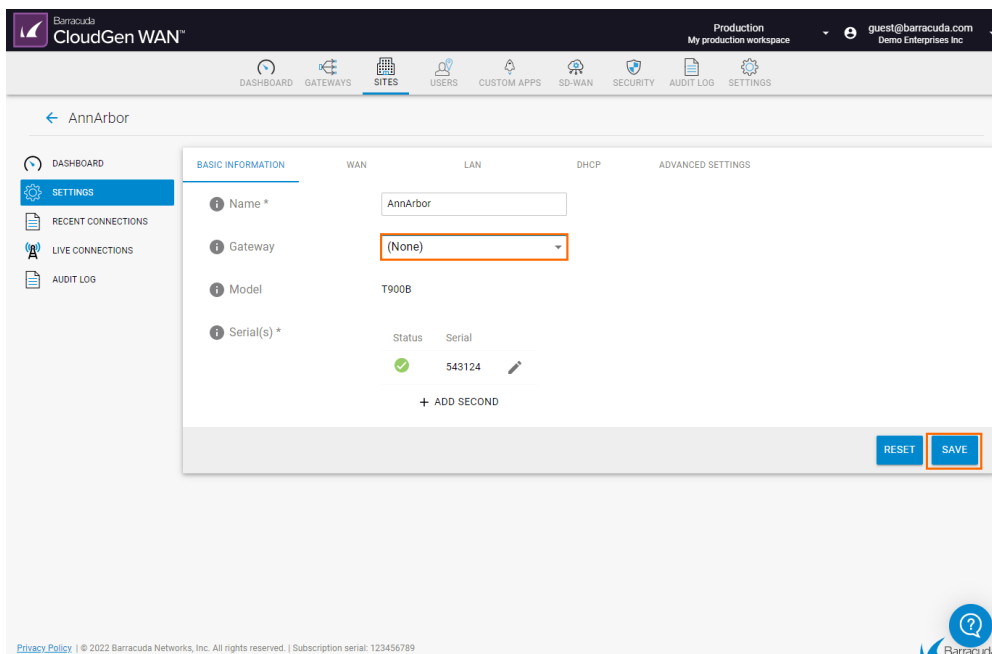
Note, however, two exceptions:

1. The operating system of the Secure Connector appliance must be updated before it is connected to the CloudGen WAN service. Please contact Barracuda Networks for the update of the Secure Connector appliance operating system.
2. The Barracuda Secure Connector is available for both the Barracuda CloudGen Firewall and Barracuda CloudGen WAN. Note, however, that as soon as you associate it with one of them, you will no longer be able to associate it with the other one.

Secure Connector appliances send all traffic to the Barracuda CloudGen WAN gateway, where gateway ACLs and security/SD-WAN policies are applied.

Stand-Alone Sites Are Now Available

Barracuda CloudGen WAN now allows you to configure stand-alone sites. These sites are not connected to a gateway, or a virtual WAN in Microsoft Azure, and can be centrally managed through the Cloud Web UI. Customers only need a Barracuda Cloud Control account and must subscribe to the Barracuda CloudGen WAN service in Microsoft Azure. An existing site can be reconfigured to become a stand-alone site. Stand-alone sites support point to site.



The screenshot displays the Barracuda CloudGen WAN Cloud Web UI. The top navigation bar includes links for DASHBOARD, GATEWAYS, SITES, USERS, CUSTOM APPS, SD-WAN, SECURITY, AUDIT LOG, and SETTINGS. The user is logged in as 'guest@barracuda.com' in a 'Production' workspace. The left sidebar shows a navigation menu with DASHBOARD, SETTINGS (highlighted), RECENT CONNECTIONS, LIVE CONNECTIONS, and AUDIT LOG. The main content area is titled 'AnnArbor' and shows the 'BASIC INFORMATION' tab for a site configuration. The configuration details are as follows:

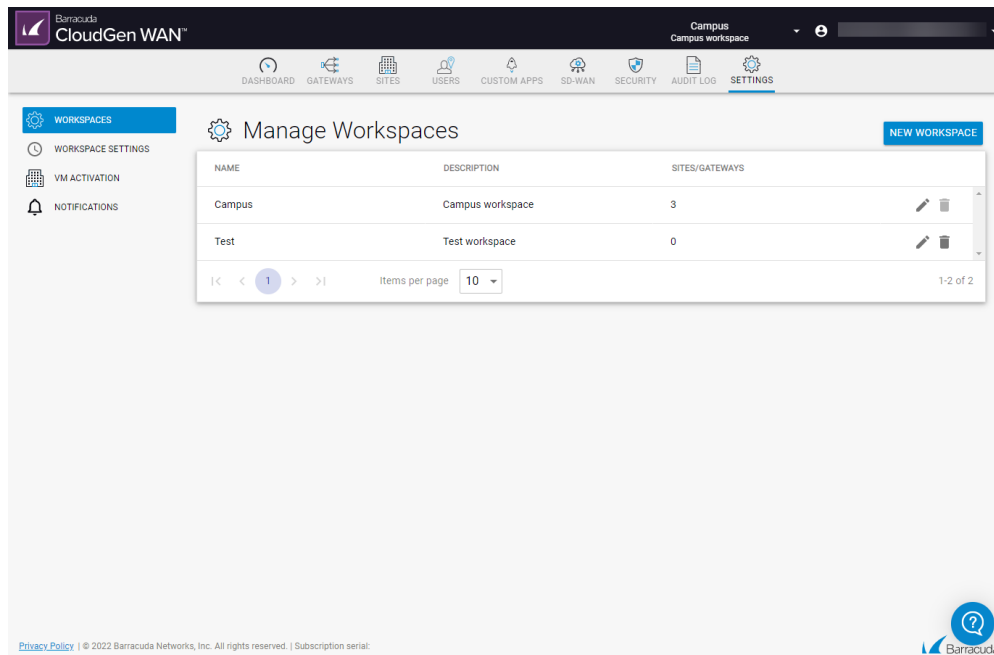
Field	Value				
Name *	AnnArbor				
Gateway	(None)				
Model	T900B				
Serial(s) *	<table border="1"><thead><tr><th>Status</th><th>Serial</th></tr></thead><tbody><tr><td>✓</td><td>543124</td></tr></tbody></table>	Status	Serial	✓	543124
Status	Serial				
✓	543124				

Below the serial list is a '+ ADD SECOND' button. At the bottom right of the configuration panel are 'RESET' and 'SAVE' buttons. The footer contains a privacy policy link, copyright information for 2022 Barracuda Networks, Inc., and a subscription serial number: 123456789.

For more information, see [How to Create a Stand-Alone Site Configuration in Barracuda CloudGen WAN](#).

Workspaces

Workspaces allow you to create configuration units that are completely independent from each other. For example, you can create a Campus workspace and an Engineering workspace where different security and SD-WAN policies are applied.



For each individual workspace, you can configure the following:

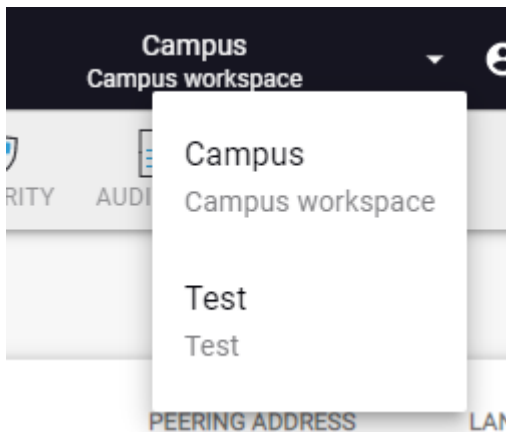
- Virtual WAN
- Gateways
- Private Cloud Edge
- Sites
- Users
- Custom apps
- SD-WAN policies
- Security policies
- Audit Log

In addition, the following workspace settings are configured for each workspace separately:

- Firmware Update Windows
- Forwarded Domains
- Log Analytics

A workspace can be connected to only one virtual WAN in Microsoft Azure.

You can easily switch between workspaces by clicking on the workspace at the top. From the drop-down menu, you can select the workspace you want.



For more information, see [Workspaces](#).

IPS

As of firmware 8.3.1, Barracuda Networks has implemented its own IPS engine, which will allow greater flexibility to address customer needs in the future. The signature database is provided by IDappcom. For more information on the signature database, see <https://www.idappcom.co.uk/>.

All false positive rules will be deleted when updating to 8.3.1 since a new set of patterns will be used.

For more information, see [IPS](#) and [Migration Notes 8.3.1](#).

Open SSL Update

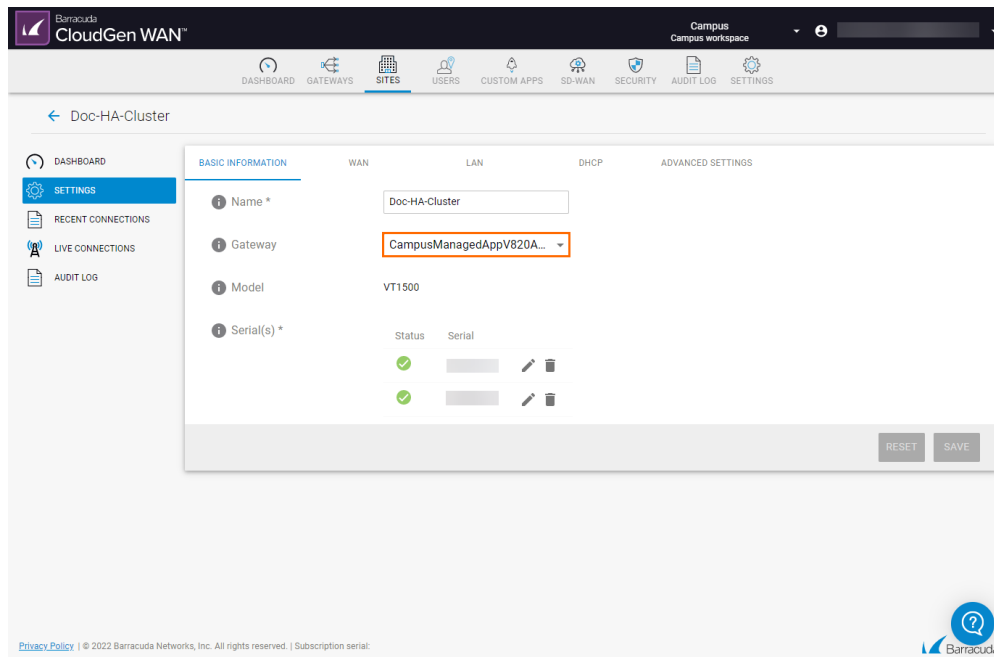
Open SSL has been updated to the newest version 3.0.1.

Routing Intent

Barracuda CloudGen WAN supports Microsoft Azure's routing intent. For more information, see <https://docs.microsoft.com/en-us/azure/virtual-wan/how-to-routing-policies>. This feature will be available in 2 to 3 weeks.

Gateway Drop-Down Menu Added in Site Configuration

Barracuda CloudGen WAN now allows you to change the gateway that a site is connected to directly in the settings of a site.



For more information, see [How to Change the Gateway of a Site](#).

Improvements Included in Version 8.3.1

- After restarting the VPN service, all BGP routes come up again as expected. BNNGF-79770
- An issue where some interfaces were not displayed has been resolved. BNNGF-79182
- A more precise text appears when hovering your mouse over a connection state. SWCS-1520
- A new connection state called "Sync" has been added. This status indicates that the connection of a high availability cluster has been synced from the primary appliance to the secondary one. SWCS-1564
- The information column of the Recent and Live connections is now displayed by default. SWCS-1619
- Azure Load Balancer probes are now handled properly. BNNGF-82114
- Unlicensed appliances now display a warning. BNNGF-77880
- The WAN hub now displays all errors correctly. BNNGF-76233
- An issue where unlicensed appliances were not provisioned has been resolved. BNNGF-76232
- Client-to-site traffic now works as expected. BNNGF-76321
- Removing old log files now works as expected. BNNGF-77020

- DHCP client leases no longer produce high memory usage. BNNGF-78135
- An issue where the firmware update took longer than 15 minutes has been resolved. BNNGF-78376
- Fixed excessive probing by site appliances for certain providers that over-provision the line.

Known Issues

- After changing the provider pinning of a WAN interface of a site, the VPN service must be restarted. BNNGF-67946
- Incoming SD-WAN connections of a private gateway always use the first WAN connection. BNNGF-84765

Available Hotfixes

Hotfix 1086 - OpenSSL 3.0.7. Affected feature is SSL Inspection where verification of X.509 certificates may cause issues during name constraint checking.

Summary:

- This hotfix updates OpenSSL to version 3.0.7
- This hotfix fixes both CVE-2022-3786 and CVE-2022-3602.

To download the package, go

to <https://dlportal.barracudanetworks.com/#/packages/5554/openssl-1086-8.3.1-167387414.tgz>.

Hotfix 1088 - Fixes issues related to reporting service for Barracuda XDR integration. BNNGF-85895

To download the package, go

to <https://dlportal.barracudanetworks.com/#/packages/5557/reporting-1088-8.3.1-170832995.tgz>.

Hotfix 1089 - Fixes a security vulnerability (reported by SEC Consult) in the local Web UI.

To download the package, go

to <https://dlportal.barracudanetworks.com/#/packages/5560/webui-sdwan-1089-8.3.1-174141891.tgz>.

This hotfix was released as a security hotfix, which means it will be automatically installed on CGW sites and gateways.

Hotfix 1092 - OpenSSL 3.0.8 update

To download the package, go

to <https://dlportal.barracudanetworks.com/#/packages/5577/openssl-1092-8.3.1-175869362.tgz>

Hotfix 1093 - Fixes compatibility issues with older hotfixes.

This cumulative hotfix includes all previous maintenance hotfixes.

To download the package, go

to <https://dlportal.barracudanetworks.com/#/packages/5581/cumulative-1093-8.3.1-176909291.tgz>

Hotfix 1094 - CVE-2022-29149 OMI vulnerability. This hotfix updates the Microsoft OMI package to version 1.7.0-0.

To download the package, go

to <https://dlportal.barracudanetworks.com/#/packages/5583/OMI-1.7.0-0-1094-8.3.1-180009149.tgz>

Migration Notes

For more information on the migration to firmware 8.3.1, see [Migration Notes 8.3.1](#).

Figures

1. existing_site_gw_none831.png
2. workspaces2_831.png
3. workspaces1_831.png
4. site_gw_drop_831.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.