

## 9.0.0 Release Notes

<https://campus.barracuda.com/doc/98207401/>

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Outdated technical features are subject to removal in order to keep the CloudGen Firewall up to date and performing properly.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Certain features will be removed completely because they have become technically obsolete; other features have become outdated and will be replaced by improved technology.

After upgrading your iOS device to iOS 17, it is not possible to connect with CudaLaunch to RDP resources!

This is a known issue and will be solved as soon as possible.

### Features No Longer Supported as of the 9.0.0 Release

#### FW Audit

As of firmware 9.0.0, FW Audit is being discontinued. If you have been using FW Audit for reporting in the past, Barracuda Networks recommends using Barracuda Firewall Insights for advanced reporting instead.

#### Web-UI

As of firmware 9.0.0, support for the Web-UI is being discontinued.

#### SMSd

As of firmware 9.0.0, the SMSd is being discontinued.

#### WANopt

As of firmware 9.0.0, WANopt is being discontinued.

## DNS Plugin

As of firmware 9.0.0, the DNS plugin has been completely removed.

## PKI (Public Key Infrastructure)

As of firmware 9.0.0, the Barracuda Firewall Control Center Public Key Infrastructure has been completely removed.

If you are still using PKI on your current firmware (earlier than 9.0.0), you must first remove all PKI configurations before upgrading to 9.0.0. Otherwise, you will not be able to upgrade to firmware release 9.0.0.

If you still need information on the PKI service for a certain reason, you can have a look at the last supported version (8.0) of this article here: [How to Configure the PKI Service](#).

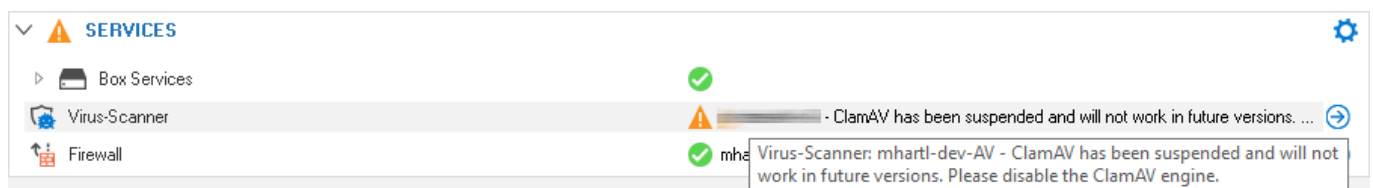
## Features that Will Become Obsolete in an Upcoming Release

### Virus Scanning with ClamAV

The Barracuda CloudGen Firewall virus scanner supports the Avira virus scanning engine. The virus scanner ClamAV will therefore become obsolete with the upcoming firmware release 9.0.1. ClamAV will then be completely removed from the firewall.

It is recommended to use only the Avira virus scanner and to disable ClamAV.

The firewall will start the service, however, the service will be highlighted with a warning notifying the customer about the deprecation.



## 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 firmware 9.0.0, Barracuda Networks recommends using at least Firewall Admin version 9.0.0. You can download this version here:

[https://dlportal.barracudanetworks.com/#/packages/5609/FirewallAdmin\\_9.0.0-277.exe](https://dlportal.barracudanetworks.com/#/packages/5609/FirewallAdmin_9.0.0-277.exe).

Due to the overall improvements in firmware release 9.0.0, Firewall Admin 9.0 no longer displays GTI for firmware versions earlier than 9.0. As of firmware release 9.0.1, this limitation has been removed.

To display GTI for firmware lower than 9.0, use the latest Firewall Admin version 8.3 instead.

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

## IMPORTANT BEFORE UPDATING

After updating a Control Center to firmware version 9.0.0, the routed VPN will fail to work due to faulty processing of the corresponding VPN configurations. [BNGF-90098]

This is a known issue and will be fixed in the upcoming release 9.0.1.

## Release Notes

Firmware version 9.0.0 is a major 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.

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.

**16.5.2023 - Hotfix 1095** - Cumulative Hotfix for release 9.0.0. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5648/cumulative-1095-9.0.0-184141413.tgz>.

**5.6.2023 - Hotfix 1098** - OpenSSL 3.0.9. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5676/openssl-1098-9.0.0-185529872.tgz>.

**20.6.2023 - Hotfix 1099** - Cumulative 9.0.0 for CloudGen Firewall and SecureEdge. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5682/cumulative-1099-9.0.0-187145908.tgz>.

**10.7.2023 - Hotfix 1101** - CloudGen Access Proxy Update. For more information, see <https://dlportal.barracudanetworks.com/#/packages/5687/CloudGen-Access-Proxy-1101-9.0.0-188116706.tgz>.

## EoL and EoS Status

For more information on which devices and services have reached EoL or EoS status, see the following:

- [Barracuda NextGen and CloudGen Firewall Appliances - EoS / EoL Definitions](#)
- [End-of-Support for CloudGen Firewall Firmware](#)

## What's New in Version 9.0.0

### VFC Models - Consolidation of Cloud/VF/SF

- VFC licenses can be used for cloud, Vx, or standard hardware installation.
- VFC models are pure service licenses without an unlimited appliance license.
- The VFC model number represents the supported number of cores (VFC1 = 1 core, VFC2 = 2 cores, ... VFC48 = 48 cores). Each VFC model handles unlimited protected IPs.
- There are two new models: VFC16 and VFC48.

The Advanced Threat Protection subscription now also works without the Malware Protection subscription added to the Energize Updates subscription. For the ATP subscription, the AV service

needs to be enabled and configured.

VFC models are pure service licenses without an unlimited appliance license. The base license expires with the EU term.

## **Backup Daemon**

The Backup Daemon is a new feature that adds to the existing options for creating and restoring backups for and from stand-alone and managed firewalls. Unlike backups stored in PAR files at a user's request, the Backup Daemon can be configured to operate autonomously at a scheduled time without any further interference. The Backup Daemon operates on the box level of an unmanaged box, a CC-managed box, and a Control Center, and must always be configured on the box level.

The Backup Daemon can create backups of the firewall configurations on the box level, on the CC level, and box & CC levels.

For more information, see [Backup Daemon](#).

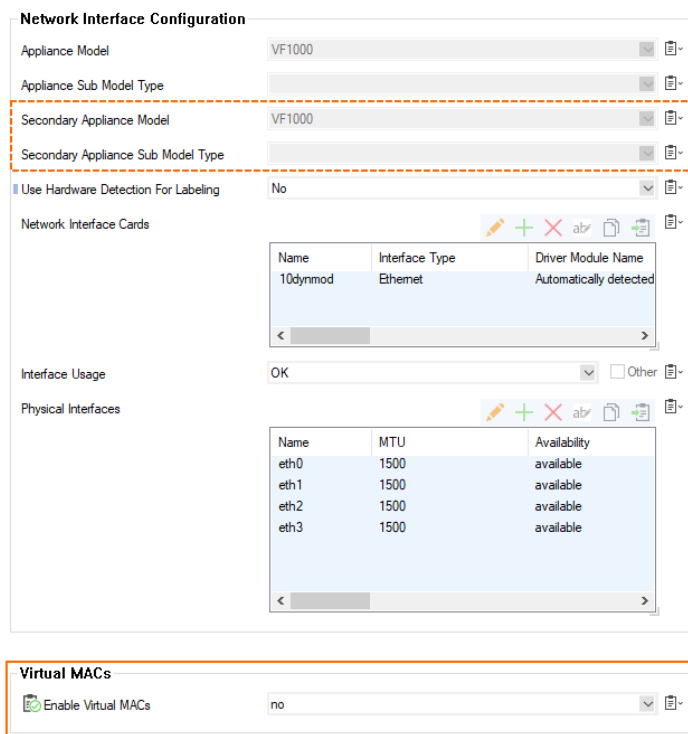
## **RCS Improvements**

The Revision Control System (RCS) has been improved and now considers GTI. The Configuration Templates framework now can read the differences between ConfTemplates and instances in the RCS. When jumping forth and back between revisions, certificate references are re-established as expected. Also, the RCS now fully supports the logging of all VPN parameters.

## **Virtual MAC Addresses**

The availability of an HA pair of CloudGen Firewalls can be compromised in networks where switches block ARP packets or where industrial TCP/IP stacks cannot send ARP packets for service IP addresses.

In order to be able to operate HA firewalls in such critical infrastructures, the application of virtual MAC addresses on an HA pair of CloudGen Firewalls now improves the overall availability.



**Network Interface Configuration**

Appliance Model: VF1000

Appliance Sub Model Type:

Secondary Appliance Model: VF1000

Secondary Appliance Sub Model Type:

Use Hardware Detection For Labeling: No

Network Interface Cards

Name	Interface Type	Driver Module Name
10dynmod	Ethernet	Automatically detected

Interface Usage: OK

Physical Interfaces

Name	MTU	Availability
eth0	1500	available
eth1	1500	available
eth2	1500	available
eth3	1500	available

Virtual MACs

Enable Virtual MACs: no

For more information, see [Virtual MAC Addresses](#).

### Automated Security Updates

Automated Security Updates is a new feature that allows you to configure the execution of scheduled firmware updates and is already activated on firmware 9.0.0. The feature runs on Control Centers and managed and stand-alone firewalls. Running the feature on the box level of a Control Center is the same as running the feature on a stand-alone firewall.

When logging into a firewall or Control Center with firmware 9.0.0 for the first time, you will be presented with a notification window informing you that Automated Security Updates is enabled by default. The window also contains information on where to disable the feature and where to change the configuration settings depending on the type of appliance.

For more information, see [Automated Critical Updates](#).

### Web Categorization Services (WCS) - Changes for URL Filters

Due to WCS upgrades, some URL Filter categories have changed. Barracuda Networks recommends checking your configuration if you are using URL Filters. In addition to improved efficacy, WCS 3.2 provides more categories that allow you to configure and refine even more granular URL policies.

The following URL Filter categories will no longer be used and will be completely removed:

- Streaming-radio-TV
- Messaging
- Moderated-forums
- Comics-humor-jokes
- Digital-cards
- Illegal-software
- Academic-cheating
- Text-audio-only
- Extremely-offensive
- Gambling-related
- Game-cartoon-violence
- Historical-opinion
- Incidental-nudity
- Profanity
- Proxy utilities
- Information-security
- Suspicious-sites
- Interactive-web-applications
- Resource-sharing
- Technical-information
- URL-redirectors

### Installation of Firmware Updates Using SSH

Manually updating a new firmware version via SSH now requires explicitly passing the path to the package.























For more information, see [How to Install Updates via SSH](#).

### New Fields for the BGP Router Service

New configuration fields have been added to the BGP configuration window at **CONFIGURATION > Configuration Tree > Assigned Services > OSPF/RIP/BGP Settings > Neighbor Setup IPv4**, window **Neighbors**, section **BGP Parameters**.

1. The field **Allow AS-in** has been added to the BGP configuration in order to allow neighbors to inject routes when AS (Autonomous System) numbers are identical.
2. The field **ttl-security** enforces the Generalized TTL Security Mechanism (GTSM), as specified in RFC 5082. Only neighbors that are the specified number of hops away will be allowed to become neighbors. This command is mutually exclusive with EGBP-multihop.

**BGP Parameters**

AS Number	<input type="text"/>	
Description	<input type="text"/>	
Neighbor Password	New <input type="text"/> Confirm <input type="text"/> Strength <input type="text"/>	
Route Reflector Client	no 	
Peer Group Affiliation	<input type="text"/>	
Update Source	No 	
Update Source Interface	<input type="text"/>	
Update Source IPv4 Address	<input type="text"/>	
Peer Filtering For Input	<input type="button" value="Set..."/> <input type="button" value="Clear"/> NOTSET: No section present	
Peer Filtering For Output	<input type="button" value="Set..."/> <input type="button" value="Clear"/> NOTSET: No section present	
Enable BFD	no 	
Advanced BFD Settings	<input type="button" value="Edit..."/> <input type="button" value="Clear"/> Disabled	
Next Hop Self	no 	
AllowAS-in	<input type="text"/>	
EBGP Multihop	<input type="text"/>	
ttl-security	<input type="text"/>	
Port	<input type="text"/>	
Weight	<input type="text"/>	

These fields are accessible in Firewall Admin only in Advanced mode.

### HTTP/2 for CloudGen Firewall

The CloudGen Firewall fully supports HTTP/2 data streams. The following firewall features now cover the HTTP/2 standard:

- Application Control
- SSL Inspection
- URL filtering
- Virus scanning
- Content detection
- Archive scanning
- Google account control
- Search string logging
- Safe search

Note that ATP currently only supports "Deliver first, then scan" for HTTP/2.

### Clone Wizard Improvements

An appliance can now be cloned into another target cluster while considering certain 'names' configured by the user.

For more information, see [How to Add a New/Clone an Existing CloudGen Firewall to/in the Control](#)



[Center](#).

## **RSA-ACE SecurID Authentication**

The configuration method and the related user interface for RSA-ACE SecurID Authentication have been reworked.

This firmware includes improvements for RSA-ACE SecurID authentication. The underlying change requires a new configuration of the RSA-ACE authentication settings after upgrading to firmware 9.0.0!

For more information, see [How to Configure RSA-ACE SecurID Authentication](#).

## **ConfTemplates Improvements**

The configuration templates have been improved and include multiple new ConfTemplate units. For example, these new ConfTemplate units not only support among many others configuring networks, routes, VLANs, or authentication but now also cover new features developed for release 9.0.0 like Automated Security Updates or the Backup Daemon.

Also, a new pool object has been created to support the automated allocation of VIPs and MIPs in conjunction with ConfTemplates.

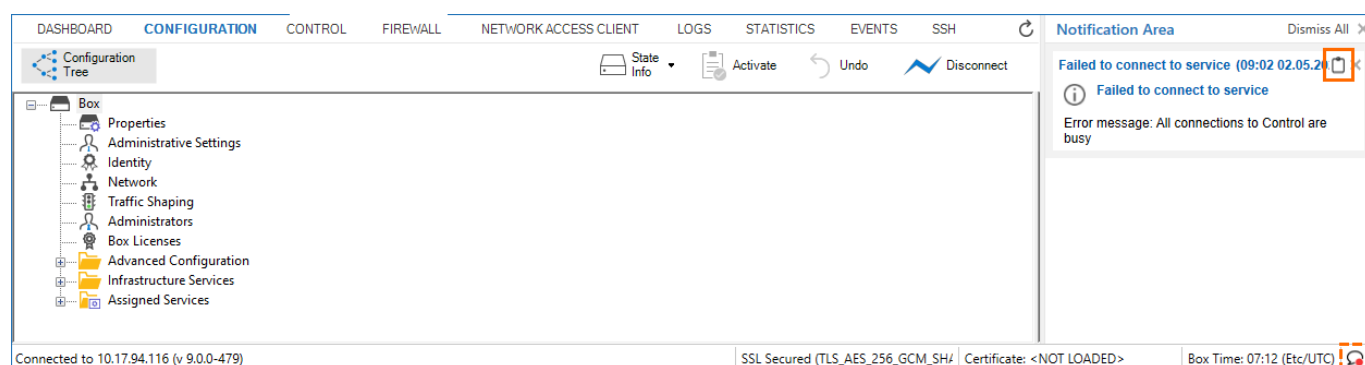
For more information, see [Configuration Templates](#).

## **Status Map**

In certain situations, the Status Map did not show the correct configuration status of a managed box. This issue has been solved, and the Status Map is now in sync with all managed boxes. The icon in the Status Map now shows the correct state of the managed box.


## **Copying Messages from the Notification Area in Firewall Admin**

It is now possible to copy messages from the notification area in Firewall Admin. Available messages will be indicated in the lower right corner with a tiny red bullet. Clicking this icon will open the notification area and expose the messages. If you want to copy a message, click the tiny clipboard symbol in the right upper corner. Firewall Admin will then put a formatted copy of the message into the clipboard that you can then use in any other text-based application.



## Zero Touch Deployment

The zero-touch daemon has become a dedicated box service. Like all other services, this ZTD service can now be started, stopped, restarted, and blocked, and no longer requires command-line interaction.

 Zero Touch Deployment

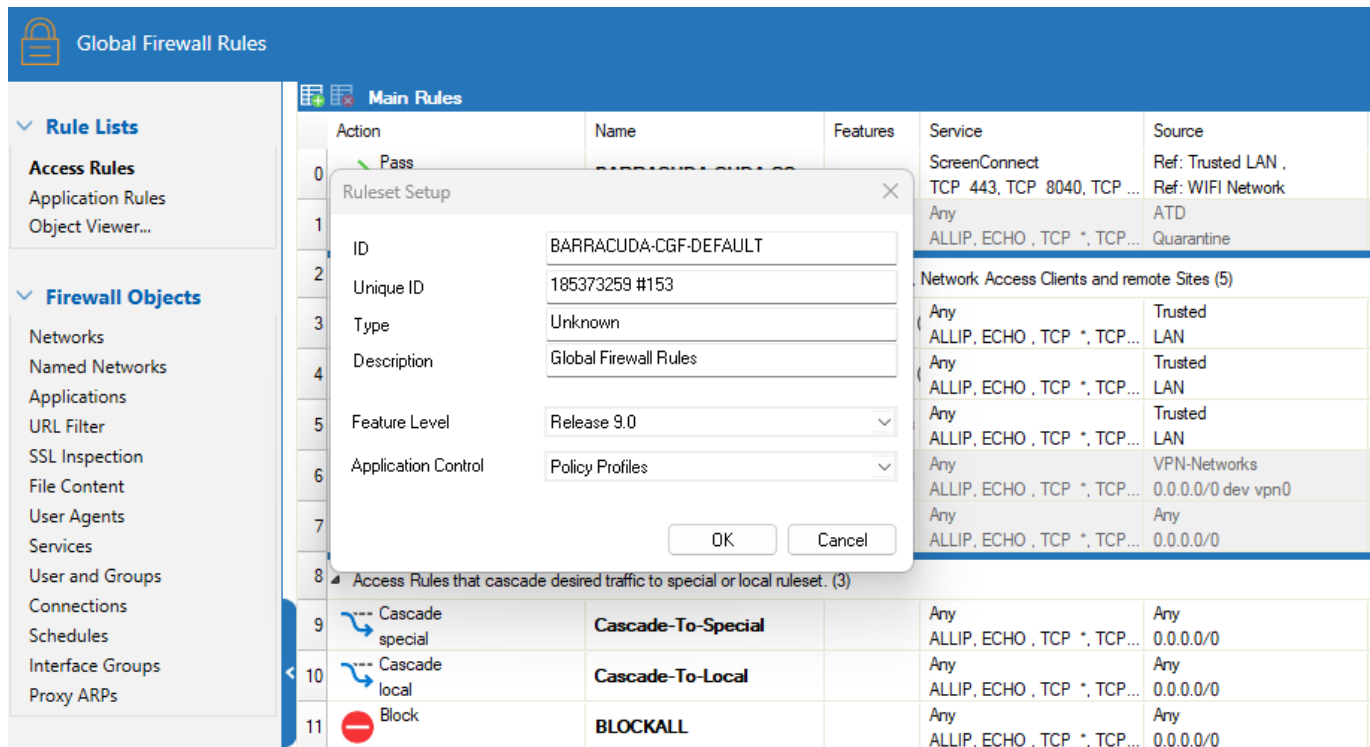
 ztd



For more information, see [Services Page](#).

## CGF Policy Profiles

As of Barracuda CloudGen Firewall release 9.0.0, it is possible to enable Policy Profiles for rule sets on the Distributed Firewall. When switching to Policy Profiles, all local and special rule sets are set to use policies as well. For more information, see [Policy Profiles](#).



**Global Firewall Rules**

**Rule Lists**

- Access Rules
- Application Rules
- Object Viewer...

**Firewall Objects**

- Networks
- Named Networks
- Applications
- URL Filter
- SSL Inspection
- File Content
- User Agents
- Services
- User and Groups
- Connections
- Schedules
- Interface Groups
- Proxy ARPs

**Main Rules**

Action	Name	Features	Service	Source
0 Pass	BARRACUDA-CGF-DEFAULT		ScreenConnect	Ref: Trusted LAN ,
1			TCP 443, TCP 8040, TCP ...	Ref: WIFI Network
2			Any	ATD
3			ALLIP, ECHO , TCP *, TCP...	Quarantine
4				
5				
6				
7				
8				
9				
10				
11				

**Ruleset Setup**

ID: BARRACUDA-CGF-DEFAULT

Unique ID: 185373259 #153

Type: Unknown

Description: Global Firewall Rules

Feature Level: Release 9.0

Application Control: Policy Profiles

OK Cancel

Access Rules that cascade desired traffic to special or local ruleset. (3)

Action	Name	Features	Service	Source
9 Cascade special	Cascade-To-Special		Any	Any
10 Cascade local	Cascade-To-Local		Any	Any
11 Block	BLOCKALL		Any	Any

## License Update Improvements

Control Center-managed CloudGen Firewalls receive automatic license and configuration updates. With unattended license renewal, new pool licenses are automatically downloaded to the Control Center and then installed on all managed firewalls using this license.

In this release, the performance has been improved.

For more information, see [Licensing CloudGen Firewalls in the Control Center](#).

## Bridging

Shared IP addresses and management IP addresses are automatically added to the bridge device as soon as the hosting interface is added to a bridge.

For more information, see [How to Configure Routed Layer 2 Bridging](#).

## VPN

The user interface for the TINA VPN tunnel settings has been improved.

For more information, see [How to Create a TINA VPN Tunnel between CloudGen Firewalls](#) and [How to Configure a Routed VPN Network](#).

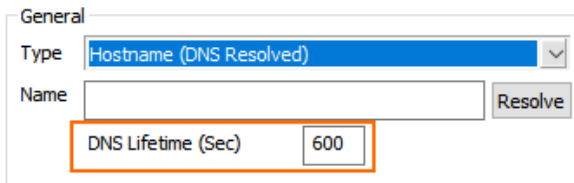
## Naming of Certificates in the User Interface

The name "Root Certificate(s)" has been replaced with the name "CA Certificate(s)" in certain configuration windows and display areas.

## Network Object for "Hostname (DNS Resolved)"

For feature level  $\geq 9.0$ , the edit field for **DNS Lifetime** in the window for creating a new network object of the type **Hostname (DNS Resolved)** will no longer be available.

Edit/Create Network Object



## Improvements Included in Version 9.0.0

### Appliances

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

### Authentication

- Domain join with SMBv2 now works as expected. [BNNGF-76010]
- SAML authentication metadata is now generated correctly for a managed box. [BNNGF-76521]
- Using special characters in the **Group Pattern** field of the **Group Policy Condition** no longer causes an issue when logging in. [BNNGF-76804]
- 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]
- The mail template in the TOTP Bulk Enrollment settings can be changed as expected. [BNNGF-81664]
- The maximum timeout for TACACS+ has been increased to 45 seconds. [BNNGF-82350]
- Client-to-site security policy exception no longer occurs on Mac OS Monterey systems in certain situations. [BNNGF-83076]
- A list view for Group File Patterns has been added to the section **Attributes** at **CONFIGURATION > Configuration Tree > Box > Infrastructure Service > Authentication Service > SAML/ADFS Authentication**. [BNNGF-83348]
- It is now possible to preselect an authentication scheme for CC Template Admins. [BNNGF-83910]
- Authentication sync now works as expected. [BNNGF-84440]

- The IKEv2 RADIUS authentication now works as expected with user info helper schemes enabled. [BNNGF-84571]
- Filters allow the use of SAML group information also in case of users with a very large number of group affiliations. [BNNGF-85601]
- When group caching is enabled, authentication via MSAD now works as expected. [BNNGF-87091]

### Barracuda Firewall Admin

- For compatibility reasons, it is no longer possible to open a DNS 7.x node in Firewall Admin 9.0. Firewall Admin 9.0 will display an appropriate notification in a window. [BNNGF-77636]
- 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 the 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]
- The feature for expanding nodes now also works for workspaces. [BNNGF-81681]
- 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]
- The edit field and the label for **DNS Resolve IPs** have been removed from **CONFIGURATION > Configuration Tree > Infrastructure Service > General Firewall Configuration > Firewall History**, section **Firewall History Limits**. Also, when right-clicking the mouse button in the table at **FIREWALL > History**, the list entry **Show Hostnames** that is displayed in the pop-up menu has been removed. [BNNGF-83111]
- When bulk-assigning licenses, HA clusters are now shown as 1 unit, and the count numbers are now calculated correctly. [BNNGF-83190]
- When using IPsec settings for client-to-site configurations, Firewall Admin no longer crashes in certain situations. [BNNGF-83373]
- When exporting a client-to-site VPN profile, it is now possible to select the authentication method SAML. [BNNGF-83378]
- The option **Transform virtual server into assigned service node** is now displayed as expected when clicking the appropriate configuration tree node. [BNNGF-83492]

- The view of **CONTROL > Network** now builds up with the expected standard speed and no longer causes long loading times with active BGP. [BNNGF-84037]
- CC administrators with an 'operator' role are now allowed to create par files and push configurations to **Zero Touch**. [BNNGF-84058]
- It is now possible to copy messages from the notification area in Firewall Admin. [BNNGF-84282]
- Labels for site-to-site QoS policies have been equalized in Barracuda Firewall Admin. [BNNGF-84322]
- Firewall Admin will show a notification pop-up window upon the first opening of a 9.0.0 appliance. [BNNGF-84498]
- A new optional column **Matching Application** has been added to SD-WAN to see which applications are used for SD-WAN. [BNNGF-84577]
- When starting the GTI editor the first time, there is now an empty group present, and all services are displayed. [BNNGF-84625]
- The column **Output IF** in Firewall Admin > **Firewall History**, now displays correct values. [BNNGF-84626]
- The **Remote Networks** list in the VPN site-to-site tunnel configuration list now displays correct netmasks. [BNNGF-84745]
- The ZTD service is called **Zero Touch Deployment** in the list view at **CONTROL > Service > Box Services**. [BNNGF-84777]
- Barracuda Firewall Admin no longer crashes in certain situations. [BNNGF-84792]
- The columns for **Primary Server** and **Secondary Server** have been removed from the firmware update view. [BNNGF-84797]
- The cluster report window is now resizable and displays cluster RCS reports for all nodes. [BNNGF-85206]
- Correctly enabled dynamic rules in a c-firewall's local and special ruleset now match as expected. [BNNGF-86072]
- WanOpt has been removed from GTI. [BNNGF-87027]
- The visibility of referenced policies in the managed box firewall tab has been optimized. [BNNGF-88425]
- Copying an IP address from a firewall rule using the **Copy <IP> to Clipboard** feature and applying it as a filter in the **Firewall View** (live or history) now works as expected. [BNNGF-88674]
- Firewall Admin 9.0 no longer displays GTI for firmware versions earlier than 9.0. [BNNGF-89002]

## Barracuda OS

- The Backup Daemon is a feature for scheduling backups on local and remote storage by configuration. [BNNGF-65796]
- BGP now works as expected for IPv6. [BNNGF-69299]
- RCS now works as expected after importing an archive.par file. [BNNGF-70065]
- BGP IPv6 neighbors are added to the IPv6 unicast address family as expected. [BNNGF-70437]
- DHCP relay now uses the correct type of IP address and works as expected. [BNNGF-71929]
- The bond interface no longer changes to interface 'e1' and the config for the secondary box can now be activated. [BNNGF-75351]

- MSAD traffic will no longer be detected as BitTorrent. [BNNGF-75606]
- Connection failover for UDP and ESP traffic has been improved. [BNNGF-76131]
- The BFD process now continues running and no longer restarts when BFD settings are updated on the fly. [BNNGF-76921]
- The **Model** label on the **CONTROL > Services** page is now displayed as expected. [BNNGF-78300]
- The integrity check logic now works as expected if a default route via shared IP is configured. [BNNGF-78794]
- The bridge no longer stops working unexpectedly in certain situations. [BNNGF-78802]
- 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]
- When downloading firmware packages on a Control Center, hotfixes are now also considered that address non-Control Centers. [BNNGF-79842]
- In rare cases, calculations caused blocked sessions that 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]
- Changing into the 'home directory' no longer causes permission errors. [BNNGF-81081]
- SNMP no longer crashes in certain situations. [BNNGF-81130]
- Block pages are now also injected into plaintext HTTP sessions that are routed between VRF instances. [BNNGF-81198]
- When the number of sessions exceeds approximately 500, the Envoy Proxy no longer terminates the sessions. [BNNGF-81285]
- The handling of IPv6 routes that are obtained through SLAAC has been improved. [BNNGF-81574]
- Gateway probing is now terminated after a route is removed. [BNNGF-81668]
- 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]
- It is now possible to change rule sets for managed firewalls operating with the 3-layer server-service architecture. [BNNGF-82830]
- Security measures have been taken for CVE-2022-0847. [BNNGF-82852]
- Cloud-info error messages no longer occur on hardware devices if they operate outside of a cloud. [BNNGF-82897]
- 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]
- A new configuration field **Allow AS-in** has been added to the BGP configuration window at **CONFIGURATION > Configuration Tree > Assigned Services > OSPF/RIP/BGP Settings > Neighbor Setup IPv4**, window **Neighbors**, section **BGP Parameters**, in order to allow neighbors to inject routes when AS (Autonomous System) numbers are identical. [BNNGF-83100]



- Connection objects are applied as expected when using network interfaces. [BNNGF-83146]
- A new field **ttl-security** has been added to the BGP configuration window at **CONFIGURATION > Configuration Tree > Assigned Services > OSPF/RIP/BGP Settings > Neighbor Setup IPv4**, window **Neighbors**, section **BGP Parameters** in order to enforce **Generalized TTL Security Mechanism (GTSM)** as specified in RFC 5082. [BNNGF-83179]
- Mounting the CIFS file system now works as expected. [BNNGF-83182]
- FRR (Fast ReRouting) has been updated to the newest version. [BNNGF-83529]
- The SSH update tool **phionUpdate** has been replaced by a new tool **installUpdate**. [BNNGF-83666]
- The IPv6 auto-configuration no longer causes issues in certain situations. [BNNGF-83906]
- DHCP links are no longer disconnected in certain situations. [BNNGF-84039]
- Cooking statistics no longer cause issues in certain situations. [BNNGF-84065]
- The bsnmd no longer consumes available CPU time in certain situations. [BNNGF-84173]
- The network mask of a shared IP on a bridged device is now applied correctly. [BNNGF-84213]
- The systemd no longer causes spikes every 10 seconds. [BNNGF-84674]
- The number of routes within a source-based table no longer flaps between 0 and another value. [BNNGF-84844]
- The GUI-to-text is now updated if the text-based config is disabled and the user interface config is used. [BNNGF-84845]
- The firewall no longer crashes in certain situations. [BNNGF-84847]
- Hotfixes that are included in other hotfixes are now also visible at **DASHBOARD > UPDATES > Installed** as expected. [BNNGF-85235]
- Modems now connect as expected. [BNNGF-85283]
- SNMP errors no longer flood the log and are now handled as 'information'. [BNNGF-85479]
- SNMPv3 is no longer blocked by the default ruleset. [BNNGF-85811]
- OSPF routes are now introduced at the configured routing table. [BNNGF-85986]
- After a network activation, the OSPF routing table is now in place as expected. [BNNGF-85987]
- If a new route is learned on one daemon and already exists in the system, it will now be replaced with a new route of a favorable metric. [BNNGF-87041]
- The Barracuda Reporting Server daemon now increases the time between retries if the connection can't be established. [BNNGF-87177]
- The access control service no longer causes restart loops. [BNNGF-87475]
- The creation of a system report now works as expected. [BNNGF-87497]
- Firewalls no longer send data if **Firewall Insights** does not respond. [BNNGF-87850]
- The user interface has been updated and now reflects 'CA' instead of 'Certificate / Root' for certificate-related labels. [BNNGF-87882], [BNNGF-87883]
- Source-based thrown boot routes are no longer removed with a soft activation. [BNNGF-87926]
- The provider name for WiFi is now handled as expected. [BNNGF-90954]

#### Cloud General

- Domain resolutions that are negatively answered will no longer be cached and will therefore improve the responding quality of the DNS server. [BNNGF-86349]



## Cloud Azure

- A failure to create the O365 network object is now handled as a warning. [BNNGF-83139]

## Cloud Google

- When deploying a new CGF in the Google Cloud, ssh public keys are set considering both the Google standard for project-wide ssh keys and individual custom keys. [BNNGF-88599]

## ConfTemplates

- After creating an SC box with ConfTemplates, the SC firmware update over CC now works as expected. [BNNGF-88646 ]

## Control Center

- A CC PAR file now contains remote execution scripts as expected. [BNNGF-75619]
- Certificate references are no longer lost in the Certificate Store when jumping between revisions in the RCS. [BNNGF-75675]
- When a vendor ID is converted from IP to hexadecimal, the colon character is no longer appended to the end of the string. [BNNGF-76967]
- 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]
- The Clone Box wizard now works with multiple default routes as expected. [BNNGF-80736]
- Overrides in linked repository nodes for the Authentication Service now work as expected. [BNNGF-80853]
- After configuration changes, a bogus "default box" is no longer displayed in the CC status map. [BNNGF-81019]
- The edit fields **Naming Replace From** and **Naming Replace To** have been added to the Clone Box wizard to move a service from a box in one certain cluster to a box in another cluster. [BNNGF-81362]
- The policy server no longer throws 802.1x error messages if not applicable. [BNNGF-81368]
- A new firewall object of type **MSP Pool** has been created that will make the assignment of VIPs/MIPs for MSPs easier. [BNNGF-82784]
- The CC license update log no longer contains unreasonable "SQL logic error or missing database" messages. [BNNGF-82937]
- Information about firmware updates for managed boxes is now updated correctly on Control Centers with firmware 8.2.1. [BNNGF-82938]
- RCS now shows changes from external LDAP admins as expected. [BNNGF-83186]
- ZTD is now displayed as a service in **CONTROL > Services > Box Services** and now can be started/stopped/restarted/blocked in the associated drop-down menu. [BNNGF-84740]
- Range-level CC admins can now kill the session of other range admins as expected. [BNNGF-84843]
- When trying to determine the boxes in a cluster, the related REST call no longer runs into any issues. [BNNGF-84899]

- IPS pattern updates now work as expected on HA firewalls. [BNNGF-85478]
- The authentication sync in a thrust zone now works correctly on a secondary box of an HA pair. [BNNGF-86590]
- Boxes now show up correctly on the Status Map. [BNNGF-87058]
- In case of a pool license being used only for one firewall of a high availability cluster, the pool license is now only assigned to that single HA partner in case of a license update. [BNNGF-87476]

## DHCP

- BOOTREPLY messages are now processed as expected after the DHCP relay service is restarted following a complete configuration update. [BNNGF-81966]
- The DHCP service now sends dynamic DNS updates in simple mode as expected. [BNNGF-83023]
- A new option with the name 'standard' has been added to the menu list for **DNS Update Scheme** at **CONFIGURATION > Configuration Tree > Assigned Services > DHCP Enterprise Configuration > Address Pools > DNS Update Configuration**. [BNNGF-83041]

## DNS

- By manually configuring the appropriate source IP addresses, multiple DNS services now work as expected. [BNNGF-78289]
- DNS query rotation now works for all configured DNS servers at **Administrative Settings > DNS Settings**. [BNNGF-81504]
- 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

- IPv6 IPS exception handling now works as expected. [BNNGF-36763]
- The Firewall Live view shows traffic throughput as expected. [BNNGF-79451]
- Salesforce traffic is now recognized correctly. [BNNGF-83185]
- The firewall no longer freezes when using IPS for UDP. [BNNGF-83189]
- Klog no longer fills up with call traces every few seconds. [BNNGF-83500]
- The setting for SSL Inspection no longer displays the wrong status if the configuration is set to **Auto** in the security policy. [BNNGF-83584]
- F Secure AV updates are now correctly detected as what they are. [BNNGF-83908]
- The Swish FTP client is now correctly detected. [BNNGF-83909]
- Offline authentication no longer times out. [BNNGF-84035]
- A backslash in a username is now correctly evaluated in a rule set and sessions are therefore no longer blocked. [BNNGF-84163]
- The firewall no longer crashes during TFTP file transfers in certain situations. [BNNGF-84256]
- Applications are now blocked as expected. [BNNGF-84432]
- When using Offline Firewall Authentication, the correct page logo is now displayed. [BNNGF-84564]

- Protocol matching now works with policies as expected. [BNNGF-85031]
- Offline authentication no longer times out. [BNNGF-85166]
- SNAT now works as expected for an HA partner in a CloudGen WAN setup. [BNNGF-85379]
- The firewall no longer crashes when applying URL categorization to IPv6 traffic. [BNNGF-85473]
- The device filter **Any Interface** now works as expected in **FIREWALL > Live**. [BNNGF-85689]
- In very rare cases, data was not sent to the FW activity log. [BNNGF-85755]
- DST NAT now handles all entries for redirection as expected. [BNNGF-85904]
- The firewall no longer crashes on LOUT if webmsg - syslog traffic is being shaped. [BNNGF-86134]
- Unused categories have been removed from the Web Coverage System (WCS). [BNNGF-86363]
- Sporadic crashes with application detection no longer occur in certain situations. [BNNGF-86561]
- DST NAT and policies no longer cause erroneous app-ruleset evaluation. [BNNGF-86080]
- Traffic shaping no longer causes the firewall to stall into a soft lock of all CPUs. [BNNGF-86654]
- Team Viewer version 15 is now blocked if an application rule is set on the Firewall for the fixed version. [BNNGF-87108]
- When SSL inspection is enabled, establishing sessions now works as expected. [BNNGF-87144]
- The system is no longer deadlocked on memory in certain situations. [BNNGF-87817]
- The firewall now handles ONCRPC packets correctly and works as expected. [BNNGF-87935]
- The TLSv1.1 is not used anymore if **Restrict Strong Ciphers Only** is chosen. [BNNGF-87939]
- The firewall log no longer contains messages like "App Connect Socket received invalid len=44". [BNNGF-87941]
- URLcat now works as expected with ports other than https 443. [BNNGF-88028]
- Traffic redirected to destination 0.0.0.0/0 will never be sink-holed. [BNNGF-88289]
- The **Schedule** firewall object works as expected. [BNNGF-88562]

## HTTP Proxy

- The HTTP proxy now starts successfully after a failover even if SSL Inspection is enabled and if there are duplicate sub-domains configured for exclusion. [BNNGF-80253]
- The HTTP proxy no longer experiences memory leaks in certain situations. [BNNGF-80387]
- The reverse proxy exchange authentication now works as expected. [BNNGF-81512]
- The proxy service no longer causes segmentation faults after transforming a box to operate the new 2-layer service architecture (Assigned Services). [BNNGF-83509]
- The traffic throughput of the reverse proxy now works as expected after a firmware update. [BNNGF-84038]

## REST

- The REST endpoints now also show the in/out bytes and packets separately. [BNNGF-76915]

- CC Admins with ACL no longer get 403 errors on certain REST API paths in certain situations. [BNNGF-80340]
- The 'Firewall Rule' REST API has been extended and now allows you to assign custom user objects. [BNNGF-82343]
- Support for global user objects has been added to REST. [BNNGF-84109]
- The REST API has been updated to provide all necessary information from the Status Map on a Control Center. [BNNGF-86060]
- The REST API queries now work as expected for LDAP and MSAD. [BNNGF-87508]
- A configuration change on a firewall rule set via REST now correctly adapts the ruleset ID. [BNNGF-88263]

## Virus Scanner

- The AV service no longer shows erroneous warnings in certain situations. [BNNGF-84301]
- The firewall currently only supports "Deliver first, then scan" for HTTP/2. [BNNGF-87349]
- A notification window is displayed that informs the user that ClamAV is deprecated, and an event will be created. [BNNGF-88471]

## VPN

- Strongswan will be activated only upon a configuration change and only if IKEv2 site-to-site OR/AND client-to-site are configured. [BNNGF-52334]
- If **HA Tunnel Sync** is enabled in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings**, a VPN tunnel now works as expected when an HA failover is initiated. [BNNGF-54419]
- If pre-authentication fails, logging in with a username in the VPN client will display an error message. [BNNGF-67672]
- Client-to-site connection no longer fails with capital letters in the certificate. [BNNGF-75138]
- Configured IKEv1 routes will no longer be introduced into the main routing table, but rather be handled as source routes. [BNNGF-78903]
- Downloading the CRL file now works as expected. [BNNGF-80823]
- IKEv2 memory leaks no longer occur when establishing VPN tunnels/transport. [BNNGF-81077]
- The 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]
- A rare cause for an issue with loss of all VPN tunnels for a GTI configuration has been fixed where the option **Dedicated Secondary Config** was active in **Properties > Operational**, triggered by box network configuration changes. This only affected box server setups. [BNNGF-83380]
- When IKEv2 uses RADIUS for authentication, it now uses the timeout values from the authentication service. [BNNGF-84576]
- SC networks are now introduced into VPN table 5 as expected. [BNNGF-84737]

- VPN tunnels no longer flap during rekeying. [BNNGF-85519]
- Memory issues no longer occur if a bulk transport is configured as a routing transport. [BNNGF-86074]
- IKEv2 phase 2 rekeying is now handled correctly. [BNNGF-86223]
- A regression has been fixed that caused IPSec tunnels to show reverse routing interface mismatch with the option **Add VPN routes to main table routing** enabled, depending on whether there were two overlapping destination networks. This affected IKEv2 with an additionally enabled option **One VPN Tunnel per Subnet Pair**, and IKEv1 in general, in both cases only with the main table routing option enabled. [BNNGF-86389]
- The QoS band is now shown in the Live View as expected. [BNNGF-86661]
- Buffer overflows are no longer occurring in the VPN log. [BNNGF-87645]

#### Known Issues

- **Barracuda OS** – When configuring a server IP for the tun1 interface in the **Shared Networks and IPs** section at **CONFIGURATION > Configuration Tree > Network**, the network activation does not work. [BNNGF-89085]
- **Barracuda OS** – If a QoS profile has been created and assigned to a physical interface, this profile will be automatically overwritten by the simple QoS band when performing an HA failover or deleting the VPN tunnel assigned to this physical interface. [BNNGF-90831]
- **Barracuda OS** – The authentication service phibs does not start after updating to version 9.0.0. [BNNGF-90848]  
As a workaround, restart the firewall after updating to version 9.0.0.
- **BarracudaOS** – Client-to-site connections to a firewall with a new VFC license currently fail due to a licensing issue. [BNNGF-90920]
- **BarracudaOS** – Special characters are not processed correctly when using the RADIUS authentication scheme. [BNNGF-90980]
- **Control Center** – Licenses are not correctly displayed for HA pairs in the Control Center. [BNNGF-84394]
- **Firewall** – Inspecting traffic for QUIC / UDP 443 is currently not supported. [BNNGF-74540]
- **Firewall** – ATP "Scan-first-then-deliver" no longer works as soon as HTTP2 is allowed. [BNNGF-87349]
- **Policy Policies** – Trusted LAN rules do not match when used in the IPS, malware, and TLS policies. [BNNGF-89593]
- **SSL-VPN and CudaLaunch** – Shared folders are no longer accessible via CudaLaunch. [BNNGS-3970]
- **Telemetry** – For managed firewalls note that settings displayed in the UI on the Control Center and the managed box can differ depending on the cluster and firmware version. [BNNGF-89044]
- **vMAC (Virtual MAC addresses)** – Swapping of MAC addresses during an HA failover does currently not work for bonded interfaces. [BNNGF-89137]
- **VPN** – Dynmesh tunnels do not get established when both sites are behind a NAT after updating to 9.0.0. [BNNGF-90377]
- **VPN** – After updating a Control Center to firmware version 9.0.0, the routed VPN will fail to work due to faulty processing of the corresponding VPN configurations. [BNNGF-90098]
- **CudaLaunch** – After upgrading your iOS device to iOS 17, it is not possible to connect with

CudaLaunch to RDP resources. [BNNGS-3975]

- **Firewall - App-Detection** - Initially failing app detection or invalid TLS certificate due to large Client Hello

Certain browsers force the use of Kyber, a post-quantum key agreement algorithm, in TLS. In turn, the Client Hello gets unusually large and initially might cause app detection to fail or an invalid TLS certificate for TLS inspection. After a page refresh in the browser, the app is detected correctly and the TLS certificate is valid.

A workaround is to disable the flag "TLS 1.3 hybridized Kyber support" / X25519Kyber768 in Google Chrome (<chrome://flags/>), Microsoft Edge (<edge://flags/>), and "security.tls.enable\_kyber" in Firefox (about:config).

For Google Chrome and Chrome OS there is also a policy that can alternatively be used to control this flag. See

<https://chromeenterprise.google/policies/#PostQuantumKeyAgreementEnabled>.

[BNNGF-93365]

## Figures

1. virus\_scanner\_removal\_user\_notification\_window.png
2. vMAC\_HA\_paired\_firewall.png
3. bpg\_parameters\_new\_two\_fields.png
4. fwa\_copying\_from\_notification\_area.png
5. ztd\_box\_level\_service\_entry.png
6. pol\_casc.png
7. network\_object\_no\_edit\_field\_for\_DNS\_lifetime\_feature\_level.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.