Release Notes 6.0.1

https://campus.barracuda.com/doc/45024313/

Barracuda Networks recommends to always install the latest firmware release of the major version to benefit from the latest security and stability improvements.

This firmware version includes a critical security issue resolved by installing Hotfix 837. For more information, see Hotfix 837 - Security Issue.

Before installing the new firmware version, back up your configuration and read all of the release notes that apply to the versions that are more current than the version that is running on your system.

Do not manually reboot your system at any time while the update is in process, unless otherwise instructed by Barracuda Networks Technical Support. Depending on your current firmware version and other system factors, upgrading can take up to 60 minutes. If the process takes longer, please contact Barracuda Networks Technical Support for further assistance.

In these Release Notes:

General

If you want to update an existing system:

- Direct updating from versions 4.2.x, 5.0.x or 5.2.x to version 6.0.0 is not possible and no countermanding is possible.
- The following update path applies: **4.2 > 5.0 > 5.2 > 5.4 > 6.0.**
- Legacy phion appliances are not supported for version 6.0.0.
- Barracuda NG Control Centers with clusters version 4.0 or lower can not be updated. Upgrade the clusters to version 4.2 before installing the update.
- Barracuda NG Firewall F100 and F101 models using the ClamAV Virus Scanner may not have enough free disk space for updating. For more information, see Migrating from 5.4.x to 6.0.x.
- Do not upgrade Barracuda NG Firewalls or NG Control Centers using Xen HVM images to 6.0.1.

For more information, see Migrating from 5.4.x to 6.0.x.

Beginning with Barracuda NG Admin version 6.0.x, Microsoft Windows XP, Microsoft Windows Server 2003 and 2003 R2 are no longer supported.

GPL Compliance Statement

This product is in part Linux-based and contains both Barracuda Networks proprietary software components and open source components in modified and unmodified form. A certain number of the included open source components underlie the GPL or LGPL or other similar license conditions that require the respective modified or unmodified source code to be made freely available to the general public. This source code is available on http://source.barracuda.com.

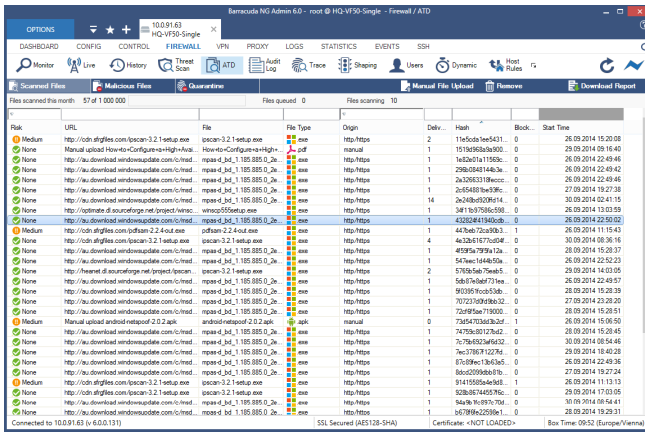
Hotfixes Included with Barracuda NG Firewall Version 6.0.1

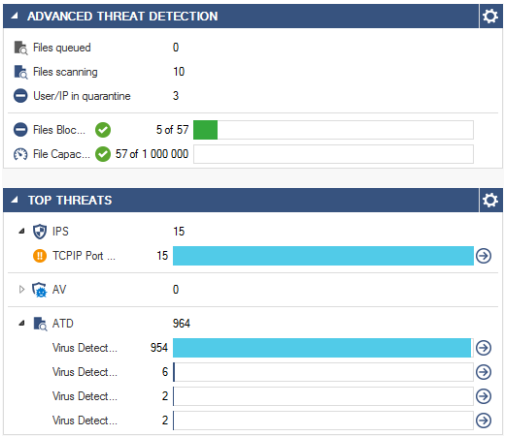
The following previously released public hotfixes are included with this release:

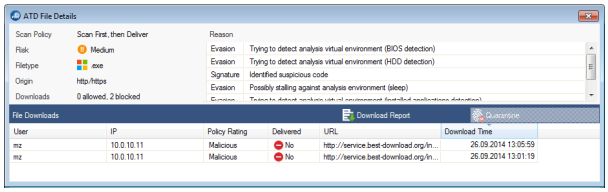
- Hotfix **631**: Reverse proxy termination point
- Hotfix **633**: Potential deadlock in Access Control Service
- Hotfix **637**: Fix for bash vulnerabilities.
- Hotfix **639**: Xen version detection issue.
- Hotfix **642**: Vulnerabilities in Squid: CVE-2014-7141 and CVE-2014-7142
- Hotfix **644**: Traffic shaping issues.
- Hotfix **645**: Fix HA sync for BGP and OSPF propagated routes.
- Hotfix **646**: Fix OpenSSL "POODLE" vulnerability CVE-2014-3566
- Hotfix **650**: HTTP proxy download progress bar.
- Hotfix **652**: SSH security update
- Hotfix **653**: Added support for Barracuda NG Firewall F1000
- Hotfix **654**: Fix for rare Application Control 2.0 engine crash
- Hotfix **663**: Fix for GHOST vulnerability CVE-2015-0235

What´s New in Barracuda NG Firewall Version 6.0.1

Advanced Threat Detection (ATD)



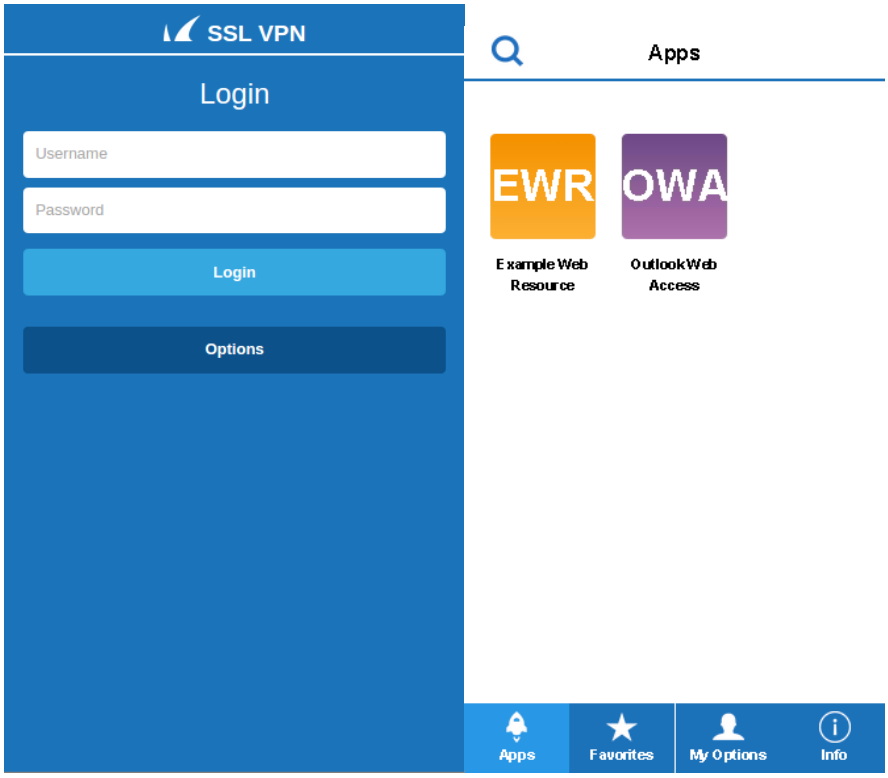




Advanced Threat Detection offers protection against advanced malware, zero-day exploits, and targeted attacks that are not detected by the virus scanner or intrusion prevention system. ATD analyzes files in the Barracuda ATD cloud and assigns a risk score. Local ATD policies then determine how files with a high, medium or low risk score are handled. You can configure email notification of the administrator and/or enable one of the automatic blacklisting policies. To check local files, you also have the option to manually upload a file via NG Admin.

For more information see Advanced Threat Protection (ATP).

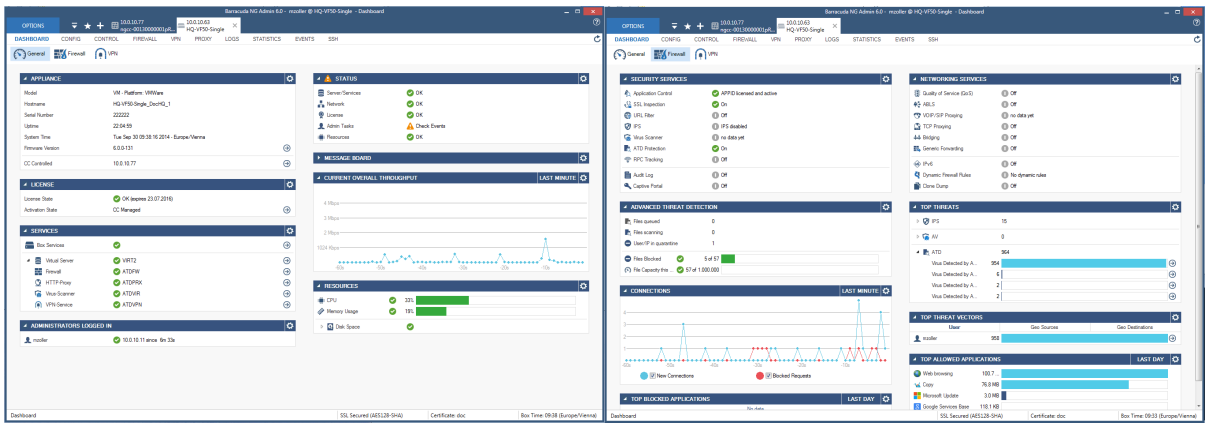
Mobile Portal for End-Users on Mobile Devices for SSL VPN

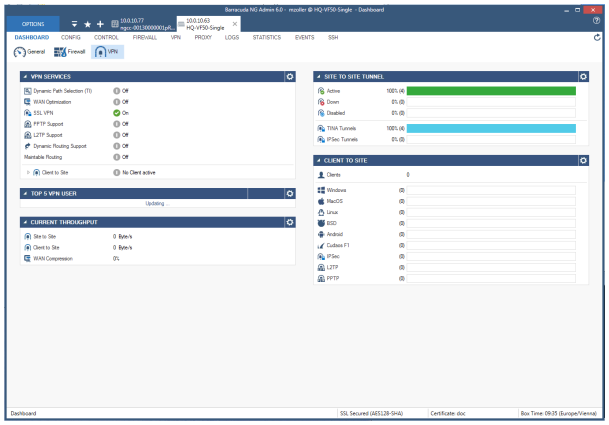


For mobile users accessing the SSL VPN, there is a new mobile portal, which has been designed for ease of use and low support costs. The mobile portal is supported by most commonly used devices, e.g., Apple iOS, Android, Windows Phone and Blackberry. When logging in, you can choose between domain and local authentication. Each web resource uses an auto-generated, contrasting icon for optimal user experience. You can also enable or disable dynamic firewall rules from the mobile portal of the SSL VPN.

For more information, see Mobile Portal.

Improved Barracuda NG Admin UI





Barracuda NG Admin 6.0 uses a new visual style and a redesigned user interface. When logging in, the new dashboard offers small, configurable, and movable elements arranged in three tabs: General, Firewall, and VPN. Each element contains specific continuously updated information, such as system resources, current firewall or VPN throughput, or number Client-to-Site VPN tunnels. Elements can be dragged and dropped freely in their tab according to your preferences.

For more information, see Barracuda NG Admin.

Improved IPFIX/Netflow Reporting

You can now send intermediate reports in a configurable interval to multiple IPFIX/Netflow collectors. Also available is an additional "Extended" IPFIX template containing additional fields such as octetDeltaCount, packetDeltaCount, reverseOctetDeltaCount, reversePacketDeltaCount, and firewallEvent.

For more information, see How to Configure Audit & Reporting with IPFIX.

Application Logging

You can now configure if and how detected applications are logged on a per-access rule basis. You can choose to log Allowed, Blocked, or All detected applications. Application logging is turned off per default.

For more information, see Advanced Firewall Rule Settings.

Mail Gateway Quarantine

The Mail Gateway now offers an interface to manage emails in the quarantine. The admin can access all emails with scan information and, if needed, allow delivery to one or more recipients for individual emails. The admin also receives a daily notification email containing a list of emails currently in quarantine.

For more information, see Mail Gateway.

Dynamic Routing

Added new **OSPF cost**, **BGP always-compare-med** and **Log Level** options to NG Admin. It is now also possible to propagate the default routes via BGP.

Compression for NG Control Center to NG Firewall Communication

You now have the option to use compression for all traffic between managed NG Firewalls and your NG Control Center. **Default**: off.

Public Cloud Images

Information on the network topology in Azure and AWS is gathered and made available via custom external network objects.

For more information, see the Public Cloud section in Custom External Network Objects.

KVM and Xen Virtual Images

KVM and Xen virtual images now support PCI Passthrough and SR-IOV.

For more information, see Best Practice - Performance Tuning on KVM Hypervisors.

NTP Peering Mode

The Barracuda NG Firewall also supports synchronizing the time using NTP peers.

For more information, see How to Configure Time Server (NTP) Settings.

Barracuda NG Firewall F1000 Revision A

The Barracuda NG Firewall F1000 with a data throughput rate of up to 40Gbps is the new flagship model in the NG Firewall line. The F1000 uses up to four field replaceable network modules that can be equipped with a combination of 32x1GbE RJ45 Copper, 16x1GbE SFP Fiber, and 8x10GbE SFP+ Fiber modules.

For more information, see Barracuda NG Firewall F1000 Revision A.

SNMP now includes Traffic Shaping and Secondary Power Supply Data

Traffic Shaping and, for Barracuda NG Firewall models F400, F600, F800, F900 and F1000, secondary

power supply information can now be queried via SNMP.

For more information, see PHION-MIB Field Descriptions.

Reboot and Shutdown for Non-ROOT Users

An Administrative Role has been added to allow non-root users to reboot and shutdown a Barracuda NG Firewall. The user can reboot or shutdown via NG Admin or command line using the new `adminshutdown` command.

For more information, see How to Configure Administrative Roles.

LDAP Group Cache

To reduce the load on LDAP servers, you can now enable caching for selected LDAP groups objects.

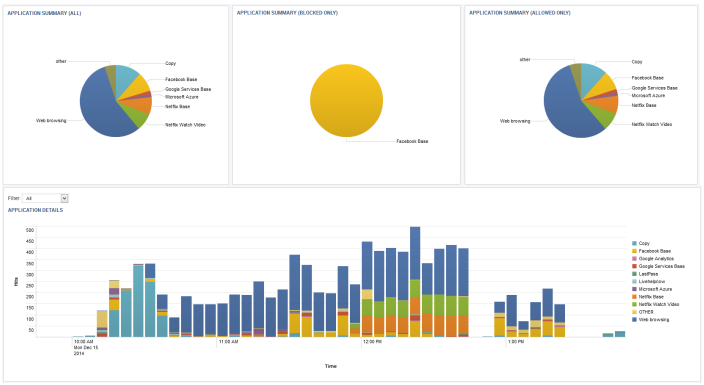
For more information, see How to Configure LDAP Authentication.

Encrypted PAR Files

You can now AES-256-CBC encrypt PCA files using either the serial number or a manual password to create an archive of your configuration. You can restore your hardware NG Firewall or NG Control Center from a PCA file without user interaction as long as the password matches the serial number of the NG Firewall.

For more information, see How to Create PAR or PCA Files on the Command Line and phionar and conftool.

Splunk Integration



Splunk is a third-party platform for operational intelligence that allows you to monitor websites, applications servers, and networks. The Barracuda NG Firewall app shows information on matched access rules, detected applications, and applied URL filter polices on various fixed and real-time timelines. Data is imported into Splunk via syslog streaming of the Firewall activity log.

For more information, see Splunk Integration.

Improvements Included in Barracuda NG Firewall Version 6.0.1

Barracuda NG Admin

- In the **NTP Settings** you can now enter decimal values for **Maximum Distance**. (BNNGF-24863)
- Moving the mouse wheel on unlocked pages no longer displays green check marks on the page. (BNNGF-25528)
- Deleting wild IPv6 routes now works as expected. (BNNGF-24847)
- NG Admin recovers gracefully when authentication error occurs after a session was lost. (BNNGF-27338)
- Changing the password via NG Admin settings now works as expected. (BNNGF-27036)
- Storing activation form now works as expected. (BNNGF-27606)
- Importing large software updates no longer runs into a timeout. (BNNGF-36932)
- Fixed graphs for the **Overall Throughput** and **Connections** widgets. (BNNGF-26568)
- Fixed error message when starting NG Admin. (BNNGF-27926)
- NG Admin no longer crashes when **reset alarm** and **mark as read** is executed on a large number of events. (BNNGF-27452)
- Added option to filter for **IPv4** traffic in **Firewall > Live** and **Firewall > Recent History**. (BNNGF-26902)
- When sorting the NG Control Center **Status** page by the **Box State Summary** column, the NG Firewalls are now displayed in the following order: unreachable, red, yellow, green, gray. (BNNGF-26662)
- Importing and exporting firewall ruleset now works as expected. (BNNGF-26393)
- NG Admin now shows correct disk space values for mounted drives. (BNNGF-26380)

- Included IPv6 networks objects into **Object Viewer**.
- IPsec group VPN policy is now showing the correct phase2 status. (BNNGF-27709)
- The **Rule Tester** now works as expected when used over connections with high latency. (BNNGF-26995)
- When editing multiple access rules, all traffic shaping bands are now visible. (BNNGF-26955)
- Added **View Rule List** option to context menu of **Cascade** access rules. (BNNGF-26938)
- Fixed typo in **Global Settings > CC Identity > CC IP Addresses.** (BNNGF-26820)

Barracuda NG Install

- Realtek driver RTL-8169 is now available. (BNNGF-24676)
- Formatting the USB key now works as expected on Windows 8.1. (BNNGF-27556)
- USB sticks are no longer formatted to 1GB. (BNNGF-27553)
- Added option to add patches and hotfixes in wizard. (BNNGF-27559)

Barracuda OS

- SSH no longer allows MD5 and 96-bit MAC algorithms. (BNNGF-24057)
- Selecting **Located in Timezone** now works as expected for Serbia. (BNNGF-24147)
- Fixed several OpenSSL vulnerabilities. (BNNGF23985)
- Fixed bash vulnerabilities CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187. (BNNGF-25485)
- Netfence Edge is now correctly detected as a flash unit. (BNNGF-24381)
- Fixed CVE-2014-3620 vulnerability in curl. (BNNGF-25260)
- Changing the IP address of the IPFIX collector now works as expected. (BNNGF-24406)
- Disabling a service now works as expected. (BNNGF-25212)
- Syslog streaming to multiple destinations now works as expected. (BNNGF-23586)
- MSAD groups with circle dependencies are now handled correctly. (BNNGF-25535)
- MSAD authentication now works as expected when one or more domains out of several are not reachable. (BNNGF-23941)
- The year is added to the date for syslog streaming. (BNNGF-27102)
- You can now disable **buildarttree** to lower system load after an update on Barracuda NG Firewall F10 or F100 models. (BNNGF-26906)
- Fixed problem causing management sessions to close if the connection is very slow. (BNNGF-26862)
- Authentication using two or more domain controllers no longer fails when the persistent connection is terminated. (BNNGF-27564)
- LDAP offline group caching now works as expected for **memberOf** and **groupOfMember** objects.(BNNGF-26987)
- HA sync now works as expected when using RCS with **Force RCS change message**. (BNNGF-26557)
- Corrupt event databases are now detected and deleted automatically. (BNNGF-26527)
- Included additional I/O load monitoring tools: iptop, sysstat (iostat,...), iftop, htop. (BNNGF-27379)
- A disk space critical event is no longer generated every 10 seconds, but only if the disk state changes. (BNNGF-26916)

- Unplugged power supplies are now correctly detected. (BNNGF-26649)
- Wi-Fi guest access tickets are now included in HA sync. (BNNGF-26476)
- HA sync now works as expected when the VIP network overlaps with the management network. (BNNGF-26428)

Network

- BDNS now flushes the cache after configuration changes. (BNNGF-25094)
- HA sync now works as expected when changing the management IP addresses on units with repository linked network objects. (BNNGF-25137)
- Fixed various UMTS connection problems. (BNNGF-23916)
- Changes to the routing configuration no longer triggers a route re-evaluation before network activation. (BNNGF-26322)
- In an HA cluster with two routes to a destination, one of which is down, a change of the virtual server state on the secondary NG Firewall no longer triggers a route re-evaluation. (BNNGF-25999)

Vx

- NG Firewalls and NG Control Centers running on VMware hypervisors now use a **disk timeout** value of **180**. (BNNGF-24335)
- **hwtool** now detects KVM without displaying an error. (BNNGF-20774)
- Fully virtualized Citrix images are now correctly detected as Xen HVM . (BNNGF-25477)

Public Cloud

- NG Firewalls in the AWS/EC2 public cloud no longer invalidate the licenses when the MAC address changes. (BNNGF-23708)
- Fixed high CPU load issue on Windows Azure NG Firewalls. (BNNGF-24403)

Barracuda NG Control Center

- Removed support for 3.4, 3.6 and 4.0 clusters in the Barracuda NG Control Center. (BNNGF-23528).
- Fixed creating 2048bit RSA/DSA keys with the **Create a Box Wizard**. (BNNGF-24460)
- GTI Editor no longer shows already deleted VPN services. (BNNGF-23556)
- FW Audit filters now work as expected when using **page up** or **page down** buttons. (BNNGF-24446)
- Showing the difference for RCS versions of **Server Properties** now works as expected. (BNNGF-24122)
- Fixed a rare condition caused by an incorrect detection of the update state. The NG Control Center sent a complete update again even though it was already successfully finished. (BNNGF-26317)
- Site-specific network objects can only use [a-z, 0-9] in the name so they do not override other network objects with the same name before the space. (BNNGF-27767)
- VPN tunnels are now generated automatically when a VPN service is set configured as a hub. (BNNGF-26305)

Access Control Service

- Checking for dword registry values now works as expected. (BNNGF-24365)

Dynamic Routing Service

- Propagating the default route via BGP now works as expected. (BNNGF-24635)
- Aggregated routes are now correctly detected as IPv4 or IPv6. (BNNGF-25192)
- The BGP option **always-compare-med** is now available via NG Admin GUI. (BNNGF-25147)
- OSPF activation now works as expected when **Quad-IP** is used. (BNNGF-23779)
- OSPF now listens on the correct interfaces. (BNNGF-23978)
- Using **ID Type From-Server** for OSPF now works as expected. (BNNGF-25465)
- OSPF config nodes in the range repository now work as expected. (BNNGF-24043)

Firewall

- In some cases traffic was assigned an incorrect QoS band. (BNNGF-23908)
- Dst NAT rules with using a subnet as the target now display the target in CIDR notation. (BNNGF-25102)
- Sync now works as expected for non-TCP sessions. (BNNGF-25027)
- SSL Interception now works with intermediate certificates. (BNNGF-24369)
- Inbound traffic shaping now works as expected for VPN tunnel traffic. (BNNGF-24311)
- Activity log and FW Audit now include **Session duration**, **transferred data** and **session start and close time**. (BNNGF-23927)
- Accumulated activity log messages with count > 1 are now written into the activity log. (BNNGF-25111)
- In rare cases using * as the MIME type caused websites to only partially load when virus scanning was enabled. (BNNGF-24682)
- Traffic Shaping Internet fallback now works as expected when using virus scanning in the firewall. (BNNGF-24768)
- Herokupp.com is no longer classified as Facebook. (BNNGF-24459)
- Fixed issue causing a kernel panic when using SSL Interception over an Ethernet Bundle interface. (BNNGF-26412)
- SSL Interception now checks expiration date of cached certificates. (BNNGF-27660)
- Updated RDP service object to include UDP Port 3389. (BNNGF-27449)
- In rare cases, the port numbers were displayed incorrectly in the firewall activity log. (BNNGF-27127)
- SSL Interception now signs untrusted certificates with the **Barracuda Known Untrusted Certificate**. (BNNGF-27045)
- UDP session are now counted correctly. (BNNGF-27001)
- FWauth (authentication/ATD/guest access) now serves HTTPS requests as expected. (BNNGF-27603)
- Rename **IPS Scanning** to **IPS Scan Mode** in **Operational IPS**. (BNNGF-27585)
- The **Management IP** object now contains all management IP addresses. (BNNGF-27542)
- Layer2 bridge names are now limited to 10 characters. (BNNGF-27088)
- Increased the upper limit for **Maximum Pending Inbound** from 65536 to 262144.

(BNNGF-27614)

VPN

- VPN tunnel now makes a fallback to original primary ISP after failover and reconnects if **Own Routing Table** is set to **no**. (BNNGF-20665)
- L2TP no longer assigns virtual IP addresses multiple times. (BNNGF-24350)
- RCS now includes changes made in the advanced VPN Server Settings, such as **IKE PSK** and **IPsec Log Level**. (BNNGF-25166)
- Fixed CVE-2014-3158 vulnerability in ppp. (BNNGF-25188)
- When establishing IPsec VPN connections, sa-attributes of type ESN are now ignored. (BNNGF-23629)
- L2TP over NAT-T now works as expected on Windows XP. (BNNGF-23660)
- VPN handshake timeout can now be configured to fix timeouts involving two-factor authentication. (BNNGF-25005)
- IPsec PSK now works for multiple VPN clients using the same public IP address. (BNNGF-23909)
- Using multiple MSAD domains for authentication now works as expected. (BNNGF-23585)
- IPsec connections using NAT traversal no longer drop if a configuration change is done. (BNNGF-24532)
- Using 192bit AES now works as expected. (BNNGF-26188)
- Resolved connectivity problems with Mocana IPsec client. (BNNGF-27115)
- Configuration changes for the VPN service no longer cause error logs for the disabled SSL VPN service. (BNNGF-27494)
- It is no longer possible to configure a Client-to-Site IPsec VPN connection without an IPsec Phase 2. (BNNGF-26590)

SSL VPN

- Users are now logged out automatically if the browser crashes or is closed manually. (BNNGF-25163)
- Custom images now display correctly in Chrome. (BNNGF-23767)
- SharePoint 2010 on Windows Server 2008 Web Resources now work as expected. (BNNGF-23601)
- You can now enter passwords with up to 60 characters on the login page. (BNNGF-23782)
- Authentication timeout is now configurable to allow for longer times needed for two-factor authentication. (BNNGF-27005)

HTTP Proxy

- Google Safe Search now works as expected with the HTTP proxy. (BNNGF-24514)
- Restarting the HTTP proxy no longer results in multiple instances of the same proxy service running. (BNNGF-24419)
- Fixed CVE-2014-7141 and CVE-2014-7142 vulnerabilities in squid. (BNNGF-25647)
- UI now works as expected with two HTTP proxies sharing the same listening IP address. (BNNGF-24429)
- Usernames with the form user@domain are now allowed for HTTP proxy ACLs. (BNNGF-23876)

- It is no longer possible to bypass authentication by using a previously authenticated IP address. (BNNGF-26922)
- HTTP Proxy download progress bar now works in combination with virus scanning. (BNNGF-24993)
- Added support for sub-CA certificates to use certificate chains for the HTTP proxy root certificate . (BNNGF-27802)
- Corrected ACLs for reverse proxy configurations containing no additional backend server. (BNNGF-26066)
- Content caching now works as expected for the HTTP Proxy in **Transparent** mode. (BNNGF-24623)
- Added TS Agent support to the HTTP Proxy. (BNNGF-26758)

FTP Gateway

- FTP connections through the FTP Gateway now work as expected. (BNNGF-24585)

Mail Gateway

- **Parallel Inbound Conn. per Peer** DoS protection now works as expected. (BNNGF-23617)
- The mail gateway can now use the virus scanner service as expected when Wi-Fi is enabled. (BNNGF-24750)
- **Sender domain check** is now omitted for empty senders if **Refuse Empty Mail from** is set to **No**. (BNNGF-23860)
- It is no longer possible to bypass the **subject-blacklist** by encoding the subject line. (BNNGF-26887)

DNS Server

- When a dynamic DNS zone is changed, the configuration is now reloaded as expected. (BNNGF-24542)

DHCP

- DHCP server now works as expected when Wi-Fi interfaces are disabled. (BNNGF-24575)
- Added "+" to the list of allowed characters for **HMAC-MD5 key**. (BNNGF-24420)

Distributed Firewall

- Landing page now works as expected. (BNNGF-24317)
- IPv6 autoconfig now works as expected. (BNNGF-23724)

Virus Scanner

- Zip files with malicious folder structure are now handled as expected. (BNNGF-27815)
- Zip files are now classified correctly. (BNNGF-27130)
- The default value for **Detect Packet** (**Virus Scanner Settings > ClamAV**) is now set to **No**. (BNNGF-27447)

DNS Server

- Updated bind to fix security issue CVE-2014-8500. (BNNGF-27477)

URL Filter

- Fixed rare issue that can lead to all requests being canceled in timeout. (BNNGF-27038)
- URL Filter no longer allows creation of more than 993 custom URL filter objects. (BNNGF-26890)

SSH Proxy

- SSH Proxy profile assignment is no longer case sensitive. (BNNGF-26694)

Known Issues

6.0.1

- HTTP Proxy: **Custom Cipher String** and **Allow SSLv3** settings only apply to reverse proxy configurations.
- HTTP Proxy: It is not possible to use ClamAV in combination with the HTTP Proxy service on Barracuda NG Firewall F100 and F101 models.
- CC Wizard: The CC Wizard is currently not supported for NG Control Centers deployed using NG Install.
- Firewall: Using SSL Interception in combination with URL Filtering and category exemptions may result in degraded performance.
- Xen HVM: Updating or Installing Xen HVM virtual NG Firewalls or NG Control Centers to version 6.0.1 is currently not supported.

6.0.0 EA

- ATD: Only the first URL in the Quarantine Tab that leads to a quarantine entry is displayed, even if the User and/or IP address downloaded more than one infected file.This can be dangerous if the first downloaded file is a false-positive.
- Firewall: It is not possible to join a **join.me** session if SSL Interception and Virus Scanning is enabled in the matching access rule.
- SSL VPN Mobile Portal: Mobile Portal configurations and settings are currently not included in PAR files.
- Virus Scanner: The virus scanning service stalls during virus pattern updates.
- NG Admin: SPoE does not work if an IPv6 virtual server IP address is used.
- NG Admin: Product activation does not work with Internet Explorer 11.
- Barracuda OS: HA sync is not possible if **Force RCS Change Message** is enabled.
- Barracuda OS: **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually.

Miscellaneous

- Terminal Server Agent: It is currently not possible to assign connections to Windows networks shares to the actual user.
- Firmware Update: Log messages similar to `WARNING: /lib/modules/2.6.38.7-9ph5.4.3.06.x86_64/kernel/drivers/net/wireless/zd1211rw/zd1211rw.ko needs unknown symbol ieee80211_free_hw` may appear while updating, but can be ignored.
- Attention: Amazon AWS/Microsoft Azure: Performing **Copy from Default** of Forwarding Firewall rules currently locks out administrators from the unit and requires a fresh installation of the system.
- Application Control 2.0 and Virus Scanning: Data Trickling is only done while the file is downloaded, but not during the virus scan. This may result in browser timeouts while downloading very large files.
- Application Control 2.0 and Virus Scanning: If the Content-Length field in HTTP headers is missing or invalid, the **Large File Policy** may be ignored.
- Application Control 2.0 and Virus Scanning: It is currently not possible to perform virus scanning for chunked transfer encoded HTTP sessions such as media content streaming. Barracuda Networks recommends excluding such traffic from being scanned.
- Application Control 2.0 and Virus Scanning: In very rare cases, if the SSL Interception process is not running, but the option **Action if Virus Scanner is unavailable** is set to **Fail Close**, small amount of traffic may already have passed through the firewall.
- Application Control 2.0 and Virus Scanning: In rare cases, Google Play updates are sometimes delivered as partial updates. These partial updates cannot be extracted and are blocked by virus scanning engine. The engine reports **The archive couldn't be scanned completely**. Either create a dedicated firewall rule that does not scan Google Play traffic, or set **Block on Other Error** in **Avira Archive Scanning** to **No.**
- High Availability: IPv6 network sessions might not be established correctly after an HA failover.
- Barracuda OS: Restoring units in default configuration with par files created on a NG Control Center may result in a corrupt virtual server. Instead, copy the par file to *opt/phion/update/box.par* and reboot the unit.
- VPN: Rekeying currently does not work for IPsec Xauth VPN connections. The VPN tunnel terminates after the configured rekeying time and needs to be re-initiated.

Figures

1. ATD_List.png
2. ATD_dashboard.png
3. ATD_details.png
4. mobile01.png
5. ssl_apps.png
6. dashboard_general.png
7. dashboard_firewall.png
8. dashboard_VPN.png
9. splunk_top.png

© Barracuda Networks Inc., 2020 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.