

Barracuda Firewall Release Notes 6.5.x

<https://campus.barracuda.com/doc/41110856/>

Please Read Before Upgrading

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 10 minutes. If the process takes longer, please contact Barracuda Networks Technical Support for further assistance.

6.5.3.002 includes updates to mitigate potential man in the middle attacks due to a security vulnerability in the SSLv3 protocol.

Some software modules of the Barracuda Firewall are vulnerable to attacks described in the security advisory CVE-2014-3566 (POODLE).

Barracuda Networks highly recommends to update your Barracuda Firewall to version 6.5.3.002.

Affected portions of the Barracuda Firewall and possible attack vectors

- **User Interface** – Starting with version 6.5.3.002 SSLv3 is disabled per default. If you must support older browsers without TLS support, you can enable SSLv3 in the expert settings on the **ADVANCED > Secure Administration** page. Append &expert=1 to the URL to display expert variables.
- **SSL VPN, Captive Portal and Guest Access** – Old browsers which only include support for SSLv3 can connect to these services using the SSLv3 protocol. Connections by browsers supporting the newer TLS protocols are not allowed to fall back to SSLv3.

What's New with Barracuda Firewall Version 6.5.4.003

- This firmware version is a maintenance release only. No new functionality has been added.

Firmware Improvements

- When the Barracuda Firewall is not connected to the Internet or has no route to the Internet, network configuration now works as expected. (BNF-4426)
- It is now possible to configure **Static Network Interfaces** on unactivated Barracuda Firewalls. (BNF-4482)

What's New with Barracuda Firewall Version 6.5.3.002

- This firmware version is a maintenance release only. No new functionality has been added.

Firmware Improvements

Web Interface

- Added expert setting to disable SSLv3 for the web interface.

What's New with Barracuda Firewall Version 6.5.2.004

Firmware Improvements

Web Interface

- The user interface now displays warning messages, if disabled static Wi-Fi interfaces are configured. (BNF-4050)
- The Wi-Fi configuration now works as expected. The number sign (#) is no longer supported in pre-shared keys, location information is now mandatory, SSID must be unique across all Wi-Fi access points, and Wi-Fi configuration automatically enables corresponding DHCP ranges if configured. (BNF-4029)
- The Preferences configuration of IPs events now works as expected. (BNF-3086)

Firewall

- Redirect to Guest Ticketing now also works on a Barracuda Firewall X100. (BNF-4028)

Barracuda OS

- Updating Barracuda Firewalls deployed behind a proxy server now works as expected. (BNF-3964)
- Support tunnels can now also be initiated from a secondary unit of a HA cluster. (BNF-3870)
- Configuration backups erroneously included secondary management IP addresses of the unit. (BNF-4017)

DHCP

- The DHCP service now starts correctly if the configuration contains a disabled Wi-Fi interface. (BNF-3963)

Firmware Improvements

Web Interface

- When saving a form the **Save** and **Cancel** buttons can no longer be clicked multiple times. (BNF-4285)

What's New with Barracuda Firewall Version 6.5.1.007

Firmware Improvements

Barracuda Cloud Control

- **Logout** button in **Basic > User Activity** now works as expected. (BNF-3596)
- It is no longer possible to change the management IP address when using the Barracuda Cloud Control. (BNF-3608)
- Network interface configuration is now disabled when displayed in group context on the Barracuda Cloud Control. (BNF-3607)
- Showing two identical static network interfaces in group context on Barracuda Cloud Control now works as expected. (BNF-3653)
- Network, service, connection, NAT and user objects now work in group context on the Barracuda Cloud Control. (BNF-3640)

Web Interface

- Fixed a security issue when invoking the **Logout** action. (BNF-3598)
- Entering the password on the BASIC > Cloud Control page when connecting to Barracuda Web Security Service now works as expected. (BNF-3618)
- The log navigation and preference elements now display as expected on the **Log** pages. (BNF-3574)
- Task manager items are now removed when task is complete. (BNF-3284)
- Renaming elements on the **Status** page now works as expected when using Firefox. (BNF-3366)
- Improved input validation for IP addresses and networks. (BNF-3287)
- Changes naming for current VPN throughput from "bps10" and "BPS" to **Bytes/10seconds**. (BNF-3484)
- Input validation for DynDNS usernames corrected to allow dashed in the username. (BNF-3669)
- Fixed UI bug in source column of **FIREWALL > Application Rules**. (BNF-3369)

- Network interface table on the **BASIC > IP Configuration** page now shows duplex and state information for every link. (BNF-2168)
- The **Add Dynamic Network Interfaces** button on the **BASIC > IP Configuration** page is disabled if all ports are already in use. (BNF-3515)
- A warning is displayed if you enter a gateway route which cannot be reached directly. (BNF-3235)
- NTP is automatically activated for the management IP if it is enabled on **BASIC > Administration**. (BNF-3544)

Barracuda OS

- Upgrade of OpenSSL to fix CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470 and CVE-2014-0076. (BNF-3714)
- Authentication Logs now contain information on captive portal authentications. (BNF-2719)
- Querying multiple domain controllers now works as expected even if the user credentials are not valid for one of the domain controllers. (BNF-3688)
- Firmware Upgrades are no longer possible if a network activation is still outstanding. (BNF-3584)

Firewall

- It is no longer possible to upload an expired certificate for SSL Inspection. (BNF-3332)
- Minimum timeout value for connection objects is now three seconds. (BNF-3313)
- Duplicate IP addresses are now visible on the **NETWORK > Routing** page. (BNF-3344)
- Terminating a session in **BASIC > Active Connections** now works as expected. (BNF-3695)
- A warning is displayed if you attempt to use a connection object for a connection which does not exist. E.g., **SNAT with 3G IP** without 3G being configured. (BNF-3236)

VPN

- VPN Network Object VPN-Local-Networks now works as expected. (BNF-3711)
- Warn when importing a VPN certificate with an empty CN value. (BNF-3725)
- Dynamic IP addresses for site-to-site VPN tunnels can only be used if **Use Dynamic IPs** is enabled. (BNF-3410)
- Fixed labeling for client-to-site authentication from "Shared Key and Certificate" to "Shared Key or Certificate". (BNF-3448)
- Added option to restart the VPN service in the Expert Variables. (BNF-3568)

SSL VPN

- Fixed issue of the SSL VPN service was not handling requests until restarted. (BNF-3701)
- Added **SharePoint** type for webforwards. (BNF-3799)

High Availability

- HA synchronization now works as expected with non-ASCII characters. (BNF-3830)

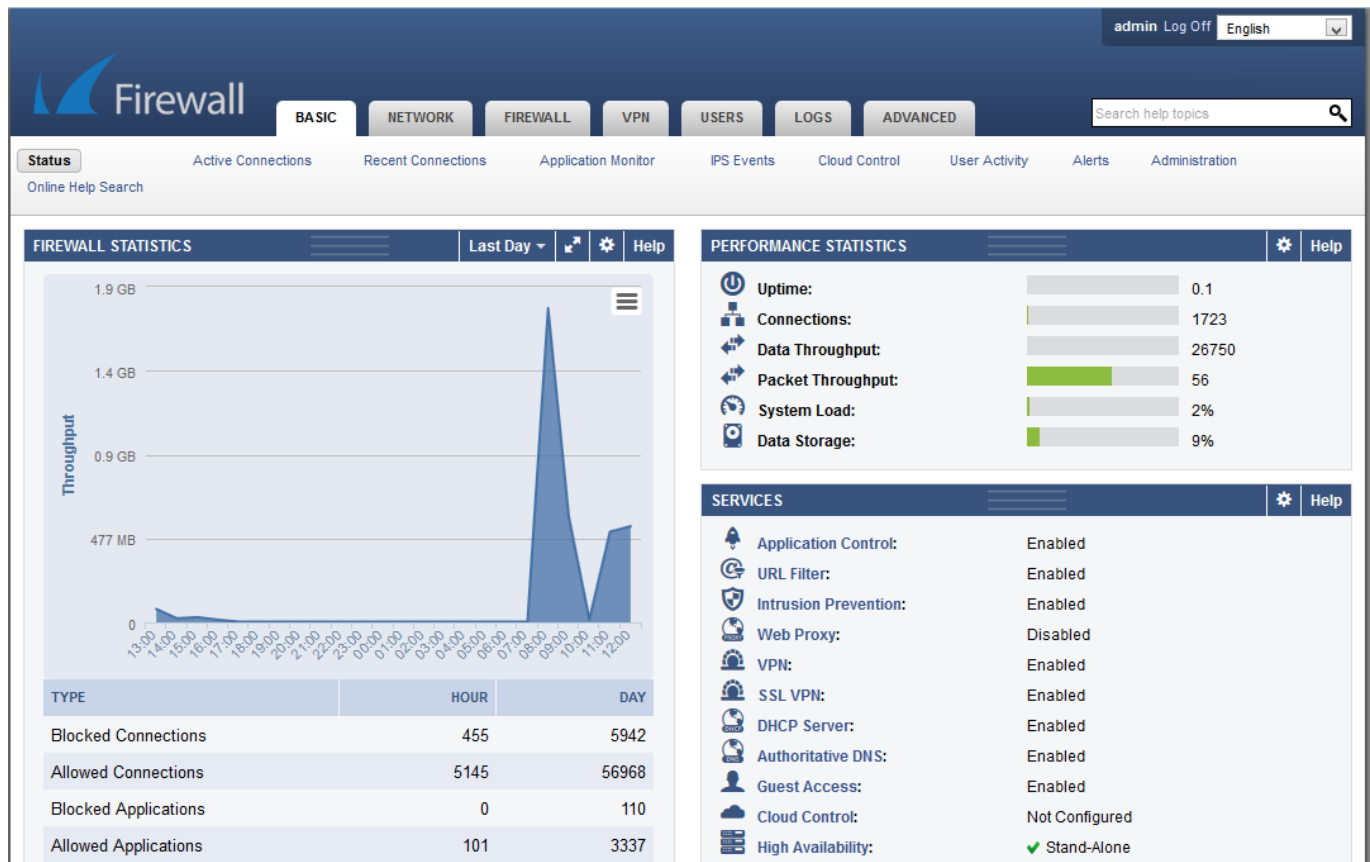
Known Issues and Limitations for 6.5.1.007

- **Barracuda Cloud Control** – In some cases the labeling of the time axis in the **FIREWALL STATISTICS** element on the **Status** page in the Barracuda Cloud Control is illegible.
- **Barracuda Cloud Control** – It is not possible to directly show the list of Recent Connections for a detected application from the **Application Monitor** page in the Barracuda Cloud Control.
- **Guest Access** – The ticketing web interface is not accessible on the management interface.
- **Backup** – It is not possible to restore old 6.1.X or 6.0.X backups on a Barracuda Firewall using firmware 6.5.0 or newer.
- **VPN** – When using the Barracuda VPN client it currently not possible to connect to a client-to-site VPN using user/password and client certificate authentication.
- **Barracuda Report Creator** – Only available for Microsoft Windows 7 and 8.

What's New with Barracuda Firewall Version 6.5.0.024

New Web Interface

The 6.5 firmware includes a completely redesigned user interface. The updated user interface is now even easier to use as it uses a new visual style, icons and popover screens instead of popup windows. The **BASIC > Status** and **BASIC > Application Monitor** overview pages are build out of small movable and configurable elements. Each element contains specific information such as connection, blocked applications, link status and many more. Elements can be dragged and dropped freely on the status page. You can also remove or add application monitor elements to the dashboard.

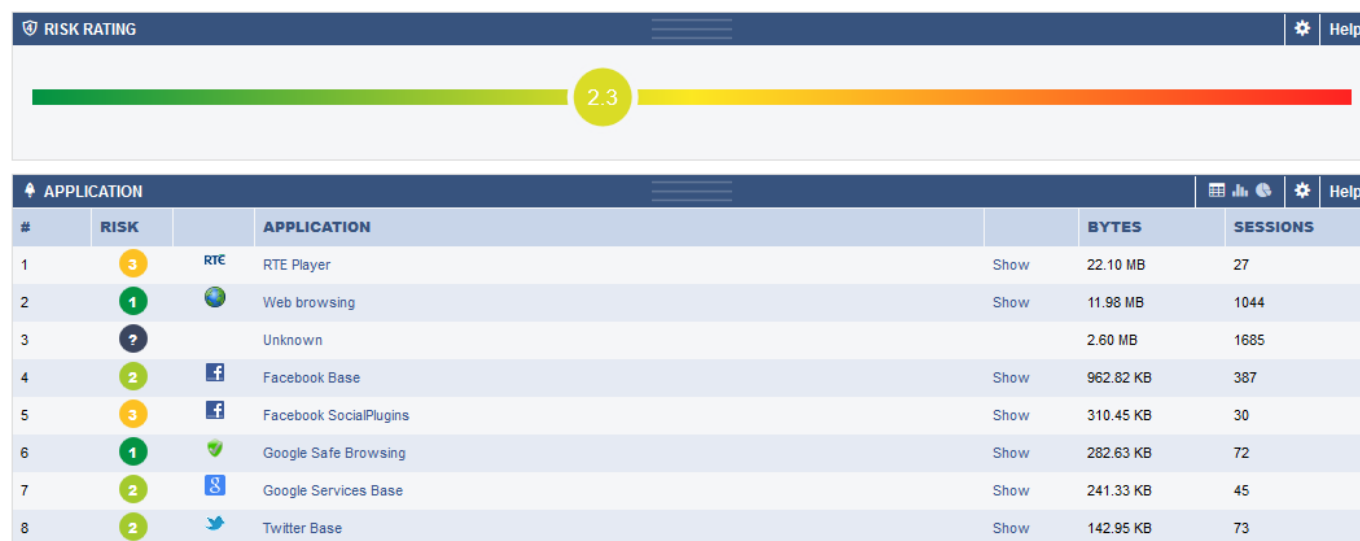


Application Control

Barracuda Firewall 6.5.0 integrates and updates the Application Control engine into the core firewall. Now the Barracuda Firewall can identify and enforce more than 1200 applications, even those that may hide their traffic inside otherwise "safe" protocols, such as HTTP. You can define dynamic application policies to establish acceptable use policies for users and groups by application, application category, location or time of day:

- Block unwanted applications for certain users and groups.
- Control and throttle acceptable traffic.
- Preserve bandwidth and speed-up business critical applications to ensure business continuity.
- Enable or disable specific subapplications (e.g., Facebook Chat, YouTube postings or MSN file transfers).
- Inspect SSL-encrypted application traffic.

Use the new application monitor to analyze application traffic, receive real-time and historical information on traffic passing through your Barracuda Firewall. Drill down through the application data by using filters based on a combination of user, time, application or risk factor. Up to 20 of these customized elements can be included on your dashboard to offer an instant system and network overview every time you log in to your Barracuda Firewall.



URL Filter

With the Barracuda Firewall 6.5.0 customers with an active Web Security subscription now have the option to use the URL Filter on the Barracuda Firewall itself, instead of having to route all internet traffic through the Web Security Service cloud. The on-box URL Filter is tightly integrated with application control in the firewall and allows creation and enforcement of effective Internet content and access policies based on the Barracuda URL database. The URL database is hosted in the cloud and continuously updated by Barracuda Networks, ensuring that your policies are always using the latest information. URL categorization performs an online lookup of the categorization for the domain in question and the Barracuda Firewall subsequently caches this categorization information.

URL CATEGORY									
#	URL CATEGORY		BYTES	SESSIONS					
1	Content Server	Show	28.61 MB	341					
2	Uncategorized		3.79 MB	2015					
3	News	Show	2.70 MB	243					
4	Search Engines/Portals	Show	933.94 KB	195					
5	Advertisement/Popups	Show	705.16 KB	79					
6	Computing/Technology	Show	607.84 KB	45					
7	Social Networking	Show	544.95 KB	107					

Client-To-Site IPsec VPN with Pre-Shared Keys

To make it easier for your Apple iOS or Android device to remotely connect to your network you can use the new client-to-site IPsec VPN with pre-shared keys. You do not have to manage X.509 certificates which have to be installed on the mobile devices.

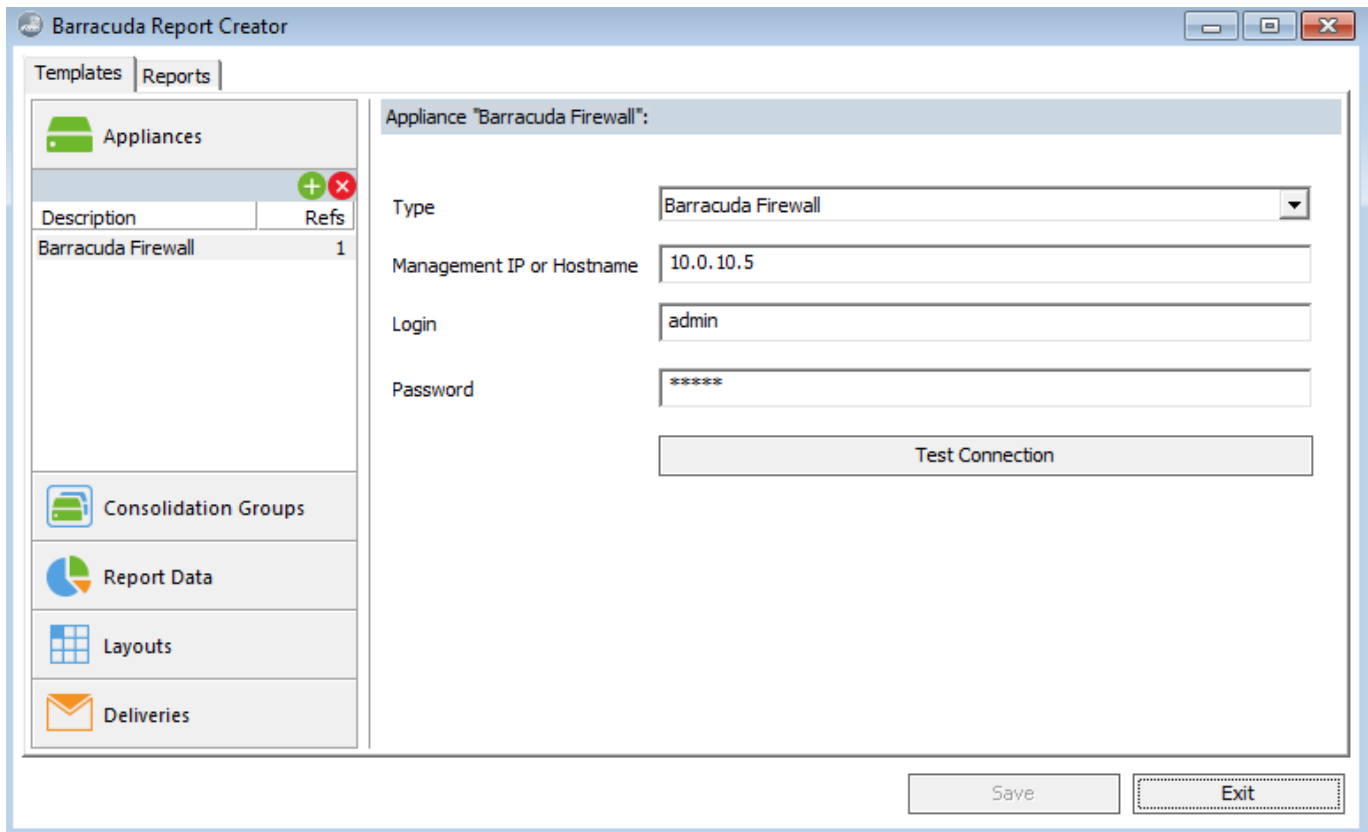
VPN Site-2-Site Remote and Local Networks

As of Barracuda Firewall Release 6.5.0 there is no more need to create specific firewall rules to allow network traffic from two networks connected via VPN. The defined **Local Networks** and **Remote**

Networks in the site-to-site VPN configuration are added automatically to these newly created dynamic network objects. The **VPN-SITE-2-SITE** firewall rule is disabled by default and enabled automatically when a site-to-site VPN is configured.

Reporting

Reporting is one of the major tasks to be managed in an enterprise. It is crucial to make bandwidth usage and all other security related information visible, reportable and presenting it in an easy-to-read format. With Barracuda Firewall 6.5.0 the new Barracuda Report Creator, directly downloadable from the **BASIC > Administration** page, makes creating IT security reports on a regular basis easy. Simply select the appliances and the required types of reports, define the layout and way of delivery and the Report Creator does the rest. (please note that the Barracuda Report Creator is only compatible to Microsoft Windows 7 and 8).



Backup to the Cloud

You now have the option to store your backups in the Cloud using your Barracuda Cloud Control account. Configure automated backups to always have a working off-site configuration backup for your Barracuda Firewall, enhancing your data security.

Important Migration Steps

If you are using one of the following features, complete the listed instructions to complete the

migration:

- **Barracuda DC Agent** – After the migration do a dummy change in **USERS > external Authentication > DC Agent** to activate the automatic logout in case the DC Agent or the Active Directory Server the DC Agent is installed on is not available.
- **Application Control** – Before you can make use of the improved Application Control you have to migrate your existing firewall rules: A migration wizard will appear every time the **BASIC > Status** page is accessed until you complete the migration. If you do not want to migrate these settings at the time of the upgrade you can continue using Application Control in legacy mode, However, certain functionality (such as new **BASIC > Status** page) will not be available until migration has been completed. During the migration the application control logic is transferred to the new **FIREWALL > Application Policy** page. Due to the different and enhanced functionality it is not possible to provide an automated migration. Parts of your application control settings will need to be re-done after upgrading to 6.5.
- **VPN** – If firmware version 6.5.0 was not preinstalled on your Barracuda Firewall you must manually add the network objects **VPN-Local-Networks** and **VPN-Remote-Networks** as well as the firewall rule **VPN-SITE-2-SITE** to take advantage of automatic updates of the VPN network objects and firewall rule when creating a site-to-site VPN.

VPN-SITE-2-SITE firewall access rule

- **Action** – Select **Allow**.
- **Name** – Enter VPN-SITE-2-SITE.
- **Source** – Select **VPN-Local-Networks**.
- **Network Services** – Select **Any**
- **Destination** – Select **VPN-Remote-Networks**.
- **Connection** – Select **No SNAT**.
- **Adjust Bandwidth** – Select **Business**.

Network Object VPN-Local-Networks

- **Name** – Enter VPN-Local-Networks.
- **Include Network Address** – Enter all **local networks** used in existing site-to-site VPNs. If no site-to-site VPN are configured enter dummy values. They will be overwritten when a site-to-site VPN is configured.

Network Object VPN-Remote-Networks

- **Name** – Enter VPN-Remote-Networks.
- **Include Network Address** – Enter all **remote networks** used in existing site-to-site VPNs. If no site-to-site VPN are configured enter dummy values. They will be overwritten when a site-to-site VPN is configured.

Firmware Improvements

Barracuda Web Security Service

- Fixed error message which users who are not logged in would receive if the **Include User Information** option was set. (BNF-1835)

Barracuda Control Center

- Fixed misleading error message when login to Barracuda Cloud Control fails. (BNF-3303)
- In some cases it was not possible to see connection objects in the BCC. (BNF-2967)
- The **VPN > Certificates** page is now displayed correctly in the Barracuda Control Center. (BNF-1788)
- The **NETWORK > DHCP Server** page is no longer accessible when using group context in the Barracuda Control Center. (BNF-3636)
- Adding identical configurations in group context now works as expected. (BNF-3653)

VPN

- In some cases port 443 for client-to-site vpn was blocked. (BNF-2610)
- VPNs using the blowfish cipher now work as expected. (BNF-3109)
- Client-to-site VPN IPsec Phase 2 configuration is only mandatory if IPsec clients are enabled. (BNF-2415)

Wi-Fi

- Improved Wi-Fi stability by fixing rekeying issues resulting from missing entropy. (BNF-2722)
- Fixed issues resulting in kernel panics. (BNF-2721)
- Changes to the Wi-Fi settings are now executed as expected. (BNF-3549)

Firewall

- Minimum timeout for connection objects lowered to three seconds. (BNF-3309)
- Firewall objects can now only be renamed if they are not in use. (BNF-3053)
- Traffic Shaping using the low and lowest QoS bands now work as expected. (BNF-3685)

Web Interface

- Firewall objects can no longer be deleted if they are still in use. (BNF-3169, BNF-3258)
- It is no longer possible to delete all NTP server entries in **Basic > Administration**. At least one NTP server has to be configured at all times. (BNF-3120)
- When downloading csv log files a different name is now used for every log file. (BNF-3138)
- PPPoE username and password configuration in protect my desk wizard is now works as expected. (BNF-3297)
- Barracuda logo is updated. (BNF-3549)
- Fixed security vulnerability when invoking logout action. (BNF-3598)
- Session termination in **Active Connections** now works as expected. (BNF-3695)

SIP Proxy

- The SIP proxy will now be enabled if you enable the **LAN-2-INTERNET-SIP** or **INTERNET-2-LAN-SIP** firewall access rules. (BNF-2679)
- SIP clients can now receive calls on non-standard SIP ports. (BNF-2879)
- SIP video (multi-port) calls now work as expected. (BNF-3115)

DHCP

- The DHCP server now checks if an interface is disabled when creating a DHCP service pool. (BNF-2709)

High Availability

- The **Advanced > Backup** and **Network > Bridging** pages are now read only on secondary unit. (BNF-2820, BNF-3231)
- Forwarding sessions on dynamic interfaces are no longer synchronized to secondary unit. (BNF-3386)

Barracuda OS

- Upgrade of OpenSSL to fix a potential man-in-the-middle attack for SSL/TLS clients and servers. (CVE-2014-0224, BNSEC-4402, BNF-3713)
- Upgrade of OpenSSL to version 1.01g to fix the openssl heartbleed bug. (CVE-2014-0160)
- The syslog daemon now restarts automatically if needed. (BNF-2919)
- RADIUS authentication now works as expected. (BNF-3224)
- After a reboot due to a power outage the system clock will not be reset to UTC time anymore. (BNF-3367)
- DynDNS over HTTPS now works as expected. (BNF-3524)
- Fixed security issues for the captive portal and guest ticketing authentication pages. (BNSEC-4395, BNSEC-4402)

Known Issues and Limitations

- **Barracuda Control Center** – In some cases the labeling of the time axis in the **FIREWALL STATISTICS** element on the **Status** page in the Barracuda Control Center is illegible.
- **Barracuda Control Center** – It is not possible to directly show the list of Recent Connections for a detected application from the **Application Monitor** page in the Barracuda Control Center.
- **Guest Access** – The ticketing web interface is not accessible on the management interface.
- **Web Interface** – After the Barracuda Firewall update and reboot you may have to wait up to 5 minutes (depending on your hardware) until you can successfully log in to your system.
- **Backup** – It is not possible to restore old 6.1.X or 6.0.X backups on a Barracuda Firewall using firmware 6.5.0 or newer.
- **Backup** – The option to backup to SMB shares has been removed. Use Barracuda Cloud Control or FTP/FTPS server as an alternative.
- **Firewall** – Removed the firewall rule tester.
- **Firewall** – After migration to the new Application Control some Application Control settings and policies have to be re-done manually.
- **Firewall** – Before migration to the new Application Control some elements on the **BASIC > Status** dashboard do not display any information.
- **VPN** – IPsec client-to-site VPN with pre-shared keys ignore external group conditions. (BNNGF-22043, BNF-3225)

- **Barracuda Report Creator** - Only available for Microsoft Windows 7 and 8.

Figures

1. releasenotes01.png
2. releasenotes02.png
3. releasenotes03.png
4. releasenotes04.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.