Barracuda Firewall Release Notes 6.1.x

https://campus.barracuda.com/doc/41093268/

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.

6.1.7.003 includes an update of OpenSSL to fix a potential Man-in-the-middle attack for SSL/TLS clients and servers. (CVE-2014-0224, BNSEC-4402, BNF-3715)

Some software modules of the Barracuda Firewall incorporate versions of OpenSSL, which are vulnerable to attacks described in security advisory CVE-2014-016 (OpenSSL Heartbleed bug). Barracuda Networks highly recommends to update your Barracuda Firewall to firmware version 6.1.5.005.

Affected portions of the Barracuda Firewall and possible attack vectors

- **User Interface** – Eavesdrop on communication with the Barracuda Firewall's user interface.
- **VPN** – The VPN functionality of the Barracuda Firewall was never compromised since the service uses OpenSSL version 0.9.8g. However, if the VPN service and management interface share the same certificate (delivered default certificate), Barracuda Networks recommends to also change the VPN certificates as described below.

Actions required

1. Update your Barracuda Firewall to version 6.1.5.005. This will upgrade OpenSSL to version 1.0.1g which is not vulnerable to the Heartbleed bug.
2. **ADVANCED** > **Secure Administration** – Replace the Barracuda Firewall's default certificate with a newly created **Private (Self-signed)** or **Trusted (Signed by a**

trusted CA) certificate.

3. **ADVANCED** > **Secure Administration** – If your are using a **Private (Self-signed)** or **Trusted (Signed by a trusted CA)** certificate, you must replace them with newly created certificates.
4. **VPN** > **Certificates** – Delete existing **SAVED CERTIFICATES** and create or upload new VPN certificates.
5. **VPN** > **Site-To-Site** – Reconfigure all IPsec tunnels to use the newly created certificates as **Local Certificate** and for authentication (if applicable).
6. **VPN > Client-To-Site** – Replace the **Local Certificate** with the newly created certificate. This is valid for all client-to-site VPN access policies.
7. **VPN** > **SSL VPN** – Select the newly created certificate in the **Server Settings** tab.
8. **FIREWALL** > **Captive Portal** – Replace the **Signed Certificate** with the newly created certificate.
9. Barracuda Networks recommends to follow best practices and change all passwords.

After installing release version 6.1.3.003 on your Barracuda Firewall, it is necessary to perform a configuration update to correctly apply all improvements.

- Open **USERS** > **External Authentication** > **DC Agent** and perform a temporary configuration change of one of the available settings, and click **Save Changes**.

Barracuda Firewall version 6.1.2.002 fixes a log rotation issue to prevent filling up the SSD. [BNF-2217]
Barracuda Networks strongly recommends updating to version 6.1.2.002 or contacting Barracuda Networks Technical Support for assistance.

What's New with Barracuda Firewall Version 6.1.7.003

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

Firmware Improvements

Barracuda OS

- Updated OpenSSL to fix a potential Man-in-the-middle attack for SSL/TLS clients and servers. (CVE-2014-0224, BNSEC-4402, BNF-3715)

What's New with Barracuda Firewall Version 6.1.6

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

Firmware Improvements

Barracuda OS

- The default certificates have been re-keyed and re-issued. Old certificates are being revoked. After updating your Barracuda Firewall, all services using the unit's default certificates, will automatically use the re-issued certificates. (BNF-3480)

Network

- DynDNS over HTTPS now works as expected. (BNF-3525)

What's New with Barracuda Firewall Version 6.1.5.005

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

Firmware Improvements

Barracuda OS

- Update of OpenSSL to version 1.0.1g to fix the OpenSSL heartbleed bug. (CVE-2014-0160)

Firewall

- Fixed access to expert settings. (BNF-3452)
- Stability improvement that prevents possible appliance reboots. (BNF-2925)

VPN

- Updated Java archive manifest information of SSL VPN applets. (BNF-3376)
- The VPN service with **Local Address** set to **dynamic** will now listen on every IP address. (BNF-3402)

What's New with Barracuda Firewall Version 6.1.5.004

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

Firmware Improvements

VPN

- The VPN service with **Local Address** set to **dynamic** will now listen on every IP address. (BNF-3402)

Web Interface

- Fixed access to expert settings. (BNF-3452)

What's New with Barracuda Firewall Version 6.1.5.002

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

Firmware Improvements

Firewall

- Stability improvement that prevents possible appliance reboots. (BNF-2925)

VPN

- Updated Java archive manifest information of SSL VPN applets. (BNF-3376)

What's New with Barracuda Firewall Version 6.1.4.008

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

Firmware Improvements

Web Interface

- Adding source or destination networks, with netmasks higher than /24, to firewall rules now works as expected. (BNF-2869)
- The smart pre-submission input validation now also works correctly with DNAT firewall rules.
- It is now possible to access release notes for the latest general and early release through the **ADVANCED** > **Firmware Updates** page. (BNF-2790)
- Configuration wizards now successfully finish, even if the Barracuda Firewall receives wrong time information from an NTP server. (BNF-2777)
- Viewing product documentation within the user interface, now also works correctly when switching to a different language. (BNF-2672)

- Adding Group Filter Patterns in **USERS** > **External Authentication** now works as expected. (BNF-3178)

VPN

- It is now possible to add IPsec VPN tunnel remote IP addresses containing .255 octets. (BNF-2913)
- The SSL VPN Java security warning no longer occurs after an update to Java 7 version 54 or higher. (BNF-3049)

Firewall

- The SIP proxy now works as expected with SIP providers outside of internal network segments. (BNF-2859, BNF-2879, BNF-2691)
- Fixed a display issue in the **Basic** > **Active Connections** screen. (BNF-2887)

Networking

- Dynamic interface control commands in **Network** > **IP Configuration** now work as expected with multiple configured dynamic network interfaces. (BNF-2886)

High Availability

- Static network interfaces introduced by a wizard are now correctly synchronized to the secondary Barracuda Firewall. (BNF-2797, BNF-2796)
- When enabling an HA cluster, the firmware now performs a validity check to ensure that the units' Management IP addresses reside within the same network and subnet.

Administration & Reporting

- The SNMP service now works as expected and occasional crashes no longer occur. (BNF-2775)

Known Issues and Limitations

- When utilizing all three possible Wi-Fi Access Points, the Barracuda Firewall models X101 and X201 may freeze and/or crash under certain circumstances.

Security

- A potential internal resource exhaustion issue was fixed. (BNSEC-3144)
- A potential nginx request line parsing vulnerability was fixed. (BNSEC-2865 / CVE-2013-4547)

What's New with Barracuda Firewall Version 6.1.3.003

Web Interface

- The Barracuda Firewall User Interface is now fully Japanese localized. Note that entering multi-byte characters is not yet supported.
- Guest networks for Wi-Fi networks can now only be configured in **USERS** > **Guest Access.** (BNF-2650)

Barracuda Firewall OS

- Improved stability due to kernel upgrade and various improvements: Updated underlying Linux kernel to 2.6.28.
- Time zone upgrades for South Africa and Israel per new 2013 DST settings.

Firmware Improvements

Web Interface

- The configuration progress spinner animation now loads correctly while saving configuration changes. (BNF-2350)

High Availability

- Secondary Barracuda Firewall units now correctly synchronize configuration data after an outage. (BNF-2746)
- Barracuda Firewalls with configured dynamic WAN interfaces can now be deployed in HA clusters as expected. (BNF-2685)
- Various stability related firmware improvements. (BNF-2742, BNF-2740, BNF-2738, BNF-2703, BNF-2686)

VPN

- A certificate upload issue in **VPN** > **Certificates** was fixed. (BNF-2699, BNSEC-2398)
- The Barracuda Firewall now accepts all ASCII characters, except #, as Site-to-Site IPsec pre shared key. (BNF-2648)
- SSL-VPN now also supports RDP for Microsoft Windows Server 2003 editions and higher. (BNF-2731)

Firewall

- Manually overriding bandwidth policies is **Basic** > **Active Connections** is now correctly disabled, if QoS is disabled in the respective firewall rule. (BNF-2443)
- Enabling or disabling PAT in Connection Objects now works as expected. (BNF-2668)
- The configured name of dynamic network interfaces is now correctly displayed in **NETWORK** > **Routing**. (BNF-2713)

Authentication Services

- Received login information from the Barracuda DC Agent now expire after a certain period of time. (BNF-2434)

Known Issues and Limitations

- When utilizing all three possible Wi-Fi Access Points, the Barracuda Firewall models X101 and X201 may freeze and/or crash under certain circumstances.