Barracuda Firewall Release Notes 6.6.X

https://campus.barracuda.com/doc/42042927/

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.

Security Advisories

Barracuda Firewall Release 6.6.2.006

6.6.2.008 includes OpenSSL updates to fix vulnerabilities described in the following security advisories:

- CVE-2015-0286
- CVE-2015-0287
- CVE-2015-0289
- CVE-2015-0292
- CVE-2015-0293

Barracuda Firewall Release 6.6.1.002

All Barracuda Firewalls automatically received BNSEC-2.1.15715 (2015-01-30) to fix vulnerabilities described in security advisory CVE-2015-0235 (GHOST). If you disabled **Automatic Updates**, update to version 6.6.1.002.

Barracuda Firewall Release 6.6.0.019

6.6.0.019 includes updates to mitigate potential man in the middle attacks due to security vulnerability CVE-2014-3566 (POODLE). The following software modules are vulnerable to attacks described in the security advisory:

- **User Interface** – As of version 6.6.0.019, SSLv3 is disabled by 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 that include support only for SSLv3 can connect to these services by using the SSLv3 protocol. Connections by browsers supporting the newer TLS protocols are not allowed to fall back to SSLv3.

What's New in Barracuda Firewall Versions 6.6.2.006 and 6.6.2.008

Barracuda Firewall version 6.6.2.008 is a maintenance release and contains no new features.

Firmware Improvements

- Improved HTTP and HTTPS stability and connectivity when using SSL Inspection and Virus Protection in the Firewall. (BNF-4860)
- It is now possible to use more than 64 URL Filter whitelist or blacklist entries. (BNF-4877)
- Content of predefined Service objects is now displayed as expected. (BNF-4556)
- DC Agent authentication now works as expected. (BNF-4865)
- Using wildcard characters on the Live and Recent Connection pages now works as expected. (BNF-4632)
- Joining the Barracuda Web Security Service now works as expected. (BNF-4876)
- Improved connection handling for MSAD authentication. (BNF-4778)

Important Migration Steps

Enable **TCP Stream Reassembly** in **FIREWALL > Settings** if you are using Virus Protection in the Firewall.

Known Issues and Limitations for 6.6.2.008

- The correct format for the Path of a custom application object is: Remove the first **/** and escape wildcard characters (* and ?) that are part of the Path with a backslash (\). For example if the URL is https://example.com/user/search.do?resetForm=yes the path can be entered as: `user/search.do\?resetForm*` where the * is used as a wildcard character and ? is escaped with a backslash because it is part of the original URL.

What's New in Barracuda Firewall Version 6.6.1.005

Barracuda Firewall version 6.6.1.005 is a maintenance release and contains no new features.

Firmware Improvements

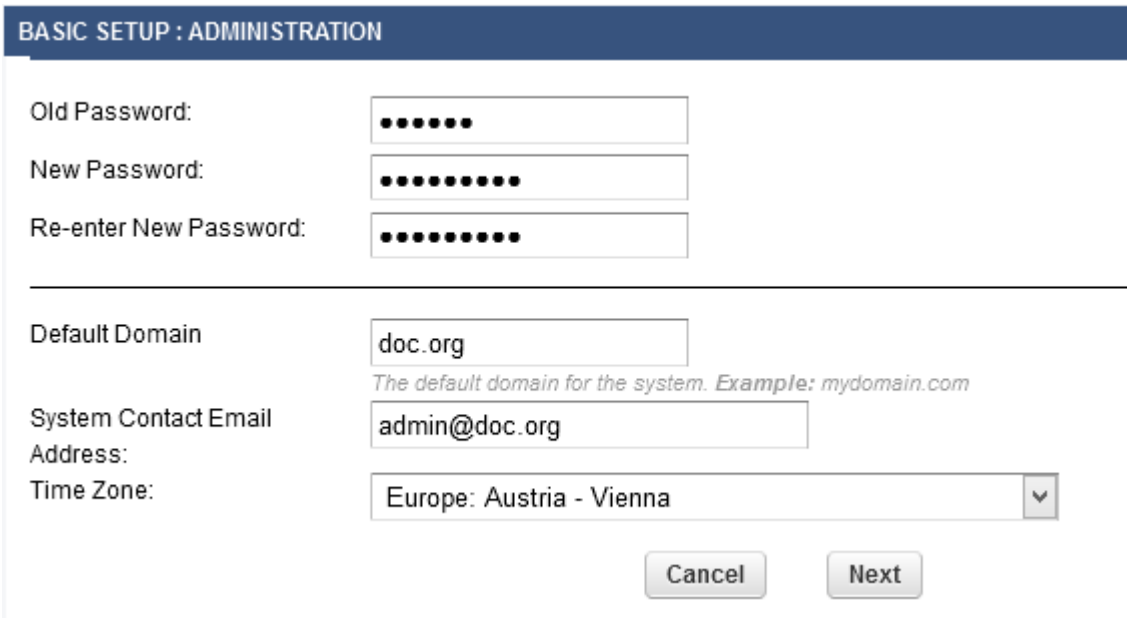
- It is now possible to open the support tunnel via Barracuda Cloud Control. (BNF-4918)
- Changing timezone and management IP address via wizard now works as expected. (BNF-4964)
- **Test at my desk** wizard no longer offers the option to set the default gateway. (BNF4953)
- DNS servers are optional in the **Basic Setup Wizard**. (BNF-4952)
- Checking the Barracuda Websecurity subscription expiration now works as expected. (BNF-4977)
- The offline activation link is no longer shown in the dashboard. (BNF-4951)

What's New in Barracuda Firewall Version 6.6.1.002

Barracuda Firewall version 6.6.1.002 is a maintenance release following 6.6.1.001 EA to fix the security vulnerability described in CVE-2015-0235 (GHOST).

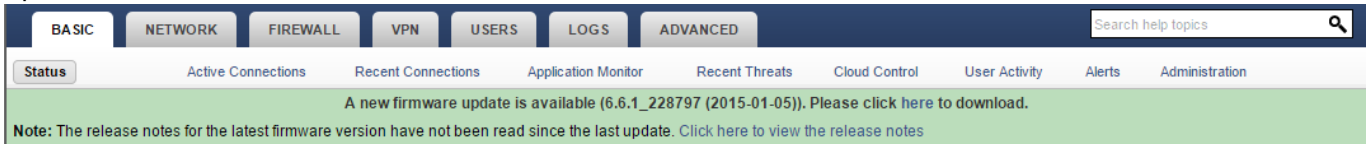
New Basic Setup Wizard

To make setting up a new Barracuda Firewall easier, the new Basic Setup Wizard will guide you through configuring all basic settings required to get up and running. You can also launch the Wizard from the **ADVANCED > Wizard** page.



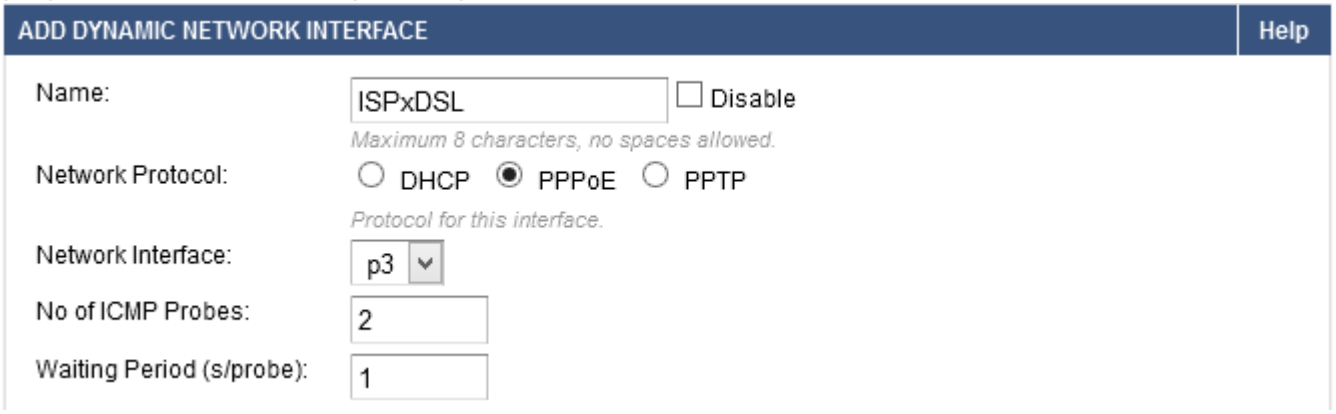
Firmware Notification

The Barracuda Firewall now notifies the admin if a new firmware version is available. If automatic updates for Security Definitions are disabled, you will also be notified if new Security Definition updates are available.



Configurable Gateway Health Check for PPPoE and PPTP

You can now configure how frequently the gateway IP address for a PPPoE or PPTP connection is pinged and after how many failed probes the connection is restarted.



Virus Protection

The Barracuda Firewall now scans these additional MIME types by default:

- MS Office
- Android APK
- PDF

Firmware Improvements

Web Interface

- Opening a support tunnel in the web interface now works as expected. (BNF-4663)
- **BASIC > Active Connections** now display values in the **Bytes/s** column as expected. (BNF-4596)
- Filters for the **Info** column on the **BASIC > Recent Connections** page now work as expected. (BNF-4577)
- Testing the configuration for external authentication servers defined in **Users > External Authentication** no longer return false positives. (BNF-4566)
- The **SSL Inspection** section on the **FIREWALL > Settings** page now displays as expected

when using Mozilla Firefox. (BNF-4543)
- Input validation was fixed to avoid Active Directory users in the DOMAIN\user format. (BNF-4415)
- Increased web interface timeout to fix "Internal Error Occurred" messages. (BNF-4333)
- **Save** and **Cancel** buttons are now disabled after the form has been submitted. (BNF-4286)

Firewall

- Adding additional entries to an existing NAT object now works as expected. (BNF-4503)
- **Redirect to Service** Access rules with the redirecting to the SSL VPN service now work as expected when the Barracuda Web Security Service is enabled. (BNF-4410)
- Fixed rare Traffic Shaping issue causing the system to crash. (BNF-4393)
- By default SSLv3 is disabled for SSL Inspection to mitigate the OpenSSL POODLE vulnerability. If needed, you can enable SSLv3 for SSL Inspection in **FIREWALL > Settings**. (BNF-4641)

Barracuda OS

- Network interruptions no longer occur on Barracuda Firewalls that do not have a Web Security Subscription. (BNF-4665)
- Dynamic network interfaces with PPTP enabled no longer start automatically when the connection start method is set to manual. (BNF-4497)
- MS-CHAP authentication configuration no longer requires a WINS server. (BNF-4463)

Barracuda Cloud Control

- Health State for the Barracuda Firewall is now displayed as expected on the Status page of the Barracuda Control Center. (BNF-4510)
- Charts on the Status page now display as expected in the Barracuda Control Center (BNF-4510)
- **Help** button now works as expected in Barracuda Cloud Control. (BNF-4511)

Report Creator

- The login to the Barracuda Firewall from the Barracuda Report Creator works as expected. (BNF-4417)

Barracuda Web Security Service

- Unauthenticated users are now able to connect via Web Security Service when **Enforce Authentication** is set to **No**, and **Include User Information** is set to **YES**. (BNF-4317)

Known Issues and Limitations for 6.6.1.002

- **Firmware Update** – Your session may time out during verification of the update package on the smaller X100 and X200 Barracuda Firewalls. Log in again to complete upgrading.
- **Backup** – It is not possible to restore old 6.0.X, 6.1.X or 6.5.X backups on a Barracuda Firewall using firmware 6.6.0 or newer.

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

Important Migration Steps

If you are experiencing problems with accessing streaming video or audio for connections using SSL Inspection, enable **TCP Stream Reassembly** in **FIREWALL > Settings**.

What's New with Barracuda Firewall Version 6.6.0.019

Virus Protection

The Barracuda Firewall now supports both virus protection on the box and in the Cloud using the Barracuda Web Security Service. On-box virus protection is enabled individually for each access rule. If a virus or malware is detected, the file is discarded and the user is redirected to a block page. Detected viruses and malware are displayed on the **BASIC > Recent Threats** page. An active Web Security subscription is required to use virus protection on the Barracuda Firewall.

SSL Inspection for Virus Protection and IPS

SSL inspection can now be used in combination with virus protection and the Intrusion Prevention System (IPS). If you do not want to scan certain websites you can now define URL Filter categories which will be exempted from SSL inspection.

Authoritative DNS

The updated ADNS service can now serve ADNS requests on both static and dynamic interfaces. You can define a health check per IP entry in a DNS record. IP entries for which the health check fails are excluded from DNS responses.

Terminal Server Agent

The Terminal Server Agent allows the Barracuda Firewall to enforce user policies for users logged in to a Microsoft Terminal Server 2008 R2 or newer. The Barracuda Terminal Server Agent on the Microsoft Terminal Server will transmit all user information to the Barracuda Firewall over an optionally SSL encrypted connection.

SIP Proxy Enhancements

The Barracuda Firewall now provides more control and access to advanced settings for the SIP proxy.

Health Checks for Static Routes

You can now define health check targets for a static routes. The Barracuda Firewall will periodically

ping all IP addresses defined as a **reachable IP** for the custom route. When one or more of these IP addresses are no longer reachable, the route is disabled until they are reachable again. You can define the heath check targets by clicking **Options** next to the custom route and adding IP addresses to the **reachable IPs** list.

Wizard for VPN Setup

It is now possible to create client-to-site VPN connections by using the **Remote Access For my Users** wizard (**ADVANCED > Wizards**). The wizard will guide you through the process of creating a client-to-site VPN for your mobile devices and remote users.

Additional DHCP Server Options

The Barracuda Firewall now provides additional DHCP options. **Vendor Options** and **Client IDs** can now be specified in the DHCP server configuration.

LDAP and Active Directory Authentication Browser

To simplify the creation of user and group policies the Barracuda Firewall now provides an easy-to-use interface to search through your LDAP or Active Directory servers. Users and groups can be added directly from the authentication browser to user objects.

Firmware Improvements

Web Interface

- Unknown applications are now displayed correctly. (BNF-4116)
- It is no longer possible to save a SNMP configuration without setting the SNMP version parameter. (BNF-4057)
- Browser certificate for SSL Inspection can now optionally be downloaded directly by users. (BNF-4021)
- The MAC address column in the **Interface** table on the **NETWORK > Routing** page now displays the MAC addresses as expected. (BNF-4001)
- Input and output interface now displayed correctly in **BASIC > Active Connections**. (BNF-3930)
- Saving the dashboard presets now works as expected. (BNF-3877)
- Filtering for **Type** in **BASIC > Application Monitor** now works as expected. (BNF-3876)
- Fixed input validation for creating a new connection object. (BNF-3872)
- Fixed input validation for creating a new service object. (BNF-3869)
- Filtering for **Severity** on the **VPN > Service Log** now works. (BNF-3863)
- Fixed duplicate custom widget issue on the **BASIC > Status** page. (BNF-3444)

Firewall

- Fixed activating/disabling redirect-to-service access rule for Barracuda Web Security Service. (BNF-3786)

Barracuda OS

- The **Protect My Network** wizard now works as expected when creating a new interface of the same type on the same interface. (BNF-3926)

DHCP Server

- The DHCP server now works as expected on bridged interfaces. (BNF-4072)

QoS

- Values entered for QoS **Choke Limit** are now validated correctly. (BNF-4073)
- QoS **Internet Degradation Threshold** now works as expected. (BNF-4056)
- Fixed the QoS profile for system updates. (BNF-3976)
- Resetting the QoS values now works as expected. (BNF-3820)
- **Bandwidth Policies** are now displayed and assigned correctly. (BNF-3685)

High Availability

- **Users > Guest Access** Login page options are no longer editable on the secondary HA unit. (BNF-3919)
- PPTP options are no longer editable on the secondary HA unit. (BNF-3918)
- Forwarding Proxy settings are no longer editable on the secondary HA unit. (BNF-3917)
- SNMP Manager settings are no longer editable on the secondary HA unit. (BNF-3916)

VPN

- Static IP address assignment is no longer allowed when using PPTP with MS-CHAPv2 or NTML authentication. (BNF-3876)
- Uploading password protected PEM certificates is no longer allowed. (BNF-3757)
- Fixed automatic network objects for site-to-site VPNs. (BNF-3711)
- Displayed route status for PPTP client-to-site VPN interface fixed. (BNF-3642)

SSL VPN

- The **Tunnel Client Application** parameter is no longer disabled after selecting IMAP4, POP3 and SMTP for an application resource. (BNF-3915)
- Fixed missing WebDAV sharename parameter when editing Network Places. (BNF-3914)

Wi-Fi

- A warning message displays if you try to edit a static Wi-Fi interface or a DHCP Server configuration using a disabled Wi-Fi interface. (BNF-4051)
- Fixed Wi-Fi configuration validation. (BNF-4030)

Guest Networks

- RADIUS authentication now works with the captive portal as expected. (BNF-3905)
- The Wi-Fi networks are now selectable as a guest network. (BNF-3861)
- Captive portal authentication errors are now logged to **LOGS > Authentication Log**. (BNF-3434)

Backup

- It is now possible to use a relative path for FTP backups. (BNF-3458)

Known Issues and Limitations for 6.6.0.019

- **Firmware Update** – Your session may time out during verification of the update package on the smaller X100 and X200 Barracuda Firewalls. Log in again to complete upgrading.
- **Backup** – It is not possible to restore old 6.0.X, 6.1.X or 6.5.X backups on a Barracuda Firewall using firmware 6.6.0 or newer.
- **Barracuda Report Creator** – Only available for Microsoft Windows 7 and 8.
- **Web Interface** – On the **BASIC > Active Connections** page the **Bytes/s** column always shows **0.00**.
- **Notifications** – System alert email notifications are currently not correctly delivered to configured recipients.

Important Migration Steps

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

- **Traffic Shaping (QoS)** – Go to **FIREWALL > QoS** and do a dummy change to activate new QoS settings for firmware updates.

Figures

1. releaseNotes662.png
2. basic_wizard_00.png
3. firmware_update_popup.png
4. ICMP_Probes.png