Release Notes

https://campus.barracuda.com/doc/9011724/

Important: Please Read Before Upgrading

Make a backup first. Before installing any firmware version, back up your configuration and read all release notes that apply to versions more recent than the one currently running on your system.

Do not manually reboot your system at any time during an upgrade, unless otherwise instructed by Barracuda Networks Support. The upgrade process typically takes only a few minutes after the upgrade is applied. If the process takes longer, please contact Technical Support for further assistance.

Firmware Version 16.0

Important: **Please read the following before upgrading to version 16.0:**

- When upgrading the firmware from version 15.x version to 16.0 or higher, the Web Categorization Service (WCS) version is updated from version 2.x to 3.x (see Web Use Categories). All the existing Barracuda Web Security Gateway policies, Exceptions, Content Filters and the Barracuda Web Security Gateway web interface are updated to reflect WCS 3.x categories. Because mapping of WCS 2.x categories to WCS 3.x categories is not exactly 1:1, some policies will shift. Some categories will appear more granular in the latest version of WCS 3.x on firmware 16.0.
- Reporting data is cleared.
- The dashboard data is reset.
- All data is cleared and starts from scratch after upgrading to 16.0.
- Web Logs are cleared.
- If you revert back to firmware version 15.0, your data and configuration will be what it was before updating to version 16.0, whether you were running WCS 2.x or 3.x on version 15.0 before you updated to 16.0.
- If you upgrade to version 16.0 and you have Barracuda Web Security Agent installations in the field:
  - If you have set up passwords on the agents, then you must upgrade your Barracuda WSA installations to version 6.0. If not, activities that require password permissions on the endpoint will no longer work with the password.
  - If you were not using passwords, then you can continue using older versions of the Barracuda WSA. However, Barracuda Networks recommends upgrading to version 6.0.
  - See also Release Notes for the Barracuda Web Security Agent version 6.0.

What's New in Version 16.0

- Microsoft Office 365, Skype, and MS Team related Microsoft Servers are exempt from inspection by default.
- Session/idle timeout parameters configured on the **USERS > Configuration** page now also apply to wireless access point login events.
- New **Remote Devices** panel on the **Dashboard** page listing Username and number of devices being protected by the Barracuda Web Security Gateway. Filter on **Last Hour**, **Last 7 days**, or **Last 30 days**.
- The **Location** column has been removed from the **BASIC > Remote Devices** log as Barracuda Safe Browser is no longer supported on mobile devices.
- Support for 16 additional Web Categories.
- Signing Support for LDAP server with Kerberos authentication.
- Terminology updates: from Whitelist --> Allow List and from Blacklist --> Block List.
- A banner is now displayed on the **BASIC > Dashboard** page for lower end models when Barracuda Content Shield is integrated with the Barracuda Web Security Gateway.
- Added HTTPS traffic support for peer proxy.
- On the **BASIC > Virus Checking** page, you can exempt trusted domains from going through ATP inspection.
- Ability to enable or disable firmware patches using the **Product Patch Management** section of the **ADVANCED > Configuration** page.
- The system uptime is now displayed in the Performance section of the **BASIC > Dashboard** page.
- Option to upload a certificate on the **USERS/GROUPS > Authentication** page for use with LDAPS.
- Option to enable the Auxiliary Port using the Administrative Console. See How to Enable Auxiliary Port Access.
- Option on the **ADVANCED > Configuration** page to enable sending outbound web traffic through a forward proxy configuration.
- The **Connection Status** and **Synchronization Latency** fields have been removed from the **ADVANCED > Linked Management** page, and help content has been revised for better ease of use.
- The **Category Definition Updates** section of the **ADVANCED > Energize Updates** page has been removed.
- The Barracuda Web Security Gateway users Web Categorization Service (WCS) version 3.0 by default.
- The ATP scan page can now be served over HTTPS as well as HTTP. Note that the user sees a warning prompt with ATP block pages and will have to click to accept the risk and continue.
- The **LDAP Server Timeout** and **LDAP Full Sync** settings have been moved to the **LDAP Settings** section of the **USERS/GROUPS > Authentication** page.
- The **Apply Session Parameters to DC Agent** setting has been moved to the **DC Agent Configuration** section of the **USERS/GROUPS > Authentication** page.
- Validations checks are provided when certificates are uploaded to these pages in the web interface:

    - **ADVANCED > Secure Administration**
    - **ADVANCED > SSL Inspection** (Available Certificates)
    - **ADVANCED > SSL Inspection** (SSL Certificate)
    - **ADVANCED > Remote Filtering**
- The Barracuda Chromebook Security Extension supports WCS version 3.x.
- Support for Skype for Business/Office365 in WCCP mode with the Cisco ASA.
- The Barracuda Web Security Gateway now sends an email alert notification to the administrator when a firmware version is released as GA (general availability).
- Added support for TLS 1.3.
- OpenSSL version upgrade to include support for TLS 1.3, and this version eliminates support for weak ciphers and old SSL protocols, thereby eliminating various security vulnerabilities.
- Novell eDirectory is no longer supported.
- Typosquatting settings are no longer supported.
- The Barracuda Reporting Server is no longer supported.
- An email alert notification is sent to the **System Contact Email Address** when Barracuda Web Security Gateway firmware is released as GA (General Release). The **System Contact Email Address** is configured on the **BASIC > Administration** page.
- Added support for downloading a missing Intermediate CA. [BNYF-23283]
- Improvements to log handling.
- Improvements to proxy authentication handling.
- Added support for Intercom.

Fixed in Version 16.0

- Fixed: Error when clicking the download link next to **Download Web Security Agent**, Apple Mac OS X 10.5 DMG version on the **ADVANCED > Remote Filtering** page. [BNYF-22934]
- Fixed: Allowed sites for inline web traffic is not logged with both HTTPS Filtering, and the HTTPS block page features enabled on **BLOCK/ACCEPT > Configuration** page and SSL Inspection is disabled and on the **BLOCK/ACCEPT > Web App Monitor** page, all of the Actions for Web Application Monitoring are enabled. [BNYF-22920]
- Kerberos users/groups lookups do not return an error when LDAP signing is enabled on the domain controller server. [BNYF-22158]
- Reports printed in PDF format work as expected. [BNYF-22413]
- When a specific category is selected, the **Users by**... reports no longer display data for all categories; the selected category filter applies as expected for this particular reports group. Only HTML reports were affected. [BNYF-20162].
- Emailing reports, upload/restore backup, and running manual backups (running once/immediate) work as expected on all hardware versions. [BNYF-16399]
- SNMP works as expected on all hardware versions. [BNYF-16322]
- Static routes are created as expected under the advanced routing table when VLANs are configured. [BNYF-16152]
- Logins to the Barracuda Web Security Gateway web interface for Delegated Admin roles work as expected after a firmware upgrade. [BNYF-15805]
- Time stamps on block pages are correct. [BNYF-14572]

- Log data rotates as expected (preventing logs from becoming too large). [BNYF-16637]
- Inline web traffic for allowed sites is logged as expected with both HTTPS filtering and HTTPS block page features enabled on the **BLOCK/ACCEPT > Configuration** page, SSL Inspection disabled, and Web Application Monitoring enabled. [BNYF-22920]
- Fixed issue where, in a clustered system, users who had idle and session timeout applied to them via the DC Agent were logged out (some hardware versions). [BNYF-22022]
- Added access.log to log rotation (set **Enable W3C Logs** to *Yes* on the **ADVANCED > Syslog** page). [BNYF-16632]
- BNYF-16282 : Fix for vulnerability CVE-57608
- Reporting/Log Storage displays as expected on the **BASIC > Status** page. [BNYF-16094]
- Fixed issue where, after re-imaging the appliance and bringing the firmware back to 15.0.0.009, then restoring the backup, policies were not being met due to the re-imaged appliance running WCS 2.0 and the backup being in WCS 3.0. [BNYF-23351]
- After changing the Locale on the **BASIC > Administration** page, J apanese text renders as expected on the block page. [BNYF-23053]
- When policies for MIME types are triggered on the Barracuda WSA, the client is redirected to the block page as expected. [BNYF-23494]
- Added mechanism to reboot the appliance when the system stalls. [BNYF-23487]
- Fixed issue where, in the Top Super Category graph, super category News and information was being incorrectly counted. [BNYF-23579]
- When updating the firmware from version 15.0 using WCS 2.0 to firmware version 16.0, all categories are migrated properly per WCS 3.0. [BNYF-23587]
- When updating the firmware from version 15.0 using WCS 2.0 to firmware version 16.0, all categories inside a custom category are migrated properly to WCS 3.0 categories. [BNYF-23607]
- After updating the firmware to the 16.0.011, all web, applications, and ATP Logs load as expected and the *Temporarily Unavailable* no longer appears. The Dashboard also displays Statistics and Graphs as expected. [BNYF-23650]
- Scheduled reports are not being deleted upon updating to 16.0 for the first time. [BNYF-23654]

Firmware Version 15.0

What's New in Version 15.0

Web Interface

- **Barracuda Content Shield (BCS) Integration** – The Barracuda Web Security Gateway can be configured to use the BCS Cloud Web Filtering Service to create and manage web filtering policies in the cloud with the easy-to-use BCS web interface. See Using Barracuda Content Shield With the Barracuda Web Security Gateway.

Policies

- Support for Web Categorization Service (WCS) version 3.0. See Web Use Categories and Web

Categorization Upgrade for Barracuda Web Security Gateway 15.x.

Backup

- Added support for SMB v2 and v3.

Logs

- Increased log storage based on model:
  - 250K log storage on the Barracuda Web Security Gateway 310
  - 500K log storage on the Barracuda Web Security Gateway 410
  - 750K log storage on the Barracuda Web Security Gateway 610
  - 1M log storage on the Barracuda Web Security Gateway 810
  - 1.25M log storage on the Barracuda Web Security Gateway 910
  - 1.5M log storage on the Barracuda Web Security Gateway 1010/1011

Miscellaneous

- Novell e-Directory authentication is no longer supported for the Barracuda Web Security Gateway.
- The option to download the **Barracuda Safe Browser** has been removed from the **ADVANCED > Remote Filtering** page.

Fixed in Version 15.0

- Fixed issue with latency for some inspected sites that were having reverse DNS lookup issues. [BNYF-15991]
- NTP synchronization works as expected with default server update01.barracudanetworks.com. [BNYF-15904]
- The HTTPS Blockpage option works as expected when **HTTPS Filtering** is enabled on the Barracuda Web Security Gateway 310Vx. [BNYF-13449]

Version 15.0.0.014

- Fixed: SNMP implementation on recent hardware revision for the Barracuda Web Security Gateway 410 and 810 models. [BNYF-16323]
- Fixed: Database error issue in the new downloadable VM images. [BNYF-20392]
- Fixed: Default NTP server name on **BASIC > Administration** page no longer shows an appended '0' after applying a new firmware version. [BNYF-16347]
- Fixed: Clustering issue where full sync was happening when only a partial sync was required. [BNYF-15707]
- Fixed: UTF-8 Characters now display properly in all parts of the web interface. [BNYF-5247]
- Fixed: Handling of username when NTLM authentication is enabled when interfacing with

Barracuda Content Shield. [BNYF-10909]

Version 15.0.0.009

- Added support for new hardware drivers.
- Improvement : Policy synchronization with chromebooks. [BNYF-16274, BNYF-16275]
- Addressed issue related to enabling connection with Barracuda Networks Support. [BNYF-16281]

Version 15.0.0.004

- Fixed: **Twitter** section on **BLOCK/ACCEPT > Web App Monitoring** page is titled correctly. [BNYF-15524]
- Fixed: Adding a Google Directory Service no longer gives a Google 400 error. [BNYF-16159]
- CVE-2018-5390 - Linux Kernel TCP implementation vulnerable to Denial of Service.
- CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479 – TCP SACK Panic vulnerabilities.

Firmware Version 14.1

KNOWN ISSUE

- When connecting to the Barracuda Reporting Server and the join is successful, the error message "Error: Network connection failed. System will automatically reconnect to the Barracuda Reporting Server when network becomes available." is displayed in the web interface. [BNYF-14761]. After reloading the **ADVANCED > Log/Report Settings** page, it shows "Barracuda Reporting Server connection established."
- When the Barracuda Web Security Gateway is upgraded to version 14.1.0, you must also upgrade the Barracuda Reporting Server to version 1.0.3 or higher. With these versions, the **Barracuda Reporting Server Serial** is required on the **ADVANCED > Log/Report Settings** page.

What's New in Version 14.1

- **Enable HTTPS Blockpage** – Ability to configure whether or not to serve the user a block page when HTTPS access is denied. Configure on the **BLOCK/ACCEPT > Configuration** page.
- Added **Throughput** and **Active Users** graphs on the **BASIC > Dashboard** page.
- **Upload WPAD/PAC** – Ability to upload a WPAD or PAC file instead of setting the client browser proxy to the Barracuda Web Security Gateway IP address on port 3128. The WPAD or PAC file specifies a URL to use for the proxy. Configure on the **ADVANCED > Proxy** page.

Web Interface

- Drop-down **Help** button control on some web interface pages, providing links to relevant Barracuda Campus articles for additional information about features configured on those pages.

- Added **ADVANCED > Log/Report Settings** page for configuring:
  - **Reports From Address** – The email address from which the Barracuda Web Security Gateway emails reports.
  - **Enable Referer Tracking in Reports** – To simplify report results, browse sessions are grouped by referer. Note that if this feature is enabled, both the referer domain and the referer category will be captured in the syslog.
  - **Hide Existing Categories When Excluding Parent Custom Category** – Setting to *Yes* hides any categories that have been added to a custom category from report data if you exclude that custom category from the report.
  - **Session Timeout in Reports** – For better accuracy in reporting on session time for browsing, sessions with no active traffic after the number minutes specified will be considered to be 'ended' by the Barracuda Web Security Gateway.
  - **Report Retention Days** – Indicates the number of days, up to 6 months, for which you the Barracuda Web Security Gateway should store reporting data.
  - **Show Full URL in Logs** – Provides option for the Barracuda Web Security Gateway to capture the query string portion of URLs in the **Web Log**.
  - **Enable Privacy Option** – When enabled, this option prevents user names from appearing in the traffic log or any reports.
  - **Anonymize NTLM User** – Provides option to log NTLM users as anonymous.
  - **Barracuda Reporting Server** – Option to connect to and use the Barracuda Reporting Server.
- Added **ADVANCED > Configuration** page with options to:
  - **Enable Spyware Protocol Filter** – Provides option to either allow or not allow the Barracuda Web Security Gateway to scan non-HTTP ports for spyware activity.
  - **Exempted Ports** – The ports you enter here are exempted from being examined by the Spyware Protocol scanning module.
  - **Enable WCS Support** – For content filtering, provides the option for the Barracuda Web Security Gateway to fetch the top 2 million domains and respective categories from the Barracuda Web Categorization Service in a one-time download, and the **Category Definition Updates** are set to *Off*. Categories for domains not in the top 2 million are fetched as needed. Disabling this feature means the local web categorization database on the Barracuda Web Security Gateway is used, with the **Category Definition Updates** running automatically as needed. For best system performance on lower Barracuda Web Security Gateway models, Barracuda Networks recommends enabling this feature.
  - **Feature Code** – Enables entry of specific feature activation codes provided by Barracuda Networks Support if needed.
  - **Pass Client IP addresses through WAN port** – Provides option to specify whether the Barracuda Web Security Gateway is to expose or hide client IP addresses in egress HTTP traffic.
  - Option to configure offline firmware updates if needed.

SSL Inspection

- New ability to add Certificate Authority (CA) certificates to the Barracuda Networks `ca-bundle.trust.crt` by uploading the SSL Certificate on the **ADVANCED > SSL Inspection** page.

Advanced Threat Protection (ATP)

- The ATP service now gives a 60 day warning on the **BASIC > Dashboard** page before the associated license expires.

Fixed in Version 14.1

- Group-based exceptions no longer fail if the LDAP group name format is `groupname@domainname.com` . [BNYF-15159]
- Fixed issue with some HTTPS sites failing to load when using the IE browser with QAT SSL hardware enabled. [BNYF-15253]

Version 14.1.0.021

- Added support for new hardware drivers.

Version 14.1.0.01 6

- Support for minor changes in the hardware.

Version 14.1.0.014

- The **Application Blocks** report in CSV format displays Application Name as expected. [BNYF-15789]
- Exceptions applied to nested Groups work as expected when using NTLM authentication. [BNYF-15814]
- In **Users By Requests** report, the LDAP Alias Name displays as expected in CSV format output. [BNYF-15791]
- When the HTTPS Filtering and HTTPS Blockpage features are enabled on the model 310 running 14.1.0 firmware, and SSL Inspection is disabled, a block page is presented for blocked HTTPS websites as expected. [BNYF-15793]
- NTLM Group exceptions based on Nested Group names with mixed case letters do not fail in versions 14.0.0 and 14.1.0.012. [BNYF-15814]

- Fixed: Kernel vulnerabilities - CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479. [BNYF-15819]

Version 14.1.0.012

- When Barracuda Web Security Gateway systems are clustered, or when the cluster Mode of a system in a cluster is changed, Barracuda Web Security Gateway internal processes are cleaned up as expected. [BNYF-15757]

Version 14.1.0.010

- Fixed issue with CSV based reports displaying current year for last year's data. [BNYF-15656]
- Timeout time frame for ATP scanning is increased from 10 to 30 seconds for **Scan First, then Deliver** option. [BNYF-15662]
- Windows updates work as expected when ATP **Scan First, then Deliver** option is enabled. [BNYF-15713]

Version 14.1.0.006

- Fixed issue seen in version 14.1.0.005 where login as *admin* failed when client machine proxied through the Barracuda Web Security Gateway on Port 3128, and the **Send Forwarded-For Header** feature on the **ADVANCED > Proxy** page was disabled. [BNYF-15634]
- Fixed issue seen in version 14.1.0.005 where login as *admin* failed when client machine proxied through the Barracuda Web Security Gateway on Port 3128, and **Supported SSL Protocols** was set to *TLSv1* on the **ADVANCED > Secure Administration** page, and **Web interface HTTPS/SSL Port** was set to *443* on the **ADVANCED > Secure Administration** page, and **Send Forwarded-For Header** was set to *Yes* on the **ADVANCED > Proxy** page . [BNYF-15620]

Version 14.1.0.005

- Capitalized letters in domain names no longer cause nested group policies to fail for Kerberos groups. [BNYF-15354]
- Fixed issue with users in OUs losing group membership. [BNYF-15443]
- Fixed issue where new system password was synchronized across clustered systems. [BNYF-15533]

Version 14.1.0.004

- New reports including Active Users, Active Users Log, Throughput Usage, and Throughput Log.
- The **HTTPS Filtering** feature configured on the **BLOCK/ACCEPT > Configuration** page can be enabled as expected when the **Enable Auxiliary Port** feature is set to *Yes* in the consconf. [BNYF-15436]