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 Technical 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.

> When reverting from version 12.0 to version 11.0, if you are using the Barracuda Chromebook Security Extension, the configuration file created on the **Chromebook Extension** tab of the **ADVANCED > Remote Filtering** page needs to be re-uploaded to the Google Admin console.

When upgrading a Barracuda Web Security Gateway to version 11.0 or higher, please note the following:

- For the Barracuda Web Security Gateway Vx, make sure the virtual machine has 4 GB of RAM or more before upgrading. See also Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Web Security Gateway Vx.
- The virus checking feature as configured on the **BASIC > Virus Checking** page now offers blocking files based on file type, *not* just MIME type as in previous versions. Barracuda recommends that the admin select file types to block with virus checking and/or ATP on that page after upgrading.
- If you are using NTLM authentication, you now need to specify a Realm, which is your Windows administrative domain name. The default setting after upgrade is the **Default Domain** you configure for the Barracuda Web Security Gateway on the **BASIC > Administration** page. To change this default value, configure on the **USERS/GROUPS > Authentication** page on the **NTLM** tab.

Only backups from version 7.1 and higher are accepted by version 9.0 and higher. If you have a backup from version 7.0.x or earlier, please contact Barracuda Technical Support for assistance.

Firmware Version 14.1

- 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 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 `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 14.1.0.014

- 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]

Firmware Version 14.0

- If you are running/joining the Barracuda Reporting Server with the Barracuda Web Security Gateway version 14.0, you may see several errors when trying to connect before connection succeeds. [BNYF-14761]
- When the Barracuda Web Security Agent synchronizes with the Barracuda Web Security Gateway, a duplicate entry is erroneously created in the Remote Devices page showing the user as SYSTEM. This requires fixes in both the Barracuda Web Security Gateway firmware and Barracuda Web Security Agent client software. [BNYF-14776]
- If you currently have Novell eDirectory as a configured directory service, you should not update to the 14.0 EA version. This issue prevents connection to the directory service, which will cause user and group-based exceptions to not apply proper policy. [BNYF-13145]
- If you are upgrading from version 12.x and had set a custom system password, that password works with version 14.0, but if you revert back to version 12.0, the same custom password is replaced by the default "admin" and must be re-set to the desired custom password. When doing so, use "admin" as the *old* password. [BNYF-14872]

What's New in Version 14.0

Virus Scanning

- **Advanced Threat Protection (ATP)** – Added **Scan First, then Deliver** option. Configure on the **BASIC > Virus Checking** page. If scanning of the file for download completes immediately, and a virus is detected, the user is served a standard block page indicating that the file has been blocked for that reason. If the scan takes longer to complete, the user is redirected to a page with a message indicating that the file is still undergoing scanning. The user can continue browsing, checking back to the new tab, which auto-refreshes, for a status update on the file being scanned. See Advanced Threat Protection Configuration for more information. ATP is available with version 11.0 and higher for model 310 and higher, and with version 12.0.0 and higher for the model 210.

Policies

- **Added support for blocking Skype for Business** – Configure on the **BLOCK/ACCEPT > Applications** page. Or, to block/accept Skype for Business traffic for specific users or groups of users, see the **BLOCK/ACCEPT > Exceptions** page.
- **Added support for blocking Hexatech VPN** – Option to block or allow Hexatech VPN application traffic so that users are not allowed to bypass internet traffic. Configure on the **BLOCK/ACCEPT > Applications** page.

Authentication

- Added Kerberos support for Forest deployments.

Alerts and Notifications

- **Notifications to Slack channels** – Use the **BASIC > Administration** page to configure the Barracuda Web Security Gateway to automatically email system alerts to the email addresses you specify, which optionally could be your Slack application. See How to Send System Notifications to Slack for more information.
- **Customizable SMTP server for alerts and notifications** – Customize the email domain for all emails sourced from the Barracuda Web Security Gateway by entering your SMTP server in the **SMTP Server** field in the **Email Notifications** section of the **BASIC > Administration** page.See How to Configure an SMTP Server to Send Alerts for more details and variables affected.

Reports

- If the **Hide Custom Categories** option on the **BASIC > Reports** page is enabled, relevant reports (such as **Categories by Requests**, for example) now show that this option is checked in the upper left of the report.

Fixed in Version 14.0

- Top rule priority is applied as expected after rearranging rules in the **List of Exceptions** table on the **BLOCK/ACCEPT > Exceptions** page. Specific to Barracuda Chromebook Security Extension. [BNYF-13502]
- '*Error rendering report*' message is no longer displayed for the **Most Recently Blocked Requests** table on the **Dashboard** page. [BNYF-13817]
- The Barracuda Web Security Agent now recognizes secure block page redirects as expected. [BNYF-13951]
- When **Enable HTTPS Filtering** is set to **Yes** on the **BLOCK/ACCEPT > Configuration** page, the Captive Portal Agreement page is now presented as expected for HTTPS sites. [BNYF-8201]
- The **Web Requests Log** report does not time out with an error. [BNYF-13647]
- **BLOCK/ACCEPT > Web App Control** blocking for Facebook like/unlike, share, and comments works as expected. [BNYF-10396]
- Statistics and graphs on the **Dashboard** page update as expected after clicking the **Clear Statistics and Logs** button on **BASIC > Administration** page. [BNYF-14138]
- Syslog data from some wireless access points no longer fills up storage and is processed as expected. [BNYF-13787]
- Changing the Syslog port works as expected when Enable W3C Logs is set to *Yes* on the **ADVANCED > Syslog** page. [BNYF-14564]

Version 14.0.0.014

- Group based exceptions no longer fail if the LDAP group name follows the format **groupname@domainname.com** . [BNYF-15159]
- Aruba AP syslog login is detected as expected, and requires version 1.0.9 Access Point Definitions. See the **ADVANCED > Energize Updates** page to get the latest definitions. [BNYF-15148]
- The "Temporary unavailable - 500 error" page no longer appears on some Barracuda Web Security Gateway web interface pages when the ATP **Scan First, then Deliver** option is enabled, and the Barracuda Web Security Gateway statistics on the **BASIC > Dashboard** page are not set to zero (0) . [BNYF-15214]
- Some HTTPS sites that failed to load when using IE browser with SSL Hardware enabled (see the **Performance Statistics** section of the **BASIC > Dashboard** page) now load as expected. [BNYF-15253]
- Added additional log detection for Ruckus Cloudpath wireless AP. This requires version 1.0.8 Access Point Definitions. See the **ADVANCED > Energize Updates** page to get the latest definitions. [BNYF-13954]

Version 14.0.0.012

- Time-based exception policies function as expected when the Barracuda Web Security Gateway is deployed in the **Asia: George - Tbilisi** time zone. [BNYF-15090]

Version 14.0.0.009

- Resolved issue where VLAN route does not persist after firmware upgrade. [BNYF-15076]

Version 14.0.0.007

- Delegated admin roles using LDAP authentication can now log in as expected after upgrading from version 12.0.0 to version 14.0.0.006. [BNYF-14977]
- When searching with a partial LDAP group or user, or wildcard (*), in the **Applies To** text box on the **BLOCK/ACCEPT > Exceptions** page, the search/lookup works as expected. [BNYF-14989]

Version 14.0.0.006

- If the default administrator password is changed before upgrading from firmware version 12.0.0.024 to 14.0.0.004, the Barracuda Web Security Gateway web interface login fails. [BNYF-14867]
- Fixed vulnerability with 7zip file compression. [BNYF-14918]
- The *ATP Subscription Not Purchased* message no longer changes to a *Code: -9* message after a firmware upgrade from 12.0.0.024 to 14.0.0.004. [BNYF-14938]

Firmware Version 12.0

What's New in Version 12.0

- **Policies**
  - **Dropbox Web Application Support** - Added support for Dropbox for business. Configure on the **BLOCK/ACCEPT > Web App Control** page.
  - HotSpot Shield & Anonymous proxy protection - Configure on the **BLOCK/ACCEPT > Web App Control** page.
  - **Typosquatting Protection** - Typosquatting relies on mistakes like typographical errors

made by web users when typing a URL or clicking on a misspelled website address in the browser. This feature checks for common typos in a clicked or manually typed URL domain name. When a common typo is discovered, the service redirects the user to a web page indicating that this might not be the legitimate site they intended to access, and provides the correct URL. Includes Dashboard statistics. Configure on the **BLOCK/ACCEPT > Configuration** page.

- **SSL Inspection**
  - Simplified configuration on the **ADVANCED > SSL Inspection** page. No need to specify *Transparent* or *Proxy* mode.
  - SSL Inspection certificate wizard simplifies selection, creation and upload of SSL certificates.
  - Options to exempt domains from inspection, inspect traffic from specific networks, and inspect traffic for specific users/groups.
  - Restriction on number of domains that can be inspected on lower models is removed.
  - ECDSA keys are now accepted for uploaded root certificates. Configure on the **ADVANCED > SSL Inspection** page.
- **Barracuda Chromebook Security Extension**
  - Added Google admin LDAP service support. Provides the ability to integrate and utilize Google Directory Service for user and group identification. Currently supports lookups for Reports, Exceptions, SSL inspection and Temporary Access. Configure on the **USERS/GROUPS > Authentication** page.
  - Support for Temporary Access feature.
  - Support for time-based policies.
- **Virus Scanning**
  - Advanced Threat Protection (ATP) enhancements - New statistics display on **BASIC > Dashboard** page as well as local caching of results. Improved speed of detection and block rate for subsequent downloads of infected files in the network.
- **Miscellaneous**
  - Application log now includes Username and Destination IP address.

Fixed in Version 12.0

- If session parameters are changed, logged off users appear as offline as expected on the **USERS/GROUPS > Account View** page. [BNYF-12777]
- When the **SSL Inspection** feature is set to **Off**, Dashboard performance statistics display as expected. [BNYF-12741]
- Null SMB password vulnerability (CVE-1999-0519). [BNYF-12771]
- Suspicious keywords are reported in email alerts as expected. [BNYF-12437]
- Empty suspicious keyword alert emails are no longer sent at the end of an hour when a user searches for non-suspicious keywords. [BNYF-12535]
- Checking **Hide Custom Categories from reports** on the **BASIC > Reports** page works as expected for the **Web Requests Log** report. [BNYF-12528]

Version 12.0.0.027

- Fixed issues that prevented some processes from properly restarting/reconfiguring after changing **Operating Mode** between *Active* and *Audit . [* BNYF-14170]

Version 12.0.0.024

- Feature: Ability to created nested level NTLM groups and apply exceptions at each level. [BNYF-2893]
- Updated QAT driver to fix cipher suites that use SHA-384. [BNYF-14062]
- HTTPS scanning works as expected on the Barracuda Web Security Gateway 910. [BNYF-13983]

Version 12.0.0.023

- Google Cloud Directory Sync (GCDS) allows sync as expected and instant SSL inspection works as expected. [BNYF-13598]
- Google Directory Services (GDS) domain name is no longer case-sensitive. [BNYF-13609]
- Reports configured for more than one **Limit Report to** filter no longer return *No Data Available* error. [BNYF-13638]
- After an authentication session expires, the new LDAP user logins from that client machine (same IP) are now recorded as expected by the session manager. [BNYF-13656]
- ATP reports and exported ATP Logs work as expected for large data. [BNYF-13710]
- When there are multiple **Inspected Networks** table entries on the **ADVANCED > SSL Inspection** page, all IP/subnet entry traffic is inspected as expected. [BNYF-13724]
- Enhancement: Enable ATP on 210 Systems. [BNYF-13774]

Version 12.0.0.018

- Resolved SSL Inspection connection crrors. [BNYF-13513]

Version 12.0.0.015

- Web content is not cached on the **ADVANCED > Caching** page if ATP is enabled on the **BASIC > Virus Checking** page. [BNYF-13388]
- NTLM reports list data as expected for activity for groups and usernames that include special characters (ex: ##Group). [BNYF-13323]

Version 12.0.0.012

- Hard bypass works as expected on the Barracuda Web Security Gateway 1011 running version 11.0.0.022. [BNYF-13321]
- Session manager no longer causing system load to increase on version 12.0.0.010 with the Barracuda DC Agent versions below 7.1.50. [BNYF-13242]
- NTLM Join domain result is no longer different in the web interface than the system when username/password is invalid. [BNYF-13061]
- Blocked encrypted Archives are not (should not be) logged as VIRUS. [BNYF-12868]

Version 12.0.0.010

- The secure administration certificate is regenerated when upgrading to version 12.0.0.008. If you are using the Barracuda Chromebook Security Extension, you will need to update the certificate in Chromebook browsers. See the **ADVANCED > Secure Administration** page. [BNYF-13207]
- Chrome browser version 58 does not support matching the Common Name in certificates. Certificates that rely on this deprecated behavior will now be rejected with: ERR_CERT_COMMON_NAME_INVALID. To avoid this issue, the administrator must re-generate the certificate to include a Subject Alternative Name extension, or to enable an option in Chrome to allow them. [BNYF-13168]
- NTLM join domain is successful with authentication. [BNYF-13181]
- Added Microsoft Edge browser for Windows 10 to the **Applications to Filter (All Ports)** defaults on the **Web Security Agent** tab of the **ADVANCED > Remote Filtering** page for Barracuda WSA. [BNYF-10285]
- Policy Alerts are sent as expected when a delegated admin email address is specified in the **Policy Alerts Email Address** field on the **BLOCK/ACCEPT > Exceptions** page. [BNYF-12926]
- Blocked Encrypted Archives are displayed in the Web Log as 'Encrypted Archive', not 'Virus Download'. [BNYF-13128]
- Added for Barracuda Web Security Gateway 410Vx - simplified configuration on the **ADVANCED > SSL Inspection** page. No need to specify Transparent or Proxy mode. [BNYF-13177]

Firmware Version 11.0

What's New in Version 11.0

Virus Scanning

- **Advanced Threat Protection (Available on 310 and higher)** - Advanced Threat Protection (ATP) is a subscription-based service that detects and blocks advanced malware, zero-day

exploits, and targeted attacks that are not detected by the Barracuda Web Security Gateway virus scanning features. The ATP service includes sandboxing capabilities and analyzes web traffic for viruses in a separate, secured cloud environment. Configure on the **BASIC > Virus Checking** page after subscribing. For more information, see Advanced Threat Protection Configuration. To subscribe, see the **Subscription Status** section of the **BASIC > Dashboard** page.
- **Configure Scanning by file type** - Ability to configure virus scanning by file types rather than MIME types on the **BASIC > Virus Checking** page. You can also configure virus scanning by MIME types if desired. This feature applies both to the Barracuda Web Security Gateway virus scanning feature as well as the subscription-based ATP scanning feature. When upgrading to version 11.0, selected MIME types will be migrated to corresponding file types. Similarly disabled MIME types will result in corresponding file types disabled after the upgrade.

Chromebook Support

- **Barracuda Chromebook Security Extension** - Barracuda Chromebook Security Extension is installed as a browser extension for Chromebooks to enforce web browsing policies you configure on the Barracuda Web Security Gateway. The extension supports SSL inspection on Chromebooks and filters all web traffic for authenticated Chromebook users. Browsing policies you configure on the Barracuda Web Security Gateway are applied by the extension to this web traffic. As of this early release, the Barracuda Chromebook Security Extension is available from the Google App Store at no cost and is configured in the Google Admin console. For more information, see How to Get and Configure the Barracuda Chromebook Security Extension.

Reporting

- **Barracuda Reporting Server integration** - The **Barracuda Reporting Server** is a hardware appliance that offers a faster, more accurate reporting option that can integrate with the Barracuda Web Security Gateway. This integration offloads reporting resources from the Barracuda Web Security Gateway, resulting in improved web filtering performance. The Barracuda Reporting Server can also provide an aggregate view of data for customers with multiple Barracuda Web Security Gateways. For more information, see Barracuda Reporting Server - Overview.

SNI Support

- Ability to detect SNI and to use that in the clientHello message sent to the server. This reduces disconnections from servers such as Amazon Web Services which require SNI to be able to serve the correct certificate. SNI detection prevents the need to contact the server to see its certificate. Clients whose browsers do not implement SNI are presented with a default certificate and hence are likely to receive certificate warnings.

SSL Inspection

- **SSL acceleration hardware** - New support for SSL hardware accelerator included in specific

appliance models. For more information about supported models, see SSL Accelerator Hardware.
- **Exempted Domains** - Optionally add any domains you want to *bypass* SSL Inspection. For example, if you have enabled any of the **Safe Search** categories in the **Safe Browsing** section of the **BLOCK/ACCEPT > Content Filter** page, you might want to exempt one or more domains. There is no limit to the number of domains that you can exempt from SSL Inspection, and there is no impact on system performance.

Remote Filtering

- **Client-side SSL inspection with the WSA for Mac** - The Barracuda Web Security Agent (WSA) for Mac can provide client-side SSL Inspection directly on the client computer, offloading resource-intensive processing from the Barracuda Web Security Gateway. This configuration is highly scalable in terms of number of users, consuming fewer resources on the Barracuda Web Security Gateway and improving system performance. For more information, see Client-side SSL inspection with the Barracuda WSA.
- **Authentication mechanism supporting multiple certificates for Barracuda Web Security Agent** - For web browsing scenarios where remote Mac users may connect to the Barracuda Web Security Gateway over possibly hostile networks, such as an unencrypted conference or other public WiFi. Create self-signed or upload trusted certificates on the ADVANCED > Remote Filtering page and configure the Barracuda WSA on each Mac with the certificate hash. This secure authentication mechanism enables the Barracuda WSA to verify the identity of the Barracuda Web Security Gateway and ensure that administrative traffic is encrypted and secure. Includes ability to store and manage multiple certificates on the Barracuda Web Security Gateway to provide for seamless transition from an expiring certificate to a new one. See Authentication with the Barracuda Web Security Gateway and the Barracuda WSA for details.

Miscellaneous

- **Syslog Support for W3C format** - Support for sending system logs to the external syslog server in W3C extended Log file format. Configure on the **ADVANCED > Syslog** page.
- The **Google Apps Regulations** section of the **BLOCK/ACCEPT > Configuration** page has been removed since YouTube For Schools was discontinued in July, 2016. The YouTube for Schools setting in the **BLOCK/ACCEPT > Content Filter** page has also been removed for the same reason. To restrict YouTube content, see How to Restrict YouTube Content On Your Network.
- **SMTP Authentication support** - If your SMTP server requires authentication, and you configure email notifications (alerts) on the **BASIC > Administration** page, you can enter the Username and Password required by your SMTP server.

Fixed in Version 11.0

Web Interface

- The configured external backup server shows as expected in the web interface. [BNYF-8188]
- The **BASIC > Dashboard** page renders properly when changing the Language drop-drown to Francais / French. [BNYF-8226]
- The Spyportal redirect message and suspicious keyword alert notification each show the correct System Name of **Barracuda Web Security Gateway** if the System Name default value on the **ADVANCED > Appearance** Page was never changed. [BNYF-8757]

Syslog

- Large syslog traffic/data from Access Point does not stall processing. [BNYF-10592]

Security

- High severity vulnerability: unauthenticated, denial of service (DoS) [BNSEC-296 / BNYF-8892]
- High severity vulnerability: persistent XSS, authenticated [BNSEC-261 / BNYF-6117]
- Medium severity vulnerability: information disclosure, insufficient authorization [BNSEC-4230 / BNYF-8596]
- Medium severity vulnerability: persistent XSS, authenticated [BNSEC-1738 / BNYF-7331]

Version 11.0.0.027

On the **BASIC > Dashboard** page, the title of the **Total Threats / Viruses** graph does not appear as *lid_39437.* [BNYF-13390]

Version 11.0.0.026

- Possible high system load that was related to automated daily refresh of the **BASIC > Dashboard** statistic reports is no longer an issue. [BNYF-13102]
- Chrome browser version 58 does not support matching the Common Name in certificates. Certificates that rely on this deprecated behavior will now be rejected with: ERR_CERT_COMMON_NAME_INVALID. [BNYF-13168]
- Reporting/Log storage in the Performance Statistics table on the **BASIC > Dashboard** page shows correct number of blocks due to ATP. [BNYF-13297]
- Fixed an issue in which, when SSL inspection is enabled on the latest hardware revision of the Barracuda Web Security Gateway, the SSL hardware driver caused the system to fail after extended usage. [BNYF-13253]
- The **ADVANCED > Remote Filtering** page does not give a *Temporarily Unavailable 500* error. [BNYF-12825]
- Suspicious Keywords reports do not show "no data available" if no email address is configured

for **Sensitive Keywords Alert Email Address**. [BNYF-12762]
- For the Barracuda Web Security Agent, the Source IP Address and Username in the Web Log page display correctly when accessing HTTPS sites in non-PLO mode. [BNYF-11937]
- CA bundle update. [BNYF-11091]
- The **Match Any** search term exception works as expected. [BNYF-12759]
- Advanced Threat Protection (ATP) continues functioning as expected when idle for more than 24 hours. [BNYF-12896]
- The cache manager is accessible to LAN hosts. [BNYF-13016]
- New proxy version disables the ACL related to **X-forwarded For** by default. [BNYF-12979]

Version 11.0.0.019

- On the Barracuda Web Security Gateway 1010/11, after firmware update to 11.0, Barracuda Web Security Gateway always responds to ping and passes traffic if Hard Bypass is enabled. [BNYF-12616]
- When secure block page is enabled, policy look-up for the Barracuda WSA in PLO mode works as expected. [BNYF-12630]
- On the **BASIC > ATP Log** page, the **Scan Completed** column displays the correct timestamp for *Error* Status log entries. [BNYF-12640]

Version 11.0.0.016

- When SSL Inspection is enabled, domains contained in *.google.com.hk are now included in alternative names for google.com, avoiding errors when browsing. [BNYF-12002]
- Host verification from an inline client succeeds when the port is included with the domain in the verification command. [BNYF-12343]
- Resolved ICAP protocol errors caused by lack of enough ICAP servers.[BNYF-12409]
- Client IP addresses added in the **Proxy Authentication Exemptions** section of the **ADVANCED > Proxy** page are exempt as expected for basic authentication. [BNYF-12103]
- When one Barracuda Web Security Gateway is configured to act as a reporting server for another Barracuda Web Security Gateway, the reporting server now shows logged events for browsing spyware sites, just as the other system does. [BNYF-12441]

Version 11.0.0.014

- Kerberos authentication works as expected after upgrading to 11.0.0.014 and higher. [BNYF-12203]
- On the **BASIC > Dashboard** page, the **Total Threats / Viruses** feature of the page does not cause a high system load when there is a high amount of data. [BNYF-12232]
- Added the following CAs to the ca-bundle.trust.crt file: [BNYF-12242]

    - GeoTrust DV SSL CA - G3
    - COMODO RSA Organization Validation Secure Server CA
- Configuration changes on the **ADVANCED > Remote Filtering** page do not result in an unrelated warning message. [BNYF-12085]
- On the **BASIC > Reports** page of the Barracuda Web Security Gateway 310(appliance and Vx) and 410Vx, the list of reports show as expected in the Productivity and Administrative sections. [BNYF-12234]
- Suspicious keyword alerts are sent as expected when there is more than one email address configured in the **Sensitive Keywords Alert Email Address** field. [BNYF-12188]
- Suspicious keyword alert emails display content properly when SSL Inspection is enabled. [BNYF-12142]
- ATP reports in PDF format display values properly in the **Status** column. [BNYF-12253]
- The Trusted Authentication feature on the **USERS/GROUPS > Configuration** page works as expected with version 11.0.0.014. [BNYF-12255]
- Updated per Yahoo Certifcate updates, preventing domain mismatch. [BNYF-12270]
- Reports generated for NTLM Groups do not return "No Data Available" error. [BNYF-12078]
- On the **Secure Administration** page, if the user is uploading a certificate and bundles that have a validation year after 2038, the cert will appear as not trusted because the chain is expired. [BNYF-12303]
- Added definition of **Clear** button on **BASIC > Dashboard** page. [BNYF-8464]
- Added that Advanced Threat Protection (ATP) only applies to certain models. [BNYF-12180]

Version 11.0.0.010

- After upgrading to version 11.0.0.009, if Kerberos authentication is configured, user can browse without receiving cache errors or pop-ups. [BNYF-12203]
- The graph on the **BASIC > Dashboard** showing the total number of viruses detected by the ATP service and the Barracuda Web Security Gateway virus scanner in the past 30 days displays accurate data. [BNYF-12206]
- After upgrading to version 11.0.0.009, the LDAP configuration continues to appear as expected in the web interface, with the LDAP options showing as available on the **BASIC > Reports** and in the **BLOCK/ACCEPT > Exceptions** pages. [BNYF-12191]
- When **Pass Client IP addresses through WAN port** is enabled, HTTPand HTTPS pages load as expected. [BNYF-12190]

Firmware Version 10.1

What's New in Version 10.1

Barracuda Chromebook Security Extension

- Barracuda Chromebook Security Extension is installed as a browser extension for Chromebooks to enforce web browsing policies you configure on the Barracuda Web Security Gateway. The extension supports SSL inspection on Chromebooks and filters all web traffic for authenticated Chromebook users. Browsing policies you configure on the Barracuda Web Security Gateway are applied by the extension to this web traffic. The Barracuda Chromebook Security Extension is available from the Google App Store at no cost and is configured in the Google Admin console. For details on how the extension works and configuration, see How to Get and Configure the Barracuda Chromebook Security Extension.

Fixed in Version 10.1

Reporting

- Categories and domain names appear in proper columns in associated reports. [BNYF-10702]

SSL Inspection

- For the Barracuda Web Security Gateway 410 with SSL Inspection enabled, Ultrasurf application blocking works as expected. [BNYF-8667]
- When SSL Inspection is enabled in **Transparent Mode** and IP-based URLs are blocked, HTTPS websites are accessible as expected. [BNYF-10494]

Authentication

- Usernames are logged correctly in the Web Log for associated web traffic. [BNYF-10807]
- When creating an exception, lookup on Groups where a group name contains an underscore (_) works as expected when NTLM authentication is configured. [BNYF-9750], [BNYF-8416]

Miscellaneous

- When a domain is unknown or part of a cached categorization entry in the Barracuda Web Security Gateway, the system will use the cached categorization results if the WCS response is lost or delayed. [BNYF-10793]
- When connected to the Barracuda Control Server (BCS), graphs for the Barracuda Web Security Gateway display properly on the **BASIC > Dashboard** page of BCS. [BNYF-11183]
- When the Barracuda Web Security Gateway is joined to the Barracuda Cloud Control (BCC), the Content Filter Lookup feature on the **BLOCK/ACCEPT > Content Filter** page works as expected. [BNYF-7374]
- The Time Zone for Moscow, Russia as configured on the **BASIC > Adminstration** page is accurate. [BNYF-9271]
- The help file for the **BLOCK/ACCEPT > Configuration** page has been updated to reflect that Captive Portal sessions automatically time out after 24 hours. [BNYF-10757]

Version 10.1.0.004

Barracuda Chromebook Security Extension

- Enhancement: Added the ability to associate Google domain users in the Barracuda Chromebook Security Extension with local LDAP Server/Active Directory. [BNYF-11561]
- Fix: The **Shared Secret** value configured for the extension is not exposed in the browser "View page source" window, nor can it be read from the command line. [BNYF-11180]
- Fix: During policy lookups, the Barracuda Chromebook Security Extension authenticates the user over a secure connection to the Barracuda Web Security Gateway. [BNYF-11326]

Miscellaneous

- Enhancement: When the **Reset** button is pressed on the Barracuda Web Security Gateway appliance, the unit reboots. The IP address cannot be changed by pressing the **Reset** button. [BNYF-10968]

Firmware Version 10.0

What's New in Version 10.0

Important Note: SSL Inspection is resource intensive, and enabling it will have an impact on system performance. The actual impact will depend on the amount of HTTPS traffic that your unit is handling. If your unit does not provide satisfactory performance after enabling SSL Inspection, contact your Barracuda sales representative to learn about hardware refresh options.

SSL Inspection

- The Barracuda Web Security Gateway 310 appliance (not Vx) now supports **SSL Inspection** with inline or forward proxy deployments for Safe Browsing. Configure on the **BLOCK/ACCEPT > Configuration** page.
- The Barracuda Web Security Gateway 410 appliance (not Vx) now supports **Transparent Mode** for SSL Inspection and the creation of self-signed certificates for SSL Inspection. If SSL Inspection is enabled on a Barracuda Web Security Gateway 410 before upgrading to version 10.0, then after upgrading, SSL Inspection will be enabled in **Transparent Mode**. Configure on the **ADVANCED > SSL Inspection** page. See Using SSL Inspection With the Barracuda Web Security Gateway for information about Transparent Mode.
- The 410 appliance (not Vx) also now supports capture and archiving of suspicious content or sensitive data patterns in chat, email, and other social media communications. Configure on the **BLOCK/ACCEPT > Web App Monitor** page.
- The Barracuda Web Security Gateway 810 now supports specifying particular domains and/or

categories with SSL Inspection. Configure on the **ADVANCED > SSL Inspection** page.

See How to Configure SSL Inspection Version 10 and Higher for a reference of SSL Inspection features by model.

User Interface

- The Barracuda Web Filter has been rebranded to the **Barracuda Web Security Gateway**.
- The **BASIC > Dashboard** page now shows **Recent Flagged Terms** instead of **Recent Search Queries** for the Barracuda Web Security Gateway 410. This reflects availability of the Web Application Monitoring feature on the 410 with this version.

Secure Administration

- Enhancement: Added the following certificates to SSL CA bundle -
  - GeoTrust Global CA. [BNYF-10803]
  - Thawte dv SSL CA - G2. [BNYF-10802]
  - DigiCert SHA2 High Assurance Server CA. [BNYF-10828]

Virtualization

- Enhancement: On the Barracuda Web Security Gateway Vx, if **Energize Updates** are disabled, expired, or terminated, all traffic is allowed regardless of policy settings. [BNYF-10322].

Fixed in Version 10.0

- NIC drivers are updated to avoid packet loss in certain models of the Barracuda Web Security Gateway. [BNYF-10426]
- Scheduling backups or performing a Test Configuration of an SMB server for reporting works as expected if the username specified does not have access to the default WORKGROUP. [BNYF-8855]
- For Barracuda Web Security Gateways connected to Barracuda Appliance Control (BAC): the Unit Health section of the **STATUS** page in BAC displays correct information about the unit when the CPU Temperature in the BWSG Performance Statistics section on the **BASIC > Dashboard** page shows 0.0 degrees Centigrade. [BNYF-9893]
- The **BASIC > Application Log** no longer shows the Destination IP in the Source IP column for certain applications. [BNYF-5333]

Version 10.0.0.020

- Application control is supported for the Barracuda Web Security Gateway 310 and higher.
- Barracuda no longer provides the Barracuda Malware Removal Tool for any model.
- Web Application Control (**BLOCK/ACCEPT > Web App Control**) is supported for the Barracuda Web Security Gateway 310 and higher.

Version 10.0.0.018

- If you enabled the Barracuda Chromebook Security Extension while running version 9.1 or earlier, and then upgrade to version 10.0, the configuration for the extension is present as expected. [BNYF-11933]
- When synchronizing configuration changes across a cluster, the Barracuda Web Security Gateway does not reboot or re-load an older configuration. [BNYF-11930]
- Proper handling of null "x-forwarded-for" header. [BNYF-11873]
- Policy requests now time out, if necessary, rather than waiting a long time. [BNYF-11870]
- Improved management of WCS lookups when there are timeouts, resulting in fewer "timeout" messages in the WCS log. [BNYF-11844]
- Updates to CFDEF (category definitions) are enabled as expected when the WCS service is enabled. [BNYF-11832]
- DNS name "=*.yimg.com" should be added under "subject alternative names" by the Barracuda Web Security Gateway to be able to fully load https://www.yahoo.com when SSL inspection is enabled. [BNYF-11759]
- The Power button works as expected on older Barracuda Web Security Gateway appliances when upgrading to version 10.0. [BNYF-11749]
- Barracuda WSA users no longer get a block page when SSL inspection mode is set to **Transparent** and web-based email is blocked for un-authenticated users, but allowed for authenticated users. [BNYF-11647]
- Peer Proxy works as expected for HTTPS sites. [BNYF-11587]
- The Barracuda Web Security Gateway ensures that Proxy and Web Application Monitoring services do not use the same port when SSL Inspection is enabled in Transparent mode, avoiding issues on some higher models. [BNYF-11576]
- CFDEF updates are downloaded regularly even when the WCS service is enabled on the Barracuda Web Security Gateway. [BNYF-11558]
- The "Configuration updated" message is only displayed in the web interface when a configuration change is made. [BNYF-10947]
- Policy Lookup Only (PLO) mode supports Google Consumer Apps. [BNYF-10314]

Version 10.0.0.016

- This version addresses an issue in manufacturing newer Barracuda Web Security Gateways with upgraded hardware.

Firmware Version 9.1

What's New in Version 9.1

- Ability to block Google consumer accounts while allowing Google hosted organizational accounts to be accessed for a specified list of Google applications. See G Suite Control Over HTTPS and Exception Policies for examples.
- Ability to categorize domains dynamically in real time.
- New option on **BASIC > Reports** page that allows hiding custom categories on reports.
- Barracuda Malware Removal Tool is no longer provided with the Barracuda Web Security Gateway version 9.1 and above.

Fixed in Version 9.1

- Enhancement: Back-end improvements to the Barracuda policy engine, especially related to application blocking. [BNYF-10148, BNYF-10151, BNYF-10166, BNYF-10294]
- Enhancement: The Barracuda Web Security Gateway now uses the Web Categorization Service by default unless previously disabled. [BNYF-10601]
- Enhancement: Content filtering performance. [BNYF-8228, BNYF-10294, BNYF-10274, BNYF-10175]
- Fix: Reporting issues related to data unavailability/inaccuracy. [BNYF-9248, BNYF-9448, BNYF-9705, BNYF-9842, BNYF-9984, BNYF-10132, BNYF-10210, BNYF-10246]
- Fix: When updating a Barracuda Web Security Gateway using Barracuda Cloud Control from version 9.0.0.003 to version 9.1.0.001, the Barracuda Web Security Gateway now remains connected to Barracuda Cloud Control. [BNYF-10663]
- Fix: On the **BASIC > Application Log** page, entries that erroneously displayed 'spysiteIN=br0' in the **Details** column now show correctly as 'Spyware Website'. [BNYF-10292]
- Fix: Reports with more than 10 records show all records in the table and a maximum of 10 records in the chart. [BNYF-9181]
- Fix: The *Weekly Performance Summary* report runs automatically as a Scheduled Report for version 9.1 and above. [BNYF-10521]
- Fix: Policy engine improvement during configuration reload. [BNYF-10645]
- Fix: The Barracuda Web Security Gateway communication with the WCS lookup is contiguous without interruption. [BNYF-10764]

Firmware Version 9.0

What's New in Version 9.0

- **New underlying application blocking engine**. Version 1.0.130 or above of the Application

Definition Updates is required (See the **ADVANCED > Energize Updates** page). Consequences are:
  - Improved performance of application blocking and strength of signature-based application detection, including service recognition, e.g. chat, video, voice and file-transfer.
  - More accurate identification of applications, with frequent updates.
  - Higher accuracy of real-time detection capabilities.
  - Blocking of over 200 additional protocols and applications.
  - Blocking of the following applications is no longer supported:
    - ASProxy
    - uTorrent
    - Twitterrific
    - Freegate
    - HotspotShield
    - IPShield
    - Icecast (in Communications group). However, the IceCast app in the Multimedia group can still be blocked.
  - The following apps will appear in the web interface with the associated name changes:
    - Real Time Streaming Protocol will now display as **RTSP**.
    - iChat AV, VoIP Stunt, and VoIP Buster will now display as **SIP**.
- **Authentication**
  - Added support for Aerohive Wireless Access Point (WAP) authentication integration. Configure on the **USERS/GROUPS > Configuration** page.
- **Energize Updates**
  - Added **Access Point Definition Updates**, released on a regular basis by Barracuda Central and for use with the Barracuda Web Security Gateway. Configure on the **ADVANCED > Energize Updates** page.

Fixed in Version 9.0

- Feature: The Barracuda Web Security Gateway can be configured to accept traffic on non-native tagged VLAN 1. See the **ADVANCED > Advanced Networking** page. [BNYF-6551]
- Fix: When the **Captive Portal** feature is enabled and an **Allow** exception is created for a set of users, those users now see the Captive Portal agreement page when visiting allowed sites. [BNYF-8662]
- Fix: A large scheduled report no longer fails to generate when you try to run the same report before the original report finishes. [BNYF-9688]
- Fix: If a group is added to an Active Directory OU, the Barracuda Web Security Gateway now detects updates to that group. [BNYF-9260]
- Fix: Scheduled Reports in HTML format to an SMB server (configured on the **ADVANCED > External Servers** page) now correctly organize sets of reports in a directory or folder as specified. [BNYF-9161]
- Fix: If custom categories are created and exceptions are created for those categories, and the Barracuda Web Security Gateway logs traffic for those categories, the captured Daily/Hourly statistics will continue to display on the **BASIC > Dashboard** page if those categories are then

deleted. [BNYF-9063]
- Fix: When accessing the Barracuda Web Security Gateway web interface from the BCS, clicking on the Release Notes link on the **BASIC > Dashboard** page displays the notes as expected, and does not give a *Temporarily Unavailable* page. [BNYF-9394]
- Fix: When using G Suite for Education with Chromebooks, it is necessary to NOT inspect specific Google subdomains in order to prevent certificate errors. These subdomains will not be ssl inspected in proxy mode if Chromebook Compatibility is enabled. [BNYF-8763]
- Fix: The YouTube For Schools feature now works when the **Streaming Media** category is set to **Monitor**. [BNYF-9090]
- Fix: Apple iOS7 users are now able to log in and proceed as **Guest** when the **Captive Portal** feature is enabled. [BNYF-8943]
- Fix: HTTPS redirection with WCCP deployments now works whether or not HTTPS Filtering is enabled. [BNYF-8902]
- Fix: Reports that contain spyware sites are no longer blocked by the Barracuda Spam Firewall because the reports no longer include actual URL links to the sites. [BNYF-4221]
- Fix: When the Clear Cache button is pressed in the Caching Options section of the **ADVANCED > Caching** page, the transaction is now logged in the **Audit Log**. [BNYF-3000]
- Fix: Active Directory Group lookup is successful when Kerberos is configured for Authentication. [BNYF-9378]
- Fix: If an OU name contains special characters, scheduled reports based on the OU execute successfully. [BNYF-9281]
- Fix: Policy Rule Checks now recognize upper case letters when testing entered URL or Domain against the domain black/whitelist on the **ADVANCED > Troubleshooting** page. [BNYF-9349]

Version 9.0.0.003

- Fix: Reverting to a factory firmware version on a Barracuda Web Security Gateway (Vx and appliance). [BNYF-8703]
- Fix: Accessing scholar.google.com with transparent SSL Inspection. [BNYF-10166]

Version 9.0.0.002

- Fix: Captive portal exclusion now works as expected for an IP subnet group when a user initiates a session by opening a phone application (before using the browser) that accesses a particular domain. [BNYF-9438]
- Fix: The Log In button on the Temporary Access portal page works as expected after a custom category that includes a comma (,) is created. [BNYF-9871]
- Fix: The user no longer encounters an error page when, after triggering a time-based quota exception, browses a Warn page. [BNYF-9880]
- Fix: Domains and subdomains added to Custom Categories are properly categorized. BNYF-9883]
- Fix: Resolved issue in which the user was unable to download a page in proxy mode if the DNS

response had CNAME instead of IP address. [BNYF-9885]
- Fix: When using Google Chrome browser, inline traffic to all Google sites, including YouTube, is blocked or allowed as expected per policy. [BNYF-9889]
- Fix: Manual Backup to Local Destination as configured on the **ADVANCED > Backups** page works as expected. [BNYF-9997]
- Fix: Updated Trusted CA bundle with additional certificates. [BNYF-10018]

Firmware Version 8.1.0, Platform 2 and Platform 3

What's New in Version 8.1.0

- **Enable Port Auth Exemption** - Allows exemption of traffic proxied to port 8080 from NTLM and Kerberos authentication. If you have a combination of a terminal server environment using either NTLM or Kerberos authentication and Windows desktop units using LDAP, for example, this feature enables a hybrid of authentication mechanisms. Windows desktop users can then authenticate via your LDAP server while terminal users can authenticate via NTLM or Kerberos in a forward proxy configuration. Make sure that LDAP and/or unauthenticated user traffic runs over port 8080.

Fixed in Version 8.1.0

- Data correctly displays in chronological order for the Web Requests Log report type in HTML, PDF, Text, or CSV formats. [BNYF-8973]
- Login override, which provides login fields in the Spyware block page for authenticated users or the Captive Portal page (when Captive Portal feature is enabled) now works as expected. [BNYF-8962]
- When clustering two or more Barracuda Web Security Gateway Vx virtual machines, making a change in the configuration of one now propagates correctly to the other. [BNYF-8895]
- When the timezone is set within 30 minutes of GMT, performance statistics and charts on the **BASIC > Status** page render correctly. [BNYF-8869]
- Creating exceptions based on Safe Search does not result in an error message. [BNYF-8831]
- Provisioning the Barracuda Safe Browser on a device with the Barracuda Web Security Gateway is successful when bookmarks configured on the **ADVANCED > Remote Filtering** page contain special characters. [BNYF-8834]
- Scheduled reports with a large time frame complete correctly. [BNYF-8777]
- Editing the **Custom Keyword Categories** on the **BLOCK/ACCEPT > Web App Monitor** page saves modifications as expected. [BNYF-8694]
- With the Captive Portal feature enabled, when an Allow exception is created for a set of users, those users now receive the Captive Portal agreement page as expected when they try to visit the allowed sites. [BNYF-8662]
- *Authenticated* policy rules are no longer applied to *Unauthenticated* Captive Portal users. [BNYF-8483]

- On the **ADVANCED > Backup** page, the **Cloud** option is available for Scheduled Backups. [BNYF-8591]
- When multiple Barracuda Web Security Gateways are connected to Barracuda Appliance Control, reports generated from the group node view include data from all connected Barracuda Web Security Gateways. [BNYF-8578]

Version 8.1.0.005

- Fix: Updated OpenSSL to address CVE-2015-0204 (commonly known as "FREAK"), CVE-2015-0286, CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-0209, and CVE-2015-0288.
- Fix: Added CA certificates for trust chain verification, additional checks with errors for self-signed certificates and expired certificates. [BNYF-7863]
- Fix: YouTube Safe Search: Safe Search can only be enforced when the user is browsing as "guest". This means that uploading and similar actions tied to a user account will not work with YouTube Safe Search enabled. [BNYF-9323]
- Fix: Active Directory Group Lookup now works as expected when using Kerberos authentication. [BNYF-9378]
- Fix: Self-signed certificates created on the Barracuda Web Security Gateway 410 for use with SSL Inspection are now correctly created with an expiration date 3 years from date of creation. Self-signed certificates for all other Barracuda Web Security Gateway models expire in 1 year from date of creation. [BNYF-9362]

Version 8.1.0.003

- Feature: Automatic scheduling of the Performance Summary report when you upgrade to version 8.1.0.003. A PDF version of the report will run weekly and be delivered by email to the address entered in the **System Alerts Email Address** field on the **BASIC > Administration** page. To remove the report from the schedule, go to the **BASIC > Reports** page and remove it from or disable it in the **Schedule Reports** table.
- Fix: Further mitigated risk of SSLv3 related POODLE vulnerability on the internal interface of the Barracuda Web Security Gateway. If you have a legacy browser or web client inside the organization that is being SSL inspected and supports only SSLv3 or below, you could possibly experience an outage. If that is the case, call Barracuda Technical Support to resolve this issue. Note that with this fix, the external interface of the Barracuda Web Security Gateway is not affected in any way. [BNYF-9355]
- Fix: SSLv3 is disabled when the Local Redirect IP address is configured to be the same as the System IP address. This is to mitigate CVE-2014-3566 (SSL POODLE). [BNYF-9333]
- Fix: Self-signed SSL certificates created on the **ADVANCED > SSL Inspection** page expire one year from date of creation, as expected. [BNYF-9362]

Version 8.1.0.002

- Enhancement: New Performance Summary report with graphs of throughput, system load, TCP connections and Active Users. This report is a tool for quickly assessing whether your Barracuda Web Security Gateway is performing at sustainable levels for your organization's current needs. Overall system performance is represented by a horizontal bar that indicates where your system is with respect to maximum thresholds. Recommended, average and peak values are provided. Use this report to help gauge whether your organization has outgrown your Barracuda Web Security Gateway and you should consider upgrading to another model.
- Fix: Port 3130 is reserved ONLY for HTTPS traffic through the Barracuda Web Security Gateway when the **SSL Inspection** feature is enabled. [BNYF-9082]
- Fix: When re-ordering policy exceptions on the **BLOCK/ACCEPT > Exception** page, exceptions with text patterns that include meta-characters now remain unaffected if they change order. [BNYF-9187]
- Fix: LDAP users are now able to log in using LDAP Proxy Authentication regardless of whether the Bind DN contains a backslash '\' . [BNYF-9165]
- Fix: SSLv3 has been disabled in the Web interface to mitigate CVE-2014-3566 (SSL POODLE). [BNYF-9226]
- Fix: When a user is removed from an LDAP group in AD, periodic automatic synchronization of group information with the Barracuda Web Security Gateway works as expected. [BNYF-8532]
- Fix: Exceptions for LDAP groups continue to be applied as expected after making changes to the exception when **Aggregate All Active Directory Domains** is also set to **Yes** on the **USERS/GROUPS > Authentication** page. [BNYF-9150]

Upgrading to Version 8.0

After upgrading to version 8.0, you'll notice that some Hourly/Daily reports on the **BASIC > Statu s** (dashboard) page will initially show **No Data Available** until the first web request is made after the upgrade. All of the data required to run reports still exists on the Barracuda Web Security Gateway and new data will begin to appear on the default dashboard as the Barracuda Web Security Gateway begins to process traffic after the upgrade.

Firmware Version 8.0

What's New in Version 8.0

Authentication

- **Proxy Authentication** - The Proxy Authentication feature has been expanded to allow selection of LDAP groups for proxy authentication. Previously, only local users were supported. In 8.0, Administrators can apply LDAP authentication to remote/mobile users who

are in the LDAP server, but are browsing outside of the network. This means that the Barracuda Web Security Gateway can be configured such that there are no unauthenticated users. See the **USERS/GROUPS > Configuration** page to configure.
- **Wireless Access Point (WAP) Support** - The WAP integration feature enables end users to surf as authenticated users via the Barracuda Web Security Gateway after authenticating against their WAP. This means that the user only needs to enter their credentials once as opposed to entering their credentials once for the WAP and then a second time to authenticate against the Barracuda Web Security Gateway. Each WAP can be configured to send its syslogs to the Barracuda Web Security Gateway on the network, which can then parse the logs for username and IP address of each authenticated user. This enables reporting on user browsing activity, bandwidth use, and more. See the **USERS/GROUPS > Configuration** page to configure.

User Interface

- **Data Pattern Categorization** - As data leaves the corporate network through a variety of web based applications, the network administrator can monitor data patterns for sensitive information to ensure compliance with corporate policies. This entails the monitoring and alerting of flagged specific data elements such as credit card numbers, social security numbers, privacy terms, and HIPAA compliance terms. See the **BLOCK/ACCEPT > Web App Monitor** page to configure.
- **Customizable Dashboards** - In addition to the wealth of information available on the default dashboard (**BASIC > Status** page), the administrator can now also create multiple dashboards with summaries of just the information about web traffic and user activity that is of top priority. Choose from various reports showing specific user browsing, bandwidth and malware statistics in drag and drop layouts.

Virtualization

- **Support for Microsoft Hyper-V** - See Hypervisor Compatibility and Deployment - VHD Package.

Fixed in Version 8.0

- YouTube Safety Search works to match Google's new implementation of enforced Safety Mode as of March 2014. [BNYF-8537]
- Log reports now show data in ascending order by date. [BNYF-8530]
- Limiting reports to **All Logged Users** no longer generates reports with **No Data Available** message. [BNYF-8458]
- Reports can now be generated that include users found in nested organizational units (OU's) in the Active Directory structure. [BNYF-8379]
- Application Exceptions can now be set for specific IP groups. For example, FTP traffic can now be blocked based on the IP group of a particular user or set of users. [BNYF-8519]

- Temporary Access administrators can now log in to bypass block pages using their LDAP credentials even if the LDAP group they belong to is named with upper case letters. Previously, LDAP group names had to be in lower case. [BNYF-8504]
- Port 22 is no longer open for SSH access on the Barracuda Web Security Gateway. [BNYF-8175]

Firmware Version 7.1.0

What's New in Version 7.1.0

SSL Inspection

- The Barracuda Web Security Gateway 610 and 810 now support inline **SSL Inspection**. In previous releases, SSL Inspection was supported only in forward proxy deployments. Moreover, applications selected on the **BLOCK/ACCEPT > Web App Control** and **Web App Monitor** pages are now subject to SSL Inspection when the feature is enabled. See How to Configure SSL Inspection Version 7.1 for details. See the **ADVANCED > SSL Inspection** page in the Barracuda Web Security Gateway web interface to configure.
- The Barracuda Web Security Gateway 910, 1010, and 1011 now SSL inspects applications selected on the **BLOCK/ACCEPT > Web App Control** and **BLOCK/ACCEPT > Web App Monitor** pages. Previously, only domains and categories (in forward proxy) specified on the **ADVANCED > SSL Inspection** page were subject to SSL Inspection.
- The Barracuda Web Security Gateway 410 now supports **SSL Inspection** with inline or forward proxy deployments for Safe Browsing and YouTube for Schools.
- The Barracuda Web Security Agent (WSA) supports **SSL Inspection** in non-Policy Lookup Only Mode, to inspect the traffic proxied by the agent. See Barracuda Web Security Agent - How it Works 7.1.

Fixed in Version 7.1.0

- RAID status tools provide correct and consistent RAID status on the **BASIC > Status** page. [BNYF-8186]
- When a delegated admin is limited to a group, and that admin runs a report, the filter for **Limit Access To** (defined on the **ADVANCED > Delegated Admin** page) is correctly applied. [BNYF-7335]
- The process of exporting to a CSV file from the **BASIC > Web Log** page does not time out if the export takes more than 5 minutes. [BNYF-8178]
- The **Manage** and **Monitor** roles as defined on the **ADVANCED > Delegated Admin** page can create scheduled reports. [BNYF-8288]
- Backups created on older firmware versions will not work on the 7.1.0 release. The retrieval and backup works as expected as long as the backup files have been created with 7.1.0 release. [BNYF-8127]

Version 7.1.0.003

- Synchronized help page in web interface for **ADVANCED > Temporary Access** page. [BNYF-8425]
- Logging into the web interface with admin credentials, or getting redirected to a block page in a maximized IE8 browser does not cause the browser to crash. [BNYF-7982]
- The Warn block page triggered by a MIME type includes a Proceed button as expected. [BNYF-8450]
- The Windows Safari browser gets filtered as expected by the Barracuda WSA with the default option 'Filter Specified Applications And Allow All Others' configured on the **ADVANCED > Remote Filtering** page. [BNYF-8221]
- When a website is blocked for the reason of spyware, all buttons and the option to run the Barracuda Malware Removal Tool are present. [BNYF-8361]

Firmware Version 7.0.1

What's New in Version 7.0.1

- **Captive Portal**
  See the **BLOCK/ACCEPT > Configuration** page for settings.
  - Option to apply **Captive Portal** to one or more IP Subnet/Groups (as defined on the **USERS/GROUPS > IP Subnets/Groups** page) as well as to unauthenticated users.
  - **Captive Portal** access to the network can allow users to browse:
    - Using their existing LDAP credentials to log in and be subject to Authenticated policies, OR
    - Only as a Guest, OR
    - Based on their choice, selecting either Guest or as Authenticated when presented with the Captive Portal splash/login page.
  - Option to present a **Logout** button for the user on a block page that displays when a policy prevents the user from accessing a requested website or application. This allows for changing users/logins.
  - Ability to exclude IP group(s) from Captive Portal.
- **Temporary Access for Teachers, Students**
  - Admin has option to allow teachers to bypass block pages with login credentials instead of, or in addition to, using tokens to provide student access to requested websites. Teacher still has option to hand out tokens to students.
  - Admin can designate entire LDAP groups as Temporary Access administrators. For example, the admin might create a group for the Science Dept. and assign all teachers in that group Temporary Access administrator rights.
- **SSL inspection**
  Configure on **ADVANCED > SSL Inspection** page.
  - Ability to limit SSL Inspection of web traffic to specific users/groups. This new option provides 2 benefits:
    - Enables the admin to better manage this resource-intensive feature.

- Prevents unauthenticated or guest users from getting certificate warnings when browsing over HTTPS because they do not have the root certificate installed in their browser.
    - Option to allow end users to download a root SSL certificate from their browsers. May also require authentication for certificate download. This option is useful if you choose to create a self-signed certificate on the Barracuda Web Security Gateway which needs to be pushed out to client browsers, instead of uploading a trusted certificate you buy from a certificate authority. Rather than pushing the self-signed certificate to browsers, you can enable users to download it.
- **Reporting** - Two new summary reports, aggregating existing reports for meaningful snapshots of network activity and Internet activity for the specified time frame.

Fixed in Version 7.0.1

- **Significant performance improvement in rendering reports and statistics**
    - Faster reporting interface
    - Faster rendering of statistics on the **BASIC > Status** page
    - Faster log in to the web interface
- **Status page**
    - Performance Statistics display and align properly. [BNYF-7742, BNYF-7750]
    - Delay in page loading at **Admin** login fixed. [BNYF-7994]
    - When **Daily** is selected in the **Hourly Web Security Gateway Statistics** section of the page, the list data is updated and displays the Top 10 records. [BNYF-7837, BNYF-7928]
- **Reporting**
    - **Network Activity Summary** adhoc report in PDF format loads and displays correctly. [BNYF-8004]
    - **Top Users by Requests to Spyware Sites** adhoc HTML report (Users by Spyware Requests report in version 6.0.1) shows accurate data when drilling down by **Hour** or **Domains** [BNYF-7771]
    - **Sessions by Users** report is present. [BNYF-7747]
- **Barracuda Cloud Control**
  When managing the Barracuda Web Security Gateway from Barracuda Appliance Control (BAC):
    - The **Web Application Control page** now displays blocked applications for both single and group view. [BNYF-7988]
    - The **BASIC > Status** page correctly displays statistics. [BNYF-6233, BNYF-7295, BNYF-7413, BNYF-7412, BNYF-7750, BNYF-7795, BNYF-7837, BNYF-7876, BNYF-7874]
    - The **BASIC > Reports** page aligns with the Barracuda Appliance Control display. [BNYF-7355, BNYF-7349, BNYF-7893]
    - Adhoc reports in HTML format display records correctly. [BNYF-7348]
    - The User/Group Lookup button works properly on the **BLOCK/ACCEPT > Exceptions** page. [BNYF-6974]
    - Policy remains as selected (either **Unauthenticated** or **Authenticated**) on **BLOCK/ACCEPT > Web App Control** page. [BNYF-7988]
- **Miscellaneous**

- Block page now renders with correct background color when user visits blocked websites. [BNYF-7993]
- Block page and log in process work properly with maximized window in the IE8 browser. [BNYF-7982]

Firmware Version 7.0

Upgrading to Version 6.x and 7.x

- After upgrading to version 6.0, reverting back to the previous firmware version or to the factory installed version is not possible.
- Note that the **BASIC > WebLog** and **BASIC > Application Log** pages get cleared on updating from 6.0.0 to 6.0.1, but the log data is still intact and will still appear in reports.
- **WARNING**: If you are currently using port 8080 as a proxy port for your client connections, note that this port is no longer available to use for proxy connections with version 7.0 and higher. Please alter the port to 3128 on your clients by modifying your GPO or PAC file.

What's New in Version 7.0

- **User Interface**
  - **New look and feel** - The new Barracuda Web Security Gateway web interface is cleaner with a new color scheme, but is functionally the same with no changes to navigation.
  - **Enhanced Dashboard** - View live feed of current TCP connections and graphs of blocked requests, user browse times and bandwidth usage for a quick picture of web traffic on your network.
  - **New controls** for viewing logs and switching graph content type on-screen.
  - **Recent Flagged Terms** - (Available on 610 and higher) This new section displays a list of the most used *suspicious keyword terms* in social media and search engine activities per settings on the **BLOCK/ACCEPT > Web Application Monitor** page. These terms are categorized in a suspicious keywords lexicon provided by Barracuda Networks and can be added to by creating a custom list on the **BLOCK/ACCEPT > Web Application Monitor** page.
  - **Improved reporting** presentation tools as described below.
  - **Limited support for Barracuda Appliance Control (BAC)**. The new web interface includes several key enhancements, especially around the dashboard (**BASIC > Status** page). Future versions of the Barracuda Web Security Gateway firmware will fully support the new web interface. You can still join your Barracuda Web Security Gateway running version 7.0 to Barracuda Appliance Control, with limited feature support.
- **Temporary Access for Teachers, Students** - This feature replaces the Temporary Whitelist role. For research projects and other classroom needs, the Temporary Access Portal enables teachers to obtain student access, for a specified time period, to websites that are typically regulated by administrators. Administrators either create credentials for teachers, or teachers simply log into the portal via LDAP. From the portal teachers can request domains and/or categories of domains for temporary student access. The Temporary Access Portal issues a

token for each request that the teacher can then give to students for bypassing block pages. To configure, see **ADVANCED > Temporary Access**. The **BASIC > Temporary Access Requests** log tracks activity by teachers who have been given credentials to request temporary access for their students. The log displays the status of tokens teachers create by username and date, including expiration date and time of tokens.

- **Web Application Monitoring (Available on 610 and higher)**
  - **Suspicious Keyword Alerts** - Applies to terms categorized as related to cyberbullying, profanity, adult or terrorism in social media interactions. Barracuda Networks provides a lexicon of keywords you want the Barracuda Web Security Gateway to flag for generating email alerts when they appear in user social media interactions or search engine activities. You can add your own categories and lists of keywords as well. See the **BLOCK/ACCEPT > Web App Monitor** page for details and to configure. The **BASIC > Status** page includes a listing of the Recent Flagged Terms (Suspicious Keywords) identified in filtered traffic.
  - **New Web App Monitor Log page** - This new page on the **BASIC** tab displays a log of all archived chat, email, user registrations and social media interaction traffic processed by the Barracuda Web Security Gateway. Configure which kinds of activities you want to capture on the **BLOCK/ACCEPT > Web App Monitor** page. Use the **BASIC > Web App Monitor Log** page to view these captured application interactions by date, source IP address, username and associated details.
- **Enhanced HTTPS Filtering**
  - **SSL Inspection** - In addition to Forward Proxy deployments with the Barracuda Web Security Gateway 610 or higher, now also available for inline deployments on certain models. See the **ADVANCED > SSL Inspection** page. Provides for granular control of web 2.0 applications over HTTPS as described above within Facebook, G Suite, YouTube and more.
  - **HTTPS Block Page** - A block page is presented when users attempt to visit a website over HTTPS that either poses a security risk, violates policy, or that falls under the *Warn* policy action. Using the HTTP block page template on the **BLOCK/ACCEPT > Block Messages** page, you can customize the text on the web page displayed by the Barracuda Web Security Gateway.
- **Reporting**
  - **New reporting engine** with enhanced performance for fast response times.
  - **Enhanced PDF and HTML presentation** with informative header, footer and easy-to-read layout.
  - **New report set**- Organized for Productivity, Safety & Liability, Web Activity, Infection Activity and Administrative (Temporary Access Requests), including:
    - Top Facebook Users by Browse Time
    - Top Users by Bandwidth on Streaming Media Sites
    - Top Gaming Domains by Requests
    - Top Users by Requests to Spyware Sites
    - Top Facebook Users by Browse Time
    - Top Social Networking Domains by Requests
    - Top Streaming Media Domains by Requests
    - Top Streaming Media Domains by Bandwidth
    - Top Users by Bandwidth on Gaming Sites

  - Top Users by Blocked Requests
  - Top Users by Browse Time on Gaming Sites
  - Top Users by Browse Time on Streaming Media Sites
  - Top Users by Browse Time on Social Networking Sites
  - Top Users by Requests to Adult/Pornography/Nudity Sites
  - Top Users by Requests to Anonymizer Sites
  - Top Users by Requests to File Sharing/P2P Sites
  - Top Users by Requests to Intolerance and Hate Sites
  - Top Users by Requests to Weapons/Violence and Terrorism Sites
  - Top Suspicious Keywords
  - Suspicious Keywords by Users
  - Top YouTube Users by Bandwidth
  - Top YouTube Users by Browse Time
  - Audit Log
  - Temporary Access Request Log
  - Categories By Temporary Access Requests
  - Domains By Temporary Access Requests
  - Users By Temporary Access Requests
- **New Audit Log** - The Barracuda Web Security Gateway maintains a log of events including logins/logouts and changes to configuration settings in conjunction with role-based administration. The new **BASIC > Audit Log** page lists these events including date, source IP address, username, role and associated details.
- **Policy Rule Checking** - From the **ADVANCED > Troubleshooting** page you can test policy rules applied to traffic on specified servers. You can verify access restrictions and exceptions that you define in the pages on the **BLOCK/ACCEPT** tab. The Policy Rule Check returns a list of all of the rules that would apply to traffic and actions (*Monitor*, *Warn*, or *Deny*) that would be taken based on the rule.
- **Support for External ICAP servers** - Ability to redirect traffic from the Barracuda Web Security Gateway to a 3rd party server. Select DLP, Antivirus, or other dedicated ICAP server on the **ADVANCED > External Servers** page. The Barracuda Web Security Gateway will first apply all configured policies to inbound or outbound traffic, and then forward the traffic to the specified ICAP server for DLP scanning, antivirus scanning or other processing.

Fixed in Version 7.0.0

Version 7.0.0.022

- Reordering of exceptions in the **List of Exceptions** table on the **BLOCK/ACCEPT > Exceptions** page works and displays properly. [BNYF-7940]

Version 7.0.0.021

- Improved performance by resolving issues with increased CPU usage. [BNYF-7678]
- Resolved issue with increased memory usage when running reports. [BNYF-7807]

https://confluence.campus.cuda-inc.com/techlib/display/BWFv60/Barracuda+Web+Security+Gateway+Web+Application+Definitions+Release+Notes