Release Notes Version 8.0

https://campus.barracuda.com/doc/45024803/

Please Read Before Updating

Before updating to a new firmware version, be sure to back up your configuration and read the release notes for each firmware version which you will apply.

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

Change in Behavior:

- Requests with content type as text/plain, are now not included in deep inspection to prevent false positives. [BNWF-19588]
- Requests with content type as “application/json”, are now validated against the JSON profile(s) associated with the service on the **WEBSITES > JSON Security** page.
- The “Max-Age” header can now have negative values. [BNWF-19097]
- The closing tag for the Barracuda Web Application Firewall inserted CSRF tokens, is now made compliant with HTML5 standard. [BNWF-18297]
- The OS Command Injection pattern group is now included in the security policy for owa, owa2010, owa2013, sharepoint and sharepoint2013. [BNWF-18681]
- If you have configured email address(es) in **System Contact Email Address** in the **BASIC > Administration > Email Notifications** section, then the system summary report is automatically scheduled to be delivered weekly to the specified email address(es).

Templates created in version 8.0 are not supported in version 7.9.x. [BNWF-20544]

Fixes and Enhancements in 8.0

Security

- Feature: Ability to enforce Brute force policy for failed login attempts. [BNWF-18785]
- Feature: The enhancement is done to the features where response contents are inspected, and create the request rewrite rule automatically on the WEBSITES > Website Translations page to remove the "Accept-Encoding" header from the request. [BNWF-17988]

- Enhancement: 'LDAP Injection', 'Python-PHP attacks', 'HTTP Specific Injection' and 'Apache Struts attacks' are extracted from "OS Command Injection" and displayed as separate blocked attack types. [BNWF-19023]
- Enhancement: Separate response pages have been introduced for AAA login pages. [BNWF-18761]
- Enhancement: When multiple IDPs are configured for SAML authentication service, the user is provided with IDP selection page while accessing the service. [BNWF-19215]
- Fix: Malformed XML request are blocked if the service is in "Active" mode, and Action Policy is configured to protect from such requests. [BNWF-14797]
- Fix: All encoded and non-encoded attack patterns are correctly blocked when Base64 decoding is turned ON. [BNWF-20239]
- Fix: Large sized base-64 encoded POST requests that matched certain action policy criteria were causing the data path to shutdown abruptly. This issue is resolved. [BNWF-20147]
- Fix: The "&" in the URL query is normalized to "&" before encrypting the URL when "URL Encryption" is enabled. [BNWF-20056]
- Fix: An SQL Injection attack vulnerability in the search option field has been fixed. [BNWF-20029]
- Fix: The max threshold for "Max Request Line Length" in **SECURITY POLICIES > Request Limits** is now limited to 64K. [BNWF-19228]
- Fix: The "Policy Fix" wizard now displays the correct parameter profile if the request has colon (:) in the parameter name. [BNWF-19103]
- Fix: "Session Timeout" is now added in **SECURITY POLICIES > Action Policy**. [BNWF-19060] [BNWF-19095]
- Fix: The square bracket ([ ]) character is now treated as sensitive parameter, and is masked in Web Firewall Logs when configured on the **WEBSITES > Advanced Security > Mask Sensitive Data in Logs** section. [BNWF-18803]
- Fix: The "Policy Fix" and "Exception Profiling Fix" now provides correct fix for "Maximum Instance of Parameter Exceeded" attacks. [BNWF-17825]
- Fix: A URL encryption issue is fixed to encode the URLs properly to handle spaces in between the URL path. [BNWF-17222]
- Fix: The NCSSOTARGET parameter is not added to the query parameter when SSO is not enabled on the **ACCESS CONTROL > Authentication Policies** page. [BNWF-15484]
- Fix: The threshold for "Max Parameter Value Length" is same in **Security Policies > Parameter Protection** and **WEBSITES > Website Profiles > Parameter Profile**. [BNWF-18862]
- Fix: OpenSSL has been upgraded to 1.0.1m.

Access Control

- Feature: The Access Control policy capabilities have been enhanced to customize and configure the login pages. [BNWF-14933]
- Fix: An issue where extra lines were getting added when the AAA session cookie was updated after the "Cookie Refresh Interval" for POST requests, has been fixed now. [BNWF-18576]
- Fix: "Login Processor Path" on the **ACCESS CONTROL > Authentication Policies** page can

now include absolute URL. [BNWF-18326]

System

- Feature: A new option “Use Last IP Address From Header for Client IP Address” has been introduced on the **ADVANCED > System Configuration** page. When set to “Yes”, the Barracuda Web Application Firewall uses the last IP address in the "X-Forwarded-For" request header as the client IP address, and displays it in the Client IP field in the logs. [BNWF-17368]
- Enhancement: The "Status" page is now renamed as "Dashboard". [BNWF-18504]
- Enhancement: 32 bit legacy WAF machines now are built with latest version 1.0.1m of OpenSSL. [BNWF-18987]
- Enhancement: Live graphs are added on the **BASIC > Dashboard** page to monitor attacks on services. [BNWF-18612]
- Fix: A memory leak issue in handling continuous file uploads as multipart/form-data, has been fixed. [BNWF-20415]
- Fix: Older units (2009 or earlier) had firmware upgrade issues due to a small firmware partition. This has been resolved. [BNWF-19986]
- Fix: User passwords now support all special characters. Some characters like "&" did not work earlier. [BNWF-19948]
- Fix: A "Trusted CA" certificate is not allowed to be uploaded in the “Upload Certificate” section on the **BASIC > Certificates** page. [BNWF-19544]
- Fix: "CUSTOM" services are not available for selection under "Graphs: Service Statistics" on **BASIC > Dashboard > Preferences**. [BNWF-18911]
- Fix: The value for "Max Header Value Length" can now be set to blank on the **WEBSITES > Allow/Deny > Header: Allow/Deny Rules** section. [BNWF-18805]
- Fix: After Firmware Upgrade, GeoIP Definition Updates retains the currently installed version if the latest version is lesser than the installed version. [BNWF-18706]
- Fix: When HTTPS port is selected as the only way to use the Barracuda Web Application Firewall web interface, the online help's search indexing was not getting updated correctly. This issue has been fixed. [BNWF-18575]
- Fix: While creating adaptive profile rules, it is possible to keep the "Trusted Hosts" field empty. [BNWF-18505]
- Fix: Critical process of the unit were failing due to certificates with duplicate serial numbers. This issue has been fixed. [BNWF-16627]
- Fix: Issue with bypass in newer machines manufactured recently, is addressed. [BNWF-20033]
- Fix: Time zone issue for Asia/Jordan-Amman region is fixed. [BNWF-18739]
- Fix: Time for Moscow Time zone is now adjusted. [BNWF-18541]
- Fix: Addition of the same cookie name with two different cases, is now permitted and does not cause a rollback. [BNWF-16856]
- Fix: Configuration rollback issue in the server hostname feature, has been fixed. [BNWF-17600]
- Fix: Rollback caused due to missing URL parameters in a URL profile, has been fixed. [BNWF-18941]
- Fix: A configuration snapshot is taken on every configuration change made on the Barracuda Web Application Firewall, and in case of rollback, the last successful working configuration

snapshot is used to restore the database. [BNWF-18578]
- Fix: When "Enable Strict SNI Check" is set to "No" for a service, then SSL handshake for requests matching the configured domain under SNI happens using the certificate associated with the service. [BNWF-19685]
- Fix: An issue wherein manual changes to the URL path of a website profile, created through the "Policy Wizard", affected further policy fixes in the same URL space. This issue has been addressed. [BNWF-18065]

Logging and Reporting

- Feature: Ability to log Client IP address and port for HTTPSVC module on the **ADVANCED > System Logs** page. [BNWF-18542]
- Feature: "Service Name" column has been added in Web Firewall Logs, Access Logs and Network Logs. [BNWF-16001]
- Feature: Logs can now be filtered based on attack category on the **BASIC > Web Firewall Logs** page. [BNWF-16890]
- Feature: Added 'Server Summary' report under 'Config Summary' on the **BASIC > Reports** page to show server configuration details like 'OOB Health Checks', 'Connection Pooling ' and 'Client Impersonation'. [BNWF-3934]
- Feature: Each log is associated with a unique ID on **BASIC > Web Firewall Logs** and **Access Logs**. Using the unique ID you can now filter the logs easily. [BNWF-4847]
- Enhancement: Log ID for each log is added while exporting the logs in CSV format. [BNWF-19272]
- Enhancement: The "Log Details" are categorized into various sections on the **BASIC > Web Firewall Logs** and **Access Logs** pages. [BNWF-19687]
- Enhancement: Ability to set the time (in military format), day/date and schedule the report. [BNWF-9164]
- Enhancement: Ability to navigate to any page in Web Firewall Logs and Access Logs by entering the page number. [BNWF-19005]
- Enhancement: Reports can now be scheduled in PDF format. [BNWF-18692]
- Enhancement: It is now possible to include/exclude timestamp and hostname in the logs that are exported to the configured syslog server. [BNWF-18741]
- Enhancement: The "Query String" column is added in the **BASIC > Web Firewall Logs** page. [BNWF-19086] [BNWF-19923]
- Enhancement: "Client Traffic Reports" on the **BASIC > Reports** page includes "Requests By Device Type" to show the most used device type(s) that accessed the services. [BNWF-18924]
- Enhancement: Notification is sent when the system encounters "Invalid International License" for Energize Updates. [BNWF-18413]
- Enhancement: Each log is now associated with a unique ID on the **BASIC > Web Firewall Logs** and **Access Logs** pages. The log ID gets exported in CSV files and syslog files with the format "%uid". [BNWF-18411]
- Enhancement: Web Firewall Logs and Access Logs can now be filtered using unique ID. [BNWF-18410]
- Fix: The URL's in reports now include domain name. [BNWF-19784]

- Fix: NTP time changes now updates the timestamp in "System Logs" on the Barracuda Web Application Firewall web interface. [BNWF-20364]
- Fix: An occasional issue that prevented downloading firewall logs has been fixed. [BNWF-20223]
- Fix: The logs on the **BASIC > Audit Logs** page now display the correct IP address under "Login IP" when reboot and shut down operations are performed. [BNWF-19736]
- Fix: The "Referer" field value with double quote is now exported properly in CSV file. [BNWF-19096]
- Fix: Exported CSV files now include "Country Code" of the user in "Web Firewall Logs", "Access Logs" and "Network Firewall Logs". [BNWF-18835]
- Fix: Added "Alert" notification if summarization mechanism fails for storing reporting data. [BNWF-18819]
- Fix: Suppressed unnecessary D-state logs that displayed in **ADVANCED > System Logs**. [BNWF-18789]
- Fix: Reports can now be filtered using a "Service" name. [BNWF-18733]
- Fix: The Network Firewall logs exported to CSV file/Syslog server now displays correct “Action” value for the configured ACL. [BNWF-18388]
- Fix: Various fields of Web Firewall Logs and Access Logs are normalized to handle malfunctioning of logs. [BNWF-18327]
- Fix: A log is generated in "System Logs" if the client certificate is not presented, and SSL handshake fails when "Client Authentication Enforced" is enabled. [BNWF-14829]
- Fix: Non-readable characters are now Hex Encoded in the logs that are exported to CSV file. [BNWF-18982]
- Fix: In a rare condition, during firmware upgrade, log database migration was creating a stray file that resulted in not showing log information in the **ADVANCED > System Logs** page, and latest information not being updated in the **BASIC > Access Logs/Web Firewall Logs** page. This issue has been fixed. [BNWF-20055]

User Interface

- Enhancement: Selecting a "Parameter Class/Custom Parameter Class" on **WEBSITES > Website Profiles > Parameter Profile** now displays details of the selected parameter class. [BNWF-16448]
- Fix: An issue that displayed junk characters in the “Extended Match” widget, has been fixed. [BNWF-19072]
- Fix: Extended Match widget now works properly in Japanese and other languages. [BNWF-18758]
- Fix: The Barracuda Web Application Firewall web interface has been enhanced to ensure HTML forms are saved without errors. [BNWF-18418]
- Fix: Internal ACL Rules were not getting created correctly when the web interface's default language and encoding was set to "Espanol". This issue has been fixed. [BNWF-17867]
- Fix: The element type "URI-path" is now available in the Extended Match widget. [BNWF-17106]

Management

- Feature: Multiple objects of similar type can now be edited using "Partial Templates" on the **ADVANCED > Templates** page. [BNWF-17643] [BNWF-19511]
- Feature: Ability to add/edit static routes through templates. [BNWF-15100]
- Feature: Ability to enforce client certificate authentication policies granularly on URL spaces. [BNWF-14927]
- Enhancement: It is now possible to avoid management port configuration of a backup while restoring the file into a new unit. This is provided using an option "Exclude Management Port Configuration". [BNWF-15223]
- Enhancement: Template UI behavior changed to have on-demand loading of 'param groups' instead of pre-loading all configuration. Greatly improves performance while creating a template (esp. Service or Security Policy). [BNWF-17451]
- Enhancement: Template dependencies are supported in 8.0, and the dependency objects can be configured while applying a template. [BNWF-18124]
- Enhancement: It is now possible to “Select All” or “Deselect All” while creating or editing a template configuration. [BNWF-19368]
- Enhancement: Configuration related enhancements have been made to ensure that the certificates are regenerated when PKI Certificates are either uploaded or deleted. This enhancement also covers user interface misbehavior problems seen in earlier firmware versions. [BNWF-19127] [BNWF-18997] [BNWF-18889]
- Fix: Editing and saving a URL/Parameter profile after applying a filter, or by selecting a profile in a sub-directory under "Directories" on the **WEBSITES > Website Profiles** page now redirects you to the same filtered page. [BNWF-19102]
- Fix: The “Organization Name” and “Organization Unit” name can now include apostrophe (') while creating a certificate on the **BASIC > Certificates** page. [BNWF-20170]
- Fix: LDAP user DN with special characters is honored on the **ADVANCED > Admin Access Control** page. [BNWF-18373]
- Fix: A memory leak issue in one of the configuration management process, which slowed down the system, has been fixed. [BNWF-20117]
- Fix: Log rotation for packet captures has been fixed. [BNWF-19932]
- Fix: The response is not chunked encoded, and the connection is not closed for HTTP/1.1 requests when the request does not match any of the configured response body rewrite rules. [BNWF-19602]
- Fix: The second page while traversing the adaptive profiles was occasionally displaying incorrect information. This issue has been fixed. [BNWF-19157]
- Fix: Duplicate configuration information was sometimes getting stored while creating a real server configuration. This issue has been fixed. [BNWF-18872]
- Fix: Requests with an authorization header are now redirected to the correct real server according to content rules. [BNWF-18134]
- Fix: Trusted hosts with overlapping subnets are now not allowed to be configured on the **WEBSITES > Trusted Hosts** page. [BNWF-15650]

High Availability

- Fix: In clustered units, Syslog traffic were incorrectly routed through MGMT interface with WAN IP even after having static route in place. This has been fixed. [BNWF-13600] [BNWF-19802]

Cloud Hosting

- Fix: Windows azure agent Version 2.0.8 is included in the Barracuda Web Application Firewall Version 8.0. [BNWF-19618]