

Release Notes Version 8.1

<https://campus.barracuda.com/doc/49054847/>

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.

- Uploaded file names are now validated for metacharacters, and if the file name contains metacharacters after the first dot, the request will be blocked. [BNWF-14832]
- Requests with Content-Type as "text/plain", are now not included in deep inspection to prevent false positives. [BNWF-19588]
- The POST body, in passive mode, is now inspected only till a predefined and hardcoded length of 8K. [BNWF-21937]
- Attempt to append extra characters than what is permissible for CAPTCHA answer, is now blocked and the client is treated as a bot. [BNWF-21353]
- GET requests with content-length headers are now allowed. [BNWF-20098]

XML RPC has been deprecated since *Version 8.0.1*. Use [REST API](#) to make API calls.

Fixes and Enhancements in 8.1

Security

- Feature: A new Web Scraping feature provides advanced protection against web scraping or harvesting threats. [BNWF-2938]
- Feature: Security policy can now be associated with the rule group of a service. This makes it possible to associate security policies granularly at a URL level rather than a service level only. [BNWF-2786]
- Feature: Ability to create Certificate Signing Request (CSR)/self-signed SAN certificate on the Barracuda Web Application Firewall. [BNWF-14144]
- Feature: HTTP Strict Transport Security (HSTS) support is added for the HTTPS services. [BNWF-20512]

- Feature: JSON key profile support is added. Specific rules and security measures can be configured for the keys in JSON requests using the JSON key profile. [BNWF-20666]
- Enhancement: It is now possible to enable “SSL Compatibility Mode” for a server, and restrict the list of ciphers to be used to connect with legacy servers. [BNWF-19436]
- Enhancement: Parameter names in the URL are now validated for metacharacters when “Validate Parameter Name” is set to “Yes”. [BNWF-19329]
- Enhancement: New identity theft patterns (microsoft-errors, oracle-errors, php-errors, postgres-errors and mysql-errors) are now available in the SECURITY POLICIES > Data Theft Protection page. [BNWF-22323]
- Security Fix: SSH protocol version 1 (v1) is completely disabled. [BNWF-21609]
- Fix: After upgrading to version 8.1, the “Default Mode For Updated Patterns” will be changed to “Active”. Therefore, all patterns that gets updated as part of the latest version of attack definition will set the “Operating Mode” to “Active” under “Attack Types” on the ADVANCED > View Internal Patterns page. [BNWF-22171]
- Fix: The “Policy Fix” for Metacharacter in parameter now removes the metacharacter found in the request from the “Denied Metacharacters” list in “Parameter Protection”. [BNWF-21926]
- Fix: The “PROT” command is now forwarded to the FTP server when SSL is enabled for the service. [BNWF-21700]
- Fix: After upgrading to 8.1 version, all JSON profiles will be configured with “application/json” as default MIME type, therefore, by default requests with Content-Type as “application/json” will be validated against JSON profiles. [BNWF-21446]
- Fix: The data path crash issue with the JSON requests having keys/values more than 256KB characters, has been addressed. [BNWF-21151]
- Fix: A rare issue that blocked the exempted client IP address/addresses configured in “Exception Clients” on the WEBSITES > Advanced Security page, has been fixed now. [BNWF-20591]
- Fix: Exception profiling fixes for the logs that have been already purged from the database, are now handled gracefully. [BNWF-20105]
- Fix: Policy fix can now handle case sensitive parameters gracefully. In other words, if the Barracuda Web Application Firewall encounters a parameter name in two different cases (uppercase and lowercase), two parameter profiles will be created for the parameter when policy fix is applied. [BNWF-13798]
- Fix: Private key will not be exported in the backup when the certificate is uploaded with “Allow Private Key Export” set to “No”.
- Fix: If “Allow Private Key Export” is set to “No” for an uploaded certificate, the private key will not be included in the certificate when the certificate is downloaded. [BNWF-20474]
- Fix: Data theft protection is now applied to responses with application/xml content. [BNWF-21001]
- Fix: A rare issue that resulted in service outage when bruteforce policy was applied, has been fixed. [BNWF-20945]

Access Control

- Enhancement: IDP entity ID is now automatically populated from the IDP metadata.

[BNWF-20776]

- Enhancement: An IDP selection response page is now automatically associated to the service that is enabled with SAML authentication service. [BNWF-19523]

System

- Feature: Ability to configure supported SSL protocols for the Barracuda Web Application Firewall web interface. (SSL protocols can be selected on the ADVANCED > Secure Administration page.) [BNWF-20528]
- Feature: Threshold for bandwidth, incoming requests/connections and live sessions for the system can now be configured in the BASIC > Dashboard page, Preferences window. If the system exceeds the configured threshold, an email notification is sent to the configured email address/addresses with the download link of the file in it. [BNWF-22387]
- Feature: Servers using hostname as the identifier can now be resolved to multiple IPs, and the system performs load balancing across these IP addresses This is especially important in IaaS environments.[BNWF-22367]
- Enhancement: SSLv3 is now disabled by default for new services. [BNWF-20774]
- Enhancement: Ability to copy an existing security policy and create a new security policy has been added. [BNWF-20350]
- Enhancement: CPU usage calculation in multi-core systems has been improved. [BNWF-15607]
- Enhancement: Square brackets are now supported in the exempted cookie list. [BNWF-21270]
- Enhancement: New servers added by name resolution will now have unique server names. [BNWF-22594]
- Enhancement: The backslash (0x5c) and SOH (%01) are now included in the default denied metacharacters list. [BNWF-21403]
- Enhancement: Re-provisioning capability has been added for Barracuda Web Application Firewall virtual machines. [BNWF-20970]
- Enhancement: The default value of "Profile Update Interval" is now set to 300 seconds to reduce the configuration update interval. [BNWF-22619]
- Fix: Memory leak issue that was observed when uploading files as multipart/form-data, has been fixed. [BNWF-22360]
- Fix: Organization Name can include ampersand (&) character when creating a certificate. [BNWF-22328]
- Fix: A race condition issue in the monitoring process that caused service outage, has been fixed. [BNWF-22251]
- Fix: Alert notification for memory usage is sent only when total memory (RAM + SWAP) exceeds 85%. [BNWF-22237]
- Fix: A trusted host group can now be deleted if it is not associated with any service. [BNWF-21970]
- Fix: Login issue that occurred when restoring the backup, has been fixed. [BNWF-21681]
- Fix: An issue that marked the service down when client impersonation was enabled, has been fixed. [BNWF-21320]
- Fix: The "URL" field in the URL profile can now be configured with the ampersand (&) character in it. [BNWF-19844]

- Fix: If the primary DNS server is not reachable, or unable to resolve the hostname, the Barracuda Web Application Firewall uses secondary DNS server (if configured) to resolve the hostname. [BNWF-22145]
- Fix: A possible race condition while processing burst of requests, is now handled gracefully. [BNWF-21695]
- Fix: In case of connection failures during backend connectivity, the errors are logged less frequently to avoid voluminous logs in the system. [BNWF-21398]
- Fix: If "<" and ">" are present in the POST request, the Barracuda Web Application Firewall normalizes these characters before pattern matching. [BNWF-21240]
- Fix: An issue that put the system into maintenance mode, has been fixed. [BNWF-22005]
- Fix: When there is no rewrite being done on the response pages by any modules in the Barracuda Web Application Firewall, the response is not chunk encoded until and unless the server itself sends the chunk encoded response. [BNWF-21171]
- Fix: A possible memory leak in the path of persistence, has been fixed. [BNWF-17331]
- Fix: An issue with hostname resolution when TTL 0 was received, has been fixed. [BNWF-21077]
- Fix: An issue where an old snapshot was loaded when web interface operation failed, has been fixed. [BNWF-19373]
- Fix: Restarting the log module will no more cause service disruption. [BNWF-21066]
- Fix: Servers configured with server names under a content rule can now be edited. [BNWF-21125]
- Fix: Threshold value for CPU Temperature is updated according to the configured temperature scale in the **ADVANCED > Appearance** page, **Web Interface** section. [BNWF-17293]
- Fix: In rare circumstances, memory leak issue observed in the configuration database, has been fixed. [BNWF-22585]

Logging and Reporting

- Feature: AMQP (1.0 version) protocol support added to export logs to external aggregators that are compliant to AMQP message queuing, including Microsoft Azure's Event Hub. [BNWF-20551]
- Feature: Ability to set the frequency to export access logs to the FTP server. [BNWF-4285]
- Enhancement: Layer 7 health check failure errors now display Source IP/Port, Destination IP/Port when the log level is set to "Information". [BNWF-20135]
- Enhancement: Custom log format can be defined for "System Logs" and "Network Firewall Logs" on the ADVANCED > Export Logs page. [BNWF-20318] [BNWF-22013]
- Enhancement: The "Log level" for "Web Firewall Logs" export is set to "1-Alert" by default. [BNWF-24190]
- Fix: Memory leak issue that was observed when logging web firewall logs at a high rate, has been fixed. [BNWF-21846]
- Fix: "Mismatched IP Cookie Replay Attack" logs are not generated on the BASIC > Web Firewall Logs page when "Cookie Replay Protection Type" is set to "None". [BNWF-21678]
- Fix: Junk characters are now handled properly while generating a unique ID for a web firewall log, and traffic is processed without interruption. [BNWF-21218]
- Fix: Server Username in FTP Access Logs can now include <domain name>/<username>. [BNWF-21035]

- Fix: An issue with unreadable characters for "Invalid Method" in access logs when the URLs come in a non-ASCII charset, has been fixed. [BNWF-18982]
- Fix: The client IP/port and server IP/port are now logged in the system logs if client certificate is not presented during the SSL handshake. [BNWF-14829]
- Fix: All fields in Web Firewall Logs and Access Logs have been normalized to handle multi-byte charsets and escape sequence characters. [BNWF-19136]
- Fix: Logs exported to the CSV format now displays the text in English irrespective of the language setting in the browser. [BNWF-19633]
- Fix: High resource utilization by logging and reporting process, has been addressed. [BNWF-20658]

User Interface

- Feature: Ability to add custom MIME types for JSON profiles. [BNWF-20372]
- Enhancement: Infinite-scrolling is implemented on the BASIC > Services page to improve performance. [BNWF-20991]
- Enhancement: The "OR" conjunction has been removed from the logs page. The logs can now be filtered using the "In/Not In (comma-separated)" options. **Note:** Old filters created and saved using the "OR" option cannot be applied. [BNWF-19765]
- Enhancement: "Outbound Attacks" has been renamed to "Cloaked Responses" in the "Attacks" graph and statistics table on the BASIC > Dashboard page. [BNWF-18198]
- Fix: It is now possible to delete URL profiles and parameter profiles when the profiles are filtered based on the directories. [BNWF-22331]
- Fix: The "api.cgi" file is no longer exposed in the web interface. [BNWF-20961]
- Fix: Directory access on the Barracuda Web Application Firewall's management web interface now returns 404 instead of 403. [BNWF-20960]
- Fix: Web interface vulnerability for caching and content-type has been addressed. [BNWF-18372]
- Fix: An issue that did not allow intermediate certificates to be uploaded when the web interface language was set to "German", has been fixed now. [BNWF-19783]
- Fix: Delay in opening edit window for URL and parameter profiles, has been fixed. [BNWF-22394]

Management

- Feature: URL optimizers has been implemented to handle large number of URL profiles, where multiple URL profiles can be coalesced into one. [BNWF-20657]
- Feature: Parameter optimizers has been implemented to handle large number of parameter profiles, where multiple parameters profiles can be coalesced into one. [BNWF-21294]
- Fix: Hard disk cleanup has been improvised to handle space issues. [BNWF-22438]
- Fix: Compilation error seen with NNM's MIB compiler for SNMP has been fixed. [BNWF-21388]
- Fix: "Total Bandwidth" and "Services: Bandwidth" graphs on the BASIC > Dashboard page now

display correct data. [BNWF-21278]

High Availability

- Fix: Local host entries are now not synchronized in the cluster environment. [BNWF-21284]

Cloud Hosting

- Feature: Auto scaling and bootstrapping capability added for the Barracuda Web Application Firewall on AWS. [BNWF-20259]
- Fix: A rare issue where creating a security policy in an AWS instance, model BWFCAW001a resulted in generating improper values. This issue has been fixed. [BNWF-21103]
- Fix: Virus scan can now be enabled on the Barracuda Web Application Firewall A2 instances in Microsoft Azure and Amazon to check the presence of viruses in the files uploaded through multipart/form-data messages. [BNWF-18922]

REST API Enhancements and Fixes

- Enhancement: URL and parameter profiles for a service can now be added/updated/retrieved/deleted using REST API. [BNWF-20804]
- Enhancement: URL client authentication can now be configured using REST API. [BNWF-20627]
- Fix: Server Name Indication (SNI) for servers can now be enabled/disabled using REST API. [BNWF-22359]
- Fix: REST API now honors camel case in server name. [BNWF-21376]
- Fix: Local administrators created on the ADVANCED > Admin Access Control page can now update/modify vsites data using REST API. [BNWF-21102]
- Fix: Updating the server details using REST API does not insert junk values into the DB. [BNWF-20819]

© Barracuda Networks Inc., 2022 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.