Release Notes Version 10.0

https://campus.barracuda.com/doc/86541385/

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.

If a server is added with the hostname, the Barracuda Web Application Firewall will automatically create server entries for all IP addresses that resolves to the configured hostname. Deleting the first server that was added with the hostname, will now delete all the automatically created server entries. [BNWF-25536]

With the OpenSSL1.1.0, certificates signed with MD5 are no longer supported. Please replace such certificates with SHA1/SHA256 signed certificates before upgrading to 10.0.x. If an upgrade is done without replacing these certificates, services using them will go down and rollbacks will occur. [BNWF-31980]

Fixes and Enhancements in 10.0

High Availability

- Feature: Email notifications to alert when the peer in the cluster goes down has been added. [BNWF-23466]

Logging and Reporting

- Enhancement: Access logs will now display “Trusted” in the Web Firewall Matched field for requests originating from Trusted hosts. [BNWF-31031]
- Fix: An issue where multiple BATP Web Firewall logs were generated for a single file upload, has been fixed. [BNWF-31963]
- Fix: An issue where the data for a specific day was not consistent between weekly and monthly reports, has been fixed.[BNWF-31428]

- Fix: An issue with the CEF format for export logs, has been fixed. [BNWF-31388]
- Fix: An issue where the Client IP from HTTP headers was not logged when the value was in the IP:Port format, has been fixed.[BNWF-30305]
- Fix: An issue where the Total Bandwidth report showed the value to be 10x the correct value, has been fixed. [BNWF-29751]

Management

- Fix:The factory shipped template for Drupal has been upgraded to address CVE-2019-6340. [BNWF-31393]
- Fix: A “Duplicate Server IP:Port” error that occurred when editing a server under rule group, has been fixed. [BNWF-31071]
- Fix: An issue where creating a private certificate for the administrative UI failed, has been fixed. [BNWF-30547]
- Fix: Corrected the error message for failing cloud backups [BNWF-29155]
- Fix: An issue where ADP connections were blocked when the Allowed Admin IP Range is configured, has been fixed.[BNWF-31614]
- Fix: The default netmask "0.0.0.0" can now be configured for static and interface routes.[BNWF-30860]
- Fix: An issue where the default ICMPv6 ACLs could not be edited, has now been fixed. BNWF-30186]

REST APIv3

- Feature: Rate-limiting for WAF configuration APIs has been enabled. Currently a request-rate of 10 API requests/second is configured as the default.[BNWF-30088]

Role-Based Administration

- Enhancement: RBA permissions for editing sub-resources from the UI and API are now consistent. [BNWF-30369]
- Fix: An issue where users were able to edit sub-resources that were not part of RBA master list while having read-only permissions on the object, has been fixed.[BNWF-30499]

Security-Advanced Bot Protection

- Feature: A new Bot Mitigation tab has been added with Advanced Bot Protection capabilities. The UI has been re-organized to move the Advanced Security, Session Tracking, Web Scraping

and Application DDoS modules to this tab.[BNWF-30115]
- Feature: Credential Stuffing Detection has been added. This feature uses a cloud-based database and requires and additional subscription. [BNWF-30173]
- Feature: Google reCAPTCHA support at Service and Rule Group Levels have been added. [BNWF-30150] [BNWF-30737]
- Feature: Comment and Referrer Spam detection capabilities have now been added. [BNWF-30285] [BNWF-29917]
- Feature: Client Fingerprinting has now been added to uniquely identify the end-client. BNWF-30066, BNWF-30699]
- Enhancement: Bruteforce protection can now use Client Fingerprint in addition to the IP address as a detection source.[BNWF-30694]

Security

- Feature: Let's Encrypt integration with the ability to generate certificates and automatically renew them has been added. [BNWF-28078]
- Feature: Custom backlisted IPs uploaded to the IP Reputation blacklist will now be in synced with other peer systems in High Availability.[BNWF-30582]
- Enhancement: SQL command injection is now enriched with patterns to check for tautologies involved in ELT and CHR functions. [BNWF-31954]
- Enhancement: Support for inspecting application/hal+json content types has been added.[BNWF-31443]
- Enhancement: Support for the "REST" FTP has been added. [BNWF-30689]
- Enhancement: Regex for the India PAN has been added to the internal data theft patterns[BNWF-30610]
- Enhancement: Support ppt and pptx files in mime type for file upload extensions, has been added.[BNWF-29918]
- Enhancement: Support for inspecting content-type:application/json-patch+json, is now added.[BNWF-29777]
- Enhancement: Support for TLS v 1.3 has been added.[BNWF-30735]
- Fix: An issue where the headers with the certificate parameters were not getting inserted as configured, has been fixed.[BNWF-31681]
- Fix: An issue where the service was not accessible when Authentication is enabled for a service on the Chrome browser, has been fixed.[BNWF-31093]

3:45 PM

System

- Fix: A rare issue with flow control in data path that could cause an outage has been fixed. [BNWF-31873]
- Fix: An issue where data path outages occurred with BRBL IP lookups has been fixed.[BNWF-31764]

- Fix: An issue where backups from a Platform 2 WAF could not be restored on a Platform 5 WAF has been fixed. [BNWF-31500]
- Fix: An issue causing high CPU utilization due to parsing CSS files containing long quoted URL strings has been fixed. [BNWF-30902]
- Fix: The Memory leak which occurred when SNI domains were added/deleted has been addressed.[BNWF-30668]
- Fix: A memory leak that occurred when a large CRL file was updated, has been fixed. [BNWF-30658]
- Fix: A memory leak in the data path process when servers are continually added and deleted has been fixed.[BNWF-30575]
- Fix: An issue with the web scraping module that resulted in a data path crash when rDNS lookups timeout, has now been fixed.[BNWF-30287]
- Fix: STM crash that occurred when caching is enabled on HTTP2 service, has been fixed.[BNWF-29988]
- Fix: A memory leak that occurred in the data-path process due to enabling SNI in HTTPS services, has been fixed.[BNWF-29882]
- Fix: Cookies are now forwarded by WAF in the format generated by server. [BNWF-29317]
- Fix: A data path crash when mask of sensitive data was turned on and the “Param Length Exceeded” condition was hit, has been fixed. [BNWF-28272]
- Fix: A possible outage due to SSL Socket Corruption, has been fixed.[BNWF-23992]
- Fix: An issue where defunct/zombie syslog-ng processes caused the UI to throw up “Temporarily Unavailable” pages, has now been fixed. BNWF-30123]

User Interface

- Enhancement: Improved the performance of certificate when many certificates are loaded in case of HA.[BNWF-31505]
- Enhancement: The load time of the Services and “Services Edit” pages have been reduced in cases where a large number of certificates are present.[BNWF-31849, BNWF-31805]
- Fix: An issue where uploading an invalid file for the offline firmware upgrade resulted in a temporarily unavailable page is now fixed to show an appropriate message. [BNWF-31637]
- Fix: An issue where the Service and Server Actions showed 'Disable' instead of 'Enable' for many non-English languages has been fixed.[BNWF-30927]
- Fix: An issue where the Interface Statistics were not showing up on appliances using a specific device driver, has been fixed. [BNWF-31076]

WAF Control Center

- Fix: An issue with the service page rendering in WCC proxy view has been fixed.[BNWF-31744]