Release Notes Version 9.2

https://campus.barracuda.com/doc/77401879/

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]

Fixes and Enhancements in 9.2

Access Control

- Enhancement: Handling IdP initiated SAML Single Logout for multiple authorization policies is now supported. [BNWF-28287]
- Fix: [SAML] Access Denied page displayed when an internal session time out expired, has been fixed.[BNWF-28441]
- Fix: When external authentication was configured, and a user entry was edited, the password edit field would be displayed. This has now been removed. [BNWF-28010]
- Fix: An issue where SAML attributes were not forwarded to the back-end server due to a missing attribute file has now been fixed. [BNWF-27486]

High Availability

- Enhancement: When a bond is created using the WAN interface, cluster heartbeats can only be transmitted over the management interface. [BNWF-28956]
- Feature: The WAN interface can now be part of a bond while in proxy mode.[BNWF-27365]

Logging and Reporting

- Feature: Support for log export to the Barracuda Reporting Server, has been added. [BNWF-28727] [BNWF-27233]
- Enhancement: HA configuration sync logs are now captured in System Logs. [BNWF-26387]
- Feature: The query string is now exported in syslogs when the %q key name is selected [BNWF-28450]
- Feature: OMS Logs can now be exported to AzureGov endpoints.[BNWF-28371]
- The concurrent-connections threshold alert has been increased to 1.8 Million connections when there are only HTTP services on the box. [BNWF-24884]
- Logs generated by the JSON Security module now display the Rule Type as “JSON Profile” or “JSON Key Profile”. [BNWF-28657]
- Fix: Exporting syslogs with the custom key name associated with %sn identifier, has been fixed. [BNWF-28338]
- Fix: Added SSL error logs for scenarios when there is a cipher mismatch or when the client certificate is not provided during client authentication.[BNWF-27944]
- Fix: An issue where access and web firewall logs were not populating has been resolved. [BNWF-27198]
- Fix: "\" is allowed in the regular expression used for "Server Username" field in FTP export logs. [BNWF-21035]
- Fix: An issue where syslog over SSL/TLS was not working, has been fixed. [BNWF-18136]

Management

- Feature: Password history enforcement for local administrators has now been increased to 12 previously used passwords. [BNWF-24083]
- Feature: Two Factor Authentication for Administrative Access is now supported. [BNWF-26763]
- Enhancement: Joomla and Drupal factory-shipped templates have now been added. [BNWF-23958]
- Fix: In some cases, creating a new security policy based on an existing policy caused configuration corruption. This has been fixed. [BNWF-29094]
- Fix: An issue where a new line used in comment field caused configuration rollbacks, has been fixed.[BNWF-28664]
- Fix: An issue where accessing the WAF Proxy view from Barracuda Cloud Control throws a temporarily unavailable page, has been fixed. [BNWF-27838]
- Fix: Rescheduling the job to export FTP access logs in case of failure, is now possible. [BNWF-27787]
- Fix: A configuration rollback that occurred when a template with SNI configuration was used has now been fixed. [BNWF-27039]

REST APIv3

- Feature: Support for complete granular Role-Based access control for all API actions [BNWF-26397]
- Feature: It is now possible to grant object-level READ/WRITE permissions from the administrator-roles (v3) API. Using this will allocate the same permission to the corresponding screens on the UI. [BNWF-28580]
- Enhancement: JSON Security Policies can now be configured. [BNWF-29200]
- Enhancement: A GET call on the administrator-roles object now returns the user's own role information if the user does not have admin permissions.[BNWF-28936]
- Enhancement: Only the factory-shipped “admin” role is allowed access by default. Any custom roles that require API access need to explicitly enable the access using the UI or API using with the “admin” role. [BNWF-28546]
- Enhancement: The performance of GET requests have been improved. [BNWF-27791]
- Enhancement: Support for manual failover/failback actions. [BNWF-26862]
- Enhancement: Support for link bonding operations. [BNWF-26657]
- Enhancement: Support for retrieval of the current operational status for Services, Servers, Links and Cluster has been added. [BNWF-26023]
- Fix: Users who do not have the certificate-management operation permission can no longer be allowed to download Certificates [BNWF-29163]
- Fix: Typo in the “administrator-ip-range” operation name, has been fixed. [BNWF-29125]
- Fix: The GET method was not working for vsites. This has been fixed. [BNWF-29066]
- Fix: The API parameter 'enable-OOB-health-checks' is renamed to 'enable-oob-health-checks'. [BNWF-28949]
- Fix: The typo in the “administrator-roles” API name, has been fixed. [BNWF-28611]

Role-Based Administration

- Feature: All operations on the Web Interface now have READ/WRITE permission toggles. The default permissions for all screens is WRITE. For guest role, all screen permissions are set to "read". [BNWF-28882]
- Enhancement: When role-based access is turned on, API privileges are now tied to specific user roles. Access has to be explicitly turned on for specific roles to use the API. [BNWF-29093]
- Fix: SAML and RSA SecurID Authentication Services are now listed in the Add/Edit administrator Role screen. [BNWF-28544]
- Fix: Support for group filter for Admin Access Control has been added. [BNWF-11903] [BNWF-5174] [BNWF-4376]
- Fix: A bug where Services RBA check can be circumvented from the Web Firewall Logs page, has been addressed. [BNWF-4620]

Security

- Feature: CRL updates are now downloaded 5 times every 24 hours. [BNWF-27204]
- OpenSSL has been upgraded to version 1.0.2o to address multiple vulnerabilities. [BNWF-28911]
- Fix: The max allowed limit for HTTP response rewrite value has been increased from 512 to 1024 characters.[BNWF-28507]
- Fix: The Maximum Number value supported by JSON Firewall has been increased. [BNWF-27701]
- Fix: An issue where the server information is visible through the cookie to the end client, has been fixed. [BNWF-25095]
- Fix: OpenSSH has been upgraded. [BNWF-18487]
- Fix: Global CSRF settings are now inherited by newly created URL Profiles. [BNWF-8962]

System

- Feature: Support for Encryption of Logs and Problem Reports as part of GDPR Compliance has been added.[BNWF-28319]
- Feature: Meta character values configured on a parameter profile are honored and take precedence over custom parameter class settings. [BNWF-3628]
- Enhancement: HTTP Compression when content-type contains "+" works now.[BNWF-26258]
- Fix: An issue where the STM process crashed when HTTP/2 was enabled, has been fixed.[BNWF-29122]
- Fix: HTTP/2: When the server sent chunked data, response headers from the WAF did not contain end-of-stream-flags. This has been fixed. [BNWF-29105]
- Fix: The Login form sent by the WAF has a HTTP body that causes issues in some cases. This body is now removed. [BNWF-29099]
- Fix: An issue where there was a data-path crash while inspecting IP Reputation at the Application Layer is now fixed. [BNWF-29079]
- Fix: When a rule group with client authentication enabled was renamed, the setting was disabled automatically. This has been fixed now and the setting is honored even after renaming. [BNWF-29031]
- Fix: An issue where hostname resolution was causing high CPU and memory usage, has been fixed.[BNWF-29004]
- Fix: The “SNI” option has now been removed for FTPSSL service.[BNWF-28620]
- Fix: When ContentLength was 0 for a WebSocket response, the connection would be closed. This is now fixed. [BNWF-28246]
- Fix: Added log rotation for omsagent logs to avoid filling up disk space. [BNWF-27980]
- Process monitoring script has been updated to monitor and control the number of instances of a specific process running concurrently. [BNWF-27891]
- Fix: An issue where toggling the connection pooling configuration resulted in a data-path crash has now been addressed.[BNWF-26944]

- Fix: An issue where “validate server certificate” required toggling the server is now fixed. It works without requiring the toggle now. . [BNWF-25634]
- Fix: An issue where Profile Optimizers took a long time to save on clustered devices is now fixed. [BNWF-25116]
- Fix: A memory leak in the consconf module, has now been fixed [BNWF-24310]
- Fix: An issue of high memory usage during CRL download, has been fixed. [BNWF-22588]
- WAF will now trigger auto repair/recovery of the configuration database if it is corrupt, reducing possibility of loss of logs in such cases. [BNWF-20087]
- Fix: An issue where WAF did not honor rule group and sent requests to the wrong server resulting in 404, has been fixed. [BNWF-10181]

User Interface

- Fix: When editing vsite data, the “loading…” spinner would not go away after the operation is completed. This is now fixed. [BNWF-28912].
- Fix: An issue with bulk edit operation of Action Policies that has colon ":" character in the action policy name, has been fixed. [BNWF-28291] [BNWF-28318]
- Fix: The "Barracuda AppSec Control Center" is now renamed as "Barracuda WAF Control Center". [BNWF-27751]
- Fix: The WAN interface can be chosen by default for the Total Bandwidth graph on the Basic > Dashboard page. [BNWF-27070]

Virtual Appliance

- Feature: Virtual instances now support 10 Gig bit Ethernet Interfaces. [BNWF-27243]
- Multi-port support is now available on Virtual Instances (other than WAN, LAN and MGMT) [BNWF-27224]

When the newer Vx instances supports multi-port, the older instances should be recreated to get the capabilities.

© 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.