Release Notes Version 9.0

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.

- In multiport HA, servers reachable via LAN1/LAN2/LAN3/LAN4 will always remain down on the secondary/backup unit. This is because, the custom virtual interface IP addresses are not configured on the secondary unit. Hence, the backend servers are not reachable from the secondary unit. [BNWF-24346]
- Vulnerability Fix: Various fixes done to ensure the reverse engineering and penetration of the Barracuda Web Application Firewall UI, is thwarted. [BNWF-24212]

Fixes and Enhancements in 9.0

Security

- Feature: The Barracuda Web Application Firewall can now send blocked client IP information to a connected Barracuda NG Firewall. This allows the Barracuda NG Firewall to block such clients at the perimeter and not allow them into the network. [BNWF-24667]
- Feature: Vulnerability Remediation Service, a free cloud service is now available on the ADVANCED > Vulnerability Reports page to scan vulnerabilities and apply patches to your web application. [BNWF-24597]
- Feature: The Barracuda Web Application Firewall now directly integrates with the ImmuniWeb and Rapid 7 vulnerability scanners. Reports from these scanners can directly be imported into the Barracuda Web Application Firewall for automatic virtual patching. [BNWF-24271], [BNWF-23353]
- Feature: The extended match capability is enhanced to support “Country Code” element type to allow the rules to be created based on Geo IP region. [BNWF-24125]
- Feature: The Barracuda Web Application Firewall is integrated with the Barracuda Advanced Threat Protection (BATP) to scan all files uploaded through multipart/form-data messages with multiple malware scanners that utilize different types of detection techniques to check for anomalies in the uploaded files, and to provide defense against zero day attacks. [BNWF-21239]
- Enhancement: PCI Compliance reports now supports PCI DSS version 3.1. [BNWF-21316]
- Enhancement: JSON requests will be parsed and analyzed as per RFC-7159. [BNWF-23621]
- Enhancement: A separate password can now be added for "Encryption" for SNMP v3. [BNWF-24852]
- Enhancement: A new configuration option "JavaScript Failure Threshold" is provided under “Advanced System Configuration” to configure the threshold to evaluate the suspicious clients. [BNWF-24383]
- Fix: Mask sensitive parameters now accepts “space” and “%20”. [BNWF-24703]
- Fix: A potential crash in a scenario involving HTTP2 and SSL, is addressed. [BNWF-24486]
- Fix: An issue that resulted in potential outage in SAML Logout when the query string size was more than 1024 bytes, has been fixed. [BNWF-25042]
- Fix: A potential crash with the Barracuda Web Application Firewall 963 FIPS model, when SSL is enabled on a service, has been addressed by disabling SNI, HTTP2 and Web Socket capability in this specific model (963). [BNWF-24351]
- Fix: CVE-2016-6304 has been addressed. [BNWF-24357]
- Fix: "Allowed Users" is now available under “Kerberos” authentication. [BNWF-24323]
- Fix: An issue in translating CSS responses with directory traversal URL tags, has been addressed.

[BNWF-24093]

- Fix: An issue that resulted in data path crash due to high traffic and enabling DDoS, has been fixed. [BNWF-24338]
- Fix: OpenSSL has been upgraded to 1.0.2k

Access Control

- Fix: Character limit for "Allowed Groups" in the ACCESS CONTROL > Authentication Policies > Edit Authorization page has been increased to 64 characters. [BNWF-24437]

System

- Enhancement: Performance is now improved for "More Actions" options (Copy, Move and Rename) on the BASIC > Services page. [BNWF-24504]
- Fix: Enabling web application firewall for 'Custom' services no longer causes a rollback/crash. [BNWF-25091]
- Enhancement: The "X509_ISSUER" macro that provides the ISSUER details from the client certificate has been added to the "Rewrite Value" list in the WEBSITES > Website Translations page, HTTP Request Rewrite section. [BNWF-23678]
- Fix: A configuration issue that occurred when the "Mode" for attack pattern was changed, has been fixed. [BNWF-24805]
- Fix: The data path crash that was observed when the uploaded files were scanned for virus, has been addressed. [BNWF-25138]
- Fix: A memory leak issue that was observed when the uploaded files were scanned for virus during heavy traffic, has been fixed. [BNWF-25122]
- Fix: When compression is enabled, an extra byte is no longer added to a zero byte file. [BNWF-24588]
- Fix: Changing the system name now does not change the “Global Threshold” value configured on the BASIC > Notification page. [BNWF-24459]
- Fix: Empty rows in response pages caused a page unavailable error and a rollback. This issue is now fixed. [BNWF-24575]
- Fix: Local users with "admin" role can now perform network connectivity tests. [BNWF-24563]
- Fix: Barracuda logs now display the correct STM version. [BNWF-24886]
- Fix: An issue that resulted in potential outage when large number of events were generated, has been fixed. [BNWF-24873]
- Fix: A configuration error that was happening while changing the attack pattern mode, has been fixed. [BNWF-24805]
- Fix: Issues with FTP ACL is now handled properly. [BNWF-24613]
- Fix: An issue that displayed "Temporarily Unavailable" error on the BASIC > Services page, has been fixed. [BNWF-24260]
- Fix: A potential issue of dropping the response data when a large tag occurs in the backend response, is fixed. [BNWF-24239]
- Fix: In race condition where the configuration was wiped out in case of data path crash, is now fixed. [BNWF-24208]
- Fix: Servers disabled through the web interface are no longer re-enabled automatically when hostname resolution is turned on. [BNWF-24191]
- Fix: When a configuration backup was restored, hostname resolution for servers did not happen. This issue is now fixed. [BNWF-24113]
- Fix: A potential issue which may cause a brief service interruption when caching was enabled is now fixed. [BNWF-24101]
- Fix: An issue with XML content POSTed in a SharePoint application, which resulted in stripping of one extra character in the requests from the client being relayed to the backend SharePoint server, is addressed. [BNWF-24043]
- Fix: The Allowed Networks and Blocked Networks under IP Reputation is now working properly after a failback. [BNWF-24007]
- Fix: An issue that deleted the service after the renaming it using the "Rename" option, has been fixed.

[BNWF-24005]

- Fix: RD gateway was inaccessible when a URL translation rule was configured and accessed through WAF. This issue has been fixed. [BNWF-23951]
- Fix: In rare cases, GET requests exceeding 1024 bytes were not handled properly. This issue has been fixed. [BNWF-23950]
- Fix: A rare case with an outage involving a race condition with SSL request processing, is addressed. [BNWF-23895]
- Fix: An issue related to host name resolution when a DNS server responded with TTL '0', has been fixed. [BNWF-23851]
- Fix: The data path crash was observed when 'Allowed file upload' is not set to MIME types, and MIME type check was applied on the uploaded file. This issue has been fixed. [BNWF-23807]
- Fix: An issue that reduced the performance of the system due to high CPU usage, has been addressed. [BNWF-23641]
- Fix: An issue with hostname resolution that was corrupting internally used hostname templates, has been fixed. Also, hostname resolution will not be applicable for disabled services/rule groups. [BNWF-24984]
- Fix: A possible memory leak that was observed with client authentication enabled at the rule group level, has been fixed. [BNWF-23449]
- Fix: An issue that resulted in configuration rollback due to duplicate URL profile in the database, has been addressed. [BNWF-6615]

- Fix: A potential memory leak in rare cases involving continuous and frequent SNMP probes, is fixed. [BNWF-24562]

- Fix: Memory leak issue that occurred during the configuration updates, has been fixed. [BNWF-23089]

Logging and Reporting

- Feature: Added support for ArcSight. [BNWF-24463]
- Enhancement: Error codes have been added to system logs that indicate failures to get client IP/port. [BNWF-24812]
- Fix: The Barracuda Web Application Firewall now logs the requests in access logs when OOB or Connection-pooling is disabled on the WAF, and when the requests are not served by the server. BNWF-24641 [BNWF-24593]
- Fix: "Policy Fix" is now applied properly for the Web Firewall Logs that are generated due to bruteforce attacks. [BNWF-24631]
- Fix: "Page Not Found" issue on the BASIC> Reports page, has been resolved. [BNWF-24589]
- Fix: It is now possible to create CSV file for Web Firewall Logs and Access Logs even when the language is set to "Japanese" language. [BNWF-24477]
- Fix: An issue with an extra ampersand being appended in Access Logs and Web Firewall Logs (after parameter pairs involved in a POST or GET request) is now fixed. [BNWF-24120]
- Fix: A new report category 'System Summary Reports' is added in the BASIC > Reports page, which includes CPU Utilization, Memory Utilization and Total Bandwidth. [BNWF-24947]
- Fix: Scheduled reports are now working properly in the instances that are deployed on Microsoft Azure. [BNWF-21104]

- Fix: The “Policy Fix” wizard in the BASIC > Web Firewall Logs page now displays the recommendations properly. [BNWF-25143]

User Interface

- Enhancement: It is now possible to disable or delete a server that is not resolving to the hostname by using "Action For Stale Server" in the ADVANCED > System Configuration page. [BNWF-23593]
- Fix: An issue that displayed unavailable error on deleting a service on the BASIC > Services page, has

been fixed. [BNWF-24541]
- Fix: Uploading an invalid ZIP file in templates displays the appropriate error message. [BNWF-23975]
- Fix: A race condition due to which configuration updates from web interface and Hostname resolver were happening in parallel and causing a service downtime. This issue has been fixed. [BNWF-23729]

Management

- Feature: Added support for 'Template' apply operation to run as a background task. [BNWF-20616]
- Enhancement: Added support for persistent cookie in case of SharePoint documents. [BNWF-24816]
- Feature: It is now possible to configure maximum threshold for HTTP and HTTPS requests/minute on the ADVANCED > System Configuration page. This is valid ONLY for first five weeks, after which the threshold will be calculated based on internal algorithm. Any sudden spike in number of transactions will be captured in System Logs. [BNWF-10543]
- Enhancement: SMTP over TLS support is added for email notifications. [BNWF-15770]
- Fix: A unique SNMP engine ID is now generated for each device that is connected to an SNMP server. [BNWF-25111]
- Fix: The max limit exceeded warning is not displayed on the WEBSITES > Website Profiles page if the URL/Parameter profiles are optimized, and the profiles are lesser than the max limit. [BNWF-24780]
- Fix: A potential memory leak in rare cases involving continuous and frequent SNMP probes, is fixed. [BNWF-24562]
- Fix: The severity level for a specific URL Profile learning status log and a specific socket failure log, are changed to reflect the right severity. [BNWF-24503]
- Fix: "SMTP Email" test now works after saving the configuration as well. [BNWF-24270]
- Fix: SNMP "GET" for Total attacks will return last fetched value if there is any error in retrieving the value from summary log database. [BNWF-24640]

- Fix: Regex pattern validation in the **ADVANCED > Libraries** page, **Custom Attack Patterns** section, has been improved. [BNWF-23850]

High Availability

- Fix: When the **Operation Mode** is changed from **Proxy** to **Bridge**, cluster **Monitor Links** will be set to **WAN** and **LAN** and they cannot be unchecked. Also, when the **Operation Mode** is changed from **Bridge** to **Proxy**, cluster **Monitor Links** will be set to **WAN**. [BNWF-24151]

Cloud Hosting

- Fix: The "Geo IP Filter" under IP Reputation on Microsoft Azure is now working as expected when firmware version is upgraded. [BNWF-23875]

REST API Enhancements

- Fix: Response page values can now be set through REST API. [BNWF-23917]
- Fix: LDAP authentication is now supported through REST API. [BNWF-18194]