Release Notes Version 7.9.1

https://campus.barracuda.com/doc/42049443/

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 you upgrade to 7.9.x from 7.8.x or previous firmware versions, older web firewall logs and access logs will no longer be available on the Barracuda Web Application Firewall web interface. It is recommended to export relevant logs using the available options under **ADVANCED > Export Logs** before doing the upgrade. If you upgrade from 7.9 to 7.9.1, the older logs will be retained on the web interface. [BNWF-18274]

Firmware upgrade on older Barracuda Web Application Firewall appliances (with serial numbers less than 241000) may fail due to lack of appropriate disc space in the partition used during upgrade. Please contact Barracuda Networks Technical Support for assistance with the firmware upgrade to 7.9.1. [BNWF-18737]

If you upgrade to 7.9.x from 7.8.x or previous versions, the attack counts generated in 7.8.x or previous versions will not be populated in the World map on the **BASIC > Status** page, as the IP reputation (Geo IP) feature was implemented in version 7.9. For this reason there is inconsistency in total attack count in the Attack table and World map on the **BASIC > Status** page.

Change in behaviour:

- Only the base URLs are logged in the **BASIC > Web Firewall Logs** page. However, the query strings are logged in the **BASIC > Access Logs** page in the **Query String** field as usual.

Fixes and Enhancements in 7.9.1

System

- Feature: The Certificate Signing Request (CSR) created on the Barracuda Web Application Firewall now uses SHA-2 algorithm. [BNWF-18359]
- Feature: PROT P and PBSZ ftp commands are now allowed for FTP SSL service. [BNWF-18163]
- Fix: Resolved data path crashes on rare race conditions triggered by specific content. [BNWF-18878]
- Fix: Database server now restarts correctly on 32 bit systems in the event of a failure. [BNWF-18866]
- Fix: In some cases, the eventmgr process shut down abruptly due to inappropriate SSL values. This issue has been resolved. [BNWF-18845]
- Fix: A race condition which caused the system to rollback configuration changes after the firmware upgrade process has been fixed now. [BNWF-18730]
- Fix: User passwords now support all special characters. Some characters like "&" did not work earlier. [BNWF-18637]
- Fix: An issue where the SNI configuration was corrupted after the upgrade, resulting in service outages, has been fixed now. [BNWF-18485]
- Fix: The monthly report of attack graph on the **BASIC > Status** page was displaying incorrect data. This issue is fixed now. [BNWF-18379]
- Fix: It is now possible to configure a single IP address as Preferred Client IP Range in the rate control pool. [BNWF-18349]
- Fix: The %s macro now works correctly and does not lead to recursion. [BNWF-18332]
- Fix: A race condition where the request was intermittently dropped when a large file was uploaded is now fixed. [BNWF-18241]
- Fix: Parentheses () are now supported in Common Name when creating allow/deny rule for client certificates on the **ACCESS CONTROL > Client Certificates** page. [BNWF-18224]
- Fix: You can now set **Chunked Encoding Response Data** to *No* to ensure the server response is not sent to the client in chunks. [BNWF-18202]
- Fix: An issue that enabled/disabled the servers associated with a service without performing OOB health checks has been fixed. [BNWF-16273]
- Fix: The GeoIP database is updated to the latest to avoid any mismatch between IP Address lookup and blocking IP address due to GeoIP policy. [BNWF-16270]
- Fix: Reorganized database file layout for optimal utilization of disk space. [BNWF-18324]
- Fix: An issue where services with both VLAN and Non-VLAN applications did not recover properly when **Bridge on Server Failure** was set to *Yes* on the **ADVANCED > System Configuration** page in bridge mode, has now been addressed. [BNWF-15635] [BNWF-15765]

High Availability

- Fix: Config sync across a cluster works correctly when one or more schema or WSDL is bound to a service. [BNWF-18848]
- Fix: In a rare instance, primary cluster configuration was lost. This has been resolved. [BNWF-18464]
- Fix: An issue where the **Join Cluster** operation resulted in deleting SNMP allowed range from the IP tables has been fixed now. [BNWF-17163]

Logging and Reporting

- Feature: During SSL transactions, the negotiated protocol version is logged in the access logs. [BNWF-18307]
- Fix: Policy fix was not displayed for the older logs in the database. This issue has been fixed now. [BNWF-18719]
- Fix: All sensitive parameters are now masked in the **BASIC > Web Firewall Logs** page when asterisk (*) wild character is configured for a service in the **WEBSITES > Advanced Security > Mask Sensitive Data** in Logs section. [BNWF-18434]
- Fix: Duplicate entries were sometimes exported in FTP export. This is now resolved. [BNWF-18286]
- Fix: Policy Fix in **Web Firewall Logs** now shows the correct fix when parameter name includes a quote character. [BNWF-18060]
- Fix: Syslog traffic was getting routed through MGMT interface with WAN IP even after having static route in place. This issue has been fixed. [BNWF-17603]
- Fix: The Policy Fix for Metacharacter in header now removes the metacharacter found in the request from Denied Metacharacters list in the Header ACL. [BNWF-14786]
- 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-14772]

Access Control

- 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]

Security

- Feature: SAML 2.0 is now supported on the Barracuda Web Application Firewall. [BNWF-15040]
- Feature: SAML 2.0 Logout functionality, SAML authentication and authorization for a protected

resource has been implemented. [BNWF-18182]
- 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-18521]
- Fix: Perfect Forward Secrecy with ECHDE and DHE ciphers can now be enabled for the Barracuda Web Application Firewall web interface (UI). [BNWF-18419]
- Fix: When CSRF protection is enabled, the system was not processing POST requests correctly on data path restarts. This issue is resolved. [BNWF-18414]
- Fix: OpenSSL commands are now correctly executed on 32 bit systems. [BNWF-18365]
- Fix: A false positive in OS Command Injection Strict rule, pattern *misc-commands* has been addressed. [BNWF-18296]
- Fix: X-Frame-Options header is now inserted in all AAA related internal responses that are sent to the client from the WAF. [BNWF-18153]
- Fix: The max threshold for **Max Request Length** in the **SECURITY POLICIES > Request Limits** is now limited to 65536 bytes. [BNWF-17966]
- Fix: There was a configuration rollback when the firmware in the system was upgraded to 7.9 version while the cookie protection feature was configured with some case specific entries in the cookie exemption list, for example ABC,abc etc. This issue is resolved. [BNWF-17164]
- Fix: OpenSSL has been upgraded to 1.0.1j.

Management

- Fix: Scheduled FTP backups now work correctly. [BNWF-18371]
- Fix: Policy wizard fix was overriding the settings in URL Profile for Max Content Length/Max Upload Files/Max Parameter Name length if these fields were configured as empty in the SECURITY POLICIES > Parameter Protection. This is fixed now. [BNWF-18107]
- Fix: An administrator role with write permission on the service can now make configuration changes to the servers associated with the service. [BNWF-18057]
- Fix: Inconsistency with the display name **Method_Not_Allowed** *vs.* **Forbidden Method** attack has been fixed. [BNWF-17994]

Cloud

- Fix: On Microsoft Azure VM instances with less than 4 GB RAM, the STM process shut down abruptly due to memory related problems while storing logs in the database. This issue has been fixed to allocate appropriate database instances as the logs events are increased. [BNWF-17934]
- Fix: Inefficient process management for name resolution of servers specified using their host name (instead of IP address) caused large memory utilization impacting A1 and A2 instances in Microsoft Azure. This is now fixed. [BNWF-18212]

Networking

- Fix: Multiple DNAT rules can now be added to a Vsite if the destination IP address and Port are unique. [BNWF-10837]