Barracuda Web Application Firewall

Release Notes Version 8.1.1

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.

Fixes and Enhancements in 8.1.1

Security

- Feature: IP Reputation policy is now enhanced to apply the policy at application layer. All policies like GeoIP, TOR, BBL, Anonymous Proxy and Satellite Provider policy can now be applied at application layer.[BNWF-20913]
- Feature: The "~" and "%" characters are allowed to be added in "Exempted Cookie". [BNWF-22965]
- Enhancement: The value of "Suspicious Clients Track Interval" under "System Configuration" is now used to expire the sessions created for bot detection when "Web Scraping" is enabled. [BNWF-23506]
- Enhancement: Weak ciphers such as SEED-SHA, IDEA-CBC-SHA, ECDHE-RSA-RC4-SHA, ECDHE-ECDSA-RC4-SHA and RC4-SHA are removed from the "default" ciphers list. These ciphers are still available in the "Available Ciphers" list, and can be used by selecting the "Custom" option. [BNWF-23314]
- Enhancement: The client evaluation script is now inserted only in the "text/html" response pages. [BNWF-23269]
- Fix: Log flooding and possible backend server load surge when there are continuous attempts to reconnect on SSL connection failure, is addressed. [BNWF-23629]
- Fix: Parsing of responses containing compression content types, is now avoided, preventing false positives during CSRF checks [BNWF-23574]
- Fix: The data path crash that was observed while evaluating clients for web scraping and DDoS protection, has been addressed. [BNWF-23380]
- Vulnerability Fix: OpenSSL is upgraded to 1.0.1t, which addresses the following CVEs: [BNWF-23379]
    - CVE-2016-2108

- ○ CVE-2016-2107
- ○ CVE-2016-2105
- ○ CVE-2016-2106
- ○ CVE-2016-2109
- ○ CVE-2016-2176
- Fix: URL Encryption is now available on all AWS and Azure WAF models. [BNWF-23319]
- Fix: An issue that was causing configuration update to fail in the Exception Profiling module, has been fixed now. [BNWF-22960]
- Fix: "libssl" and "libcrypto" are made from OpenSSL 1.0.1u package for the recent vulnerabilities. [BNWF-24357]
- Fix: OpenSSL has been upgraded to 1.0.1t.

Access Control

- Feature: Provided UTF8 encoding support for extended ASCII characters for LDAP authentication. [BNWF-23330]
- Enhancement: Extended ActiveSync support to authenticate using internal LDAP users and handle pre-authentication with internal LDAP server. [BNWF-23003]
- Enhancement: SAML "authnrequest" now supports signed requests. [BNWF-22497]
- Enhancement: Added Support for the "AuthnContextClassRef" in the SAML "authnrequest" sent to the IDP. [BNWF-22496]
- Enhancement: CRL validation support added for client authentication enabled rule groups. [BNWF-19867]
- Fix: A possible crash when device-ids are missing in Active Sync requests, has been fixed. [BNWF-23565]
- Fix: Group authorization for user names having special character is now honored. [BNWF-23329]
- Fix: The "redirect URL" buffer size for SAML is increased to 4096 characters. [BNWF-23120]
- Fix: Domain part of "domain\username" login is made as case insensitive. [BNWF-23094]
- Fix: Username in uppercase letters are now honored when authenticating to the RADIUS server for admin access control. [BNWF-22973]

System

- Feature: The Redirect URL now supports "%d" option to copy the domain name from the HTTP request. [BNWF-23230]
- Feature: A "Comment" section is now available for "Exception Networks" under IP reputation Filter. [BNWF-22934]
- Enhancement: Maximum length of Subject Alternative Name (SAN) field, while creating new certificates, is increased from 512 characters to 2048 characters. [BNWF-23442]
- Enhancement: The max number of URL/Parameter profiles are limited to 5000 on the units that are having less than 4GB RAM size. [BNWF-23153]

- Enhancement: The maximum number value configurable for a JSON policy is now set to 999999999999999. A value of "0" will be considered to an infinite value. [BNWF-23106]
- Enhancement: Implemented support for handling nested groups across different domains on the Barracuda Web Application Firewall. [BNWF-17273]
- Enhancement: If the Web Firewall Policy binding in the rule group level is left empty, it would inherit the policy defined in the service level.
- Fix: Networking module hang during reboot in the presence of VLAN on management interface in Bridge mode, is now fixed. [BNWF-23896]
- Fix: An issue in the Server host name resolution using local host configuration on the BASIC > IP Configuration page, is fixed. [BNWF-23845]
- Fix: Data path crashes observed while logging the attack details for a service with no server associated, has been fixed. [BNWF-23735]
- Fix: A race condition resulting in a failure to bring up the networking module when server name is configured under Rule Group, is now fixed. [BNWF-23645]
- Fix: A possible rare crash in the connection pool module, is fixed. [BNWF-23572]
- Fix: A race condition while accessing the request related data structures caused a rare outage. This issue has been addressed. [BNWF-23534]
- Fix: Alert email is now sent when the data path resource usage exceeds 50%. [BNWF-23530]
- Fix: A rare race condition that may lead to a crash when hidden or session-invariant parameter checks are chosen, has been addressed. [BNWF-23515]
- Fix: A bug introduced in version 8.1 which may result in the flow control failing on the backend connections, causing increased memory usage during large downloads, is addressed. [BNWF-23511]
- Fix: Server Name extension is now sent to the backend server, when SNI is enabled for Rule group Server. [BNWF-23489]
- Fix: Alert for memory usage exceeding will be sent only if the total memory (RAM + Swap) exceeds 85%. [BNWF-23488]
- Fix: A star(*), a 'referer' and an 'user-agent' header-acls are added by default to the services configured on the Barracuda Web Application Firewall for reference and are kept disabled. [BNWF-23440]
- Fix: Optimizations to achieve a smaller memory footprint for processing a single HTTP/HTTPS request. [BNWF-23287]
- Fix: A rare occurrence of junk entries in the left panel of URL profiles when the "Delete All" operation is performed, has been addressed. [BNWF-23161]
- Fix: An issue that resulted in not displaying all services on the BASIC > Services page, has been addressed. [BNWF-23044]
- Fix: A data path issue seen while parsing JSON data, has been fixed. [BNWF-23017]
- Fix: Its now possible to download the backup through a support tunnel. [BNWF-22834]
- Fix: The private key is no longer exported in the backup if "Allow Private Key Export" is set to "No" for the certificate. [BNWF-21262]
- Fix: An issue where the reports/stats collection process filled up the storage space, has been addressed now. [BNWF-23692]
- Fix: Uploaded File name containing metacharacters %00%01%1b%7f in file extension are now blocked irrespective of mode of the service. [BNWF-14832]
- Fix: Upgrade process taking more time to complete, has been fixed. [BNWF-22978]
- Fix: In rare conditions, upgrading to 8.1.1 version was getting stuck due to an invalid log file.

This issue has been fixed. [BNWF-22990]

- Fix: A potential memory leak when processing POST body with erroneous syntax, is addressed. [BNWF-24202]
- Fix: An issue that caused slow database migration on upgrading to the latest version, has been addressed. [BNWF-22978]
- Fix: An issue that occasionally displayed "Temporarily Unavailable" page in the web interface after rebooting the system, has been fixed. [BNWF-24104]
- Fix: Added model 962 performance numbers for thresholds. [BNWF-24369]
- Fix: An issue related to host name resolution in which DNS server responded with TTL '0', has been fixed. [BNWF-23851]
- Fix: An issue related to host name resolution in which services continued to remain active even when DNS server was not responding/reachable, has been fixed. [BNWF-23028]

Logging and Reporting

- Feature: When the option to mask sensitive data is chosen and the HTTP referrer field contains this data, it is masked in the access logs. [BNWF-23546]
- Feature: A new section "System Summary Reports" is added on the BASIC > Reports page. This section includes CPU and Memory Utilization reports. [BNWF-22736]
- Feature: Added a new report 'Exception List' under 'Config Summary'. This report displays all IP Reputation Pools that are associated with service(s) and IP address(es) that are exempted from this pool. [BNWF-20937]
- Enhancement: Policy Fix for GEO_IP_BLOCK and TOR_IP_BLOCK attacks on Layer 7 is now available in Web Firewall Logs. [BNWF-23203]
- Enhancement: Failed connection requests now log the server IP address/port and destination IP address/port in the system log. [BNWF-22549]
- Fix: Syslogs are now sent through proper routes. [BNWF-23693]
- Fix: Client IP address, port and proxy IP address are now displayed correctly in Access Logs. [BNWF-23108]
- Fix: Destination IP address is now sent properly in the "Alert" message to the Microsoft Azure's Event Hub. [BNWF-24094]
- Fix: An issue resulting frequent logging process crash, has been fixed. [BNWF-24361]

User Interface

- Feature: Added 'Vsite' and 'Service Group' as filtering criteria on the BASIC > Services page. [BNWF-22856]
- Fix: A warning message is displayed when conflicting configuration for "Adaptive Learning" and "Exception Profiling" is detected. [BNWF-23636]
- Fix: Issues with the bulk edit of Services/Servers using "More Actions", has been addressed. [BNWF-22939]
- Fix: Page Not Found issue on log pages, has been addressed. [BNWF-22628]

- Fix: Health events now display the hostname/IP address of the server. [BNWF-22617]
- Fix: Creating ECDSA certificate with "secp256k1" Elliptic Curve (EC) is not supported now. This has been removed from the web interface as most of the web browsers do not support this curve. [BNWF-23857]

Management

- Enhancement: The clock source in the kernel is changed to HPET for 862 and 962 models. [BNWF-23399]
- Fix: "Allowed Methods" and "Content-Types" values under URL Profiles are now properly added when using a template. [BNWF-23676]
- Fix: "processCountHigh" and "memoryUsageHigh" trap definitions are added to the MIB file. The REVISION timestamp is updated to 'Aug 14 2014'. [BNWF-23608]
- Fix: Frequent reconnection attempts to the Barracuda Cloud Control, has been addressed. [BNWF-23568]
- Fix: A possible false alarm regarding low CPU Fan Speed, has been addressed. [BNWF-23451]
- Fix: Certificates page is optimized to handle large number of certificate uploads. [BNWF-23395]
- Fix: The "Apache Struts" patterns are updated to check for method and redirect based attack vectors. [BNWF-23218]
- Fix: An issue that caused the Management Interface to go down on an upgrade, has been addressed. [BNWF-23195]

High Availability

- Fix: Allowed 5 seconds deviation in cookie access time for clustered Barracuda Web Application Firewalls for better session management. [BNWF-23707]

Cloud Hosting

- Enhancement: Configuration backups and templates can now be used to specify the bootstrapping configuration in AWS Auto scaling. [BNWF-23304] [BNWF-23303]
- Fix: Fixed an issue where WAF was showing wrong cluster information on UI during AWS Autoscaling. [BNWF-22838]
- Fix: An issue that displayed inconsistent cluster information on the web interface in the AWS/Azure cluster environment, has been addressed. [BNWF-22536]
- Fix: An issue that was affecting configuration synchronization between the clustered instances during AWS Autoscaling events, has been addressed. [BNWF-22269]

REST API Enhancements

- Fix: An issue with retrieving a Vsite using REST API, has been fixed. [BNWF-23051]
- Fix: ECDSA key type is now supported while creating certificate through REST API. [BNWF-20741]