Release Notes Version 11.0

https://campus.barracuda.com/doc/95258499/

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 that 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 resolve to the configured host name. 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]
- Attackdef 1.172 is shipped with this firmware. It has changes relevant to the firmware's interoperability with the Barracuda Block Listed IP database. [BNWF-32541]
- On instances deployed on Microsoft Azure, if you are upgrading the Barracuda CloudGen WAF from versions earlier than v10.1.1, you might encounter issues with the Azure Managed Identities and Service Principal Names configured under **BASIC > Azure Configuration**. To resolve this issue, Barracuda Networks recommends you to use the latest CloudGen WAF image (i.e, 10.1.1) available on the Azure Marketplace or contact Barracuda Networks Technical Support for further assistance [BNWF-47993].

Fixes and Enhancements in 11.0

Features

Client-Side Protection

Barracuda Networks augments security with complete support for Content Security Policy(CSP) and

Sub Resource Integrity(SRI) validations.

- **Content Security Policy** is used to control the behavior of the client's browser. A full-featured wizard supporting all CSP directives enables administrators to control the resources that can be loaded in the client's browsers and direct the behavior of the various elements, tags, and other aspects of the web pages within the client's browser. Directives such as frame ancestors help in protecting against clickjacking attacks. [BNWF-46278] [BNWF-46278] [BNWF-25949]
- **Sub Resource Integrity** is a security feature that enables browsers to verify that resources they fetch are delivered without unexpected manipulation. This protects the applications from supply chain attacks that may be targeted at resources such as JavaScript, images, and other content loaded from third-party servers. [BNWF-46278]

These capabilities can be deployed in Report Only mode or in Block mode. In Report Only mode, all the violations of the policies are reported to the Barracuda Threat Intelligence Service and can be viewed using the Barracuda Threat Intelligence Service dashboard.

Advanced Bot Protection

Barracuda Advanced Bot Protection capabilities protect our customers against many types of automated attacks. Barracuda Networks continues to enhance the capabilities to detect and protect against automated attacks.

- Credential Stuffing attack protection has been enhanced to support applications that communicate credentials via JSON / AJAX requests or HTTP Basic Authentication mechanisms. [BNWF-33998]
- Brute Force Policy can now be triggered by matching a set of text patterns in the HTTP response body [BNWF-44932]

Security & Access Control

In this release, additional protection for APIs and Web Socket have been introduced along with multiple other enhancements.

- **JWT Validation:** JSON Web Tokens (JWT) are a common mechanism of representing claims securely, especially in the context of APIs. With version 11.0, the Barracuda WAF adds support for validating JWT tokens issued by the Authorization server. This feature is available on Barracuda WAF models 660 and higher. [BNWF-46375]
- **Web Socket Security:** Traffic on WebSocket can now be inspected for protocol violation and other exploits by the WebSocket security feature on the WAF. Administrators can configure the WebSocket security profile by navigating to **Websites > WebSocket Security**. [BNWF-25386]
- **Tarpit:** Suspicious clients can be tarpitted (slowed down) for time interval configurable from UI. [BNWF-46274]
- **Single Log Out (SLO) support for SAML**: SAML for Access Control has been enhanced to support SLO in which a logout response for any of the participating applications resident on the WAF will send a logout command to all participating SSO applications. [BNWF-33520]

Traffic Management

- **HTTP/2**: With this release, the Barracuda WAF adds support for HTTP/2 for WAF-to-server communication in addition to the client-to-WAF communication that has been supported from earlier releases. [BNWF-25380]
- **Direct Server Return**: The Barracuda WAF service can now be configured behind a load balancer service with Direct Server Return. This capability is used in rare scenarios where traffic from the server must be bypassed due to application considerations. This requires changes on the web server as well. [BNWF-46377]
- **IP Address from TCP Options (additional CDN Support)**: In many cases where the Barracuda WAF is deployed behind a CDN, the actual IP address of the client is encapsulated in the TCP "Options" field by the CDN infrastructure. The Barracuda WAF supports the reading of client IP and port from the TCP "Options Address" field. [BNWF-46376]

System Management

- **Auto Configuration Engine**: Customers with a Barracuda Advanced Bot Protection license can now use the statistical and machine learning-enabled configuration recommendation engine. This engine analyzes traffic patterns to recommend configurations that would make the existing deployments more secure.
- **SAML for Role Based Administration:** All user identity stores that support SAML, such as Azure AD or Microsoft AD/FS, can be integrated with the Barracuda WAF to enable Role Based Administration for the WAF administration. [BNWF-32912]
- **Alien Vault SIEM** is now supported by the Barracuda WAF.

Enhancements

Security & Access Control

- **Enhancement**: ReCAPTCHA functionality has been enhanced to support wild card characters for domains and to allow duplicate site and secret keys. [BNWF-46337]
- **Enhancement**: Same Site attribute can now be configured from the Cookie Security page. By default, this attribute will not be added by the WAF, which can be configured later to either Lax/Strict/None. [BNWF-33938]
- **Enhancement**: Bots configured in "Allowed List" are exempted from the "Fingerprint Challenges Exceeded" action policy. [BNWF-46059]
- **Enhancement**: Factory templates for Typo3, Magento, PrismWeb, and OsCommerce are now available in the **Advanced > Templates** page. [BNWF-33582]
- **Enhancements**: Users can now configure the OpenID Connect scope per URL by navigating to **Access Control > Authentication Policies > Add/Edit Authorization > OpenID Connect Scope**. [BNWF-44803]
- **Enhancements**: The host header value can now be excluded for authentication redirects. [BNWF-33989]
- **Enhancements**: Brute Force Policy be triggered by matching a set of text patterns against the

HTTP response body [BNWF-33840]

- **Enhancements**: Multiple domain controller IP addresses can be added for same Kerberos Domain Controller realms. [BNWF-30237]
- **Enhancements**: Ability to configure a minimum value for the JSON number value ("Max Number Value") in the JSON limit policy and JSON profile, along with the violated value being logged correctly in the Firewall logs. [BNWF-29392]

System Management

- **Enhancement**: Virusdef update will get triggered once a day instead of every hour to reduce resource contentions. [BNWF-47608]
- **Enhancement**: The new option "Blocklisted Category" for the Client Type filter drop-down list under Access/Web Firewall Logs has been added. [BNWF-47599]
- **Enhancements**: Users can now filter results on host name with 128 characters. [BNWF-30092]
- **Enhancement**: Support to collect statistics from more than 128 server objects under one service is now provided. [BNWF-47439]
- **Enhancement**: Disk space utilization on some Web Application Firewall models has been optimized to save logs and core files more efficiently. [BNWF-47349]
- **Enhancements**: The extended match now has a drop-down option, HTTP/2.0 as HTTP version. [BNWF-47054]
- **Enhancement**: The OpenSSL version running on the WAF has now been upgraded to OpenSSL 1.1.1i to fix security vulnerabilities. [BNWF-47016]
- **Enhancement**: The WEBSITES tab has a new DataTables widget. [BNWF-46144]
- **Enhancement**: JavaScript inserted for client identification is made non-finger-printable. Direct access to the JavaScript is no longer allowed. [BNWF-45577]
- **Enhancement**: On the Dashboard page, details for each interface now include rx_missed_errors counter details. [BNWF-33459]
- **Enhancement**: The upper limit for "Max Array Elements" and "Max Siblings" is now increased to 8192 from 1024 and 2048 respectively in the JSON limit policy and JSON profile. [BNWF-30529]
- **Enhancement**: The protocol / TLS version used between the WAF and the web server will now be logged in the Access logs [BNWF-26234]
- **Enhancement**: The log details now show the country name instead of country code. [BNWF-25889]
- **Enhancement:** Advanced Analytics dashboard is updated to improve the performance and visualizations. [BNWF-47616]

Fixes

- **Fix**: The UI output showing the incorrect value for the FAN- and CPU-related params on the Dashboard page for the new WAFs with the Aewin motherboards has been fixed.[BNWF-48217]
- **Fix**: An issue on 460/V460 models where Let's Encrypt certificate generation/renewal was failing has been fixed. [BNWF-48105]
- **Fix**: Delay caused by the stats collector process during datapath start has been fixed. [BNWF-47992]
- **Fix**: A new category under **Basic > Certificates** for managing certificates used for validating JSON web tokens has been added. [BNWF-47967]
- **Fix**: An issue that occurred with the bulk edit for ACLs turning their status automatically to On has now been fixed. [BNWF-47933]
- **Fix**: Support has been extended to have max concurrent HTTP2 streams as 100. [BNWF-47844]
- **Fix**: An issue where RBA was not honored for SECURITY POLICIES has been fixed. [BNWF-47677]
- **Fix**: An issue where the log rotation was not occurring for certain files, which led to unwanted disk usage, has been fixed. [BNWF-47553]
- **Fix**: Notifications for log storage on P5 instances has been fixed. [BNWF-47534]
- **Fix**: An issue where pagination was failing on the Website Profile page when the config changed has been fixed. [BNWF-47498]
- **Fix**: An issue where the user was being shown as "active" on the **Basic** > **Services** page even though the session was expired has been fixed. [BNWF-47478]
- **Fix**: Audit logs for automatic fixes from exception learning has been fixed. [BNWF-47437]
- **Fix**: An audit log for the the Firmware Revert operation that will show up in the Audit Logs UI has been added. [BNWF-47414]
- **Fix** : An issue where the Dashboard and Reports were failing to load on certain occasions due to the summary DB being corrupted has been fixed. [BNWF-47344]
- **Fix**: An issue where the TLS Protocol Version was not correctly passed to the web server when the HTTP Request Rewrite feature was used has been fixed. [BNWF-47341]
- **Fix**: Static routes with the same IP/Mask with different default gateways on the different Vsites are now shown correctly on **Networks > Routes** page. [BNWF-47301]
- **Fix**: An issue where OpenID was not working when the backend application initiated an OpenID request has been fixed. [BNWF-47092]
- **Fix**: An issue with the Serial console has been fixed. [BNWF-47080]
- **Fix**: A configuration wipeout issue caused due to the configuration agent crashing has been fixed. [BNWF-47071]
- **Fix**: A problem with BATD functionality when the request URL length was exceeding 1K has now been fixed. [BNWF-47070]
- **Fix**: The datapath crash while feeding the element parsing structure has been fixed.[BNWF-47057]
- **Fix**: An issue due to the misconfiguration in the attributes map configuration that caused an outage for service bound to the SAML authentication service has been fixed. [BNWF-46962]
- **Fix**: Support for NTLM authentication on a WebSocket-enabled service has been added. [BNWF-46960]
- **Fix**: Application-specific graphs will be populated and seen on the Dashboard for all systems

irrespective of the model [BNWF-46864].

- **Fix**: The configuration rollback issue after the automatic attack definition update has now been fixed.[BNWF-46830]
- **Fix**: An issue in which browsers were showing "ERR_SSL_KEY_USAGE_IN" for self-signed certificates created on the **Basic** > **Certificates** page has been fixed. [BNWF-46758]
- **Fix**: A Kerberos issue involving the intermittent timeout of applications has been addressed, and error logging has been enhanced to be part of the System log. [BNWF-46756]
- **Fix**: An issue where SNI domain bindings were getting corrupted when Let's Encrypt certificates were auto-renewed has been fixed. [BNWF-46751]
- **Fix**: An issue with the rate control module that was causing the Barracuda Web Application Firewall to freeze has been fixed. [BNWF-46698]
- **Fix**: An issue with the Backups to Keep functionality due to which the most recent scheduled backup was getting deleted (instead of the oldest backup) has been fixed.
- **Fix**: An issue where some of the services were showing an incorrect status on the console during the system startup sequence has been fixed. [BNWF-46590]
- **Fix**: Issue where the SNMP community string was not honored when changed via UI has been fixed. [BNWF-46568]
- **Fix**: A memory leak in a 192-byte segment due to app map content base has been fixed. [BNWF-46533]
- **Fix**: An issue where Navigation options were not working in BCC for JSON security has been fixed. [BNWF-46435]
- **Fix**: TLS versions that were getting disabled when a certificate was added to SNI Domains via API call has been fixed. [BNWF-46431]
- **Fix**: An issue with the synchronization of Exception Networks in IP Reputation across the units in HA has been fixed. [BNWF-46391]
- **Fix**: An issue where all filters where not loading up properly on the UI has been fixed. [BNWF-46387]
- **Fix**: An outage due to rate control has been addressed. [BNWF-46348]
- **Fix**: A configuration rollback issue due to duplicate Vsite IDs being allocated in the configuration has been fixed. [BNWF-46343]
- **Fix**: An issue where the template of a service was not getting applied for SNI certificates even when the certificates were present in another unit has been fixed. [BNWF-46302]
- **Fix**: A long User Agent header from Firefox causing the SAML library to crash has been addressed. [BNWF-46258]
- **Fix**: Severity for log indicating that the SNMP manager process is utilizing high CPU has been changed to "Info" from "Error". [BNWF-46244]
- **Fix**: An issue with snmpget for OID 1.3.6.1.4.1.20632.8.26 (Virusdef updates) has been fixed. [BNWF-46195]
- **Fix**: Datapath memory leak in a 64-byte segment due to internal cookies has been fixed. [BNWF-46194]
- **Fix**: Datapath crash while computing SSL fingerprints has been fixed [BNWF-46176]
- **Fix**: Issue while monitoring datapath memory usage on Platform 5 boxes has been fixed. [BNWF-46151]
- **Fix**: HTTP2 crash while closing idle HTTP2 session has been fixed. [BNWF-46107]
- **Fix**: Log storage usage percentage for P5 instances now displays correctly on **Basic > Dashboard**. [BNWF-46002]

- **Fix**: An issue due to which the hostname resolution process was exiting abruptly while deleting a server has been fixed. [BNWF-45892]
- **Fix**: An issue due to which the Default System Log Level configuration (available on **Advanced > System Configuration > Advanced > Logging**) was not working has been fixed. [BNWF-44823]
- **Fix**: X-Frame-options, X-Content-Type-Options and X-XSS-Protection headers have been added for authentication redirect pages. [BNWF-34039]
- **Fix**: An issue with OpenID Connect where users were getting a service unavailable error (503) on accessing the application has been addressed. [BNWF-33738]
- **Fix**: HTTP security headers provided by the Web Application Firewall's management interface has been updated. [BNWF-32839]
- **Fix**: An issue with normalizing characters in non-ASCII range causing false positives has been addressed. [BNWF-31011]
- **Fix**: An issue where the Proxy IP was not displayed properly in the Access Logs for HTTP2 requests has been fixed. [BNWF-30398]
- **Fix** : Changing the Vsite "Active On" option is not allowed if two units are not in the same state. [BNWF-29720]
- **Fix**: Module log level configuration will now persist even after a reboot or traffic manager restart. [BNWF-28208]
- **Fix**: Policy wizard fix for "Too many parameters" for a content rule bound to a different security policy than the service has been fixed. [BNWF-26463]
- Fix: Changed the text from DSR mode to Enable Loopback Adapter under **Edit Service > Advanced Configuration**. [BNWF-48288]
- Fix: Datapath crash while handling JSON payload has been fixed. [BNWF-48443]
- Fix: WAF now supports the Client Secret Post, Client Secret JWT, and Bearer Access Token Authentication method also to validate the JWT token with Authorization server. [BNWF-47555]
- Fix: An issue with the application layer health check for a hostname server configured with SNI has been addressed. [BNWF-48484]
- Fix: An issue where a few tabs were not visible via the Barracuda Cloud Control has been fixed. [BNWF-48258]
- Fix: Datapath crash while computing client fingerprint has been fixed. [BNWF-48674]
- Fix: An issue where Navigation options was not working in BCC for JSON security has been addressed. [BNWF-46435]
- Fix: A memory leak in DDOS path has been fixed. [BNWF-48131]
- Fix: The data path process crash that was seen when parallel JWT requests were sent and validated with Internal method, has been addressed. [BNWF-48197, BNWF-48006]
- Fix: UI inaccessibility due to unwanted logs filling up log storage has been addressed. [BNWF-48483]
- Fix: An issue where the system storage was getting exhausted due to excess logging of process monitoring has been addressed. [BNWF-48673]
- Fix: A bug that resulted in datapath outage when using Credential Stuffing Protection has been fixed. [BNWF-48515]

REST API

Enhancements:

- REST API v3.x now supports performing IP reputation lookups. [BNWF-31932]
- Logs REST API has been enhanced to support log filters to search specific types of log entries. The REST API version is v3.2. [BNWF-46783]

Fixes:

- **Fix**: An issue with the REST API v3.x that did not affect the changes done for GeoIP Allowed Networks/Blocked Networks has been fixed. [BNWF-29902]
- **Fix**: An issue with REST API validations that allowed users to create more than the allowed number of characters for the Sensitive Parameter Names field has been added. [BNWF-47407]