Release Notes Version 11.0.1

https://campus.barracuda.com/doc/96016156/

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 hostname. 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].

Features

- Feature: Ability to exempt client profile validations on IP addresses and IP address ranges. [BNWF-49269]

Fixes and Enhancements in 11.0.1

Security and Access Control

- Enhancement: Web Scraping now uses Advanced Threat Intelligence (ATI) for improved client classification. [BNWF-49263]
- Enhancement: Client fingerprint mechanism has been upgraded to support a wider range of applications. [BNWF-48931]
- Enhancement: AAA now allows LDAP users from 128 groups or more. [BNWF-48172]
- Enhancement: The 'Enable Client Fingerprinting' parameter has been moved from the BASIC > Services to the BOT MITIGATION > Bot Mitigation page. [BNWF-49548]
- Enhancement: User can now end the OpenID Connect session by redirecting the client to the redirect URL with "logout" as an HTTP query parameter. [BNWF-47078]
- Enhancement: CAPTCHA Validation is now enforced at the level of application session to avoid problems for clients coming from NAT'ed IP addresses. Only the sessions that solve the CAPTCHA are allowed to access the requested resources. Other clients that have not solved the CAPTCHA but may be coming from the same IP address will continue to be challenged or will be blocked. [BNWF-49261]
- Enhancement: Policy fix added for JSON minimum number value attack. [BNWF-47663]
- Enhancement: Max Cache Size can be configured for JSON Web Token (JWT) requests on ACCESS CONTROL > Web Token Validation > Add Validation Endpoint. [BNWF-48449]
- Enhancement: Deep inspection is now applied for text/plain content types in POSTs. [BNWF-14836]
- Fix: Enabling "Send Basic Authentication" resulted in duplication of domain name in the Authorization header sent to the server. This issue has been fixed. [BNWF-49808]
- Fix: Updated aggregate outbound IP ranges for Twitterbot are allowed from 11.0.1 firmware. [BNWF-47053]
- Fix: RADIUS and LDAP authentication services now allow special characters in the password. [BNWF-27264]
- Fix: The Action label in the Trusted Hosts section on the Access Control > Authentication Policies > Edit Auth Policy page has been changed from 'Default' to "Process". [BNWF-45918]
- Fix: Rule Group and JWT Profile can now be configured with the same name. [BNWF-49816]
- Fix: Group Mapping feature for SAML Admin SSO now correctly maps the group names to the WAF admin roles. [BNWF-48664]
- Fix: Bearer Token JWT Auth Mechanism field can now be configured as empty. [BNWF-48510]
- Fix: JWT Public keys uploaded using REST API are now displayed properly on the BASIC > Certificates page. [BNWF-48441]
- Fix: The Safari browser version should be 14.1.2 or higher to have SAML Single Sign-on to work properly. [BNWF-48542]
- Fix: Issue with the 'Policy Fix Wizard' where the JSON limit policy was being set to Empty has been fixed. [BNWF-47853]
- Fix: The Barracuda WAF now normalizes inputs containing special characters like CR and LF inside the buffers that could be attempts to evade detection of malicious input. [BNWF-49605]
- Fix: After upgrading to the 11.0.1 firmware version, SAML Single Sign-on must be reconfigured.

Certificate for signing requests must be created or uploaded and then associated with the SAML configuration. [BNWF-49930]
- Fix: An issue that displayed a blank entry for "suspicious clients" when client IP addresses were marked as suspicious due to the CAPTCHA policy has been fixed. [BNWF-49947]
- Fix: It is now possible to configure http:// in the URI path of an Allow-Deny rule. [BNWF-47156]
- Fix: Requests that do not include CRLF characters after header values are dropped with the attack category as “Protocol Violations”. [BNWF-46197]

REST API

- Fix: APIs to configure the SAML RBA are now available. [BNWF-48114] Note: When you upgrade from firmware 11.0 to 11.0.1 with SAML RBA configuration, SAML RBA needs to be reconfigured. If not, SAML Single Sign-On (SSO) will not work.
- Fix: An issue that caused an accumulation of a huge number of API requests from the ADP service has been fixed. [BNWF-49274]

Advanced Bot Protection

- Fix: Username and password parameters for Credential Stuffing Protection now allows all possible characters. [BNWF-49709]

Client-Side Protection

- Fix: In Offline upgrade, an issue seen in CSP/SRI due to failure of installing the dependency module has been fixed. [BNWF-48896]
- Fix: An issue where client fingerprint was not being generated when CSP was configured with mode as “Block” and script as “Include Nonce” has been fixed. [BNWF-49493]

Backup and Restore

- Fix: An issue where the upload directory was not being set properly while restoring a backup from an older firmware has been fixed. [BNWF-48869]
- Fix: The mode of internal attack patterns does not change after the backup restore. [BNWF-47908]

Logs and Reports

- Enhancement: Scheduling Reports now supports multiple filtering criteria based on the type of reports similar to the UI behavior. [BNWF-45363, BNWF-45365]
- Fix: Enforcing "Policy Fix" on a Web Firewall Log for 'Response Header Suppressed' attack does not cause configuration rollback. [BNWF-48265]
- Fix: An issue with template logging where logs were being lost after applying a large template has been fixed. [BNWF-48211]
- Fix: Log recovery mechanism has been added to recover the logs if there is any issue in saving logs to the intermediate log storage database, i.e., MongoDB. [BNWF-47373]
- Fix: Monitoring mechanism has been added to restart MongoDB if the memory usage by the mongod service is more than 10% of the available RAM. [BNWF-49502]

- Fix: Masking of sensitive data fields appearing in web firewall log details had an issue with case sensitivity of the chosen parameter to mask. This is now fixed. [BNWF-48933]

System Management

- Enhancement: Exception learning now supports learning from IPv6-trusted hosts as well. [BNWF-48188]
- Enhancement: The number of trusted CA certificates that can be associated with a service for verifying client certificates has been increased to 256. [BNWF-48485]
- Enhancement: Internal processes have been optimized to improve the system performance, especially for single-core instances. [BNWF-34515]
- Enhancement: The internal cookie of the Barracuda Web Application Firewall is no longer logged as "Unrecognized". [BNWF-47238]
- Enhancement: Ability to create and upload certificates for SAML Single Sign-On on the ADVANCED > Admin Access Control page. [BNWF-49665]
- Fix: A validation issue that allowed users to set the Allow/Deny rule sequence to more than 255, which is not supported, has been fixed. [BNWF-33756]
- Fix: Data-path crash caused by incorrect key profile in Passive mode has been fixed. [BNWF-33919]
- Fix: Removal of Ethernet cable of active link now changes the active link to the next available active link in the Active-Backup bonding mode on the 964D model. [BNWF-49597]
- Fix: Reboot or shutdown no longer takes a long time in a fully configured VM instance. [BNWF-49565]
- Fix: Non-English language characters are now allowed in Subject Alternative Names (SAN) when creating a certificate. [BNWF-49514]
- Fix: Large templates with SNI certificates mapping in the service template can now be applied successfully. [BNWF-49453]
- Fix: Firmware and Log Storage value no longer changes on the BASIC > DASHBOARD web interface when the page is refreshed. [BNWF-48856]
- Fix: Graphs on the BASIC > Dashboard page are now displayed properly when the language is set to French. [BNWF-47606]
- Fix: An issue where website translation was not working due to an extra space in the header has been fixed. [BNWF-33942]
- Fix: An issue where template import was exposed to certain security issues has been fixed. [BNWF-22692]
- Fix: If the WAF can fetch a client's entry from the database, which is dynamically populated by looking into the traffic pattern, it uses the "Client Type" information from the same database to validate the client. [BNWF-49507]
- Fix: Issue related to LE Certificate Renewal failure due to another certificate generation has been fixed. [BNWF-49887]
- Fix: Bond interfaces can now be created with WAN or LAN in the name string. [BNWF-49460]
- Fix: An issue that triggered unwanted alerts with event ID 62002 has been fixed. [BNWF-49272]
- Fix: The buffer data is streamlined and now sends in correct sequence. [BNWF-48832]
- Fix: In Bridge mode, moving a service from one Vsite to another Vsite has been disabled. [BNWF-47878]
- Fix: Data path process disruption that was seen after the FTP SSL service was enabled and the

resources on the FTP server were accessed has been fixed. [BNWF-49465]
- Fix: An issue due to which the system experienced high CPU utilization during the processing of requests through modules like bruteforce, tracking suspicious clients, lockout, and others, has been addressed. [BNWF-49125]
- Fix: Monitors for the request processing have been updated to check for erroneous or accidentally launched instances of the worker processes. [BNWF-48902]
- Fix: Incorrect validation errors during editing of URL profiles have been removed. [BNWF-48827]
- Fix: Duplicate URL and Parameter profiles are no longer created when 'Adaptive Learning' and 'Exception Learning' are on for a service and when a policy fix is performed. [BNWF-49260]
- Fix: Server hostname resolution in Turbo mode now works for all service types. [BNWF-49752]
- Fix: Turbo mode hostname server resolutions are now better managed to allow the creation of servers with local host IP addresses (127.0.0.x). [BNWF-49564]
- Fix: Configuring the same WAN IP and port combination for Services and Administrative access caused UI to be inaccessible. This issue has been fixed. [BNWF-47187]