Release Notes Version 10.1

https://campus.barracuda.com/doc/91980704/

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 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]

Fixes and Enhancements in 10.1

- **Feature**: A new cloud dashboard (Advanced Analytics Dashboard) for units with an active ABP subscription is now available in beta. This can be opened by clicking on the button in the Bot Statistics widget. [BNWF-33712]
- **Feature**: The Barracuda Advanced Bot Protection cloud has been updated with new Machine Learning models and integrated with the Infisecure bot engine. This capability requires an additional subscription [BNWF-33011]
- **Feature**: A new method for detecting stolen credential attacks, Credential Spraying, has been added. This is in addition to the existing Credential Stuffing protection and requires the Advanced Bot Protection subscription. [BNWF-32954]
- **Feature**: Support has been provided to detect the web development kits for all the requests generated through these tools. [BNWF-32655]
- **Feature**: Support for reCAPTCHA v3 has been added. [BNWF-32646]
- **Feature**: Tarpit capability as a follow-up action has now been added. With this, suspicious clients can be slowed down based on their risk scores. [BNWF-31987]
- **Feature**: The 'SameSite' cookie attribute is honored similar to other cookie attributes.

[BNWF-30631]

- **Feature**: OCSP stapling is now supported. [BNWF-21897]
- **Feature**: OpenID Connect is now supported. [BNWF-24025]
- **Feature**: SMB support has been deprecated and will no longer be available for the Barracuda Web Application Firewall v10.1 users. [BNWF-24008]
- **Enhancement**: The Problem Report file name now has the device serial number prefixed with the name. [BNWF-33554]
- **Enhancement**: JSON key profiles can now be created for keys starting with underscore (_). [BNWF-33492]
- **Enhancement**: There is now a notification available for Network Alerts. This option sends out an alert in case of issues with the internal iptables rules. [BNWF-33486]
- **Enhancement**: Support for configuring SAML user attribute string ""user"" as SAML Local_ID, has been provided. [BNWF-33245]
- **Enhancement**: The upgrade header is forwarded to the backend server when WebSocket is enabled at the service level. [BNWF-33147]
- **Enhancement**: ECDSA certificates now show to the associated services and SNI domains in Certificate reports. [BNWF-32843]
- **Enhancement**: The User Interface for BOT MITIGATION pages has been improved for ease of use and loading speed. [BNWF-32723]
- **Enhancement**: SMTP has been enhanced to use TLS1.2. [BNWF-32718]
- **Enhancement**: A new CAPTCHA state macro “%cs” is now available for Access Logs export. [BNWF-32478]
- **Enhancement**: SAML support for HTTP 2.0 has been added. [BNWF-32454]
- **Enhancement**: The hostname field in web firewall logs and access logs now show up to 127 characters. [BNWF-32217]
- **Enhancement**: Support has been added for the new MIME type 'application/x-dosexec' in Barracuda Advanced Threat Detection. [BNWF-32130]
- **Enhancement**: A new Client Profile feature is now available in the Security Policies tab. This feature works with the Advanced Bot Protection to support risk-score-based blocking. [BNWF-32106]
- **Enhancement**: The certificate reports now show SNI domain names as a separate section. [BNWF-31699]
- **Enhancement**: The 'Attacks by Category' report has been enhanced to show a stacked graph for better readability and interpretation. [BNWF-31529]
- **Enhancement**: A new hostname macro “%h” has been added for Web Firewall Logs export. [BNWF-31264]
- **Enhancement**: The Top Attacking Region/Country report now shows the world map with the geographical distribution of the number of attacks. [BNWF-31528]
- **Enhancement**: “Select/Deselect All” options are now available in multiple parts of the UI. [BNWF-30863]
- **Enhancement**: Barracuda Advanced Threat Protection logs now include the size of the file inspected. [BNWF-30856]
- **Enhancement**: Locked-Out client fingerprints can now be viewed and cleared out from the UI [BNWF-30715]
- **Enhancement**: The 'Secure Browsing' tab has been moved from the Websites tab to the Advanced tab menu and is visible ONLY when 'Enable Secure Browsing' is enabled (ADVANCED

> System Configuration > Advanced > Security Management). This feature will be deprecated in the near future. [BNWF-30120]
- **Enhancement**: Client Fingerprinting logic has been improved for better tracking. [BNWF-30066]
- **Enhancement**: IDP metadata for SAML services can now be automatically updated. [BNWF-24512]
- **Enhancement**: An option to configure domain name for SNI servers has been provided through URL translation. [BNWF-25755]
- **Enhancement**: Layer-7 health checks now make HTTP/1.1 requests if the host header is provided through UI. [BNWF-786]
- **Fix**: A path attribute has been added to the internally generated cookies for client tracking. [BNWF-33820]
- **Fix**: New attacks have been added to the Global Threshold under Notifications. [BNWF-33638]
- **Fix**: An issue with SAML session persistence has been fixed. [BNWF-33457]
- **Fix**: An outage in the response parsing of the data path that occurred due to the ABP module has been addressed. [BNWF-33634]
- **Fix**: An issue where attack names were missing some reports have been fixed. [BNWF-33600]
- **Fix**: A service outage that occurred due to data ingestion of the ABP feature has been fixed now. [BNWF-33555] [BNWF-33501]
- **Fix**: An issue that occurred in the Response page Headers where some characters were getting encoded in the response has been fixed. [BNWF-33485]
- **Fix**: An issue with REST API where the appID was not being honored at the time of service creation has been fixed now. [BNWF-33476]
- **Fix**: An issue with enforcement of override ciphers in the data path has been addressed. [BNWF-33447]
- **Fix**: WAF will not allow creating a service on the port that is already in use by system services. [BNWF-33382]
- **Fix**: A possible outage in the metacharacter detection module is addressed. [BNWF-33376]
- **Fix**: The support for larger values under JSON Max Number value field has been increased. [BNWF-33366]
- **Fix**: The LDAP user BindDn size can handle more than 1024 bytes correctly. [BNWF-33361]
- **Fix**: The Let’s Encrypt feature now supports SAN parameters. [BNWF-33344]
- **Fix**: An issue with forwarding X509 macros to backend servers when POST body is more than 1K has been fixed now. [BNWF-33269]
- **Fix**: A service outage that occurred during client authentication at Content Rule level has been fixed now. [BNWF-33267]
- **Fix**: A fix to avoid data path crashes while computing/manipulating utm cookies has been added. [BNWF-33156]
- **Fix**: A possible outage in processing a large number of client IPs for their reputation and history of attacks has been addressed. [BNWF-33155]
- **Fix**: Clients accessing OWA can now be fingerprinted. [BNWF-33128]
- **Fix**: Potential flooding of system logs when events get generated from chunked requests has been addressed. [BNWF-33080]
- **Fix**: Cookies are exempted from length checks when a wild card header rule in Allow/Deny/Redirect rules is created. [BNWF-33029]
- **Fix**: An issue where System Summary Reports were not saved while using Firefox has now been

fixed. [BNWF-32567]
- **Fix**: The Session Tracking cookie for HTTPS services now has the Secure attribute set. [BNWF-32393]
- **Fix**: Warning banners are not displayed once the user has acknowledged them. [BNWF-32308]
- **Fix**: An issue where IP addresses were not deleted from a connected Barracuda CGF has now been fixed. [BNWF-32255]
- **Fix**: An issue with logging the correct proxy IP when requests come in through persistent connections has been addressed. [BNWF-32251]
- **Fix**: An issue in the IP reputation-policy, specifically with countries belonging to Eurasia, has been fixed. [BNWF-32247]
- **Fix**: An issue where some configurations of response rewrite rules result in an outage when certain vectors arrive as payloads is now addressed. [BNWF-32118]
- **Fix**: XML Firewall now inspects the content type “ajax/help”. [BNWF-32053]
- **Fix**: Spaces in the host match that were causing problems with SAML authentication has been fixed. [BNWF-32012]
- **Fix**: Security and Traffic filters now support multiple values, and reports get filtered based on all multiple conditions. [BNWF-31909]
- **Fix**: An issue with the 'Extended Match' for Country Code with a single value has been fixed. [BNWF-31892]
- **Fix**: The 'Edit Administrator Role' page of ADVANCED > Admin Access Control, where the service group of the allowed services defaulted to 'checked' state, has been fixed. [BNWF-31857]
- **Fix**: The display of URL translation rules for different groups has been fixed. [BNWF-31851]
- **Fix**: The severity for 'Profile agent is restarting' log is changed to INFO from ERROR. [BNWF-31799]
- **Fix**: An issue with offline upgrade due to which an error "Page not found" occurred on Firmware Upload has been fixed. [BNWF-31638]
- **Fix**: An issue that occurred because of which the Action Policy Bulk Edit feature not working if the GUI was in Japanese, has been fixed. [BNWF-31550]
- **Fix**: Now multiple rule group servers can be deleted at once. [BNWF-31507]
- **Fix**: An issue where the Fix option was not available when the Attack was Deny ACL Match is now fixed. [BNWF-31086]
- **Fix**: An issue with normalizing characters in non-ASCII range that caused false positives has been addressed. [BNWF-31011]
- **Fix**: An issue with high CPU utilization with “Parse URL in Scripts” enabled that occurred for some CSS or JS files has been fixed. [BNWF-30954]
- **Fix**: An issue that occurred while performing Bulk Edit operations on the Networks tab when the locale is selected as Japanese has been fixed. [BNWF-30899]
- **Fix**: In certain scenarios, services stopped working because Connection Pool was failing. This issue has been addressed now. [BNWF-30889]
- **Fix**: An issue that displayed an error when the IP Lookup did not match anything in the IP reputation database has been fixed. [BNWF-30006]
- **Fix**: The user role can now be edited for RADIUS server users. [BNWF-27987]
- **Fix**: An intermittent issue when storing the Web Application Firewall backups in the cloud while connected to Barracuda Cloud Control has been fixed. [BNWF-27920]
- **Fix**: An issue that displayed "Page not found" on Audit log page because of rendering wrong DB

file location access has been fixed. [BNWF-22628]