



Release Notes Version 9.1.1

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.

If a server is added with the hostname, the Barracuda Web Application Firewall will automatically create server entries for all IP addresses that resolves 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]

Fixes and Enhancements in 9.1.1

Security

- When the Content-Length is zero on the response header, WebSocket connections would fail. This is now fixed. [BNWF-27916]
- An issue where the error message did not specify the actual error while creating a JSON profile has now been fixed. [BNWF-27661]
- Request containing data in XML format and Content-Type as application/xml will be parsed for vulnerabilities based on XML firewall configuration. [BNWF-27501]
- The number of Client certificate-based Allow/Deny Rules (per service), is now increased to 255. This was previously limited to 10 rules. [BNWF-27441]
- When the Service was set to Active mode and an associated URL Profile was set to Passive mode, attacks matching the URL Profile were blocked. This has now been fixed to ensure that the traffic is only logged and not blocked. [BNWF-27159]
- It is now possible to allow or deny meta characters in filename extensions. These checks will allow or block based on the Active/Passive mode of the associated Service. [BNWF-26627]
- Client connections using Proxy protocol that do not have a valid proxy protocol header are now dropped as per the spec. [BNWF-26623]
- A rare race condition where a failure to connect to the backend server while processing a request which caused a datapath outage is now fixed. [BNWF-25826]
- The DDoS and WebScraping Policy settings now have a toggle to detect mouse events. [BNWF-24561]
- A race condition that caused the datapath to go down while disabling a service, has now been fixed. [BNWF-15876]
- The persistent cookie used by the WAF for load balancing is now encrypted. [BNWF-14743]
- Fix: OpenSSL has been upgraded to 1.0.2l.



Access Control

- It is now possible to configure the Kerberos Service Principal Name (SPN) at the rule group level. Earlier, this was only possible at the Service level. Authentication for multiple domains under a single service is now possible with this change. [BNWF-27250]

Role Based Administration

- LDAP Authentication (for both Active Directory and OpenLDAP), is now enhanced to support Nested groups. [BNWF-26932]

Logging and Reporting

- An issue where logs were not generated when the virus scan failed for large files is now fixed. [BNWF-27981]
- An issue where the “Attacks by Category” reports did not match the count in Web Firewall Logs has now been fixed. [BNWF-27860]
- An issue where the “Performance Summary on Selected Service” report showed incorrect data is now fixed. [BNWF-27543]
- Performance improvements on lower end boxes like 360/460 for Logging and Reporting have now been implemented. [BNWF-27411]
- A rare issue which resulted in the client IP and port recorded in web access logs to be 0 (zero) is now fixed. [BNWF-27395]
- FTP access logs configurations are now synced to peer box if two WAFs are in cluster. [BNWF-27357]
- An issue where PDF reports were not generated when the GUI administration port was changed is now fixed. [BNWF-27102]
- An issue with the time scale on the “Attacks by Hour” report is now fixed. [BNWF-26907]
- Failures conditions in Connection Pooling are now logged in the System Logs. [BNWF-26665]
- All Traffic and Security reports can now be filtered using the Service IP and Service Port. [BNWF-19875]
- The log level for session timed out logs, has been changed from LOG_WARNING to LOG_INFO. Please enable the log level for "HTTPSVC" to INFO to see these logs. [BNWF-28219]

User Interface

- The Total Bandwidth graph is now enhanced to show multiple interface data on multiport box and WAN interface is the default interface. [BNWF-26166]



- An issue where the bulk edit for SSL Configuration was not working is now fixed. [BNWF-26043]
- It is not possible to bulk edit the Service Mode in the Services UI. [BNWF-25600]
- A new configuration option option "Count Auth Response Codes" is now available in the Bruteforce Prevention module. When enabled, it will count all error response codes as failure responses, otherwise it will ignore '401' and '407' response codes while counting the error responses.
[BNWF-25356]
- It is now possible to specify a Comma Separated list (4096 characters) of IP addresses in the extended match for the Client IP header. [BNWF-25287]
- An issue where the "Stop Capture" button on the TCPDUMP UI was not responding is now fixed. [BNWF-24986]
- The "Allowed API IP Range" setting in the Administration Settings is now deprecated and removed. [BNWF-22765]
- An issue where hashes (####) are displayed instead of Radio buttons when editing a Service using the Barracuda Cloud Control is now fixed. [BNWF-16291]

System and Management

- CPU usage threshold alerts now use the average value over a 5 minute period, instead of the average value of a 1 minute period. [BNWF-27813]
- An issue where creating a service with Non-ASCII characters was failing is now fixed. [BNWF-27750]
- The time taken to apply a large configuration set with over 2000 URL profiles has now been reduced. [BNWF-27723]
- An issue where system statistics collection consumed large amounts of disk space has now been fixed. [BNWF-27606]
- An issue where re-enabling an already enabled service resulted in a crash is now fixed. [BNWF-27600]
- Editing the configuration of any Service child object (Server etc.,) caused the GUI to show the first page of the Services list even when the edited Service was on a later page. This has now been fixed. [BNWF-27160]
- High CPU usage because of a logging module is now fixed. [BNWF-27058]
- An issue where the System IP and routes were wiped out post a clear configuration operation is now



fixed. [BNWF-26986]

Rest API

- [APIv3] When a Service name used camel casing, editing a content rule server under it caused configuration rollbacks. This is now fixed. [BNWF-27747]
- [APIv3] An issue where editing an IPv6 Server Port caused a “Duplicate Server IP:Port” error is now fixed. [BNWF-27662]
- [APIv3] An issue where API commands to update or delete a specific server might choose the wrong one under a different service is now fixed. [BNWF-27461]

