Release Notes Version 9.2.1

https://campus.barracuda.com/doc/79465440/

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 9.2.1

- Feature: Complete support for Barracuda reporting Server (BRS) [BNWF-29965]
- Feature: The ability to export logs to Cloud Syslog Services such as SumoLogic and Loggly has been added. [BNWF-29315]
- Feature: New macros X509_SAN_EMAIL and X509_IAN_EMAIL are introduced to configure the request rewrite rule to extract email fields from "Subject Fix: Alternative Name" and "Issuer Alternative Name" extensions from the client certificate.[BNWF-29261]
- Enhancement: A version of openssl, is now available in the problem report infrastructure. [BNWF-29908]
- Enhancement: The firmware release of WAF integrates with brs release version 1.0.3.570 and above. [BNWF-29449]
- Enhancement: The ability to add weak ciphers to the selected ciphers via REST API v3 for a service is enhanced. [BNWF-29431]
- Enhancement: Pagination and SEARCH BY feature for JSON security page has been implemented. [BNWF-27210]
- Enhancement: File extensions which are case insensitive at Parameter Profile level (same behavior as Global Parameter Protection level)is supported. [BNWF-23493]
- Enhancement: Content rule persistence idle timeout maximum value is extended from 1800 seconds to 86400 seconds. [BNWF-23405]
- Enhancement: An issue related to periodic download of CRLs has been fixed by decreasing the timeout value to 2 secs and allowing retries to be configured by the administrator. [BNWF -30126]
- Fix: The failure encountered when creating a private certificate for secure administration of webUI, has been fixed. [BNWF-30547]

- Fix: An issue with SAML single logout not logggig out from all the applications accessed from that browser/client, has been fixed. [BNWF-30511]
- Fix: By enabling Client impersonation, only one rule group server was reachable at the time of reboot. This issue has been fixed. [BNWF-30361]
- Fix: An issue with STM failure when the CRL file is loaded for Custom SSL service, has been fixed. [BNWF-30242]
- Fix: An issue with STM Crash on 9.1.1.008, has been fixed. [BNWF-30219]
- Fix: An issue where the offline upgrade of virusdef failed on the older hardware(s) with lesser /tmp partition, has been fixed. [BNWF-30164]
- Fix: An issue when the GET API calls for "Servers" and "Rule group servers" returning an incorrect key, has been fixed. [BNWF-30143]
- Fix: An issue with the jobs scheduler which was causing a spike in the system load, has been fixed. [BNWF-30119]
- Fix: An issue when the local administrator user was added on HA units, has been fixed. [BNWF-30100]
- Fix: The outage caused during a virus scan of a file with more than 256 characters in the filename, has been fixed. [BNWF-30010]
- Fix: An issue which resulted in a crash when the service was disabled, has been fixed. [BNWF-29987]
- Fix: The SSH as an admin to WAN/LAN/MGMT interfaces now can use an upgraded version of OpenSSH which has some vulnerabilities addressed. [BNWF-29980]
- Fix: An issue with the "Update ID" field displaying incorrect values in the "Edit Action Policy" page, is now fixed. [BNWF-29977]
- Fix: The username which has a backslash is unable to login via Radius authentication, has been addressed. [BNWF-29900]
- Fix: Inconsistency in WEBSITE > Website Translation page, has been fixed. [BNWF-29869]
- Fix: Failure to FTP access logs in some cases, has been fixed [BNWF-29853]
- Fix: Memory leak in data path when HTTP2 is enabled, has been fixed. [BNWF-29847]
- Fix: Unable to set the default value as "None" for External ldap service, has been fixed. [BNWF-29828]
- Fix: WAF-OMS plugin error for export logs when the host IP is configured as public IP, has been addressed.[BNWF-29795]
- Fix: The inconsistency between Dashboard graph data and Reports graphs data, has been fixed. [BNWF-29751]
- Fix: An issue in adding IPv6 Network ACLs via API-v3, has been fixed. [BNWF-29612]
- Fix: Umlauts characters for LDAP (admin access control) username and password is allowed. [BNWF-29602]
- Fix: An issue with the TCPDump functionality which was causing a "Temporarily Unavailable" on the GUI, has been addressed. [BNWF-29577]
- Fix: All services with write permissions will be displayed in the "More Actions" drop-down list. [BNWF-29509]
- Fix: Issue with configuring Network ACLs with port 21 have been resolved [BNWF-29451]
- Fix: The System logs generated on every FTP request is now reduced when the server is disabled by OOB [BNWF-29447]
- Fix: The factory monitoring-manager role was unable to see logs, has been fixed. [BNWF-29411]
- Fix: The factory audit-manager role was unable see any logs, has been fixed. [BNWF-29410]

- Fix: A possible outage in the config management which causes the configuration to go out of sync with the data path, has been addressed. [BNWF-29053]
- Fix: An issue with Web firewall policy wizard, has been fixed. [BNWF-28980]
- Fix: The HA state transition while recovering from Failed-Failed state in Manual mode, has been addressed. [BNWF-28860]
- Fix: When the client authentication is enabled at rule group level and the rule group names have similar names, a bug in the firmware caused false positives and thus rendered unnecessary client authentication requests. This has been fixed now. [BNWF-28558]
- Fix: Data path using high CPU while parsing URLs in CSS, is addressed. [BNWF-28156]
- Fix: An issue with an automatic host name server resolution, which could have caused a possible downtime for an application, has been fixed. [BNWF-28069]
- Fix: Features such as BATP and Anti-DDoS have been disabled on Hourly/Metered. [BNWF-27552]
- Fix: Evasion of the file extension check using apache double extension vulnerability (eg. filename.php.jpg) is addressed. [BNWF-14517]
- Fix: The memory leak that occurred in the logging module on accessing the services through private IPs, has been fixed now. [BNWF-29979]
- Fix: An issue with Azure, when a service was created along with a new service group due to which a Temporarily unavailable page was getting displayed, has been fixed now.[BNWF - 30003]
  Note that this issue occurs only when Azure Multi IP is enabled.

When the newer Vx instances supports multi-port, the older instances should be recreated to get the capabilities.