Release Notes Version 7.8.1

https://campus.barracuda.com/doc/36405266/

Please Read Before Updating

Before installing any firmware version, be sure to make a backup of your configuration and read all release notes that apply to versions more recent than the one currently running on your system.

Do not manually reboot your system at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support. The update process typically takes only a few minutes after the update is applied. If the process takes longer, please contact Barracuda Networks Technical Support for further assistance.

- Please make sure that the system has attack definition 1.45 if the system is being upgraded using the offline upgrade process.
- The upgrade to 7.8.1 may take little longer time due to kernel upgrade. For this reason, you might see the web interface coming up before the actual upgrade completes. It is recommended to wait for few minutes (approximately 10 minutes) after the web interface comes up, and then continue accessing the box.

Fixes and Enhancements in 7.8.1

Security

- Feature: Tor exit nodes can now be blocked from accessing services. [BNWF-15295]
- Feature: An irreversible hash is performed on the user passwords including the admin password to ensure password secrecy in the system. [BNWF-14816]
- Enhancement: The CSRF token embedded in the form can have validity period/expiry time set when CSRF Prevention is set to "Forms" or "Forms and URLs". [BNWF-15346]
- Enhancement: The double decoding is now applied to URL before deep inspection. [BNWF-15286]
- Enhancement: The encryption algorithm used for backup file now supports multibyte/wide characters. [BNWF-15276]
- Enhancement: Support for normalization of Microsoft %u encoding before deep inspection. [BNWF-15221]
- Enhancement: Deep inspection is now applied for "text/plain" content types in POST body parameters. [BNWF-14836]
- Fix: An issue with flow control in SSL layer, which may affect large size SSL transactions is addressed. [BNWF-15736]

- Fix: The CSRF protection for forms with action URL as "#" was causing false positives. This issue has been fixed. [BNWF-15219]
- Fix: An issue where authorization policies not getting displayed has been fixed. [BNWF-15205]
- Fix: False positives in CSRF protection in case of direct access to URL from a valid reference has been fixed. [BNWF-15183]
- Fix: Protection against Apache range header DoS has been added. No more than 5 range-bytes can be requested. [BNWF-15104]
- Fix: XML data which has TRANSACTION node is masked now. [BNWF-15065]
- Fix: Mime type detection works for multiple file uploads. [BNWF-14679]

Networking

- Enhancement: Prioritization of Network ACL is now supported. [BNWF-15237]
- Fix: IP rules for MGMT static routes get correctly synchronized on the secondary in the cluster. [BNWF-15533]
- Fix: Upper limit for network ACL priority has been removed. [BNWF-15172]
- Fix: Interface status will not be shown as DOWN if the IP address has not been configured. [BNWF-15076]
- Fix: STM crash issue during a brute force attack where more than 2 million concurrent connections are attempted on the Service has been resolved. [BNWF-14842]
- Fix: Restoring a backup does not affect the values of management routes and system routes of a system. [BNWF-14710]

Access Control

- Feature: The domain information of the client is forwarded to the server along with the user credentials in the Basic Authentication Header when Send Basic Authentication is set to Yes (ACCESS CONTROL > Authorization). [BNWF-15444]
- Feature: For MS LDAP authentication, if the server indicates an expired password, the Barracuda Web Application Firewall can redirect the user to reset it. [BNWF-14830]
- Fix: Accessing a page with multiple web links in Kerberos authentication service was sometimes causing the user to get logged out abruptly. This issue has been fixed. [BNWF-15667]
- Fix: LDAP lookups for RBA now supports group filters. [BNWF-14562]

Cloud Hosting

- Feature: Ability to automatically get the DNS server IP address during provisioning of the Barracuda Web Application Firewall Vx in the Azure cloud. [BNWF-15143]

System

- Feature: Automatic recovery from a Bypass state is now possible without the need for rebooting the appliance. [BNWF-15491]
- Feature: Optimizations to reduce the overall configuration commit times for large configurations. [BNWF-14810]
- Enhancement: Henceforth, the attack definitions are not activated automatically until "Enable Auto Apply Attack Definition" is set to Yes on the ADVANCED > System Configuration page manually. This setting is implemented to ensure that the activation of definition can be carried out during the production maintenance window. [BNWF-15250]
- Enhancement: Apart from the "admin" user, LDAP users with "admin" role also have permissions to restore backup. [BNWF-15238]
- Enhancement: The new version 7.8.1 has an updated core kernel to address rare kernel panics reported on Barracuda WAF. [BNWF-14817]
- Enhancement: FTP Allowed Verbs list now includes MLSD and MLST commands. [BNWF-7302]
- Enhancement: IP Reputation Filter is now available in Bridge mode. [BNWF-14761]
- Enhancement: Some important processes which relate to the management of the Barracuda Web Application Firewall now run with constrained privileges to prevent any misuse of privileges by potential attackers. [BNWF-14851]
- Enhancement: TCP dump captures bi-directional traffic for specified IP/Port. [BNWF-14729]
- Fix: Option to use SSL v3.0 in addition to all TLS versions for back-end SSL added. [BNWF-15735]
- Fix: A race condition in datapath process when Authentication was enabled for a SSL service has been fixed. [BNWF-15519]
- Fix: An issue where the Service was showing Active even when all servers were down has been fixed. [BNWF-15511]
- Fix: The "default" policy in Action Policy now includes secure-browsing, slow-client-attack, and captcha. [BNWF-15384]
- Fix: A possible race condition in case of arrival of multiple pipelined requests has been fixed. [BNWF-15246]
- Fix: Cipher suite preference can now be enforced from the service rather than relying only on the client's preference. [BNWF-15231]
- Fix: Chained certificates uploaded in PFX format are now arranged according to the certificate hierarchy. [BNWF-15015]
- Fix: Instances of Certificates page not getting displayed issue has been fixed. [BNWF-15192]
- Fix: The redirect URL can now include query string parameters in it. [BNWF-15139]
- Fix: Configuration rollbacks during "Policy Fix" operation in Web Firewall Logs has been fixed. [BNWF-15136]
- Fix: Issue with a possible outage when learning is enforced from trusted hosts, is fixed. [BNWF-15016]
- Fix: If the installed attackdef version is higher than new firmware's attackdef, firmware upgrade will not upgrade the attackdef. [BNWF-14995]
- Fix: Response body rewrite now honors Content Type: application/json. [BNWF-14952]
- Fix: All cipher suites are carried over to the upgraded version when the firmware version of the

Barracuda Web Application Firewall is upgraded. [BNWF-14938]
- Fix: In rare cases FTP proxy was aborting connection randomly when multiple files were uploaded. This issue has been fixed now. [BNWF-14891]
- Fix: Configuring a rewrite condition with the macro X509_OU for a request rewrite rule is not allowed. [BNWF-14760]
- Fix: Caching a large number of big size files was causing the STM process to crash. This issue has now been fixed to handle. [BNWF-14730]
- Fix: Concurrent session issue while uploading the wsdl/schema file is resolved. [BNWF-5468]

Logging and Reporting

- Feature: The interface IP address information is now included in problem report files as well as configuration snapshot files to aid troubleshooting. [BNWF-14790]
- Fix: Unit serial number is added to the file names generated by the reporting module. [BNWF-15079]
- Fix: Logs exported via FTP now export completely, upto a maximum of 500K entries. [BNWF-15034]
- Fix: Special characters such as ? In the requests are correctly handled to ensure that the syslog entries are not sent with incorrect Syslog Facility. [BNWF-14991]

Management

- Feature: Redirect action can be configured as temporary redirect or permanent redirect resulting in the Barracuda Web Application Firewall using 301 or 302 response codes respectively. [BNWF-12212]
- Fix: Service related statistics can be enabled in the BASIC > Status page only if there is atleast one service of type HTTP. [BNWF-15039]
- Fix: It's now possible to generate and download Problem Report in the Japanese web interface. [BNWF-14736]
- Fix: Relative URLs can be specified in redirect URL for Action Policy. [BNWF-12401]

High Availability

- Feature: Under Bridge mode, (Link Loss Carry Forward) LLCF is now supported. If enabled, either WAN or LAN going down causes the other one to be brought down forcibly. [BNWF-6070]
- Fix: In Bridge mode, the disjoin operation is not supported if the Primary unit is in Passive state. [BNWF-15374]