Release Notes Version 7.8

https://campus.barracuda.com/doc/30114103/

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.

Fixes and Enhancements in 7.8

Security

- Feature: Barracuda IP reputation database (BBL) is now integrated with the Barracuda Web Application Firewall. [BNWF-13834]
- Feature: The extension "*.css" is added by default to the list of Excluded URL patterns under the website profiles. [BNWF-13661]
- Enhancement: New action policies have been added for DDoS policies using Captcha based protection.[BNWF-14655]
- Enhancement: Response body rewrite is now performed for the content-type "application/x-java-jnlp-file" too. [BNWF-14608]
- Enhancement: OWA 2010 is added to the list of default Security Policies. [BNWF-11698]
- Fix: Sensitive parameter names that needs to be masked can include colon (:) in it. [BNWF-14281]
- Fix: The sensitive parameters in the query string are cloaked when a request matches the rule group. [BNWF-14641]
- Fix: The encoded parameters in the URL are not decoded once the SSO Cookie Update Interval is triggered. [BNWF-14522]
- Fix: The follow up action in the action policy feature is now fixed to check for values in the x-forwarded-for headers. [BNWF-14255]
- Fix: SOAP1.2 requests are checked for attacks and blocked. [BNWF-14220]

- Fix: Secure browsing feature is now compatible with Safari and Firefox browsers running on Macintosh computers. [BNWF-14204]
- Fix: A reflexive XSS vulnerability in the URL ACL name field has been fixed. [BNWF-14151]
- Fix: An attack variant of an SQL injection attack that uses white space characters for obfuscation can be blocked through an addition of a new pattern called "SQL-Command-strict" to the SQL Strict pattern list. [BNWF-13371]
- Fix: All the configured Authorization policies in the Access Control > Authorization page are now visible to an administrator. [BNWF-13481]
- Fix: Cookie entries can include a # in the name. [BNWF-13479]
- Fix: Forceful browsing of /README URI is not allowed. [BNWF-12046]
- Fix: The SSLv3/TLS attack referred in CVE-2009-3555 has been addressed. [BNWF-4970]
- Fix: Response headers are suppressed/cloaked for all pre-defined security policies. [BNWF-4444]
- Fix: Pattern algorithm can now be configured for input types and attack types. [BNWF-889]
- Fix: OpenSSL has been upgraded to 1.0.1e.

Networking

- Enhancement: The ACLs , routes for the management network are now synchronized as part of the configuration synchronization in a cluster. [BNWF-14453]
- Enhancement: Ability to have system IP address on a VLAN interface. [BNWF-5013]
- Fix: Source port range and destination report range options are disabled if the protocol selection is "All-Protocols" during ACL configuration. [BNWF-14203]
- Fix: The configuration file restore operation on a different system ensures proper import of static routes created under the management network group. [BNWF-14202]
- Fix: Multiple source NAT policies can be created if the source port value is different in each policy. [BNWF-14180]
- Fix: An issue where the interface routes were not persistent across reboots has been fixed. [BNWF-13846]
- Fix: The external syslog server communication is initiated through the required interface after checking the routing table. [BNWF-13600]
- Fix: With certain NAT or firewall devices, aggressive socket recycling could lead to dropped SYN requests due to differing timestamps sequences from the devices for multiple hosts behind them. The system now employs a safer alternative of reusing sockets that works well with remote NAT devices and doesn't reduce performance either. [BNWF-11488]

System

- Feature: Persistence method based on HTTP headers can be configured for server load balancing under the service configuration. [BNWF-14124]
- Feature: A certificate revocation list can be configured on the Barracuda Web Application Firewall. [BNWF-13739]

- Feature: Ability to unblock clients that got blocked due to a follow up action configuration. [BNWF-13707]
- Feature: It is now possible to select the required cipher suites for SSL negotiation. [BNWF-13769]
- Feature: Multiple certificates can be associated to a single Service, using SNI. [BNWF-13678]
- Enhancement: Client IP address is logged in the System Logs when the verification of client certificate fails. [BNWF-14493]
- Enhancement: Report graphs are now displayed with all legends in High Chart layout. [BNWF-14364]
- Enhancement: Remote Support can now be enabled through console to override the disable option set in web UI. [BNWF-14574]
- Enhancement - The default access control login page for a service can be modified to include a descriptive text. [BNWF-13502]
- Enhancement: Widget to select HTTP Methods has been added to filter the logs (Web Firewall and Access Logs). [BNWF-1359]
- Fix - The appliances that are not connected to the internet for activation can now be activated offline. [BNWF-13873]
- Fix: Browsers cannot save the password for the authentication login page automatically. [BNWF-14362]
- Fix: Trusted hosts IP addresses are also checked while inserting values for client IP address if "Header for Client IP address" option is configured. [BNWF-14640]
- Fix: A service group cannot be deleted until all the Services within the group are deleted. [BNWF-14465]
- Fix: An issue where a TCP connection between the client and the Barracuda Web Application Firewall was getting abruptly closed due to receiving a 401 response from the back-end server during NTLM authentication handshake has been fixed. [BNWF-13826]
- Fix: When authentication service is created to use LDAP over SSL, credentials are not cached thus allowing valid credentials to be used after a failed login attempt. [BNWF-13801]
- Fix: An issue which resulted in heart beat traffic with the wrong version being used after a firmware upgrade is now fixed. [BNWF-13730]
- Fix: It is now possible to configure a rewrite condition while configuring a request rewrite rule. [BNWF-13726]
- Fix: Template for URL ACLs now displays only the list of Service(s) that have URL ACLs configured in it. [BNWF-11432]
- Fix: Administrator can set the required ICMP response code while configuring Network ACLs. [BNWF-12382]
- Fix: Passive mode FTP on Microsoft IIS FTP is supported. [BNWF-13298]

Logging and Reporting

- Feature: Client IP addresses are included in system logs messages generated for renegotiation and handshake abortions. [BNWF-13781]
- Enhancement: Ability to change the font type while generating the reports in HTML or PDF format. [BNWF-12772]

- Fix: An issue while filtering the logs (Web Firewall/Access/Audit Logs) using Time as an additional filter has been fixed. [BNWF-13691]
- Fix: The virtual IP address is not duplicated in the database after the firmware upgrade. [BNWF-13778]
- Fix - Booting up issues on virtual machine instances installed on Citrix XEN Hypervisor have been fixed. [BNWF-14270]
- Fix: Server Time field in access logs was not displaying proper time in some cases. Fixed now. [BNWF-14410]
- Fix: In some cases, the cookie tampered logs were not logged due to the event manager process crashing. This issue has been fixed. {BNWF-14460]
- Fix: All necessary fields as prescribed by ArcSight SIEM are now added in the log format while configuring export log. [BNWF-13899]
- Fix: The log severity for the OCSP status check logs has been changed from error to Notice/Information. [BNWF-13841]
- Fix: In rare cases, the Web Firewall and Access Logs were not updated correctly. This issue has been fixed. [BNWF-13716]
- Fix: An issue that resulted in the configuration summary report for the URL profile and ACL getting generated as a blank report is now fixed. [BNWF-13660]
- Fix: Custom headers in the Access Logs display proper information. [BNWF-12987]
- Fix: Issue of logging random IP addresses when Header Name for Actual Client IP is specified and header has non-numeric value has been fixed. [BNWF-12979]

User Interface

- Feature: IP lookup tool is now provided to check the IP categorization based on location. [BNWF-13740]
- Feature: Bulk edit option has been provided to edit file upload extensions. [BNWF-13659]
- Enhancement: Bulk edit option is available for ACLs, Static Routes, Interface Routes and Custom Virtual Interfaces. [BNWF-11621]
- Fix: The X509_subject macro is now handled correctly in request rewrite rules. [BNWF-14723]
- Fix - Local Host Map entries on the BASIC > IP Configuration page can now be bulk edited. [BNWF-13998]
- Fix: CPU Utilization graph on the BASIC > Status page displays accurate value for the time scale "Month". [BNWF-14344]
- Fix: When CSRF protection is enabled under the URL protection, a PCI report generation on the Barracuda Web Application Firewall will show CSRF protection as "fully satisfied". [BNWF-14052]
- Fix : An issue which prevented an admin from editing the "More action" link in the Japanese language UI is now fixed. [BNWF-13733]
- Fix: An issue which resulted in the security policies not getting shown in the UI after a join cluster operation has been fixed. [BNWF-13728]
- Fix: Syslog details contain login/logout activity of Guest user. [BNWF-12828]
- Fix: Preferences option is available to set the Parameter profiles to be displayed per page. [BNWF-12692]
- Fix: Trusted certificates getting deselected automatically while editing the Service has been

fixed. [BNWF-11008]

Management

- Enhancement: FTP Allowed Verbs list now includes MLSD and MLST commands. [BNWF-7302]
- Fix: An STM crash due to the brute force prevention feature is now fixed. [BNWF-14553]
- Fix: In some instances, the website profiles page displayed the directory structure information incorrectly. This has been fixed. [BNWF-14478]
- Fix: It is now possible to backup configuration remotely using NTLMv2 authentication. [BNWF-14450]
- Fix: Ability to configure a custom admin role with permission to APPLY-FIX-FOR-ATTACKS which allows the user to apply policy violation fix rules in web firewall logs. [BNWF-14372]
- Fix: An issue where the SNMP agent on the Barracuda Web Application Firewall would not respond to SNMP queries due to heavy system load has been fixed. [BNWF-14321]
- Fix: SMB share names with white space can now be added during remote backup configuration. [BNWF-14296]
- Fix: Having a password less than five (5) characters in SNMP Manager was preventing further configuration changes under the Administration tab. This issue has been fixed now. [BNWF-14188]
- Fix: It’s possible to configure `--no-check-certificate' option while specifying the target URL for wget troubleshooting option. [BNWF-14059]
- Fix: An issue where client impersonation feature stopped working after a firmware upgrade is fixed. [BNWF-13820]

High Availability

- Fix: Join Cluster operation does not remove Management routes on the secondary/backup device. [BNWF-14420]
- Fix: An issue where the services stopped working due to incorrect system gateway information during cluster synchronization tasks has been fixed. [BNWF-14359]
- Fix: Cookie persistency is applied during HA failover. [BNWF-13927]
- Fix: In some instances, the services were not getting failed over to the peer system in the HA. This is now fixed. [BNWF-13684]
- Fix: Service disruption after recovering from network partitioning in cluster where the failback mode was set to manual has been fixed. [BNWF-14776]