Release Notes Version 7.9

https://campus.barracuda.com/doc/41108408/

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.

Change in behaviour:

- Only the base URLs are logged in the **BASIC > Web Firewall Logs** page. However, the query strings are logged in the **BASIC > Access Logs** page under **Query String** as usual.

Fixes and Enhancements in 7.9

Security

- Feature:A new feature, URL Encryption encrypts all end user exposed URLs to prevent forceful browsing and tampering attacks. [BNWF-1923]
- Feature: Authentication Services now allow multiple domains per service, allowing authentication across multiple domains by specifying domain\username. Logins with no specified domain use the configured default domain for the service to authenticate. [BNWF-16648]
- Feature: The Barracuda Web Application Firewall supports Perfect Forward Secrecy with ECDSA and RSA certificates and associated ciphers. The key exchange mechanism supported is Elliptic Curve DHE. [BNWF-15085]
- Enhancement: Added support for ECDHE ciphers for Perfect Forward Secrecy (PFS).
- Enhancement: Admin accounts can now be configured with password policies such as minimum strength, expiry and maximum retries. View locked admins on the **ADVANCED > Admin Access Control** page. Only admin users can clear the lockout for a locked admin. [BNWF-9385]
- Feature: Users can customize back-end SSL, including SNI extensions in the TLS header, if the server requires it. [BNWF-16566]
- Enhancement: The Authentication module now accepts domain\username for LDAP

authentication and correctly sends the username to the back-end in the Basic Authentication header. [BNWF-16184]
- Enhancement: The Authentication module now supports dual authentication against LDAP and RSA SecurID / Radius with OTP. [BNWF-16032]
- Enhancement: Default mode for new and updated patterns can now be configured as **Active**, **Passive**, or **Off** from the **ADVANCED > System Configuration** page. By default, these values are set to **Active** for a 360/460 but to *Passive* for a 660 and above. [BNWF-16021]
- Enhancement: Internal attack patterns can now be configured as **Active**, **Passive**, or **Off**, individually. [BNWF-15991]
- Enhancement: The redirect URL size for the global and local URL ACL rules has been increased to 1K. [BNWF-16215]
- Enhancement: LDAP authentication now supports usernames with backslash and other special characters. [BNWF-16973]
- Enhancement: It is possible to clone the values of an existing security policy and create a new security policy using **Create Template** on the **ADVANCED > Templates** page. [BNWF-16264]
- Fix: The Slowloris attack is split into two different attack IDs, named slow client attack and slow read attack. [BNWF-15998]
- Fix: Maximum headers are now restricted to 1024 and the header size to 128K, even in passive mode, to prevent DoS attacks. [BNWF-14890]
- Fix: The **State or Province name** of a Self-signed certificate created on the **ADVANCED > Secure Administration** page can now contain the space character. [BNWF-16951]
- Fix: Virus scanning correctly handles any request lacking a **Filename** attribute. [BNWF-16923]
- Fix: An OpenSSL issue reported in CVE-2014-0160 is now fixed. [BNWF-16810]
- Fix: File Upload Mime Types length has been increased to 128. [BNWF-16401]
- Fix: An SQL Injection attack vulnerability was fixed. [BNSEC-4406 / BNWF-16387]
- Fix: The response is not chunk encoded when **CSRF Prevention** and **Hidden Parameter Protection** is set to **None**. [BNWF-16256]
- Fix: An issue where DDoS policy was not getting deleted has been fixed. [BNWF-16246]
- Fix: An issue after applying a new attack definition when the latest attack patterns were not displayed on the **ADVANCED > View Internal Patterns** page has been fixed. [BNWF-16223]
- Fix: URLs in a request containing a hash (#) character are now blocked by a matching URL ACL blocking rule. [BNWF-16190]
- Fix: Policy Fix wizard now shows the correct recommendation for *File upload size exceeded* attack. [BNWF-16177]
- Fix:
  An issue with the learning module which caused a configuration rollback while learning paramet ers with ascii characters outside the printable range (e.g., 00, 01, etc.)
  has been fixed. These parameters are now skipped during the learning process. [BNWF-16116]
- Fix: Authorization policies with the same name across multiple services are now displayed on the **ACCESS CONTROL > Authorization** page. [BNWF-16048]
- Fix: The Barracuda Web Application Firewall
  uses the custom cipher list (if specified) for SSL handshake with clients
  when SNI is enabled for an HTTPS service. [BNWF-15954]
- Fix: Parameter names are now inspected to prevent attacks in the request. [BNWF-14454]
- Fix: Disabling **Offline Upgrade** sets **Automatic Update** to **ON** for all definitions. [BNWF-14307]

- Fix: Applying a new attack definition pattern no longer requires a restart of any internal service, and does not disrupt production traffic flow. [BNWF-6828]
- Fix: OpenSSL has been upgraded to 1.0.1h.

System

- Enhancement: Configure the time interval a client is considered suspicious on failing the CAPTCHA test using the field **Suspicious Clients Track Interval** in **ADVANCED > System Configuration**. [BNWF-17172]
- Enhancement: Specify whether a client which passed CAPTCHA validations is checked for bruteforce violations or not, using the field **Enable Bruteforce Checks for Validated Clients**. [BNWF-17053]
- Enhancement: The data path is now more resilient in a failure of the event management framework during system startup. [BNWF-16981]
- Enhancement: The list of locked out client IP addresses is now available on the **WEBSITES > Advanced Security** page. [BNWF-16854]
- Enhancement: Network Interfaces can now be disabled or enabled from the consconf. [BNWF-16176]
- Enhancement: Infrastructure to generate systemlog with alert for DRDY error is now available. [BNWF-16159]
- Enhancement: Adaptive Profiling can be restricted to certain response codes. [BNWF-4415]
- Enhancement: Configure partial matches for the cookie exempt list by specifying cookie exemptions like ctl*, *ctl, etc. [BNWF-592]
- Enhancement: Upper limits for the maximum characters/numbers allowed in each field during certificate creation are now enforced. [BNWF-16909]
- Enhancement: A certificate associated with a service, server, or a rule group cannot be deleted on the **BASIC > Certificates** page. [BNWF-16849]
- Enhancement: Using a new variable **Persistence Across Services**, under **ADVANCED > System Configuration > ADVANCED** section, cookie persistence is now available across services with the same server IP address but different ports. [BNWF-9419]
- Fix: In race conditions, traffic was not sent to the back-end servers even when the servers were up and running, and resulted in 408 timeout error. This issue has been fixed. [BNWF-17547]
- Fix: Fixed a latency issue in Instant SSL Services caused when Transfer Chunk Encoded responses were not sent to clients when the back-end server response included "Connection : Close". [BNWF-17371]
- Fix: Blank space after the IP address in the value of X-Forwarded-For header now logs client IP address in **BASIC > Access Logs**. [BNWF-17160]
- Fix: **ADVANCED > System Configuration > Set Failure Action = Drop connection** setting now works for Services of type **Redirect**. [BNWF-17150]
- Fix: An issue with the reboot process on appliances with SMB configuration has been fixed. [BNWF-17001]
- Fix: Request Buffering is no longer reset and now maintains its original value **Full** after upgrading to firmware version 7.8. [BNWF-16917]
- Fix: A stats collection framework memory leak has been fixed. [BNWF-16661]

- Fix: A server type selected on the **ADVANCED > Backups** page **Destination** is now reflected in the web interface and database. [BNWF-16660]
- Fix: Requests with Host headers followed by port number and a space are now honored. [BNWF-16414]
- Fix: Issues with re-imaging the device have been fixed. [BNWF-16338]
- Fix: An issue with the upper limit of 30 for the CRL name resulting in CRL configuration files getting overwritten has been fixed. Upper limits of up to 60 characters are now accepted. [BNWF-16298]
- Fix: An issue with services not being displayed after changing the service group name has been fixed. [BNWF-16263]
- Fix: A service can now be created on a port being used in the system. [BNWF-16239]
- Fix: An issue resulting in an STM process crash because of an abnormal number of X-Forwarded-For headers in a single request, has been fixed. [BNWF-16231]
- Fix: Cookie Update Interval set on the **ACCESS CONTROL > Authentication** page is now applied to requests with the POST method. [BNWF-16144]
- Fix: The **Copy** operation on the **BASIC > Services** page now copies website translation rules associated with the service. [BNWF-16076]
- Fix: An issue where the CRL Auto update configuration was not taking effect has been fixed. [BNWF-16005]
- Fix: An issue resulting in an STM process crash when a service, with authentication feature turned on and bound to a trusted hosts group, was disabled has been fixed. [BNWF-15845]
- Fix: An issue that caused configuration database corruption due to multiple STM related process instances running at the same time has been fixed. [BNWF-15758]
- Fix: An issue that caused the configuration snapshot to be corrupted and resulted in continuous rollbacks, has been fixed. [BNWF-15747]
- Fix: An issue that caused bad netmask length error in snmpd has been fixed. [BNWF-15737]
- Fix: An issue that caused an STM process crash during a configuration change process that resulted in a rollback, has been fixed. [BNWF-15227]
- Enhancement: Live charts are now implemented for CPU Utilization and Memory Utilization on the **BASIC > Status** page. [BNWF-15098]
- Fix: An issue that caused an STM process crash due to a process related to the website translation feature has been fixed. [BNWF-15088]
- Fix: An issue where a client sending multiple requests in the same TCP connection resulted in the logs displaying the server IP address only for the first request has been fixed. [BNWF-14367]

Logging and Reporting

- Enhancement: The reporting module has been overhauled and includes many new canned reports out of the box, including reports by geography.

  All log entries and report data prior to this update, with the exception of attack reports (counts only) for the past 10 days, will be lost. If you have not already done so, you should export the log data prior to updating.
- Feature: A new page, **BASIC > Notifications**, provides configurable notification policies for

system and security events.[BNWF-15973]
- Enhancement: System logs now capture installation information of definition updates. [BNWF-15829]
- Enhancement: The **Not In** filter operation is added for log fields with multi-select option in the logs (Web Firewall Logs, Access Logs, Audit Logs, System Logs and Network Firewall Logs). [BNWF-15809]
- Enhancement: A new column, Clickjacking, has been added in the access log indicating the request is protected from Clickjacking attacks. [BNWF-15458]
- Enhancement: Some access reports are not available by geography. [BNWF-15435]
- Enhancement: It is now possible to customize log data sent over syslog. [BNWF-15256]
- Enhancement: The **Blocked Requests by Services** report and **Attack Action** filter is available on the **BASIC > Reports** page. [BNWF-14999]
- Enhancement: You can now apply a filter to the **Security** and **Traffic** reports to limit a report to specific data. [BNWF-10841]
- Enhancement: Front-end timeout (Keepalive timeout) is now logged in the web firewall logs. [BNWF-16262]
- Enhancement: The '=' and '\' signs have been escaped for the following fields in the exported ArcSight logs: [BNWF-16551]
    - Web Firewall Logs: %adl and %u
    - Access Logs: %cs1, %cs2, %cs3, %q, %u
    - Audit Logs: %add, %ov, %nv
- Fix: The **Timestamp** and **Hostname** fields were logged twice by syslog-ng in the exported logs. This issue is now fixed. [BNWF-16949]
- Fix: Problem Report can now be downloaded when the language is set to Korean. [BNWF-16117]
- Fix: Admin password change is now logged properly in the **BASIC > Audit Logs** page. [BNWF-16038]
- Fix: Timestamp is displayed properly in the access logs when **W3C Extended Format** is **Log Format**. [BNWF-17500]

User Interface

- Enhancement: The web interface has been updated across all tabs and pages.
- Enhancement: Bulk edit option for management routes is now available [BNWF-15814]
- Enhancement: Admins can now monitor real time CPU, Memory, Bandwidth consumption from the Status page. [BNWF-15254]
- Enhancement: Test widgets for regexes are now available for attack types on the **ADVANCED > Libraries** page. [BNWF-3599]

Management

- Feature: Ability to view the statistics for the interfaces (WAN, LAN and MGMT) on the **BASIC > Status** page and **ADVANCED > Advanced Networking** page. [BNWF-15258]

- Enhancement: A completely new templates module allows template creation of existing policies and many other new features.
- Enhancement: It is now possible to add/remove IP addresses from the trusted host group through the Rest API. [BNWF-16009]
- Enhancement: It is now possible to View/Download Certificates through the Rest API. [BNWF-15988]
- Enhancement: For networking and troubleshooting, a **Sendgarp** button is added on the HA page, which sends three gratuitous ARPs to all active services on the box. [BNWF-15480]
- Enhancement: An option has been added to perform manual bypass from Consconf. [BNWF-15259]
- Fix: Request validation from the user is required before deleting network ACL. [BNWF-15521]
- Enhancement: Counters have been added for URL and Header ADRs. [BNWF-15134]
- Enhancement: The hostname for SNMP is now configurable. [BNWF-15067]
- Enhancement: Clear Configuration option has been added in Consconf. [BNWF-11966]
- Enhancement: It is now possible to exempt an IP address from the Lockout list by adding it to the exception list of the Bruteforce policy.[BNWF-14403]
- Enhancement: Host and URL are now separated in the Web Firewall logs. [BNWF-4403]
- Enhancement: Admin users can now access the Barracuda Web Application Firewall consconf through SSH. [BNWF-17376]
- Fix: In bridge mode, it is now possible to use the management port for system traffic, such as reaching the update server, license server, NTP, etc. [BNWF-15257]
- Fix: An issue where SNMP polling results for **number of active services** was inconsistent has been fixed. [BNWF-16701]
- Fix: An issue where the web server process for the system management incorrectly listened on 0.0.0.0:443 resulting in HTTPS services not working has been fixed. [BNWF-16249]
- Fix: Sensitive parameter names can now include underscore (_) at the beginning in **Mask Sensitive Data** on the **WEBSITES > Advanced Security** page. [BNWF-15935]
- Fix: Configuration backup now works when there are non exportable private keys in the system. [BNWF-3073]
- Fix: A RADIUS/Local administrator with admin role can now establish a support connection on the **ADVANCED > Troubleshooting** page. [BNWF-15682]
- Fix: It is now possible to bind up to 64 trusted certificates to an HTTPS service. [BNWF-15357]
- Fix: An issue where the RSA Private Key appeared twice in the Certificate file when a certificate was uploaded has been fixed. [BNWF-14622]
- Fix: Graphs on the **BASIC > Status** page display data correctly when **Preference** is set to **Day**. [BNWF-14551]
- Enhancement: FTP Allowed Verbs list now includes the PWD command. [BNWF-10164]

High Availability

- Fix: An issue that caused configuration failure when an IP Reputation Pool was added in a High Availability environment, has now been fixed. [BNWF-16241]
- Fix: In Bridge mode:
    - The Join Cluster operation cannot be performed if **Bypass on Failure** is **Yes** on the

Primary unit.
- Setting **Bypass on Failure** to **Yes** is not allowed when the units are in cluster. [BNWF-15163]

Cloud Hosting

- Fix: Saved backups can be deleted from the Cloud. [BNWF-17599]
- Fix: An issue where the service was getting configured on an incorrect subnet in the Azure environment has been fixed. [BNWF-16632]