Release Notes Version 7.7

https://campus.barracuda.com/doc/28475717/

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.

Fixed in Version 7.7

Security

SSL

- Fix for SSL renegotiation vulnerability, CVE-2009-3555.[BNWF-11177]
- Fix for SSL BEAST attack, CVE-2011-3389: ciphers can be preferred or enforced. [BNWF-12541]
- Back-end SSL connections from the Barracuda Web Application Firewall to the web servers can now be validated using trusted certificates. [BNWF-4963]
- OCSP certificate validation is supported. [BNWF-10260]
- Fix: OpenSSL has been upgraded to 0.9.8x.

Cookie Security

- Internally generated cookies for signing and encryption now reflect the path and expiry set by the application. [BNWF-10073]
- Cookies are no longer dropped if the Action Policy setting mismatched-IP-cookie-replay-attack is set to None. [BNWF-8771]

Website Profiles

- The learning of Parameter profiles is improved by removing the restrictions of name lengths from the existing 255 character limitation. [BNWF-11309]
- The upper limit for Max Content Length and Max Value Length has been increased for profiles: [BNWF-1602]
    - Max Content Length is now configurable up to 1GB for URL profiles
    - Max Value Length is now configurable up to 1GB for Parameter profiles.
    - In rare cases profiling engine was adding duplicate parameter profiles without considering the case and length of the parameter's name. This issue has been fixed. [BNWF-10521]
    - Apply Fix option is now available for unknown content types in POST body in added URL profiles. [BNWF-10256]
    - It is now possible to import URL profiles having parameter profile names more than 64 characters. [BNWF-9221]

Request Limits

- Request limits can now be set to a discrete length: [BNWF-10872]
    - Max Request Length – increased to 512k
    - Max Request Line Length – increased to 128k
    - Max URL Length – Increased to 16k
    - Max header length is increased to 64k. [BNWF- 9255]
    - Issues with multiple simultaneous large file (1.5 GB or larger) uploads resolved. [BNWF-8431]
    - In rare cases Keep Alive headers were triggering false positives when the value is not a numeric. This issue is fixed now. [BNWF-12215]
    - Strict patterns added to help prevent SQL injection, OS command, Cross Site Scripting and Remote File Inclusion based attacks. [BNWF-4486]

XML Validations

- Error handling added for malformed WSDL files. [BNWF-11229]

Allow / Deny Rules

- A configuration rollback no longer occurs when two URL ACL deny rules have similar URL matches which differ in case. [BNWF-10636]

Access Control

- The Barracuda Web Application Firewall now does not perform anonymous bind request to the LDAP server when authenticating the user. [BNWF-12081]
- SiteMinder response attributes are now sent along with the initial request to protected resources. [BNWF-12591]
- When creating an authorization rule, the upper limit for the Allowed Users field has been

extended to 45 characters. [BNWF-12045]
- Logs of the Access Control Module are now integrated into the System logs. [BNWF-10147]
- Users are now authenticated even when LDAP bind password is reconfigured in the LDAP configuration for external authentication of admin access control users. [BNWF-8317]
- Local RBA users are now required to enter a confirm password when adding or editing Local Administrators. [BNWF-7331]

Networking

- Back-end servers can now reach the internet even when both SNAT and Stateful Network Firewall are enabled. [BNWF-10458]
- Independent default gateways can now be configured for WAN, LAN and MGMT interfaces. [BNWF-4868]
- After upgrade, servers on the LAN side can now reach the internet without manually disabling and re-enabling SNAT. [BNWF-4965]
- Default gateways can now be configured per VLAN. [BNWF-7181]
- Independent network settings can now be configured for each Vsite. [BNWF-6354]

System

- Chunked encoded responses from the server without the terminating "/r/n" at the end are now processed by the Barracuda Web Application Firewall. [BNWF-3050]
- Persistence Idle Timeout for client IP persistence is increased to 86400 seconds. [BNWF-10125]
- Huge welcome banners are now supported for FTP services. [BNWF-10968]
- Client Impersonation feature now works in one-arm proxy deployment. [BNWF-6721]
- The session timeouts can now be configured larger than 180 seconds. [BNWF-4660]
- POST requests are now handled correctly when Content-Type contains "Charset=". [BNWF-10224]
- SSL renegotiation is now honored when initiated from the back-end server. [BNWF-8239]
- The rare case in which huge FTP downloads were terminated, no longer occurs. [BNWF-3289]
- URL encoded POST- Requests with parameter values greater than 1M in URL encoded POST are now allowed. [BNWF-10107]
- In rare circumstances malformed HTTP requests caused latencies. This issue is now fixed. [BNWF-5033]
- The configured port range for FTP Passive mode is now correctly utilized by the clients. [BNWF-7957]
- Packet captures taken from the Troubleshooting page now have .pcap extension without any integer appended (e.g., pcap0). [BNWF-7655]
- LAN and MGMT interfaces can now be configured from the console. [BNWF-9039]
- Increased STM stability under large values of null parameters.
- Uploading a PFX file that does not have a password is allowed. [BNWF-7355]
- Issue regarding rendering energize update page has been resolved. [BNWF-11160]

- Connection pool was getting timed out after 180 seconds in spite of configured value being higher. This issue is fixed now. [BNWF-7024]
- Administrators can now configure From Address for the email notification alerts sent by the Barracuda Web Application Firewall. [BNWF-13177]
- SNMP's default community string is changed to "cudaSNMP". [BNWF-13017]

Management

Backup

- Configuration can now be backed up to SMB shares in Windows 2008 R2. [BNWF-10084]
- In rare circumstances generating a backup file resulted in a file of zero bytes being created. This issue has been fixed. [BNWF-11637]
- The process of generating a problem report can be customized to include specific components (e.g., configuration or backup). [BNWF-11664]

SNMP

- In certain cases SNMP traps were not generated when back-end server failure was detected. This issue has been fixed. [BNWF-12102]
- The SNMP monitoring feature has been enhanced to support monitoring of concurrent SSL Connections in real time. [BNWF-5512]
- All SNMP metrics supported on the NC-gateway product are now supported on the Barracuda Web Application Firewall. [BNWF-9942]
- By default SNMP will not be listening on all interfaces, but only on the system IP.

Migration

- It is now possible to change the web firewall policy of a service belonging to a Vsite, when migrating from NC-Gateway. [BNWF-9852]

User Interface

Security Policies

- Changing the configuration of Security Policy options no longer results in the UI navigating incorrectly.
- Adding exception patterns under Security Policies > URL Protection no longer results in the blocked attack types check boxes getting unchecked. This issue has been fixed. [BNWF-11827]
- Changing the Global URL ACL rule in a custom Security Policy no longer results in a configuration rollback. [BNWF-4216]

- Bulk edit is now available for the Cookie Exempted parameter on Security Policies > Cookie Security page. [BNWF-10504]
- Editing values of the Data Theft Protection parameters for the policies other than "default" and saving resulted in context switching back to default policy. This issue has been fixed. [BNWF-10635]
- NIC advanced configuration UI is also enhanced to show operational and configured autoneg status. [BNWF-13039]

Services

- The rare circumstance where a service creation operation resulted in the error message "Duplicate value not allowed for Sequence Number, Sequence Number", no longer exists. [BNWF-12593]
- Trusted certificates can now bind to a real server in order to validate the back-end SSL communication. [BNWF-4963]
- Comments window is now available for various objects on the Basic > Services page. [BNWF-10724]
- Bulk edit is now available for services and servers. [BNWF-10836]

IP Configuration

- Form values entered are retained after an invalid submit on the BASIC > IP Configuration page. [BNWF-5327]

Energize Update

- UI now shows the date for the Currently Installed Version of virus definitions. [BNWF-7692]

Logging and Reporting

Logging

- Additional error handling added to the logging module. [BNWF-10897]
- Exporting logs to CSV format honors existing query filters. [BNWF-10996]
- All logs capture Module ID of the Module where the log was generated. [BNWF-7271]
- In Access logs, the server IP address was incorrectly recorded as 0.0.0.0 when the response status code is a 404. This issue is fixed now. [BNWF-8323]
- In Audit Logs, configuration changes made by the admin are now always captured in the Audit logs. [BNWF-11220]
- In some cases SQL injection attacks were not getting logged. This issue has been fixed. [BNWF-11787]
- In System Logs, system hostname / unit name can now be added to custom syslog format. [BNWF-6689]

- Policy Wizard Apply Fix to an existing URL profile is improved. [BNWF-10256]
- Attack definition updates no longer automatically restart STM, an alert message is displayed on the Basic > Status page indicating new definition is synchronized and to apply the definitions the administrator needs to reboot the system. [BNWF-13012]

Export Logs using Syslog

- Syslog can now be transported using the following connections/features:
    - TCP connection. [BNWF-1456]
    - SSL enabled TCP connection. [BNWF-180]
    - SSL enabled TCP connection with SSL Client Authentication. [BNWF-2137]
    - Additional flexibility added to export log format.

Reports

- Certificate Status Report on the BASIC > Reports page displays issue and expiry dates of certificates. [BNWF-9787]
- Issue while generating HTML reports to be emailed to administrators has been fixed. [BNWF-8882]