Release Notes Version 10.0.1

https://campus.barracuda.com/doc/90444925/

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 resolve 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]

- With the OpenSSL1.1.0, certificates signed with MD5 are no longer supported. Please replace such certificates with SHA1/SHA256 signed certificates before upgrading to 10.0.x. If an upgrade is done without replacing these certificates, services using them will go down and rollbacks will occur. [BNWF-31980]
- Attackdef 1.165 is shipped with this firmware. It has changes relevant to the firmware's interoperability with the Barracuda Block Listed IP database. [BNWF-32541]

Fixes and Enhancements in 10.0.1

High Availability

- Fix: An issue with the config sync process getting stuck during logging, has been fixed. [BNWF-32728]

Logging and Reporting

- Enhancement: "%rrf" is the new macro added to export the Risk Score Reason to syslog servers. [BNWF-32579]

Management

- Enhancement: It is now possible to create templates containing URL and Parameter Profile Optimizers. [BNWF-32624]
- Fix: An issue with the Barracuda CloudGen Firewall integration, where deletion of IP's from a connected CGF failed, has been fixed. [BNWF-32255]
- Fix: An issue with the creation of a new security policy based on an older custom security policy that was created in 9.2.1 or earlier has been fixed now. [BNWF-32047]
- Fix: An issue where applying templates containing Client Certificate authentication with CRL and Allow/Deny configuration failed has now been fixed. [BNWF-31821]
- Fix: An issue where creating server hostnames in camelCase was not allowed, has been fixed. [BNWF-32840]

REST APIv3

- Enhancement: Custom IP Blocklist can now be uploaded using REST APIv3.1. [BNWF-30079]
- Fix: Support for REST API v3.1 for configuring 'Secure Administration' for the Barracuda WAF has been added. [BNWF-31916]

Role-Based Administration

- Fix: An issue where editing administrator roles on a clustered device do not sync to the other devices in the cluster, has been fixed. [BNWF-32175]
- Fix: The Server Group for allowed services was automatically set to the "checked" state in the Admin Access Control settings. This has been fixed. [BNWF-31857]
- Fix: Editing a user-role and adding "READ ALL" permissions to an object will now retain the previously set WRITE permissions for that object as-is unless they are explicitly edited. [BNWF-32092]
  Fix: An issue in the ADVANCED > Admin Access Control > Edit Administrator Role page where the service group of allowed services which is default to 'checked' state, has been fixed. [BNWF-31857]

Security-Advanced Bot Protection

- Feature: Integrated the Infisecure Bot Protection engine with the Barracuda Advanced Bot Protection engine. For more information on the Infisecure acquisition: http://ow.ly/qvAo50vwJ3C [BNWF-32656]
- Feature: Detection of WDK usage if client traffic is generated using these tools. This is part of

the Advanced Bot Protection capability and can detect web automation including headless browsers. [BNWF-32655]
- Feature: A Client Profile is now created for all incoming clients to track their history on an application. This feature is available as a part of the Advanced Bot Protection subscription and is calculated based on client actions using the ABP Cloud. [BNWF-32106]
- Enhancement: All incoming clients are assigned a fingerprint by default even if JS is disabled. This feature requires an Advanced Bot Protection subscription. [BNWF-32413]

Security

- Feature: DTP now works for application/json content [BNWF-30596]
- Enhancement: Support for new MIME type "application/x-dosexec" in the Barracuda Advanced Threat Detection has been added. [BNWF-32130]
- Enhancement: Content-type "ajax/help" is now inspected by the XML Firewall and has been added as part of the Known Content Types. [BNWF-32053]
- Fix: Stricter header checks have been implemented to prevent possible evasions used in HTTP Smuggling attacks. [BNWF-32921]
- Fix: All vulnerabilities found in the HTTP2 path have been addressed. [BNWF-32660]
- Fix: The Barracuda WAF product line has been fixed to address the following vulnerabilities in HTTP/2: CVE-2019-9512, CVE-2019-9513, CVE-2019-9514, CVE-2019-9515, CVE-2019-9516, CVE-2019-9517, CVE-2019-9518, CVE-2019-9511. [BNWF-32656]
- Fix: IP addresses classified as "Fake Bots" are now enforced on a Service level instead of a global level. [BNWF-32261]
- Fix: An issue in the IP reputation-policy specifically with countries belonging to the EURASIA region has been fixed. [BNWF-32247].
- Fix: An issue with the "Extended Match" for Country Code with a single value, has been fixed. [BNWF-31892]

System

- Fix: An issue where CPU spikes were observed due to cron job sequencing has been addressed. [BNWF-32894]
- Fix: An issue that in which all the logs from the system showed incorrect system timezone on VM instances, has been fixed. [BNWF-32869]
- Fix: An issue where the LDAP bin password could be leaked has been fixed. Thanks to Steven Campbell from Rapid7 for reporting this issue. [R7-2019-39] [BNSEC-8552, BNWF-32834]
- Fix: A memory leak observed in the HTTP2 module, has been fixed. [BNWF-31815]
- Fix: An issue with secure administration where HTTP requests to the admin UI were not automatically redirected to HTTPS has been fixed. This issue occurred when "HTTPS Only" was enabled and a reboot occurred. [BNWF-31756]
- Fix: A rare issue where the configuration updates were not working after firmware upgrade has been fixed. [BNWF-31190]

- Fix: An issue with normalization where non-ASCII characters triggered false positives has been addressed. [BNWF-31011]
- Fix: A memory leak in the data-path process that happened when client authentication is enabled at the content-rule level, has been fixed now. [BNWF-28833]
- Fix: An issue where the SNMP Agent is stuck at 90% due to a large number of backend servers is resolved. [BNWF-24444]
- Fix: A rare datapath outage when Advanced Bot protection features are enabled, has been addressed. [BNWF-32889]
- Fix: Added log rotation to the cluster management log files. [BNWF-32710]
- Fix: An issue that resulted in a subsystem crash due to saml misconfiguration for which the subsystem (shibd) had to be restarted after an outage, has been fixed. [BNWF-32283]

User Interface

- Enhancement: Locked-out client fingerprints can now be viewed and cleared from the UI. [BNWF-30715]
- Enhancement: Adding servers using FQDN/Hostname no longer requires turning on Advanced Settings. [BNWF-22927]
- Fix: An issue in URL Profile templates in which the "Allowed Methods" parameter values were not being honored, has been fixed. [BNWF-32845]
- Fix: An issue where the Access Logs and Web Firewall Logs did not show up on the GUI, has been fixed. The logs were being exported normally to any configured export log servers. [BNWF-32807]
- Fix: An issue with the Parameter Profile page not getting refreshed, has been fixed. [BNWF-32761]
- Fix: An issue with the "Firmware Updates" page not showing up if the Patch System database is unavailable, has been fixed. [BNWF-32708]
- Fix: Rendering time improved on Websites > Allow Deny Rules page. [BNWF-32293]
- Fix: The "Secure Browsing" page has been moved from the Websites tab to the Advanced tab. This feature will be deprecated in a future release. [BNWF-30120]
- Fix: An issue where the UI displayed an error when an IP Lookup did not find matches in the IP reputation database, has been fixed. [BNWF-30006]
- Fix: Exception profiling page load performance has been improved and "Temporarily Unavailable" errors are fixed. [BNWF-27219]