Release Notes Version 5.3.0.002

https://campus.barracuda.com/doc/44436063/

Before installing any firmware version, back up 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 update unless otherwise instructed by Barracuda Technical Support. Depending on your current firmware version and other system factors, updating can take up to 10 minutes. If the process takes longer, contact Barracuda Technical Support for further assistance.

- By default, SSL 3.0 is enabled due to the wide use of the protocol. Since SSL 3.0 is vulnerable to the POODLE (CVE-2014-3566) attack, Barracuda recommends that you disable SSL 3.0 for all SSL services configured on the Barracuda Load Balancer ADC.
- Barracuda also recommends that you use the server IP address when configuring a server, as a server configured with the hostname might not resolve to the proper server IP address in some cases.

Features

- SSL hardware support is now available.

Fixes

- Certificates with an expiration date after 2037 had issues when being uploaded to the Barracuda Load Balancer ADC. [BNADC-3026]
- Logs counted on the **BASIC > Status** page consumed greater than expected CPU time, resulting in the system hanging or crashing. [BNADC-3061]
- The failover/failback time in the High Availability environment has been enhanced to handle large configurations. [BNADC-3534]
- It is now possible to change an HTTP/HTTPS service to an INSTANT SSL service with content rules configured in it. [BNADC-3795]
- The server monitoring process now retains the previous state of servers (Up or Down) if it is unable to perform the test. [BNADC-4269]
- Services are now created with the enabled status only. [BNADC-4480]
- The Cookie Path and Client IP Header fields no longer display example values and X-Forwarded-For respectively, since these values could be confused with the default values. These fields are now kept blank. [BNADC-5270]
- An issue that automatically enabled cookie security when URL redirect was configured on the Barracuda Load Balancer 340 and 440 has been fixed now. [BNADC-5284]
- Enabling/Disabling the TCP time stamp through the web interface is now reflected in the back-end. [BNADC-5370]
- The Enable SSL Compatibility Mode feature was added to the server configuration to enable or

disable cipher suits for the server. BNADC-5379

- Disabling the server on the Barracuda Load Balancer ADC web interface was not applied to the back-end. A recovery mechanism added to the server monitoring process resolves this issue. [BNADC-5390]
- Monitor Group is now supported for Global Server Load Balancing (GSLB) services. [BNADC-5402]
- There is no longer a memory leak issue when changing the configuration. [BNADC-5404]
- The hostname no longer resolves to a new server IP address, setting the server Status to Down in the web interface. [BNADC-5424]
- The Barracuda Load Balancer ADC now accepts larger sized certificates associated with the SNI domain. [BNADC-5607]
- For High Availability, failover/failback ALERTS and TRAPS are now sent even if the system assumes the same state (Active) after recovering. [BNADC-5655]
- An issue with the Simple HTTP/HTTPS server monitor test is now fixed. [BNADC-5675]
- An issue that prevented the deletion of a renamed service is now fixed. [BNADC-5683]
- An issue with the cookie update interval is now fixed. [BNADC-5691]
- The Active-Active issue for High Availability is fixed. [BNADC-5702]
- A faulty internal process no longer causes the system to use 99% of the CPU. [BNADC-5723]
- During the migration process from Barracuda Load Balancer Version 4.2.3.004 to Barracuda Load Balancer ADC Version 5.x, the persistence cookie parameters are now transferred properly. [BNADC-5742]
- Users are now being redirected to the page specified in Auth Password Expired URL on the **ACCESS CONTROL > Authentication** page when the password expires. [BNADC-5764]