Release Notes Version 5.2.0.004

https://campus.barracuda.com/doc/42044491/

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 Networks 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 Networks 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 Networks recommends that you disable SSL 3.0 for all SSL services configured on the Barracuda Load Balancer ADC.
- Barracuda Networks also recommends that you use the server IP address when configuring a server, as the server configured with the hostname might not resolve to the proper server IP address in some cases.

Features

- Server Name Indication (SNI) extension can be enabled in the TLS header for backend SSL if server requires. [BNADC-2761]
- Supports Mime Types to validate uploaded file extensions. [BNADC-2083]
- Supports Certificate Revocation List (CRL) validation for client certificates. [BNADC-3039]
- Supports Online Certificate Status Protocol (OCSP) validation for client certificates. [BNADC-3301]
- Supports Intel QuickAssist Technology for SSL acceleration in the Barracuda Load Balancer ADC 840 and above. [BNADC-3353]
- For a Layer-7 HTTP/HTTPS service, if all servers are down, then the custom error response page to be displayed to the client can be configured by the administrator. [BNADC-3664]
- You can now select if you want to retain the configuration or clear the configuration from the system when the unit is being removed from the cluster. [BNADC-3375]
- Certificates and Certificate Signing Request (CSR) now use SHA-256 digest for signing. [BNADC-4573]
- SSL and TLS negotiated versions are now displayed for SSL connections in the **BASIC > Access Logs** page. [BNADC-4806], [BNADC-4909]
- The Barracuda Load Balancer ADC supports Perfect Forward Secrecy with ECDSA and RSA certificates and associated ciphers. The key exchange mechanism supported is Elliptic Curve DHE. [BNADC-3041]

Enhancements

- The Redirect Rule feature is now supported in the Barracuda Load Balancer ADC 340 and 440. [BNADC-4604]

- You can now configure the WAN IP address, network mask, and gateway when restoring the Barracuda Load Balancer 4.x backup file to the Barracuda Load Balancer ADC. [BNADC-4436]

Fixes

- When an SSL service was changed to non-SSL service, the certificate associated with the server was not getting deleted from the backend. Hence, the administrator was unable to delete the certificate on the **BASIC > Certificates** page. This issue has been fixed now. [BNADC-3042]
- The Location Definition is now displayed for the Barracuda Load Balancer ADC 340. [BNADC-3773]
- There is now a UI option to enable and disable TCP timestamps. [BNADC-3960]
- The RC4-MD5 cipher is now listed in Available Ciphers. [BNADC-4192]
- A predefined policy "ibm_domino" is now available for the IBM Domino server on the **SECURITY > Security Policies** page. [BNADC-4206]
- The test delay setting configured by the admin for monitoring the server health was not working as expected and instead initiated probes after the default interval of 10 seconds. This issue has been fixed. [BNADC-4005]
- An issue where a certificate was being associated with the server automatically has been fixed. [BNADC-3931]
- A possible race-condition with cookie persistence, which caused empty cookie or broken persistency has been fixed. [BNLB-4909]
- The AAA feature is now available in the Barracuda Load Balancer ADC 340 and 440. [BNADC-4535]
- The configured values of Connection Pooling timeout parameters are now set properly when the L7 services are migrated from the Barracuda Load Balancer to the Barracuda Load Balancer ADC. [BNADC-4536]
- On rare occasions, the persistency module was introducing cookies with blank values which resulted in the persistency module not working for services. This issue has been fixed. [BNADC-4433]
- SSLv3 is disabled for web interface access to mitigate POODLE attack (CVE-2014-3566). [BNADC-4806]
- An issue which resulted in the administrator getting a web page error upon restoring a backup file has been fixed. [BNADC-4562]
- During the migration process from the Barracuda Load Balancer to the Barracuda Load Balancer ADC, the SNI domain list configuration was not getting migrated successfully causing a configuration roll back. This issue has been fixed. [BNADC-4812]
- The logs are not generated for the service and the associated content rules when **Enable Access Logs** is set to **No**. [BNADC-4868]
- Fixed double free with L7 UDP services. [BNADC-4849]
- When SSL services were modified after upgrading the firmware from 5.1.1 to 5.2, the selected cipher list was not displayed. This issue has been addressed. [BNADC-4891]