Release Notes Version 11.0 Cloud

https://campus.barracuda.com/doc/96020616/

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 that 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 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 1.172 is shipped with this firmware. It has changes relevant to the firmware's interoperability with the Barracuda Block Listed IP database. [BNWF-32541]

- On instances deployed on Microsoft Azure, if you are upgrading the Barracuda CloudGen WAF from versions earlier than v10.1.1, you might encounter issues with the Azure Managed Identities and Service Principal Names configured under **BASIC > Azure Configuration**. To resolve this issue, Barracuda Networks recommends you to use the latest CloudGen WAF image (i.e, 10.1.1) available on the Azure Marketplace or contact Barracuda Networks Technical Support for further assistance [BNWF-47993].

Fixes and Enhancements in 11.0 Cloud

- **Enhancement**: Basic Nutanix tools are included for deployment on the Acropolis Hypervisor.
- **Enhancement**: The OMS Package version has been upgraded to the latest version. [BNWF-49339]
- **Enhancement**: You can now create and upload certificates for SAML Single Sign-On on the **ADVANCED > Admin Access Control** page. [BNWF-49771]
- **Enhancement**: The number of trusted CA certificates that can be associated with a service for verifying client certificates has been increased to 256. [BNWF-49550]

- **Enhancement**: Let's Encrypt certificate creation and renewal is now validated using a Global ACL instead of URL ACLs. [BNWF-48257]
- **Fix**: Reboot or shutdown no longer takes a long time in a fully configured VM instance. [BNWF-49892]
- **Fix**: An issue that failed to associate Let's Encrypt renewed certificates to a service with the uppercase name has been addressed. [BNWF-48524]
- **Fix**: An issue where the logs from the WAF stopped reaching the AWS CloudWatch service has been addressed. [BNWF-47203]