Release Notes Version 12.1

https://campus.barracuda.com/doc/98214662/

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.

Fixes and Enhancements in 12.1

Logs and Reports

Features and Enhancements:

- All log pages (Web Firewall Logs, Access Logs, Audit Logs, Network Firewall Logs and System Logs) now provide the following:
  - **Import/Export Filters** – Ability to import or export predefined log filters into or from different Barracuda WAF units. [BNWF-49559]
  - **Filter on Load** – Ability to set a saved filter as a default filter that loads every time you visit a log page. [BNWF-49740]
  - “Saved” and “Custom” filter options. [BNWF-52532]
  - Factory-shipped log filters. [BNWF-49732]
- URL profile and ACL summary reports now display learned URLs depending on the user's preference. [BNWF-47501]

Fixes:

- Fix: Client Type filter is now available in the Audit Logs filter option. [BNWF-29496]
- Fix: Web Firewall Logs now report the correct attack name and attack type in the logs. [BNWF-24155]

Advanced Bot Protection

Features and Enhancements:

- **Bot Identifier** – Ability to add a bot to the Allow list either from the bot dictionary provided by the Barracuda Advanced Threat Intelligence (ATI) service or a custom bot signature.
- **hCaptcha** – A new CAPTCHA challenge type based on hCAPTCHA has been introduced. [BNWF-46920]
- **Bot Library integration for allowed bots** – Ability to create new allow bots from the predefined list of bots that are provided by ATI services. [BNWF-52528]
- Ability to add custom bots based on ASNs as Identifier. [BNWF-52527]

Fixes:

- Fix: An issue in the Advanced Bot Protection module that resulted in data-path outage during a credential-stuffing check has been fixed. [BNWF-52765]
- Fix: The "ABP_ATI" module has been added to the Module list at **ADVANCED > System Logs**. [BNWF-51159]
- Fix: An issue resulting in intermittent disruption of traffic due to ABP license validity checks has been fixed. [BNWF-52711]

Security

Feature and Enhancements:

- It is now possible to allow traffic from ASNs specified in the IP Reputation policy. [BNWF-52542]
- CAPTCHA policy does not enforce the CAPTCHA challenge if the service is configured in Passive mode. [BNWF-52713]
- **Extended Match Enhancement** – The element type “SSL-Version” in extended-match expressions can be configured to match the value of TLSv1.3. [BNWF-32970]
- **Account Take Over Protection** – Login failures for servers responding with 200 OK response code and error message in the response page can now be detected based on the response data. The 'Auth Response Identifier' in the Brute Force policy should be configured to enable this capability. [BNWF-53020]

Fixes:

- Fix: An issue where web scraping policies were getting created from the DDoS service without a valid license is now fixed. [BNWF-52887]
- Fix: An issue in the reCAPTCHA service endpoint that resulted in a continuous loop in the challenge mechanism has been resolved. [BNWF-52710]

System

Features and Enhancements:

- OpenSSL has now been upgraded to version 1.1.1q. [BNWF-52610]
- Password change for the Administrator login is now mandatory after the firmware upgrade if the default password is used for login. It also changes the console password if the default password is used. [BNWF-33278]

Fixes:

- Fix: The 'Security Definition Updates' section has been removed from the **ADVANCED > Energize Updates** page because it is being deprecated. [BNWF-52966]
- Fix: An issue that resulted in outages due to the tarpit module has now been fixed. [BNWF-52712]
- Fix: Subject language in the alert notification now changes as per the "Default Language and Encoding" set on the **BASIC > Administration** page. [BNWF-50701]

Traffic Management

Features and Enhancements:

- **Time-Based Rules** – Ability to create time-based policies to apply the rules on the service traffic for a specific period. You can define the start and end time for the rules (content rules, URL ADRs), and they are effective only during the specified time range. [BNWF-46837]
- **Redirect Service** – Virtual services with the service type “Redirect Service” can be set to redirect traffic permanently (based on response code 301) or temporarily (based on response code 302). [BNWF-46570]

Fixes:

- Fix: An issue in the data-path that resulted in modification of the response page when brute force pattern matching is used has now been fixed. [BNWF-52844]

API Security

Fixes:

- Fix: Updated the API endpoints used by the WAF to communicate with the CloudGen Firewall(s). [BNWF-52413]
- Fix: Blocked attack types are now reflected in the URL profile as part of the API import functionality. [BNWF-52876]

Cloud

- Fix: An issue where the WAF's application IP was being changed back to System IP on the peer unit in the Azure Multi-IP configuration scenario has been fixed. [BNWF-53038]