Barracuda WAF and GDPR Compliance

https://campus.barracuda.com/doc/84312323/

Overview

General Data Protection Regulation (GDPR) was adopted by the European Union (EU) and took effect on May 25, 2018.

GDPR is designed to give more control to individuals over their personal information and data. It is intended to put guidelines and regulations on how the data is processed, used, stored or exchanged outside the EU and EEA areas.

While deploying the Barracuda Web Application Firewalls in GDPR compliant environments, administrators should ensure that capabilities related to encryption of logs, reports and backup are configured accordingly.

Understand the Terminology

Customer – a person who interacts with an application that is deployed in a GDPR compliant environment and is protected by the Barracuda Web Application Firewall.

Administrator – individuals who manage Barracuda Web Application Firewalls. These individuals may also be responsible for other functions relating to security of personal data such as access, deletion, and modification of data. Administrators may also manage the permissions of users, groups, and user accounts.

Organization – licensed customers who own user data and are responsible for compliance. These organizations provide mechanisms and relevant privacy notices to the individuals who engage with the organizations. The notices must describe how a user's information is collected and used, and if any consents are required. If individuals want to know about or delete their stored information, the organizations must respond to such requests.

Why GDPR is important

GDPR ensures that the protection of personal data remains a fundamental right for EU citizens. It aims at modernizing outdated privacy laws and has the potential to impact any business that collects

data in or from Europe.

How Barracuda WAF supports GDPR

The Barracuda Web Application Firewall is compliant with these rules. It provides administrators with services and resources to help them comply with GDPR requirements that may be applicable to their operations, such as encryption, backup and log export. The Barracuda Web Application Firewall is committed to protecting the customer's privacy and providing the customers with clear and concise details about the data that is collected and used.

The **ADVANCED > System Configuration > GDPR Compliance** section of the web interface allows you to enable or disable the encryption of all logs and problem reports by using an encryption key. You can create your own encryption key or use the default key `Barracuda Networks is your new best friend` provided by Barracuda Networks.

> When creating your own encryption key, ensure that you meet the following requirements:
>
> - The length of the key should not be less than 10 characters
> - The length of the key should not exceed 128 characters

Enable Log Encryption - By default, this is set to *No.* You can enable log encryption by setting the parameter to *Yes.* A default key `Barracuda Networks is your new best friend` is provided by Barracuda Networks, and can be used for encryption.

> It is *strongly* recommended that you provide your own key for encryption.

Key to be used for Encryption - The key used for encrypting and decrypting the log file/problem report. By default, `Barracuda Networks is your new best friend` key is selected.

Decrypting a Log File/Problem Report

To decrypt a log file/problem report, use OpenSSL on any Linux or Windows host machine:

1. Download the relevant log file/problem report.
2. Type `gpg < filename >` to start the decryption.
3. Specify the encryption key that you created. The log file/problem report is now decrypted successfully.