Barracuda WAF-as-a-Service

Data Protection and Security

TABLE OF CONTENTS

Overview

This document walks through security measures in place to protect customer data accessed by Barracuda Networks. This document includes a description of the facilities that process data by Barracuda WAF-as-a-Service and descriptions of operational and organizational controls enforced by Barracuda Networks.

1. Product Security

1.1 Barracuda WAF-as-a-Service

Barracuda Networks offers WAF-as-a-Service which delivers protection to customer web apps, provides comprehensive protection from all OWASP recognized security risks, DDoS attacks, and even the most advanced zero-day threats. For more advanced users, Barracuda WAF-as-a-Service offers a level of control traditionally reserved only for on-premises and public cloud solutions.

2. Data Center Standards and Protection

2.1 Storage Facility Standards

Barracuda Networks leases space in a number of Tier 3 & 4 datacenters worldwide. Each Barracuda Networks datacenter is equipped with:

- Controlled access systems requiring key-card authentication.
- Video-monitored access points
- Intrusion alarms
- Locking cabinets
- Climate Control systems
- Waterless fire suppressant systems
- Redundant power (generator backup, UPS, no single point of failure)
- Redundant Internet connectivity

2.2 Data Access, Transmission and Storage

Only authorized Barracuda employees from the WAF-as-a-Service operations, engineering and support teams have access to the backend systems storing the data, used only for administering, troubleshooting and maintaining the system. Employees must enter their corporate credentials and authenticate using SSH keys before accessing any data.

All Barracuda communications/data is encrypted transit using industry-standard TLS encryption. Customer application traffic can be either unencrypted or encrypted with the SSL or TLS protocol(s) chosen by customers in their application configuration. Barracuda highly recommends customers encrypt their application traffic using a modern TLS protocol.

All customer data is encrypted at rest using AES-256 encryption.

2.3 Locations

Barracuda maintains a network of datacenters by geographic location around the globe and requires that each meet defined security requirements. The cloud infrastructure for Barracuda WAF-as-a-Service is deployed in the following geographical regions. Customer data is stored in the respective region where the customer is located. Any transfer of customer data outside the European Union will be done in compliance with the GDPR and applicable local privacy laws. Barracuda's Standard Contractual Clauses are located within our DPA at the following address: https://www.barracuda.com/company/legal/trust-center

Americas - Colocation

- US East - Virginia
- US West - California
- US Central - Illinois

EU - Colocation

- EU West – Netherlands

3. Operations and Organizational Controls

Barracuda Networks employees are expected to be competent, thorough, helpful, and courteous stewards of customer email that is stored on Barracuda Networks products and in Barracuda Networks datacenters. Barracuda Networks has established a number of measures to ensure that customers and their data are treated properly.

3.1 New Hires and Orientation

All new employees are required to accept and acknowledge in writing Barracuda Networks' policies for non-disclosure and protection of Barracuda and third-party confidential information, including acceptable use of confidential information. In the course of assisting customers with their technology solutions, Barracuda support technicians understand that they may come into contact with customer communications and/or customer data and they are not to view the contents of that data without explicit permission from the customer. Barracuda Networks employees are not to disclose the contents of that customer data to a third party under any circumstances.

New technical support employees are provided a job description and expectations when hired regarding maintaining the confidentiality and security of customer data.

3.2 Training

Technicians who support Barracuda WAF-as-a-Service are prepared in a variety of ways. New tier 1 technicians receive class time training with tier 2 technicians and the support management team. New support technicians also spend a period of time as understudies to an established technician for each product in which they intend to become certified.

All Barracuda Networks support technicians receive ongoing training in product-specific training sessions.

3.3 Oversight

Access to Barracuda WAF-as-a-Service servers is limited to approved Barracuda Networks personnel on an 'as needed' basis. The management team checks the status of support personnel through periodic ticket review and call monitoring. Each tier 1 technician is attended by and reports to a tier 2 technician. Each tier 2 is responsible for no more than four tier 1 technicians.

Support for Barracuda WAF-as-a-Service is provided out of. USA and EU support teams. Support calls from customers in the United States are generally handled by technicians in the United States. Support calls from customers outside the United States could be routed to any of these facilities.

When an employee or contractor leaves Barracuda, a formal process is in place to immediately revoke physical and network access to Barracuda Networks facilities and resources.