Barracuda Content Shield

Data Protection and Security

TABLE OF CONTENTS

Overview

Barracuda Content Shield provides cloud-based protection against web-based threats. Powered by Barracuda's extensive threat intelligence network, Barracuda Content Shield delivers powerful content filtering and protects users from malicious sites and inappropriate content, helping to keep your business safer and employees more productive.

1. Product Security

1.1 Barracuda Content Shield

The Barracuda Content Shield service uses publicly signed and trusted certificate to prevent malicious interference with SSL traffic between the Barracuda Content Shield Suite (endpoint machines) and the service. During the handshake that takes place when an SSL/TLS 1.2 connection is established, the client (endpoint) can authenticate the server it is talking to by validating that the server certificate was issued by a Certificate Authority that the client trusts.

2. Data Transmission and Storage

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 Storage

Log data is transmitted from client (endpoint) via AES 128-bit encryption. Barracuda Content Shield is enabled on AWS Elasticsearch via SSL connection. Data at rest is stored in an AES 256-bit encrypted format.

2.3 Data 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 Content Shield 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

US

- AWS Region - US East

EU

- AWS Region – EU Ireland

3. Operations and Organizational Controls

Barracuda Networks employees are expected to be competent, thorough, helpful, and courteous stewards of customer data 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 Content Shield 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 Content Shield servers is limited to approved Barracuda Networks personnel on an 'as needed' basis. 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 Content Shield is provided from all our support regions. 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.