Barracuda CloudGen Access

Data Protection and Security

TABLE OF CONTENTS

Overview

Barracuda CloudGen Access provides a modern approach to securing remote users to corporate resources and applications over traditional VPN. Confidently rollout remote access capabilities to your employees while ensuring compliant access for on premise and cloud applications. Barracuda CloudGen Access is deployed on Barracuda's cloud infrastructure and is delivered to customers in a Software-as-a Service (SaaS) model.

1. Product Security

1.1 Barracuda CloudGen Access

Barracuda CloudGen Access supports TLS protocol to encrypt data flow between the application and the proxy. Additionally, the customers manage the keys for the data in transit and we manage the keys for the data at rest.

Customers can configure user roles to manage access privileges to CloudGen Access. We support admin roles, SSO and authentication via username and password.

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

Barracuda CloudGen Access utilizes AWS PostgreSQL and Elastic Search for storing and streaming relational data (i.e., configurations, user directories and access logs). All cloud storage data at rest is encrypted via AWS KMS keys.

2.3 Data Locations

The primary storage location for the Barracuda CloudGen Access is as set forth below: Customer data is stored in the respective region where the customer is located. Any transfer of customer data outside the regions will be done in compliance with the GDPR and applicable local privacy laws. Barracuda's Privacy Policy and Privacy Shield certification are located at: https://www.barracuda.com/company/legal/privacy.

- **US**: AWS Region - US East – 1

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 email without explicit permission from the customer. Barracuda Networks employees are not to disclose the contents of that customer email 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 email.

3.2 Training

Technicians who support Barracuda CloudGen Access 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 Email CloudGen Access 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 CloudGen Access 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.