Barracuda Appliance

Data Protection and Security

[1] https://campus.barracuda.com/product/campus/doc/46207817/barracuda-networks-sunset-policy/

TABLE OF CONTENTS

[1] https://campus.barracuda.com/product/campus/doc/46207817/barracuda-networks-sunset-policy/

Overview

This document describes Barracuda's security controls as they apply to physical and virtual appliances. Security controls of Barracuda hosted services are described separately on our Trust Center.

1. Product Security

1.1 Barracuda Physical and Virtual Appliance Security

Barracuda physical and virtual appliances are closed systems: Barracuda provides all updates to the operating system and applications required to ensure the security and functionality of the product.

To ensure security or our products, Barracuda:

1. Implements strict change control processes during the development process.
2. Monitors security feeds to identify vulnerabilities that could affect product components.
3. Performs authenticated host and application level security scans prior to each firmware version release.
4. Exposes our products to continuous external security testing via our bug bounty program.

Product security issues are typically resolved via updates to currently supported firmware versions [1]. Critical security issues are addressed, when possible, with targeted patches called Security Definitions. All customers with current support contacts are eligible to receive firmware updates and Security Definitions. However, to get security updates, customers must ensure their appliances are running a supported version. Customers in dark environments should contact support for guidance on applying firmware updates and security updates.

2. Access Control & Security Recommendations

2.1 Barracuda Physical and Virtual Appliance Access Controls

Technical support of Barracuda appliances can, at times, employ the Barracuda Support Tunnel service to allow an authorized technician to directly access the unit. Access to the device is only possible when the customer consents to that access by opening the Support Tunnel.

User access to the Support Tunnel service is limited to authorized support and engineering personnel. Regular access control audits are conducted to ensure that only authorized personnel are allowed to access the system. All activity performed on customer units is logged to a central logging system monitored by our Security Team. Logs of activity are maintained for 90 days.

2.2 Security Recommendations

Security appliances sit in a privileged position in customer networks. Care must be taken to prevent unauthorized access to the administration interface. Administrative credentials should be stored securely and rotated when users with access to them leave the company or change roles.

[1] https://campus.barracuda.com/product/campus/doc/46207817/barracuda-networks-sunset-policy/

Barracuda appliances ship with HTTP access to their management interfaces enabled. This should be considered a temporary solution while procuring and installing an official SSL certificate for the devices. Due to the requirements for generating such a certificate, Barracuda Networks cannot perform this step for customers. Once a certificate is installed, the appliance should be configured to only allow access to the management interface over HTTPS. See product documentation for details.

Our products also have product specific controls that support limiting access to the administrative interface. Consult the product documentation and consider implementing the option to increase the security of your device – especially if the user interface is exposed to the public internet.

3. Incident Response

3.1 Incident Response

For product security incidents which pose immediate threats to users – such as shellshock and other vulnerabilities that affect large portions of the internet - documented incident response procedures are provided to Barracuda employees. Incidents are recorded and communicated to Barracuda operations, IT, legal, and security personnel as noted in the incident response procedures. As necessary, incidents are escalated for resolution.

Continuous monitoring of incidents is performed to ensure measures are taken to ensure a resolution.

Barracuda does not provide incident response services for physical or virtual appliances hosted in customers' premises or public clouds.

[1] https://campus.barracuda.com/product/campus/doc/46207817/barracuda-networks-sunset-policy/