Barracuda
Your journey, secured.

PCI DSS Compliance

with Barracuda CloudGen Firewall

WHITE PAPER

NETWORK SECURITY

About Payment Card Industry Data Security Standard (PCI DSS) requirements

To combat identity theft and security breaches, major credit card companies collaborated to create the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. It applies to all entities involved in payment card processing—including merchants, processors, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder account data. The 12 PCI DSS requirements are organized into 6 subcategories that prevent credit card fraud through increased controls around data and its exposure to compromise. To be fully compliant, an organization must satisfy all 12 requirements.

Barracuda CloudGen Firewall can help your organization satisfy every specific requirement of PCI DSS compliance version 3.2.1 (released in May 2018) The bulk of this document maps specific PCI DSS requirements to specific features and capabilities of the Barracuda CloudGen Firewall. Requirements that are not listed specifically herein are not addressed by Barracuda CloudGen Firewall. However, all such cases, Barracuda business partners can provide services to help you meet these requirements.

About Barracuda CloudGen Firewall

Barracuda CloudGen Firewall helps you protect vital data in today's rapidly evolving networks. It makes it easy to address the complex vulnerabilities created by the explosion of mobile and BYOD devices, increased dependence on web-based applications, and remote network users. Barracuda Firewall Control Center gives you a powerful and intuitive centralized management portal to easily deploy, configure, update, and manage multiple units from a single location. It also provides comprehensive, real-time network visibility and reporting. Barracuda CloudGen Firewall helps you ensure PCI-DSS compliance across large numbers of users and multiple sites with minimal IT resources and personnel.

Executive summary

Barracuda CloudGen Firewall was designed to protect separate network segments with tailored security policies. There are two architectural options: Separate Barracuda CloudGen Firewall appliances or instances can be used as individual network segmentation gateways to protect each network segment. Or a single high-performance CloudGen Firewall unit can be used as a central network segmentation gateway that protects multiple network segments with separate security policies.

Our support for **virtual systems** means that the Barracuda CloudGen Firewall can also be used easily to implement network segments within a virtual environment.

Support for Amazon AWS, Microsoft Azure, and Google Cloud Platform enables customers to extend secure network segmentation policies and PCI DSS compliance to leading **public-cloud** providers.

Barracuda CloudGen Firewall can block threats according to policy. Depending on the severity of the threat, highly granular actions can be assigned on a per firewall rule base enabling the Barracuda CloudGen Firewall to allow, block, or log questionable traffic based on severity, location, user/group, type, and Layer 7 application detection.

As part of the Barracuda Energize Updates subscription, automatic signature updates are delivered on a weekly schedule (or on an emergency basis) to ensure that Barracuda CloudGen Firewall is constantly up to date. If the firewall unit is centrally managed, the pattern updates are conveniently distributed by Barracuda Firewall Control Center.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
1.1	Establish and implement firewall and router configuration standards that include the following:	**Barracuda CloudGen Firewall** is a full next-generation stateful firewall providing market-leading network security and data protection. Multiple firewalls can be managed through **Barracuda Firewall Control Center** allowing full centralized management. The Control Center's Firewall Audit Viewer aggregates traffic information from multiple firewalls in one central location. For auditing purposes, you can activate the Revision Control System (RCS) (to support requirement 1.1.1). The RCS records and reports on all configuration changes to your system. You can generate reports about specific configuration versions and administrator IP addresses, or search for information using multiple parameters. Barracuda CloudGen Firewall can be placed between the DMZ and the internal network, and can secure access via one or more internet connections (requirement 1.1.4). Role-based administration lets you create granular administrative policies to enforce sophisticated access controls (requirement 1.1.5). The built-in application control engine lets you grant or restrict access and/or prioritize bandwidth allocations for certain application or sub-applications. You can add custom application patterns to the rapidly growing built-in database, in order to manage in-house applications as well (requirement 1.1.6). In conjunction with RCS, this ensures consistent documentation of internet access, as well as bandwidth and application/sub-application use.
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	**Barracuda CloudGen Firewall** acts as a network segmentation gateway to police the border between trusted and untrusted networks. It supports rigorous security policies to allow only required traffic for specific protocols or applications (requirement 1.2.1). It can also be used as a secure perimeter firewall between wireless networks and data environments (requirement 1.2.3). Separate Barracuda CloudGen Firewall appliances can be used to protect each network segment. Or a single high performance CloudGen Firewall appliance can be used as a central network segmentation gateway that protects multiple network segments, with separate security policies. A single CloudGen Firewall appliance can easily manage hundreds of separate network segments.
1.3	Prohibit direct public access between the internet and any system component in the cardholder data environment.	**Barracuda CloudGen Firewall** can be easily configured to prevent direct access between the internet and system components in the cardholder network segment. It can implement and manage a network zone for a DMZ (requirement 1.3.1), ensure that inbound internet traffic can only access IP addresses in the DMZ (requirement 1.3.2), prevent direct connections (requirement 1.3.3), protect internal IP addresses (requirement 1.3.4), only allow specifically authorized outbound traffic (requirement 1.3.5), perform stateful inspection (requirement 1.3.6), segregate a network zone for cardholder data (requirement 1.3.7), and implement NAT as well as proxy services (requirement 1.3.8). The CloudGen Firewall gives you full control over what enters and leaves your network based on user, time of day, location, protocol, and application. High availability ensures continuity of service, and site-to-site VPN seamlessly integrates remote sites into a secure network architecture.
1.4	Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the internet…	**Barracuda Network Access Client** provides a powerful firewall for PCs that you can roll out and configure centrally via Barracuda CloudGen Firewall. Unsanctioned local changes to the personal firewall can be denied. The Barracuda Network Access Client can also ensure that only computers meeting centrally defined security and health standards can connect to the organization's network.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network...	**Barracuda CloudGen Firewall** and associated documentation encourages customers to change supplied defaults (usernames, passwords, and IP addresses) before deployment. In addition, the Setup Wizard enforces password change.
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry accepted system hardening standards...	**Barracuda CloudGen Firewall** can help you meet this requirement by ensuring that only specific protocols, services, or applications are allowed to access specific services or network segments. If they are not required, they are blocked by default.
2.3	Encrypt all non-console administrative access using strong cryptography.	Administrative access to **Barracuda CloudGen Firewall** is encrypted using SSL. Administration is done via a dedicated Windows executable.
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data.	The virtualized versions of **Barracuda CloudGen Firewall** (for VMware, Hyper-V, KVM, and XenServer) allow deployments in virtualized networks on a single platform. This is ideal for shared hosting providers, as they can segregate the data from different organizations, while using a single platform.

Protect Cardholder Data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: ...	**Barracuda CloudGen Firewall** manages secure site-to-site (and client-to-site) VPN tunnels, across public networks, to deliver secure and stable remote office or cloud connectivity. VPN tunnels can be secured using either IPSec or the Barracuda hybrid protocol (IPsec's ESP and enhanced key exchange). Supported encryption includes AES-128/256, 3DES, DES.
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	**Barracuda CloudGen Firewall**'s generic pattern matching provides DLP functionality and can be set up to include blocking non-encrypted PANs (credit card numbers).

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Barracuda's **Malware Protection** provides gateway-based protection against malware, viruses, spyware, and other unwanted programs inside SMTP/S, HTTP/S, POP3, and FTP traffic. The built-in **Web Filter** enables highly granular, real-time visibility into online activity, broken down by individual users and applications, letting you create and enforce effective internet content and access policies. It protects user productivity, blocks malware downloads and other web-based threats, enables compliance by blocking access to inappropriate websites and servers, and provides an additional layer of security alongside application control. Barracuda **Advanced Threat Protection** uses next-generation sandbox technology including full- system emulation to catch advanced persistent threats, zero-day malware, and all advanced malware designed specifically to evade detection. Advanced Threat Protection on Barracuda CloudGen Firewall ensures flexible and simple deployment into existing networks because no additional hardware is required. Resource-intensive sandboxing is offloaded to the Barracuda Advanced Threat Protection Cloud. It gives you full policy control over how PDF documents, Microsoft Office Files, EXEs/MSIs/DLLs, macOS executables, iOS executables, Android APKs, compressed files, and archives are emulated and delivered to the client. Based on identified malware activity, infected users can be automatically quarantined, thereby preventing the malware from spreading within the network.
5.2	Ensure that all anti-virus mechanisms are maintained as follows: ...	Barracuda's **Malware Protection** receives multiple signature updates per day. A virus scanner log can also be enabled for different levels to enable debugging or auditing. The built-in **Web Filter** engine can be set to have an hourly or continuous update interval. You can log which requests are allowed and denied, and specify the types of statistics that are generated for the service. Barracuda **Advanced Threat Protection** automatically scans traffic and uses a full OS emulation in a next-generation sandbox to prevent harmful code from entering the network via downloads or attachments. When malicious traffic is detected, both user and administrator are informed in real time.
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	**Barracuda Network Access Client** is tightly integrated into Windows' Security Center and its Health Status capabilities. This enables administrators to define health status parameters (e.g., antivirus engine versions, pattern database versions, personal firewall is active, etc.) that are mandatory for accessing the network.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking...	Barracuda CloudGen Firewall's antivirus and intrusion detection mechanisms provide risk ranking as well as CVE information for found security risks. Updates to all Barracuda CloudGen Firewall deployments can be enforced centrally via **Barracuda Firewall Control Center**.
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches...	**Barracuda CloudGen Firewall** administrators are automatically and proactively informed about available firmware updates, security patches, etc. Albeit updating the system to the latest firmware and/or applying the latest patches is highly recommended, it is not mandatory to operate the security infrastructure.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	**Barracuda CloudGen Firewall** can be used to enforce access control policies via firewall rules that enforce granular access control based on users, user group, subnet, time, application, and protocol. In addition, the **Barracuda Network Access Client** can ensure that only healthy PCs and authenticated users are able to connect to the corporate network. Two-factor authentication is also available by combining different authentication types (e.g., password and token (OTP, SMS PASSCODE).
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed…	**Barracuda CloudGen Firewall** can implement access control policies based on user groups. For example, you can only allow members of a specified Active Directory user group to access a particular network segment containing cardholder data, and only during normal business hours.

Requirement 8: Identify and authenticate access to system components

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows…	Implementing user authentication and user objects per firewall rule, allows **Barracuda CloudGen Firewall** to control network access for authenticated users.
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate…	**Barracuda CloudGen Firewall** supports numerous authentication types, including Microsoft Certificate Management, Microsoft Active Directory, LDAP, RADIUS, MSNT, RSAACE, External X509 certificates, SMS PASSCODE, RSA tokens, and smart cards. In addition, ensuring that all PCs connect to the network via Barracuda's Network Access Client (NAC), means that users can only connect to the network via highly secure two-factor authentication and only from healthy PCs.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	The different authentication types (listed above) can also be combined to implement rock-solid multi-factor authentication on **Barracuda CloudGen Firewall**. For even tighter security, it is possible enforce the use of strong or specific ciphers.
8.4	Document and communicate authentication policies and procedures to all users including…	All passwords used to connect to **Barracuda CloudGen Firewall** are rendered unreadable during transmission using strong cryptography.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
10.1	Implement audit trails to link all access to system components to each individual user.	**Barracuda CloudGen Firewall** allows the use of separate administrative accounts for each system admin with varying privileges. Every Barracuda CloudGen Firewall, as well as Firewall Control Center, includes a built-in change control system that documents in detail what configuration entry has been changed by what login user from what IP at what time.
10.2	Implement automated audit trails for all system components to reconstruct the following events.	The audit service in **Barracuda Firewall Control Center** aggregates all audit information, across multiple firewalls, related to firewall sessions. It also allows complex queries. This enables the implementation of automated audit trails for those who have accessed (or attempted to access) cardholder data.
10.3	Record at least the following audit trail entries for all system components for each event:	**Barracuda CloudGen Firewall** implements detailed logging of data passing through the firewall. This data can be used to see who has accessed what network segment when.
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	**Barracuda CloudGen Firewall** can continuously synchronize time using the network time protocol (NTP) and a trusted NTP Server.
10.5	Secure audit trails so they cannot be altered.	The log files that constitute an audit trail are securely stored on **Barracuda CloudGen Firewall** or **Barracuda Firewall Control Center** so that they cannot be altered. All traffic relating to the logs is encrypted. In addition, the syslog service collects Revision Control System (RCS), as well as log messages, from Barracuda CloudGen Firewall devices that are managed by Barracuda Firewall Control Center and streams those log messages to an external log host or sends them to the HA partner (with or without SSL encryption). This means that even changes made by the root user can be tracked and audited.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	On **Barracuda CloudGen Firewall** and **Barracuda Firewall Control Center**, you can configure notifications for specific system events. These event notifications can be sent via email or SNMP trap messages. Notifications can be configured for the different event types.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Logs can be easily exported from **Barracuda CloudGen Firewall** devices and **Barracuda Firewall Control Center** for archiving.

Requirement 11: Regularly test security systems and processes

PCI DSS REQUIREMENT		BARRACUDA NETWORKS SOLUTION
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises...	**Barracuda CloudGen Firewall** provides easy to use out-of-the box Intrusion Prevention System (IPS) against a vast number of exploits and vulnerabilities in operating systems, applications, and databases to prevent network attacks such as: • SQL injections • Arbitrary code executions • Access control attempts and privilege escalations • Cross-Site Scripting • Buffer overflows • Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks • Directory traversal attempts • Probing and scanning attempts • Backdoor attacks, Trojans, rootkits, viruses, worms, and spyware

Barracuda
Your journey, secured.