

Barracuda Web Site Firewall Ensures PCI DSS Compliance

E-commerce sales are estimated to reach \$259.1 billion in 2007, up from the \$219.9 billion earned in 2006, according to The State of Retailing Online 2007 study conducted by Forrester Research and Shop.org. While e-commerce continues to mature as a sales channel, it is met with a similar rise in cost due in part to Web site hacks and data leakage incidents. Identity theft cost U.S. businesses and consumers \$56.5 billion in 2005 as reported by the 2006 Identity Fraud Survey Report published by Javelin Strategy & Research.

In response to the increase in identity theft and security breaches, major credit card companies collaborated to create the Payment Card Industry Data Security Standard (PCI DSS) for merchants, processors and point-of-sale providers handling and storing sensitive account information. The current PCI DSS Version 1.1 outlines 12 procedures and system requirements to securely store and access Primary Account Number (PAN) information. While there are no penalties levied by the PCI Security Standards Council responsible for managing the requirements, credit card issuers and financial institutions can enforce PCI DSS compliance by offering incentives and issuing fines.

Barracuda Web Site Firewalls protect networks against unauthorized access, data leakage, site defacement and other malicious attacks by hackers that compromise both the privacy and integrity of vital data. By installing a Barracuda Web Site Firewall, businesses that store, process and/or transmit credit card numbers can protect their Web applications and sensitive data and achieve PCI DSS compliance in one easy step.

Payment Card Industry Data Security Standard (PCI DSS) Requirements

The 12 PCI DSS requirements are organized into six main categories and mandate the proper use of firewalls, message encryption, access controls, network monitoring and the need for an information security policy. To be fully compliant, an organization must satisfy all 12 requirements.

- *Maintain a Secure Network: Requirements 1 and 2*
 - Install and maintain a firewall configuration to protect cardholder data
 - Do not use vendor-supplied defaults for system passwords and other security parameters
- *Protect Cardholder Data: Requirements 3 and 4*
 - Protect stored cardholder data
 - Encrypt transmission of cardholder data across open, public networks
- *Maintain a Vulnerability Management Program: Requirements 5 and 6*
 - Use and regularly update anti-virus software
 - Develop and maintain secure systems and applications
- *Implement Strong Access Controls: Requirements 7, 8, and 9*
 - Restrict access to cardholder data by business need-to-know
 - Assign a unique ID to each person with computer access
 - Restrict physical access to cardholder data
- *Regularly Monitor and Test Networks: Requirements 10 and 11*
 - Track and monitor all access to network resources and cardholder data
 - Regularly test security systems and processes
- *Maintain an Information Security Policy: Requirement 12*
 - Maintain a policy that addresses information security

Source: PCI Security Standards version 1.1 - <http://www.PCISecurityStandards.org>.

RELEASE 1 SEPTEMBER 2007

Identity theft

- 73 percent of respondents said their crime involved a credit card
 - Average time spent by victims resolving the problem is about 40 hours
 - Emotional impact is similar to victims of violent crimes
- Source: Identity Theft Resource Center, 2003 survey

PCI Security Standards Council

Founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to enhance payment account security.

Noncompliance fines

In 2005, Visa imposed \$3.4 million in noncompliance fines. In 2006, fines reached \$4.6 million to banks, which were later passed on to noncompliant merchants

Today's merchants and organizations should be most concerned with PCI DSS Section 6.6, which addresses the development and maintenance of secure systems and applications. By June 30, 2008, all Web applications handling credit card and account information must undergo an extensive audit of all custom application code or implement a Web application firewall, to protect Web servers from attacks and hackers attempting to exploit any application code vulnerabilities.

A code audit places considerable burdens on a company with the mass quantity of code to review, time required to prepare and execute a code review, and considerable cost to undergo an audit for each application and throughout an applications lifecycle for any code changes. The greatest setback in conducting an audit is the expense in reorganizing the programming team to fix the discovered vulnerabilities in each application rather than continuing to innovate and drive companies forward in the marketplace. Once code reviews are conducted, quarterly reviews must be maintained to account for any change in the application code.

The simpler alternative to satisfy PCI DSS Section 6.6 compliance and ensure overall Web security is to invest and implement a comprehensive Web application firewall. This option not only protects Web applications from any attacks, it ensures a layer of security regardless of the application code.



Barracuda Networks Enables PCI DSS Compliance

Barracuda Web Site Firewalls are designed as easy and cost-effective solutions to achieve PCI DSS compliance. Barracuda Web Site Firewalls protect your Web site from attackers leveraging protocol or application vulnerabilities to instigate data theft, denial of service (DoS) or defacement of your Web site. Unlike traditional network firewalls or intrusion detection systems that simply pass HTTP or HTTPS traffic for Web applications, Barracuda Web Site Firewalls proxy this traffic and insulate your Web servers from direct access by hackers.

In addition to satisfying the time-sensitive need to install a Web application firewall by June 30, 2008, Barracuda Web Site Firewalls ensure PCI DSS compliance across major requirements with a host of other advanced technologies.

Requirement	Barracuda Web Site Firewall
1 - Install a Firewall	Acts as a network firewall and a Web application firewall to delineate the Demilitarized Zone (DMZ) and consolidate the application security infrastructure to reduce complexity and administrative overhead
3 - Protect data	Proxies all inbound and outbound Web traffic to insulate Web servers from direct access by attackers
4 - Encryption	Provides easy SSL encryption even if the application or server does not enable SSL encryption for inbound and outbound Web traffic

PCI DSS Section 6.6

Ensure that all Web-facing applications are protected against known attacks by applying either of the following methods:
 - Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security audits
 - Installing an application layer firewall in front of Web-facing applications

Challenges to an Application Code Audit

- The average security defect takes 75 minutes to diagnose and six hours to fix. (Pentagon Study)
- Every 1,000 lines of code average 15 critical security defects. (US Dept. of Defense)
- The average business application has 150,000-250,000 lines of code. (Software Magazine)

6 - Protect Against Vulnerabilities	Safeguards custom development, legacy and thirdparty applications from known and zero-day attacks as well as the industry-accepted top 10 Web application vulnerabilities
7 - Restrict Access	Utilizes role-based administration to enforce security policies for accessing systems and SSL administration
10 - Track and Monitor Access	Provides logs and reports of application access and security violations

Barracuda Networks Provides Comprehensive Protection Against Top 10 Application Vulnerabilities

The most significant set of requirements is PCI DSS Section 6.5 as it highlights the greatest security risks -- the industry-accepted top 10 application vulnerabilities. The top 10 application vulnerabilities compiled by Open Web Application Security Project (OWASP), address ways hackers exploit vulnerabilities in bad application code.

The Barracuda Web Site Firewall directly address each of the requirements in section 6.5.

Section 6.5.1 Unvalidated Input

Explanation and Examples: Tamper with an HTTP request to bypass a site's security mechanisms, also known as forceful browsing, command insertion, cross-site scripting, buffer overflows, SQL injection, cookie poisoning and hidden field manipulation

Barracuda Web Site Firewall solution: Validates incoming and outgoing session content against legitimate application behavior and usage

Section 6.5.2 Broken Access Control

Explanation and Examples: Exploits inconsistent code across Web applications to gain unauthorized access to other users' accounts, view sensitive files or use authorized functions

Barracuda Web Site Firewall solution: Sets up and enforces authorization and access control policies to authenticate user access requests via integrated LDAP, RADIUS, CA SiteMinder and RSA Access Manager interfaces

Section 6.5.3 Broken Authentication and Session Management

Explanation and Examples: Leverages security weaknesses in authentication and session state to tamper with cookies, form fields or tampering with other authentication tokens, and hijack sessions

Barracuda Web Site Firewall solution: Fully terminates and proxies every connection gaining visibility into each unique user session, then automatically encrypts session cookies and assigns unique session-IDs to ensure secure user sessions

Section 6.5.4 Cross-Site Scripting (XSS) Attacks

Explanation and Examples: Injects malicious code within a script from a trusted source intent on accessing cookies, session tokens, attack a local system, gain access to sensitive information stored by a browser or spoof content to confuse the user

Barracuda Web Site Firewall solution: Validates user input by terminating session and inspecting incoming requests before forwarding it to the backend servers, blocking it prior to executing within a browser

OWASP

A worldwide free and open community focused on improving the security of application software. OWASP strives to make application security "visible" for people and organizations to make informed decisions about application security risks.

Section 6.5.5 Buffer Overflows

Explanation and Examples: Floods the memory capacity of one buffer to execute a malicious program on the adjacent "overflow" buffer to steal passwords or confidential information, alter system configuration, install backdoors or launch other attacks

Barracuda Web Site Firewall solution: Rejects any file from in invalid Web page and limits total Web request length across applications

Section 6.5.6 Injection Flaws

Explanation and Examples: Relays malicious code through a Web application to another system, such as the operating system, database or an external program

Barracuda Web Site Firewall solution: Inspects each request from a Web application to the backend systems for malicious code and blocks any malicious request prior to reaching the application server

Section 6.5.7 Improper Error Handling

Explanation and Examples: Exploits error messages that reveal detailed information about the OS and server versions, directories, patch levels, internal addresses and known platform vulnerabilities

Barracuda Web Site Firewall solution: Cloaks details of Web application infrastructure and blocks error messages being displayed on the Web

Section 6.5.8 Insecure Storage

Explanation and Examples: Leverages the difficulty to properly code encryption for the storage of credit card numbers, account records or proprietary information

Barracuda Web Site Firewall solution: Filters and intercepts outbound traffic to prevent the transmission of sensitive information. Also blocks or masks attempts to access credit card numbers, Social Security numbers, client records or any other specified data type.

Section 6.5.9 Application Denial of Service (DoS)

Explanation and Examples: Attempts to degrade application performance or crash an application by generating excessive session traffic to specific URLs affecting server performance

Barracuda Web Site Firewall solution: Slows down access requests to the Web site if a violation is detected, preventing application DoS attacks

Section 6.5.10 Insecure Configuration Management

Explanation and Examples: Exploits common configuration problems, such as unpatched holes in operating systems, unnecessary default accounts and unnecessary services enabled

Barracuda Web Site Firewall solution: Acts as the DMZ to proxy inbound and outbound Web traffic to neutralize any configuration vulnerabilities

For more information on the Barracuda Web Site Firewall, please visit <http://www.barracuda.com/websitefirewall> or call a Barracuda Networks regional sales representative at 1-888-ANTI-SPAM for a free 30-day evaluation.

About Barracuda Networks, Inc.

Established in 2002, Barracuda Networks, Inc. is the worldwide leader in email and Web security appliances. Barracuda Networks also provides world-class IM protection, application server load balancing and message archiving appliances. More than 50,000 companies, including Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, NASA and Europcar, are protecting their networks with Barracuda Networks solutions. Barracuda Networks' success is due to its ability to deliver easy to use, comprehensive solutions that solve the most serious issues facing customer networks without unnecessary add-ons, maintenance, lengthy installations or per user license fees. Barracuda Networks is privately held with its headquarters in Campbell, Calif. Barracuda Networks has offices in eight international locations and distributors in more than 80 countries worldwide. For more information, please visit www.barracuda.com.



Barracuda Networks

3175 S. Winchester Boulevard
Campbell, CA 95008
United States
+1 408.342.5400
www.barracuda.com
info@barracuda.com