



MEETING PCI DSS MERCHANT REQUIREMENTS WITH A WATCHGUARD[®] FIREBOX[®]

FEBRUARY 2008

Introduction

Over the past few years there have been several high profile security breaches that have resulted in the loss of credit information and individual account data for millions of credit card users, including:

- June 2005 – a hacker infiltrates the network of CardSystems Solutions Inc. and accesses potentially 40 million credit card numbers retained by a company that processed payment data for MasterCard International Inc. and other companies.¹
- January 2007 – an unauthorized intrusion into the computer systems that process and store information related to customer transactions of the TJX Companies, Inc., results in the theft of at least 45.7 million credit and debit card numbers.^{2, 3}

The goal of the Payment Card Industry Data Security Standard (PCI DSS) is to create a framework for good security practice around the handling of cardholder data. A PCI-compliant operating environment is one in which the cardholder data exists (i.e., it does NOT refer to the whole corporate network), and PCI DSS defines the requirements for how access to this data must be controlled, monitored, logged, and audited.

¹ 40M credit cards hacked; Breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards, July 27, 2005, Jeanne Sahadi, CNN/Money.

² Retailer TJX reports massive data breach Credit, Debit data stolen. Extent of breach still unknown, January 17, 2007, Paul F. Roberts, Info

³ TJX breach involved 45.7m cards, company reports, March 28, 2007, Jenn Abelson, The Boston Globe

The objective of this white paper is to clearly outline how firewall deployment impacts meeting PCI DSS standards for a PCI DSS merchant. Tables include a description of each PCI DSS standard and then show how the WatchGuard Firebox family of appliances achieves these requirements.

Please note that the steps required for a company to achieve PCI DSS compliance vary based on that company's architecture; it is not possible to identify a single, "generic" network solution and Firebox configuration for achieving PCI DSS compliance.

PCI DSS Overview

The potential for loss from security breaches prior to the recent high profile incidents was well recognized by each of the major credit card vendors, who responded by creating their own information security programs:

- Visa Card Information Security Program
- MasterCard Site Data Protection
- American Express Data Security Operating Policy
- Discover Information and Compliance
- JCB Data Security Program

Each company's intentions were roughly similar: to create an additional level of protection for customers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data.

In 2004, the credit card companies came together and the Payment Card Industry Security Standards Council was formed to align their individual policies and create the Payment Card Industry Data Security Standard (PCI DSS) in December 2004. In September, 2006, the PCI standard was updated to version 1.1 to provide clarification and minor revisions to version 1.0.⁴

The goal of PCI DSS is to create a framework for good security practice around the handling of cardholder data. It does *not* define the security requirements for your whole IT infrastructure

PCI DSS applies to every organization that processes credit or debit card information, including merchants and third-party service providers that store, process, or transmit credit/debit card data. Any company involved in processing, storing, or transmitting credit card numbers *must* be compliant with the standard or risk losing the ability to process credit card payments, as well as risk being fined for violations up to \$100,000 per incident. It's not enough to simply make a statement confirming compliance; merchants and financial institutions must have their compliance status validated by outside vendors who are a certified PCI DSS Qualified Security Assessor (QSA).

Merchants and Merchant Levels

For PCI DSS, a merchant is defined as any company that accepts credit or debit cards in exchange for goods or services. Merchants are categorized into one of four levels, based on the transaction volume. The higher the transaction volume a company has, the greater the impact of a security breach is likely to be, warranting tighter security requirements. As a result, the higher the credit card transaction volume a merchant organization has, the more stringent the requirements are for achieving PCI DSS compliance.

For Level 1 merchant organizations, compliance is achieved by undergoing an annual on-site security audit, quarterly network scans and validation by a qualified security assessor (QSA) and approved scanning vendor (ASV). Level 2 and 3 merchants must comply with the PCI DSS Self Assessment Questionnaire and undergo a

⁴ http://en.wikipedia.org/wiki/PCI_DSS

quarterly network scan, which must be validated by both the merchant and an ASV. For Level 4 merchant, it is recommended that the organization comply with the PCI DSS Self Assessment Questionnaire and to have an annual network scan. Note that for a Level 4 merchant, if a breach has been reported or found, VISA reserves the right to move the Level 4 merchant to a Level 1. If so, the Level 4 merchant must abide by the Level 1 validation requirements. Hence, Level 4 merchants are strongly encouraged to consider the PCI DSS-recommended actions as mandatory.

PCI DSS Merchant Levels

Level	Description
1	<ul style="list-style-type: none">• Any merchant processing over 6,000,000 transaction per year• Any merchant that has been involved in a hack or attack that caused a data disclosure• Any merchant that PCI determines should be at Level 1 to minimize risk to cardholder data
2	Any merchant processing 1,000,000 to 6,000,000 transactions per year
3	Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year
4	<ul style="list-style-type: none">• Any merchant processing fewer than 20,000 e-commerce transactions per year• All other merchants, regardless of acceptance channel, processing up to 1 million transactions per year

Fines Associated with Non-Compliance

ALL of the deadlines for meeting PCI DSS have passed, which means that **ANY** merchant that does not comply with the standard is at risk of being fined. Visa USA has announced that it will start fining banks that process merchant transactions (which will pass the costs on to the merchant) between \$5,000 and \$25,000 per month if their Level 1 or 2 merchants have not demonstrated compliance. In addition, the fines of \$10,000 per month may already be assessed today for prohibited data storage by a Level 1 or Level 2 merchant.

Companies that are not yet compliant will be fined up to \$500,000 by the card brand companies if compromised, not including any civil liabilities (which typically dwarf this amount). Any company still in business and needing to continue transaction after such a compromise will automatically “restart” at Level 1 status, making future achievement of compliance significantly more expensive.

PCI DSS Compliance and Requirements Overview

In order to achieve PCI DSS compliance, a merchant must demonstrate 100% conformance with the requirements of the standard, but being compliant today does not mean indefinite compliance. To ensure that a PCI-compliant merchant is able to incorporate new technologies and to respond to new ways of hacking personal data, there are continuing auditing responsibilities that must be undertaken to retain PCI DSS compliance.

There are 12 requirements that must be satisfied in order to achieve compliance, addressing the technologies, policies, and procedures that must be in place. The requirements are organized into six main control objectives:

- **Build and Maintain a Secure Network**
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- **Protect Cardholder Data**
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
 - Requirement 10: Track and monitor all access to network resources and cardholder data
 - Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
 - Requirement 12: Maintain a policy that addresses information security

Breeding a “Culture of Security”

Take the PCI DSS conformance out of the equation for a moment and ask yourself, “Do we have a culture of security within our organization?” What this means is:

- 1) Do we educate and train each other on best security practices for our business?
- 2) Do we have a security policy that is up-to-date, that people are aware of, and do we have a way to review it, change it as needed, and to enforce it?
- 3) Do we have the controls – be they policy-driven, technical, or whatever – to be able to make sure that we stay compliant within the policy that we’ve created?

If you have those factors, you have a security culture – and when you have a security culture, regardless of the regulatory or industry compliance standards you have to meet, you’re going to have a sound framework from which you can adapt to them.⁵

There’s No Such Thing as “Certified PCI DSS Compliant”

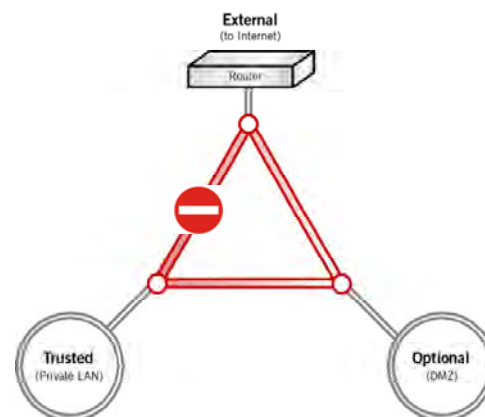
Where firewalls are concerned, there is no product that is going to be “certified PCI DSS compliant.” It’s just a myth. Any network firewall, and by extension a unified threat management (UTM) appliance that combines a network firewall with other features (such as anti-virus and intrusion prevention services), can be a part of *becoming* compliant, but it’s only going to cover a certain portion of the compliance requirements.

For companies seeking PCI DSS compliance, it is important to design a network with appropriate physical and logical boundaries to segregate the PCI-compliant operating environment. The PCI DSS monitoring scope must also be made manageable. To this end, the strong segregation capability available with the application proxy technology of the WatchGuard® Firebox® X family of UTM appliances is ideally suited to meeting these requirements.

⁵ *Cutting through Compliance Clutter*, February 2008, WatchGuard Radio Free Security interview Chris Squier, CISSP.

Zoned Networks

All Firebox appliances support the zoned network architecture for creating a Demilitarized Zone (DMZ), as required by PCI DSS. In this architecture, only the servers contained within the DMZ are accessible from the Internet, and the cardholder data is contained within the Trusted network zone. As required by PCI DSS, WatchGuard application proxy technology provides detailed control over the traffic that passes between network zones. This enables administrators to block all traffic by default and to define which traffic is allowed to pass from one zone to the next, including protocols, ports, content (e.g., MIME types, file types, and URLs) and verbs (e.g., HTTP GET). Via this architecture, communication between the Trusted zone and the Internet can be completely prohibited, and those between the Trusted and DMZ zones can be strictly limited to traffic that meets the PCI DSS and corporate communication requirements.



Beyond supporting the required network architectures, there are strong logging, monitoring, and auditing component required by PCI DSS, all of which are supported by WatchGuard Firebox appliances. In addition, the security subscriptions available for all WatchGuard Firebox appliances – including Gateway AntiVirus/ Intrusion Protection Service, WebBlocker, and spamBlocker – are a perfect complement to PCI DSS standards.

Compliance with the PCI DSS standards can only be achieved via a combination of PCI DSS operating environment network architecture (including firewall deployment) and security practices, procedures, and policies. Compliance can only be granted via independent assessment by a Qualified Security Assessor (QSA). As a result, it is not possible to define a single recipe for achieving compliance.

PCI DSS Requirements Impacted by Firebox Deployment

The tables below list PCI DSS requirements that a Firebox deployment addresses. This is not a complete set of the PCI DSS requirements; those that cannot be addressed by a Firebox deployment have not been included. The comments explain how a WatchGuard Firebox appliance complements each requirement.

Note: PCI DSS Requirement sections 3, 7, 9 and 12 are not included in these tables as they do not affect a network firewall deployment.

1. Install and maintain a firewall configuration to protect cardholder data

Req #	Requirement Details	Comments
1.2	Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.	The Firebox proxy architecture is ideal for meeting this requirement. The proxy architecture provides detailed granular control over which protocols, ports, and content are allowed through the firewall. This is achieved by blocking all traffic by default and defining a proxy policy that allows only approved traffic to pass into the PCI DSS operating environment. The Firebox IPS and AV services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts.
1.3	Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include items 1.3.1 through 1.3.8 below.	Using a zoned network architecture such as the one described in the Introduction, WatchGuard Firebox family of firewalls can be configured so that traffic from the Internet into the public-facing servers in the DMZ, and from the DMZ into the Trusted zone is restricted to only approved traffic types.

1.3.1	Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)	Using the zoned network architecture described above, Firebox appliances can be configured so that the only IP addresses that are accessible from the Internet are contained within the DMZ. The same configuration can be used to ensure that none of the IP addresses in the Trusted zone are visible or accessible from the Internet.
1.3.2	Not allowing internal addresses to pass from the Internet into the DMZ	This requirement refers to blocking any traffic from the Internet that has an RFC1918 IP address (i.e. IP addresses in any of the following ranges 10.0.0.0/32, 172.16.0.0/20 or 192.168.0.0/16) from entering the DMZ. Fireboxes can be configured to ensure that communication coming from the Internet from any RFC1918 IP address is blocked.
1.3.3	Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)	The objective of this requirement is to ensure that only traffic that is part of a legitimately established TCP/IP connection passes through the firewall, which is a basic approach to detecting and preventing malicious intrusion attempts. Firebox appliances include stateful inspection firewalls and other technologies, such as Protocol Anomaly Detection and Intrusion Prevention Services that can be used to meet or exceed the objectives of this requirement.
1.3.5	Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	The Firebox proxy architecture provides detailed granular control over which protocols, ports and content are allowed through the firewall. The Firebox IPS and AV services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts.
1.3.6	Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration	This requirement only affects a Firebox if used as primary router. If this is the case, then the WatchGuard System Manager may be used to define and deploy a synchronized configuration to each Firebox.
1.3.7	Denying all other inbound and outbound traffic not specifically allowed	The Firebox proxy architecture is uniquely able to fulfill the objectives of this requirement by creating detailed policies that define only the traffic that is allowed into and out of the network. All other traffic is blocked.
1.3.8	Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)	If a Firebox X Edge appliance is used as the wireless access point, the wireless network can be isolated from both the DMZ and Trusted network zones.
1.4	Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	The requirements in section 1.4 relate specifically to the use of zoned network architecture to segregate cardholder data so as to ensure that it cannot be accessed directly via the Internet. WatchGuard Firebox appliances support network zones, and they can be configured to create a DMZ for all public-facing servers and a Trusted zone where the cardholder data resides. They can also be configured to ensure that no traffic can pass from the Internet into the Trusted zone, or vice versa. All traffic to and from the Internet therefore has to go via the public servers in the DMZ, with the Firebox configured to ensure that all traffic from the Trusted zone to the Internet is blocked, ensuring that all external traffic comes from the IP addresses in the DMZ.
1.4.1	Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic	
1.4.2	Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	
1.5	Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	Network Address Translation (NAT) is a standard feature in all Firebox appliances.

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

The “system” referred to in this requirement is the whole PCI DSS environment and it encompasses databases, endpoints, network infrastructure, etc. The idea is to essentially ensure that it is not possible for a system to be compromised by anyone who is able to identify the system components and try the default passwords for the devices used. Password management for Firebox appliances is easily achieved via the management interface.

2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	Firebox appliances' proxy architecture provides detailed granular control over which protocols, ports, and content are allowed passage through the firewall. This is achieved by blocking all traffic by default and defining a proxy for those specific protocols that are allowed. The Firebox IPS and AV services can also provide security for those protocols that are allowed.
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	All management communications with Firebox appliances are done via a secure encryption-based protocol.

4. Encrypt transmission of cardholder data across open, public networks

4.1	Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSec) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are the Internet, Wi-Fi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).	All e-Series Firebox appliances running Version 10 firmware support IPSec and SSL VPN communication.
4.1.1	For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSec VPN, or SSL/TLS. Never rely exclusively on wired equivalency privacy (WEP) to protect confidentiality and access to wireless LAN. If WEP is used, do the following: <ul style="list-style-type: none"> • Use with a minimum 104-bit encryption key and 24 bit-initialization value • Use ONLY in conjunction with Wi-Fi protected access (WPA or WPA2) technology, VPN, or SSL/TLS • Rotate shared WEP keys quarterly (or automatically if the technology permits) • Rotate shared WEP keys whenever there are changes in personnel with access to keys • Restrict access based on media access code (MAC) address 	Wireless networks are inherently insecure, but there are some circumstances where they cannot be avoided. In these cases, the standard requires that the wireless operating environment be physically segregated from the wired environment and appropriately firewalled. When a Wi-Fi solution must be used, the Firebox X Edge supports WPA2 and can be combined with either an IPSec or SSL VPN to achieve the objectives of this requirement.

5. Use and regularly update anti-virus software or programs

5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware	All Firebox appliances provide Gateway AntiVirus support that serve to reduce the ingress of malware into the network, helping to meet the objectives of this requirement.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	All Firebox appliances provide automatic updates of the Gateway AntiVirus signature database, helping to meet the objectives of this requirement. In addition, the appliance Logs are updated whenever traffic is denied by the Gateway AntiVirus and whenever the signature sets are updated.

6. Develop and maintain secure systems and applications

6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	WatchGuard LiveSecurity® Service gives you access to updates and enhancements for Firebox products, including minor software patches and new software versions.
6.2	Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	WatchGuard LiveSecurity Service Rapid Response Team, a dedicated group of network security experts, monitors the Internet to identify emerging threats, then delivers LiveSecurity Service alerts that describe what can be done to address each new menace.
6.6	<p>Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:</p> <ul style="list-style-type: none"> • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security • Installing an application layer firewall in front of web-facing applications <p>Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement</p>	<p>This requirement specifically addresses the potential vulnerabilities in applications accessible from the Internet and it refers specifically to the use of web application firewalls to provide a robust mechanism to mitigate application vulnerabilities (e.g., SQL injection, cross site scripting).</p> <p>In combination with a web application firewall, Fireboxes provide an additional layer of protection. The HTTP proxy is a high-performance content filter that examines web traffic to identify suspicious content, which can be a virus, spyware, or other type of intrusion. It can also protect your web server from attacks from the external network.</p>

8. Assign a unique ID to each person with computer access

8.2	<p>In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> • Password • Token devices (e.g., SecureID®, certificates, or public key) • Biometric 	Firebox appliances support authentication via Active Directory, which streamlines authentication, saving time and eliminating hassles.
8.3	Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSec) with individual certificates.	Firebox appliances support two-factor authentication, including RADIUS, SecureID, and individual VPN certificates.
8.4	Encrypt all passwords during transmission and storage on all system components.	All management communications with Firebox appliances are done via a secure encryption-based protocol, and Firebox appliances store their password information in an encrypted format.

10. Track and monitor all access to network resources and cardholder data

One of the gray areas of the standard, DSS Requirement 10 should be treated carefully – if misinterpreted, it can have the most significant impact on the effort and costs required to achieve compliance. The basic objective is to ensure that all access to stored cardholder data is logged, but the extended objective is also to ensure that any configuration changes to the network components used to access and/or isolate the stored data are also logged. All log data should be stored and periodically monitored to identify any potential or actual security breaches (either via routine audit/test or actual attack). In the case of a compromise, this data is essential for tracing the cause and identifying the network vulnerability so that it may be remedied.

A PCI-compliant environment should be designed with the appropriate physical and logical boundaries to segregate the PCI-compliant operating environment and to make PCI DSS monitoring scope manageable. Trapping all that can be logged is NOT the point of the monitoring requirement; protection of cardholder data is paramount, and therefore should be the focus of all logging activity.

Practical monitoring of the network for all but the smallest organization is best done using something like a Security Information Management (SIM) solution. These solutions will continually analyze the data logs from the various network components and use data correlation techniques to attempt to identify and alert the system administrator of any security breaches. Key aspects of a PCI DSS-compliant environment to enable meaningful monitoring are:

- Consistent time stamping amongst network equipment for data correlation
- Identity management solution (e.g., Microsoft Active Directory)
- Event management storage (including firewall data, that must be configured to send data to the SIM)

Firewalls are considered to be an infrastructure component, i.e., a carrier and/or handler of cardholder data. As such, they need to be configured to send logs to the SIM. Exactly what data must be logged is not defined in the standard, and this should be determined as a tradeoff between security and business criteria. At the highest level, firewalls need to be able to provide the following:

- Ability to send logs to the SIM, most typically via SNMP
- Compatibility with the chosen identity management solution
- IDS, IPS and antivirus solutions – the actions of which must also be logged
- Wireless networks require special attention as they are fundamentally insecure. Every precaution must be taken to secure against wireless hacks.

10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	Pertains to being able to trace each login activity to an individual. Per comments above, it is best to use an Active Directory type solution for tracking identity and logging access. All Firebox appliances support authentication via Active Directory.
10.2	Implement automated audit trails for all system components to reconstruct the events listed in 10.2.1 through 10.2.7	When reading the PCI DSS specification to understand the impact on a firewall deployment, it is easy to believe that all of the logging requirements pertain to the firewall also. In reality, these requirements are requirements for the whole PCI DSS operating environment, and if it is possible to capture and log this information elsewhere, then it is not necessary for this information to be logged at the firewall.
10.2.1	All individual user accesses to cardholder data	
10.2.2	All actions taken by any individual with root or administrative privileges	
10.2.3	Access to all audit trails	
10.2.4	Invalid logical access attempts	
10.2.5	Use of identification and authentication mechanisms	
10.2.6	Initialization of the audit logs	
10.2.7	Creation and deletion of system-level objects	
10.3	Record at least the following audit trail entries for all system components for events listed in 10.3.1 through 10.3.6	For a firewall deployment, this requirement pertains to ensuring that any configuration changes to the network components used to access and/or isolate the stored data are logged. All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated.
10.3.1	User identification	
10.3.2	Type of event	
10.3.3	Date and time	
10.3.4	Success or failure indication	
10.3.5	Origination of event	
10.3.6	Identity or name of affected data, system component, or resource	

10.4	Synchronize all critical system clocks and times.	All Fireboxes support NTP synchronization.
10.5	Secure audit trails so they cannot be altered.	This can be achieved in by either configuring the Firebox to send log data to a SIM via SNMP, or by using the Firebox logs in their raw form. If the Firebox logs are used, then the Log server must be on a secure machine (interaction with the Firebox is secure). Firebox appliances also support sending log data to syslog servers, but this is not recommended as this is not a secure solution.
10.5.4	Copy logs for wireless networks onto a log server on the internal LAN.	If Firebox X Edge wireless access points are used, this is achievable by using WatchGuard Log server.
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.	WatchGuard Log Viewer can be used to search Firebox appliance logs sent to the WatchGuard Log server for specific event types.

11. Regularly test security systems and processes

11.4	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	Firebox Intrusion Prevention Service (IPS) security subscription can be used to address this requirement. While it is not recommended that the Firebox IPS solution be the only IPS system deployed in the network, use of the Firebox IPS is a great complement to addressing this requirement.
------	---	--

Summary

Any company that accepts credit or debit cards in exchange for goods or services must already be compliant with the PCI DSS requirements. As of June 30, 2008 all web-facing applications must also be protected by a web application firewall.

The keys to achieving PCI DSS compliance are:

- Fostering a culture of security within the organization
- Designing, deploying, and maintaining a secure networking infrastructure, a necessary component of which is a firewall.

While the notion of a “PCI DSS-compliant” firewall is a myth, application proxy-based firewalls are particularly well suited to meeting the requirements of the standard.

In particular, the PCI DSS standard requires a zoned network architecture where all traffic into the trusted portion of the network is blocked by default so that only the specific protocols, ports, and content allowed by the corporation’s security policy are allowed to pass into the Trusted zone. Implementing and securing this type of network architecture is exactly what an application proxy-based firewall is ideally suited for.

Compliance with the PCI DSS standards cannot be achieved by the deployment of a single network component. It can only be achieved via a combination of PCI DSS operating environment network architecture (including firewall deployment) and security practices, procedures, and policies. As a result, it is not possible to define a single recipe for achieving compliance.

The WatchGuard Firebox X family of UTM products is ideally suited to building and maintaining a PCI DSS-compliant network environment thanks to the strong segregation capability available with the built-in application proxy technology. For more information about our powerful network security solutions, visit us at www.watchguard.com or contact your reseller.

WatchGuard provides a useful, no-nonsense guide to establishing a strong network security policy. For your free copy, visit www.watchguard.com/infocenter/whitepapers/security_policy.asp.

References

1. www.pcicomplianceguide.org
2. PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, June 2007, Tony Bradley, et al
3. *Payment Card Industry (PCI) Data Security Standard, Version 1.1*, September 2006, PCI Security Standards Council (www.pcisecuritystandards.org)
4. *Cutting Through Compliance Clutter*, February 2008, WatchGuard Radio Free Security interviews Chris Squier, CISSP

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis.

©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, and LiveSecurity are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners.

Part. No. WGAG66504_011209