PSC
Payment and Security Experts

Implementing PCI

A Guide for Network Security Engineers

Updated For PCI Data Security Standard Version 1.2.1

Tom Arnold, CISSP, ISSMP, CFS, CPISM/A, PCI/QSA
Partner, PSC

Sponsored by Juniper Networks, Inc.

Juniper NETWORKS

PSC

Abstract

As with the prior version, this paper provides architectural guidance for network security engineers who are responsible for implementing systems and technologies that are in compliance with the PCI Data Security Standard (PCI DSS).[1] The paper has been updated to include changes made in the PCI DSS between versions 1.1 and 1.2.1, and to reflect updates and advances in Juniper Networks' product lines. The paper analyzes the requirements that are specifically related to network security and describes approaches for achieving compliance in accordance with the spirit of the standard, while respecting the cost of deployment. At the conclusion, a section covering next steps for the network engineer provides general guidance for the engineer chartered with implementing PCI compliant network architecture.

[1] "Payment Card Industry Data Security Standard" Payment Card Industry Security Standards Council. Version 1.2.1. July 2009.

PSC

Contents

List of Figures

List of Tables

PSC

Introduction

This paper is not for the comfortable CIO or Director of Information Infrastructure who knows, for sure, that all of his critical business data are secure. Nor is it for the CEO who sleeps soundly at night knowing that her company's most critical data resources are under round-the-clock surveillance, with information security controls that would make the U.S. Department of Defense proud.

No, this paper is not for them. It's for the rest of the information technology industry—all those who worry each time they read a news story about hackers stealing credit card numbers from business systems; or about sensitive business secrets that are stolen and used against a company; or about military technology secrets that have been accessed by hackers.

Since the time this paper was first introduced until now, we have seen the nature and type of security threats evolve. SQL Injection and Web application attacks have become very prevalent as tools for both internal and external attack vectors. These exploits are frequently coupled with the inclusion of polymorphic malware that is used to siphon and extract sensitive data from within victim organizations.

In response to these expanding threats, the need to compartmentalize access to sensitive locations and to data contained therein has become even more critical. The concept of granting access on a *need-to-know basis* has been around for a long time as well. To some extent, this same technique has been used with large databases in that a user login has been coupled with a role (commonly referred to as *permissions*), and then data access is restricted or granted appropriately. Unfortunately, each access barrier and each security system is subject to some level of compromise.

The updated PCI DSS continues to implement the concept of *Defense in Depth*. The updated standard has clarified many overlapping security requirements and introduced several new defenses in an attempt to address trends observed as a result of reported data compromises. The 12 sections and 253 individual requirements of the PCI DSS describe security requirements and layered controls between perimeter networks, application servers, business processes, and critical data.

As with the prior version, this paper opens with a brief overview of the PCI DSS, including a discussion of theory and the difference between actual compliance with the standard and demonstration of compliance. It is important to describe the applicability and scope of the PCI DSS. These sections are critical for a network security engineer charged with design of solutions or selection of network technologies to address requirements.

Beyond the brief overview of the PCI criteria, this paper focuses on those elements and requirements that need to be addressed by network security solutions and technology. The detail sections of this report review the specific requirements of the DSS related to network security. The intent is to focus on techniques for designing a PCI network security solution and to provide important considerations that need to be included in any selection or analysis. Lastly, the detail sections illustrate the category and type of products that may be used to address the various requirements.

JUNIPER NETWORKS

PSC, when in the role as an independent assessor, has a policy of not endorsing any specific commercial product. Furthermore, PSC does not receive any material gain from any product our clients select to solve a security issue. That being said, PSC provides suggestions to our customers on technologies that meet requirements. To this end, each of the detail sections lists representative products from Juniper Networks that may be deployed, or areas that an integrator or network engineer should consider, to implement a similar solution. The Juniper Networks symbol at the left highlights the solution discussions.

Important notes are included to highlight areas where either the PCI DSS may not be entirely clear or to call attention to potential traps. In many cases, these *important notes* are used to point out conditions where traditional retailers or businesses with large legacy environments may want to pay special attention. Look for this symbol for *important notes*.

About the Author

Tom Arnold (tom@paysw.com) is a partner with PSC (www.paysw.com), a firm specializing in payments, security, and compliance for companies that accept or process consumer payments. His experience over the past 20 years includes roles as VP of Engineering, Chief Technology Officer, and Chief Software Architect, and he has developed products for a variety of software companies. He is a Certified Information Systems Security Professional (CISSP) and an Information Systems Security Management Professional (ISSMP), and he has a broad background in engineering and deploying secure software applications. Over his career, he has led large engineering teams and understands the principles of engineering quality products. Tom's

experience includes development of payment processing applications, high-performance credit card processing switches, and several secure data vaults for protecting sensitive information.

He has been consulted and has provided expert testimony to U.S. Federal Courts. He has given expert testimony to the U.S. House of Representatives, Committee on Commerce, Subcommittee on Telecommunications, Trade and Consumer Protection. And, he has testified before the U.S. Senate, Committee on Banking. He has been consulted by numerous regulatory agencies, including the Department of Commerce, Department of Treasury, Department of Justice, World Trade Organization, European Union Tax Ministers, Organization for Economic Cooperation and Development, and the U.S. Fair Trade Commission.

Status of this Document

This document is a *working whitepaper* describing systems and solutions for protecting critical consumer credit card information. To the best of the author's knowledge at the time of writing, the elements discussed address PCI requirements related to the current version 1.2.1 release of the PCI DSS.

The PCI DSS is under the control of the PCI Security Standards Council and is under constant evaluation and revision.

Comments and contributions are solicited for potential future versions of this paper. All comments should be addressed to the author at the e-mail address listed in the *About the Author* section.

Not too long ago, criminal hackers (crackers) stole the author's personal credit card data from a retailer as part of a very large security compromise. As both a consumer and insider in the payments industry, he understands both the personal pain and the business challenge that this kind of security breech can cause. Given that his account number was not the only one acquired, he knows that the bank that issued that account suffered substantial cost when they had to notify account holders, close accounts, and reissue new credit cards. These were direct costs and did not account for the loss of goodwill incurred by the merchant whose database was compromised. In short, this situation was bad for consumers, bad for banks, and bad for merchants. Further, there are more than a couple of IT architects and network engineers out of a job and with destroyed resumes who worked inside that company.

Scope of this Paper

This paper is for all businesses which operate systems that store, process, or transmit consumer credit card information. All topics and discussions are intended for both service providers (companies that provide some credit card processing service for merchants), and merchants that are traditional retailers and e-tailers. This paper is *not* a dissertation on cryptography or a detailed description of business practices and security controls required to achieve full compliance with the PCI DSS. Instead, it explores the area of network security controls exclusively.

Although this paper covers technical topics that are frequently relegated to network or information security gurus, the information is intended for IT infrastructure and IT management as well.

Primary audience includes:

- Network Architects
- Information Security Engineers
- Network Engineers
- Information System Architects
- Systems Designers

Secondary audience includes:

- IT Infrastructure Managers
- Chief Security Officers
- Chief Information Officers
- Chief Technology Officers

PSC

Quick Technical Tour of the PCI DSS

Administered by the PCI Security Standards Council, the PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

The PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International to address the growing issue of cardholder account security across the entire industry.

The PCI DSS aligns the Visa International Account Information Security (AIS) program, the Visa USA Cardholder Information Security Program (CISP), MasterCard's Site Data Protection (SDP) program, the American Express Data Security Operating Policy (DSOP), and Discover's Discover Information Security and Compliance (DISC), streamlining requirements, compliance criteria, and validation processes.

The core of the PCI DSS is a group of principles and accompanying requirements around which the specific elements of the standard are organized. There are 12 such principles in the Standard. I have outlined the essence of the 12 principles here:

1. Build and maintain a secure network.
2. Configure system security parameters.
3. Protect cardholder data at rest.
4. Protect sensitive data in transit.
5. Implement tools to protect against malicious software and viruses.
6. Develop and maintain secure applications.
7. Implement a process to authorize system access based on need-to-know.
8. Implement strong user authentication.
9. Physically secure systems and network devices.
10. Implement automated audit logs and protect log data.
11. Monitor and test security controls.
12. Maintain an information security policy and incident response plan.

These principles are described and broken down into 253 individual, detailed requirements. It should be apparent that the principles cover more than network security exclusively. The principles were conceived based on the results of actual forensic investigations, and they focus on all aspects of securing systems. As mentioned before, the intent is to create an environment where security considerations are implemented throughout the business and information technology areas. In reading the PCI DSS, one will quickly recognize that a significant percentage of requirements deal with process and procedural controls.

For the network engineer or architect, the requirements in principles 1, 2, 4, 6, 10, and 11 should be of primary interest. These requirements will be analyzed, in depth, later in this paper.

PCI Applicability

Understanding the applicability of the PCI DSS is *extremely* important. First and foremost, the PCI DSS is focused on protecting cardholder information. For an organization to successfully demonstrate compliance with the PCI criteria, it must show that all 253 requirements in the full PCI DSS are in place related to all systems that store, process, or transmit cardholder information. Below is a direct extract from the PCI DSS that defines what data elements constitute cardholder information.

The applicability of PCI is an extremely important concept for IT management and any network architect to fully understand. For many organizations, questions arise like: *How do we apply the requirements and know when a system or network needs to be in scope? Or, do we have to apply all 253 requirements to the whole network?*

The following Applicability Table illustrates commonly used elements of cardholder and sensitive authentication data; whether *storage* of each data element is permitted or prohibited; and if each data element *must be protected*. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

Table 1: PCI DSS Applicability Table

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder name*	Yes	Yes*	No
	Service code*	Yes	Yes*	No
	Expiration date*	Yes	Yes*	No
Sensitive authentication data**	Full magnetic stripe	No	N/A	N/A
	CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN block	No	N/A	N/A

***** These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices, if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

****** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

Here are a few quick definitions of terms to help understand the Applicability Table.

Table 2: PCI DSS Applicability Table Definition of Terms

Primary Account Number or PAN	This is the 13, 14, or 16 digit account number on the payment instrument. We commonly refer to this as the *"credit card number."* The term credit card number is specifically not used in the PCI DSS as the PAN can refer to any type of branded payment card.
Service code	This is a code found on track 1 or track 2 of the magnetic stripe. The value is represented as the 3 digits to the right of the expiry date.
Sensitive authentication data	This term references specific data elements that are either printed on the plastic card or on the magnetic tracks, or are derived from a cryptographic operation from an authorized PIN pad. These data elements are used either to validate the card and account number, or to confirm the presence of an authorized cardholder.
Full magnetic stripe	This term references the full track 1 or track 2 data found on the magnetic stripe of the credit card. The term references either track 1 data or track 2 data. This data is commonly read from a point-of-sale terminal when the consumer's card is swiped. To learn more about this data, please see ISO standard 7813.
CVC2/CVV2/CID	These refer to the non-embossed numbers (either three or four digits) found printed on the plastic payment card. The values are intended to help mail order, e-commerce, or other card-not-present merchants to verify that the purchaser has possession of the card when placing an order. The values are not intended for retailers or card-present merchants to collect.
PIN/PIN block	The PIN is the actual unencrypted PIN known by the cardholder. The PIN block is the encrypted value generated by a certified PIN pad when a consumer types the PIN into the device. These devices are usually found attached to point of sale (POS) systems or automated teller machines (ATMs).

Understanding the Scope of PCI

In an attempt to demystify the scope of PCI, and having understood the applicability of PCI to the types of data being protected, the following clearly states how to determine whether a system should be in or out of scope for PCI DSS compliance.

All systems and networks that store, process, or transmit cardholder information must be in compliance with the PCI DSS.

It is important to remember that "cardholder information" refers to the data elements defined in the PCI Applicability section. Determining scope is not always straightforward, even though the terms of this scope statement are actually quite clear. Here is an example to help determine scope:

If there is a system on a network (say it has IP address 10.10.10.25) that *does not* store, process, or transmit card data, but that system is able to reach machines that do store, process, or transmit cardholder data, then the system is *in scope*. If the server on 10.10.10.0/24 is unable to see or connect such that no user on the system could traverse to any systems that store, process, or transmit card data, then the system is *out of scope*.

Sound easy?

Although this may seem simple, there are complexities related to determining scope in some situations. The reader is strongly advised not to try to make determinations on complex scope issues without consulting with a PCI Qualified Security Assessor (QSA). To find a QSA near you, contact PSC at the number on the last page of this paper.

Transport Encrypted Cardholder Data

So now that we understand the basics of what cardholder data is based on the preceding PCI Applicability table and discussion, let's consider the impact if the data is transmitted encrypted and ask the question: Is encrypted cardholder data still considered cardholder data that must be protected according to the PCI DSS?

There are several reasons that this is an extremely important question when considering network design. As we all know, the scope of the PCI DSS requirements related to the network domain is based on LAN segments that host servers that store and process cardholder data, as well as the segments where cardholder data is transmitted. That said, if encrypted cardholder data is not in scope for PCI DSS, then we may have discovered another clue that can be used to reduce the overall scope of compliance across network segments.

Let's see how the PCI Security Standards Council weighs in on this topic.

> Is encrypted cardholder data considered cardholder data that must be protected in accordance with PCI DSS?
>
> The [PCI Security Standards] Council will be developing more formal guidance around this topic, leveraging information that is received through the various channels of the [PCI] DSS lifecycle feedback process. Until the Council provides further guidance, the following should be taken into consideration regarding encrypted cardholder data.
>
> Encryption solutions are only as good as the industry-approved algorithms and key management practices used, including security controls surrounding the encryption/decryption keys ("Keys"). If Keys are left unprotected and accessible, anyone can decrypt the data. The [PCI] DSS has specific encryption key management controls ([PCI] DSS 3.5 and 3.6), however, other [PCI] DSS controls such as firewalls, user access controls, vulnerability management, scanning, logging, and application security provide additional layers of security to prevent malicious users from gaining privileged access to networks or cardholder data environments that may grant them access to Keys. It is for this reason that encrypted cardholder data is in scope for PCI DSS.
>
> However, encrypted data may be deemed out of scope if, and only if, it has been validated that the entity that possesses encrypted cardholder data does not have the means to decrypt it. Any technological implementation or vendor solution should be validated to ensure both physical and logical controls are in place in accordance with industry best practices, prohibiting the entity, or malicious users that may gain access to the entity's environment, from obtaining access to Keys.
>
> Furthermore, service providers or vendors that provide encryption solutions to merchants who have administrative access and controls to Keys along with the management of termination points for encryption to process transactions,

are required to demonstrate physical and logical controls to protect cryptographic keys in accordance with industry best practices (such as NIST referenced in PCI DSS requirement 3.6), along with full compliance with PCI DSS.

Merchants should ensure that their solution providers who provide key management services and/or act as the point of encryption/decryption are in compliance with PCI DSS. Merchants should be aware that encryption solutions most likely do not remove them completely from PCI DSS. Examples of where DSS would still be applicable include usage policies, agreements with service providers that deploy payment solutions, physical protection of payment assets and any legacy data and processes (such as billing, loyalty, marketing databases) within the merchant's environment that may still store, process, or transmit clear text cardholder data, as that would remain in scope for PCI DSS. [2]

Network Segmentation and Scope

Now that we have an understanding about what cardholder data is, let's consider the topic of network segmentation.

The concept of segmenting a local area network so as to reduce the scope of compliance with the PCI DSS survived in version 1.2.1. That said, the terms and guidance on segmentation were completely rewritten by the Standards Council. Let's take a look at the actual guidance.

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a "flat network"), the entire network is in scope for the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, routers with strong access control lists, or other technology that restricts access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing, or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows, via a dataflow diagram, helps us fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and will be used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon such things as a given network's configuration, the technologies deployed, and other controls that may be implemented. [3]

Here is a summary of the key differences between this statement and prior guidance on network segmentation from earlier versions of the PCI DSS.

- Changed wording to state that network segmentation is not a requirement but it can help in: reducing scope and cost of the assessment, reducing cost and difficulty of maintaining PCI DSS controls, and reducing the risk to the organization.

[2] "Is encrypted cardholder data considered cardholder data that must be protected in accordance with PCI DSS?" PCI Security Standards Council FAQ Article #10359. 1/22/2010

[3] "Payment Card Industry Data Security Standard" Payment Card Industry Security Standards Council. Version 1.2.1. July 2009. Page 6.

- Clarifies that "Without adequate network segmentation (sometimes called a 'flat network'), the entire network is in scope of the PCI DSS assessment."
- Recommends "Documenting cardholder data flows via a dataflow diagram [as this] helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment."
- States that if network segmentation is in place to reduce scope, "the assessor must verify that the segmentation is adequate to reduce the scope of the assessment."
- References new Appendix F - PCI DSS Reviews − Scoping and Selecting Samples, which provides information and examples of the effect of scoping during a PCI DSS assessment.
- Eliminated consideration explanations of when a merchant and/or service provider would be required to undergo an annual onsite review.

Now that you have a sound understanding of PCI Applicability, rules related to scoping, whether or not encrypted cardholder data is still cardholder data that requires protection under PCI DSS, and you understand network segmentation, let's put your knowledge to the test.

Situation 1: An entity uses SSL to protect form data that is posted at an internal call center website. The entity uses SSLv3 certificates obtained from a recognized, public certificate authority and supports only encryption with a minimum of 128 bit key length. The data is transmitted across network segment A, through segment B and to a server on segment C. Assume that each network segment is an isolated VLAN protected by firewalls. Given what you read above, are segments A and B in scope for the full requirements of the PCI DSS?

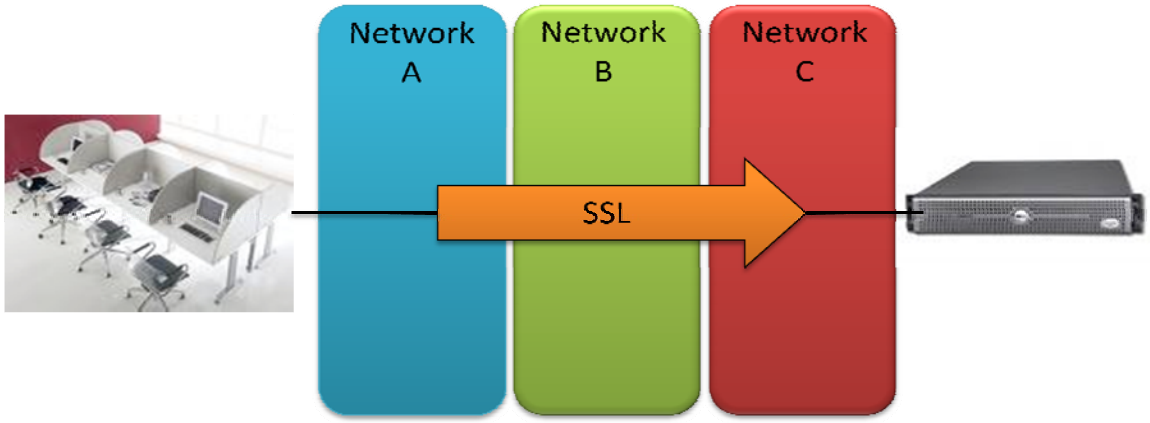

Figure 1: Use of SSL/TLS (Situation 1)

Situation 2: The same entity changes its encryption strategy to use RSA with a 2048 bit encryption key. In essence, a small browser side script in the call center Web application encrypts the cardholder data using the public portion of a Pretty Good Privacy (PGP) key. The private portion of the PGP key is stored in a hardware security module (HSM) that is in a server hosted on segment C. Full key management procedures that would be in full compliance with sections 3.5 and 3.6 of the PCI DSS exist for managing the storage and protection of the private key on the server. The private key does not exist outside of the HSM that stores the key. Is network segment B out of scope for the full requirements of the PCI DSS, assuming that proper network segmentation controls are found to be in place?

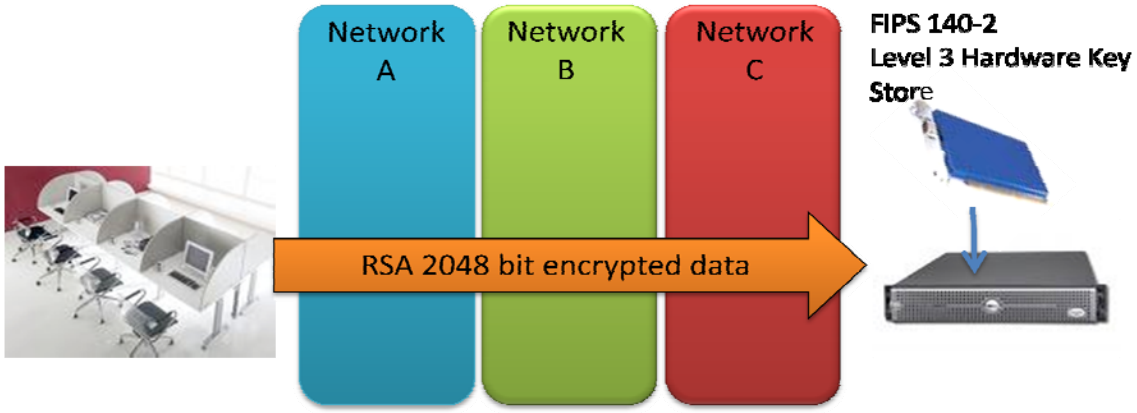

Figure 2: Private key in a hardware security module (Situation 2)

If you answered yes to both of these situations, then you might want to think about taking a class and a test to become a PCI DSS QSA. The answers to both are yes. The secure, managed storage and possession of the encryption key makes all the difference in the world, even inside a corporate network. Now I must point out that we are assuming that the network is appropriately segmented to restrict traffic, and in the second example, that a minimum of a Federal Information Processing Standard (FIPS 140-2 Level 3) hardware key storage device is being used. An internal PCI card version is illustrated. These devices provide secure storage of the private/secret cryptographic keys, and allow software applications to use standard cryptographic programming interfaces to securely access data elements. In this example, the inbound data would remain encrypted until the payment application selects to decrypt the cardholder data and pass it to the processor.

Combining firewall technology with network access controls can facilitate strong network segmentation. The Juniper Networks® SRX Series Services Gateways, either standalone or when coupled with the Juniper Networks Unified Access Control solution, can be used to enforce identity-based segmentation rules such that user access is sandboxed, and only user access with a specific need-to-know level of authorization can gain access to protected resources.

Network Security Domains

As mentioned earlier in the introduction of the 12 principles, only a subset focuses on the data network. The following is a review of the PCI DSS principles and high-level requirements that apply to the network. The actual requirements will be examined later.

Table 3: PCI DSS Network Principles and High-Level Requirements

Requirement 1: Install and maintain a firewall configuration to protect data.	Firewalls are computer devices that control computer traffic allowed between a company's *network (internal) and untrusted networks (external)*, as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from *untrusted networks*, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from *untrusted networks* can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for

any computer network.

Notice how in the definition of this requirement, the PCI DSS is now using the concept of an "untrusted network" instead of referencing the public Internet. This concept is important to keep in mind. *Even an internal business network can be considered untrusted.*

Requirement 2:

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

This section is about much more than just changing a few default passwords. It focuses on the security of the actual devices on the network. Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information. Although most of the requirements in this section apply to servers, several pertain to setup and configuration of network components.

Requirement 4:

Encrypt transmission of cardholder data across open, public networks.

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Wrongly configured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Most network architects feel that the requirements in this section are easily met by using SSL, but there are a few important areas of concern, especially in the area of wireless devices.

Requirement 5:

Use and regularly update antivirus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and trojans—enters the network during many business-approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Antivirus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

Although the subsections of this requirement are for host-based defenses on servers and systems within the cardholder data environment, network-based solutions can be effective when used in combination with host-based systems. The Juniper Networks SRX Series for the branch with integrated antivirus provides increased security for network and mobile devices by blocking viruses, worms, trojans, and other malware from entering the network.

Requirement 6:

Develop and maintain secure systems and applications.

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, *which must be installed by the entities that manage the systems***.** All *critical systems* must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Most of the requirements in this section deal with software development, change management, and application security. That said, a few of the requirements here must be considered and may have a significant impact on the network. They both involve patching system components and keeping up-to-date on patches.

Requirement 7:

Restrict access to cardholder data by business need-to-know

In prior versions of this standard, the basic message was that an organization must have a process of defining permissions to access data based on job descriptions. And, that there is a process for approving access to computer resources based on these permissions. In the current version of the standard, the requirement about having an automated access control system was added. For many companies, this means that applications and system-level access are controlled by an automated access control

system. For small environments, this may be achieved by correctly configuring pluggable authentication modules (PAMs) in a Linux server. More advanced sites will address this requirement using RADIUS and LDAP directory servers.

Requirement 8:

Assign a unique ID to each person with computer access.

This is one of my favorite requirements that does not say what it means. Instead, they could have said, "Establish and enforce clear password policies," but no, they stuck with user IDs.

This requirement covers a multitude of areas that are well beyond the network and network access controls. In this paper, we focus in on access to network segments and not individual hosts or applications. That said, the reader is advised that there is a whole, vast area of these access controls that must be represented by applications and host operating systems in order to achieve compliance with these requirements. The network is only one small component of the solution.

Requirement 10:

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

Logging mechanisms and the ability to track user activities are critical *in preventing, detecting, or minimizing the impact of a data compromise.* The presence of logs in all environments allows thorough tracking, *alerting,* and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

To most network engineering specialists, this requirement seems rather benign. Packet analyzers and bandwidth monitors have been used for quite a while. But: *If a packet analyzer captures deep packet data and stores the data for offline analysis, is this a system that stores cardholder data? And, lot's of it?* If you think the answer is no, go back and reread the earlier sections. Yes, this is a significant problem given the fact that there is no requirement to encrypt communications on internal networks. Ouch! *The sections in Requirement 10 must be considered with extreme care.* In one company, a deep packet analyzer was attached to the core switches that could hold up to 20 terabytes of packet data for analysis. No one in the security department ever considered that this tool could be attacked and compromised through the application's Web reporting interface, until the interface was made public by accident.

Requirement 11:

Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to *ensure that security controls continue to reflect a changing environment.*

This requirement covers the routine testing of security controls and must be implemented to verify that network controls are verified on a routine basis. The recommended frequency for these tests ranges from daily to annual.

Detailed Review and Approach

This section provides a detailed review of each requirement that relates to network security controls. Each subsection covers the requirements in detail, provides important interpretive information, and illustrates a solution using products from the Juniper Networks product line.

It is important to point out that Juniper Networks security solutions were chosen for these illustrations because they represent a diverse set of offerings that support the range from small to very large installations, while suitably addressing the spirit of PCI. PSC as a QSA maintains our full independence from all hardware companies and accepts no commission or payment on the purchase of any hardware from Juniper Networks or other companies. Our intent is to provide illustrative solutions.

Requirement 1: Install and Maintain a Working Firewall

This requirement covers perimeter security requirements for firewalls and border routers. The first section mandates the establishment of a configuration standard. The later sections provide detailed guidance for perimeter firewalls, demilitarized zone firewalls (DMZs), and routers.

It's important to take a moment and understand the lineage of the PCI DSS. This standard was first conceived in late 1998 by a team at Visa USA and was first published as the Cardholder Information Security Program (CISP)

standard. Back then, the primary security threat was Internet vulnerabilities against electronic commerce sites and Web technologies. Although these threats are still very real and present, the threats now include traditional retailers who implement IP technologies to communicate with their stores. Unfortunately, the firewall model base in the PCI DSS hasn't kept up with this changing threat and still the legacy of e-commerce architecture remains. That said, retailers and traditional companies may need to consider interpreting the requirements and working with a qualified security assessor (QSA) who understands retail systems to document the controls.

Illustrated Controls

Following is a look at the specifics of Requirement 1. This section illustrates the types of solutions that can be implemented. As noted before, makes and models of Juniper Networks equipment will be used to further illustrate the control.

Table 4: Requirement 1 Specifics

1.1 Establish firewall and router configuration standards that include the following:	All of the subsections in this section describe the contents of a configuration standard, as well as details about perimeter and DMZ firewalls and the way that firewalls and routers are managed.
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall and router configurations	This is a section of the documented standard that describes a process for approving and testing all new external network connections and changes to firewall and router configurations. *And yes, this means network engineers can't just make any change they would like to firewall and router rules.* This requirement means that firewall changes should go through a review and a change management process. Later, in the PCI DSS, sections 6.3 and 6.5 describe change control and change management processes. Some organizations choose to integrate their network change process with the IT system's change process. If your organization does not do this, be sure to document a clear process at this point.
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	This requirement seems very simple and straightforward, but the number of organizations that don't keep a diagram is amazing. This diagram does not need to be printed out. It can be kept in a drawing application. The configuration standard will need to mandate that this diagram is kept current, and you will need to show an auditor the diagram.
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	There are still several organizations that don't have firewalls. This requirement mandates that the organization's configuration standard must require that firewalls be present at each Internet connection and between any DMZ and internal network zone.

Unfortunately, section 1.1.3 is another legacy requirement that may not fit some of the traditional retailers. Suffice it to say at this point, if a retailer chooses to create a secure network segment where retail processing PCI data is stored, a firewall needs to protect that retail segment. This is a great way to reduce the overall scope for PCI compliance in a very large organization.

1.1.4 Description of groups, roles, and responsibilities for logical management of network components	The configuration standard must describe the individuals and groups responsible for management of network components. This section must also identify the manager responsible for approving all configuration changes to firewalls.
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation	The configuration standard should list all of the ports and services necessary for the business. The next two sections require documented justification for any service (other than HTTP, HTTPS, SSH, or VPN) that may be configured in the firewall. These justifications can be included with the list of services or referenced to a change

of security features implemented for those protocols considered to be insecure	management system.
1.1.6 Requirement to review firewall and router rule sets at least every six months	There are two parts to this requirement. The first states that the configuration standard must mandate that reviews of *firewall and router rule sets* be established at least every six months. In order to review if rule sets are appropriate, one must have something to compare the rules with. This is where the prior port list and change documentation comes in. The six-month review of the rules should compare what is actually configured in the firewalls with the documented configuration standard list and approved change documents. This review must be documented to provide evidence for the second part of the requirement. The second part of 1.1.8 requires the auditor to examine the evidence from a six-month review. Most good PCI auditors will be looking to see how the review was performed and whether there was a standard to compare against.

JUNIPER NETWORKS All Juniper firewalls and secure routers have the ability to export reports from firewall configurations to facilitate this review process. One key feature of SRX Series products is that a network engineer can include a comment with the policies. One suggestion would be to include the name of the business and a reference to the justification and change documents that support this rule. When the report is exported, this reference can be quickly cross-referenced and checked. Juniper firewalls also provide routing services. Juniper Networks SRX Series Services Gateways could be installed to protect large networks of retail stores and the reports generated from these routers included in the review.

Suggestion: If your company is using a work tracking or trouble tracking system, make a note in that system that you've completed a quarterly review. For that matter, a quick trick is to record four trouble tickets in advance with dates listed in each quarter to remind your administrators to perform the review. Once the review is done, these tickets provide wonderful evidence that the review has been completed.

1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	Now that all firewall rules are documented, the requirement says that firewalls must be built and implemented. JUNIPER NETWORKS High-end SRX Series products for the data center can be configured to protect corporate sites, while branch SRX Series products can be used to protect individual retail stores. These SRX Series devices can also be configured, alongside the Juniper Networks AX411 Wireless LAN Access Point, to provide in-store wireless services. The SRX Series devices, when integrated within Unified Access Control as enforcement points, can dynamically restrict access to untrusted networks based on user identity and role.

Requirement 1.2 was updated a few years ago to include the term "untrusted." This is actually an important note, and large retailers and legacy businesses need to pay attention to it. *Consider this: If a network of 1,300 retail stores is connected using a DSL network, is this an untrusted network even though you use a point-to-point VPN? How much can you trust an MPLS network? Does your company want to take the risk of not having a firewall on the corporate side of this network? Is a large router sufficient to protect against attacks?*

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	This subsection has two unique components. The first component of the requirement is to design and implement inbound firewall rules that limit traffic to that which is necessary for the cardholder environment. Many companies stop with this and believe that their systems are now protected. Unfortunately, missing the second part of this requirement has resulted in open security vulnerabilities that permit an attacker to export stolen data. Therefore, it is extremely important to model acceptable outbound traffic and implement strong access lists for internal servers accessing the outside Internet. Think about it, *should your database server be opening a port 80 connection to a server in China?* Juniper Networks SRX Series Services Gateways, or the SRX Series in conjunction with UAC, can dynamically restrict inbound traffic to the cardholder data environment based on the user's identity, location, and device security state. Standalone SRX Series or the SRX Series in conjuction with UAC can also limit outbound traffic from within the cardholder data environment. Also, UAC when combined with the standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances or with the IPS capabilities of the SRX Series can ensure that specific application access is restricted while a user is within the cardholder data environment.
1.2.2 Secure and synchronize router configuration files.	Basically this says that any startup, saved configuration file must be the same configuration file that is actually running on the firewall and routers. We don't want a router failing and then rebooting with an old configuration.

The Juniper firewall configuration files can be extracted to a secure backup device. It is recommended that these files be exported after any major network configuration change. After the configuration files are exported, take openssl or a similar tool to calculate a Message Digest 5 (MD5) hash for each configuration file. Save this calculated hash in a separate location. Be sure to write in your configuration standard that you'll calculate the MD5 hash again prior to loading a configuration file. Now, your configuration files are secure. A file integrity tool would work, but would be overkill. If the network engineer has a better idea or doesn't want to calculate a signature for each of the files, then whatever method is used must be equivalent to at least this. As a side note, Juniper Networks STRM Series Security Threat Response Managers provide a set of reports that can assist with this.

1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	This requirement was part of the old 1.3.8 of the PCI DSS v 1.1. The requirement is to have a firewall between *any* wireless network and the cardholder data environment. This is one of the few sections where the PCI DSS mandates a level of network segmentation. If you need to review the guidance for segmenting a network, go back to the prior section on that topic. Also, the word "any" means exactly that… any wireless network, regardless of whether cardholder data passes through the wireless network or not.

A real problem exists for the large retailer who uses wireless inventory devices for markup and markdown work in the store. These devices must be able to open a connection to the in-store controller to update prices on merchandise. As such, a separate firewall may be difficult. This is an area where the AX411 Wireless LAN Access Point, fully managed by Juniper Networks SRX Series Services Gateways for the branch, might help. The nice part is that real firewall policies can be created on the branch SRX Series that will control traffic from these wireless LAN access point devices. The wireless controller side of the branch SRX Series is built into the SRX Series platform, so no separate wireless policy management is required. For large retail networks, Juniper Networks Unified Access Control can be used to dynamically apply these policies in conjunction with the AX411 and the SRX Series as policy enforcement points for the branch devices as well.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	This requirement and its subsections underwent significant changes in the PCI DSS v 1.2.1. In essence, the requirement mandates that there be no direct (inbound or outbound) access between the Internet and any system component in the internal cardholder data environment. As a note, all design decisions related to how these requirements are met must also be documented in the appropriate section of the firewall configuration standard.
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	This is the first of several requirements mandating that a DMZ be implemented for any inbound and outbound traffic from the internal cardholder data environment. Most people believe this requirement applies to Internet e-commerce sites, which it does, and more. This requirement can impact inbound mail, FTP of catalog images from suppliers, and other important business traffic for non e-commerce companies. That said, this requirement also covers outbound traffic. We'll visit the outbound traffic component later in the sub requirements of this section, where the function of the DMZ is further explained related to outbound traffic from the internal cardholder data environment.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	This requirement provides that any inbound traffic from the Internet must be routed to IP addresses that are within a DMZ. This means that the internal e-mail server that is on a backend network must reside in a DMZ.
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	Here is the requirement that further clarifies the requirement in section 1.3.1. Limiting inbound traffic between the Internet and cardholder data environment to servers on a DMZ is basically the same thing that was required in 1.3.2. The major issue with this requirement is that it mandates that there can be no direct connections outbound between servers within the cardholder data environment and the public Internet. In essence, this means that either a proxy or reverse Network Address Translation (NAT) be used within the DMZ. In essence, an internal server that is going to address a URL like https://transaction.securepaymentprocessor.com *must address* an IP address that is specified on the DMZ and cannot open a direct connection to this "authorized" URL.
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	Yes. This is a bit of renumbering of old requirements. This is our anti-spoofing requirement that says internal IP addresses should not be source IP addresses on outside interfaces.
1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	Just in case you didn't understand the significance of requirements 1.3.1 and 1.3.3 related to outbound traffic, the PCI DSS v 1.2.1 restates the requirement discussed in 1.3.3 one more time.

Let's pause and think about a case. Let's assume that a large retailer has a firewall installed to isolate a set of network segments (let's call it a "Zone") where the retail network router is connected and retail polling server, transaction switches, batch processors, and a data vault storing live credit cards are installed. The polling server converts cards to surrogates and sends only surrogates to loss prevention (LP) and sales audit systems. The LP and sales audit systems are on a network outside the SRX Series. *Now, if the Web and mail servers are in a DMZ, has the retailer complied with this requirement*? Yes. As a matter of fact, the retailer is in much better shape, because all of the non-PCI servers are actually in a DMZ! Think about it. [4]

[4] To learn more about credit card surrogates, see: Arnold, Tom. Credit Card Information Surrogate "A Method and System for using surrogates to integrate PCI-level security for legacy information systems." A White Paper. March 2007

Standalone SRX Series gateways, or the SRX Series in conjunction with UAC, can limit access based on a number of factors. These include user identity inbound and outbound access to the cardholder data environment, as well as limiting traffic to and from the cardholder data environment to only authorized individuals attempting access from secure locations. The STRM Series has several reports that help monitor compliance, including traffic by protocol and Internet to DMZ traffic.

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	This is a clear requirement that helps describe how the PCI DSS defines a minimum requirement for a firewall.
1.3.7 Place the database in an internal network zone, segregated from the DMZ.	"The database" as specified here should be interpreted to be any database that is a database within the cardholder data environment. So, if you have a database that stores transactions and lives with the Internet e-commerce Web server, then that database *must* be on the other side of the DMZ/internal firewall.
1.3.8 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).	NAT and PAT are standard features on most firewalls. SRX Series Services Gateways support both NAT and PAT.
1.4 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	This requirement mandates that personal firewall software be installed on any mobile or remote laptops that are capable of connecting to the public Internet on their own, as well as connecting to the company network. A couple of points to highlight: (1) *Many network engineers think this deals with split tunneling. It doesn't*. Also, in this paper, there has been reference to a Zone that is secured by a large firewall where all of the cardholder data is processed or stored; (2) *This applies only to laptops that can connect to the Zone*. If you need help with this one, contact a QSA who knows retail. Some access control systems, like Juniper's UAC agent or Juniper Networks Junos® Pulse used in conjunction with UAC, will help guarantee that personal firewalls are operational before authorizing a remote or local network connection. The full, 802.1X-enabled UAC agent also includes a personal firewall. This goes a long way toward protecting systems while they're connected, but a potential problem remains if the user is capable of shutting off the firewall during local use and then encounters malicious software prior to opening the connection. UAC solves this problem for local use, while Juniper Networks SA Series SSL VPN Appliances can address this for remote usage. Both the UAC solution and SA Series SSL VPN Appliances include a host checking capability, which determines if the endpoint device meets a baseline of security and access policy that has been predetermined by the enterprise *before the device is allowed connection or access to the network*. These checks include checking to see if a device's personal firewall is operational. In addition, the STRM Series provides reports on DMZ traffic screening to help facilitate controls over this area.

Criteria for Selecting Solutions

A few thoughts when selecting a technology solution for PCI compliance:

- When selecting firewall technologies, consider choosing one that fully integrates with other network security components. This will allow the retailer to have a single management console to control each component.
- There is nothing called a "PCI Compliant Product." So, if a sales representative of one of these systems claims that you'll be PCI compliant if you just use their product, call someone else.
- Never buy a product from your PCI Qualified Security Assessor. Does it make sense that this person would sell you a product and then audit his or her own product?

Requirement 2: Always Change Vendor-Supplied Defaults

This requirement wants organizations to have their own unique configuration standard for systems and servers that store, process, or transmit cardholder data.

Illustrated Controls

Following is a look at requirements in section 2. As with the prior section, an illustrated control and description of the types of solutions that can be implemented to meet the requirements are provided.

It is very important to note that these controls will be looked at from the perspective of the network components—not from application or server perspectives. Readers are encouraged to locate a qualified security assessor who is familiar with their particular business to obtain more detailed guidance.

Table 5: Requirement 2 Specifics

2.1 Always change vendor-supplied defaults such as passwords and simple network management protocol (SNMP) community strings, and eliminate unnecessary accounts before installing a system on the network.	This applies to the network components as well as all system components. Most hardware will be preconfigured with settings that allow the product to start and be used. Hardware companies rarely intend for network components to be used with their default configurations.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure that wireless device security settings are enabled for strong encryption technology for authentication and transmission.	A great tee shirt at a conference last year read: *"Social Engineering Specialist"* on the front, and then on the back: *"Because there's no patch for human stupidity."* This requirement is a clear duplicate of the prior one. The only reason that it's here is simply that people somehow believe that wireless networks are special and the rules don't apply to them. Change the settings on *all* network devices! One more thing. The PCI DSS v 1.2.1 testing criterion for this requirement eliminates all references to Wired Equivalent Privacy (WEP) security controls. *WEP is now dead.* Any company using WEP encryption to protect its wireless network will automatically *not be compliant* with the PCI DSS. Juniper Networks AX411 Wireless LAN Access Point, fully managed by the branch SRX Series platforms, can be configured with Wi-Fi Protected Access 2 (WPA2), providing strong wireless encryption between wireless LAN clients and external AX411 wireless LAN access points.
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.	A commonly asked question is: *"Why does this requirement exist or what is it protecting?"* The answer is quite simple and frequently network engineers are fully aware of it. Protocols like Telnet pass their authentication credentials in the clear. If someone comes onto your poorly protected wireless network, all they need to do is begin sniffing. "*Ah, wait a minute*," the network administrator says. *"You can't sniff a switched network."* If anyone reading this paper truly believes this, then you

	better make certain and change all the defaults. Wireless networks can easily be sniffed and administrative usernames and passwords to anything can be captured. Don't make it easy on the bad guys, especially if they're already inside. JUNIPER NETWORKS The security and network equipment from Juniper fully support SSH and SSL to protect administrative sessions.

Criteria for Selecting Solutions

A few thoughts when selecting a technology solution for PCI compliance:

- Remember, this requirement is about all vendor defaults, not just passwords.
- When selecting network technologies, make certain they support encrypted administrative sessions.
- Almost every default setting is available on Google. When someone says that there is no need to change that default, just ask if they changed the keys to their house after they moved in.

Requirement 4: Encrypt Transmission of Cardholder Data

Remember, the remainder of Requirement 2 and all of Requirement 3 are being skipped, because this paper deals with those portions of PCI DSS that apply to network engineers. Beyond the actual cardholder data, one of the key things that the provisions in this section protect is the passing of authentication credentials. Or so the authors of PCI DSS would like to think. Unfortunately, since the writing of this version, several new vulnerabilities have been uncovered that are still not covered by the PCI DSS.

Requirement 4 covers the protection of cardholder data (and other things) while in transit. The core requirement covers the transmission of data across public networks. Transport encryption is not a requirement for internal local area networks, and this presents special challenges. After explaining the vulnerability and reason that administrators need to use encryption for all non-console administrative traffic, the authors of PCI DSS just threw this all aside. If you're in major retail, you'll understand when you consider the traffic that goes between the master and slave registers in a store or the traffic between registers and the store controller. Every time a credit card is swiped, the most sensitive data moves (in clear text) between devices on the network. According to the folks at the card associations, there would be too much push back if they adopted a requirement to protect the traffic with encryption, so they insist that intrusion detection systems be used. This will be discussed more in Requirement 11. If a merchant has the capability to encrypt this traffic, just do it.

Illustrated Controls

Following is a look at requirements within Requirement 4. This section will provide an illustrated control and description of the types of solutions that can be implemented to meet the requirements.

Table 6: Requirement 4 Specifics

4.1 Use strong cryptography and security protocols, such as secure sockets layer SSL/TLS and IPsec, to safeguard sensitive cardholder data during transmission over open, public networks.	This requirement was included only because, in many companies, network engineers are asked to acquire SSL certificates to protect the transmission of data. It is most important to note that only strong SSL is authorized, meaning SSL v3 or better. The scope of this requirement is limited to transmissions over open, public networks. This means that there is no issue if the traffic between a cash register and in-store controller is left unprotected. Now, consider this problem when coupled with the issue illustrated in the next requirement.  One key tool that can be used here is an SSL VPN for remote devices in the field as well as for remote, mobile users. Juniper Networks SA Series SSL VPN Appliances provide a remote SSL VPN access solution. Also, Juniper Networks SRX Series Services Gateways (standalone or in conjunction with UAC) apply strong cryptography and security protocols—such as a secure IPsec tunnel and tunneled Extensible Authentication Protocol (EAP) types—to data transmitted from a client endpoint to the appropriate networked access or security device.
4.1.1 Ensure that wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. *For new wireless implementations, it was prohibited to implement WEP after March 31, 2009. For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*	This requirement provides basic guidance for transport security over wireless networks. The requirement is specifically intended for 802.11x wireless networks that *transmit cardholder data*. Unfortunately, the challenge with in-store wireless networks is not limited to those devices that transmit consumer payment information. In most retail environments, there are a number of different devices that include wireless price checkers, handheld inventory sets, and connected systems on pushcarts used to mark price changes. Because this requirement has been narrowly scoped in two ways (the limit on transmitting card data and the limit based on use of wireless technology), many of these other devices go unsecured and leave major retailers wide open for attack. Recall the earlier discussion on transport security and the issue that traffic between the registers and other in-store or in-network systems is not required to be encrypted. This makes the attack vector quite easy actually. Set up a wireless eavesdropping device and dump network traffic to a small drive. Capture all of the network packets. Examine these packets for passwords. The attacker just might get lucky and see the password of a corporate maintenance administrator. Capture the packets between the registers and other devices during business hours. This should yield full credit card track data, PIN blocks, consumer names, and full credit card data. The most significant change in the PCI DSS from version 1.1 to 1.2.1 is that the use of WEP must be completely phased out by June 30, 2010.  Juniper Networks AX411 Wireless LAN Access Point, fully managed by branch SRX Series devices, supports a rich set of 802.11i wireless encryption that encrypts cardholder information across simple, wireless LAN retail branch environments. Furthermore, Juniper Networks Odyssey Access Client, Juniper's powerful 802.1X supplicant, ensures that any data—including cardholder data—transmitted over a wireless network uses robust, government-approved encryption to protect credentials and transmitted data.
4.2 Never send unencrypted PANs by end user messaging technologies	The prohibition on sending unencrypted PANs via e-mail or other end user messaging technologies is rarely a network architecture concern, except for some of

(for example, e-mail, instant messaging, chat).	the new security technologies that are just becoming available.  SRX Series Services Gateways and IDP Series Intrusion Detection and Prevention Appliances have the capability to identify unencrypted transmission of confidential cardholder data across multiple protocols. The SRX Series can redirect questionable traffic based on policy for additional inspection of suspect traffic.

Criteria for Selecting Solutions

A few considerations when selecting a technology solution for PCI compliance:

- Perform a risk analysis about what is really at stake for your business. PCI cares about protecting a very limited amount of data during transmission.
- Consider the technology present in your field locations and the types of security controls protecting it.
- Use the proper form of transport encryption and use it liberally.
- Don't cut corners in this area. If you want your POS software vendor to use TLS or SSL to protect communications between registers and controls, then have them do it. If they refuse, find another vendor.
- Make absolutely certain they support encrypted administrative sessions.
- It's amazing how many people ask: *Do I really need to turn encryption on? Won't it be slower?* As soon as a retailer says that to a PSC auditor, they go on the cash-basis only shopping list. Unfortunately, this list is pretty long.
- If you can't protect the transmission of cardholder data between devices, you must do everything to protect access to the network.

SRX Series Services Gateways for the branch are suitable for stores, since they can perform double duty as a router, wireless access point, and fully functional firewall. Each network port, including the wireless, can be separately controlled or switched off. Further, policies can be established that will limit the introduction of foreign devices. When coupled with application access control platforms, it may be possible to reliably detect rogue devices. And when coupled with the Juniper Networks Unified Access Control solution, the SRX Series gateways become identity- and role-enabled, allowing for dynamic access control based on a user's identity and role.

Requirement 5: Use and Regularly Update Antivirus Software or Programs

Classically, PCI DSS Requirement 5 describes requirements for hosts to operate antivirus and anti-malware software. Although this document is specifically for network engineers, I've chosen to include a small section covering this, since several network appliances are now capable of scanning network traffic for malicious software, and are capable of enforcing policies to ensure that antivirus is activated on workstations prior to granting access. All of these approaches are excellent supplements to the base requirements described in PCI DSS section 5, but are not replacements for the fact that production servers must be protected by antivirus, anti-malware software.

SRX Series Services Gateways for the branch support integrated antivirus to act as a first line of defense against propagation of viruses, spyware, trojans, and other malware. Also, SRX Series with IPS and standalone IDP Series devices block many spyware, trojans, and other malicious software. UAC ensures that antivirus software is up-to-date and operational prior to access or connection, and that devices meet security policies before they access the network. It also checks to ensure that antivirus and other anti-malware software is enabled throughout the network session. UAC also includes Enhanced Endpoint Security (EES), which checks devices before connection for spyware, keyloggers, etc. This latter defense is extremely important when mobile or employee-owned systems have remote access to the network.

PSC

Requirement 6: Develop and Maintain Secure Systems

Most of Requirement 6 focuses on developing and deploying secure code for applications, but there are a couple of requirements that are important for the network architect and security engineer to understand.

Illustrated Controls

Following is a review of each requirement in section 6.

Table 7: Requirement 6 Specifics

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritizing patch installations. For example, by prioritizing critical infrastructure (public-facing devices and systems, databases) higher than less critical internal devices, one could ensure that high priority systems and devices are addressed within one month, and less critical devices and systems are addressed within three months.	This requirement has two sub requirements that are relevant for network devices. Subsection 6.1a stresses the importance of keeping software and firmware up-to-date. A network firewall is basically a dedicated hardware device that runs software, and, as with any software, there may be defects or opportunities for improvements. It is important for all network components operating in the Zone (environment where card data is stored, processed, or transmitted) to be kept up-to-date. Subsection 6.1b of this section mandates that any critical security patches be tested and deployed within 30 days of release. JUNIPER NETWORKS Juniper Networks Unified Access Control can help achieve compliance with this requirement. UAC not only checks every endpoint device for the latest application, OS, and other related patches prior to network connection and access, but throughout the network session as well. UAC also ensures that patches are installed in a timely manner prior to allowing a device network access.
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	This requirement covers several areas beyond the network, but is very important to the network and security engineer. In essence, the requirement mandates that a process be in place that will identify new security threats and watch for patches and solutions. JUNIPER NETWORKS UAC automatically validates that antivirus, anti-spyware, and anti-malware signatures and other files are up- to-date. So, when a device's antivirus, anti-spyware, and anti-malware software and patches are being checked by UAC prior to or during network access, the enterprise can be assured that UAC is checking anti-malware and patches to the latest, most up-to-date software from manufacturers.
6.4 Follow change control procedures for all changes to system components. The procedures must include the following: 6.4.1 Documentation of impact 6.4.2 Management sign-off 6.4.3 Testing of operational functionality 6.4.4 Back-out procedures	For this version of the PCI DSS review, I've chosen to include PCI DSS section 6.4 and references to the appropriate subsections. The elements of this section present a unique problem for the network engineer. Although documentation of impact, management sign-off, and having a back-out plan are really nothing new when considering a change procedure, the issue arises around how a network configuration is tested. In the case of application software, most companies have separate development, test, and production environments. This is usually not the case with firewalls, access control systems, switches, and routers, yet the PCI DSS is very explicit that operational functionality must be tested prior to release. Unfortunately, there is no one-size-fits-all solution to this requirement, and each company will need to identify its own specific process related to testing of changes. I'm frequently asked: "What types of changes need to be tested?" The answer is presented in the requirement: "*all changes,*" even firewall policies, since the standard uses the term "system components."

	Although Juniper does not have a dedicated Web application firewall product, SRX Series Services Gateways with IPS or IDP Series Intrusion Detection and Prevention Appliances can partially comply with this requirement through Web application attack signatures. This helps protect environments against cross site scripting, SQL injection attacks, and other attacks. In addition, the STRM Series provides reports to summarize Web application threats, helping to meet PCI 6.5 requirements.

Criteria for Selecting Solutions

A consideration when selecting a technology solution for PCI compliance:

- Make certain that the provider of network equipment will provide regular news and information about product updates.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

As noted earlier, Requirement 7 focuses on user authorization. This is not a requirement that can be fulfilled by implementing technology alone. Any vendor that says its product fully complies with all elements of this requirement is selling snake oil. The reality is that the primary elements mandate that the business link access to computing resources (especially those that store, process, or transmit cardholder data) to job functions, implementing the *need-to-know* principle. For instance, a store manager that does not investigate individual chargeback requests does not need to see individual cardholder account numbers. Having the authorization code and transaction ID will be enough for the manager to perform his or her job. This level of analysis can frequently be a far greater task than implementing a directory server.

But enough said about the hard part; the second section of this requirement involves using an automated access control system. In essence, this would be an automated environment that encapsulates the permission policies and access rules defined during the definition step.

Illustrated Controls

Following is a review of each requirement in section 7.

Table 8: Requirement 7 Specifics

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	This is the analysis and documentation of permission policies based on job descriptions and a staff member's sensitive data need-to-know status.

7.2 Establish an access control system for system components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	This requirement includes criteria that cover a few key components of the access control system. (1) The system must cover all system components. Remember, this is the magic word for everything from network devices, system-level access for servers, and application-level access. (2) The access control system must be configured to enforce privileges assigned to individual users based on job classification and function (the results of the work from the first section). (3) The access control system must enforce a default "deny all." This last element is a requirement to implement a concept of "least privilege." As an illustration, a general user account should have no access to the corporate file server, yet a person in finance or accounting may have access to the transaction data on the finance server that supports that individual's financial accounting job. In reality, automated access control systems do a lot more than what is required in these three elements of the PCI DSS. JUNIPER NETWORKS The Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers along with UAC and SRX Series Services Gateways can be configured to enforce a full user access control environment across network, server, and applications.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Earlier, we described a network segmentation strategy where a secure segment of the network is isolated by a firewall. This secure segment is where cardholder data is stored, processed, and transmitted. The objective in building this segment was to get cardholder data off the rest of the network. This secure segment was referred to as the Zone. The reader should be thinking about the Zone while reading the requirements in this section.

The objective of this requirement is to mandate a set of minimum technologies that must be used to administer user authentication and a minimum set of password policies. There are 25 individual and unique requirements in this section of the PCI DSS that apply to all access control systems and not just the network. Assuming that we have Web servers, application servers, client/server applications, a mainframe, several UNIX boxes, and various MS Windows machines in our Zone, all of the provisions of this requirement apply to each one of these components, regardless of how we control access to the network.

This portion of the paper covers a very small subset of the impact of the requirements in this section of the PCI DSS. The reader is reminded that compliance with the provisions of this requirement *must* be demonstrated on all components, systems, and applications that store, process, or transmit cardholder data. One network device solution is never enough in this area, and to this date, there are no universal access control products that will interface with legacy environments. For instance, we haven't seen one that will assume control of Resource Access Control Facility (RACF), client/server applications (e.g., Powerbuilder or SQL*Forms), or a custom Web services application, for that matter. Also, most *modern* application developers have yet to discover the wonders of directory services and few, even running Web technologies, will interface with a universal network access control scheme.

It's worth restating that the majority of the technical issues related to this requirement can be found in applications and not the network layer. Many times, users who are not on the company network need to access applications.

Illustrated Controls

Following is a review of each requirement in section 8 that applies to network access control or access to actual network components.

Table 9: Requirement 8 Specifics

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	This requirement has been included as it is the only one that deals with the actual name of the requirement. In essence, it mandates that a unique user name be assigned to a user before allowing access to system components. Names like *Administrator, root, admin* and others are not unique.
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: • Password or passphrase • Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	There are a huge number of people who try really, really hard to overcomplicate this one. This is a procedural control that mandates using a mechanism in conjunction with the unique user name (from 8.1) that will be used to recognize the user when attempting to log in. Remember this applies to much more than network access alone. The requirement applies to application access as well. JUNIPER NETWORKS Tools like SRX Series Services Gateways, standalone or in conjunction with UAC, can help enforce the password and authentication policies on the network. Application access is the most critical component of this requirement as well.
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPsec) with individual certificates.	This is the first requirement in this section that applies to the use of technology and network access. Let's begin by taking the key components apart and understanding the meaning of the parts. *Two-factor authentication*: This is the combination of two of something you have, something you are, or something you know. Something you know is like a password. *Remote access to the network*: This means that access is not initiated from within the local area or wide area network. Access is coming from the outside. *By employees, administrators, and third parties*: This is who. The third parties are frequently outsourcing managed service companies. JUNIPER NETWORKS This is an area where several vendors have products that can facilitate the remote authentication for outside access to the network. Juniper Networks SA Series SSL VPN Appliances help facilitate and support remote two-factor access. The SA Series SSL VPN is also capable of managing access to all LAN segments and is a solution that can help facilitate various compensating controls. The capability for dealing with rogue devices is interesting. For even more granular access control and authentication, UAC can be implemented in conjunction with SA Series appliances to effectively segregate network access based on user identity; or SBR Enterprise Series Steel-Belted Radius Servers can be implemented to deliver additional AAA/RADIUS capabilities. Also, Juniper Networks Odyssey Access Client fully supports two-factor authentication. The SRX Series can enforce access control based on user, group, application/service, and zone-based segmentation policies. Those policies can be implemented and applied through the UAC solution. The SRX Series can be configured to support two-factor authentication (X.509 digital certificates, TACACS+, RADIUS, or LDAP).

The real challenge presented by PCI DSS for the large retailer is how to segment the network such that this section is limited to remote access to the Zone, and not the entire network. Assuming that the firewall protecting the Zone limits network access to only authorized services (as defined in PCI DSS Requirement 1 et al) and it can be demonstrated that an average user on the rest of the network cannot traverse into the Zone, then the scope of these requirements will be limited. That said, some of the newer technologies offered by network access control systems like Juniper Networks Unified Access Control can help limit the ability of network users and device traffic to traverse into the Zone.

8.4 Render all passwords unreadable during transmission and	*What's wrong with using Telnet to manage older switches and routers on the network?* This requirement gives you the answer! When attacking a network, the

storage on all system components using strong cryptography (defined in PCI DSS Glossary, Abbreviations, and Acronyms).	*old school* approach of doing a bit of Address Resolution Protocol (ARP) poisoning and sniffing switched networks will frequently yield administrative accounts to all of those wonderful devices when the credentials are passed in the clear. Yes, switched networks can be sniffed. It's easy! Applications aren't immune to this either. Frequently, database accounts and application service account credentials are passed in the clear. This is a very serious problem for applications. Consider using a message digest of the password and passing that.  Juniper Networks SRX Series Services Gateways can encrypt passwords on their own and also work in conjunction with UAC to encrypt all passwords.
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components	This is the password management policy section of the PCI DSS. The 16+ subsections of this requirement provide the details for password management policies. Whatever systems and applications are managing user passwords, these requirements must be complied with if the system or application is storing, processing, or transmitting cardholder data.  Use of an automated policy management tool like UAC and the new STRM Series Security Threat Response Managers from Juniper allows a user to administer these policies for systems and network components. Some other tools are frequently used in this area to include Windows Domain Controllers or LDAP directory servers.

Criteria for Selecting Solutions

A few considerations when selecting a technology solution for PCI compliance:

- Analyze the magnitude of your organization's problem related to management and authentication of users.
- Always consider the scope of PCI in your design. How large is your problem? How large would you like it to be?
- Integrated network access control products are in the early days of implementation. Several of these products can actually help you reduce the scope of PCI across your organization's network.
- Don't forget applications and legacy systems. These don't go out of scope because it's hard to manage RACF.
- Requirement 8.4 needs to be tested and proved. Don't just ask your application programmers if passwords are encrypted. Put a sniffer like Ettercap and Wire Shark onto your "*secure*" network and see what sort of authentication credentials you can pick up. If these applications and servers are on the same network where cardholder data is stored, processed, or transmitted, then you have a significant problem to address. Also, if your network engineer says, "*There are a couple of older switches that use Telnet"*—this is trouble!

Requirement 9: Physical Security and Access Controls

Although no network equipment vendor can claim to provide video surveillance, personnel controls, physical access controls, and paper shredding, there is an opportunity to combine physical and logical access control systems. In essence, the network access control can be linked to the physical badge door access control system as an additional authorization value. In essence, a user must have authorized physical access as well as a registered username and password to gain access to the network.

UAC in conjunction with partner products can ensure that a user who enters an area secured by a card/badge reader and does not scan his or her badge prior to entering the secure area (tailgating another person entering, for example) will not be able to access the network. UAC, in conjunction with physical security partners and through its implementation of the Interface to Metadata Access Point (IF-MAP) standard specification from the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) workgroup ties physical with network security together seamlessly.

Requirement 10: Track and Monitor All Access to Network

In an earlier requirement, there is a description of a segmented network isolated by a firewall where cardholder data is stored, processed, and transmitted. Remember, it was called the Zone. A reasonable conclusion now would be that the subsections of requirement 10 cover the tracking and monitoring of events that occur throughout the Zone. The objective is twofold: use logs to identify trends that may suggest a security compromise is being attempted, and detect that a security compromise has occurred.

Illustrated Controls

Following is a review of relevant requirements in section 10.

Table 10: Requirement 10 Specifics

10.2 Implement automated audit trails for all system components to reconstruct the following events. (The PCI lists many sub requirements at this point. See the PCI DSS for details):	This is fairly clear. The firewall, managed switches, routers, intrusion detection and prevention system (IDS/IPS) sensors, and any servers need to have automated audit trail and logging activated. A good general guideline: If it's connected to the Zone, then activate event logging. The subsections of this section list the minimum type of actions that should be logged. The rest of these sections list functions and processes that support logging. JUNIPER NETWORKS An automated security management system that analyzes logs to identify significant events is an important tool. The STRM Series is just such a tool, as it includes several reports based on log analysis.
10.4 Synchronize all critical system clocks and times.	Time synchronization is very important. In a nutshell, there *must* be two or three internal, trusted timeservers where all of the systems and network devices within the Zone will get their time. Then, these two or three (at most) timeservers will be the only devices permitted to synchronize their clocks with an external time source.
10.5 Secure audit trails so they cannot be altered.	This is the beginning of several requirements related to the protection of audit logs.
10.5.2 Protect audit trail files from unauthorized modifications.	In this very general requirement, the PCI DSS gives no advice as to how logs should be protected or what metrics should be implemented. Regardless, one can easily assume that system permissions will help achieve this goal by limiting write access to the log records.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	This provision raises a lot of concern and is frequently questioned by network architects and engineers who ask, *"Does this mean we have to copy the logs?"* Yes! Network devices tend to be storage constrained, and copying the logs to a central log server allows records to be maintained and examined.

The real challenge presented by PCI DSS for the large retailer is how to transport event and audit logs from the hundreds or thousands of retail locations back to a central, secured log server. Most retail sites run autonomously and may only upload data to corporate systems once a day. It must be pointed out that there are several options for complying with these requirements. One strategy says that the aggregation of log records should occur at the local retail site. Slave registers or back office/POS controllers are convenient resources. And then, once a night the aggregated log records are transmitted with the transaction logs to a corporate audit server for long-term storage. There are several possible models, but each has distinct challenges and disadvantages.

10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	This requirement underwent significant change in the PCI DSS update. In essence, it requires capturing log records for external facing technologies onto a centralized internal log server or media. The important distinction is the use of the term

	"external-facing" technologies. One might argue that this includes perimeter devices, websites, wireless access points, or any device that has any form of public access. It may not include devices like database servers and other internal technologies. For a large retailer who has wireless inventory devices in its stores that connect to the in-store back office controller, this requirement is in scope and must be complied with.
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 meet compliance with Requirement 10.6	Thank goodness for the "note". It would be terrible to think about a human having to review hundreds of thousands of logs each day. This is where the use of a security information management (SIM) system really helps. The SIM has a set of rules and signatures that it uses to compare and correlate log events. As the review takes place, the SIM looks for matches and raises alerts as necessary.
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).	This requirement provides guidance from the PCI DSS as to how long the aggregated audit logs need to be maintained. For a large retail environment, this adds up to a very large amount of data.

The PCI DSS requires you to have a data retention policy that governs how long you retain your organization's critical data. There is no debate that log data is *critical* data. So, an organization's data retention policy must reflect this storage requirement.

Criteria for Selecting Solutions

A few considerations when selecting a technology solution for PCI compliance:

- When selecting network components, be certain each device supports both local and remote log capture. This will facilitate the security and transfer of log data.
- Remote syslog capability would be a strong plus.
- Plan on configuring your log server to include file integrity monitoring tools like Samhain. This server should also be under centralized access control and limit access to log resources to security staff.
- Smaller organizations may want to sign up for the services provided by a managed security systems monitoring firm. There are a few of these firms that will facilitate capture and aggregation of log data.
- For large organizations, consider using a Security Information Management (SIM) system for aggregation and automated analysis of log records. When testing a SIM, run the same experiment multiple times to verify that the SIM properly alerts for the condition. For instance, try touching a log record in a system and see if the SIM alerts.

Juniper Networks has released a tool that will help perform log aggregation and log analysis—STRM Series Security Threat Response Managers. This tool is intended to be a tightly integrated SIM for analysis and identification of potential security issues from across the network. The STRM Series allows an application programmer and systems engineer to use syslog to remotely log application and system events to the tool. This allows the tool to correlate application, system, and network events. Currently, there are a variety of tools on the market that perform this function, and there are outsourced services that perform managed security systems monitoring. To facilitate

research and investigation of activity, the SRX Series devices can be utilized to view on-box logs and reports from the Juniper Networks J-Web Software graphical user interface or command-line interface (CLI).

Requirement 11: Regularly Test Security Systems and Processes

This requirement contains several provisions that are extremely important and frequently confused. The objective of these requirements is to ensure that security controls and precautions are actually working. Consider a situation where a network engineer turns on intrusion detection in a firewall. Is the network fully protected because this was switched on? Has anyone attempted to run an attack on the network to see the alarms sound? I'm most frequently reminded of a fire in San Francisco where the building landlord installed a fire suppression sprinkler system. Too bad when the fire struck, the system wasn't working. Most of the sections in this requirement involve performing routine security tests to verify that network, system, and application security controls are operational. With that said, there is one requirement that stands out related to the network that is worth discussing.

Illustrated Controls

Following is a review of the requirement related to network security in section 11.

Table 11: Requirement 11 Specifics

11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	Let's take a closer look at this. First, consider the scope of PCI when considering the placement of network-based intrusion detection systems. The term "all network traffic" refers to traffic involved in the authorization, settlement, and clearing of credit card data. If your network is segmented and sensitive data is maintained in a Zone, then this system monitors the traffic coming into the Zone and within the Zone. If your network is flat and all systems are visible to all users, then the solution must cover the entire network. Next, consider that there are two forms of intrusion detection systems (IDS): one network IDS and one host IDS. These IDS systems act in the same way that a car alarm works. When someone does something bad, the alarms should sound. The requirement also describes an intrusion prevention system (IPS). These are systems that perform some action as a result of the alarm. Just like in the movie Entrapment, when they unplug the network cable, the IDS sounds the alarm but it is the IPS that lowers the iron doors.

An important fact to remember is that an IDS system is only as good as the ability of the sensors to actually detect a problem. Also, these systems are only good if the alarms are accurate. The SRX Series with IPS or IDP Series appliances provide on-line subscription updates to definition files and information needed to tune the sensors. The SRX Series also provides fully integrated firewall and other security components. Both SRX Series and IDP Series devices are managed via the Juniper Networks Junos Space tool, the same central management tool for all Juniper security and networking solutions. Another important resource is the STRM Series, the security information-monitoring tool from Juniper that will evaluate alarms and alerts from all network components, including the IDP Series or integrated IPS in the SRX Series, to help the administrator identify potential issues.

Criteria for Selecting Solutions

A few considerations when selecting a technology solution for PCI compliance:

- Understand a clear point—there is no magic involved with IDS or IPS systems.
- IDS and IPS do not prevent attacks on your network. They are tools that measure the fallout from the attack that just occurred. Remember the fire alarm. When it goes off, it's either a false alarm or the building is already on fire.
- IDS and IPS systems must be monitored. It's extremely important to use automated tools to evaluate alerts from these applications and identify any false-positive conditions. This is why a tool like the STRM Series that performs broad

log analysis and specifically performs correlation analysis on log entries is important. Otherwise, the alarms from the IDS will be just like the car alarm in a parking garage. Does anyone really notice it?

Next Steps for the Engineer

Ask questions and get help from a qualified security assessor (QSA) who knows and has direct experience in your business. A QSA with skills in large retail can help evaluate security architectures to determine if they are either suitable or beyond best practice. In addition to this general advice:

- Study the PCI requirements.
- Don't read too much into them.
- Remember that the scope and applicability of PCI govern each requirement.
- Plan how to address the requirements.
- Consider using a vendor with a fully integrated product offering like Juniper Networks.

Who Is PSC?

With offices in the USA, UK, Canada, and Australia, PSC is a leading PCI assessor and Approved Scanning Vendor. PSC is one of an elite few companies qualified globally to provide expert services and solutions to organizations that require specialist compliance or consulting support in the areas of Payments, Security, or Compliance.

PSC's focus is exclusively on clients that accept or process payments or technology companies in the payment industry. All staff members at PSC have either worked within large merchant/retail organizations or services providers. Each partner at PSC has held executive management positions with responsibilities for payments and security.

Our approach includes a high-touch, hands-on methodology that helps guide our clients from consideration of strategic alternatives all the way through implementation and sustaining activities. The partners at PSC work closely with clients to understand their objectives, produce pragmatic and actionable plans, and aid in execution as required.

PSC is certified globally as a Qualified Security Assessor Company (QSAC) for the PCI Security Standards Council.

PSC is certified globally as an Approved Scanning Vendor (ASV) for the PCI Security Standards Council.

PSC is a Qualified Payment Applications Security Company (QPASC) and a Qualified Payment Applications Security Assessor (QPASA) for Visa in over 100 countries.

To ensure independence, PSC does not represent, resell, or receive commissions from any third-party hardware, software, or solutions vendors.

To contact PSC for more information or assistance, please call +1.408.228.0961 or go to http://www.paysw.com.