Juniper Networks PCI Compliance Architecture

Protecting confidential credit card information, securing networks, and meeting requirements of PCI standards

Challenge

Businesses that accept credit cards require an architecture that protects primary account numbers and other confidential cardholder information that is securely processed, transmitted, and stored through a network.

Solution

Juniper's Payment Card Industry (PCI) architecture integrates with your IT team's workflow, helping to meet and even exceed compliance requirements. The Juniper solution replaces multiple devices, easily integrating with the overall corporate network, security, and compliance strategy, increasing the overall security profile of your IT infrastructure.

Benefits

- Cost-effectively satisfies PCI DSS requirements while increasing the overall security profile of your network
- Properly secures primary account numbers and associated personal credit card holder information
- Supports and validates information security policy through comprehensive auditing and reporting
- Ensures standards compliance, reducing risk and liabilities while protecting brand value and reputation

The Payment Card Industry Data Security Standard (PCI DSS) is designed to secure and protect primary account numbers and associated personal credit card holder information. Achieving PCI DSS compliance greatly reduces the potential for credit card information theft and fraud. If a business is not in compliance, the right to accept and process personal credit for payment may be denied or expensive fines can be levied. Even worse for a business that is the victim of fraud is the potential loss of customer loyalty and serious damage to brand value.

Juniper has developed a comprehensive and secure network architecture for PCI DSS compliance. Employing firewalls as the primary building block, this architecture combines with other security solutions to safeguard the network and meet all PCI control objectives for protecting cardholder information.

The Challenge

Retailers today are facing persistent attacks from hackers attempting to steal credit card information for financial gain. These attacks are not only costly to the industry, they also damage the targeted retailer's brand image and reputation. Retailers and credit card processors must be able to securely process, transport, and store primary account numbers (PANs) and other associated personal information.

To minimize credit card fraud, the PCI Security Standards Council has developed a data security standard that governs how organizations that meet a minimum threshold of credit card transactions and sales must process, transmit, and store credit card information. Fines may be levied against companies that fail to pass mandatory compliance testing, and the right to accept and process consumer credit for the payment of goods may be denied.

Many retailers are struggling to meet these PCI compliance requirements while controlling their IT- and network security-related costs. Retailers realize they must comply with the PCI DSS not only to continue accepting and processing consumer credit cards, but also to protect their reputation—not to mention their customers' personal data. Retailers want solutions that provide full compliance at the lowest possible cost.

Payment Card Industry Compliance

The PCI DSS is designed to secure and protect stored, processed, and transmitted PANs and associated personal credit card holder information. Achieving PCI DSS compliance greatly reduces the threat of credit card information theft and fraud.

Juniper Networks has developed a comprehensive, secure network architecture for PCI DSS compliance that utilizes firewalls as the primary building block, combined with additional solutions that create a truly secure network that meets the control objectives of protecting cardholder information (see Table 1).

Table 1. Key Juniper Platforms Deployed to Satisfy PCI DSS Control Objectives

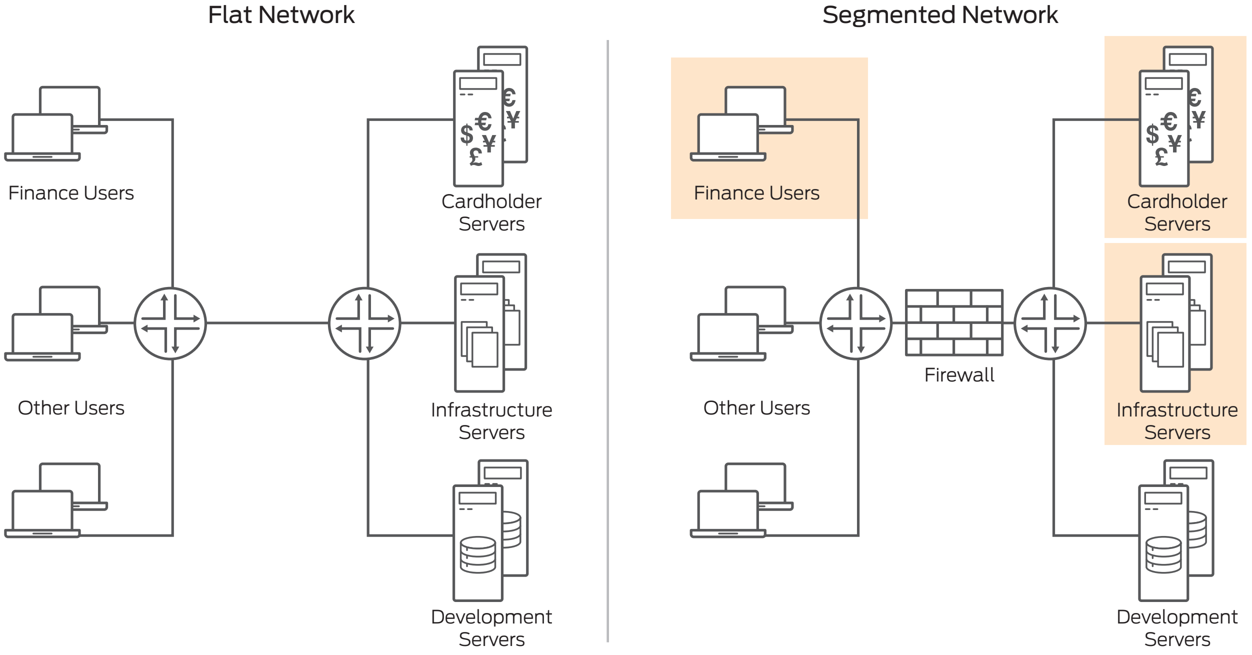
Requirements	Control Objective	Juniper's Key Solution Platform
1 and 2	Build and maintain a secure network	Firewalls
3 and 4	Protect cardholder data	Firewalls, SSL VPN, and/or IPsec VPN
5 and 6	Maintain a vulnerability management program	IDP, antivirus, Juniper Sky ATP, and Juniper Secure Analytics
7, 8, and 9	Implement strong access control measures	Firewalls, user-firewall integration with Active Directory/LDAP, integration with third-party NAC vendors
10 and 11	Regularly monitor and test networks	IDP, Juniper Sky ATP, Juniper Secure Analytics
12	Maintain an information security policy	Not applicable

Reducing PCI Scope Through Network Segmentation

PCI DSS compliance applies to all organizations with any component that touches their cardholder data environment (CDE). With more than 300 requirements, compliance can be costly and complex, creating a tremendous burden for businesses. However, organizations can reduce the scope of their compliance requirements by implementing network segmentation that isolates their CDE. This effectively narrows the amount of infrastructure that is exposed to PCI DSS compliance, not only reducing the cost and complexity of PCI compliance but also providing operational and security benefits. Through network segmentation, you can reduce the:

- Scope of the PCI DSS assessment
- Cost of the PCI DSS assessment
- Cost and difficulty of implementing and maintaining PCI DSS controls
- Risk to an organization by consolidating cardholder data into fewer, more controlled locations

Without adequate segmentation (also known as a flat network), the entire infrastructure is subject to the PCI DSS assessment. Network segmentation can be achieved a number of ways, such as through properly configured network firewalls, routers with access controls, and other technologies that restrict access to a particular segment of a network. In order to be considered out of scope for PCI DSS, a system component must be properly isolated or segmented from the cardholder environment to the point that, if it were compromised, it would not impact the security of the CDE.



- Since there is no segmentation, all the systems will fall under PCI DSS scope

- Segmented network using firewall ensures that traffic is limited to finance users
- Scope of PCI audit is reduced to only finance users, cardholder servers, and infrastructure servers

Figure 1: Flat networks vs. network segmentation

The Juniper Networks PCI Compliance Architecture

Using network segmentation to reduce the scope of the network subject to compliance is just one way that Juniper Networks supports organizations in their efforts to achieve PCI compliance. As detailed below, Juniper addresses the majority of PCI DSS requirements.

Requirement #1—Install and maintain firewall configurations to protect cardholder data: Fundamental to PCI DSS compliance is Requirement 1, which dictates that businesses must install and maintain a firewall configuration to protect cardholder data. Juniper Networks® SRX Series Services Gateways directly satisfy several subsections within Requirement 1. High-end SRX Series products can be configured to protect large corporate sites and data centers, while branch SRX Series products can protect individual retail stores. SRX Series firewalls examine all network traffic and block transmissions that do not meet the specified security criteria. Additionally in the data center, Juniper Networks Contrail Controller provides secure network segmentation that can be used to isolate PCI-related traffic and assets.

Multiple firewalls can be managed through Juniper Networks Junos Space® Security Director, which allows for central configuration and control across the entire network architecture. A single rule set for common security policy can be applied across all firewalls with a single mouse click, reducing administrative overhead and TCO.

Requirement #2—Do not user vendor-supplied defaults for system passwords and other security parameters: Cyber criminals will often try well-known default vendor passwords and settings in their attacks. Retail merchants frequently fail to change their default passwords or settings; this information, combined with hacker tools, makes it easy for savvy cyber criminals to make an unauthorized entry.

Juniper's security products satisfy all system password configuration rules outlined in Requirement 2. The SRX Series firewalls do not include default passwords, requiring users to create their own before configuration can begin. This ensures that system parameters and policies are robustly secured.

Requirement #3—Protect stored cardholder data: Not applicable.

Requirement #4—Encrypt transmission of cardholder data across open, public networks: This core requirement requires strong encryption algorithms to ensure that cyber criminals cannot access confidential cardholder data that is being transmitted over public networks.

A VPN connection can link two LANs (site-to-site VPN), or a remote dial-up user to a LAN. Traffic flowing between these two points must pass through shared resources such as routers, switches, and other network equipment on the WAN or public Internet without compromising cardholder data. The most common way of securing these VPN communications is to create an IPsec tunnel. SRX Series firewalls implement standards-based IPsec VPNs that support site-to-site connectivity across multiple network architectures.

Requirement #5—Protect all systems against malware and regularly update antivirus software and programs: Enterprises are required to protect all systems against current and evolving malware threats that find their way into the corporate bloodstream through infected e-mails and other online activities by employees. Constant monitoring for new exploits against newly discovered vulnerabilities is needed to keep network protection up-to-date against the latest attack methods.

Juniper security products include sophisticated threat detection against known and unknown threats, providing immediate protection against previously unseen malware, zero-day exploits, and advanced persistent threats. Network-borne attacks against vulnerabilities on client and server systems are immediately blocked inline before any damage can take place. The lateral spread of malware is detected and prevented from further infecting the internal network.

SRX Series firewalls provide comprehensive threat protection through Juniper‘s unified threat management (UTM) service, which acts as the first line of defense against the propagation of advanced malware. Juniper provides real-time updates to keep UTM software up-to-date to protect the network against the most recent attacks. These software updates are easy and cost effective, and can even be installed remotely. Juniper also offers anomaly detection for non-signature based zero-day exploit protection. Juniper's UTM includes features like antispam, antivirus, and content and Web filtering.

Juniper also offers the cloud-based Juniper Sky™ Advanced Threat Prevention (Juniper Sky ATP) service, which uses real-time information to arm businesses with advanced anti-malware protection. Juniper Sky ATP's identification technology uses a variety of sophisticated machine learning techniques to quickly detect, prevent, and defend against impending cyber attacks such as advanced persistent threats and ransomware. As a cloud-based service, Juniper Sky ATP is always up-to-date; no local firewall updates are required. The service provides a centralized Web interface for performing management tasks and running drill-down reports.

Requirement #6—Develop and maintain secure systems and applications: Security vulnerabilities allow criminals to breach enterprise systems and applications to access cardholder data. Installing vendor-provided patches eliminates vulnerabilities and prevents exploitation. All critical systems must be updated to be compliant with PCI DSS regulations.

Working in conjunction with our security partners, Juniper delivers solutions that meet these requirements by developing and maintaining secure systems and applications. SRX Series firewalls and Juniper Networks EX Series Ethernet Switches are tightly integrated with third-party network access control (NAC) solutions, ensuring that antivirus software is up-to-date and operational and that all end devices meet the necessary security policies before they access the network. They also check to ensure that antivirus and other anti-malware software is enabled throughout the network session.

Furthermore, the Juniper Networks Secure Analytics solution provides extensive scanning capabilities that check to see if up-to-date patches have been applied on devices within the network. It further scans the environment checking for critical software vulnerabilities that may exist within applications, databases, servers, and network devices. Any newly discovered vulnerabilities are assigned a risk ranking to assess the threat level they pose to the organization.

Requirement #7—Restrict access to cardholder data by business need-to-know: Access controls allow merchants to permit or deny access to PAN and other cardholder data based on a business need-to-know basis. Logical access controls permit or deny the use of payment devices, wireless networks, PCs, and other computing devices, and control access to digital files containing cardholder information.

SRX Series firewalls can be used to enforce access control policies through firewall rules that impose granular access control based on users, groups, and applications. Through the SRX Series User Firewall service, application usage can be restricted on a per-user basis by applying granular policy-based control to applications, limiting access to cardholder data to those performing “need to know” business functions. The User Firewall service tightly integrates with Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP), providing visibility into and control over application and network usage by specific user-defined roles, enabling secure access to authorized applications.

Requirement #8—Identify and authenticate access to system components: Each person with access to critical data and systems must be documented and authorized. A unique identification is applied to all accounts, including point of sale (POS), administrative accounts, and accounts with access to stored cardholder data. Policies that enforce minimum password strength, limit the number of failed password attempts allowed, and account for the departure or termination of employees should also be implemented.

Juniper provides a number of authentication methods, including Microsoft Active Directory, LDAP, RADIUS, integration with third-party vendors, and the ability to assign unique user IDs with password policies. Administrators can define minimum password strength rules, lock out users after a specified number of failed login attempts, and reset passwords and perform immediate revocation for terminated users.

Juniper Networks Secure Analytics provides complete auditing and alerting for access, data, and configuration changes to the system and databases containing cardholder data. JSA can quickly detect multiple failed login attempts on critical infrastructure systems, ensuring that only authorized personnel are allowed access. JSA also leverages existing user identity information within log data from authentication devices, VPN devices, and databases to keep a history and audit trail of user identity assignments to IP addresses, as well as a history of database access. Any detected violations or threats to PCI policies are flagged.

Requirement #9—Restrict physical access to cardholder data: Not applicable.

Requirement #10—Track and monitor all access to network resources and cardholder data: Detailed reporting and logging mechanisms are required to track user activities that are critical for effective security forensics and to determine the root cause of security breaches. To prevent such breaches, organizations must regularly monitor and test networks to find and fix vulnerabilities.

Juniper products provide extensive audit trails for all SRX Series configuration changes to properly track and monitor all access to network resources and cardholder data. Logs can be easily aggregated from multiple devices and locations, providing insightful reports and event correlation. Security teams gain insight into collected alarms, traffic flows, threats, and URL filtered traffic. In addition, SRX Series firewalls with intrusion prevention system (IPS) can capture events even as cyber attacks are underway, providing critical information for the security team.

JSA, used in conjunction with SRX Series firewalls, provides unparalleled log collection, analysis, correlation, and auditing capabilities that allow organizations to provide thorough tracking and analysis, including superior log analytics with distributed log collection and centralized viewing. Deep forensic inspection analyzes all log data and network communications to understand activity around an access offense. File integrity monitoring on critical servers that house sensitive customer information can be monitored to ensure that no data breaches have occurred. Predefined support for PCI compliance provides ready-made reports on the protection of designated assets and network components, managing incidents related to these resources.

Requirement #11—Regularly test security systems and processes: Many organizations perform little or no regular testing on the adequacy of the security controls governing their network and Internet-facing website applications. Failure to periodically run internal and external network scans to identify weaknesses can prove costly when back doors are left open to hackers. Organizations may be protected at any given moment, but new vulnerabilities appear constantly, which is why networks are required by PCI to be constantly tested, patched, and hardened.

Juniper Networks satisfies the subsections of Requirement #11 in multiple ways. JSA performs regular scans to ensure that software vulnerabilities are identified across applications, databases, servers, and network equipment so that administrators can provide up-to-date patches that ensure vulnerabilities are not exploited.

Juniper’s IPS, working in conjunction with Juniper Sky ATP, provides comprehensive detection of both known and unknown threats, offering immediate protection against new zero-day attacks. Juniper's IPS also constantly monitors for new exploits against recently discovered vulnerabilities to keep network protection up-to-date. Network-borne attacks against vulnerabilities on client and server systems are immediately blocked inline before any damage can take place. The Juniper solution protects against the vast number of exploits and vulnerabilities in operating systems, applications, and databases to prevent network attacks such as:

- Probing and scanning attempts
- SQL injections
- Cross-site scripting
- Buffer overflows
- Backdoor attacks, trojans, rootkits, viruses, worms
- Access control attempts and privilege escalations
- Arbitrary code escalations
- Denial of service (DoS) and distributed denial of service (DDoS) attacks

Requirement 12: Maintain a policy that addresses information security for all personnel: Not applicable.

PCI Solution Components

Juniper's PCI compliance architecture includes firewalls, encryption, IDP, UTM, NAC, RADIUS, and security incident and event manager reporting. Due to Juniper's standards-based approach, portions of the PCI compliance solution can be deployed alongside other third-party security solutions already in place, or it can be deployed in its entirety. In both scenarios, Juniper's architecture provides a comprehensive and cost-effective PCI DSS compliance solution that includes:

- SRX Series firewalls that cost-effectively scale from small retail locations to large centralized data centers to regulate the protocol and traffic flow between different networks
- EX Series switches that exceed the abilities of other vendors' 802.1X switches in offering user entitlement controls
- Intrusion detection and protection (IDP) that identifies application anomalies and suspicious behavior, as well as provides detailed reporting
- Unified threat management (UTM) that protects networks and users from advanced malware and advanced persistent threats
- Juniper Sky ATP, which quickly identifies and defends against sophisticated malware and impending cyber attacks.
- SSL VPN or IPsec encryption that protects cardholder data in transit
- Secure Analytics appliances that provide security incident and event management (SIEM) functionality for detailed reporting and network security audits

Table 2: PCI DSS Subsection Requirements Addressed by Juniper Networks Solutions

Requirements	Regulation Description	Subsection
1	Install and maintain a firewall configuration to protect cardholder data	1.1, 1.2, 1.3
2	Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.2, 2.3
3	Protect stored cardholder data	Not applicable
4	Encrypt transmission of cardholder data across open, public networks	4.1, 4.2
5	Use and regularly update antivirus software or programs	5.1, 5.2, 5.3
6	Develop and maintain secure systems and applications	6.2, 6.5
7	Restrict access to cardholder data by business need-to-know	7.1, 7.2
8	Assign a unique ID to each person with computer access	8.1, 8.2, 8.3, 8.5
9	Restrict physical access to cardholder data	Not applicable (refers to physical security)
10	Track and monitor all access to network resources and cardholder data	10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7
11	Regularly test security systems and processes	11.1, 11.2, 11.3, 11.4
12	Maintain a policy that addresses information security for employees and contractors	Not applicable

Juniper Networks Professional Services

Juniper Networks Professional Services Security Practice offers two JumpStart services that incorporate PCI networking standards into the design and implementation components of the solution: Secure Retail/Distributed Enterprise and Software-Defined Secure Network (SDSN). In addition, professional services also offer automated solutions to validate the network against PCI networking standards as well.

Summary

Juniper's PCI compliance architecture provides a robust, end-to-end solution for properly protecting sensitive cardholder data, as well as the business. This architecture, combined with proper network security policies, least-privileged access control, and advanced malware and threat detection, provides a complete PCI compliance solution.

Juniper's open, standards-based architecture offers a simple, flexible way for businesses to meet their unique PCI DSS compliance needs. This flexibility allows the architecture to be modified over time to address new threats and compliance requirements. Juniper's best-in-class network security portfolio, combined with our performance and reputation, makes this architecture an ideal solution for any organization seeking to meet or enhance security for PCI compliance.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3510619-001-EN June 2017