WHITE PAPER

A SECURE NETWORK FOR CREDIT CARD TRANSACTIONS

Addressing PCI Compliance with Juniper Networks Unified Access Control

Table of Contents

Executive Summary 1
Introduction 1
How Juniper Helps Your Firm Achieve Compliance 2
A Leader in Network Access Control 2
Juniper Networks Unified Access Control 3
Addressing PCI DSS with UAC 4
Building and Maintaining a Secure Network 4
Protecting Cardholder Data 5
Maintaining a Vulnerability Management Program 6
Implementing Strong Access Control Procedures 6
Regularly Monitoring and Testing Networks 7
Conclusion 8
About Juniper Networks 8

Table of Figures

Figure 1: Flexible standards-based access control 3
Figure 2: Juniper Networks Unified Access Control 4

Executive Summary

A security breach involving customer data can be devastating to retail and consumer companies and lead to a host of business problems—from negative publicity and impact on corporate reputation to loss of customer trust, fines, investigations and litigation. The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of requirements developed to help companies avoid these problems by ensuring the security of credit cardholder data. U.S. merchants, as well as those in Europe and Asia doing business with or in the U.S., must now meet minimum levels of security when they process, transmit and/or store cardholder data and personal information throughout a purchase or transaction.

The PCI DSS is a multifaceted, 12-part security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. In fact, PCI is considered one of the most comprehensive data security standards in a cluster of regulations that have emerged over the past decade. Meeting its requirements, however, is both complicated and expensive for many companies, often necessitating the redesign of basic infrastructures.

Juniper Networks® helps retailers and consumer companies address this significant challenge with Juniper Networks Unified Access Control (UAC), which manages network access and delivers the control, visibility, and monitoring of applications and users needed to sustain regulatory compliance while mitigating exposure to today's rapidly evolving threat landscape. UAC provides advanced protection of networks and applications while reducing the complexity and cost of deploying and managing access control. It also extends access control to network traffic by implementing security policy enforcement broader and deeper into the network's core and outward to the network's edge. Delivering comprehensive visibility into the network, this powerful solution leverages Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to correlate user identity and role information on network usage and application traffic. This enables more effective tracking and auditing of network and application access, and allows administrators to isolate threats and take specific, configurable policy action against them.

UAC allows retailers and consumer organizations to adhere to the core tenets of PCI, helping to ensure the security of their networks and data centers, and delivering the necessary information and reports needed for compliance audits, while maintaining high performance, availability and reliability for their overall business.

Introduction

The PCI DSS was developed by the major credit card companies and banks as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security assaults. A company processing, storing or transmitting cardholder data must be PCI DSS-compliant to avoid losing the ability to process credit card payments, and is liable for fines if they do not comply.

PCI DSS originally began as five different company-specific programs: Visa Card Information Security Program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and the JCB Data Security Program. These companies formed the Payment Card Industry Security Standards Council, and on December 15, 2004, aligned their individual policies and created the PCI DSS. In September 2006, the standard was updated to version 1.1. These companies also put together the PCI Security Standards Council to administer the standard, with a mandate to provide advisory services and drive technical standards among the credit card companies themselves, step up enforcement, and consider incentives for compliance.

The PCI DSS aims to reduce the risk of an attack by mandating that vendors maintain firewall configurations, eliminate vendor-supplied defaults for security parameters, encrypt transmission of cardholder data, regularly update antivirus software, restrict access to data, and monitor all access to network resources. The PCI DSS also calls for companies that handle credit card transactions to maintain a policy that addresses information security, performs frequent security audits and network monitoring, and forbids the use of default passwords. Merchants and consumer organizations must be validated with an audit by a Qualified Security Assessor (QSA) company. (A complete list of QSAs is available from the PCI Security Standards Council.)

The security requirements of the PCI DSS apply to all system components. System components are defined as any network component, server or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder or sensitive authentication data. By segregating the segments that store, process or transmit such information, administrators may increase security by reducing the scope of the environment to be protected. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances and other security appliances. Server types include but are not limited to Web, database, authentication, mail, proxy, network time protocol and domain name servers (DNS). Applications include all purchased and custom applications, internal and external, as well as Web-based applications. For complete PCI DSS specifications, please go to https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

While U.S. firms were given the deadline of June 30, 2007 to achieve compliance, it is expected that the number of organizations achieving PCI DSS compliance will be small. Companies face huge challenges in meeting this standard in the United States, as well as in Europe and Asia for companies doing business with or in the U.S. A recent survey conducted by The Logic Group in Europe revealed that only three percent of respondents are fully PCI DSS-compliant. While some companies have simply accepted paying fines as a cheaper solution, the Gartner Group states that, "Protecting customer data is much less expensive than dealing with a security breach in which records are exposed and potentially misused. The Payment Card Industry compliance requirements provide enterprises with good justification to increase data protection." (IT Compliance Institute)

In addition, in October 2007, Visa International announced a new payment applications security mandate for retail and consumer companies. This calls for new merchants that want to be authorized for payment card transactions to use only Payment Application Best Practice (PABP)-validated applications, and is scheduled to be implemented by 2010. This announcement has further intensified the pressure on retailers and service providers to become compliant.

How Juniper Helps Your Firm Achieve Compliance

Meeting the requirements of the PCI DSS is a complex process; in fact, a significant percentage of retailers have still not achieved compliance, and as a result face regulatory fines as well as all the risks and costs associated with a security breach or lost customer data. Juniper responds to this mission-critical need with a world-class depth of security capabilities and breadth of products and solutions to help meet regulatory demands. Acknowledged throughout the industry for security innovation and leadership, Juniper provides retailers and consumer organizations with all of the building blocks needed to secure their corporate network and cardholder and personal data, including comprehensive network access control (NAC).

A Leader in Network Access Control

Network access control, or NAC, is the ability to control network and application access based on compliance with corporate network and security policies. These policies may include ensuring that users and their devices meet and maintain a minimum baseline of endpoint security, addressing network and application access and authority of specific users and user roles, and making sure that all users or devices attempting network and/or application access meet a baseline of criteria stipulated by the corporation. Policies can be based on various criteria, such as user identity, device identity, device health, device and/or network location and so on. A network access control solution can ensure that an appropriate, authorized connection is properly made to the appropriate network by both user and device. It also ensures that users and their devices meet all corporate authentication and security policies. Thus, network access control has become a critical, "must have" component in today's business networks.

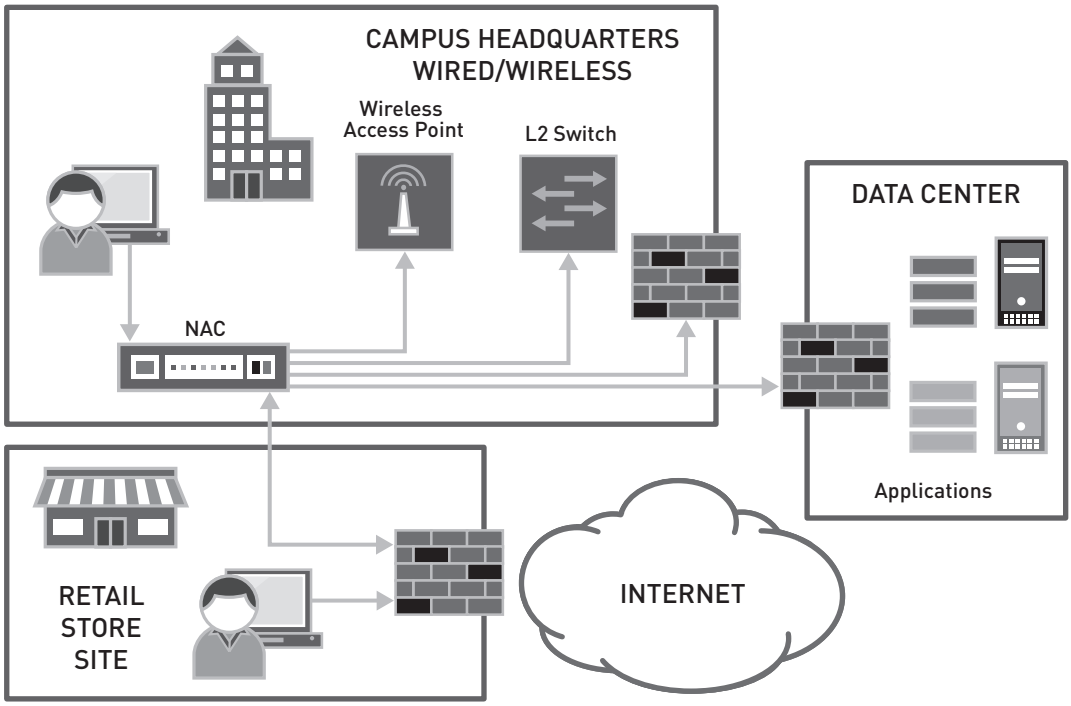

Figure 1: Flexible standards-based access control

Because of their breadth of capabilities and depth of function, network access control solutions frequently cut across the entire enterprise network as well as a number of internal, corporate departments and functions (Figure 1). A network access control deployment can span virtually every IT discipline, from desktop management to desktop security, network infrastructure to administration. It also can—and should—include individuals and resources involved in regulatory compliance, such as PCI.

The trend in today's businesses is for a more mobile and remote workforce, a greater use of outside contractors, and an increased number of vendors, guests and partners—all requiring access to the corporate network and its resources. Retailers and consumer organizations are no different, and therefore deal with a number of critical network issues, including a dramatic increase in the number of network access points and mission-critical assets, sensitive data being transmitted over various known and unknown wireless networks, varying unmanaged or ill-managed endpoints and mobile devices, and a widely diverse user base.

At the same time, the security and resiliency of networks is challenged more often by sophisticated attacks—from zero-day exploits and crimeware to rootkits, botnets and zombies—as well as increased threat volume and speed, more demanding applications, and the carelessness and sometimes casual attitude of many users when it comes to following, instituting or updating security measures. Network administrators are looking for elegant solutions that address and manage these challenges while providing the flexibility to prioritize and evolve, remain non-disruptive to business operations, and leverage existing infrastructure investments.

Juniper Networks Unified Access Control

Juniper Networks Unified Access Control combines the best of access control and security technologies while leveraging existing enterprise investments and deployments to provide a faster ROI. UAC leverages existing network infrastructure and components, working seamlessly across heterogeneous network environments.

All policy is created in and pushed by the Infranet Controller, a hardened, centralized policy server at the heart of UAC. User identity, device state and network location are collected by dynamically deployable cross-platform agents, available in either full or lightweight modes, or via an agentless mode wherever installing a software client is not feasible.

At Layer 2, UAC delivers powerful, standards-based 802.1X wired or wireless network security with its strong network credentials, transmitted data protection, and robust protocol support (tunneled Extensible Authentication Protocol or EAP), as well as its use of Advanced Encryption Standard (AES) with WiFi Protected Access 2 (WPA2).

UAC can fully integrate with any vendor's 802.1X enabled access point or switch, including Juniper Networks EX Series Ethernet Switches, delivering rich policy enforcement capabilities. At Layers 3-7 in conjunction with Juniper firewalls—including Juniper Networks SSG Series Secure Services Gateways or Juniper Networks ISG Series Integrated Security Gateways with integrated IDP Series Intrusion Detection and Prevention Appliances, UAC delivers unparalleled access control to and protection of sensitive stored information and assets, including cardholder data.

Every UAC component, including the Infranet Controller, UAC Agent and enforcement points, is built on field-tested, widely deployed products:

- Juniper Networks SA Series SSL VPN Appliances, with their legacy of dynamic endpoint assessment and seamless interaction with the Authentication, Authorization and Accounting (AAA) backbone
- Juniper Networks Odyssey Access Client (OAC), the market-leading 802.1X client/supplicant
- Juniper Networks SBR Series Steel-Belted Radius Servers, the de facto standard for RADIUS servers and appliances.

The result is a vendor-agnostic, comprehensive, reliable and uniquely flexible solution that combines user identity, device security state information, and network location to create a session-specific access control policy for each user attempting network access (Figure 2).

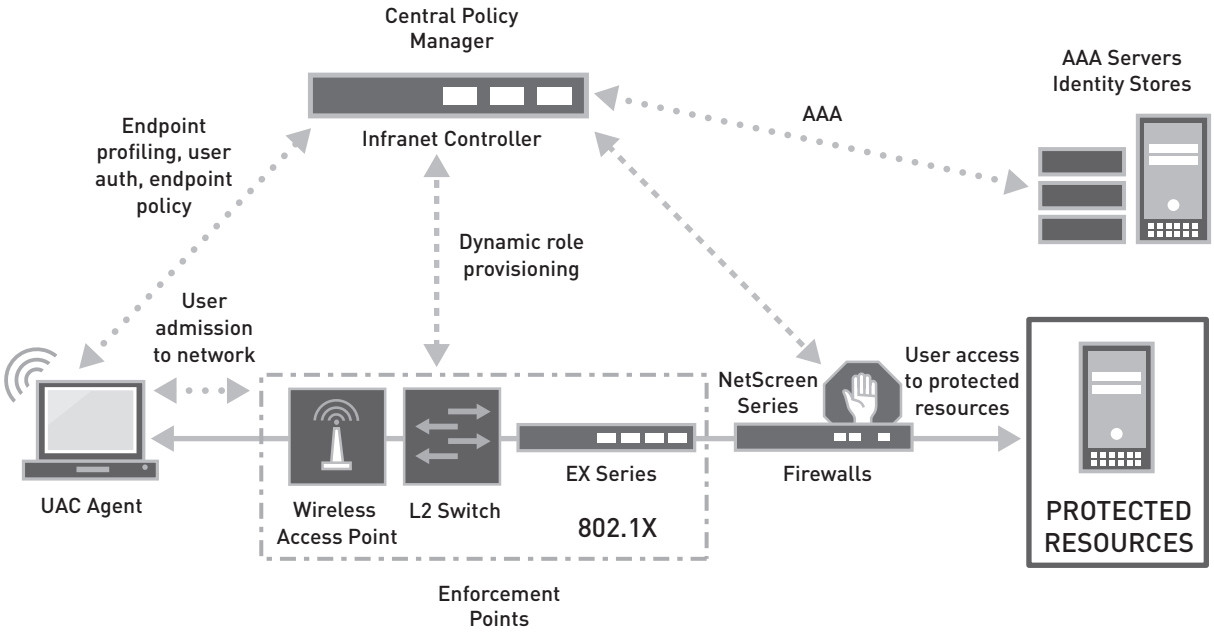

Figure 2: Juniper Networks Unified Access Control

Addressing PCI DSS with UAC

Empowered by UAC's formidable array of functionality and capabilities, retailers and consumer organizations are able to meet the advanced security requirements of the PCI DSS. Let's examine how UAC addresses each of the PCI Data Security Standard's 12 requirements, which revolve around the key areas of building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, and regularly monitoring and testing networks.

Building and Maintaining a Secure Network

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

To keep unauthorized or unwanted traffic off the network and out of the data center, a firewall provides the most fundamental and critical protection. UAC enhances this through its Layer 3 application access control capabilities, where network access enforcement is delivered via Juniper's powerful, expansive array of firewalls, such as the SSG Series and ISG Series, available with the IDP Series for protocol monitoring and enhanced threat control.

UAC ensures that traffic from untrusted users and devices can be denied network and/or application access at Layer 2 via 802.1X switches—such as the EX Series Ethernet Switches—and access points, or at Layer 3 using Juniper firewalls. UAC can also protect cardholder data by helping enterprises efficiently segment their networks at Layer 2 or Layer 3, segregating systems that store, process and/or transmit cardholder data and enacting additional restrictions on user access.

UAC leverages Juniper firewalls at Layer 3 by dynamically restricting connections and traffic between publicly accessible servers and system components that store cardholder data. Security administrators may utilize UAC's granular access control in conjunction with Juniper's firewalls and standalone IDP Series to configure dynamic packet filtering. In addition, using Juniper firewalls at the perimeter and its own 802.1X capabilities, UAC can control wireless network traffic and can ensure that personal firewalls are engaged on endpoint devices before they are granted access to the network. If a user's device does not have a personal firewall, the UAC Agent provides one. Unified Access Control and its enforcement points collectively restrict direct access between external networks and components storing cardholder data, and, when used in conjunction with other Juniper products such as the SSG Series, ISG Series, ISG Series with IDP, or standalone IDP Series, implements IP masquerading to prevent internal addresses from being translated or revealed .

Juniper firewalls can be dynamically leveraged as part of UAC not only to enforce access control policies, but to apply security policies such as deep packet inspection, antivirus and URL filtering on a per user or session basis. At Layer 3, UAC dynamically configures authentication files, enabling the enterprise to control and configure Juniper firewalls on the fly. With UAC in place, organizations can constantly evolve access and security policies for cardholder data based on the fast-changing needs of the network and its users.

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

As a basic security measure, default settings should never be used for security parameters. Juniper's security and access products support changing vendor defaults from installation through configuration, helping to ensure that system parameters and policies are configured to effectively prevent misuse. IDP Series Intrusion Detection and Prevention Appliances can also prevent or identify situations where security parameters are incorrectly configured.

In addition, UAC ensures that configuration standards address known and new security vulnerabilities, can aid in identifying and disabling unnecessary and insecure services and protocols, and can lock down network connections and access parameters to protect against inadvertent or intentional configuration changes. In wireless environments, the UAC Agent or Odyssey Access Client facilitate encryption, authentication, and secure data and credentials transport using Wi-Fi Protected Access (WPA or WPA2) encryption.

Protecting Cardholder Data

Requirement 3: Protect stored data

To protect stored cardholder data, Juniper products offer full security enforcement and can be configured to require a specific set of criteria before full credit card numbers are displayed on a need-to-know basis. For wired or wireless networks, the UAC Agent, as well as OAC when used in conjunction with a tunneled EAP type (such as EAP-Tunneled Transport Layer Security [EAP-TTLS] or Protected Extensible Authentication Protocol [EAP-PEAP]) and WPA2 with AES encryption, can assure that cardholder data, as well as network credentials including usernames and passwords, are protected and transmitted safely and securely. UAC ensures that encryption keys are protected against disclosure or misuse, key access is restricted, and secure access to cardholder data storage is provided only to authorized users. OAC—standalone or in conjunction with UAC—can implement key management processes and procedures that include key generation, secure distribution, and the changing or destruction of older keys.

For auditing purposes, the IDP Series checks for and logs violations to this requirement, to identify any incident or site where credit card numbers are transmitted in clear text.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

UAC, via the UAC Agent or OAC, provides strong cryptography to support the transmission of cardholder data, based on its support for the 802.1X and EAP standards that provide robust encryption during public network transmissions. The UAC Agent or OAC encrypts wireless network transmissions based on the WPA/WPA2 standard. Here again, the IDP Series has the ability to identify unencrypted transmissions of cardholder data, helping to meet security protocols. UAC can also redirect questionable traffic from unknown or untrusted users or devices based on established corporate networking and security policies. When used together with the IDP Series, UAC can take prohibitive actions against threatening users or devices already on the network. For example, if the IDP Series detects a network threat, it can signal the Infranet Controller that there is anomalous behavior taking place on

the network. Based on this information, the Infranet Controller can take that information from the IDP Series and correlate the threat to a specific user and/or device. UAC can then take decisive action against the threatening user and/or device, placing the device into a quarantine network, restricting user access, or even disabling the network session entirely.

UAC can also invoke a native IPsec client, which is included as part of the UAC Agent and is compatible with any other IPsec client, to ensure user and device validation prior to granting access to network resources, and to authenticate user traffic. UAC also employs dynamic IPsec for optional encryption, creating an IPsec tunnel to provide even more protection for data and credentials communicated within the network.

Maintaining a Vulnerability Management Program

Requirement 5: Use and regularly update antivirus software

Juniper Networks Unified Access Control can ensure that every device that attempts network access has loaded and is running a variety of endpoint security software, including antivirus, anti-spyware and personal firewall, to name a few. UAC checks devices for current software versions and configuration requirements, among other criteria, and network access can be denied and users instructed to manually update or automatically remediate their antivirus software or other offending endpoint security software as needed, or to modify device configurations. UAC can also check devices for registry entries, specific files, media access control (MAC) addresses and custom checks, as well as OS and application software patches and hotfix updates. Juniper firewalls also include integrated antivirus software that complies with automated updates and includes anti-spyware, anti-adware and anti-phishing capabilities. UAC can apply these integrated endpoint security capabilities against specific devices. Additionally, Juniper provides daily signature updates for the PCI-required intrusion detection and prevention solution.

Requirement 6: Develop and maintain secure systems and applications

Working with its partners, Juniper provides a powerful series of solutions for developing and maintaining secure systems and applications. UAC ensures that system components and software are running updated patches, denying access until updates are made, and protecting against newly discovered vulnerabilities. Additionally, Juniper's security portal may be incorporated to provide timely security notices for patch updates. UAC can assist companies in assuring that security patches, and system and software configuration changes are implemented prior to deployment by enabling them to define policies that address these changes. If the changes have not been implemented or have been implemented incorrectly, the solution can identify and quarantine the affected devices until remediation. UAC can also ensure and enforce compliance with change control procedures for modifications. Tasks such as these can be addressed within separate development and test environments segmented at Layer 3, with Juniper firewalls deployed as access enforcement points.

UAC can also detect unauthorized custom applications and block the devices on which they reside in real time, quarantining the devices as needed. In conjunction with the standalone IDP Series, UAC can identify and stop malicious users or devices on a network. The IDP Series also provides buffer overflow protection.

Additional security processes are supported in conjunction with Juniper's security solutions. For example, Juniper firewalls enforce policy from the network layer to the application layer with deep packet inspection. Juniper Networks Network and Security Manager can also be used to help assure proper work flow for change control on Juniper devices.

Implementing Strong Access Control Procedures

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

UAC provides granular and dynamic access control, a powerful tool in restricting access to sensitive data such as cardholder information. UAC can be configured to support a pre-established policy for access to servers storing specific, sensitive data and, when configured at Layer 3 with Juniper firewalls, can restrict resource and cardholder data access to a specific group of users or roles. UAC supplies administrators with a log that shows who accessed the restricted systems and data stores and when. When used in conjunction with the IDP Series, UAC can provide enhanced visibility and monitoring of restricted systems and data stores, correlating user data and roles to IP addresses to provide a detailed information trail on restricted data access suitable for audits.

Requirement 8: Assign a unique ID to each person with computer access

This PCI DSS requirement can be addressed by UAC when used in conjunction with SBR Series Steel-Belted Radius Servers, the de facto standard for AAA/RADIUS servers and appliances. UAC has components of the SBR Series integrated into its Infranet Controller to deliver proper user authentication, credentials management,

and to effectively address 802.1X transactions. The SBR Series can also provide detailed information on user/device authentication and authorization through its robust accounting and reporting capabilities, as well as on administrative access and modifications made to any SBR Series server or appliance. At the same time, the UAC Agent and OAC support user names and passwords, two-factor authentication, token devices and biometric devices, and can aid password encryption and management. Two-factor authentication assists companies that fear incidents caused by stolen or lost passwords or that desire a greater level of authentication security.

Requirement 9: Restrict physical access to cardholder data

While carrying out network security initiatives, companies must also take fundamental physical security precautions. Retailers and consumer organizations can support this requirement with a physical "lock and key" building infrastructure, well planned video surveillance, and biometrics and other high-level security systems for sensitive data center environments. UAC can also provide a second layer of access control, acting as a backup to restricting physical access. Should an unauthorized user or guest be granted entry to the company and attempt to access the network by connecting to an available Ethernet wall jack or via wireless access, UAC can thwart the access attempt immediately.

Regularly Monitoring and Testing Networks

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

Unified Access Control offers audit trails and logs on user sessions and authorizations, providing granular tracking and auditing of users, devices, network and application access, and even network traffic. Together with any Juniper firewall platform, UAC can monitor network traffic for viruses and malicious content. In conjunction with IDP Series products, UAC also associates user names and roles with application and asset access, and can identify and take decisive action against users or devices exhibiting anomalous behavior.

Leveraging the standards-based architecture of UAC, including use and adoption of the open standards for access control produced by the Trusted Network Connect (TNC) work group of the Trusted Computing Group (TCG), UAC works seamlessly with a variety of Security Information and Event Management (SIEM) products, including Juniper Networks STRM Series Security Threat Response Managers, to provide log aggregation and event correlation. The STRM Series delivers advanced log management capabilities, SIEM, and Network Behavior Anomaly Detection (NBAD) to address log management, threat detection, and compliance and audit requirements. SIEM/SIM/SEM vendors generally collect data via SYSLOG, SNMP and/or Proprietary Agent. Juniper's interoperable UAC can support most SIEM/SIM/SEM products via its log data.

Requirement 11: Regularly test security systems and processes

To test security systems and processes, UAC leverages ISG Series firewalls with integrated IDP, Host Checker and standalone IDP Series, including Layer 7 policies such as IDP policies or URL filtering, to provide additional levels of dynamic threat management. It should be noted that while UAC can be leveraged to address security systems testing, UAC itself provides dynamic rather than static security, and therefore does not require as much testing as traditional security mechanisms. To support regular network tests, Juniper has also partnered with leading network vulnerability testing partners.

Requirement 12: Maintain a policy that addresses information security

UAC supports flexible policy creation and maintenance to deliver robust support for PCI compliance enforcement. The central Infranet Controller pushes the UAC Agent (or, in agentless mode) to the endpoint device, collecting information such as user credentials and the device's state of security and health. It also serves as the interface to existing enterprise AAA infrastructure. Once the user credentials and device security and health state are validated, the Infranet Controller dynamically implements appropriate access policies for each user/session and pushes those policies to enforcement points throughout the network. The Infranet Controller also delivers post-admission access control, continuing to collect endpoint device state information and matching that data against policy changes for the life of the network connection. Each successive layer of policy in UAC adds more granularity to overall access control and stronger compliance with PCI DSS.

UAC also provides information to support well informed decision-making and consistent improvements in overall security and PCI compliance enforcement.

Conclusion

Juniper Networks Unified Access Control provides the robust, flexible access control and security measures needed to achieve adherence with PCI DSS. This innovative solution—whether used alone or in conjunction with Juniper's firewalls, AAA/802.1X products, integrated security offerings, EX Series Ethernet Switches, or IDP Series appliances—serves as the foundation for a highly integrated, secure data stronghold. Working by itself or with best-in-class partners, Juniper's ability to integrate UAC with its firewalls, switches, 802.1X products, AAA/RADIUS servers and appliances, IDP Series appliances, unified threat management (UTM)-enabled offerings, STRM Series, and other Juniper security and access control products—as well as its capacity to leverage existing network infrastructure and components, and work across heterogeneous networks—sets the company apart from other vendors claiming to offer security products that address PCI compliance. Juniper delivers a comprehensive solution comprised of appliances, devices and software that addresses PCI compliance across the enterprise.

These interoperable solutions offer retailers and consumer organizations needed flexibility when deploying network access control and threat management, enforcement and manageability with a variety of malleable deployment options that efficiently address credit card transactions and effectively protect cardholder data and network credentials.

Delivering solid investment protection and a quick return on investment, Juniper empowers retail and consumer businesses to achieve the security standard they need to serve their customers, while exceeding regulatory requirements, maintaining their corporate reputation, and achieving competitive success.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net.**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

2000263-002-EN Sept 2010 Printed on recycled paper