TECHNOLOGY WHITE PAPER

Facilitate PCI DSS compliance with the Nuage Networks SDN platform

nuagenetworks
From Nokia

CONTENTS

Executive summary

The payment processing value chain is undergoing a rapid transformation with the proliferation of transactions beyond the typical brick and mortar point of sale. Banks and merchants that process payments are adopting cloud-based infrastructures to adapt their operations to these changes. While the underlying networking and compute infrastructure evolves, banks and merchants must ensure the security and integrity of consumer data by conforming to Payment Card Industry (PCI) standards established by the PCI Security Standards Council.

The PCI Data Security Standards (PCI DSS) are the key standards established by the Council for technical and operational system components included in or connected to cardholder data. Endorsed by major credit card companies worldwide, PCI DSS require merchants and service providers that store, process or transmit cardholder data to adopt information security controls and processes to ensure cardholder data is protected.

TekSecure Labs, a division of Tekmark Global, is a leading provider of technology risk management services that ensure the highest level of network security for mission critical applications. It is certified by the PCI Security Standards Council to perform assessments of enterprise environments to validate compliance with PCI standards.

TekSecure Labs audited and tested the software-defined networking (SDN) solutions offered by Nuage Networks™ from Nokia to determine if these solutions conform to PCI DSS requirements. This assessment was conducted over five months beginning in January 2016 and ending in May 2016. At the end of the test period, **TekSecure Labs concluded that Nuage Networks SDN and security solutions for cloud/datacenter and branch networks make it easier for organizations to achieve PCI compliance by facilitating adherence to key PCI requirements**. In addition, there are no known limitations within the Nuage Networks solution components that will inhibit an organization's ability to become PCI compliant, or maintain its existing compliance.

This paper presents the methodology and detailed findings of the TekSecure Labs evaluation for IT professionals that are deploying Nuage Networks SDN solutions within their Cardholder Data Environments (CDE) and auditors conducting PCI assessments of those environments. It provides an overview of the security disposition of the Nuage Networks SDN solutions for deployment in a CDE in accordance with PCI DSS.

Understanding the standards

Last year over $US227 billion credit card transactions were used to purchase goods and services around the world. These transactions were processed using various payment systems and supporting technologies. Yet the threat of a breach or compromise continues to be a real concern for all banks and merchants.

The PCI Security Standards Council was established in 2006 to define a standard framework that would safeguard credit card data and reduce fraudulent transactions.

PCI DSS outline technical and operational requirements organizations must follow to protect cardholder data. The standards are designed to ensure that any companies that accept, process, store or transmit credit card information maintain a secure environment. The goals and high-level technical operational requirements of PCI DSS are outlined in Table 1.

TABLE 1. PCI DSS overview

GOAL	PCI DSS REQUIREMENTS
Build and maintain a secure network	■ Install and maintain a firewall configuration to protect data. ■ Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data	■ Protect stored cardholder data. ■ Encrypt transmissions of cardholder data and sensitive information across open public networks.
Maintain a vulnerability management program	■ Use and regularly update anti-virus software. ■ Develop and maintain secure systems and applications.
Implement strong access control measures	■ Restrict access to data by business need-to-know. ■ Assign a unique ID to each person with computer access. ■ Restrict physical access to cardholder data.
Regularly monitor and test networks	■ Track and monitor all access to network resources and cardholder data. ■ Regularly test security systems and processes.
Maintain an information security policy	■ Maintain a policy that addresses information security.

Nuage Networks SDN for datacenter and branch networks

Virtualized Services Platform (VSP) and Virtual Network Services (VNS)

The Nuage Networks Virtualized Services Platform (VSP) provides a unified SDN platform for datacenter, private cloud, and public cloud, as well as wide area networks (WAN). Nuage Networks Virtualized Network Services (VNS) platform enables a software-defined WAN (SD-WAN) to automate provisioning and securely inter-connect enterprise branch networks and datacenters.

The key components of the Nuage Networks SDN solutions for both datacenter and branch networks are explained below.

Virtualized Services Directory (VSD)

The Virtualized Services Directory (VSD) serves as a policy, business logic, and analytics engine for the abstract definition of network services. Through an intuitive graphical user interface (GUI), administrators can define and refine application network designs and incorporate enterprise network policies.

Virtualized Services Controller (VSC)

The Virtualized Services Controller (VSC) serves as a centralized control plane for datacenter and branch networks. It maintains a per-tenant view of network and service topologies. To avoid vendor lock-in, VSC uses open network application programming interfaces (APIs) and protocols, such as OpenFlow, to orchestrate the network independent of datacenter networking hardware.

Virtual Routing & Switching (VRS)

The Virtual Routing and Switching (VRS) component of the Nuage Networks solution is a Layer 3 software switch installed on the hypervisor that serves as a virtual endpoint for network services. Through VRS, changes in the compute environment are immediately detected, triggering instant policy-based responses in network connectivity to ensure that the needs of applications are met.

Network Services Gateway (NSG)

The Network Services Gateway (NSG) acts as a branch router/Internet access device and serves as the network-forwarding plane for customers' network services at their locations. The NSG is available in both physical and virtual form factors. It can run on either dedicated appliances, commodity x86 servers, or as a virtual machine (VM).

7850 Virtualized Services Gateway (VSG)

In many real-world installations, datacenters are a mix of virtualized and non-virtualized assets. To help all datacenters benefit from automation and network virtualization, a new breed of gateway is needed. The Nuage Networks 7850 Virtualized Services Gateway (VSG) is a high-performance gateway appliance that bridges VSP overlay networks between virtual and bare-metal applications for a fully automated network infrastructure.

Nuage Networks' SDN security features for addressing PCI requirements and reducing PCI scope

Isolation and micro-segmentation for a secure network

- Virtual networks (Layer 3 domains) provide network isolation between IT environments across datacenter and branch networks.
- Embedded Layer 3 and Layer 4 distributed firewalls with stateful access control lists (ACLs) enable "micro-segmentation" in the datacenter cloud, as well as perimeter security at branch networks to restrict both user and system access to corporate applications and data. Micro-segmentation includes the ability to enforce fine-grained security policies between individual application workloads (even those sharing a common server), enabling a "zero-trust" model (as defined by Forrester Research) within multi-tenant cloud environments where all application traffic is blocked unless explicitly allowed.
- Security policies — including ingress/egress policies, as well as forwarding policies — can be defined to protect any workload in the datacenter and cloud, including VMs (multi-hypervisor), bare-metal, and containers. The security policies are enforced closer to the workload on Nuage Networks VRS software deployed on hosts running VMs, container workloads, as well as on virtual routing and switching gateways (VRS-Gs) that connect to bare-metal workloads.

Transport security with IPSec encryption and secure socket layer (SSL) to protect cardholder data

- IPsec encryption for WAN traffic over both public and private networks.
- Support for TLS 1.2 and strong ciphers for communication to VSD GUIs and APIs.

Platform security for developing and maintaining secure systems and applications

- VSP security validated based on third party security assessments that included architecture review, as well as penetration testing.
- Product Security Incident Response Team (PSIRT) advisories prioritized as part of the software development life cycle process.
- VSP and solution components are hardened based on security testing as part of the software release process.

Authentication and role-based access for strong access control

- Integration with Lightweight Directory Access Protocol (LDAP) for authentication policy controls (e.g., failed logins, session time-outs).
- Role-based access control to restrict administrative access to the system based on user role (e.g., Cloud Service Provider (CSP) administrator, network designer, network operator, etc.).
- Secure onboarding of branch devices (NSGs) using two-factor authentication.
- Access to NSG administrative interfaces limited to trusted sources via secure shell (SSH) authentication.
- Ability to deactivate NSGs on demand in the event of unauthorized access.

Auditing and security monitoring for regular monitoring and testing

- Logging of user logins and policy changes with contextual information about who has made a change, the change that was made, and when the change was made.
- ACL flow logging that enables auditing of all allowed or denied flows (policy violations) that match a particular ACL entry.
- Policy-based mirroring for select traffic flows for security analytics and monitoring.
- Ability to automate responses for integrity checks and threat detection through integration with endpoint detection and response systems.
- Self-monitoring by the NSG to ensure that it is connected to the controller at all times. If the NSG becomes disconnected from its controller for a period greater than a configured duration it revokes itself and becomes isolated from the network.

Templates, ingress/egress/forwarding policies for maintaining an information security policy

- Enterprise-wide information security policies can be easily defined and updated using templates. Any virtual network instantiated based on the template inherits the global policies automatically.
- Policies can be defined using logical grouping of endpoints. Any endpoints that are assigned to a policy group are subject to the policy regardless of IP address, location, or subnet.
- Policies can be applied on both ingress and egress at the endpoint or the physical gateway.
- Forwarding policies provide the ability to insert advanced security services (e.g., Next-Generation Firewall (NGFW), unified threat management (UTM), etc.) for both datacenter and branch network traffic flows.

Third party assessment of Nuage Networks SDN solution for PCI compliance

TekSecure Labs conducted a PCI compliance assessment of Nuage Networks SDN and security solutions for cloud/ datacenter and branch networks. These solutions are based on the Nuage Networks VSP. The solution components that were tested include the Nuage Networks:

- Virtualized Services Directory (VSD)
- Virtualized Services Controller (VSC)
- Virtualized Services Gateway
- Virtualized Routing and Switching components (VRS, VRS-G)
- Network Services Gateway (NSG)

Test methodology

The security audit process consisted of multiple rounds of testing based on a methodology structured to evaluate conformance to the PCI DSS requirements. Testing of the infrastructure consisted of several test cases and was executed in a logical and repeatable manner. This phased approach consisted of both automated and manual testing for specific vulnerabilities in an attempt to identify weaknesses that could lead to the exposure of PCI cardholder data.

The test methodology included:

- Evaluation of relevant architectural, procedural, and provisioning capabilities.
- Execution of automated tools to identify common vulnerabilities. Tools included port and vulnerability scanners, as well as more specialized tools for targeting a particular service on the device, such as Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), and Hypertext Transfer Protocol Secure (HTTPS).
- Review of automated scan results and execution of manual test cases.
- Analysis against standards of good practice published by PCI and TekSecure Labs' own expertise in developing baseline hardening and system accreditation guides.

The following criteria were assessed as part of the review:

- Solution design and architecture
- Solution implementation and management
- IP networking schema
- Operating system configuration
- Policy configuration and definition
- Allowed inbound (ingress) and outbound (egress) services
- Surrounding firewall security issues
- End-to-end encryption
- Zone segmentation and isolation
- Traffic access controls
- Disabled default services (e.g., Bootstrap Protocol (BOOTP), Finger, small services)
- Delegation of privileged use in accordance with job function
- Controls over administrative access

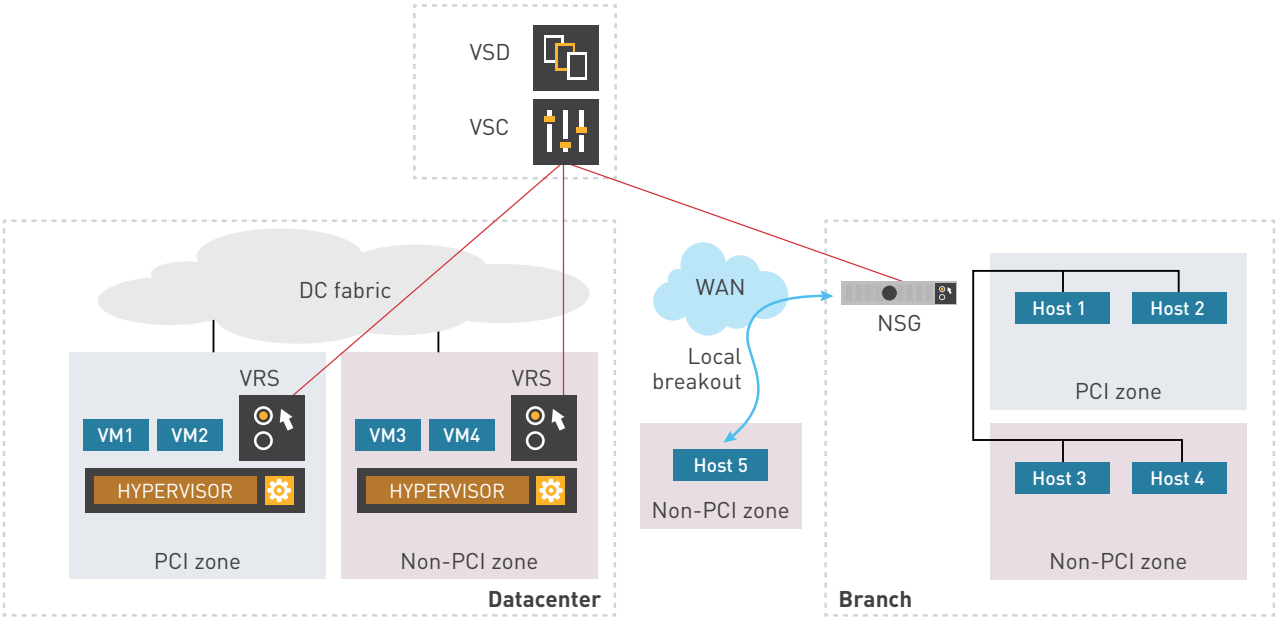
Test topology

The test network used for the assessment reflected a typical retail customer topology with two zones:

- **PCI Zone:** A network segment that is part of the customer's CDE where credit card information is processed, stored or transmitted on the network.
- **Non-PCI Zone:** A network segment containing back office business functions not considered in scope for PCI.

A single domain was instantiated with four subnets for each of the PCI and non-PCI VMs/hosts in the datacenter and branch. Local breakout to an external untrusted host was also configured (Figure 1).

FIGURE 1. Test network for assessment of Nuage Networks security solutions



Centralized egress/ingress policies were configured (via the VSD) for segmentation of traffic as shown in Table 2.

TABLE 2. Egress/ingress policies for segmentation of traffic on the test network

SOURCE	DESTINATION	PROTOCOL	PORT/SERVICE	ACTION
Non-PCI	PCI	*	*	Deny
Non-PCI	Non-PCI	*	*	Allow
PCI	PCI	*	*	Allow
Non-PCI	External host	*	*	Allow
PCI	External host	*	*	Deny

Note: Policies can also be defined granularly at protocol and port level.

Test Results

Table 3 maps PCI DSS controls to the capabilities of the Nuage Networks SDN solution. Some controls require integration with a complementing technology to meet or enhance compliance objectives. Controls related to documentation and/or operational procedures are not included in the table.

TABLE 3. PCI DSS controls mapped to the capabilities of the Nuage Networks SDN solution

PCI DSS REQUIREMENT	CONTROLS ADDRESSED	DETAILS
Install and maintain a firewall configuration to protect data	1.1.4, 1.2, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8	■ Components include firewall functionality. VSP policies ensure separation of network traffic between different logical zones. ■ Policy allows only specific connections. ■ Configurations are managed and stored centrally within the VSP. ■ The VSP solution is designed to enable communication only through established network policies (which ensure restricting access to only authorized networks/services). ■ Policies, as with firewall rules, dictate both inbound and outbound traffic flow. Without an explicit policy, network traffic cannot pass routing devices. ■ Stateful firewall supported in the solution. ■ The SDN is capable of protecting network assets, but the protection is based on the network/policy design, so may vary by network.
Do not use vendor-supplied defaults for system passwords and other security parameters	2.1, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.3, 2.6	■ NSG supports a non-privileged account. Default password changed after first login. Password login can be disabled and SSH authentication used instead. In addition, access can be restricted for a specific set of source IP addresses. ■ Access to services is restricted to the Nuage Networks support network. ■ Architecture supports an implementation requiring dedicated functions per server. ■ Network services that are not needed are disabled. ■ Remote access is secure. ■ As the evaluated solution may be available to shared hosted providers, Appendix A of the PCI DSS (V3.2) was reviewed. The evaluated solution meets Appendix A of the PCI DSS. This is dependent upon the customer's configuration of the solution.
Encrypt transmission of cardholder data across open, public networks	4.1	■ Secure communication is supported — Internet Protocol Security (IPsec) — but the specific policy is dependent upon the final customer implementation/design. ■ Secure control plane communication between Nuage Networks components using TLSv1.2.
Develop and maintain secure systems and applications	6.3, 6.3.1, 6.5.3	■ PSIRT advisories in the software development life cycle (SDLC). ■ Independent third party security testing conducted for the VSP using source-assisted penetration testing (both black-box and white-box testing). ■ NSG onboarded using secure bootstrapping. ■ Security mechanism for automatically revoking a compromised NSG.
Restrict access to cardholder data by business need to know	7.1.1, 7.1.2, 7.2, 7.2.1, 7.2.3	■ Cardholder data will not be stored in VSP/VNS components. ■ User access to VSP/VNS management interface can be restricted using an existing directory service, such as LDAP or Active Directory. ■ Any access requires a policy entry and only authorized traffic is permitted. Therefore, an implicit deny rule is default. ■ VSP permits separate accounts/roles. ■ Root login disabled on NSG.

PCI DSS REQUIREMENT	CONTROLS ADDRESSED	DETAILS
Assign a unique ID to each person with computer access	8.1.1, 8.1.2, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.1, 8.2.3, 8.2.5, 8.3	■ LDAP recommended to enforce: ■ Account locking mechanism ■ Session timeouts ■ Password complexity and aging ■ NSG remote access requires SSH authentication and iptables (an application to configure the Linux kernel firewall) ruleset that allows connections from a specific set of hosts.
Track and monitor all access to network resources and cardholder data	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6	■ Sufficient logging can be enabled. ■ A centralized log server and security information and event management (SIEM) solution is recommended. ■ Alarms displayed in VSD for various events.
Regularly test security systems and processes	11.4, 11.5	■ Nuage Networks components have been hardened using normal development security best practices and processes. However, post deployment, the components must be included in the customer's operational test processes, including the scanning and penetration testing requirements, file integrity monitoring, etc. ■ Integrity checks for NSG software upgrades.

Conclusion

Banks and merchants that process credit card transactions must protect the security of cardholder data by adhering to the technical and operational requirements set forth by the PCI Security Standards Council. As retail branches and datacenters implement SDN infrastructures they want assurance that compliance to PCI Data Security Standards is not compromised.

The security audit conducted by TekSecure Labs consisted of multiple rounds of testing based on a methodology that included several test cases executed in a logical and repeatable manner. This phased approach included both automated and manual testing for specific vulnerabilities in an attempt to identify weaknesses that could lead to the exposure of PCI cardholder data.

Based on this assessment, TekSecure Labs concluded that the Nuage Networks VSP and VNS solutions support a customer's requirement to meet PCI DSS 3.1. The analysis revealed that the Nuage Networks technology can provide a PCI DSS (v3.2)-compliant solution when coupled with an external authentication directory service, extended log retention, network intrusion prevention service, and a secure remote access policy. In addition, TekSecure Labs determined that this technology can be used for network segmentation and isolation to reduce the scope of compliance.

Given the results of the analysis, the Nuage Networks SDN solutions provide a viable cloud/ datacenter and branch network infrastructure solution for merchants and service providers that store, process or transmit transaction data. The Nuage Networks solutions adhere to PCI security guidelines and provide capabilities to enhance the application of security and access policies that will protect cardholder data.

Appendix – Letter of Opinion from Tekmark Global Solutions

May 31, 2016

Tekmark® Global Solutions, LLC (Tekmark) provides IT, telecom, security, and consulting and staffing services to enterprises worldwide, including dozens of Fortune 500 companies. For over 35 years, our team has demonstrated expertise in developing and integrating information systems, network intrusion protection, technology, and business processes improvement.

Tekmark's TekSecure Labs division is a market leader in providing security solutions for businesses of all sizes and types. TekSecure Labs provides comprehensive network security, integrated managed services, and a portfolio of technology risk management solutions through a suite of products and services designed to ensure the highest level of network security for mission critical applications. Additionally, TekSecure Labs is a certified Payment Card Industry (PCI) Approved Scanning Vendor (ASV), certificate number 3894-01-10, and has assisted other organizations with leading industry compliance requirements.

Tekmark conducted a PCI compliance assessment of Nuage Networks Software Defined Networking and Security solutions for Cloud/ datacenter (VCS) and Branch networks (VNS). These solutions are based on a common platform called Virtualized Services Platform (VSP). The solution components tested includes Virtualized Services Directory (VSD), Virtualized Services Controller (VSC), Virtualized Routing and Switching components (VRS, VRS- G) as well as a Network Services Gateway (NSG).

Based on the assessment, Tekmark has determined that Nuage Networks Software Defined Networking and Security solutions can support a PCI DSS (v3.2) compliant solution when coupled with an external authentication directory service, extended log retention, network intrusion prevention service, and a secure remote access policy is applied. In addition, Tekmark has determined that this technology can be used for network segmentation and isolation to reduce the scope of compliance. This assessment started in January 2016 and completed in May 2016.

The security audit process consisted of multiple rounds of testing, following a methodology defined by Tekmark. Testing of the infrastructure consisted of several test cases and was executed in a logical and repeatable manner. This phased approach consisted of both automated and manual testing for specific vulnerabilities in an attempt to identify weaknesses that could lead to the exposure of the PCI cardholder data. Page 2 includes an overview of the testing methodology.

Jeremiah Sahlberg
Chief Information Security Officer
Tekmark Global Solutions, LLC

Acronyms

ACL	Access Control List
API	Application Programming Interface
BOOTP	Bootstrap Protocol
CDE	Cardholder Data Environments
CSP	Cloud Service Provider
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IPsec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
NGFW	Next-Generation Firewall
NSG	Network Services Gateway
PCI	Payment Card Industry
PCI DSS	PCI Data Security Standards
PSIRT	Product Security Incident Response Team
SDLC	Software Development Life Cycle
SDN	Software Defined Networking
SD-WAN	Software-Defined WAN
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
UTM	Unified Threat Management
VM	Virtual Machine
VNS	Virtualized Network Services
VRS	Virtual Routing and Switching
VRS-G	Virtual Routing and Switching Gateway
VSC	Virtualized Services Controller
VSD	Virtualized Services Directory
VSG	Virtualized Services Gateway
VSP	Virtualized Services Platform
WAN	Wide Area Network

References

1. "Virtualized Service Platform: Policy-based security automation and micro-segmentation overview", Nuage Networks Whitepaper http://www.nuagenetworks.net/resources/whitepapers/

2. Payment Card Industry Security Standard Council Data Security Standard https://www.pcisecuritystandards.org/

3. Visa Breach: https://usa.visa.com/support/small-business/data-security.html

4. MasterCard Security: https://www.mastercard.us/content/dam/mccom/en-us/documents/rules/SPME-manual-final-march-2016.pdf -

nuagenetworks
From Nokia