White Paper

Cisco ACI and PCI Compliance Scope Reduction: Verizon Audit, Assessment, and Attestation

[1] Cisco Industry Solutions: The Art of Compliance

Contents

Executive Summary

Every time customers use a credit card to make a purchase, they are trusting that the company they purchase from will keep their cardholder data safe. However, reports of data breaches at well-known organizations show that personal information can be compromised. That's why compliance with industry regulations is so important.

Cisco® Application Centric Infrastructure (ACI) uniquely addresses the security needs of the next-generation data center. Instead of the traditional access controls, ACI uses an application-centric approach and policy-based operations model. ACI simplifies Payment Card Industry (PCI) compliance and reduces the risk of security breaches with dynamic workloads while maintaining policy and compliance.

Verizon assessed the PCI compliance posture of the Cisco ACI lab environment. The assessment included the ACI management GUI and ACI fabric (spine and leaf switches). Verizon concluded that ACI can be configured to meet PCI compliance requirements in a customer cardholder data environment.

Verizon also assessed the capability of ACI to provide segmentation for the purpose of isolating PCI system components. Verizon concluded that ACI meets or exceeds the capabilities of traditional segmentation approaches, which use routers and VLANs with explicit, specific access controls[2].

PCI Background

What Is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data.

PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD).

PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional, and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements[3].

Why Is PCI Compliance Important?

Customers put their trust in companies managing their cardholder data every time they make a purchase. They trust that the company will not only deliver the product or service promised, but also that the company will keep their details safe. However, every new report about a data breach makes them a little more concerned that their personal information may be compromised.

The PCI security standards are not law (except in a few U.S. states), and so noncompliance is not punishable by imprisonment; instead, it's enforced through terms of business as part of the contract between the merchant, acquirer, and other parties. Companies that choose not to comply are likely to get less beneficial commercial terms (and may even be refused service), and those that suffer a breach and are found to be noncompliant are likely to face significant penalty fees.

---

[2] Verizon Statement of Opinion

[3] Payment Card Industry (PCI) Data Security Standard, Requirements and Security and Assessment Procedures

Although PCI DSS compliance is not a legal requirement, many territories already have data breach disclosure laws, and the coming few years are likely to see a significant increase in the coverage and power of these laws.

In January 2015, President Barack Obama outlined a plan to push for a federal data breach disclosure law covering all U.S. companies. The proposed law would oblige companies to notify potential victims of a suspected data breach within 30 days. Almost all states already have a data breach law, and many of these are more stringent than Obama's proposal. Some cover only defined industries - typically insurance and healthcare - but set tighter time limits, as short as 5 days, and several include financial penalties.

In March 2014, the European Parliament approved the European Commission's draft proposal to overhaul the 1995 data protection directive. This proposed directive would establish a single, pan-European law for data protection with a supervisory authority. Companies that fail to comply could be fined up to 5 percent of their annual revenue. The law would apply to all companies selling to EU citizens, regardless of where the company is based. Another area in which the law is having an effect on information security is insurance. Several recent cases have confirmed that insurers are not liable to pay for the cost of breaches under commercial general liability policies. And a growing number of companies are finding their claims under specialized data breach insurance policies rejected because they have failed to take adequate security measures[4].

PCI Compliance Requirements

For a company and its infrastructure to be considered PCI compliant, the company must meet the 12 requirements in the standard, working with the acquiring bank and using the tools offered through the PCI Security Standards Council (SSC). PCI DSS compliance is an ongoing process, not a one-time event. Therefore, a company needs to continuously assess its operations, fix any vulnerabilities that are identified, and make the required reports to the acquiring bank and card brands with which the company does business.

In security terms, PCI DSS compliance means that a company adheres to the PCI DSS requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. In operational terms, compliance means that the company is taking appropriate steps to make sure that customers' payment card data is being kept safe throughout every transaction, and that customers - and the company - can have confidence that they're protected against the distress and cost of data breaches.

If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard. You can find out your exact compliance requirements only from your payment brand or acquirer[5].

Becoming Certified as a PCI-Compliant Organization

Qualified Security Assessor (QSA) companies are organizations that have been qualified by the council to have their employees assess compliance with the PCI DSS standard. QSAs are employees of these organizations who have been certified by the council to validate an entity's adherence to the PCI DSS[6].

A Verizon QSA performed an assessment of the PCI compliance and segmentation capabilities of the Cisco ACI solution. Note that different QSAs from different organizations assess and validate companies and their scoped infrastructure individually. Every PCI audit is different, which is why the QSA should be included throughout the entire the process to achieve the goal of a passed PCI audit.

[4] Verizon 2015 PCI Compliance Report
[5] PCI Security Standards Council's Resources for Merchants
[6] PCI Security Standards Council's Approved Companies & Providers

Note: An individual product cannot be considered PCI compliant. A company or business and its properly configured in-scope PCI infrastructure for handling customer card data is what can be certified as PCI compliant.

Verizon's PCI Security Practice

Verizon is a highly respected security consultancy and a trusted voice in the PCI community. Verizon has one of the largest and most geographically distributed teams of QSAs in the world. This scope gives Verizon exceptional insight into what is needed to implement sustainable controls and achieve compliance.

Since 2009 Verizon has conducted more than 5000 assessments, most for Fortune 500 and large multinational companies. Verizon has provided other cardholder data security services since 2003. Verizon also gains valuable insight from running one of the largest global IP networks and managing more than 4000 customer networks. In addition to all this experience, Verizon has invested in extensive research programs, published several of the industry's preeminent ongoing research reports, and made targeted acquisitions of leading security companies, such as Cybertrust.

Verizon's PCI security practice has been approved by the PCI SSC for QSA, Payment Application QSA (PA-QSA), QSA Point-to-Point Encryption (P2PE), and PA-QSA P2PE. Verizon is also an approved PCI Forensic Investigator (PFI) company. As well as security certifications, many of Verizon's QSAs have deep industry knowledge, gained from years of experience working in the retail, hospitality, financial services, healthcare, and other sectors. Being able to draw on this experience helps all Verizon security professionals appreciate customer challenges and put compliance in the context of industry-specific security standards and regulations.

For additional resources related to this research and to find out more about Verizon's PCI security compliance services, please visit http://www.verizonenterprise.com/pcireport/2015[7].

Reducing PCI Scope with Cisco ACI Segmentation and Policy

Establishing PCI Scope

Scoping is the foundation for PCI compliance. The bigger and more complex your processes and systems for storing, processing, transmitting, and accessing CHD, the more difficult it will be to achieve and maintain compliance. Scope reduction is the primary means by which you can limit the size of the compliance task. But scoping does not just affect compliance.

Reducing the DSS scope will result in lower total cost of ownership (TCO), make maintenance of security controls easier, and reduce risk by limiting the attack surface.

For all these reasons, it is strongly recommended that organizations consider implementing a sound scope-reduction strategy. You should do this at the start of your compliance initiative because almost everything else is based on the defined compliance environment. Scope reduction may involve fundamental changes to network architecture and to business processes, and it's not always an easy task. The challenge is to do it without adversely affecting service or incurring prohibitive costs[8].

[7] Verizon 2015 PCI Compliance Report
[8] Verizon 2015 PCI Compliance Report

Traditional Segmentation Challenges

Network segmentation isolates particular groups of users and computers into logical segments on a network to allow security enforcement points to permit or deny traffic between those groups. Traditionally, this discrete separation uses access controls based on network addresses, VLANs, and firewalls. Companies can then apply controls to determine the traffic flows that are permitted between these groups to meet compliance targets. A benefit of this approach is that the network area separated from the PCI environment is no longer within the scope of PCI compliance, simplifying the auditing process in general.

Unfortunately, this method of segmentation can be difficult and time consuming to manage:

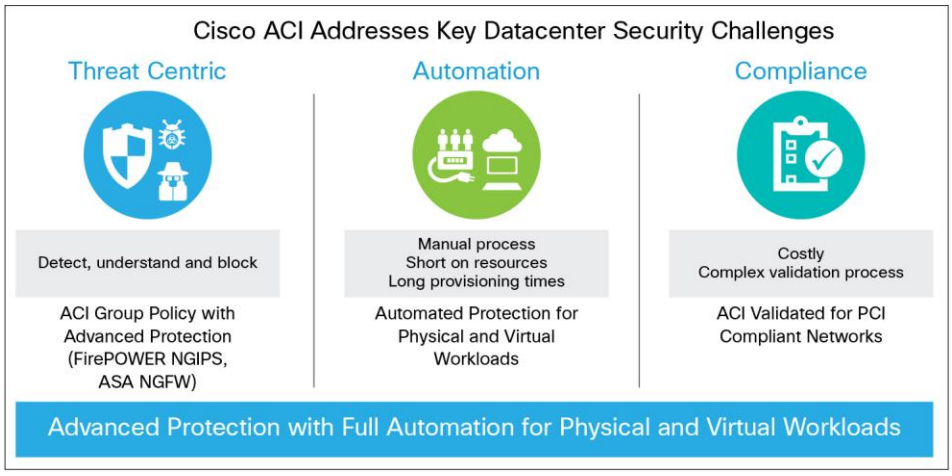
- For some industries, such as healthcare and retail, the activity of implementing a PCI network that is separate from the current “flat” network can be a daunting task because of the scale and complexity of the organizations and the associated costs.
- Access control lists (ACLs) and firewall rules based on IP addresses tend to grow and become hard to audit as more applications are introduced.
- Management of the segmentation policies is manual, with the risk of rules being misconfigured; each branch office needs to be identified individually because each site has its own addressing scheme, making policy management for those branch offices tedious and sometimes difficult.

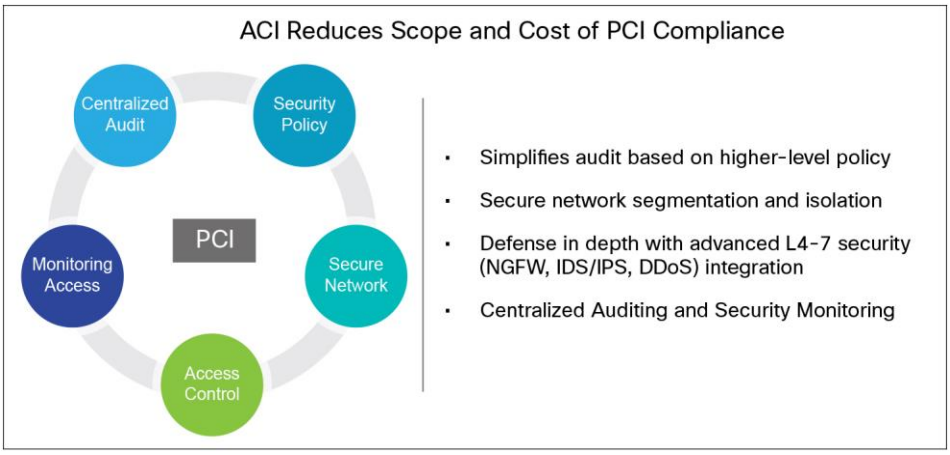
Cisco ACI Segmentation and Policy

The main function of Cisco ACI, in combination with the Cisco Application Policy Infrastructure Controller (APIC), is to simplify the operational aspects of compliance by consistent application and automation of a policy across the infrastructure. This solution helps ensure that segmentation techniques that are defined in policy are enforced across infrastructure platforms.

ACI enables unified security policy lifecycle management with the capability to enforce policies anywhere in the data center across physical and virtual workloads. It offers complete automation of Layer 4 through 7 security policies and supports a defense-in-depth strategy with broad ecosystem support while enabling deep visibility, automated policy compliance, and accelerated threat detection and mitigation. ACI is the only approach that focuses on the application by delivering segmentation that is dynamic and application centered (Figure 1).

Figure 1. Cisco ACI





ACI abstracts away tedious-to-implement and error-prone traditional network concepts such as subnets, VLANs, ACLs, quality of service (QoS), and services and uses a policy-based model. Using the ACI policy model, the administrator simply defines an application profile that specifies different groups of devices and tiers of an application ("who") and inserts contracts that identify who can talk to whom, and what each group member is allowed to talk about.

ACI provides segmentation through isolated multitenancy on a single physical fabric and uses the groups - endpoint groups (EPGs), bridge domains, private networks (similar to Layer 3 Virtual Routing and Forwarding [VRF] instances) - and contracts to segment PCI-related hosts from hosts that are out of scope. Contracts are similar to access lists and are used to deny all traffic access except business-justified access. By bringing the higher-level application language used by the ACI policy model to the network, segmentation and scope reduction can be easily achieved.

Most importantly, ACI implements an allowed list "zero trust" model in which no communication is allowed between EPGs until contracts are in place. This approach is quite different from traditional "plug-and-play" Ethernet switching, in which trust and policy are based on physical location and VLAN boundaries, and traffic is allowed unless blocked listed.

Benefits of segmentation and the allowed list policy-based approach with ACI include:

- Policy-based segmentation: ACI enables detailed and flexible segmentation of both physical and virtual endpoints based on group policies, thereby reducing the scope of compliance and mitigating security risks.
- Automated compliance: ACI helps ensure that the configuration in the fabric always matches the security policy. Cisco APIs can be used to extract the policy and audit logs from the APIC and create compliance reports (for example, a PCI compliance report). This feature enables real-time IT risk assessment and reduces the risk of noncompliance for organizations.
- Integrated Layer 4 security for east-west traffic: The ACI fabric includes a built-in distributed Layer 4 stateless firewall to secure east-west traffic between application components and across tenants in the data center.

- Open security framework: ACI offers an open security framework (including APIs and OpFlex protocol) to support advanced service insertion for critical Layer 4 through 7 security services such as an intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), and next-generation firewall (NGFW) services (such as the Cisco Adaptive Security Virtual Appliance (ASAv), the Cisco ASA 5585-X Adaptive Security Appliance, and third-party security devices) in the application flow regardless of their location in the data center. This feature enables a defense-in-depth security strategy and investment protection.
- Deep visibility and accelerated attack detection: ACI gathers time-stamped network traffic data and supports atomic counters to offer real-time network intelligence and deep visibility across physical and virtual network boundaries. This feature enables accelerated attack detection early in the attack cycle.
- Automated incident response: ACI supports automated response to threats identified in the network by enabling integration with security platforms using northbound APIs.

For more information about ACI objects such as tenants, EPGs, bridge domains, and more, please refer to the following white paper: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731310.html.

Validation Overview

PCI DSS Requirements

To be considered PCI compliant, a company must maintain, document, and prove a configured infrastructure that meets PCI DSS requirements, which include:

- Build and maintain a secure network and systems:
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect cardholder data:
  - Requirement 3: Protecting stored cardholder data.
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks.
- Maintain a vulnerability management program:
  - Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.
  - Requirement 6: Develop and maintain secure systems and applications.
- Implement strong access control measures:
  - Requirement 7: Restrict access to cardholder data by business and need to know.
  - Requirement 8: Identify and authenticate access to system components.
  - Requirement 9: Restrict physical access to cardholder data.
- Regularly monitor and test networks:
  - Requirement 10: Track and monitor all access to network resources and cardholder data.
  - Requirement 11: Regularly test security systems and processes.
- Maintain an information security policy:
  - Requirement 12: Maintain a policy that addresses information security for all personnel[9].

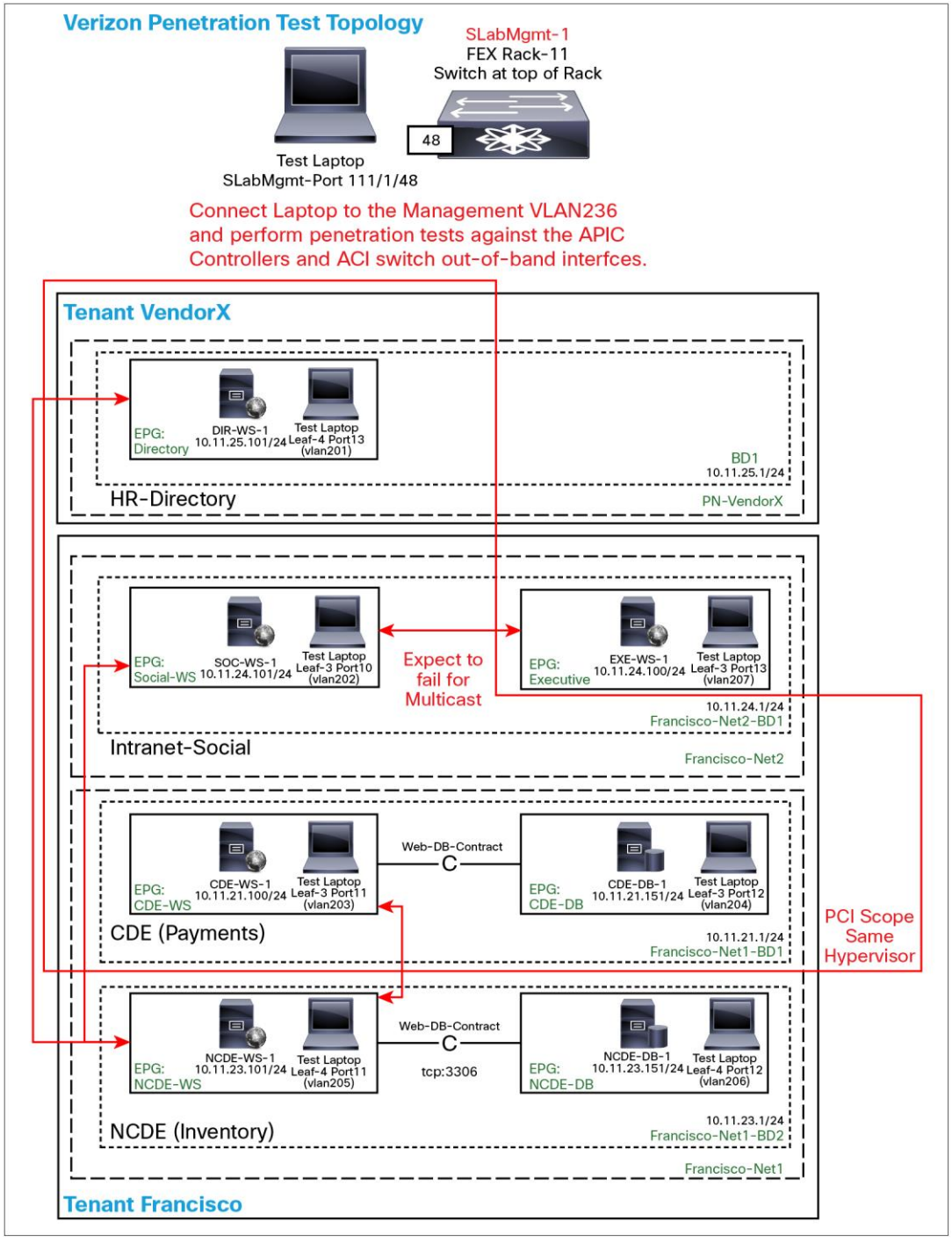
[9] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures

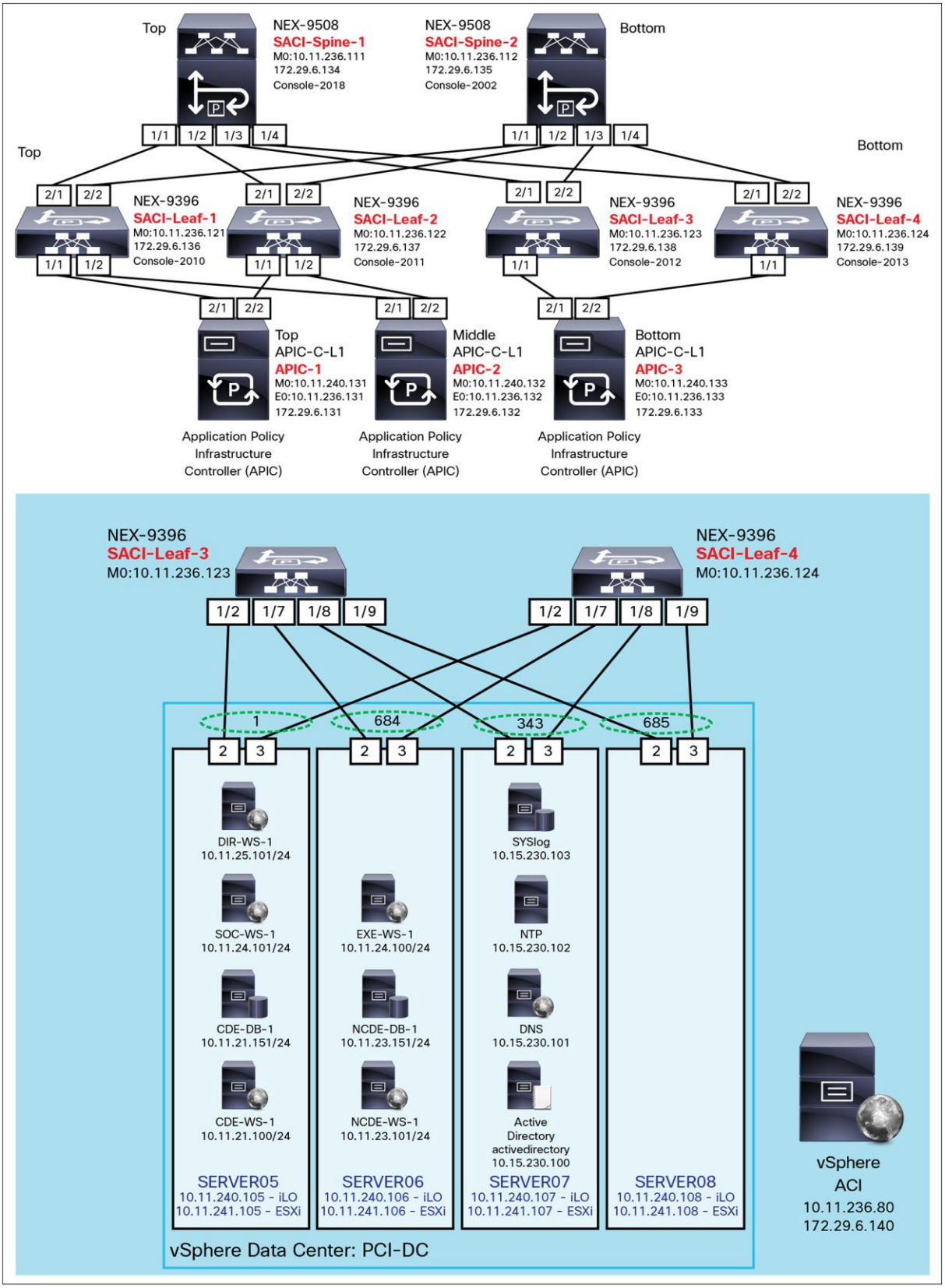
Note: Shared hosting providers have additional PCI DSS requirements. Refer to Appendix A in the following document for hosting provider requirements: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

Cisco ACI PCI Lab Topology

Figure 2 illustrates the Cisco ACI topology built for the Verizon PCI penetration test and audit.

Figure 2. Cisco ACI Topology for Verizon PCI Penetration Test





Validation Details

Capability Assessment

Verizon QSA assessors were invited into Cisco's laboratories to evaluate the effectiveness of an infrastructure based on Cisco ACI for the purposes of reducing PCI scope and passing a PCI audit. Verizon performed and observed a series of tests, including network penetration testing, to evaluate network segmentation using tenants, EPGs, contracts, private networks, and bridge domains.

Based on assessment and observations, Verizon concluded that the ACI objects tested meet, and exceed, the intent of segmentation, as required by the PCI DSS, for purposes of PCI scope reduction and restriction of access to cardholder data.

Note: The scope of the initial PCI audit outlined in this document included tenant, inter-EPG traffic, bridge domain, and private network isolation. Layer 4 through 7 service integration and external Layer 3 connections were not included in this phase of the ACI PCI audit. These features will be included in a later audit.

Cisco and Verizon evaluate Cisco products for PCI environments using the same methods that are used to evaluate a merchant's environment. Each component requires that specific capabilities be deployable in a compliant environment.

Verizon Statement of Opinion

Verizon's Statement of Opinion validating that the Cisco ACI lab setup and configuration successfully adhered to PCI DSS standards is presented here in Figure 3.

Figure 3. Verizon Statement of Opinion Regarding Cisco ACI PCI DSS Compliance

[[Need Figure 3]]

Statement of Opinion

Regarding PCI validation and network segmentation testing performed by Verizon on the Cisco Application Centric Infrastructure (ACI) solution.

prepared for **Cisco Systems, Inc.**

Contents

Executive Summary

Cisco Systems, Inc. (Cisco) engaged Verizon to conduct PCI compliance validation and a Penetration Test of the Cisco Application Centric Infrastructure (ACI) solution in a lab environment. The PCI compliance validation was conducted over several WebEx sessions, from December 5, 2014 to February 10, 2015. The Penetration Test assessment was conducted from February 24, 2015 to February 27, 2015.

PCI Compliance Validation

Verizon assessed the PCI compliance posture of the Cisco ACI lab environment, including ACI management GUI and ACI fabric (core and leaf switches). While some PCI compliance recommendations were made during the assessment, Verizon believes the Cisco ACI solution can be configured to meet PCI compliance requirements within a customer cardholder data environment. Verizon also assessed the Cisco ACI's ability to provide segmentation, for purposes of segmenting and/or isolating PCI system components and believes the solution meets or exceeds the capabilities of segmentation using routers VLANs with explicit, granular ACLs. While the solution can be used for purposes of traditional PCI segmentation, it is important to note the solution does not provide stateful packet inspection, and therefore, would not meet PCI requirements for segmentation of wireless networks.

Penetration Testing

Verizon found that the ACI implementation successfully enforced network segmentation during the engagement. Verizon found that multicast and broadcast traffic was forwarded between Endpoint Groups (EPG) located in the same Bridge Domain (BD). Prior to the test, Cisco acknowledged that this is expected behavior.

Based on the results of the ACI Penetration Test, Verizon found that while ACI can successfully perform network segmentation, proper configuration of ACI policies is required in order to ensure effective enforcement across the environment in which it is deployed.

Scope and Approach

PCI Validation

Verizon performed an assessment of the PCI compliance and segmentation capabilities of the Cisco ACI solution. A Verizon Qualified Security Assessor (QSA) performed the following validation through several conference calls and WebEx sessions, December 5, 2014 through February 10, 2015:

- Reviewed supporting architecture components (documentation and on console) - Cisco ACI Controller (Management Console), ACI Core Switch and ACI Leaf Switch components
- Observed authentication settings and ability to forward authentication to Active Directory to support PCI password and lockout requirements
- Observed command-line OS hardening for ACI Controller, Core and leaf switch components (configured services (GUI), listening services (CLI), authentication settings, syslog settings, administrative service settings (e.g. SSH, HTTPS, SNMP), NTP settings, and audit trail settings
- Observed ACI fabric policy creation for ingress/egress fabric filtering
- Observed live access attempts, captured log output (Splunk Logs), and Nessus scan results for ingress and egress access attempts, originating from untrusted and trusted sources

Penetration Testing

Cisco engaged Verizon to conduct a Penetration Test of the ACI solution in a lab environment. The scenarios undertaken during the ACI Penetration Test were:

- Conduct Kickoff Meeting: Verizon conducted a kickoff meeting with Cisco to review the objectives of the ACI Penetration Test, to obtain any additional required information, and to exchange contact information.
- Perform Internal Penetration Test: Given network diagrams and access to Cisco's lab environment, the Verizon consultant evaluated the effectiveness of ACI's network segmentation controls.
- Test Scenario: Verizon conducted the network segmentation testing in Cisco's lab environment. Cisco configured the lab to contain two Tenants, each with one or multiple Private Networks, Bridge Domains, and Endpoint Groups (EPG). Virtual Machines were deployed in each EPG, and network segmentation between the constructs was enforced by ACI. The Verizon consultant also connected a test laptop to each EPG. Finally, Verizon moved between all EPGs and attempted to communicate with the VMs and test laptop in each EPG, across each construct boundary.
- Statement of Opinion: Verizon prepared a Statement of Opinion based on the network segmentation testing performed by Verizon within Cisco's lab environment.

Opinion

Based on the results of the ACI PCI validation and Penetration Test, it is Verizon's opinion that ACI can successfully perform network segmentation, although proper configuration of ACI policies is required in order to ensure effective enforcement across the environment in which it is deployed. It is also Verizon's opinion that the Cisco ACI solution can be configured to meet and not impede PCI compliance requirements within a customer cardholder data environment.

Penetration Test Detailed Methodology

The following excerpts from Verizon's penetration test outline the test scenarios, phases, and tools used.

Lab Environment

Cisco provided the Verizon security consultant with access to a lab in which network segmentation was implemented using Cisco ACI. The lab environment consisted of the following ACI logical constructs:

- Tenants
- Private networks
- Bridge domains
- Endpoint groups (EPGs)

Network Segmentation Test Scenarios

The test scenarios used a multitenant environment. Cisco configured the lab to contain two tenants, each with one or multiple private networks, bridge domains, and EPGs. Virtual machines were deployed in each EPG, and network segmentation between the constructs was enforced by ACI. The Verizon consultant also connected a test laptop to each EPG. Finally, Verizon moved between all EPGs and attempted to communicate with the virtual machines and test laptop in each EPG, across each construct boundary.

Network Segmentation Penetration Testing

In the aforementioned scenarios, Verizon conducted network-based penetration testing of the lab environment. The objective of the penetration testing was to attempt to bypass the network segmentation controls implemented via ACI. Steps undertaken in the process are as follows:

Phase I: Discovery

Verizon captured packets on the network segment, gathering information pertaining to the environment from the observed traffic.

Phase II: Probing

Verizon sent a series of probes to segmented hosts to confirm that network segmentation was functioning as designed. These probes included:

- Ping (Internet Control Message Protocol [ICMP], Transmission Control Protocol [TCP] ping, User Datagram Protocol [UDP] ping, etc.)
- Traceroute
- Various types of port scans

Phase III: Spoofing

Verizon attempted to bypass ACI network segmentation policies by sending packets with various combinations of spoofed IP and MAC addresses.

Phase IV: Exploitation

Verizon attempted to bypass ACI network segmentation by using VLAN double-encapsulation. Verizon also attempted to exploit issues related to misconfigured ACI policies.

Tools Used

- Wireshark
- Ping
- HPing (packet generator)
- Traceroute
- TCPtraceroute
- Nmap (port scanner)
- Scapy (packet crafting tool)
- Yersinia (network protocol exploitation tool)
- Ettercap (network security testing tool)

Infrastructure Penetration Testing

Verizon conducted network-based vulnerability testing of the ACI infrastructure and blind, unauthenticated testing of web applications. The objective of the penetration testing was to identify security weaknesses that could be exploited by motivated, malicious individuals to gain unauthorized access to the infrastructure. Where a vulnerability was identified, Verizon sought to demonstrate the capability to gain unauthorized access to systems or sensitive data through exploitation of the issue identified. Verizon used a series of vulnerability scanning tools and manual techniques to identify, validate, and exploit security vulnerabilities. Testing was conducted in four phases: discovery, vulnerability identification, verification, and exploitation.

Phase I: Discovery

Verizon performed reconnaissance to gather information, including registration data, operating system version and patch level, and service version and configuration.

Phase II: Vulnerability Identification

Verizon used a combination of commercial and open-source tools to identify security vulnerabilities in tested systems.

Phase III: Verification

Vulnerabilities identified by these tools were confirmed by our security staff to verify that there were no false positives.

Phase IV: Exploitation

Verified vulnerabilities were exploited to demonstrate that unauthorized data or system access can be obtained.

Network Vulnerability Testing

Verizon performed base-level security scans of all the hosts to identify services and issues within these services. After this scan was complete, manual techniques were employed to identify risks that automated tools cannot identify. The testing techniques included:

- Host identification: Identify live hosts through ICMP, reverse Domain Name System (DNS) lookup, and port scans for common services.
- Network route mapping: Map the network route to each system using traceroute and VisualRoute.
- Operating system identification: Identify the operating system of each host through analysis of responses to specially crafted TCP/IP packets.
- Network services enumeration: Enumerate the services available on each system through TCP and UDP port scanning by using tools such as Nmap.
- Network service exploration: Build a detailed profile of each service through automated and manual banner grabbing and service exploration without exploiting any service vulnerabilities.
- Vulnerability identification: Use commercial and open-source vulnerability scanners to identify known vulnerabilities on each system.
- Vulnerability exploitation: Use commercial, open-source, and private exploitation tools and methods to gain access to the system or sensitive data.

Tools Used

- Nmap
- Ping and traceroute
- Nessus
- WebInspect
- Burp Suite Professional
- Metasploit

Conclusion

The Cisco ACI solution simplifies both the scope of infrastructure handling cardholder data required to be in an audit, and the ease of passing a PCI audit by leveraging the Cisco ACI architecture. Verizon's Qualified Security Assessors (QSA) have validated within Cisco's labs that Cisco ACI can be used to reduce the scope for PCI and simplify the management of segmentation.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-734518-00 05/15