



# CHAPTER 1

## Solution Overview

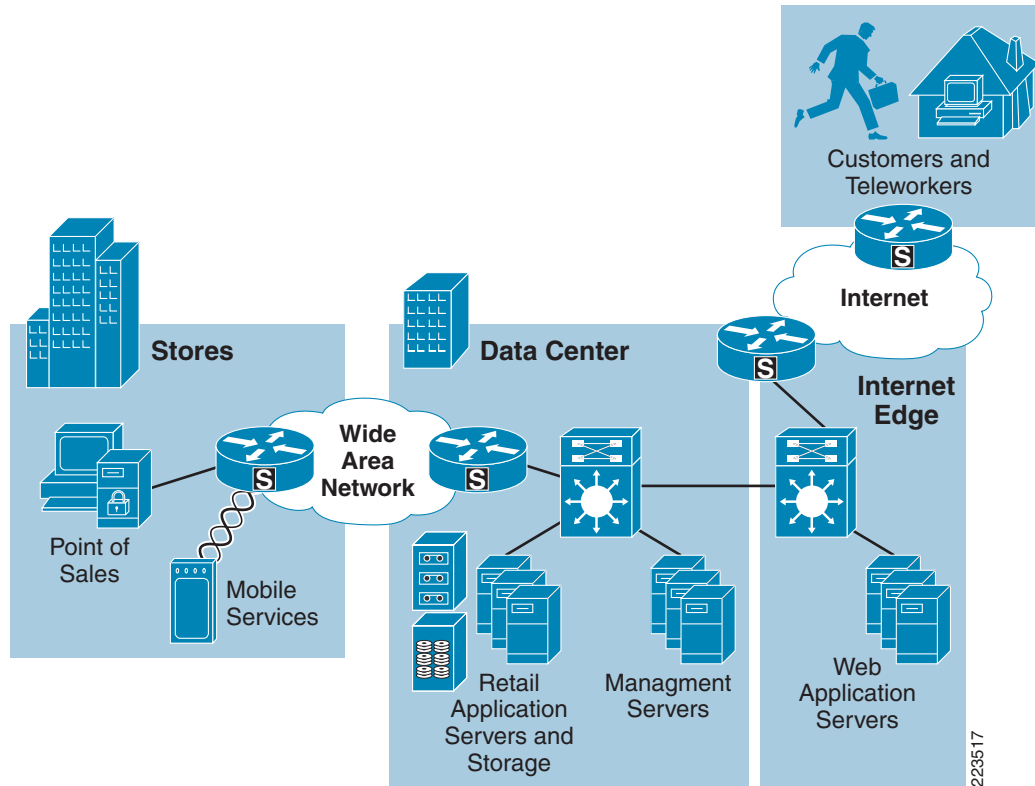
---

### Executive Summary

The Cisco PCI Solution for Retail is a set of configurations and recommendations for data at rest and data in motion on wired and wireless networks. The solution is designed to conform to the Payment Card Industry (PCI) Data Security Specification (DSS) 1.2. The solution was built and tested using point-of-sale (POS) systems, payment devices, wireless client devices, data encryption software, Cisco network infrastructure, and validated by a PCI Qualified Security Assessor (QSA) audit partner. The result is a set of retail store, data center, and Internet edge designs that simplify the process of a retailer becoming PCI compliant.

To pass PCI compliance, a retail company must address its procedures, security policies, and technical infrastructure so that it can demonstrate adherence to the PCI v1.2 specification sub-requirements. A QSA must perform an audit of the company to verify that each applicable sub-requirement is either addressed or deemed not applicable to that specific company. Once a company becomes compliant, there are ongoing requirements to maintain compliance. The Cisco PCI Solution for Retail demonstrates how to build the infrastructure, secure data in transit and at rest, and how to monitor and maintain the configurations. [Figure 1-1](#) show the Cisco PCI Solution for Retail conceptual architecture.

Figure 1-1 Cisco PCI Solution Conceptual Architecture



## Solution Justification

The PCI DSS version 1.2 affects all retailers that process, store, or transmit credit or debit card information over their networks. Cisco customers have asked for a comprehensive recommendation on how to design, manage, monitor, and remediate a store network that has been audited and meets QSA audit guidelines.

## Target Market

Retailers who process payment transactions are required to meet PCI DSS guidelines. Typical mid-market and enterprise retailers process 100,000 or more payment card transactions per year and are therefore part of the target market. By modeling retail store networks, data center and the Internet edge infrastructures, the solution is adaptable to many different retail deployments. Payment card companies and their merchant banks have differing guidelines around the world in the way they classify Merchant levels and the corresponding method of demonstrating compliance. Consult your payment card company or merchant bank for specific details on their requirements based on the number of transactions your business stores, process, or transacts per year. [Table 1-1](#) lists and describes different PCI merchant levels that are common with Visa, Inc. in the United States (source Visa USA).

**Table 1-1 PCI Merchant Levels**

Merchant Level	Description
1	<ul style="list-style-type: none"> <li>Any merchant, regardless of acceptance channel, processing over 6,000,000 VISA transactions per year.</li> <li>Any merchant that has suffered a hack or an attack that resulted in an account data compromise.</li> <li>Any merchant that VISA, at its sole discretion, determines should meet the level 1 merchant requirements to minimize risk to the VISA system.</li> <li>Any merchant identified by any other payment card brand as level 1.</li> </ul>
2	Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 VISA transactions per year.
3	Any merchant processing 20,000 to 1,000,000 VISA e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 VISA e-commerce transactions per year, and all other merchants, regardless of acceptance channel, processing up to 1,000,000 VISA transactions per year.

## Applications and Services Supported by the Solution

The primary applications that are supported by the Cisco PCI Solution for Retail include:

- Highly secure transport of payment card information across the wired and wireless network.
- Highly secure storage of data at rest, at the electronic cash register, on an in-store server, or in the data center.
- The solution includes network and systems management, monitoring, and remediation services.

## Solution Benefits

The solution demonstrates how to create retail networks that conform to PCI DSS 1.2 guidelines. Customers can simplify the process of becoming PCI compliant by building a similar network with the recommended configurations and best practices.

In addition, the solution provides the following benefits:

- Insight into the Cisco Connected Retail architecture based on global best practices.
- A scalable set of reference designs that can be used as a reference during the PCI compliance process.
- A detailed analysis and mapping of Cisco, and partner components and their relationship with PCI DSS sub-requirements.
- Insight into compensating controls and best practices to harden retail network and data systems.
- A centralized management “tool kit” that provides operational efficiency compared to managing the distributed endpoints individually.

- Insight into the PCI audit process by providing a lab model and associated Report on Compliance (ROC) from Verizon Business (QSA).

## Solution Features and Component Highlights

The solution features and components consists of the following:

- [Network Systems](#)
- [Hosts and Servers](#)
- [Monitoring and Management](#)
- [Encryption](#)
- [Authentication](#)
- [Policy](#)
- [Other Applications and Services](#)

### Network Systems

- **Routing**—Cisco Integrated Services Router (ISR), mid-range routers and Catalyst 6500 Supervisor's provide routing services across the architecture. Each retail store uses either a single or pair of ISRs to consolidate WAN services, routing, identity, and security services into a single platform with local and centralized management services. The same platform can also serve as the hub for network quality-of-service (QoS), voice call control, and other application services. The WAN aggregation and Internet Edge routers are Cisco 7206VXR routers that support a wide variety of WAN interfaces and allow specific types of traffic into the data center.
- **Switching**—Cisco Catalyst Ethernet switches connect the IP endpoints to the routed services. Catalyst switches support LAN speeds from 10Mbps to 10Gbps. They can also integrate Power over Ethernet (PoE) services over the same cable to power wireless access points, IP telephones, and other 802.3AF-based devices. Catalyst switches use VLANs, access control and quality-of-service to segments LAN traffic based on security or business requirements.
- **Wireless**—Cisco Unified Wireless network provides centrally managed wireless connectivity to mobile computers and phones. The same wireless infrastructure includes integrated wireless intrusion detection, highly secure connectivity, and central management through the Wireless Control System (WCS). Each retail store network shares the same dual-radio infrastructure design regardless of the size of the store. This permits adequate network capacity for high-bandwidth retail applications such as streaming media to mobile kiosks or digital signs. It also provides adequate path isolation and segmentation to ensure that payment data is separately encrypted from the other types of retail business data. The Unified Wireless network can operate as distributed access points with local management, or as a centrally managed wireless-controller-based system.

Specific Cisco Unified Wireless network systems used in this solution include:

- Cisco 1100-series and 1200-series access points simultaneously support 2.4Ghz and 5Ghz 802.11 network connectivity, advanced security services, and central management control.
- Cisco Unified Wireless Controllers include the Wireless LAN Control Module for the ISR platform and the 4000 Series controller used in the large store. The small store features the Hybrid-Remote-Edge-Access-Point (H-REAP) protocol with centralized controller modules. This design supports local authentication in the event that the store loses connection to the central controller.

- Services Aggregation
  - Cisco Catalyst 6500's provide the high-performance, highly scalable and highly available platform to transport payment traffic from the store WAN routers, across the core switches and down to the Server Access Layer.
  - Firewall Services Modules (FWSM) are used to allow or block traffic, based on a central policy.
  - Cisco Adaptive Security Appliances can also be used to deliver Firewall, IDS, and VPN services.
  - Intrusion Detection Module 2 (IDS2) is used to monitor and enforce policy sent from central management system.
  - Cisco Application Control Engines filter content and balance traffic loads based on central policy.
  - Wireless controllers, part of the Cisco Unified Wireless architecture, centralize the control and management of wireless infrastructure installed across the network.
  - These systems work together to segment payment and POS transaction log traffic based on central policy.
- Storage
  - Electronic cash registers, POS servers, and other PCs are used to recreate a typical retail POS transaction environment. Storage Area Network director-class switches connected to EMC storage disks create a typical data center storage environment.
- Internet Edge
  - Edge routers, security appliances, high-performance, and highly secure services aggregation switches connect Internet services to the enterprise data center network.
  - E-commerce, main, and web servers and hosts are connected to the inside of the Internet edge simulating web application servers.

## Hosts and Servers

- Point-of-Sale—NCR POS terminals and SurePOS servers running the NCR Advanced Checkout System software were used to create a typical retail environment. Earlier version of the solution used IBM and Wincor-Nixdorf POS devices. These devices use a combination of RSA data security applications to encrypt access to critical payment or administrative data on the system. Cisco Security Agent (CSA) software delivers application firewall, file integrity, anti-virus, and host intrusion prevention services. It can be configured to specifically allow retail business application functions within each device. It can stop “day zero” attacks and be customized to meet the wide-ranging requirements of retail business computing at the cash register, desktop, kiosk, or server level.
- Payment Devices—VeriFone and IBM payment devices were used to simulate a retail payment environment. These devices must meet PCI Payment Encryption Device (PED) specifications to be used in the solution.
- Host and Server Security—CSA is a combination of software installed on each Windows or Linux-based POS device in the store including payment devices, POS registers, and POS servers. CSA is also installed on each of the solution management servers in the data center. CSA can also be installed on store manager PCs and any other desktop or server installed at the retail business location.

- Centralized Cisco management services manage, monitor, provision, analyze, remediate, and report on all elements of the distributed system. These services can also create reports for audit and forensic requirements.

## Monitoring and Management

The suite of Cisco management applications used in this solution includes:

- Cisco Security Manager (CS-M)—The operational control platform for the security services distributed across ISR routers and security appliances. It can design, provision, and report on firewall, IDS/IPS, and VPN services throughout the retail store networks.
- Cisco Security Monitoring, Analysis and Response System (CS-MARS)—Central log monitoring, correlation, and reporting platform for Cisco network device security alerts (e.g., ASA/FWSM/ISR firewall logs and wired and wireless IDS/IPS alerts) within the large, medium, and small retail environments, as well as the data center environment. In addition, Cisco Security Agent alerts are forwarded to CS-MARS created holistic event correlation system across the enterprise.
- Cisco Security Agent Management Center (CSAMC)—The central management, provisioning, and reporting system for the CSA software installed on POS and store operation devices in each retail store network.
- Wireless Control System (WCS)—The central manager of the Unified Wireless network infrastructure and services installed in each retail store network.
- CiscoWorks LAN Management System (C-LMS)—Supports the central control and collection of running and startup configurations from a wide array of Cisco network devices. C-LMS uses Cisco Discovery Protocol, SNMPv3, and other management protocols to securely communicate from the data center to the retail store network.
- CiscoWorks Network Compliance Manager (C-NCM)—Tracks and regulates configuration and software changes throughout the network infrastructure. IT provides superior visibility into network changes and can track compliance based on PCI guidelines and company policy.

## Encryption

Two forms of encryption are used to meet PCI guidelines: data at rest and data in motion.

### Data at Rest Encryption

- RSA File Security Manager—File level encryption system used to encrypted sensitive data in the stores or data center.
- RSA Key Manager—Enterprise class key management system used to manage the secure delivery and use of encryption keys throughout the enterprise.
- RSA enVision—A log management and analysis application that is used to manage the RSA SecurID tokens that are part of the authentication component provided below.

### Data in Motion Encryption

- Cisco Virtual Private Network (VPN) software—Used to encrypt payment data as it is transmitted across any public network segments. VPNs typically use IPsec with either 3DES (triple DES) or 256-bit AES encryption.

- Secure Socket Layer (SSL) services—Used to encrypt traffic from Internet-based web applications and when remotely administering infrastructure devices (SSHv2).
- Wi-Fi Protected Access version 2 (WPA2)—Used between wireless clients and Cisco access points uses AES encryption for POS and payment data transmitted across the in-store wireless LAN (WLAN).

## Authentication

Accounting, Authorization and Authentication (AAA) services used to determine identity and authorize access to systems, devices or services within a components. Highlights of authentication:

- Cisco Secure Access Control Server (CS-ACS)—The central AAA service broker of the infrastructure and remote access elements of the solution CS-ACS is used to enforce the management and control policy for operational access to the network devices and services running on the network. CS-ACS provides access control for network, host, and servers used throughout the solution.
- RSA Access Manager—The access control system required for the RSA applications in the solution.
- RSA Authentication Manager software—Works with RSA Authentication Agents to enhance security with strong, two-factor user authentication provided by the time synchronous-based RSA SecurID tokens. This solution was required of remote users accessing retail payment applications or VPN-based connections to the Internet edge.

## Policy

Two ways to look at policy within this solution include the management of policy and the creation of policy to enforce PCI guidelines:

- Cisco Security Manager is the operational control platform for the security services distributed across Cisco routers and security appliances. It can design, provision, and report on firewall, IDS/IPS, and VPN services throughout the retail store networks.
- Cisco Security Agent (CSA) can also enforce host and server level policy by limiting access to specific files, folders, and services. CSA is managed through CSA management console which maintains the central policy and can quickly ensure that new devices meet a baseline-level of requirements through its behavioral approach threat deterrence.

## Other Applications and Services

The following application services and partner products were required to create the operational environment and meet the PCI requirements but are not specifically part of the overall solution set:

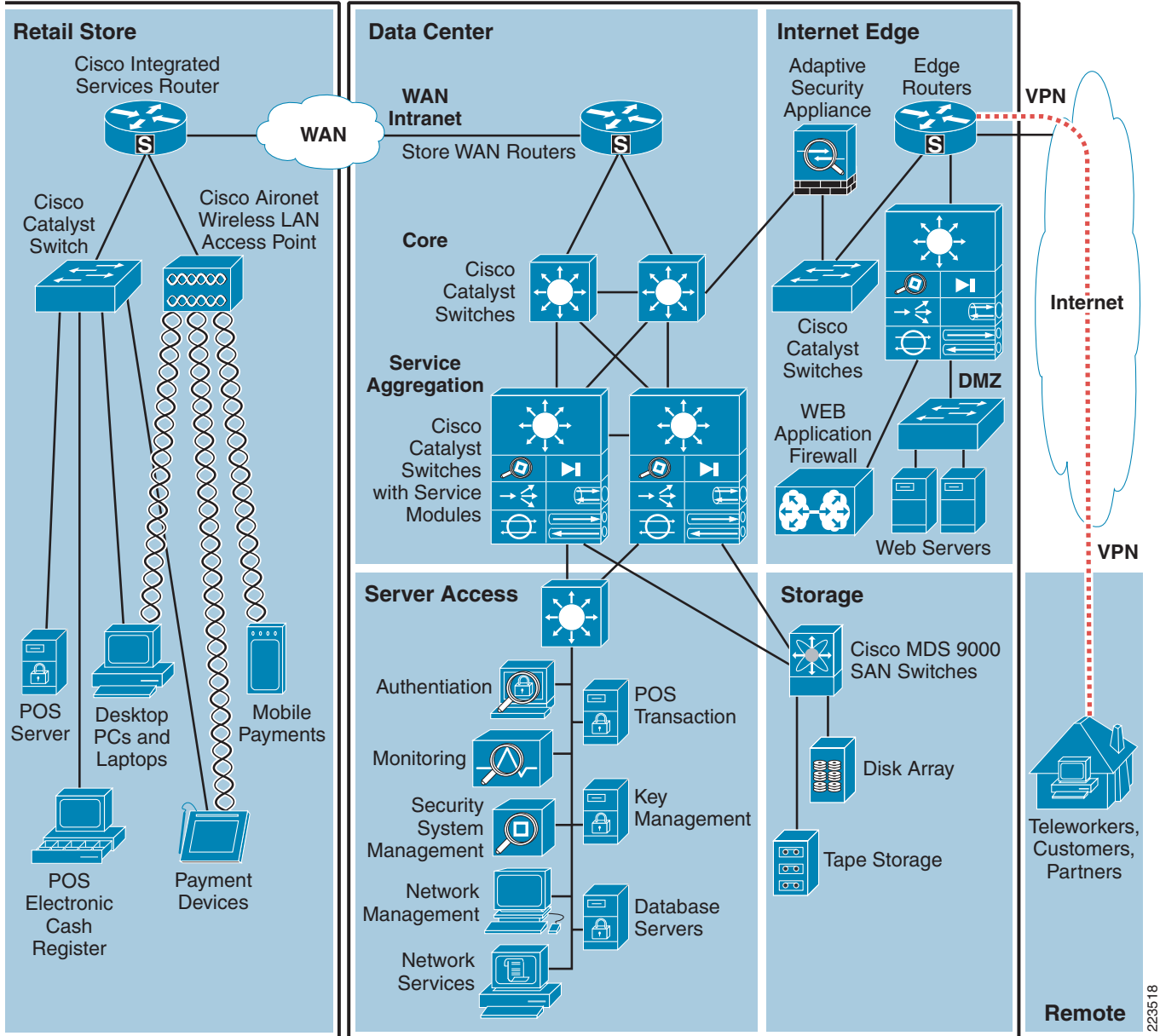
- Microsoft Active Directory
- Microsoft DNS/DHCP server
- Microsoft Exchange server for alert notification services
- Microsoft Retail Management Server POS software
- Intermec wireless handhelds
- Network Time Protocol server for central time management
- Wincor-Nixdorf POS hardware

- IBM POS hardware

These are covered in more detail in Chapter 4, “Implementing and Configuring the Solution,” and the appendices.

Figure 1-2 shows a conceptual view of the Cisco PCI Solution for Retail.

Figure 1-2 Cisco PCI Solution for Retail—Conceptual View



223518

# Scope of the Solution

## Architecture

Cisco and its solution partners have a wide range of products portfolio that could potentially be used to address the PCI specification. The products selected for this solution were chosen for their immediate relevance to a retail company with an enterprise business network and data security environment, while allowing auditing and lab testing within the project timelines.

This solution guide includes store reference designs that connect to a central data center over a wide-area network. It also includes Internet edge reference designs that transport Internet-based users to the Extranet or De-Militarized Zone (DMZ). The solution includes and assumes centralized management, but does not include central connection to an actual retail payment or adjudication service.

This release of the Cisco PCI Solution for Retail can be used as a foundation to build upon additional products and location reference designs in the future. This solution includes the following:

- Reference store designs that connect to a central data center over a private wide-area network.
- Data center design and centralized management servers that assist a retailer business in satisfying PCI requirements.
- An Internet edge design that connects Internet-based consumers, workers, and partners to data center or DMZ-based applications.

The solution does *not* include the following:

- Data center connections to the actual payment service provider, acquiring bank or other merchant services.
- Actual e-commerce architecture, systems, and applications.

## PCI Compliance

Most of the PCI standards (for example, PCI DSS 1.2, <https://www.pcisecuritystandards.org/index.htm>) are focused on policy and procedure within a retail company. However, specific sub-requirements of the PCI standard address technical infrastructure and its configuration. The Cisco PCI Solution for Retail provides Cisco networking equipment, partner software applications, reference architecture, and configurations to satisfy this technical infrastructure aspect of the PCI compliance process. Although this solution does provide related guidance to some of the policy-based sub-requirements, companies seeking to become PCI compliant should contact a security service provider for assistance with their security policy and company procedures.

The Cisco and partner products used in this solution successfully addressed the PCI specification within this specific set of configurations. Retail Companies purchasing these products to address PCI should consult a QSA for their own particular environment because elements within it may differ from this solution.

# Solution Results

These results are applicable to the specific solution that was created and audited in the Cisco lab. For detailed notes on each solution feature and the audit findings, strengths, and weaknesses, see [Chapter 3, “Solution Components—Best Practices and PCI.”](#) Specific implementation and configuration details are provide in [Chapter 4, “Implementing and Configuring the Solution.”](#) Finally, for a complete audit report by Verizon Business on this specific lab, see [Appendix F, “Report on Compliance \(ROC\).”](#)

[Table 1-2](#) summarizes the solution features per PCI requirement.

**Table 1-2** *PCI Requirements Satisfied by the Cisco PCI Solution for Retail*

Solution Feature	PCI Value
<b>Requirement 1: Install and maintain a firewall configuration to protect cardholder data</b>	
Cisco Firewall Service Module (FWSM), Cisco Adaptive Security Appliance (ASA)	Network security (firewall segmentation/filtering), stateful filtering
CiscoWorks (LMS and NCM), C-SM	Configuration management/secure configurations
<b>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.</b>	
ISRs, FWSM, ASA, switches, wireless devices, WCS, CS-ACS, CiscoWorks (LMS and NCM), Cisco Security Agent (CSA), CS-M	Vendor defaults changed
WCS/wireless controllers	Wireless security (WPA/WPA2, SSID broadcast disabled)
ISRs, FWSM, ASA, switches, wireless controllers (CSA Manager, CS-M, CiscoWorks (LMS))	Best practice security parameters enabled
ISRs, FWSM, ASA, switches, wireless controllers (CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS)	Non-console encrypted administrative access
<b>Requirement 3: Protect stored cardholder data</b>	
NCR Advanced Checkout Solution (NCR-ACS) software and terminals	Certified to PCI PIN entry device standard requirements
Verifone VX and MX payment devices	Certified to PCI PIN entry device standard requirements
RSA File Security Manager and Key Manager application	Encrypt access to secure data stored on POS devices and servers
<b>Requirement 4: Encrypt transmission of cardholder data across open, public networks</b>	
Wireless controllers	WPA wireless security
ISRs, Cisco 7200VXR -series routers, ASA	Provide IPsec VPN encryption for data across the retailers' wide area network or Internet-based network circuits.
<b>Requirement 5: Use and regularly update anti-virus software or programs</b>	
CSA	Anti-virus protection, malware/spyware protection, alerting
<b>Requirement 6: Develop and maintain secure systems and applications</b>	
CiscoWorks (LMS and NCM), CS-M (Workflow mode)	Change control and enforcement of compliance configurations
Cisco ACE XML Gateway	Web application protection from OWASP attacks.
<b>Requirement 7: Restrict access to cardholder data by business need-to-know basis</b>	

**Table 1-2 PCI Requirements Satisfied by the Cisco PCI Solution for Retail (continued)**

ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Least-privilege, role-based access
<b>Requirement 8: Assign a unique ID to each person with computer access</b>	
ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Unique user IDs, authenticated access, encrypted passwords, no group/shared IDs/passwords
ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Password strength requirements
ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Account lockout requirements
<b>Requirements 9: Restrict physical access to cardholder data</b>	
No products were tested or audited for this requirement at this time.	See note below <sup>1</sup>
<b>Requirement 10: Track and monitor all access to network resources and cardholder data</b>	
ISRs, Cisco 7200VXR, switches, wireless devices, WCS, CS-ACS, CiscoWorks (LMS) CSA, RSA applications, NCR applications	Audit trails, time synchronization
NCR-ACS terminals, RSA File Security Manager, RSA Key Manager, Cisco CSA	Audit access to actual cardholder data and audit trail data
Ciscoworks (LMS and NCM)	Centrally archive audit log records
<b>Requirement 11: Regularly test security systems and processes</b>	
Wireless controllers	Rogue wireless AP/device detection
ISRs, ASA, IDSM2 (sensor), CS-M (policy, signature updates)	Network IDS
CSA	Host-based IDS
CSA	File integrity
<b>Requirement 12: Maintain a policy that addresses information security for employees and contractors</b>	
Verizon Business, Cisco Advanced Services	Creation and maintenance of security policy

1. Cisco video surveillance and monitoring systems can be implemented to meet this requirement, but this was out of scope of this phase's solution testing effort.

