White Paper

PCI Compliance for Branch Offices: Using Router-Based Security to Protect Cardholder Data

Using credit cards to pay for goods and services is a common practice. Credit cards enable easy and cost-effective business transactions. However, hundreds of millions of personally identifiable customer records have been breached in both high- and low-profile attacks. Many of these instances have involved credit card information.

As a result, there is increased pressure to comply with industry mandates and state and federal regulations, which have been created to enhance privacy, national security, and, in many cases, corporate accountability. Fines, penalties, and lawsuits are just some repercussions of what a company might face if a security breach occurs and the company is out of compliance at the time of the breach. The long-term effect of noncompliance is damage to the company's brand, or reputation, from which they sometimes never recover.

The PCI Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) applies to all businesses, public and private, in any industry that processes, transmits, or stores credit card transactions and cardholder information. PCI DSS provides guidance for securing payment card data and includes a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. Payment card brands such as Visa International, MasterCard Worldwide, Discover Financial Services, JSI, and American Express all require PCI compliance, and any company that fails to comply with the requirements risks stiff penalties.

PCI DSS version 2.0 went into effect January 1, 2011. The lifecycle process for changes to the PCI DSS currently spans three years. During this timeframe, the PCI Council continuously evaluates evolving technology and threats, and, if necessary, may make mid-lifecycle changes to the standards or may provide ongoing supplemental guidance about these issues. The basic 12 requirements of the PCI guidelines have remained consistent.

PCI Compliance and Cisco IOS Security for the Branch

Cisco IOS® security technology offers businesses the necessary tools to help avert a credit card data breach by applying security throughout the foundation of the network. Cisco IOS security is built into the router and switch infrastructure, providing unprecedented value to branch offices, where resources may be limited. Table 1 describes in detail how Cisco IOS security helps to meet PCI requirements.

Table 1. How Cisco IOS Security Maps to PCI DSS Requirements

PCI Requirement	Cisco Technology
Install and maintain a firewall configuration to protect data.	Cisco IOS Firewall
Do not use vendor-supplied defaults for system passwords and other security parameters.	Cisco IOS Software

PCI Requirement	Cisco Technology
Protect stored cardholder data.	—
Encrypt transmission of cardholder data and sensitive information across public networks.	Cisco® VPN Advanced Integration Module (AIM) for Cisco Integrated Services Routers (ISRs)
Use and regularly update antivirus software.	—
Develop and maintain secure systems and applications.	Cisco Product Security Incident Response Team (PSIRT) site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ISRs
Restrict access to data by business need.	AAA with Cisco Secure Access Control Server (ACS)
Assign a unique ID to each person with computer access.	Cisco Secure ACS
Restrict physical access to cardholder data.	—
Track and monitor all access to network resources and cardholder data.	Cisco IOS Software and Cisco NetFlow
Regularly test security systems and processes.	Cisco IOS Intrusion Prevention System (IPS), IPS AIM
Maintain a policy that addresses information security for employees and contractors.	—

With integrated firewall, VPN, and intrusion prevention and detection (IPS/IDS) capabilities, Cisco ISRs can securely scale to meet a business's PCI compliance requirements. The ISR's primary function is segmentation of PCI scope and then enforcement of that new scope boundary, and has five primary functions in relation to PCI.

- As a router, directing traffic between networks to segment a network into subnetworks and isolate sensitive information from non-sensitive information, thereby reducing the overall scope of the cardholder data environment.
- As a router with access control lists (ACLs), restricting traffic between the cardholder data environment and other areas of the network.
- As a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network.
- As an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment.
- As a VPN system, encrypting all traffic going to and from the store across open and public networks.

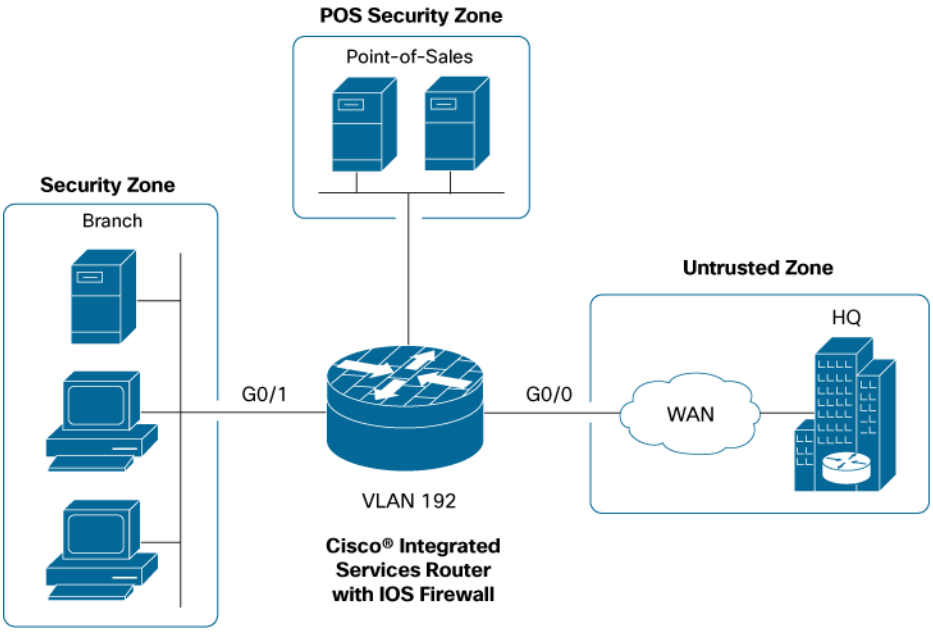
Cisco IOS Zone-Based Policy Firewall

The Cisco IOS Zone-Based Policy Firewall feature runs on Cisco ISRs, securing Internet connectivity and protecting mission-critical resources behind the router. This feature uses security zones to segment the network and protect cardholder data; zones are based on strict user or group policies that provide:

- Granular stateful inspection that tightly controls network service access and enforcement between and outside security zones.
- Classification of users, devices, or protocols into groups and then applying those groups to ACLs to create access control policies for those groups.
- VRF-aware firewall functions that provide virtual firewalls for isolated route space and overlapping addresses.

IT administrators can create a set of fixed policies for the network and make sure that all devices and applications in a security zone adhere to PCI DSS rules (Figure 1).

Figure 1. Cisco IOS Zone-Based Policy Firewall Security Zones



Cisco IOS Zone-Based Policy Firewall also performs stateful inspection, provides alerts, and monitors events using syslog. Cisco IOS Zone-Based Policy Firewall further enforces protocol conformance by inspecting and discarding protocols such as HTTP, Simple Mail Transfer Protocol (SMTP), peer-to-peer protocols, Session Initiation Protocol (SIP), and Skinny Client Control Protocol (SCCP), eliminating unwanted traffic and conserving bandwidth. It can automatically take the necessary steps to mitigate malicious activity coming from unauthorized access from inside or outside the network.

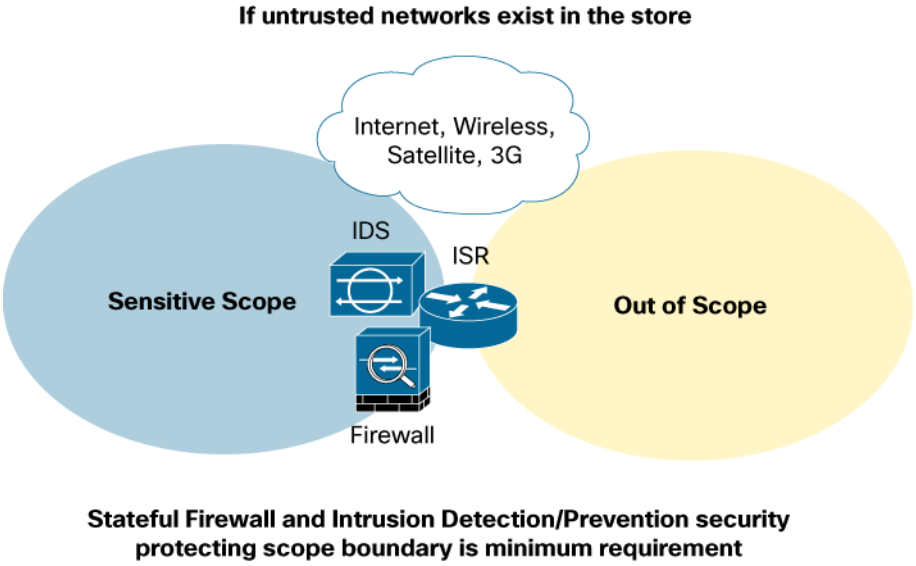
Cisco IOS IPS

Cisco IOS IPS is an inline, deep-packet-inspection-based solution that satisfies PCI DSS requirements through the deployment of endpoint security technologies and controls. This enables Cisco IOS Software to effectively analyze network traffic for malicious code and mitigate attacks. Using Cisco IOS IPS with Cisco IOS Firewall can provide an integrated solution that optimizes management and administration efficiencies. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, it is also critical to distribute a network-level defense to stop malicious traffic close to its entry point at branch or telecommuter offices.

Cisco IOS IPS:

- Works with Cisco IOS Firewall, control-plane policing, and other Cisco IOS security features to protect the router and networks behind the router.
- Provides networkwide, distributed protection from numerous attacks, worms, and viruses that exploit vulnerabilities in operating systems and applications.
- Eliminates the need for a standalone IPS device in branch and telecommuter offices and in small and medium-sized business networks.

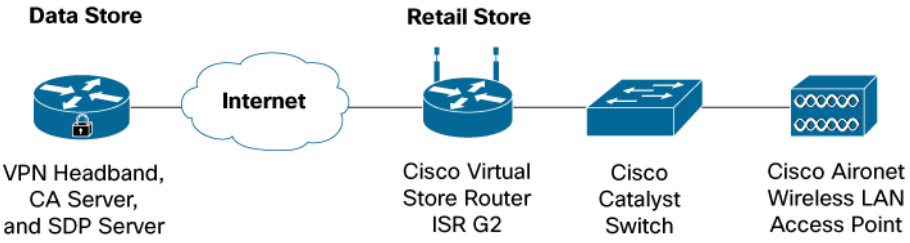
Figure 2. Segmented Store Topology



Cisco IOS VPN

According to PCI, public WAN link connections are considered untrusted public networks. A VPN is required to securely tunnel traffic between the store and the enterprise network. A Cisco ISR can be used to encrypt the transmission of cardholder data across open, public networks such as 3G/4G/Wi-Fi, and satellite technologies using SSL and IPSec technologies. The following example describes equipment located at the store and the data center headend router. Figure 3 shows a simplified Cisco IOS VPN topology.

Figure 3. Cisco VPN Topology



Cisco IOS VPN technology connects the stores to the data center over the Internet, using a secure, encrypted tunnel to secure sensitive information. Cisco VPN technologies that can protect the data in transit and provide a secure access to the stores' networks include EasyVPN and Dynamic Multipoint VPN (DMVPN).

Cisco Security Manager

Cisco Security Manager is a powerful yet easy-to-use solution for configuring firewall, VPN, and IPS policies on Cisco security appliances, firewalls, routers, and switch modules. Cisco Security Manager helps enable enterprises to manage and scale security operations efficiently and accurately. Its end-to-end tools provide consistent policy enforcement, quick troubleshooting of security events, and summarized reports from across the security deployment.

Cisco Security Manager supports integrated provisioning of firewall, IPS, and VPN (most site-to-site, remote access, and SSL) services across Cisco IOS Software-based routers such as Cisco Integrated Services Routers and Aggregation Services Routers.

Cisco Secure Access Control Server

A centralized user database (Active Directory) and Cisco Secure Access Control Server (ACS) TACACS services can be used to restrict access to cardholder data and assign a unique ID to each person with computer access. Individual user IDs are assigned, and roles are defined and based on group membership. Cisco routers are configured to use an AAA model for user-based access. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function. By default, no users are allowed access unless specifically configured and assigned appropriate passwords.

Staying Compliant

Cisco IOS security technologies help:

- **Separate, divide, and isolate network traffic.** The firewall is the center point inside the network and is critical for PCI compliance. A common firewall policy such as Cisco IOS Zone-Based Policy Firewall examines the source and destination zones from the ingress and egress interfaces. It is not necessary that all traffic flowing to or from an interface be inspected. Individual flows in a zone pair can be designated to be inspected using policy maps that may be applied across the zone pair. The policy map will contain class maps that specify the individual flows.
- **Demonstrate compliance in the event of an attack or audit.** An audit can be stressful for any IT administrator, and can be even more so when there is a possible security breach at the time of the audit. Cisco can provide tools that map to PCI requirements and that demonstrate and validate compliance. Combining best practices and extensive networking technology expertise, Cisco has developed a set of architectures in a lab environment with PCI requirements in mind. If properly deployed and maintained, these architectures can help achieve PCI compliance.
- **Performance where it counts.** Cisco integrated services routers are designed for fast, scalable delivery of business-critical applications. Cisco IOS Firewall provides protection and performance that is suited for small to medium-sized branch office deployments, particularly in commercial environments. This integrated solution is ideal for organizations seeking a cost-effective PCI compliance solution.

Conclusion

Any organization that accepts, processes, or stores credit card information must comply with PCI standards. Cisco IOS security technologies can help ensure compliance:

- Cisco IOS Zone-Based Policy Firewall can define network security zones, prevent action on cardholder data being leaked outside of security zones, and apply policies to inspect and mitigate malware threats and unauthorized data access and transfers.
- Cisco IOS IPS effectively analyzes network traffic for malicious code and mitigates attacks.
- Cisco VPN encrypts sensitive cardholder data across the WAN.

For More Information

For more information about how Cisco can help you meet your PCI compliance needs, visit the following resources:

http://www.cisco.com/go/routersecurity
http://www.cisco.com/go/iosfw
http://www.cisco.com/go/iosips
http://www.cisco.com/go/csmanager
http://www.cisco.com/go/pci
http://www.cisco.com/go/pci2

For more information about the PCI Security Standards Council, visit https://www.pcisecuritystandards.org.

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 C11-682532-00 08/11