



Payment Card Industry Compliance on Cisco Catalyst Series Switches

Why Should I Care About Payment Card Industry (PCI) Compliance?

Credit card theft reached an all-time high in 2007. The Payment Card Industry Data Security Standard (PCI DSS), introduced in 2005, applies to all businesses, public and private, in many industries that process, transmit, or store credit card transactions. The goal of PCI is to increase protection of customer credit card information.

PCI Deadlines and Effects

PCI compliance deadlines in 2007 and 2008 have been set, dependent on geography and the size of a merchant. If a company does not achieve PCI compliance by these dates, acquiring banks will issue monthly fines until the company does become compliant. The fines can range from US\$5000 to \$25,000 and can increase further over time. The card brands (Visa, MasterCard, American Express, JCB, and Discover) may also raise the service transaction fees for noncompliant companies.

The PCI standard provides 12 security requirements to which companies must adhere:

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update antivirus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

PCI Compliance on Cisco Catalyst Series Switches

An end-to-end Cisco® network can be a vital component in your overall PCI compliance strategy. Cisco Catalyst® Series switches can play an important role in the PCI process.

Figure 1. Cisco Catalyst 3750, 4500, 6500 and 2900 Series Switches



Cisco Catalyst Series switches contain many integrated tools that facilitate the construction of a self-defending network. These tools both apply to network-level interactions in a PCI-compliant network and protect the device itself.

At a network level, VLAN segmentation on Cisco Catalyst switches is the most robust way to reduce the PCI scope of a customer business. Segmenting point-of-sale (POS) data into its own VLAN reduces the PCI audit scope from the entire network to just those POS VLANs and saves companies thousands of dollars during the audit process. Common user traffic can be separated from payment card traffic at either Layer 2 using VLANs or Layer 3 using Virtual Routing and Forwarding instances, which addresses PCI Requirement 1.

In addition, all Cisco Catalyst Series switches support per-port 802.1x authentication, restricting users' access to the network until they have been properly identified, a major requirement of PCI DSS Requirements 7 and 8.

Tracking users and usage is also a primary component in the PCI DSS specification. The use of integrated, hardware-enabled Cisco NetFlow can play an important role in auditing network usage. NetFlow instances feed up to a Security Incident and Event Manager (SIEM) device, such as the Cisco Security Monitoring, Analysis, and Response System, to track all events on the network. NetFlow provides intelligence across the entire network, which no other technology can do as well. NetFlow helps to meet PCI Requirement 10.

At the device level, Cisco Catalyst Series switches support a common set of infrastructure protection capabilities, known collectively as the Cisco Catalyst integrated security features. These capabilities protect the switches from common intrusion or denial-of-service attacks.

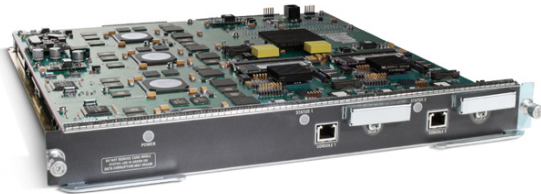
Access to the switches can be encrypted using industry-standard Secure Shell Protocol. Access can also be restricted and logged using built-in authentication techniques. All of the switches also support timed session terminations, to avoid situations where an administrator terminal session might be hijacked by an unauthorized user. These features meet specific requirements throughout PCI, such as Requirements 2 and 8.

Finally, PCI DSS recommends keeping all software up to date in order to prevent avoidable security holes. Cisco SMARTnet® Service provides you with access to the latest switch software on demand. In addition, the Cisco Product Security Incident Response Team (PSIRT) works with industrywide security researchers and other bodies to keep you well informed about any security-affecting software anomalies, helping to address PCI Requirement 6.

Integrated Services on the Cisco Catalyst 6500 Series Switch

The flagship of the Cisco Catalyst Series switches, the Cisco Catalyst 6500 Series Switch, is especially well suited for PCI-compliant networks. Its modular design allows for the insertion of multiple service modules, each of which can help in complying to PCI DSS.

Figure 2. Cisco Catalyst 6500 Series Wireless Services Module



- **Firewall Services Module:** Provides integrated virtual firewall services to restrict access to customer data storage repositories (PCI Requirement 1).
- **Intrusion Detection System Services Module:** Enables organizations to minimize risk and maximize business continuity by rapidly identifying unauthorized access (PCI Requirement 11).
- **Wireless Services Module:** PCI DSS identifies wireless networks as a particular vulnerability that a PCI compliant network must address. The Cisco Catalyst 6500 Series Wireless Services Module offers centralized security policies, wireless intrusion prevention system (IPS) capabilities, and Layer 3 fast secure roaming for WLANs (PCI Requirements 2, 4, and 11).

- **Programmable Intelligent Services Accelerator (PISA):** Enables industry-leading integrated security through authentication and threat defense features to help ensure network availability and the integrity of communications for credit card transactions (PCI Requirement 10).
- **Cisco IPSec VPN Shared Port Adapter:** Provides infrastructure-integrated IPSec VPN services to meet the need for hardware-accelerated encryption of secure transactions (PCI Requirement 4).

What Are the Benefits of PCI Compliance?

Although achieving PCI compliance will require some investment of time and resources for most businesses, it has both direct and indirect benefits:

- Meeting deadlines prevents fines, penalties, and transaction fee increases.
- Avoids negative publicity and legal liability because data breaches are prevented.
- Helps ensure uninterrupted ability to provide credit card payment services.
- Increases customer protection, which increases their confidence and loyalty.
- Strengthens security on the overall network for other sensitive data assets.

Cisco and PCI Compliance

Cisco has been one of the leaders in the networking industry in providing customers with deployment guidance for achieving PCI compliance.

- The Cisco PCI Validated Architectures, which passed a PCI technology audit, provide design and implementation guidance, architectural views of how to build a PCI DSS network, device-specific configurations for each component in the network, and the PCI Report of Compliance by the qualified security assessor (QSA).
- Cisco Catalyst Series switches provide scalable platform choices, so that the network can be “right-sized” to your particular performance requirements and budget.
- Cisco offers a choice of deployment models, which are adaptable to your internal operational requirements. PCI networks can be constructed with an integrated services model, where the majority of capabilities are integrated into the network switch itself. Alternately, Cisco offers network appliances for each service function, so that they can be managed separately.
- Cisco PCI Advanced Services help customers get compliant and stay compliant. Cisco PCI Advanced Services perform readiness assessments and remediation services for customers before a PCI audit is performed and monitoring services to help the customer stay PCI compliant continually.

Additional Resources

Cisco PCI Validated Architecture:
<http://www.cisco.com/web/strategy/retail/pci.html>

Cisco compliance information:
<http://www.cisco.com/go/compliance>

Cisco PCI Compliance Advisor:
<http://www.pcicomplianceadvisor.com/>