BEYOND PCI COMPLIANCE

Cisco and SAP PCI Compliance Solution for Retail

Executive Summary

Threats to data security are increasing daily; criminals are becoming more sophisticated, new regulations are introduced. How can retailers stay ahead of the dangers? The only possibility is through a combination of advanced infrastructure, progressive software, and pervasive policies. Retailers need partners that are committed to staying ahead of the threats.

Cisco and SAP have formed a unique partnership to provide the most comprehensive data security support available to the retail industry. Through this partnership, we are working together to produce integrated, validated, and audited solutions using our combined products and services. We are helping retailers achieve compliance through best practices, compliance report examples, implementation details, and compensating controls. Independent qualified security assessor (QSA) companies have been engaged to audit our combined products and labs.

This document outlines key principles and best practices that retailers should adhere to, and presents a set of recommendations on ways to combine network-level and application-level security in a coherent, trustworthy fashion.

Payment Card Industry Data Security Standards (PCI DSS)—What It Means to Retailers

Data security requirements are now a permanent feature of retailers' compliance obligations. The Payment Card Industry Data Security Standard (PCI DSS) is designed to protect the privacy of customers, as well as payment card and merchant data. However, meeting PCI requirements has proved to be a challenge for many retailers. To help address this, Cisco and SAP have joined forces creating a set of audited architectures that support a secure environment for credit card data, cardholder information, point-of-sale (PoS) transaction logs, and database records. This collaboration helps retailers meet their PCI compliance requirements while minimizing infrastructure complexity and simplifying integration with retail applications.

Overview of PCI DSS

Retailers of various sizes are subject to increasingly complex requirements in order to continue providing secure payment processing. The bare essentials of PCI DSS cover areas of network infrastructure, authorization, systems monitoring and management, data management, application software, and business policy. The principles at the heart of PCI DSS are expressions of the current best practices used in many industries to protect information. Compliance with PCI DSS is not necessarily the end of the road, and should be considered to be the minimum standard of security that a retailer

should implement to protect customer information. Threats to data security will continue to evolve; therefore, retailers should be prepared for ongoing investments in order to provide the level of protection their customers expect.

History—Analysis of Data Theft

Clever security breaches compromise the environment at different levels. Attacks can be executed through the Internet from anywhere in the world, or by physically removing store equipment. It is possible to identify and capture network packets by attaching a laptop and using protocol analyzer (or "sniffer") software such as WireShark and/or NetStumbler. These packets can be captured on a wired (10/100/1000BaseT) or wireless (802.11a/b/g/n/FH) network. When unencrypted data is travelling on the network, these plain packets can be captured and viewed by anyone with the proper equipment. Attacks can come from outside the organization as well as within, so it is critical to maintain a multi-tiered security architecture and strong policies. Criminals continue to become better organized and employ more sophisticated techniques. The result is that security is not a one-time event, but must be considered an ongoing endeavour.

Examples of past breaches include the following:

- Physical theft of store point-of-sale terminals and in-store processors
- Keyboard and malicious software removal interceptors
- Attaching to the store network
- Attaching to the store wireless network
- Attaching to the head-office network
- Head-office databases
- Bogus calls to head-office service-oriented architecture services
- Insecure business-to-business connections
- Internet connections and Web sites
- Unauthorized employee access

Current Requirements

PCI DSS compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The program applies to all payment channels, including retail (brick and mortar), mail and telephone order, and e-commerce. PCI DSS offers a single approach to safeguarding sensitive data for all card brands.

The PCI DSS framework provides the tools and measurements needed to protect against cardholder data exposure and compromise. To pass PCI compliance standards, a retail company must address its procedures, security policies, and technical infrastructure so that it can demonstrate adherence to the PCI v1.1 specification subrequirements. A qualified security assessor must perform an audit of the company to verify that each applicable subrequirement is either addressed or deemed not applicable to that specific company. Final compliance is accomplished by having the audit submitted and accepted by each of the individual payment brands directly.

The PCI Data Security Standard consists of twelve requirements and corresponding sub-requirements categorized in Figure 1.

Table 1 PCI Data Security Standard

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	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
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Details regarding the PCI DSS requirements can be found at the following URL:

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

In the past, some retailers assumed that these responsibilities rested with the software application companies providing point-of-sale and related programs. In fact, a great deal of responsibility lies with the retailer. It is only through the proper implementation and use of applications and networking devices, along with a comprehensive set of policies, that compliance can be achieved and maintained.

Future—Payment Application Best Practices (Vendors Step Up)

In the spirit of partnership, software vendors worked with the retailers to help implement solutions where possible. With the evolution of PCI DSS, payment application vendors were strongly encouraged to tighten up their software applications, and to address known risk areas within the applications and how they are implemented.

PABP Certification

In response to retailers' requests, Visa USA and its partners developed the *Payment Application Best Practices* (PABP) certification, which applies to providers of payment systems and software. Companies including SAP and its business partners have invested substantial sums to ensure that their applications meet these requirements. A key aspect of attaining this certification is a third-party audit by a Visa-accredited organization.

Several SAP® applications, including the SAP Point-of-Sale (SAP PoS) application, have had additional security functionality incorporated in the software. SAP PoS is used in thousands of stores, and most recently, Version 9.5 was subject to this independent audit and now has attained the PABP certification.

For more information, refer to the following URL:

http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html.

Retailers that implement SAP PoS have a significantly higher probability of passing a PCI audit. However, there are other key areas they need to address that are part of their overall retail systems security architecture.

Implications of a Security Breach

In recent years, there have been widespread reports in the press and other news media of theft of credit card and other sensitive information from a variety of companies. In 2007 in the United States, there were over 443 breaches exposing over 127 million individuals[1].

In some cases, theft occurred due to lack of physical security, network security, or business policy. As the sophistication of the thieves increased, they began attacking the application software itself.

Several well-known retailers had been attacked through their wireless networks, and a quick response to lock down those networks was not sufficient. Others simply had equipment stolen from the premises.

In some cases, lack of clear business policies led to employees inadvertently opening the door to a security breach. From a liability perspective, retailers are facing significant fraud on the order of millions of dollars. Further, MasterCard Worldwide has imposed fines on merchants that have not met their requirements to keep transactions secure, and Visa is taking aim at the largest merchants in the United States with fines that start at $10,000 a month and can rise to $100,000 a month. Most importantly, retailers need to maintain the confidence of their customers. Store operators have to improve their security to reassure shoppers that their information is secure. The potential net loss to a retailer in some cases far exceeds the annual profit generated by the business. Lack of PCI DSS compliance is a serious business risk, making it an issue not only for the CIO, but the entire company including the CFO and CEO.

Retailers have been frustrated by a lack of guidance on how to protect themselves and their customer data. At the same time, payment acquirers including major credit card providers and banking networks are demanding that the retailers put protection in place. Unfortunately, until PCI DSS emerged, there was little guidance on where to begin. Yet PCI DSS and the associated PABP standard for software and solution vendors is still not enough.

It is important to recognize that no single product or process can achieve PCI compliance. A comprehensive approach that encompasses people, processes, and technology is the key to meeting the compliance. The best practices in the PCI standard are what security professionals at SAP and Cisco recommend on a daily basis.

Benefits of Becoming PCI Compliant

Cisco and SAP recommend an architectural approach to security and business continuity using a *defense in-depth* approach. This architecture applies security technology and processes throughout the network, from the application to the network core for both wired and wireless media. Neither application nor network security alone is sufficient, and both can be easily compromised if business practices and policies are not in place or enforced.

1. Identity Theft Resource Center 2007 breach list: www.idtheftcenter.org

Most industry experts agree that the best way to achieve and maintain PCI compliance is to adopt a strategic, holistic approach to network-security risk management and compliance that includes the network infrastructure, policies, and procedures. The ability to centrally manage systems, network services, and security is essential to a holistic solution. In addition to simplifying retailers' approach to PCI requirements, central management improves operational efficiency and potentially accelerate will delivery of future retail applications.

PCI compliance is just the beginning, however. Country, state or province, and local regulations may also require a company to safeguard data. An SAP and Cisco architecture can support a company's efforts to meet current and future regulatory requirements, while also enabling a retailer to securely undertake new business initiatives and improve company-wide risk management.

Service Oriented Architecture

A service-oriented architecture (SOA) is a new-generation software architecture that defines the use of loosely coupled services to support the requirements of business processes and users. Resources on a network in an SOA environment are made available as independent services that can be accessed via standard protocols and transports without the knowledge of their underlying platform implementation.

SAP is the recognized leader in enterprise SOA. Enterprise SOA is a blueprint for an adaptable, flexible, and open IT architecture for developing services-based, enterprise-scale business solutions. With the SAP NetWeaver® technology platform as the foundation, enterprise SOA moves IT architectures to higher levels of adaptability, and moves companies closer to the vision of real-time enterprises by elevating Web services to an enterprise level. For more information on enterprise SOA, visit: www.sap.com/platform/esoa/index.epx.

Cisco is the recognized leader in Enterprise Service-Oriented Network Architecture (SONA). SONA is an architectural framework that delivers business solutions to unify network-based services such as security, mobility, and location with the virtualization of IT resources. With SONA you can take advantage of a wide range of Cisco products, expertise, proven designs, and services, aligned with those of our partners, to help you build an innovative, competitive enterprise. For more information on Cisco's SONA, visit: www.cisco.com/go/sona.

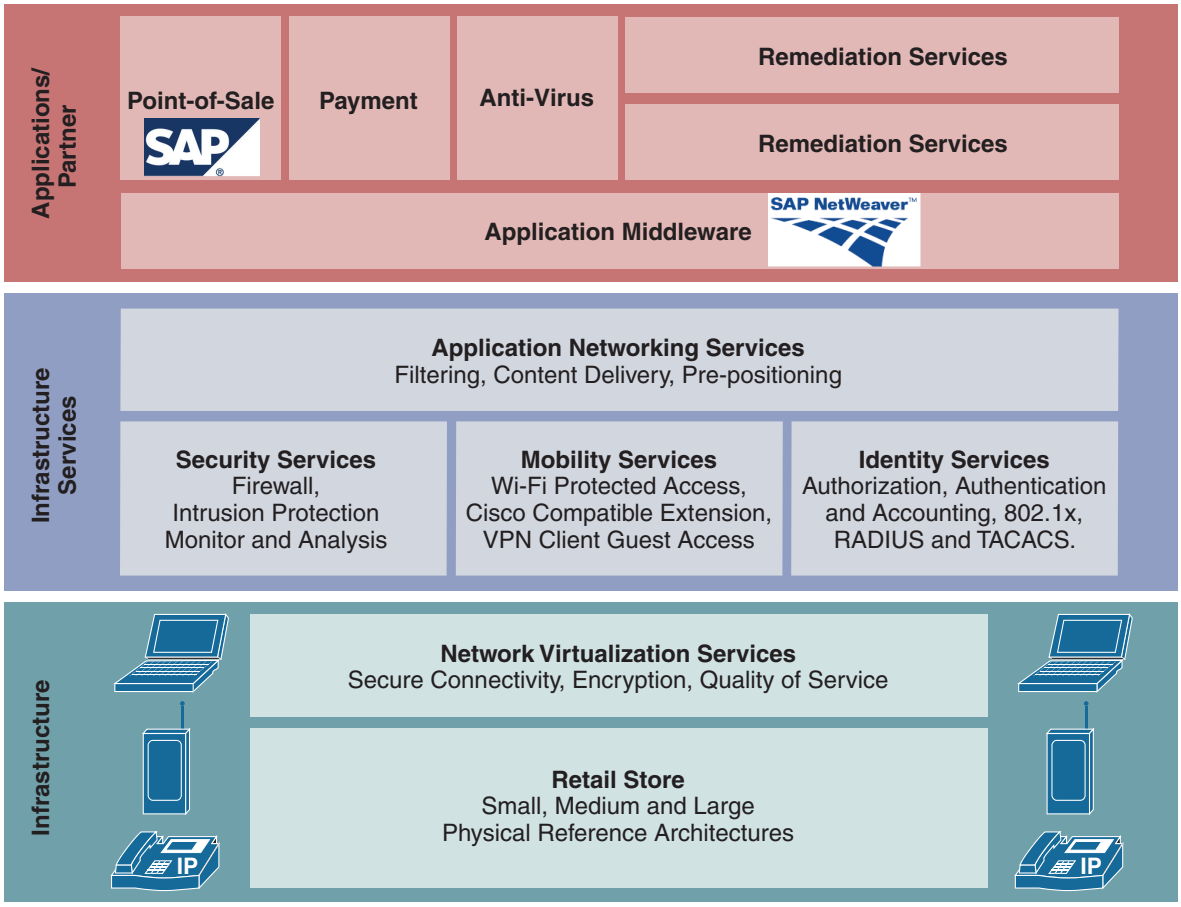
Retailers face critical challenges as they attempt to build secure retail system solutions. Over time, stores have evolved to contain multiple proprietary systems and infrastructures, such as PoS, telephony, and security. Information "islands" within applications and functions are difficult to manage and secure. Sharing information and services is almost impossible.

In response to these challenges, Cisco and SAP have designed retail systems that seamlessly and securely link in-store operation networks and applications. The Cisco Intelligent Retail Network (IRN) is the foundation for a set of common services to a broad range of applications and devices. This integrated retail system enables a single, centrally-managed secure network of:

- Consistent and efficient data integration
- Support for cross-functional and channel operations
- Improved security, availability, and manageability

The Intelligent Retail Network, Cisco's framework for PCI compliance, is a service-oriented network architecture for retailers (see Figure 1). The Intelligent Retail Network reference designs serve as the foundation of an ideal retail enterprise infrastructure.

Figure 1 Cisco Intelligent Retail Network



Cisco's Intelligent Retail Network enables retailers to streamline business operations, accelerate decision making, and improve customer satisfaction by:

- Boosting productivity by connecting people, places, and information
- Improving customer satisfaction by enhancing the shopping experience
- Increasing revenue by improving decision making through utilization and delivery of data
- Securely and reliably protecting brand image and assets

The Cisco Intelligent Retail Network architecture can be integrated with existing retail systems or infrastructure for ease of implementation. Capabilities of the IRN range from a simple retail solution at PoS to enterprise-wide, media-rich customer environments. For more information regarding Cisco's Intelligent Retail Network, refer to the following URL: www.cisco.com/web/strategy/retail/irn.html.

SAP's Audited Products

SAP engaged TrustWave Holdings Corporation to conduct an assessment and to validate compliance with Visa USA's PABP. This report is based on the assessment of SAP Point-of-Sale (PoS) application Version 9.5.

This application is designed for general merchandise and multi-format retailers. It is a highly configurable PoS application that includes an easy-to-use business-rules engine. In addition to PoS functionality, the application includes back-office functionality for store-level management and reporting.

Cisco's Audited Products

Cisco's PCI Solution for Retail is a set of configurations and recommendations for wired and wireless retail networks, designed to conform to the PCI DSS 1.1 specification. The solution was built and tested using PoS systems, wireless client devices, Cisco network infrastructure, and validated by a PCI quality qualified security assessor audit partner.

Infrastructure Services

Process control is simplified by using common infrastructure services for security, mobility and identity, and management. These are key advantages that aid in operational reporting and the policy requirements of achieving PCI compliance. Using fewer services that are shared across more intelligent devices increases the operational efficiency of the whole system.

- *Security services* are used extensively in the PCI Solution for Retail architectures. These services are a combination of in-store security services shared across multiple physical devices, central management in the data center, and virtual access to the security control plane from anywhere in the retail network.
- *Firewall services* in the Integrated Services Router (ISR) are used within each store architecture, securing both application and interface services.
- *Intrusion detection and prevention systems* (IDS/IPS) also run with the ISR router, Unified Wireless Network, and at the PoS host and server levels within the solution architecture. The combination of these systems is centrally managed through the Cisco management applications in the data center.
- *Monitoring, analysis, and remediation* data is correlated by the CiscoSecure ARS application in the data center. This application not only does correlation and monitoring, but can also remediate network attacks dynamically or through reactive alarm notifications.
- *Mobility services* are another important area in an Intelligent Retail Network. Retailers are demanding support for mobile PoS applications operating on handheld computers or mobile PoS kiosks. The Cisco Unified Wireless Network supports a very scalable set of WLAN systems ranging from single access points to systems connecting thousands of access points as a single, centrally managed domain. The retail store networks use various WLAN systems, depending on the requirements of the store category.
- *Identity services* are used to ensure that authenticated and authorized users are allowed access to retail network systems. Cisco Secure ACS provides the central management of the RADIUS and TACACS+ systems configured on each network device throughout the architecture. A central LDAP-based directory service enhances CS-ACS in helping it meet the requirements of PCI. The use of a distributed network time-service ensures consistent synchronization of network and application events, and allows better correlation of events.

Infrastructure Products

- *Cisco Integrated Services Router*—The Cisco Integrated Services Router (ISR) consolidates data, network, and security into a single platform with local and centralized management services.
- *Cisco Catalyst Ethernet Switch and Network Switch Module*—The Cisco Catalyst Ethernet Switch provides connectivity for the IP end points to the routed networks and WAN services.
- *Wireless Access Points and Controllers*—Cisco produces several product lines of wireless access points and control systems. Products in PCI compliance testing used the LWAPP architecture in lieu of autonomous access points. The LWAPP architecture is able to meet a wider variety of compliance requirements including IDS scanning and easier centralized management.
- *CiscoWorks LAN Management System*—The CiscoWorks LAN Management System (LMS) provides a network management function that addresses specific PCI 1.1 requirements.
- *Cisco Security Manager*—Cisco Security Manager is a powerful yet easy-to-use solution for configuring firewall, VPN, and intrusion prevention system (IPS) policies on Cisco security appliances, firewalls, routers, and switch modules.
- *CSA Manager*—CSA Manager manages Cisco Security Agent, which delivers application firewall, file integrity, and host intrusion prevention services.
- *Cisco Security Monitoring, Analysis and Response System (CS MARS)*—CS MARS is an appliance-based, all-inclusive solution that allows network and security administrators to monitor, identify, isolate, and counter security threats.
- *Cisco Access Control Server (ACS)*—The ACS provides secure authentication service for ISRs, switches, wireless APs, wireless controllers, LMS, and CSM.

QSA Audit Results

This solution passed the QSA audit performed by CyberTrust (now Verizon Business). The network architectures required only a few compensating controls for device management and file integrity monitoring. Products that Cybertrust found most useful included CSA Manager and the CSA clients on the various management servers and the comprehensive network architecture. The detailed implementation guide and results of the audit can be found in the *PCI Solution for Retail Design Guide* available here: www.cisco.com/web/strategy/retail/pci_imp.html.

Conclusion and Recommendations

SAP and Cisco have joined forces to address the ever-increasing threat to payment card systems used by retailers around the globe. In addition to the checklist of steps below, Table 2 highlights several SAP and Cisco products that have been audited by independent QSAs and proven to meet the PCI DSS and PABP requirements of today's enterprise systems. The following checklist will help accelerate your PCI compliance efforts:

1. Partner with a qualified security assessor
2. Upgrade your SAP software
3. Properly implement and secure your Cisco networking equipment
4. Regularly patch software vulnerabilities
5. Institute change management
6. Institute or update business policies

7. Perform proactive testing
8. Follow the 12-Step PCI DSS guidelines
9. Encourage personal ownership of enterprise security

Table 2 shows PCI requirements that can be satisfied by Cisco and SAP products when implemented as a complete solution as validated in the *Cisco PCI Solution for Retail Design Guide*.

Table 2 PCI Requirements for SAP and Cisco Products

Products and Features	PCI Value Satisfied for the Requirement
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	
Cisco Integrated Services Routers (ISR)	Network security (firewall segmentation/filtering), stateful filtering
CiscoWorks (LMS), Cisco Security Manager (CSM)	Configuration management/secure configurations
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	
ISRs, catalyst switches, wireless devices, wireless control server (WCS), access control server (ACS), CiscoWorks (LMS), Cisco Security Agent (CSA), CSM	Vendor defaults can be changed
WCS/wireless controllers	Wireless security (WPA/WPA2, SSID broadcast can be disabled)
ISRs, switches, wireless controllers, CSA Manager, CSM, CiscoWorks (LMS)	Best-practice security parameters enabled
ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS)	Non-console encrypted administrative access
SAP® Point-of-Sale (SAP POS) application	Best-practice security parameters enabled
Requirement 3: Protect Stored Data.	
SAP POS	Encryption of cardholder data
SAP POS	No storage of PIN, CVV, CVV2, and CVC2 information
Requirement 4: Encrypt transmission of cardholder data across open, public networks.	
Wireless controllers and access points	WPA wireless security
Site-to-site and multisite VPN encryption	3DES and AES encryption
Requirement 5: Use and regularly update anti-virus software or programs.	
CSA	Anti-virus protection, malware/spyware protection, alerting
Requirement 6: Develop and maintain secure systems and applications.	
SAP POS, CiscoWorks (LMS), CSM (workflow mode), Cisco Proactive Automation of Change Execution (PACE)	Change control
Requirement 7: Restrict access to cardholder data by business need-to-know.	

Table 2 PCI Requirements for SAP and Cisco Products (Continued)

ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS), SAP POS	Least-privilege, role-based access
Requirement 8: Assign a unique ID to each person with computer access.	
SAP POS, ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS)	Unique user IDs, authenticated access, encrypted passwords, no group/shared IDs/passwords
SAP POS, ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS)	Password strength requirements
SAP POS, ISRs, switches, wireless controllers (CSA Manager, CSM, CiscoWorks (LMS), CS-MARS, ACS, WCS)	Account lockout requirements
Requirement 10: Track and monitor all access to network resources and cardholder data.	
SAP POS, ISRs, switches, wireless devices, WCS, ACS, CiscoWorks (LMS), CSA	Audit trails, time synchronization
Requirement 11: Regularly test security systems and processes.	
Wireless controllers and access points	Rogue wireless AP/device detection
ISRs (sensor), CSM (policy, signature updates)	Network intrusion detection system (IDS)
CSA	Host-based IDS, file integrity

Reference Information

For further information, refer to the following:

- PCI Security Standards Council: www.pcisecuritystandards.org/
- Cisco's PCI solution for retail - Blueprint: www.cisco.com/web/strategy/retail/pci_imp.html
- Visa's cardholder information security program for payment applications, PABP: http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html
- Securing servers to pass compliance: www.CISecurity.com
- Enterprise Branch Security Design Guide: www.cisco.com/univercd/cc/td/doc/solution/e_b_sdc1.pdf
- PCI Compliance Using the Cisco Self-Defending Network: www.cisco.com/application/pdf/en/us/guest/netsol/ns625/c654/cdccont_0900aecd80421160.pdf
- The SANS Security Policy Project: www.sans.org/resources/policies/

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe