



**CISCO INTEGRATED NETWORK SECURITY:
BUILDING A SELF-DEFENDING NETWORK**

CISCO INTEGRATED NETWORK SECURITY: BUILDING A SELF-DEFENDING NETWORK

“Networks have evolved from closed systems to more open, sophisticated systems. As a result, security threats have grown exponentially, both at the network perimeter and from within. Cisco has responded with a strategy to integrate security services into the network infrastructure. This provides a flexible, cost-effective, and comprehensive approach to secure today’s extended network.”

Zeus Kerravala
Vice President, Enterprise
Computing and Networking
Application Infrastructure and
Software Platforms,
The Yankee Group

Each day, forward-thinking organizations reinvent how they conduct business by adopting Internet-based network solutions. The results—competitive advantage, new sources of revenue, and optimized business processes.

Increasingly, mission-critical business applications and services are deployed on open networks with substantial connections to the public Internet. Without appropriate security policies, processes, and products, Internet connectivity can compromise the very gains in productivity that help make today’s companies more profitable and that enable them to serve a larger and more diverse customer base.

Security enables enterprises to confidently extend the network to customers, partners, and remote/mobile employees, thus increasing revenues sources, efficiency of business processes and employee productivity.

In some industries, data privacy and the threat of litigation has become a government mandate. U.S. healthcare providers must comply with the Health Insurance Portability and Accountability Act (HIPAA), U.S. financial services providers are governed by the Gramm-Leach-Bliley Act, and U.K. companies must adhere to the Turnbull Report on Internal Control for public companies, as well as the Data Protection Act of 1995.

As sensitive information transverses public and private network infrastructures, security controls and policies for risk mitigation (and that display due diligence) are necessary to ensure that this information is protected according to higher-level privacy policies and regulatory requirements.

THE CISCO VISION

Cisco Systems® is a trusted partner that empowers its customers to safely deploy critical business applications and processes on intelligent information networks to help them increase productivity and gain competitive advantage. These networks are integrated, resilient, and adaptable. The confidence that comes from knowing that company business processes and information assets are secure is a critical factor in unlocking tremendous gains in productivity and dynamic growth.

Other security vendors can provide point products to achieve a base level of security for IP networks. Cisco®, however, delivers advanced, integrated network security systems and services required for mission-critical corporate networks.

Cisco continues to add security intelligence to the network infrastructure, understanding that security is not just an afterthought—it is fundamental to business processes, and ultimately to business success.

BUILDING THE SELF-DEFENDING NETWORK

The Cisco Self-Defending Network strategy describes the Cisco vision for security systems. As the nature of threats to organizations continues to evolve, so must the defense posture of the organizations. In the past, threats from both internal and external sources were relatively slow-moving and easy to defend against. In today's environment, where Internet worms spread across the world in a matter of minutes, security systems—and the network itself—must react instantaneously.

The foundation for a self-defending network is integrated security—security that is native to all aspects of an organization. Every device in the network—from desktops through the LAN and across the WAN—plays a part in securing the networked environment through a globally distributed defense. Such systems help to ensure the privacy of information transmitted and to protect against internal and external threats, while providing corporate administrators with control over access to corporate resources. The Cisco approach to security has evolved from a point product approach to this integrated security approach. The continued evolution of our vision involves the incorporation of capabilities from other security vendors. In the Cisco Network Access Control initiative, for example, Cisco is working with antivirus vendors to help ensure that infected devices are not allowed entry into the network. These self-defending networks will identify threats, react appropriately to the severity level, isolate infected servers and desktops, and reconfigure the network resources in response to an attack.

The Cisco vision of the Self-Defending Network brings together Secure Connectivity, Threat Defense and Trust and Identity Management System with the capability of infection containment and rogue device isolation in a single solution.

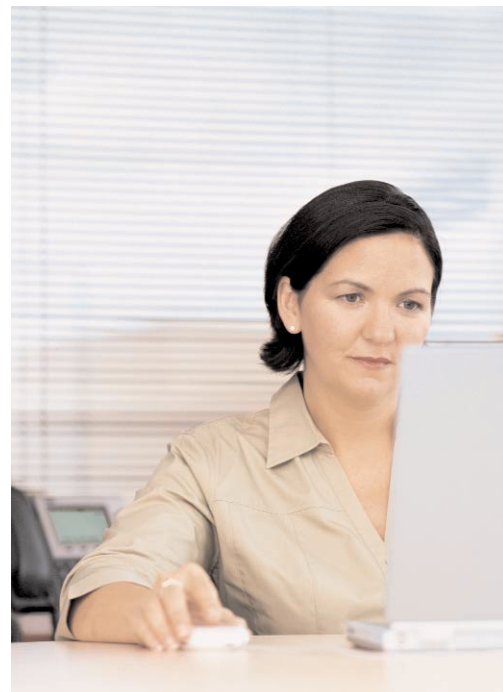
CRITICAL ELEMENTS OF NETWORK SECURITY

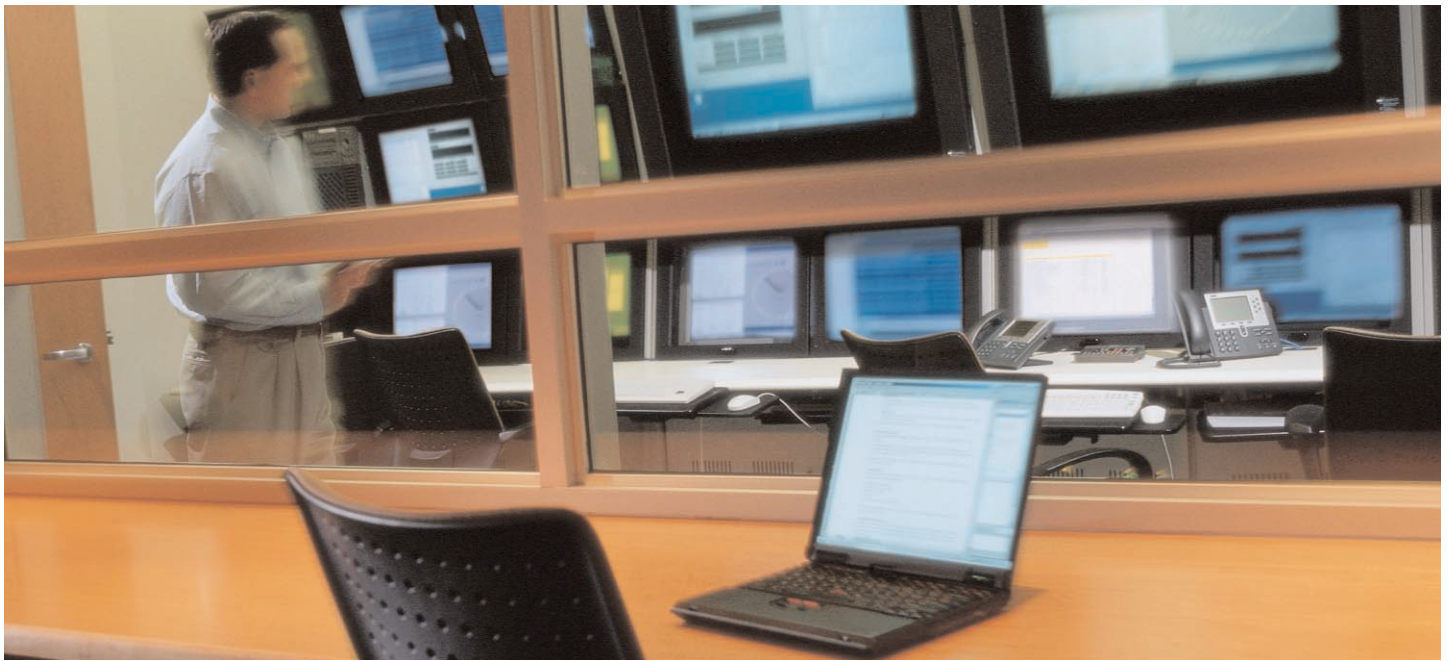
Cisco Integrated Network Security solutions incorporate three elements that Cisco believes are critical to effective network security.

Threat Defense System

Threats today—both known and unknown—continue to become more destructive and frequent than in the past. Internal and external threats, such as worms, denial of service (DoS) attacks, man-in-the-middle attacks, and Trojan horses, have the ability to significantly affect business profitability. The Cisco Threat Defense System provides a strong defense against these known and unknown attacks.

Appropriate security technologies along with advanced networking intelligence are required to effectively defend against attacks. To be most effective, these technologies must be implemented throughout the network, rather than just in point products or technologies because the source of an attack can start anywhere and instantly spread across all network resources. The Cisco Threat Defense System enhances security in the existing network infrastructure, adds comprehensive security on the endpoints (both server and desktops), and adds dedicated security technologies to networking devices and appliances, proactively defending the business, applications, users, and the network. The Threat Defense System protects businesses from operation disruption, lost revenue, and loss of reputation.





The Cisco Threat Defense System comprises several critical technologies and products enabling security integrated in routers, switches, and appliances: firewalls, network-based intrusion protection sensors, detection instrumentation, and traffic isolation techniques. Endpoint protection is enabled through the Cisco Security Agent.

Secure Connectivity System

With increased network connectivity comes increased exposure. As organizations adopt the use of the Internet for Intranet, Extranet and teleworker connectivity, such as broadband “always-on” connections, maintaining security, data integrity and privacy across these connections is paramount.

LAN connections, traditionally considered trusted networks now also now require higher levels of security. In fact, internal threats are ten times more financially damaging than external threats. Preserving the confidentiality and integrity of the data and applications that traverse the wired or wireless LAN needs to be an important part of business decisions.

The Cisco Secure Connectivity System uses encryption and authentication capabilities to provide secure transport across untrusted networks. To protect data, voice, and video applications over wired and wireless media, Cisco offers IP Security (IPSec), Secure Sockets Layer (SSL), Secure Shell (SSH) and Multiprotocol Label Switching (MPLS)-based VPN technologies

in addition to extensive security capabilities incorporated into Cisco wireless and IP Telephony solutions ensuring the privacy of all IP communications

Cisco solutions offer flexible, reliable connectivity through the integration of dynamic routing, multiprotocol support, and the widest array of connectivity options in the industry.

Trust and Identity Management System

A Trust and Identity Management System is critical for e-business and underpins the creation of any secure network or system. It entails providing or denying access to business applications and networked resources based on a user’s specific privileges and rights.

The Cisco Trust and Identity Management System focuses on network-based admission control. After validating the identity of a user or device, and its compliance with corporate security policy, access to certain resources or portions of the network can be enabled. The network is responsible for identification, authorization, and enforcement. Cisco’s Trust and Identity solution, which includes the Cisco Secure Access Control Server (ACS), authentication protocols such as 802.1X, and AAA (Authentication, Authorization and Accounting) capabilities in Cisco switches and routers, has the flexibility to provide a high level of detail in access rights and to create quarantine zones for noncompliant endpoints, and the ability to block unauthorized access entirely.

Figure 1 Cisco PIX Security Appliance



CISCO INTEGRATED SECURITY SOLUTIONS— A FAMILY OF NETWORK SECURITY OFFERINGS

Cisco award-winning security products, delivery, support, and consulting services provide the security solutions that businesses require.

Integrated Firewall, VPN, and Intrusion Protection—

Cisco PIX 500 Series Security Appliance

The Cisco PIX[®] 500 Series Security Appliance (Figure 1) is the world's leading firewall, providing unmatched reliability, scalability, and capability. Offered as a series of specialized appliances and as an integrated module for Cisco Catalyst[®] switches, Cisco PIX security appliances offer an innovative hybrid security architecture—including stateful inspection and integrated IPSec VPN capabilities. Cisco PIX security appliances deliver the highest levels of security and performance, supporting more simultaneous connections than any other firewall, with an unsurpassed speed.

Cisco Security Routers and Cisco Catalyst Switches

Cisco has directly integrated security into the network infrastructure through enhanced security features in Cisco routers and Cisco Catalyst switches, providing unparalleled flexibility and cost savings for security deployments. By taking advantage of these network devices, organizations can enable sophisticated, end-to-end security policy enforcement using their investments in Cisco infrastructure. Running across Cisco routers and Cisco Catalyst switches, Cisco IOS[®] Software includes standards-based, full-featured MPLS and IPSec VPN support for remote access and branch office connectivity. Routers and Cisco Catalyst switches also include a robust stateful firewall and intrusion detection system (IDS), with the ability to scale performance through plug-in acceleration modules. And finally, Cisco routers and Cisco Catalyst switches are the primary access control mechanisms to allow or disallow endpoint connectivity to networked resources.

Cisco IDS

The Cisco IDS provides real-time intrusion protection for the network perimeter, extranets, and the increasingly vulnerable internal network. The system uses sensors, which are high-speed network appliances, to analyze individual packets and detect suspicious activity. If the data stream in a network exhibits unauthorized activity or a network attack, the sensors can detect the misuse in real time, forward alarms to an administrator, and remove the offender from the network.

Endpoint Security Solutions—

Cisco Security Agent

The Cisco Security Agent is endpoint protection software that resides on personal computers and servers. CSA goes beyond conventional solutions by identifying and preventing malicious behavior before it can occur, removing potential known and unknown (“Day Zero”) security risks such as Internet worms.

Figure 2 Cisco VPN 3000 Series Concentrators



Cisco Remote Access VPN Solutions—

Cisco VPN 3000 Series Concentrator

Cisco VPN 3000 Series Concentrators (Figure 2) are remote access VPN platforms that combine high availability, high performance, and scalability with the most advanced encryption and authentication techniques available. Use of the latest VPN technology vastly reduces communications costs. Cisco VPN 3000 Series Concentrators are the only scalable platforms to offer field-swappable and customer-upgradeable components. These components, called Scalable Encryption Processing (SEP) modules, enable users to easily add capacity and throughput. The flexibility of the Cisco VPN 3000 Series allows both IPSec and SSL VPN tunnel termination for enhanced flexibility and reduced cost of ownership.

Cisco VPN Client Solutions—

Cisco VPN Client

The Cisco VPN Client enables secure connectivity for remote access VPNs, including support for e-commerce, mobile user, and telecommuting applications. Compatible with Windows, Linux, Solaris, and Macintosh operating systems, the Cisco VPN Client provides a complete implementation of IPSec standards, including Data Encryption Standard (DES) and Triple DES (3DES), AES encryption, and authentication through digital certificates, one-time password tokens, and pre-shared keys, RADIUS, NT Domain, Active Directory/Kerberos and LDAP authorization. The Cisco VPN Client is supported across most Cisco head-end platforms, including Cisco VPN 3000 Concentrators, Cisco PIX firewalls, and all VPN enabled-Cisco routers.

Cisco Content Management Solutions—

Cisco SSL Acceleration

Cisco offers the industry's most complete and high-performance solutions for supporting SSL-based intranets, extranets, and Internet applications. Cisco solutions optimize SSL transactions to free server capacity, scale site performance, increase reliability of secure transactions, and simplify user certificate management, reducing both capital and operational expenditures.

Content Access Management and Content Filtering

Cisco delivers solutions for managing content access at the network edge, giving corporations and schools options for blocking objectionable Web content and filtering URLs. The benefits—better management of Web access and reduced liability exposure.

Cisco Trust and Identity Management Solutions—

Cisco Secure Access Control Server

Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS or TACACS+ server system. It controls AAA for users who access corporate resources through a network. Using Cisco Secure ACS, network managers can control user access to the network, authorize different types of network services for users or groups of users, and keep an accounting record of all user actions in the network. In addition, network managers can use the same AAA framework to manage (via TACACS+) the administrative roles and groups and control how they change, access, and configure the network internally.

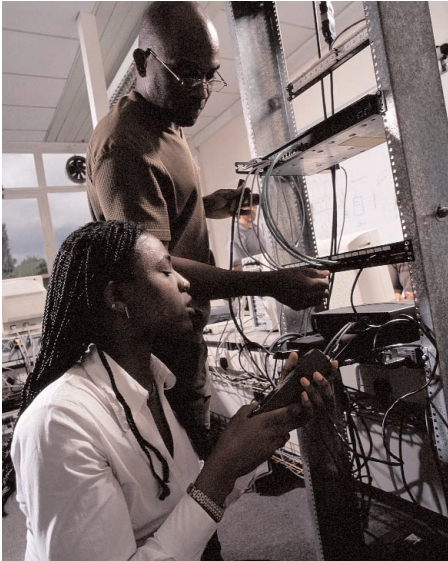
As the policy creation engine for the Cisco Network Admission Control solution, Cisco Secure ACS provides the intelligence and control that underpins an organization's security policy.

Cisco Security Management Solutions—

Integrated Management via Cisco Works VPN/Security Management Solution (VMS)

CiscoWorks VMS provides an innovative approach to enterprise-wide infrastructure management. This enhanced solution delivers greater network security through automation that streamlines and improves the management of remote firewalls. It allows for faster deployments and upgrades through a simple, easy to use Web interface. It leads to higher productivity and lower total cost of ownership (TCO) through intelligence that allows business process and policies to be followed and adhered to, preventing unnecessary business disruptions. CiscoWorks VMS now scales from the basic entry version that supports up to 5 devices, to a high-end version for support of more than 1000 Cisco IOS security routers. CiscoWorks VMS also provides higher productivity and great return on investment through its integration with other CiscoWorks tools, which manage your network infrastructure.





CISCO OFFERS THE FOLLOWING NETWORK SECURITY SERVICES:

- Cisco Security Agent Implementation Services
- IP Telephony Security Review
- Network Security Design Development
- Network Security Design Review
- Network Security Implementation Engineering
- Network Security Implementation Plan Review
- Network Security Optimization
- Security Posture Assessment

Single and Multiple Device Management

Each platform offers its own intelligent GUI for single device management. Productivity and TCO improve through simple to use, Web-based GUIs. CiscoWorks VMS can also be used for multi device management.

CiscoWorks Security Information Management Solutions (SIMS)

Designed for large networks, CiscoWorks SIMS collects and analyzes security events from Intrusion Detection Systems, firewalls, operating systems, applications and anti-virus devices. This security information is correlated statistically, evaluated according to defined security rules, and presented in real time by priority to administrators in a format that can be acted upon. CiscoWorks SIMS includes multi-vendor capabilities for Cisco integrated net-work security solutions. Its award-winning features are based on netForensic's technologies and help organizations to protect their productivity gains and reduce operating costs.

CISCO SERVICE AND SUPPORT

The Cisco model for service and support is based on the understanding that taking advantage of the power of the Internet not only speeds the resolution of networking issues, but also enables customers to access critical information quickly, to educate themselves, and to work proactively to improve overall network performance.

Cisco.com is the foundation of a suite of interactive networked applications that provide immediate, open access to Cisco information, resources, and systems. Through Cisco.com, direct customers and partners have access to numerous applications, including the Cisco Internet Technical Support (ITS) applications, which deliver comprehensive technical support solutions online. To help achieve maximum network uptime, technical assistance is available around the clock from Cisco Technical Assistance Center (TAC) networking engineers. For more information, visit:

<http://www.cisco.com/tac>

Cisco Advanced Services for Network Security

Cisco Advanced Services consultants hold expert-level CCIE® and CISSP certifications and have experience in planning, designing, implementing, and optimizing large network security infrastructures for leading business enterprises and government organizations.

Plan and Assess. Cisco can provide you with a comprehensive evaluation of your organization's network security posture. Delivered by security experts with extensive field experience, the Cisco Security Posture Assessment provides a snapshot of the security state of your network by conducting a thorough evaluation of your network devices, servers, desktops, and databases. Cisco experts analyze your network security in reference to industry best practices, identifying vulnerabilities that could threaten your business. Based on in-depth analysis, Cisco offers recommendations on how to improve your overall network security and prioritizes actions for remediation.

Design. Cisco can work with you to design a strong self-defending network. Using an in-depth, architectural approach, Cisco experts can help you develop a multilayer defense against directed attacks from hackers, viruses, and worms. Cisco can recommend improvements to your existing security design, including network topology, device placement, and connectivity. Taking into consideration all the aspects of network security such as scalability, performance, and manageability, Cisco can recommend protocol, policy, and feature configurations to better secure against threats.

Implement. A self-defending network must be not only strategically designed, but also carefully deployed, configured, and integrated into the network infrastructure. After your security solution design is set, Cisco engineers can support your team through implementation tasks to help you integrate a new solution into your production environment. Strengthening your team's ability to meet aggressive schedules while minimizing costly disruptions to your infrastructure, Cisco engineers can deliver the expertise needed to deploy, integrate, and manage the security solution.

Optimize. After your security solutions have been successfully designed and deployed, your network infrastructure will be ready to support increased demands that may arise from changing business dynamics or growing network requirements. As network conditions change, Cisco engineers work with you to perform optimization checks to help ensure that your network security infrastructure continues to meet performance objectives.

Cisco Outsourcing Services

Cisco Managed Security Services Solutions

To enable service providers to take advantage of growing demand for secure managed services and VPN services, Cisco has many service offerings for fast and cost-efficient service introduction. Managed VPN services based on IPSec, MPLS, or both permit service providers to augment existing connectivity services with remote access and site-to-site options, and to offer value-added services for IP telephony, e-commerce, supply chain management,



and content delivery. Managed security services, such as managed firewall and managed intrusion detection, represent value-added offerings that can be bundled with other services.

Whether offering managed VPN services, managed security services, or both, you can take advantage of capabilities of the Cisco routers and Cisco Catalyst switches that you currently use for connectivity. By using your current investment, you minimize deployment costs and maximize service opportunities for new revenue streams.

The Cisco Powered Network Program

Service providers who display the Cisco Powered Network mark are telling you about their services. They have earned the right to display this mark by maintaining high levels of network quality and by building their services with Cisco equipment—the same equipment on which virtually all Internet traffic travels today. The services these providers offer are reliable and secure.

Cisco Channel Partners

The Cisco Security Specialization Program recognizes Cisco channel partners who have developed the skills required to sell, design, install, and support Cisco network security solutions for customers. As Internet business solutions are rapidly adopted, Cisco security specialization partners can meet the growing demand for critical security implementation and support services.

Cisco Training Services

Cisco Security Certifications

Cisco security certifications provide individuals and organizations with a metric to validate the skills and competencies of security professionals, using best-of-class training and exams. The CCSP™ and the three focused certifications—Cisco VPN Specialist, Cisco Firewall Specialist, and Cisco IDS Specialist—satisfy an industry demand to provide a certification career path in the IT security market. CCSP certification helps to ensure that your staff is successful implementing complete end-to-end security solutions.

Security-Focused Authorized Cisco Learning Partners

Many authorized Cisco Learning Partners worldwide focus on Cisco security training, offering courses, remote labs, self-study materials, and other resources on the latest security technologies. These include Advanced Cisco PIX Firewalls, Cisco Secure Intrusion Detection System, Cisco SAFE Design Implementation, and Managing Cisco Network Security. A Learning Locator, course information, exam dates, and a detailed list of security focused partners are available at:

<http://www.cisco.com/go/training>

Cisco Security Ecosystem

The security products, technologies, and services in the Cisco portfolio are fundamental elements of a successful network security solution. A comprehensive approach to network security must address other areas as well—creating a “security ecosystem” that takes full advantage of the benefits delivered by the Cisco product line. This ecosystem includes several important elements, such as interoperable third-party products, implementation services, customer support, and compatible service offerings.

The Cisco AVVID Security Partner Program is a testing and co-marketing program that validates the interoperability of complementary, third-party security solutions with Cisco products. The program evolves independent products into more-effective security solutions and offers trusted and tested security implementations for Cisco customers.

Summary

Cisco—Building Your Self-Defending Network

The Cisco vision for security—empowering Cisco customers to safely improve their productivity—is what drives the Cisco commitment to your network security and to your long-term success.

Today, Cisco delivers integrated security solutions that enable secure internetworking by embedding feature-rich security capabilities in the Cisco infrastructure, and providing numerous security-specific appliances, software, and consulting services.

Cisco security solutions enable your business to cost-effectively take advantage of the Internet economy with the confidence you need to explore next-generation opportunities and the explosive growth they bring.

To learn more about Cisco Integrated Security and Building a Self-Defending Network visit:

<http://www.cisco.com/go/security>

<http://www.cisco.com/selfdefend>

<http://www.cisco.com/securitynow>



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 International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 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.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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

 Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, CCIE, CCSP, Cisco IOS, and PIX are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0402R) BU/LW5701 0404