SOLUTION OVERVIEW

CISCO INTEGRATED NETWORK SECURITY IN HIGHER EDUCATION INSTITUTIONS

Build a Self-Defending Network with Cisco Integrated Security Solutions

EXECUTIVE SUMMARY

Academic environments must protect their communications infrastructures from a growing number of threats that include viruses, worms, information theft, and data sabotage. An effective network security solution must closely integrate networking and security services at the device and network levels. It should provide secure connectivity, threat defense, robust trust and identity management systems, network management and analysis, and support for wireless connectivity. Cisco Systems® offers its customers the most comprehensive integrated security portfolio for securing small, midsize, and large networks.

CHALLENGE

In today's computing environment, protection of intellectual property and data, including research data, clinical data, and business and personal information is paramount for administrators of higher education institutions. Recent studies describe some of the new threats and their resources, and the staggering costs these threats can incur:

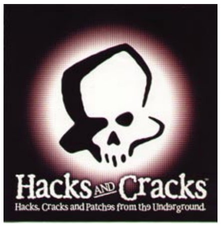
- US$202 million is lost to "cyber crime" every year by enterprises in the United States
- More than half of cyber-crime financial losses are internal
- The U.S. government will experience more than 300,000 Internet attacks this year
- More than 400,000 Webpages contain some form of network-intrusion tool
- Cyber crimes on enterprises are estimated to take place every 20 seconds

Addressing new and growing network security risks—while increasing an institution's flexibility and capacity to innovate—is a delicate balancing act. Meeting the demands of "anytime, anywhere" access, along with the open nature of the academic computing environment and the growing reliance on e-learning, distance learning, telecommuting, remote connectivity, and mobile applications, requires an institution's technology infrastructure to be robust enough to protect information integrity as well as privacy.

Cost of Poor Network Security

A higher education institution's data network has become a critical resource that supports education, research, administrative services, and campus communications. Faculty, students, and staff depend on the reliability and capability of this network and on the associated applications, data resources, services, and online communities of colleagues for much of what they do. Maximum network reliability has become mandatory.

The integrity and reliability of the network is constantly under attack from sources within and outside the network environment. Network intruders use academic resources to stage illegal peer-to-peer services, invade servers, and steal or destroy information. They can also use the institution's servers to launch attacks on remote sites or use the network to steal copyrighted intellectual property for personal use.



In March 2003, network intruders broke into the network of the University of Texas (UT). The largest university in the United States with more than 55,000 students and faculty members at its Austin campus, UT was faced with one of the most extensive security breaches at a university. A 20-year-old UT student broke into the network and stole information about students and faculty. Although there was no evidence that the student used the information for malicious purposes, such a breach is costly; it affects the credibility of the university's network and could create legal liability.

At the peak of Sobig.F attacks (August 2003), which sent large volumes of virus-infected, unsolicited e-mail, the University of North Carolina at Chapel Hill was filtering more than 100,000 infected messages from its incoming mail every hour. In 12 hours, the university filtered 1.5 million copies of the virus, said John L. Oberlin, associate vice chancellor for information technology. The Pima County Community College District in Tucson, Arizona took its entire network down one afternoon so that technicians could clean up from the Nachi worm. Approximately 2000 overtime hours were spent restoring the network. "The biggest cost," says Lawson, director of computing and information technology at the University of Vermont, "is it's just consuming the staff at a time when they ought to be doing something better." (*Chronicle of Higher Education Section: Information Technology* Volume 50, Issue 2, Page A42)

The cost of implementing incomplete, traditional security solutions is high. A report filed by the U.S. Federal Bureau of Investigation (FBI) in 2003 revealed that many organizations spend close to US$1 million a year recovering from the effects of cyber crime—far more than the cost of implementing a complete security solution. Table 1 shows the costs associated with various computer crimes in the United States in 2003.

Table 1. High Costs of Computer Crimes

Type of Cyber Crime	Cost (Millions)
Theft of proprietary information	US$70.1
Financial fraud	US$10.2
Networked data sabotage	US$5.1
Virus	US$27.4
Insider net abuse	US$65.6
System penetration by outsiders	US$2.8
Other (laptop theft, telecommunications fraud, wiretapping, insider access)	US$9.4
TOTAL	US$202.4

Integrated Network Security

The steady increase in virus incidents, denial-of-service (DoS) attacks, and similar threats facing all Internet-connected institutions has made network security a top priority for senior-level executives and IT managers. According to Michael A. McRobbie, vice president for information technology at the Indiana University System, investing in procedures, training, and equipment that can make networks more secure is well worth the expense for higher education institutions. “In a time of increased national security concerns, pressure is mounting for colleges to gain better control of their computer networks, or risk losing federal grant money for research,” McRobbie told an audience at the EDUCAUSE annual meeting.

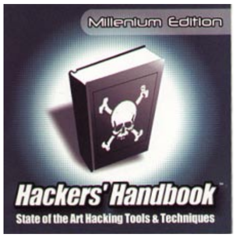
Why has it become more important than ever to implement an extensive system to combat these threats?

- The methods and tools available to network intruders are increasingly sophisticated. The security strategies and technologies required to manage these threats need to be comprehensive and multilayered to provide in-depth protection.
- Network attacks are increasingly more sophisticated but the “open sharing” of information and tools allows individuals with minimal technical knowledge to duplicate a security attack. Often, it is as easy as downloading the tool from the Internet and launching it against targets. This availability and easy access increases the number of network attackers.
- The number of attacks is increasing exponentially. The CERT Coordination Center’s tally topped 50,000 attacks by the end of 2001, more than doubling the nearly 22,000 incidents in the previous year. Each “incident” corresponds to a report filed by a company or organization struck by an intruder, worm, virus, or other Internet attack. The Blaster worm alone affected more than one million devices.

How can institutions create a robust defense against both directed attacks by malicious intruders and indiscriminate attacks from viruses and worms? In both cases, the answer is to develop a complete network security system that integrates in-depth, multilayer security into the network.

Cisco Systems tightly integrates networking and security services at the device and network levels.

- Secure devices—Cisco® integrates security features into all devices, including routers, switches, servers, security appliances, VPN devices, intrusion detection systems (IDSs), wireless LAN (WLAN) equipment, telephony equipment, client devices, and access control servers.
- Secure networks—Cisco offers embedded security throughout the network, including the data center, campus, WLAN, network edge, metropolitan-area network (MAN), branch offices, home offices, telephony systems, mobile access points, and services.

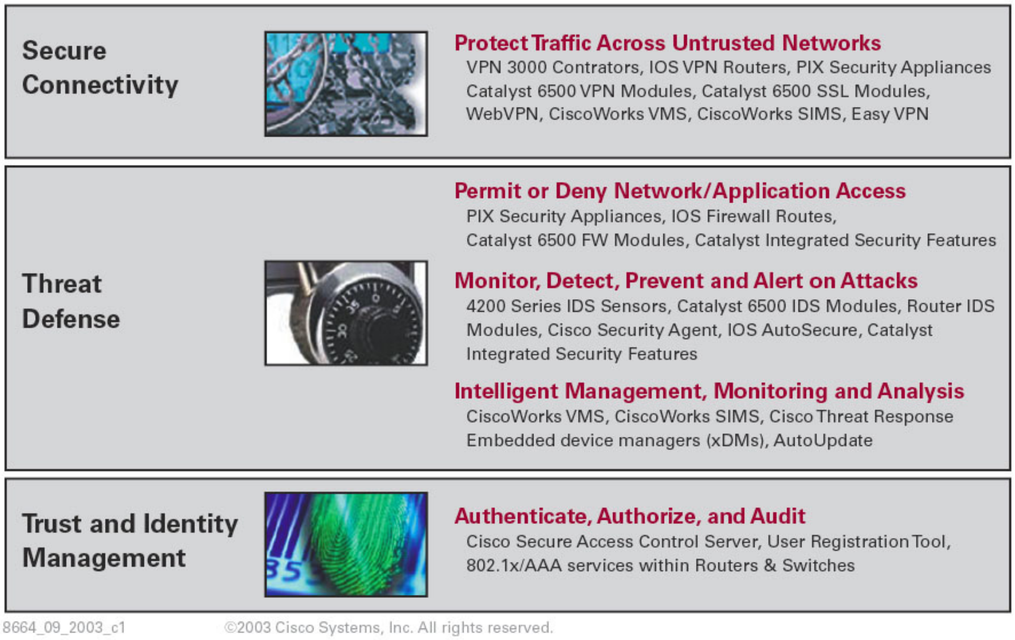


SOLUTION

Cisco offers its customers a comprehensive integrated security portfolio for securing small, midsize, and large networks.

Figure 1

Cisco Integrated Security Solutions—Comprehensive, Flexible and Collaborative Network and Endpoint Security



Secure Connectivity

Protect Traffic Across Untrusted Networks

VPN 3000 Contrators, IOS VPN Routers, PIX Security Appliances Catalyst 6500 VPN Modules, Catalyst 6500 SSL Modules, WebVPN, CiscoWorks VMS, CiscoWorks SIMS, Easy VPN

Threat Defense

Permit or Deny Network/Application Access

PIX Security Appliances, IOS Firewall Routes, Catalyst 6500 FW Modules, Catalyst Integrated Security Features

Monitor, Detect, Prevent and Alert on Attacks

4200 Series IDS Sensors, Catalyst 6500 IDS Modules, Router IDS Modules, Cisco Security Agent, IOS AutoSecure, Catalyst Integrated Security Features

Intelligent Management, Monitoring and Analysis

CiscoWorks VMS, CiscoWorks SIMS, Cisco Threat Response Embedded device managers (xDMs), AutoUpdate

Trust and Identity Management

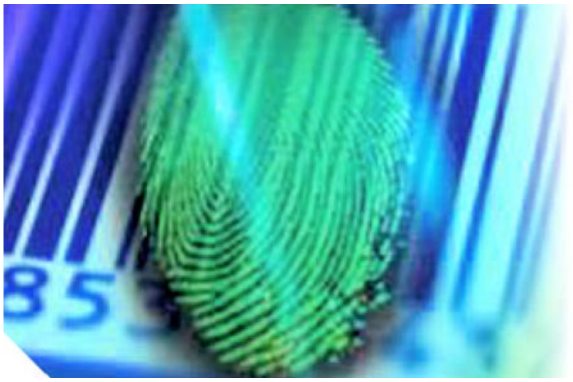
Authenticate, Authorize, and Audit

Cisco Secure Access Control Server, User Registration Tool, 802.1x/AAA services within Routers & Switches

Secure Connectivity

WANs typically connect a portion of an organization to the core network over an untrusted network—for example, the Internet, a service provider network, or a broadband connection. Maintaining data integrity across these connections is paramount. LAN connections, traditionally considered trusted networks, are requiring higher levels of security connectivity as well. Internal threats are the majority of threats today, and while these threats may not always be malicious in intent, they are more damaging than external threats. Preserving the integrity of the data and applications that traverse the wired or wireless LAN needs to be an important part of business decisions.

With secure connectivity, organizations benefit from increased user productivity, business efficiencies, and confidentiality of critical information. The Cisco Secure Connectivity System uses many forms of VPNs to provide flexible and pervasive secure connectivity solutions, such as IP Security (IPSec), Secure Sockets Layer (SSL) VPN, and Multiprotocol Label Switching (MPLS) VPN. VPNs protect both data and voice over IP (VoIP) applications, over multiple wired and wireless media. Combine these VPN solutions with dynamic routing, multiprotocol support, and the widest array of connectivity options in the industry, and the Cisco Secure Connectivity System is a best-in-class solution for VPN deployments.



Threat Defense

Threats today—both known and unknown—are more destructive, frequent, and global than in the past. Internal and external threats such as worms, 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.

To effectively defend against the various attacks, a comprehensive security and network services solution must be implemented throughout the network, rather than using point products or technologies. The Cisco Threat Defense System, through enhancing security in the existing network infrastructure, adding comprehensive security on the endpoints (both server and desktops), and adding dedicated security technologies to critical parts of the network, proactively defends the business, users, and the network. The Cisco Threat Defense System protects businesses from operation disruption, lost revenue, and loss of reputation.

The Cisco Threat Defense System includes several technologies and products that build the defense-in-depth solutions, including firewalls; network IDSs; endpoint protection with Cisco Security Agent; network services in the router and switches such as Network-Based Application Recognition (NBAR), Committed Access Rate (CAR), private VLANs, and port security; Network Admission Control (NAC); content security; and security management.

Trust and Identity Management Systems

As the importance of e-business in a networked economy builds, so will the needs and benefits associated with identity management. No longer relegated to the IT "back burner," identity management and other security issues have emerged as vital enablers of e-business strategy by reducing administrative and operational costs; facilitating relationships with customers, business partners, and employees; and safeguarding organizations' assets.

The Cisco Trust and Identity Management System focuses on network admission control based on device and user credentials and policies. What applications the user has access to, and what they do not have access to, as well as whether the device is allowed on the network is all part of network admission control. The Trust and Identity Management System performs network admission control and identifies the user at different levels of authentication, such as Layer 2 with 802.1x, posture assessment, and an integrated identification approach throughout the network.

Management and Analysis

Integral to a scalable and operationally efficient security system is management and analysis. The ability to provision and manage networks that include different devices and endpoints is a crucial part of any integrated security solution.

The Cisco Security Management Suite provides a management-in-depth approach for efficient security management. Using device managers to provide thorough device management and provisioning capability across the broad range of Cisco security devices provides the depth of device knowledge that is needed when deploying devices throughout the entire network. A central management system to provision, manage, and troubleshoot the network from a systematic perspective—multiple devices, multiple endpoints, multiple locations—allows the Cisco Security Management Suite to provide operational efficiencies for a customer that is deploying the defense-in-depth security strategy.

WLAN Security

With the increased reliance on WLANs, institutions are more concerned about network security. With a WLAN, transmitted data is broadcast over the air using radio waves—any WLAN client within range of an access point can receive data transmitted to or from the access point. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors, or even outside the building that houses the access point.

A recent article in *The Wall Street Journal* described two network intruders with a laptop and a boom antenna who drove around Silicon Valley, CA, "sniffing" for stray WLAN signals. They were able to pick up signals from numerous companies that had not turned on their WLAN security features.

The Cisco Wireless Security Suite for the Cisco Aironet® Family provides robust wireless security services that closely parallel the security available in a wired LAN. The Cisco Wireless Security Suite provides an enterprise-class solution that offers freedom and mobility to end users while maintaining a secure network environment.

Secure Internet Content Management

As higher education institutions extend Web applications and Internet access to students and staff, they need to manage the use of the Internet and bandwidth. Cisco Application and Content Networking System (ACNS) Software running on a Cisco content engine offers organizations several flexible options to block objectionable Web content, filter URLs, and manage their Internet usage policies.

URL filtering does the following:

- Enables management of Internet usage policies to block, allow, delay, coach, or simply report on student and staff Web access
- Increases staff and student productivity by limiting access to unproductive Web content
- Reduces legal liability exposure
- Recaptures wasted bandwidth
- Enhances Internet security

As institutions continue to move mission-critical applications and communications to the Web, port 80 (HTTP) traffic is increasing and becoming a security issue for many institutions. Research indicates that more and more network traffic is Web traffic. Web application security is becoming an important requirement to protect sensitive data. One of the primary functions of Cisco content engines is to serve as security gateways for port 80 traffic and content requests by providing authentication, authorization, and accounting (AAA), virus blocking, and URL filtering.

ARCHITECTURE

The SAFE Blueprint from Cisco is a comprehensive security "best practices" model that enables organizations to safely engage in e-business. Using a modular approach that simplifies security design, rollout, and management as networks grow and change, the SAFE Blueprint enhances networks built on Cisco AVVID (Architecture for Voice, Video and Integrated Data).

The principle goal of the SAFE Blueprint is to provide customers with best-practice information for designing and implementing secure networks. The SAFE Blueprint serves as a guide to network designers considering the security requirements of their networks. The SAFE Blueprint takes an in-depth approach to integrated network security design, focusing on the expected threats and the methods of their mitigation, rather than simply on firewall or IDS placement. This strategy results in a multidimensional, layered approach to security, where the failure of one security system is not likely to lead to the compromise of network resources.

The SAFE Blueprint currently models numerous scaled deployments—from a large-scale, fully resilient enterprise network to a remote user with a personal computer and an Internet connection. Technology-specific papers are available for IPSec-based VPNs, campus IP telephony, and WLANs. Specific best practices for worm and virus mitigation are addressed as well.

CASE STUDIES

University of Central Florida: Integrated Security Approach

Located in Orlando, Florida, UCF educates approximately 42,000 students on its main campus and 21 regional delivery sites. More than 23,000 students take online courses.

Like virtually all institutions of higher education, the UCF campus data network has become a critical resource that supports education, research, administrative services, and campus communications. "The network is a part of how we teach and how we do business," says John C. Hitt, president of UCF.

> **"The SAFE Blueprint gives us a modular environment. If there is a problem in one department, I have the ability to isolate the department from the rest of the network and work on that one incident. I look at the Cisco security product line as a can of Legos; I can plug in and piece these products together as I need to fit every problem. For every problem there's a solution to fit it."**
>
> –Robert D. Scott, Associate Director, Computer Services, University of Central Florida (UCF)

Maximum network reliability is mandatory. "The network has become absolutely mission-critical," says Joel Hartment, vice provost, Information Technologies and Resources at UCF. "Employees and students depend on the network for important services every day, 24 hours a day. Security issues are a threat to that level of capability."

Network security threats were costing the university money and time. The steady increase in viruses, DoS attacks, and similar threats facing all Internet-connected institutions made it clear that improved network security and monitoring were required. In early 2000, a network security administrator was brought in to develop and implement a comprehensive security plan, including policies, technologies, and management. UCF implemented a security solution that included:

- Perimeter security with Cisco PIX® security appliances and Cisco Catalyst® 6500 Series service modules
- Intrusion protection with Cisco IDS sensors and the Cisco Catalyst 6500 Series IDS Service Module to accurately identify and classify known and unknown threats, including worms, DoS attacks, and application-level attacks
- Secure wireless and VPN connectivity using Cisco VPN 3030 concentrators to establish secure connections across TCP/IP networks, including the Internet

There is a new sense of security at UCF. More than three years after extensively securing its network, UCF management benefits from knowing that the university's data and integrity are substantially protected from both internal and external risks. For example, the IT team was able to quickly respond to the Nimda worm in 2001, preventing it from spreading across the UCF network. Cisco technology enabled the team to track the affected machines and immediately remove them from the network.

Minnesota State Colleges and Universities: Cisco PIX Security Appliance is the Clear Winner

Minnesota State Colleges and Universities (MnSCU) is a network of 34 two-and four-year state colleges and universities, serving 140,000 students each semester and producing 27,000 graduates a year. The MnSCU system is composed of 53 campuses that span the state, offering geographically accessible educational opportunities to Minnesota citizens.

After an internal privacy and security gap analysis/audit, the MnSCU board of trustees decided to increase perimeter security across the entire MnSCU network of more than 70 sites. A security steering committee made up of CIOs from MnSCU campuses undertook an evaluation of market-leading firewall products, including CheckPoint FireWall-1 and the Cisco PIX security appliance.

> **"Most sites were converted from a router access list to the Cisco PIX firewall with no more than a few hours of setup time and about 15 minutes of downtime."**
>
> –Michael Janke, Director of Network Services, Minnesota State Colleges and Universities

Adding to its four-person staff was not an option, so the team focused on ease of administration. “We have a small staff and Minnesota is a very large state,” says Michael Janke, director of network services at MnSCU. “Many of our sites are a four- to six-hour drive away and, in winter, it can be minus 40 degrees outside. We get snow by the foot, not by the inch. We needed a firewall that could be managed remotely and could eliminate our staff’s need to go out and tend to an ailing firewall.”

When the votes were counted, the decision was to go with the product that could be operated and managed remotely, and had a lower initial purchase price, as well as lower ongoing maintenance costs. The Security Committee decided in favor of the Cisco PIX security appliance.

The less-complicated Cisco PIX appliance was a real benefit for Janke’s staff, a boon to its productivity and to eliminating travel during long Minnesota winters. “With other competing products, you have a firewall that depends on an ordinary operating system and hard drive to boot and run. A Cisco PIX device boots from Flash and I know it will boot. I also know I can modem into a Cisco PIX device and maintain it remotely,” says Janke.

For many of MnSCU’s 55 sites, the purchase price of the competing product was two to three times more than the Cisco PIX security appliance purchase price. The Cisco PIX security appliance also has far lower yearly maintenance costs. The annual Cisco SMARTnet® support contract on the Cisco PIX appliance includes hardware, software, and free upgrades. For the competing product, MnSCU would have had to pay multiple annual maintenance fees as well as the annual upgrade fees. “For some sites,” says Janke, “the multiple annual maintenance fees of the competing products were more than the cost of a new Cisco PIX firewall!”

MnSCU has deployed 55 Cisco PIX security appliances throughout its network infrastructure. The next phases of MnSCU’s overall network security project will include the deployment of **Cisco** IDSs and remote-access VPNs throughout its network.

National University of Singapore: Balancing Network Security with Open Access

The National University of Singapore (NUS) campus spans 10 student faculties; 35,000 network points; 2000 servers; and 30,000 users—of which about one-third also have concurrent wireless access.

Although network security is very important, network accessibility is also a top requirement. “The campus network is different from a bank because it needs to facilitate research and connectivity above all else,” says Mr. Roland Yeo, network manager for the campus network at NUS. “The most important issue here is balancing security with openness.”

> **“Others simply could not scale up to the performance and reliability we were looking for when handling high bandwidth and DoS traffic.”**
>
> –Roland Yeo, Network Manager for the Campus Network, National University of Singapore

As the overall planner and manager of campus network access, the WLAN, Internet peering, and the international research network in NUS, Yeo found that the nature of the campus's connectivity is also different from that of a typical enterprise. Because of new applications and protocols arising from the multitudes of student projects, a security system, he says, needs to be both flexible and adaptable.

After careful investigation and planning, NUS purchased 14 Cisco firewall services modules (FWSMs). NUS chose Cisco because of its performance, flexibility, and lower cost of ownership.

The FWSM offers one of the fastest firewall data rates on the market today, at up to 5-Gbps throughput, 100,000 connections per second, and one million concurrent connections. Up to four modules can be installed in a single chassis. In evaluation trials, Yeo found that the Cisco FWSM was the only firewall, among several well-regarded brands, to not only stop numerous network attacks, but that allowed friendly traffic to pass through transparently.

There was also a need to protect traffic across multiple network segments easily and intuitively. "People used to think of firewalls as devices between internal and external networks, but today, internal networks must also be shielded from each other," Yeo says. Because the Cisco FWSM resides in a switch that controls the VLAN routing, managing different levels of VLAN security in the campus is relatively easy.

WHY CISCO

Cisco is uniquely positioned to help institutions secure their networks. Industry-leading Cisco platforms, including routers, switches, security appliances, IDSs, and VPN concentrators, provide the foundation for securing an institution's network and maintaining data integrity and availability of online services. The breadth and depth of solutions based on the SAFE Blueprint, combined with an ecosystem of best-in-class, complementary products, partners, and services, enable higher education institutions to deploy robust, secure networks.

Network security should not be just an add-on or overlay, but an essential and integral part of the network infrastructure—from the perimeter to the core. Most competitors offer point products that leave vulnerable gaps in network security. Cisco takes a unique approach to protect your network with integrated solutions that embed security throughout the entire network.

Cisco Integrated Network Security solutions incorporate the most comprehensive selection of feature-rich security services (such as IPSec, VPNs, security appliances, IDSs, anomaly detection, and identity management) that can be flexibly deployed on standalone Cisco appliances (including Cisco PIX devices, IDSs, and VPN concentrators); security hardware and software modules for routers and switches; and security software agents for desktop and servers.

Cisco offers customers:

- A comprehensive, end-to-end security solution from one source
- A flexible and modular solution that allows you to choose the best options for your network
- The SAFE Blueprint for network security—a series of tested engineering best practices to create tight security for networks of all sizes and types
- Protection for the latest technologies, such as wireless solutions and IP telephony
- Award-winning support services
- Partnerships with worldwide leaders in network security
- Excellent quality, standards-based development, and certified products

Cisco provides solutions to comprehensibly secure and protect your desktops, servers, and networks. Cisco has the breadth and depth of expertise to provide the necessary integration of security components into your network. With Cisco Integrated Network Security solutions, you can easily and efficiently integrate security within your network and with services involving data, voice, video, storage, and wireless technologies. Cisco customers benefit from the lowest total cost of ownership and the highest return on investment because they can flexibly deploy and manage security services on Cisco routers, switches, and security appliances using their existing investments in IP infrastructure.

FOR MORE INFORMATION

For more information about the comprehensive Cisco security portfolio, contact your local Cisco account representative, or visit:

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

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 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