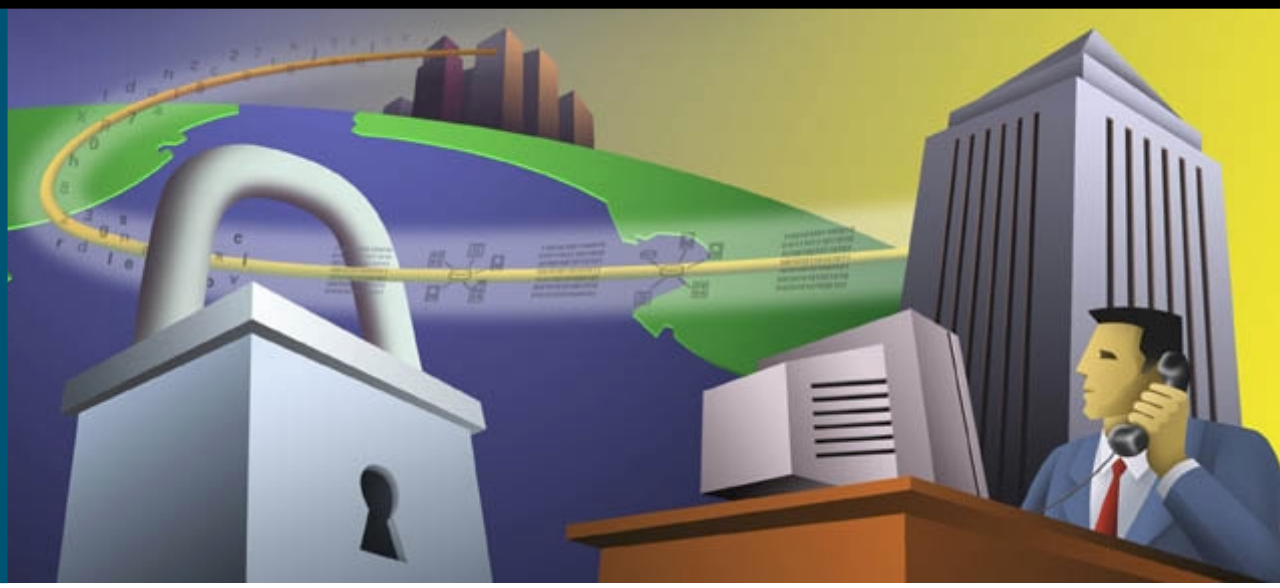
A Beginner's Guide to **Network Security**



An Introduction to the Key Security Issues for the E-Business Economy

With the explosion of the public Internet and e-commerce, private computers, and computer networks, if not adequately secured, are increasingly vulnerable to damaging attacks. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to networks. And all computer users, from the most casual Internet surfers to large enterprises, could be affected by network security breaches. However, security breaches can often be easily prevented. How? This guide provides you with a general overview of the most common network security threats and the steps you and your organization can take to protect yourselves from threats and ensure that the data traveling across your networks is safe.

Importance of Security

The Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide. The volume of traffic moving over the Internet, as well as corporate networks, is expanding exponentially every day. More and more communication is taking place via e-mail; mobile workers, telecommuters, and branch offices are using the Internet to remotely connect to their corporate networks; and commercial transactions completed over the Internet, via the World Wide Web, now account for large portions of corporate revenue.

While the Internet has transformed and greatly improved the way we do business, this vast network and its associated technologies have opened the door to an increasing number of security threats from which corporations must protect themselves. Although network attacks are presumably more serious when they are inflicted upon businesses that store sensitive data, such as personal medical or financial records, the consequences of attacks on any entity range from mildly inconvenient to completely debilitating—important data can be lost, privacy can be violated, and several hours, or even days, of network downtime can ensue.

Despite the costly risks of potential security breaches, the Internet can be one of the safest means by which to conduct business. For example, giving credit card information to a telemarketer over the phone or a waiter in a restaurant can be more risky than submitting the information via a Web site, because electronic commerce transactions are usually protected by security technology. Waiters and telemarketers are not always monitored or trustworthy. Yet the fear of security problems can be just as harmful to businesses as actual security breaches. General fear and suspicion of computers still exists and with that comes a distrust of the Internet. This distrust can limit the business opportunities for companies, especially those that are completely Web based. Thus, companies must enact security policies and instate safeguards that not only are effective, but are also perceived as effective. Organizations must be able to adequately communicate how they plan to protect their customers.

In addition to protecting their customers, corporations must protect their employees and partners from security breaches. The Internet, intranets, and extranets enable fast and effective communication between employees and partners. However, such communication and efficiency can of course be impeded by the effects of a network attack. An attack may directly cause several hours of downtime for employees, and networks must be taken down in order for damage to be repaired or data to be restored. Clearly, loss of precious time and data can greatly impact employee efficiency and morale.

Legislation is another force that drives the need for network security. Governments recognize both the importance of the Internet and the fact that substantial portions of the world's economic output are dependent on it. However, they also recognize that opening up the world's economic infrastructure to abuse by criminals could cause major economic damage. National governments are therefore developing laws intended to regulate the vast flow of electronic information. Furthermore, to accommodate the regulations enacted by governments, the computer industry has developed a portfolio of security standards to help to secure data and to prove that it is secure. Businesses that do not have demonstrable security policies to protect their data will be in breach of these standards and penalized accordingly.

"I have found that inadequate network security is usually caused by a failure to implement security policies and make use of security tools that are readily available. It's vital that companies complete professional risk assessments and develop comprehensive security plans and infrastructures that are publicly supported by upper management."
—Mark Carter, COO, CoreFacts, LLC, Data Recovery and Analysis Firm

Threats to Data

As with any type of crime, the threats to the privacy and integrity of data come from a very small minority of vandals. However, while one car thief can steal only one car at a time, a single hacker working from a basic computer can generate damage to a large number of computer networks that wreaks havoc around the world. Perhaps even more worrisome is the fact that the threats can come from people we know. In fact, most network security experts claim that the majority of network attacks are initiated by employees who work inside the corporations where breaches have occurred. Employees, through mischief, malice, or mistake, often manage to damage their own companies' networks and destroy data. Furthermore, with the recent pervasiveness of remote connectivity technologies, businesses are expanding to include larger numbers of telecommuters, branch offices, and business partners. These remote employees and partners pose the same threats as internal employees, as well as the risk of security breaches if their remote networking assets are not properly secured and monitored. Whether you want to secure a car, a home, a nation, or a computer network, a general knowledge of who the potential enemies are and how they work is essential.

Who are the enemies?

Hackers

This generic and often over-romanticized term applies to computer enthusiasts who take pleasure in gaining access to other people's computers or networks. Many hackers are content with simply breaking in and leaving their "footprints," which are joke applications or messages on computer desktops. Other hackers, often referred to as "crackers," are more malicious, crashing entire computer systems, stealing or damaging confidential data, defacing Web pages, and ultimately disrupting business. Some amateur hackers merely locate hacking tools online and deploy them without much understanding of how they work or their effects.

Unaware Staff

As employees focus on their specific job duties, they often overlook standard network security rules. For example, they might choose passwords that are very simple to remember so that they can log on to their networks easily. However, such passwords might be easy to guess or crack by hackers using simple common sense or a widely available password cracking software utility. Employees can unconsciously cause other security breaches including the accidental contraction and spreading of computer viruses. One of the most common ways to pick up a virus is from a floppy disk or by downloading files from the Internet. Employees who transport data via floppy disks can unwittingly infect their corporate networks with viruses they picked up from computers in copy centers or libraries. They might not even know if viruses are resident on their PCs. Corporations also face the risk of infection when employees download files, such as PowerPoint presentations, from the Internet. Surprisingly, companies must also be wary of human error. Employees, whether they are computer novices or computer savvy, can make such mistakes as erroneously installing virus protection software or accidentally overlooking warnings regarding security threats.

"Ninety-one percent of respondents detected employee abuse of Internet access privileges."

—Annual Computer Security Institute and FBI Survey, 2001

Disgruntled Staff

Far more unsettling than the prospect of employee error causing harm to a network is the potential for an angry or vengeful staff member to inflict damage. Angry employees, often those who have been reprimanded, fired, or laid off, might vindictively infect their corporate networks with viruses or intentionally delete crucial files. This group is especially dangerous because it is usually far more aware of the network, the value of the information within it, where high-priority information is located, and the safeguards protecting it.

Snoops

Whether content or disgruntled, some employees might also be curious or mischievous. Employees known as "snoops" partake in corporate espionage, gaining unauthorized access to confidential data in order to provide competitors with otherwise inaccessible information. Others are simply satisfying their personal curiosities by accessing private information, such as financial data, a romantic e-mail correspondence between coworkers, or the salary of a colleague. Some of these activities might be relatively harmless, but others, such as

previewing private financial, patient, or human resources data, are far more serious, can be damaging to reputations, and can cause financial liability for a company.

What can these enemies do?

Viruses

Viruses are the most widely known security threats, because they often garner extensive press coverage. Viruses are computer programs that are written by devious programmers and are designed to replicate themselves and infect computers when triggered by a specific event. For example, viruses called macro viruses attach themselves to files that contain macro instructions (routines that can be repeated automatically, such as mail merges) and are then activated every time the macro runs. The effects of some viruses are relatively benign and cause annoying interruptions such as displaying a comical message when striking a certain letter on the keyboard. Other viruses are more destructive and cause such problems as deleting files from a hard drive or slowing down a system.

A network can be infected by a virus only if the virus enters the network through an outside source—most often through an infected floppy disk or a file downloaded from the Internet. When one computer on the network becomes infected, the other computers on the network are highly susceptible to contracting the virus.

"85 percent of respondents detected computer security breaches within the last 12 months, up 42% from 1996."

—Annual Computer Security Institute and FBI Survey, 2001

Trojan Horse Programs

Trojan horse programs, or trojans, are delivery vehicles for destructive code. Trojans appear to be harmless or useful software programs, such as computer games, but they are actually enemies in disguise. Trojans can delete data, mail copies of themselves to e-mail address lists, and open up computers to additional attacks. Trojans can be contracted only by copying the trojan horse program to a system, via a disk, downloading from the Internet, or opening an e-mail attachment. Neither trojans nor viruses can be spread through an e-mail message itself—they are spread only through e-mail attachments.

Vandals

Web sites have come alive through the development of such software applications as ActiveX and Java Applets. These devices enable animation and other special effects to run, making Web sites more attractive and interactive. However, the ease with which these applications can be downloaded and run has provided a new vehicle for inflicting damage. A vandal is a software application or applet that causes destruction of varying degrees. A vandal can destroy just a single file or a major portion of a computer system.

Attacks

Innumerable types of network attacks have been documented, and they are commonly classified in three general categories: reconnaissance attacks, access attacks, and denial of service (DoS) attacks.

- Reconnaissance attacks are essentially information gathering activities by which hackers collect data that is used to later compromise networks. Usually, software tools, such as sniffers and scanners, are used to map out network resources and exploit potential weaknesses in the targeted networks, hosts, and applications. For example, software exists that is specifically designed to crack passwords. Such software was created for network administrators to assist employees who have forgotten their passwords or to determine the passwords of employees who have left the company without telling anyone what their passwords were. Placed in the wrong hands, however, this software can become a very dangerous weapon.
- Access attacks are conducted to exploit vulnerabilities in such network areas as authentication services and File Transfer Protocol (FTP) functionality in order to gain entry to e-mail accounts, databases, and other confidential information.
- DoS attacks prevent access to part or all of a computer system. They are usually achieved by sending large amounts of jumbled or otherwise unmanageable data to a machine that is connected to a corporate network or the Internet, blocking legitimate traffic from getting through. Even more malicious is a Distributed Denial of Service attack (DDoS) in which the attacker compromises multiple machines or hosts.

Data Interception

Data transmitted via any type of network can be subject to interception by unauthorized parties. The perpetrators might eavesdrop on communications or even alter the data packets being transmitted. Perpetrators can use various methods to intercept the data. IP spoofing, for example, entails posing as an authorized party in the data transmission by using the Internet Protocol (IP) address of one of the data recipients.

Social Engineering

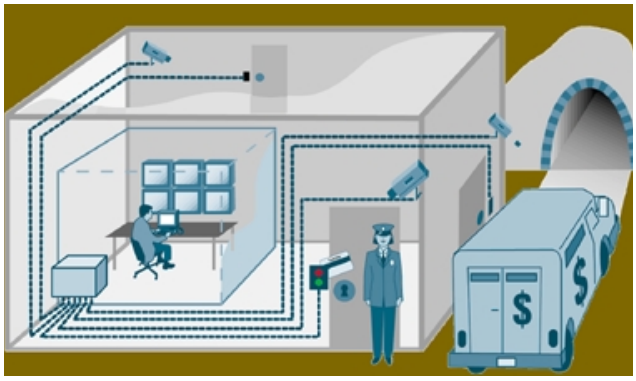
Social engineering is the increasingly prevalent act of obtaining confidential network security information through non-technical means. For example, a social engineer might pose as a technical support representative and make calls to employees to gather password information. Other examples of social engineering include bribing a coworker to gain access to a server or searching a colleague's office to find a password that has been written in a hidden spot.

Spam

Spam is the commonly used term for unsolicited electronic mail or the action of broadcasting unsolicited advertising messages via e-mail. Spam is usually harmless, but it can be a nuisance, taking up the recipient's time and storage space.

Security Tools

After the potential sources of threats and the types of damage that can occur have been identified, putting the proper security policies and safeguards in place becomes much easier. Organizations have an extensive choice of technologies, ranging from anti-virus software packages to dedicated network security hardware, such as firewalls and intrusion detection systems, to provide protection for all areas of the network.



Like a building, a network requires multiple layers of protection to be truly secure.

After such solutions are instated, tools can be deployed that periodically detect security vulnerabilities in the network providing ongoing, proactive security. In addition, professional network security consultants can be engaged to help design the proper security solution for the network or to ensure that the existing security solution is up to date and safe. With all of the options currently available, it is possible to implement a security infrastructure that allows sufficient protection without severely compromising the need for quick and easy access to information.

Top Ten Security Tips

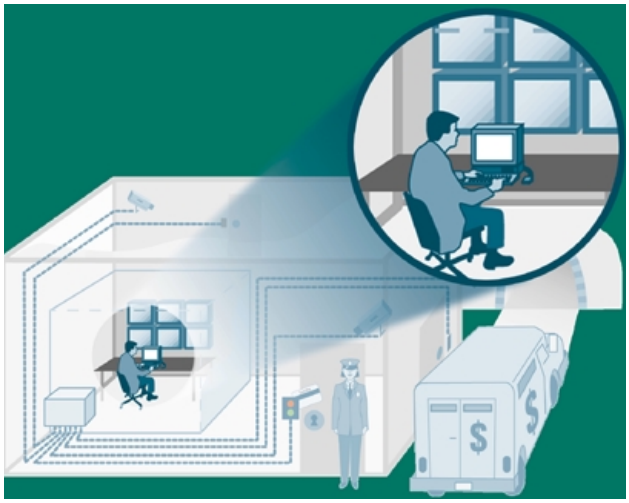
1. Encourage or require employees to choose passwords that are not obvious.
2. Require employees to change passwords every 90 days.
3. Make sure your virus protection subscription is current.
4. Educate employees about the security risks of e-mail attachments.
5. Implement a complete and comprehensive network security solution.
6. Assess your security posture regularly.
7. When an employee leaves a company, remove that employee's network access immediately.
8. If you allow people to work from home, provide a secure, centrally managed server for remote traffic.
9. Update your Web server software regularly.
10. Do not run any unnecessary network services.

Anti-virus Packages

Virus protection software is packaged with most computers and can counter most virus threats if the software is regularly updated and correctly maintained. The anti-virus industry relies on a vast network of users to provide early warnings of new viruses, so that antidotes can be developed and distributed quickly. With thousands of new viruses being generated every month, it is essential that the virus database is kept up to date. The virus database is the record held by the anti-virus package that helps it to identify known viruses when they attempt to strike. Reputable anti-virus software vendors will publish the latest antidotes on their Web sites, and the software can prompt users to periodically collect new data. Network security policy should stipulate that all computers on the network are kept up to date and, ideally, are all protected by the same anti-virus package—if only to keep maintenance and update costs to a minimum. It is also essential to update the software itself on a regular basis. Virus authors often make getting past the anti-virus packages their first priority.

Security Policies

When setting up a network, whether it is a local area network (LAN), virtual LAN (VLAN), or wide area network (WAN), it is important to initially set the fundamental security policies. Security policies are rules that are electronically programmed and stored within security equipment to control such areas as access privileges. Of course, security policies are also written or verbal regulations by which an organization operates. In addition, companies must decide who is responsible for enforcing and managing these policies and determine how employees are informed of the rules and watch guards.



Security Policy, Device, and Multidevice Management functions as a central security control room where security personnel monitor building or campus security, initiate patrols, and activate alarms.

What are the policies?

The policies that are implemented should control who has access to which areas of the network and how unauthorized users are going to be prevented from entering restricted areas. For example, generally only members of the human resources department should have access to employee salary histories. Passwords usually prevent employees from entering restricted areas, but only if the passwords remain private. Written policies as basic as to warn employees against posting their passwords in work areas can often preempt security breaches. Customers or suppliers with access to certain parts of the network, must be adequately regulated by the policies as well.

Who will enforce and manage the policies?

The individual or group of people who police and maintain the network and its security must have access to every area of the network. Therefore, the security policy management function should be assigned to people who are extremely trustworthy and have the technical competence required. As noted earlier, the majority of network security breaches come from within, so this person or group must not be a potential threat. Once assigned, network managers may take advantage of sophisticated software tools that can help define, distribute, enforce, and audit security policies through browser-based interfaces.

How will you communicate the policies?

Policies are essentially useless if all of the involved parties do not know and understand them. It is vital to have effective mechanisms in place for communicating the existing policies, policy changes, new policies, and security alerts regarding impending viruses or attacks.

Identity

Once your policies are set, identity methods and technologies must be employed to help positively authenticate and verify users and their access privileges.

Access Control Servers function like door access cards and the gatekeeper that oversees site security, providing centralized authorization, authentication and accounting (AAA) for traffic and users.

Passwords

Making sure that certain areas of the network are "password protected"—only accessible by those with particular passwords—is the simplest and most common way to ensure that only those who have permission can enter a particular part of the network. In the physical security analogy above, passwords are analogous to badge access cards. However, the most powerful network security infrastructures are virtually ineffective if people do not protect their passwords. Many users choose easily remembered numbers or words as passwords, such as birthdays, phone numbers, or pets' names, and others never change their passwords and are not very careful about keeping them secret. The golden rules, or policies, for passwords are:

- Change passwords regularly
- Make passwords as meaningless as possible
- Never divulge passwords to anyone until leaving the company

In the future, some passwords may be replaced by biometrics, which is technology that identifies users based on physical characteristics, such as fingerprints, eye prints, or voice prints.

Digital Certificates

Digital certificates or public key certificates are the electronic equivalents of driver's licenses or passports, and are issued by designated Certificate Authorities (CAs). Digital certificates are most often used for identification when establishing secure tunnels through the Internet, such as in virtual private networking (VPN).

Access Control

Before a user gains access to the network with his password, the network must evaluate if the password is valid. Access control servers validate the user's identity and determine which areas or information the user can access based on stored user profiles. In the physical security analogy, access control servers are equivalent to the gatekeeper who oversees the use of the access card.

Access Control Lists and Firewalls are analogous to door locks on building perimeters that allow only authorized users (those with keys or badges) access in or out.

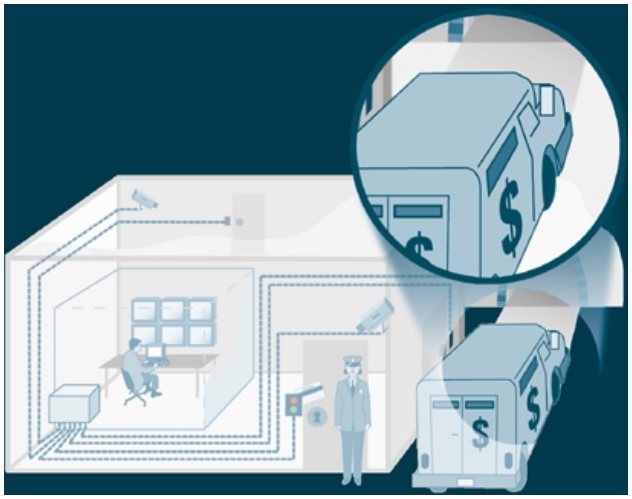
Firewalls

A firewall is a hardware or software solution implemented within the network infrastructure to enforce an organization's security policies by restricting access to specific network resources. In the physical security analogy, a firewall is the equivalent to a door lock on a perimeter door or on a door to a room inside of the building—it permits only authorized users, such as those with a key or access card, to enter. Firewall technology is

even available in versions suitable for home use. The firewall creates a protective layer between the network and the outside world. In effect, the firewall replicates the network at the point of entry so that it can receive and transmit authorized data without significant delay. However, it has built-in filters that can disallow unauthorized or potentially dangerous material from entering the real system. It also logs an attempted intrusion and reports it to the network administrators.

Encryption

Encryption technology ensures that messages cannot be intercepted or read by anyone other than the authorized recipient. Encryption is usually deployed to protect data that is transported over a public network and uses advanced mathematical algorithms to "scramble" messages and their attachments. Several types of encryption algorithms exist, but some are more secure than others. Encryption provides the security necessary to sustain the increasingly popular VPN technology. VPNs are private connections, or tunnels, over public networks such as the Internet. They are deployed to connect telecommuters, mobile workers, branch offices, and business partners to corporate networks or each other. All VPN hardware and software devices support advanced encryption technology to provide the utmost protection for the data that they transport.



Virtual Private Networks (VPNs) are analogous to armored cars that carry precious cargo to an assigned drop-off point to ensure secure and confidential passage.

Intrusion Detection

Organizations continue to deploy firewalls as their central gatekeepers to prevent unauthorized users from entering their networks. However, network security is in many ways similar to physical security in that no one technology serves all needs—rather, a layered defense provides the best results. Organizations are increasingly looking to additional security technologies to counter risk and vulnerability that firewalls alone cannot address. A network-based intrusion detection system (IDS) provides around-the-clock network surveillance. An IDS analyzes packet data streams within a network, searching for unauthorized activity, such as attacks by hackers, and enabling users to respond to security breaches before systems are compromised. When unauthorized activity is detected, the IDS can send alarms to a management console with details of the activity and can often order other systems, such as routers, to cut off the unauthorized sessions. In the physical analogy, an IDS is equivalent to a video camera and motion sensor; detecting unauthorized or suspicious activity and working with automated response systems, such as watch guards, to stop the activity.

Intrusion Detection is analogous to a surveillance camera and motion sensor detecting activity, triggering alerts, and generating an armed response. Scanning is like a security guard that checks and closes open doors or windows before they can be breached.

Network Scanning

Network scanners conduct detailed analyses of networked systems to compile an electronic inventory of the assets and detect vulnerabilities that could result in a security compromise. This technology allows network managers to identify and fix security weaknesses before intruders can exploit them. In the physical security analogy, scanning is like conducting a periodic building walk-through to ensure that doors are locked and windows are closed. It helps to evaluate and understand risk, thereby allowing corrective action to be taken.

Expertise

While electronic scanning tools can be very thorough in detecting network security vulnerabilities, they may be complemented with a security assessment by professional security consultants. A security assessment is a concentrated analysis of the security posture of a network, highlighting security weaknesses or vulnerabilities that need to be improved. Periodic assessments are helpful in ensuring that, in the midst of frequent changes in a network, the security posture of the network is not weakened. In the physical security analogy, a periodic security assessment such as scanning is like a guard periodically patrolling the entire secured area, checking locks on doors and windows, reporting any irregularities that might exist, and providing guidance for correction.

The Result

As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks.

Want to know more?

For further information on network security and how Cisco Systems products and technologies help address security problems and take advantage of the many benefits networks have to provide, please visit the Cisco Systems Web site at 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 Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www.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 Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

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 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

03/01 BW6967