WHITE PAPER

MANAGED SECURITY SERVICES—PARTNERING FOR NETWORK SECURITY

EXECUTIVE SUMMARY

The threats to network security and the vulnerabilities to attack, as well as the skills and sophistication of the attackers, are constantly evolving. As companies deploy more complex e-business models, expand their mission-critical networks with new intranet, extranet, and e-commerce applications, and support a growing mobile workforce, network security technologies are increasingly vital in preventing intrusion and theft of company data assets, and in eliminating network security vulnerabilities.

With the heightened importance of network security, companies are looking to service providers for easy and reliable access to advanced security services and expertise, and to offload management functions so that they may focus on their core competencies.

Given the high risk and cost of security breaches and the challenges of staying abreast of security threat prevention and vulnerability assessments, an increasing number of IT managers across companies of all sizes are exploring ways to take advantage of the expertise and services offered by managed security service providers to enhance network security. By using a managed security services provider, IT managers can direct internal resources to network enhancements that can help grow business and increase productivity, instead of focusing on ongoing operations. Managed security services from service providers can scale from simple equipment monitoring to comprehensive security management and remote site support with dedicated resources, providing IT organizations with tremendous flexibility and control while minimizing security risks and costs.

SECURITY CHALLENGES

Safeguarding data and networks in today's business environment is a complex endeavor. The challenges include:

- *Increased security threats as the use of wide-area networking, the Internet, and remote access grows.* With increased access comes added security risk. Financial, insurance, medical, real estate, and professional services have a high proportion of mobile workers, business travelers, and telecommuters who require secure access to home networks.
- *Increasing malicious attacks in the form of viruses, worms, and Trojan horse attacks, such as Blaster, Code Red, and Slammer.* These attacks spread rapidly and can quickly overwhelm IT resources.
- *The rise in spam.* 40 percent of all e-mail sent is spam; this number is expected to rise to 60 percent by 2007.
- *The threat of impersonation.* The rapid growth in wireless communications and networking has increased the possibility that an intruder could gain access to vital network resources and data by assuming the identity of a trusted user.
- *The cost of "day zero" damage.* Day zero attacks exploit new, unknown vulnerabilities that are difficult to guard against. Attackers spend a great deal of time working on these exploits, trying to find a hole in a specific product, implementation, or protocol. Their secrets are traded like valuable resources, often on Internet Relay Chat channels or private underground Websites.
- *The pace of security threat advances and increasing potency of attacks.* Communications technologies, hardware, and software continue to rapidly evolve, making it challenging to keep vulnerability and response assessment current. While large organizations may be able to afford IT specialization and dedicated resources, it is difficult for small and medium-sized organizations to stay abreast of the latest security technologies and practices.

- *The growing complexity of e-business models.* As more business is conducted over the Internet, the types of services and information that are exchanged are increasingly complex and vulnerable to attack.
- *Customer concerns regarding security and privacy*. Guarding the privacy of their personal information is of enormous concern to customers. Complying with privacy regulations can be considered just a business cost, but many companies understand that establishing a reputation for safeguarding customer privacy can also be a selling point.
- *Compliance with regulations.* Government regulations in the United States and other countries, such as the Gramm-Leach-Bliley Act (GLB), the Health Insurance Portability and Accountability Act (HIPAA), and the Government Information Security Reform Act (GISRA), compel organizations to improve security to protect end users. HIPAA, for example, requires end-to-end encryption of data traveling between medical locations.

With these security challenges to the network, businesses are turning to service providers for managed security services for support. Businesses use managed security services to:

- Improve security posture: identify security threats and vulnerabilities and recommend responses.
- Enhance reliability 24 hours a day, 365 days a year.
- Focus IT resources on supporting in-house applications and networks.
- Protect IT investments and systems.
- Conduct business on the Internet securely.
- Reduce cost through economies of scale.
- Deploy services faster.
- Reduce IT costs.
- Reduce the need to hire specialized IT resources.

SECURITY THREATS

The biggest threats to network security over the past two years have been from viruses, worms, and distributed denial-of-service (DDoS) attacks, which caused the most significant business disruptions and financial losses. Malware, spyware, and new multivector “turbo” worms are becoming increasingly sophisticated—and their damage more devastating. The severity of these threats can be attributed to the dozens of vulnerabilities waiting to be exploited, the availability of worm source code online, recycled exploits, and the ease of editing existing worms. However, it is the secondary effects of worms and DDoS attacks that have wreaked the most havoc. Their propagation mechanisms increase traffic loads and cause additional processing on network devices (random scanning for vulnerable destinations, header variances, or unicast traffic sent to multicast addresses, for example). At the core network level, the aggregate effects of a worm can be substantial.

“...a shift in the biggest problems [have been] toward denial of service attacks.”

—FBI/CSI Cybercrime Report 2004.

Virus

A virus is a piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programs from Websites. They can be sent by other users via e-mail, or in recent cases, can identify vulnerable systems and infect them through a network or the Internet. The virus lies dormant until circumstances cause its code to be executed by the computer. Some viruses can be quite harmful, erasing data or causing your hard disk to require reformatting.

Worms

Worms are designed to gain control of endpoints such as servers or notebook and desktop computers in order to instigate an attack, steal data, send spam, or initiate a DoS attack. While worms are primarily designed to sabotage endpoints, their scanning activities can overwhelm the network. For example, with SQL Slammer, User Datagram Protocol (UDP)-based unicast traffic directed to multicast addresses caused high rates of network device processing. This slowed down regular TCP/IP traffic and led to denials of service that compromised both hosts and the availability of business applications.

DDoS Attacks

A DDoS attack is propagated by a hacker targeting a network device. Once the hacker has control of the device, he or she can instruct it to flood the network, thereby preventing legitimate network traffic or disrupting connections to a specific system or individual. DDoS attacks can also cause the destruction or alteration of configuration information and the physical destruction or alteration of network components. Outbound DoS attacks from an enterprise can be just as devastating to network services as an inbound DoS attack targeting that enterprise. A disturbing trend is the proliferation of botnets, vast networks of computers that have been unknowingly recruited as ‘zombies’ when a piece of code was sent to them in a viral e-mail—usually from an Internet chat room—instructing the computer to leave an Internet port open and accept commands. At a given moment, the hacker instructs all the infected ‘zombie’ computers to, for example, fire page requests at servers, unleashing a vast DDoS attack from thousands—and potentially hundreds of thousands—of PCs. Attacks from botnets brought down the Google, Microsoft, and Yahoo sites in June 2004. Always-on broadband connections make it more likely that thousands of zombies may be available at any one time.

Man in the Middle Attacks

In a man in the middle attack, attackers abuse weak or nonexistent authentication mechanisms between two endpoints. Between these endpoints, the attacker can view information passing back and forth, and can even modify or inject data going into such a connection. These attacks are used to intercept passwords, account numbers, or financial records.

Other Attacks

Many of other types of attacks can also occur, such as brute force dictionary-based password cracking, unauthorized access or snooping of data from wireless networks, and illicit use of telephony networks to gain access to free long-distance calling.

Managed Security Service Offerings

Managed security services can be thought of as layers of defense, with the layers being:

- Prevention
- Detection
- Response

Prevention services, such as managed firewalls, keep intrusions out. Detection services identify when an intrusion is occurring or has occurred. Response services take action to defend against potential intrusion when it is detected. One advantage of working with a managed security provider is that security services can be scaled to meet an organization's security requirements. This flexibility allows companies working with managed service providers to dramatically reduce service outages and operational expenses, thereby increasing return on investment (ROI). An ROI tool presentation to help businesses determine if out-tasked security would be beneficial is available at: http://www.cisco.com/en/US/netsol/ns465/networking_solutions_presentation0900aecd80127e9b.shtml.

Service foundations are the fundamental services deployed before layering other enhancements or additional services. Managed firewall and IP Security (IPSec) VPN are two foundation services in a managed security portfolio. The enhanced services can be offered as standalone services or bundled enhancements. For instance, a managed firewall service can have additional services such as antivirus, content filtering, and authentication services provided together in a bundle from the service provider. Managed security offerings are evolving into layered services that can be tailored to an enterprise's security plan.

Managed Firewall Service

All service providers offering managed firewall service use either a dedicated device or software on the router or switch.

Managed firewall services for enterprise customers typically consist of a Cisco® PIX® 525 or 535 firewall at customer headquarters, and Cisco PIX 515 firewalls at branch offices. Alternatively, service providers can install Cisco 1800, 2800, or 3800 Series integrated services routers, or other Cisco routers with Cisco IOS Firewall Software, at the branch offices. Service providers could also manage an internal firewall, using Cisco PIX 515 firewalls, for example, to protect systems within the clients' LANs.

To add value or options, service providers can offer Web portals for reporting, 24-hour-per-day monitoring, service-level agreements (SLAs), high-availability options, and customer network management.

Relying on a managed security service provider allows business customers to be confident that their network security is constantly up-to-date, despite the rapid pace of technology change in both hardware and software. Small and midsize businesses can also be offered a managed network-based firewall service inside a VPN—a secure way to handle traffic between sites and remote workers that does not overwhelm their technical resources.

Managed Intrusion Detection and Prevention Systems

Most managed security service providers offer intrusion detection and/or prevention services. Intrusion detection systems (IDSs) watch the network to see if suspicious activities are occurring, and provide an alert if something is seen that is outside of normal network behavior. Intrusion prevention systems (IPSs) provide an additional level of security by automatically taking action based on detected events to protect from an attack. For example, an IPS could, in the event that it noticed a pattern of activity that indicated a possible DDoS attack, shut off network access for the suspected attacker.

While companies can implement IDS and IPS directly, managed IDS and IPS services offer valuable benefits. By design, an IPS reacts to many situations. "False positives" can be the result of a temporary surge in Web activity or other normal traffic patterns. Service providers offering IPS service can monitor both normal and suspicious network activities and alert their customers only when a real attack is in progress, saving the customer time.

To provide managed IDS/IPS services, service providers typically install Cisco IDS 4230 sensors or Cisco Catalyst® 6000 Series IDS/IPS modules on critical network segments, and would install host sensors on hosts and critical systems behind the external firewall. Intrusion prevention is now available as a software option on Cisco 2800 and 3000 Series routers. In addition, service providers can add additional value by including 24-hour-per-day monitoring, failover, load balancing, SLAs, and automatic response services.

Managed VPNs

More service providers are offering managed virtual private network (VPN) services. Service providers can offer Layer 2 or Layer 3 VPN services, based on Cisco technology, on native IP or Multiprotocol Label Switching (MPLS)-enabled networks, with optional security provided by IPSec and Secure Sockets Layer (SSL). These services allow businesses to securely extend their networks to remote and teleworking team members, without overburdening their internal resources.

Managed Antivirus Protection

Managed antivirus protection systems provide organizations with the means to establish an overall network admission control system that allows them to stay current as new threats emerge and prevents local users from infecting the network. Most attacks come from trusted users that inadvertently breach security protocols.

Managed antivirus protection is part of Network Admission Control (NAC), a Cisco Systems sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, organizations can provide network access to endpoint devices such as computers, personal digital assistants (PDAs), and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.

NAC is the result of a multivendor collaboration between leading security vendors, including antivirus providers such as TrendMicro, Symantec, Network Associates, Computer Associates, Microsoft, and IBM. NAC extends the use of existing communications protocols and security technologies, such as Extensible Authentication Protocol (EAP), 802.1x, and RADIUS services. The NAC framework combines existing investments in network infrastructure and security technology to provide a secure admission control service, which can be offered as a managed customer premises equipment service.

Managed Endpoint Threat Protection

Managed endpoint threat protection stops servers or desktop computers (also known as endpoints) from executing code that they should not execute, protecting against worms and other potentially malicious attacks, such as a Web server or Linux servers.

Service providers offer this service through Cisco Security Agent, which provides threat protection for server and desktop computing systems by identifying and preventing malicious behavior, thereby eliminating known and unknown security risks and helping to reduce operational costs. Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, operating system integrity assurance, and audit log consolidation, all within a single product. Cisco Security Agent analyzes behavior rather than relying on signature matching to provide robust protection with reduced operational costs.

Service providers can install, manage, maintain, and update this service for your business.

Managed Authentication and Identification Services

Managed authentication and identification services help businesses verify the identities of users requesting access to the network, which in today’s business environment includes remote workers, teleworkers, and external partners.

Service providers add value by providing 24-hour, 365-days-a-year authentication services. A range of authentication options—static passwords, one-time use passwords, and encryption based on user identity can be used.

Service providers use Cisco Secure Access Control Server (ACS) to provide centralized authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a network access servers, Cisco PIX firewalls, routers, and switches. With Cisco Secure ACS, a managed security service provider can quickly administer accounts and globally change levels of service offerings for entire groups of users.

Managed Content Filtering

Content filtering allows businesses to regulate what flows in and out of their company networks. It can govern the Internet content that is made available to users, and can provide protection from malicious content sent to a computer user either through the Internet or by e-mail.

Service providers that offer managed content filtering add value by being able to offer a variety of filters that can monitor network traffic down to the packet level to identify and prevent harmful or unauthorized access to a company's secure network. The service provider enforces whatever rules a company wishes to use to determine which types of traffic, which users, and which kinds of data are allowed in.

Network traffic can be filtered by time of day, user-level access controls, or service limits (a specific dollar amount), giving service providers great latitude in designing the services that they can provide. Content filtering services based on Cisco service control engines can implement wire-speed content filtering either in the service provider's network, or as a device on your company's premises.

DDoS Protection

Many company Websites have suffered from illegal DDoS attacks, and many more than once. DDoS attacks are a threat to businesses worldwide. Designed to elude detection by today's most popular tools, these attacks can quickly incapacitate a targeted business, causing huge losses in revenue and productivity.

Because DDoS attacks are among the most difficult to defend against, responding to them appropriately and effectively poses a tremendous challenge for all Internet-dependent organizations. Because service providers play such a large role in the wide-area connectivity to the Internet, they are the perfect partners to help businesses mitigate these attacks.

Service providers offering DDoS protection rely on a Cisco solution set that includes two components: a detector and a guard. The service is based on one or more detectors, which act as an early warning system that can provide in-depth analysis of the most complex DDoS attacks. The detector passively monitors network traffic, looking for any deviation from "normal" or baseline behavior that indicates a DDoS attack.

When an attack is identified, the detector alerts the guard, providing detailed reports as well as specific alerts to quickly react to the threat. When the guard is notified that a target is under attack, traffic destined for the target is diverted to the guard associated with the targeted device, whether in the network or based on the customer premises. The traffic is then subjected to a rigorous five-stage analysis and filtering process designed to remove all malicious traffic while allowing "good" packets to continue flowing uninterrupted.

Managed DDoS protection services can concurrently protect multiple potential targets, including routers, Web servers, domain name server (DNS) servers, and LAN and WAN bandwidth.

Ongoing Vulnerability Assessment

Maintaining an adequate level of security requires ongoing vigilance. Every business needs to monitor its security posture on an ongoing basis and correct any weaknesses that are identified. Managed security service providers can offer more comprehensive and technically sophisticated vulnerability assessments than many organizations can provide on their own.

Other Services

Service providers can provide other value-added services that businesses can rely upon to develop unique security defensive postures, including:

- Consulting—Service provider consulting and implementation services can extend an IT staff's capabilities during overlapping projects and busy times.
- Emergency response—Service provider emergency response teams can provide forensic analysis when attacks occur and when vulnerabilities are assessed.
- Education and training—To keep a company's technical staff up-to-date with the latest technologies, a service provider can provide ongoing training and education courses.

DECISION TREE

When evaluating the role of managed security services in an organization, organizations should begin by assessing current and projected security requirements. Basics include:

- **Organizational structure**—Consider the security requirements for headquarters, branches, and remote offices (locally, nationally, and worldwide); LAN, MAN, or WAN networks; mobile and offsite workforce; number of workers supported; and so on.
- **Network access and availability**—Bandwidth, application, and usage requirements for both internal and remote workers.
- **Information assets**—Hardware, applications, and critical data.
- **Industry requirements**—Particular security needs may depend on the industry. For example, financial institutions and banks carry greater risk.
- **Government regulation**—Organizations must be in compliance with network security requirements due to government regulations. For example, financial institutions are now subject to the security requirements of the Basel II accords on the security of financial data.

The material presented here can provide a starting place for discussion regarding a business's unique needs with a managed security service provider.

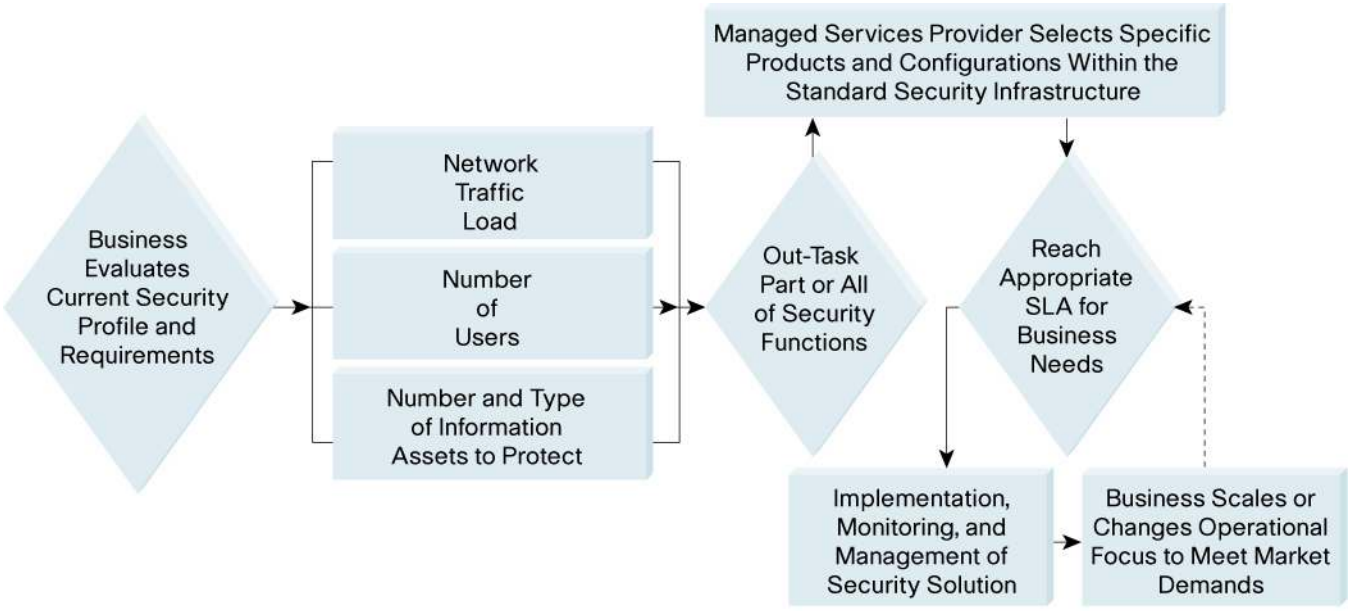
Profiling the Security Needs of a Business

Table 1 presents the security needs of businesses, based on their size. Figure 1 depicts the security decision-making process.

Table 1. Business Security Needs

Small Business	Midsize Business	Enterprise Business
• Low complexity • Low traffic volume • Fewer types of information assets to protect (servers, databases, applications) • Varying amount of risk associated with each asset	• Medium complexity • May host dozens of servers, multivendor hardware and software platforms, and multiple applications • Several different types of information assets • Varying levels of risk associated with each asset	• High complexity • High bandwidth requirements • Many types of information assets • Maximum risk associated with company assets • Large number of remote locations and teleworkers • Varying levels of security risk dependent on business division or workgroup

Figure 1
Security Decision Flowchart



Assessing a Managed Security Service Provider

Finding the right managed security service provider to meet a business's security requirements can begin with assessing and prioritizing business objectives (Table 2).

Table 2. Assessing Manager Security Service Offerings

	Requirement	Advantages Offered by a Managed Service Provider	√
1.	**Access to security expertise and the latest technological advances**	• Service provider expertise • Service provider best practices	
2.	**Excellent customer service**	• 24 hour monitoring • Real-time incident reporting • Administrative control • Onsite support • Reliable service backed by SLA • Responsive support staff	
3.	**Compatibility with existing equipment**	• Interoperability with existing security controls and legacy LAN and WAN environments	
4.	**Protection of WAN connections**	• Protection of Internet-based VPNs • Protection of MPLS VPNs • Secure Internet access service, bundled broadband connectivity, and Web hosting	
5.	**Full suite of managed security offerings**	• May include implementation, management, and training services	
6.	**Consulting services**	• Specialized knowledge on security functions	

	Requirement	Advantages Offered by a Managed Service Provider	√
7.	**Processes and procedures to manage threats and incidents effectively and quickly**	• Specified response times for handling incidents • Real-time reports detailing incidents and threats	
8.	**Flexible "a la carte" offerings and security service bundles**	• Organizations can expand out-tasked services as trust in managed security service provider grows • Organizations can retain control over select security functions to maximize workflow, if needed • Create cost-effective, end-to-end security solutions	
9.	**Maintain Web sales presence to produce revenue**	• Protect Internet links from DoS attacks to maintain Web sales presence • Protect organization from the threat of Web blackout and from extortion threats	

Strategies for Out-Tasking Security Services

Table 3 lists managed security services that address the strategic network security needs of organizations of all sizes.

Table 3. Managed Services Supporting Business Strategies

	Business Strategy	Managed Security Services
Enterprise business	Ensure current security operations can effectively mitigate potential security risks and attacks	• Managed firewalls • Managed intrusion detection and intrusion prevention services • Consulting on overall security policy and architecture
	Protect information flowing in and out of organization	• Authentication • Encryption • Public Key Infrastructure (PKI) • VPN
	Proactively "bulletproof" network	• Policies and technologies in place to secure network against current and future threats • Content security services (e-mail and Web scanning) • DoS protection • Intrusion detection • Vulnerability analysis
Small to midsize business	Extend Internet usage as a way of replacing or expanding existing WAN connectivity	• Managed firewalls • Virus scanning • Managed intrusion detection and intrusion prevention services

SUPPORTED SERVICE OFFERINGS

Cisco can help companies find security partners to provide the services discussed in this white paper. For assistance, visit: http://www.cisco.com/cpn.

WHY CISCO

Cisco Systems is the leader in networking. Service providers have recognized that Cisco security solutions and technologies offer them a competitive advantage when providing managed security services. An increasing number of service providers are offering managed security services to business customers based on Cisco solutions that include Cisco firewalls, VPN concentrators, intrusion prevention devices, DDoS detectors and guards, and desktop software, as well as many network hardware and software components to provide a wide range of network-based services.

Cisco Powered Network Designation

Since 1997, Cisco has awarded the Cisco Powered Network designation to service providers that deliver their services over a network built from end-to-end with Cisco products and technologies, and that meet Cisco standards for network support. Companies that select a service provider with a Cisco Powered Network designation know that their services are delivered over the same high-quality Cisco equipment that powers their own networks. For companies seeking a provider of managed security services, the Cisco Powered Network designation provides even more assurance.

To identify services with a Cisco Powered Network designation, look for the following logo on the service provider's advertisements and other promotional materials.

Cisco Powered Logo

Nearly 400 of the most successful service providers worldwide are members of the Cisco Powered Network Program. They offer a wide range of network-based services—over networks built with Cisco products and solutions—for small and large businesses alike.

FOR MORE INFORMATION

To learn more about managed security services for business security, visit www.cisco.com and www.cisco.com/go/managedsecurity.

Visit www.cisco.com/go/managedservices for Cisco overviews on other managed services, including:

- VPN services
- Business voice services
- Metro Ethernet services

OTHER RESOURCES

Packet, Q1 2004 (Vol. 16 No. 1) (Security Issue) Cisco Systems, http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac253/about_cisco_packet_issue_home.html

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

DM/LW8386 05/05

Printed in USA