Managed **Security** Services

Service providers offering managed security services stand to gain substantially in the coming years as companies of all sizes significantly increase spending on network security.

Service providers can help businesses stop intruders from shutting down networks, removing password files, stealing online corporate assets, intercepting sensitive e-mail, and fraudulently misrepresenting data or users. Security breaches like these affect companies where it matters most: at the bottom line. As a result, information technology (IT) executives worldwide are devoting larger portions of their IT budgets to network security every year.

By providing reliable, effective, and affordable managed security solutions, service providers can help customers protect their information—and their businesses. This paper describes the managed security market in the United States and Canada. It examines growth prospects, market segments, and services. The paper also presents some important Cisco security solutions that service providers can use to protect their customers from security threats.

Market Opportunity

Companies large and small now recognize how important Internet security can be to their businesses. Although information technology spending is down around the globe, companies spend increasingly more on IT and network security each year.

Businesses are purchasing managed security services for many reasons:

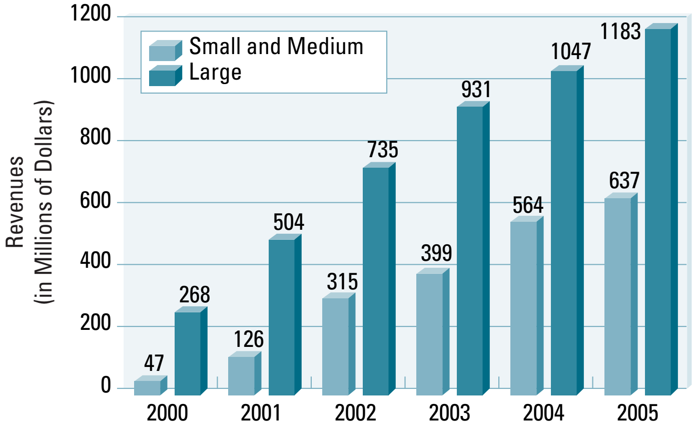
- To boost security quality
- To cut security costs
- To reduce the need to hire specialized IT resources
- To get security systems up and running faster
- To reduce capital investments

Service providers can capitalize on these needs by offering services such as perimeter security, secure connectivity, intrusion detection, authentication, and policy management as well as security consulting, implementation, management, and training. Cisco infrastructure customers require limited hardware investment to launch managed security services, which makes these offerings even more attractive.

The Yankee Group, a prominent industry-analysis firm, conducted a study of the managed security market. Combining small and medium-sized businesses (SMBs) and enterprises, they estimate that the managed security market was $315 million in 2000 and that it will grow to more than $1.8 billion by 2005, as Figure 1 reveals. This forecast includes services for firewall management, virtual private networks, intrusion detection, virus scanning, Web site security assessments, monitoring, applet scanning, content inspection, and URL blocking.

Figure 1

Managed Security Market Potential by Company Size



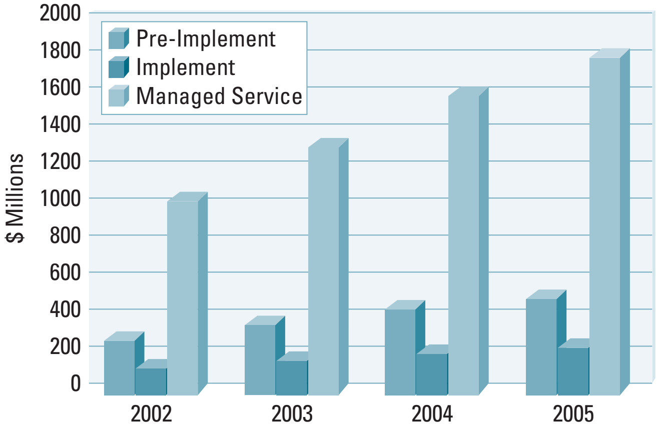
Source: Yankee Group, 2001

Security Market Forecast by Service

Figure 2 provides a revenue forecast of the security market by service type. *Pre-Implement* includes security consulting and solutions design. *Implement* includes deploying the solution but leaving management control with the enterprise. *Managed Service* includes outsourced solutions that tailor security services to specific companies.

Figure 2

Security Market Forecast by Service



Source: The Yankee Group, 2001

Key Market Drivers

A combination of business, technology, and regulatory factors drive today's managed security services market:

- Growing importance of e-business
- Rising use of the Internet and remote access
- Increasing complexity of e-business models
- Fear of security breaches
- Lack of end-user confidence in Internet security
- Dynamic technology
- Government regulation (such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act) that compels organizations to improve security to protect end users
- Complexity of deploying public key infrastructure (PKI) and certificate management systems

Benefits of Managed Security Services

In a 2001 survey of 240 small, medium-sized, and large companies, international market research and consulting firm Infonetics found that respondents cited reliability as the leading criterion for choosing an outsourced managed security service. Other managed security benefits that companies value include:

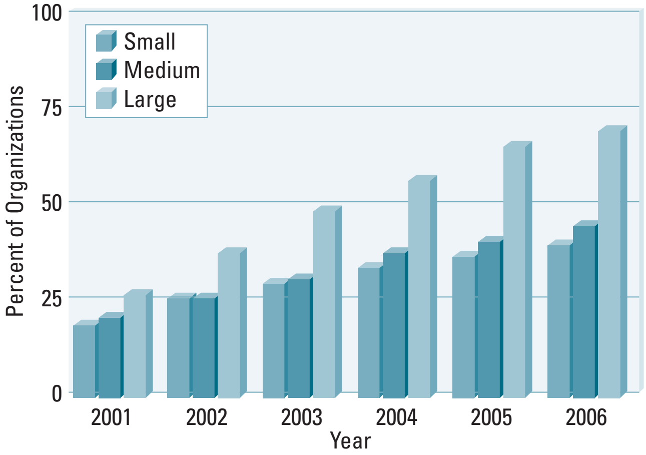
- Improved security
- Lower cost from economies of scale
- Faster deployment
- Improved efficiency of in-house IT staff
- Access to the latest security technologies
- Increased time and resources to devote to core business

Market Adoption by Customer Size

As Figure 3 illustrates, smaller companies are most likely to subscribe to managed security services. These companies can more cost-effectively capitalize on a service provider's experience, economies of scale, and technology than they can build security capabilities on their own.

Figure 3

Adoption Rate of Managed Security by Company Size



To best meet the varying managed security needs of these market segments, service providers should develop services that support a range of access speeds, protect varying numbers of assets (such as computers and servers), and accommodate different numbers of users. This approach allows service providers to offer flexible security-service packages.

According to Infonetics, small, medium-sized, and enterprise companies today spend more on firewalls than on any other managed security service, but intrusion detection represents the fastest growing security service. Firewalls protect internal computers and networks from unauthorized access, and intrusion detection systems alert administrators to network or host server breaches.

Enterprise Businesses

Enterprise organizations tend to internally manage some network security requirements, but few companies have the expertise to build complete solutions themselves. Consequently, service providers can serve as consultants, helping enterprises to assess their security strengths and weaknesses and to develop security policies. This approach allows customers to outsource certain services rather than every aspect of their security programs.

Even large organizations such as banks and government departments that traditionally handle all their security in house are gradually outsourcing some security services. Service providers that enable large enterprises to control their network security services stand to make the greatest gains in this market.

Small and Medium-Sized Businesses

Strong outsourcing candidates, SMBs want managed firewalls and managed intrusion detection systems. Economical, one-box router and firewall devices are ideal solutions for these markets.

Segmentation by Industry Vertical

To target specific industries, service providers should use different service bundles. Driven by regulatory pressures, competition, or both, organizations in the financial, government, and health-care sectors require more stringent security controls than do companies in other industries. Service providers can cater to these high-need clients by combining managed firewall, intrusion detection, and virtual private network (VPN) services.

Service Description

IDC, a leading market research firm, categorizes managed security services into four life-cycle phases:

- Consulting
- Implementation
- Management
- Education and training

Service providers should strive to address their clients' network security needs at each life-cycle phase. Service providers that lack the resources to offer services throughout their clients' life cycles should consider partnering with other companies to fill service gaps.

Phase I: Network Security Consulting Services

Many companies enter the security services life cycle in the consulting phase. Others subscribe to consulting services when they change their IT infrastructures. Consulting therefore offers service providers a way to win new business and generate extra revenue from existing customers. Service providers can partner with security consultants, IT companies, or integration firms to offer security consulting services, or they can build these services into their own portfolios.

Even companies that manage their own network security are candidates for consulting services, which can include:

- Reviewing and developing security policies
- Determining enterprise security needs and developing security plans
- Assessing technical weaknesses by testing current network security
- Analyzing routers, switches, firewalls, and other security controls to look for security shortcomings in operating systems, legacy equipment, databases, and network security services
- Auditing systems to determine how well they comply with government regulations or industry standards

Phase II: Network Security Implementation Services

At this stage, companies have a security plan. Now they need to implement the hardware and software to follow that plan. Service providers should note that clients usually hire their security consultants to handle implementation as well.

Implementation services can include:

- Reviewing and recommending security products
- Acquiring, inspecting, and connecting security hardware
- Obtaining, installing, and testing software
- Implementing access policies
- Setting up terminal ports, clients, users, groups, databases, and directories
- Integrating the new system into the network
- Training IT and other personnel

Phase III: Network Security Management Services

At this stage, customers have assessed their security needs and have implemented the security hardware and software to address those needs. They now require security management services that capitalize on their newly implemented systems. These management services can include firewall provisioning, intrusion detection, VPNs, content filtering and blocking, virus protection, and vulnerability testing.

Service providers can choose to offer end-to-end security management solutions, or they can provide security services individually. This latter approach allows service providers to gain a client's confidence with one security offering and then promote others as the relationship evolves.

Security management services can include:

- Managing security devices 24 hours per day
- Creating processes to escalate issues and respond to problems
- Authenticating users
- Employing managed firewall services to restrict network protocols and traffic
- Detecting intrusions or unauthorized access to networks, systems, services, applications, or data
- Protecting outsourced e-mail services, gateways, and firewalls from viruses
- Responding to security breaches or other security incidents

Phase IV: Network Security Education and Training Services

In this fourth phase, service providers can help clients learn about the network security products and technologies that protect their assets. Training can range from general security awareness sessions to product information clinics to formal certification programs.

Service providers that lack the resources to train clients may want to partner with other organizations to offer these types of services.

Service Offering by Customer Segment

This paper divides the market for managed security services into two main segments: enterprise organizations—businesses with more than 1000 employees—and small and medium-sized businesses defined as those with 1000 or fewer employees.

Segmenting markets according to size helps service providers offer solutions that fit with their clients' traffic loads and number of users, servers, databases, and applications.

Enterprise Businesses

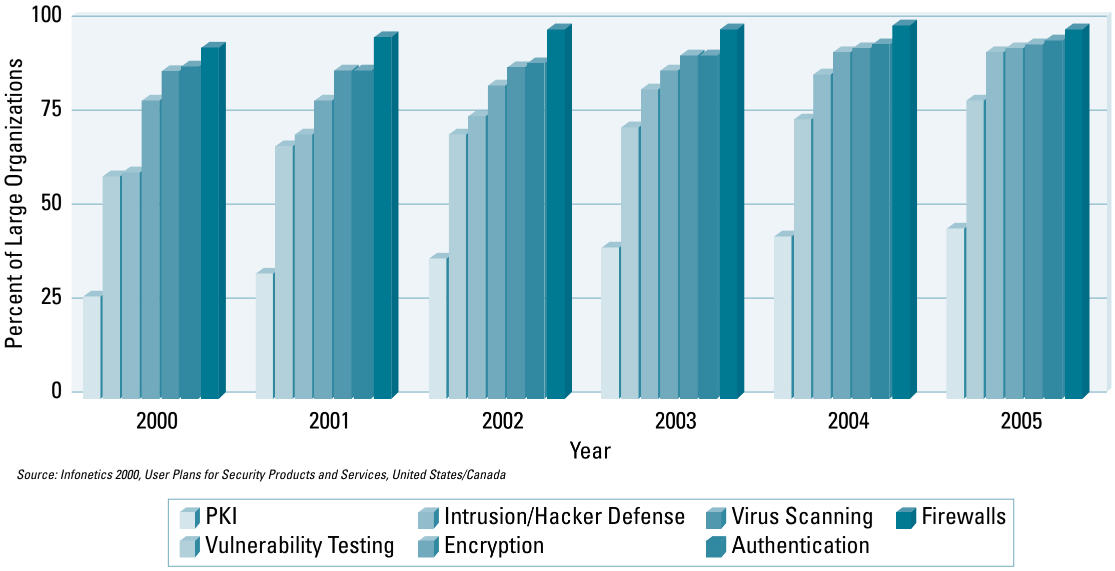
Enterprise businesses typically operate networks with high-bandwidth connectivity, employ numerous teleworkers, and oversee multiple remote sites. These companies often need to protect a wide variety of information assets, each with potentially different security levels.

Customer Requirements

As Figure 4 illustrates, more than half of all enterprises today deploy firewalls, virus scanning, intrusion detection, encryption, authentication, and vulnerability testing services. According to Infonetics, this number will increase to 75 percent by 2004. Note that even though the firewall market seems saturated, many large firms are likely to implement second and third firewalls to further improve security.

Figure 4

Large Business Security Technology Usage



Source: Infonetics 2000, User Plans for Security Products and Services, United States/Canada

Enterprises typically rely on in-house IT experts to provide these security services, but service providers are gaining business in this market by offering the following:

- Access to security expertise and the latest security technology
- Compatibility with existing equipment
- A full suite of managed security offerings
- Individual security services and secure service bundles
- Consulting, implementation, and training services
- Effective and rapid management of threats and incidents that could compromise network security
- Excellent customer service
- Partnerships with best of breed vendors
- Penalty-based service-level agreements (SLAs)
- Lower prices from economies of scale

Service providers that offer these features can help large businesses:

- Focus on core competencies
- Free staff from day-to-day security administration
- Reduce operational costs
- Take advantage of service provider expertise and economies of scale
- Capitalize on incident reports
- Identify potential security threats and attacks

Solution Sets

It is recommended that service providers sell managed security services individually. This approach allows enterprises to outsource portions of their network security operations while keeping the ability to change policies, manage real-time user access, update services online, and control other security-related activities—important concerns for large businesses.

This paper looks briefly at two services that service providers can offer individually: managed firewall and intrusion detection.

Managed Firewall Services

Managed firewall services for enterprise customers typically consist of a Cisco PIX® 525 or Cisco PIX 535 Firewall at customer headquarters and Cisco PIX 515 firewalls at branch offices. Alternatively, service providers could install Cisco 1700, 2600, 3600, 3700, or other Cisco series routers with Cisco IOS® Software at the branch offices. Service providers could also manage an internal firewall, such as Cisco PIX 515s, 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, SLAs, high-availability options, and customer network management.

Intrusion Detection Services

To provide managed intrusion detection services, service providers would typically install Cisco IDS 4230s or Cisco Catalyst® 6000 Series IDS modules on critical network segments. Service providers would also install host sensors on hosts and critical systems behind the external firewall. They could add value by including 24-hour-per-day monitoring, failover, load balancing, SLAs, and automatic response services.

Positioning

Service providers compete primarily with in-house IT teams. Consequently, service providers should position their managed services as reliable, allowing customers to control policy changes and user access. As well, service providers should show that by reducing security breaches and associated downtime, they can help corporate IT teams better support in-house applications and networks—an attractive productivity boost.

Small and Medium-Sized Businesses

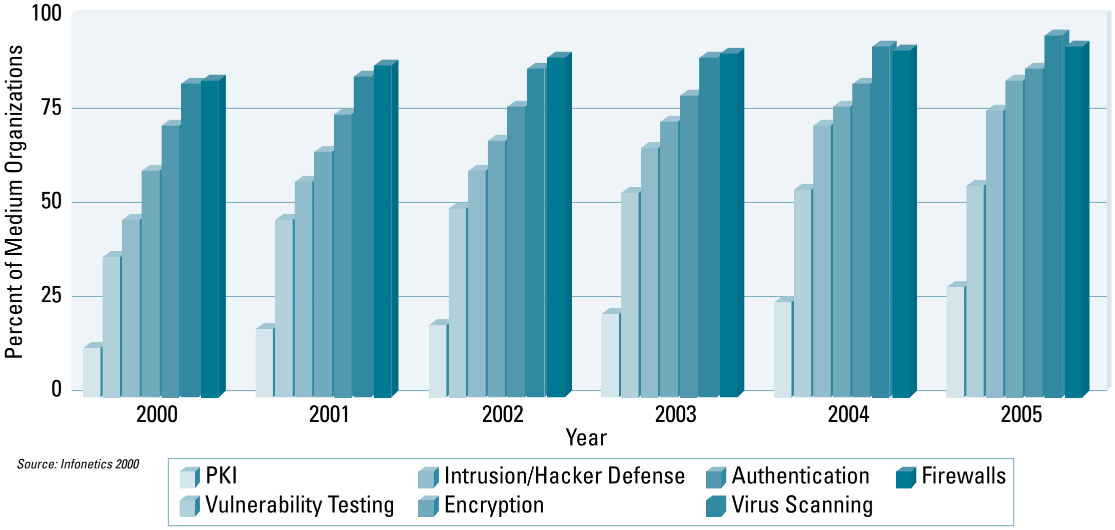
With fewer employees and branches, SMBs typically have lower bandwidth connectivity than do large businesses. They also need to protect fewer information assets, they are more price-sensitive, and they are more likely to outsource than are enterprise clients.

Customer Requirements

As Figure 5 illustrates, IDC reports that more than 75 percent of medium-sized businesses use virus scanning and firewalls. The chart also reveals that between 50 and 75 percent of medium-sized companies employ several security technologies.

Figure 5

Medium-Sized Business Network Security Technology Usage

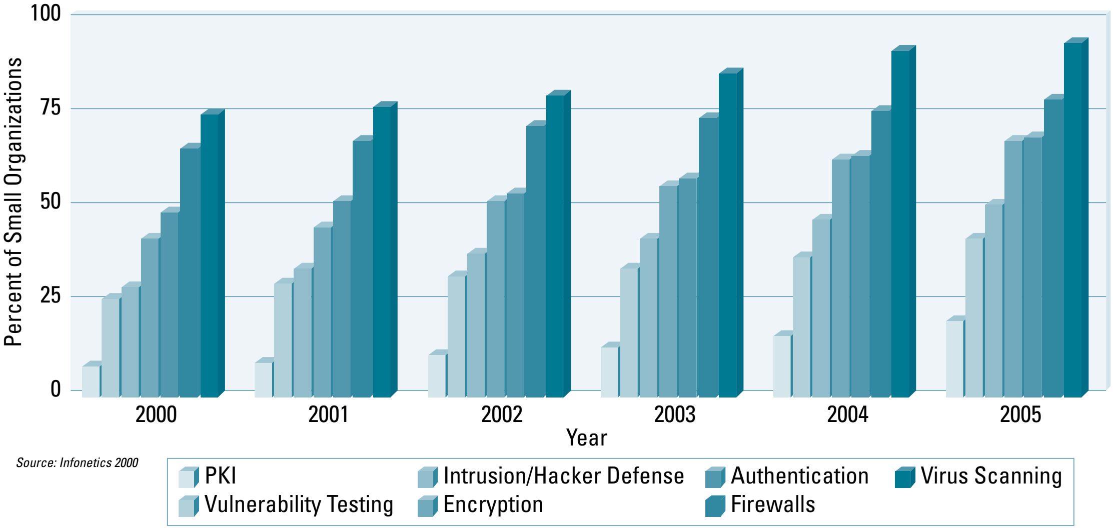


Source: Infonetics 2000

Figure 6 below indicates that small organizations are least interested in network security services. Yet, these customers are more inclined to purchase managed security services than are either medium-sized or enterprise businesses. Small businesses are more likely to subscribe to virus scanning and firewall services.

Figure 6

Network Security Technology Usage by Small Businesses



Source: Infonetics 2000

SMB customers want managed security service providers to do the following:

- Protect their IT investments and systems for relatively low monthly fees
- Allow them to conduct Internet business securely
- Enable them to focus on their core businesses
- Act as a single resource for security services
- Bundle Internet access, VPN, and Web hosting with managed security or offer these services as options
- Provide access to security expertise and the latest security technology
- Produce frequent incident reports
- Identify security threats and attacks
- Recommend responses
- Offer excellent customer service
- Guard broadband Internet connections

Solution Sets

With less in-house expertise and fewer resources, customers in the SMB segment will more readily outsource their security solutions than will enterprise businesses. Outsourcing allows SMBs to take advantage of the skills and economies of scale that service providers offer—an important benefit.

Unlike large businesses that want service providers to provide individual security services, SMBs prefer bundled services. Service providers that bundle managed firewall and intrusion detection services with Web hosting, high-speed Internet access, or VPN services will therefore appeal to this segment. Service providers may want to avoid promoting consulting and implementation services because the SMB segment may find them too expensive.

A typical managed solution for the SMB market would consist of a Cisco PIX 515 Firewall or Cisco IOS Software within either a Cisco 1700, 2600, 3600, or 3700 series, or other router. Service providers would provide intrusion detection service based on Cisco IOS Software to all critical segments over an IP Security (IPSec) protocol site-to-site and over a remote-access VPN network. Optionally, service providers could manage host sensors on hosts and critical systems behind the external firewall.

Positioning

Service providers compete primarily with other service providers for SMB business revenues. To best appeal to this market, service providers should promote their network security expertise and position their services as reliable and attractively priced.

Cisco Security Solutions

Service providers can use Cisco products to provide an extensive variety of security services. This section describes some of the most powerful and popular Cisco security technologies and solutions available today.

Cisco Secure Integrated Software

The security feature set in Cisco IOS software is collectively called the Cisco Secure Integrated Software and includes the firewall feature set, intrusion detection feature set, authentication proxy feature set, and port application mapping feature set. Service providers can add Cisco Secure Integrated Software to the Cisco 800, uBR900, 1400, 1600, 1700, 2500, 2600, 3600, 3700, 7100, 7200, and 7500 series routers. The software is also available on the Cisco Catalyst 5000 Series Route Switch Module (RSM).

Cisco PIX Firewall

Customers that want even greater security can install Cisco PIX firewalls, which are standalone firewall appliances. Providing unmatched reliability and functionality, the Cisco PIX Firewall scales to fit a wide variety of customer requirements and network sizes. Several models exist, ranging from high-capacity units that can handle half a million concurrent connections to lower-capacity versions designed for the small office-home office (SOHO) market.

A Cisco Firewall Solution

Companies can use both Cisco Secure Integrated Software and Cisco PIX firewalls to establish multiple lines of defense. For instance, companies could put their external servers—Web, e-mail, public File Transfer Protocol (FTP), and others—behind Cisco routers equipped with Cisco Secure Integrated Software. The routers serve as the first line of defense.

Cisco PIX firewalls represent the second line of defense. In the event of a first-line network security breach, Cisco PIX firewalls help prevent intruders from accessing corporate private network servers, mail hubs, and clients. To further strengthen security, service providers can deploy host-based and network-based intrusion detection systems, which are discussed below.

Cisco Intrusion Detection System

The Cisco Intrusion Detection System (IDS) allows businesses of all sizes to identify and reduce network threats. It helps them to detect, prevent, and react to unauthorized network activity.

The Cisco IDS includes network-based (NIDS) sensors and host-based (HIDS) sensors. The NIDS primarily address attacks targeted at network devices, network services, and applications. The HIDS protect servers against operating system and application attacks. Each is described briefly here.

Cisco Network-Based IDS Sensors

The Cisco Intrusion Detection System is a real-time network-based IDS (NIDS) designed for banks, the military, and other organizations that operate critical networks. Cisco engineered its IDS family to prevent denial-of-service attacks, detect intruders, and defend e-commerce business.

Cisco IDS scales to meet a wide variety of customer requirements and network sizes and consists of three models: the Cisco Catalyst 6000 IDS, the Cisco IDS 4230, and the Cisco IDS 4210.

Cisco Host-Based IDS Sensors

Network intruders frequently target host servers. Consequently, Cisco developed its IDS Host Sensor to identify attacks and prevent unauthorized access to critical server resources. Whereas other host defense systems merely detect problems, the Cisco IDS Host Sensor lessens potential damage by stopping intruders from accessing servers.

Cisco Access Control Server

The Cisco Secure Access Control Server (ACS) allows organizations to centrally control network login and user privileges from a Web-based graphical interface. Using Cisco ACS, network administrators can determine which account information to record for security audits or account billing. They can also set up network access and command controls for lower level network administrators.

Cisco Security Management Tools

VPN/Security Management Solution

CiscoWorks VPN/Security Management Solution (VMS), an integral part of the SAFE Blueprint from Cisco, combines Web-based applications for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems. Table 1 lists CiscoWorks VMS modules and their functions.

Table 1 CiscoWorks VPN/Security Management Solution Components

Module	Usage
Management and Monitoring Centers:	
Management Center for PIX Firewalls	Configures PIX firewalls
Management Center for IDS Sensors	Configures network-based IDS
Management Center for VPN Routers	Configures VPN routers
Monitoring Center for Security	Monitors network and host-based IDS events, Cisco IOS Software, and PIX syslog
Auto Update Server	Permits configurations to be pulled from update server
Common Services	Provides a set of common software and services for the management centers
Cisco Secure Policy Manager	Configures PIX firewall, Cisco IOS firewall, and VPN
Cisco IDS Host Sensor and Console	Configures host-based IDS, to protect critical servers
VPN Monitor	Monitors IPSec-based site-to-site and remote access
VPN Resource Manager Essentials	Provides operational management such as software distribution, change audit, and syslog analysis
CD One/CiscoView	Provides graphical device management

Cisco Partners

Several partners provide management solutions for Cisco security products. Two of these solutions are noted here.

SolfSoft is a UNIX-based management tool that supports the Cisco Secure Integrated Software Firewall and Cisco PIX Firewall. It allows users to define, deploy, enforce, and audit security policies from a central location.

netForensics features a full set of e-business security management reporting services. It allows users to analyze Internet security devices postmortem and produce reports.

Cisco Security Training Services

Cisco offers numerous security courses and a Cisco Security Specialist designation. Please refer to the Cisco Security Training Services Web site at:

www.cisco.com/warp/public/10/wwtraining/certprog/cqs/security for details.

Cisco Secure Consulting Services

Cisco Secure Consulting Services help companies protect their IP networks. Rather than concentrating on policy-intensive exercises and reviews, Cisco security consultants focus on network bits and bytes—uncovering security gaps, fixing them, and removing intruders when they strike.

Cisco offers two types of security consulting services: a Cisco Security Posture Assessment that allows organizations to understand the security strengths and weaknesses of their networks and a Security Design Review that provides expert insights into and reviews of existing network security plans and design documents.

Network Management System (NMS) and Operations Support System (OSS) for Managed Security Services—For the SMB

The Cisco Internet OSS for Managed Security Services solution, focused on small and medium-sized businesses, provides network management support for IP VPN services throughout their life cycles. Using a unique plug-n-play architecture, the OSS offers a carrier-class VPN management solution. This solution enables service providers to provision VPN services including automated device configuration and routing auditing. The solution also performs service-assurance functions such as VPN-aware fault and alarm management, and it measures and monitors service-level agreements.

Moreover, the Cisco Internet OSS solution enables customers to deploy IPSec VPNs quickly using Internet Key Exchange (IKE) and IPSec tunnels between routers based on Cisco IOS Software, Cisco VPN 3000 Series concentrators, or Cisco PIX Firewall devices. Customers can deploy these VPNs automatically with minimal user input, which allows getting new IP VPN services to market quickly.

The Cisco VPN Solution Center (VPNSC) also supports router console provisioning and templates. This support enables operators to adopt other security-related services such as firewalls (for both Cisco IOS Software and PIX Firewall), Network Address Translation (NAT), or even quality of service (QoS). By automating service and network provisioning, Cisco VPNSC simplifies managing complex carrier-class IP VPN services. Features that improve ease of use, free network administrators for other tasks, and enable IP VPN services to easily scale reduce costs and enhance a provider's competitive advantage.

The Cisco Internet OSS for Managed Security Services solution will improve productivity by automating tasks, reduce operating expenses through fault-free and fault-recovered service deployment; and protect revenues by monitoring service-level agreements.

Network Management Solution Components

The Cisco Internet OSS for Managed Security Services solution takes advantage of the following products:

Cisco VPN Solution Center (VPNSC)—Provides service provisioning, device configuration, and management capabilities for service providers offering Multiprotocol Label Switching (MPLS)-based services, IPSec-based IP VPN services, or both. Cisco VPNSC enables service providers to accelerate time to market, gain a competitive advantage, and generate revenue faster.

Cisco VPNSC 2.2 can be used to provision security services such as firewalls as well. Moreover, the next version of VPNSC will enable service providers to offer an even broader range of security services, including IDS services.

Cisco CNS Configuration Engine featuring Cisco CNS 2100 Series Intelligence Engine—Provides an intelligent network interface to applications and users. It enables customers to integrate, deploy, and configure Cisco customer premises equipment (CPE)-based network devices while improving productivity with minimal training. The Cisco CNS 2100 Series is fully integrated with the Cisco Configuration Express ordering solution.

Cisco Info Center—Designed to help operators focus on important network events. Offering a combination of alarm reduction rules, filtering, customizable alarm viewing, and partitioning, the Cisco Info Center is a highly configurable client/server application that provides multidomain service assurance and service-level monitoring. It also offers diagnostics tools for network fault and performance monitoring, trouble isolation, and real-time service-level management for large networks.

Cisco VPN Policy Manager—Provides fault and alarm management that correlates network-element-layer alarms to service-level faults, VPN sites, and faults that affect customer service levels. It enables service providers to manage IP VPN network services including flow-through provisioning and service assurance.

Cisco CNS Notification Engine—Provides carrier-class, fault-management capabilities that focus on detecting, diagnosing, and resolving network faults. The software application enables users to proactively poll device status and convert Cisco IOS Software syslog messages into Simple Network Management Protocol (SNMP) traps and notifications.

Cisco CNS Performance Engine—Combining embedded intelligence with scalable fault management, configuration, accounting, performance, and security (FCAPS) and IP management, the Cisco CNS Performance Engine locally processes and correlates performance metrics for particular services and application domains. It easily integrates with the service-level management, rating, and billing mediation applications that service providers depend on to manage and bill for services.

Future Directions

In the coming years, governments will more actively regulate industries—financial, healthcare, and online commerce in particular—to ensure that customer data remains secure. Prompted by regulation and the threat of lawsuits, businesses will place greater emphasis on network security.

Nevertheless, hackers and intruders will continue to invent cunning ways to sneak into computers and networks. To counter these threats and mitigate potential damage, companies will depend on the expertise and technology of managed security service providers.

One of the world's foremost Internet security experts, Cisco Systems will continue to develop reliable, advanced internetworking security products and services. As they have always done, managed security service providers will be able to rely on Cisco to effectively protect their customers' information assets, their reputations, and their profitability.

For More Information

To learn more about Cisco Managed Security Services, please contact your Cisco account manager.

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

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

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