Cisco Systems

Solutions Guide

Securing Your Business Network: Cisco **Integrated Network Security** Solutions

"Networks have evolved from closed to more open, sophisticated systems. As a result, security threats have grown exponentially both at the network perimeter and from within. Cisco is the first with an articulated strategy to integrate security services into the network infrastructure. This is the most logical, cost-effective approach to secure today's extended network in a comprehensive fashion."

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

Securing Your Business Network: Cisco **Integrated Network Security** Solutions

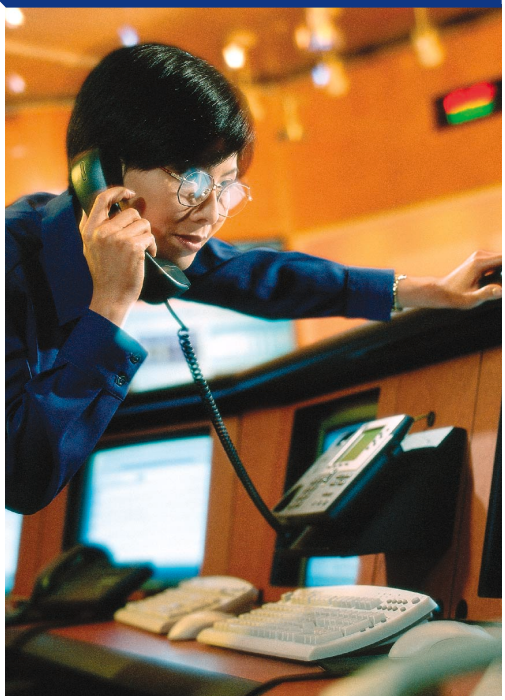
Each day, forward-thinking organizations reinvent how they conduct business by adopting Internet-based network solutions. The results: competitive advantage, new sources of revenue, and optimized business processes.

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

One risk is network security breaches, which can result in damaging losses.[1] Another risk is the fear of security breaches, which can cause organizations to delay implementing Internet-based solutions they need to stay competitive. In today's dynamic business environment, this reluctance can quickly reduce a company's growth potential and erode its profitability.

In some industries, network security has even become a government mandate. U.S. healthcare providers must comply with Healthcare Insurance Portability and Accountability Act (HIPAA), U.S. financial services providers are governed by the Gramm-Leach-Bliley Act, and U.K. companies must adhere to the Turnbull Report on Internal Control for public companies as well as the Data Protection Act of 1999.

[1] 44% of respondents in the Computer Security Institute's Computer Crime and Security Survey (April 2002) were willing and/or able to quantify financial losses. The total: $455 million, (www.gocsi.com/press/20020407.html)



The Cisco Vision

Cisco empowers its customers to safely deploy critical business applications and processes on interconnected IP networks, to help them increase productivity and gain competitive advantage. The confidence that comes from knowing that company business processes and information assets are secure is the key that can unlock tremendous gains in productivity and dynamic growth.

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

If your networks are built on a Cisco infrastructure, we are uniquely positioned to help you secure your network. That's why we continue to add security intelligence to your Cisco infrastructure in ways that are ubiquitous, integrated, and transparent. And that's why customers have made Cisco the leader in network security. We understand that security isn't just an afterthought—it's fundamental to your business processes and ultimately your success.

The Cisco Integrated Network Security Solution Strategy

Cisco delivers integrated network security solutions on modular, scalable platforms that include Cisco routing and switching infrastructure as well as security-specialized appliances, along with security management software, consulting, and educational services.

Advanced security features, such as dynamic policy enforcement in response to attacks and misuse, provide real-time enterprise protection. Embedded software solutions, plus hardware-based accelerators for firewalling, encryption, and intrusion detection, transform your Cisco network into a secure and protected scalable, reliable infrastructure. And by employing a policy-based management approach, Cisco makes it easy to define, enforce, and audit security for users and devices throughout your enterprise.

Critical Elements of Network Security

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

1. Extended Perimeter Security

This element provides the means to control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Routers and switches with access control lists and stateful firewalls, as well as dedicated firewall appliances, provide this control.

2. Data Privacy and Secure Connectivity

When information must be protected from eavesdropping or tampering, the ability to provide authenticated, confidential communication on demand is crucial. Two complementary architectures satisfy this requirement.

MPLS-based VPNs ensure confidentiality via traffic separation, similar to the technique used in trusted Frame Relay or ATM network environments. MPLS is best deployed at the network core. IPSec VPNs, in turn, employ a flexible suite of encryption and tunneling mechanisms at the IP network layer. IPSec is most useful at the local loop, edge, and off-net.

Using either or both architectures to establish a secure VPN is specially important when conducting business transactions across the Internet or intranets, creating the challenge of managing, scaling, and ensuring reliable transactions for new traffic types, such as Secure Sockets Layer (SSL) for secure Web sessions.

3. Identity

Identity is the accurate and positive identification of network users, hosts, applications, services, and resources. Standard technologies that enable identification include authentication protocols such as RADIUS and TACACS+, Kerberos, and one-time password tools, as well as new technologies such as 802.1x, digital certificates, and smart cards. New requirements for flexible policies, scale, and mobility are assuming an increasingly important role in identity solutions.

4. Intrusion Protection

To ensure that a network remains secure, it's important to regularly test and monitor the state of security preparation. Network vulnerability scanners can proactively identify areas of weakness, while intrusion detection systems can monitor and reactively respond to security events as they occur. Using intrusion-protection solutions, organizations can obtain unprecedented visibility into both the network data stream and the security posture of the network.

5. Security Management

As networks grow in size and complexity, the requirement for centralized management tools to manage device, configuration, and security events grows as well. Sophisticated tools, ones that can define, distribute, enforce, and audit the state of security policy through browser-based user interfaces, enhance the usability and effectiveness of network security solutions.

Cisco Integrated Security Solutions: A Family of Network Security Offerings

Cisco award-winning security products and consulting services provide the building blocks of these critical elements, delivering the network security solution that your business needs.

Cisco PIX 500 Series Firewall

The Cisco PIX™ 500 Series Firewall (Figure 1) is the world's leading firewall, providing unmatched reliability, scalability, and functionality. Its integrated design for specialized appliances and Cisco Catalyst® switch modules, and its innovative hybrid security architecture—which includes stateful inspection as well as IPSec and MPLS VPN capabilities—deliver the highest levels of security and performance. The Cisco PIX Firewall handles more simultaneous connections than any other firewall, yet its speed is unsurpassed.

Figure 1 Cisco PIX Firewall

Cisco Security Routers and Switches

Cisco has directly integrated security functionality into the network infrastructure through enhanced security features and functionality in Cisco routers and switches, providing unparalleled flexibility and cost savings for security deployments. By taking advantage of these network devices, organizations can enable sophisticated security policy enforcement throughout the network and use their investments in Cisco infrastructure. Running on all Cisco routers and switches, Cisco IOS® Software uses standards-based, full-featured MPLS and IPSec VPN technology that supports remote access and branch office connectivity. Routers and switches also include a robust stateful firewall and intrusion detection system supporting more than 100 signatures.

Cisco VPN Client

The Cisco VPN Client enables secure connectivity for remote access VPNs, including support for e-commerce, mobile user, and telecommuting applications. Compatible with Windows, Linux, Solaris, and Macintosh operating systems, the Cisco VPN Client provides a complete implementation of IPSec standards, including DES and Triple DES encryption, and authentication through digital certificates, one-time password tokens, and pre-shared keys.

Cisco SSL Acceleration Solutions

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

Content Access Management and Content Filtering

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

Cisco Intrusion Detection System (IDS)

The Cisco Intrusion Detection System is the industry's first real-time, network intrusion detection system that can protect the network perimeter, extranets, and the increasingly vulnerable internal network. The system uses sensors, which are high-speed network appliances that analyze individual packets to detect suspicious activity. If the data stream in a network exhibits unauthorized activity or a network attack, the sensors can detect the misuse in real time, forward alarms to an administrator, and remove the offender from the network.

Figure 2 Cisco VPN 3000 Series Concentrators

Cisco Secure Access Control Server (ACS)

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

Cisco VPN 3000 Series Concentrator

The Cisco VPN 3000 Series concentrators (Figure 2) are a family of remote access VPN platforms and client software that combine high availability, high performance, and scalability with the most advanced encryption and authentication techniques available. Use of the latest VPN technology vastly reduces communications expenditures. Cisco VPN 3000 Series concentrators are the only scalable platforms to offer field-swappable and customer-upgradeable components. These components, called Scalable Encryption Processing (SEP) modules, enable users to easily add capacity and throughput.

CiscoWorks VPN/Security Management Solution (VMS)

Cisco VMS provides an innovative approach to enterprise-wide infrastructure management. This enhanced solution delivers centralized operational network, security, and application management through the integration of network and security element management and monitoring. It contains costs, saves time, and eases the management of network-integrated security.

CiscoWorks Hosting Solution Engine

CiscoWorks Hosting Solution Engine (HSE) is a turnkey network management appliance that monitors, activates, and configures a variety of e-business services in Cisco powered data centers. CiscoWorks HSE provides services such as discovery, configuration, monitoring, and reporting for Cisco content switching and SSL solutions as well as data center devices such as Cisco PIX firewalls.

Cisco Security Consulting Services

Cisco Secure Consulting Services provide you with unparalleled network security expertise. Applying their backgrounds in critical information protection operations in military and commercial environments, Cisco security engineers develop Security Posture Assessments. These engagements include the comprehensive security analysis of large-scale, distributed client networks both externally, from the perspective of an outside hacker, and internally, from the perspective of a disgruntled employee or contractor. In a customer engagement, Cisco compiles, analyzes, and concisely presents its findings to the client, with operational-level recommendations to better secure the enterprise network and enable it to reach its full business potential. Cisco also offers Incident Control and Recovery services—a short-notice emergency deployment to customer sites when a network has suffered an attack. Cisco works with the client to restore the network to full operations as quickly as possible.

Cisco Managed Security Services Solutions

To enable service providers to take advantage of growing demand for secure managed services and VPN services, Cisco has a range of offerings designed for fast and cost-efficient service introduction. Managed VPN services based on IPSec, MPLS, or both permit service providers to augment existing connectivity services with remote access and site-to-site options and to offer value-added services for IP telephony, e-commerce, supply chain management, and content delivery. Managed security services, such as managed firewall and managed intrusion detection, represent value-added offerings that can be bundled with other services.

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

Cisco Security Ecosystem

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

Cisco Security Partner Program

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

Cisco Security Specialization

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

Cisco Security Certifications

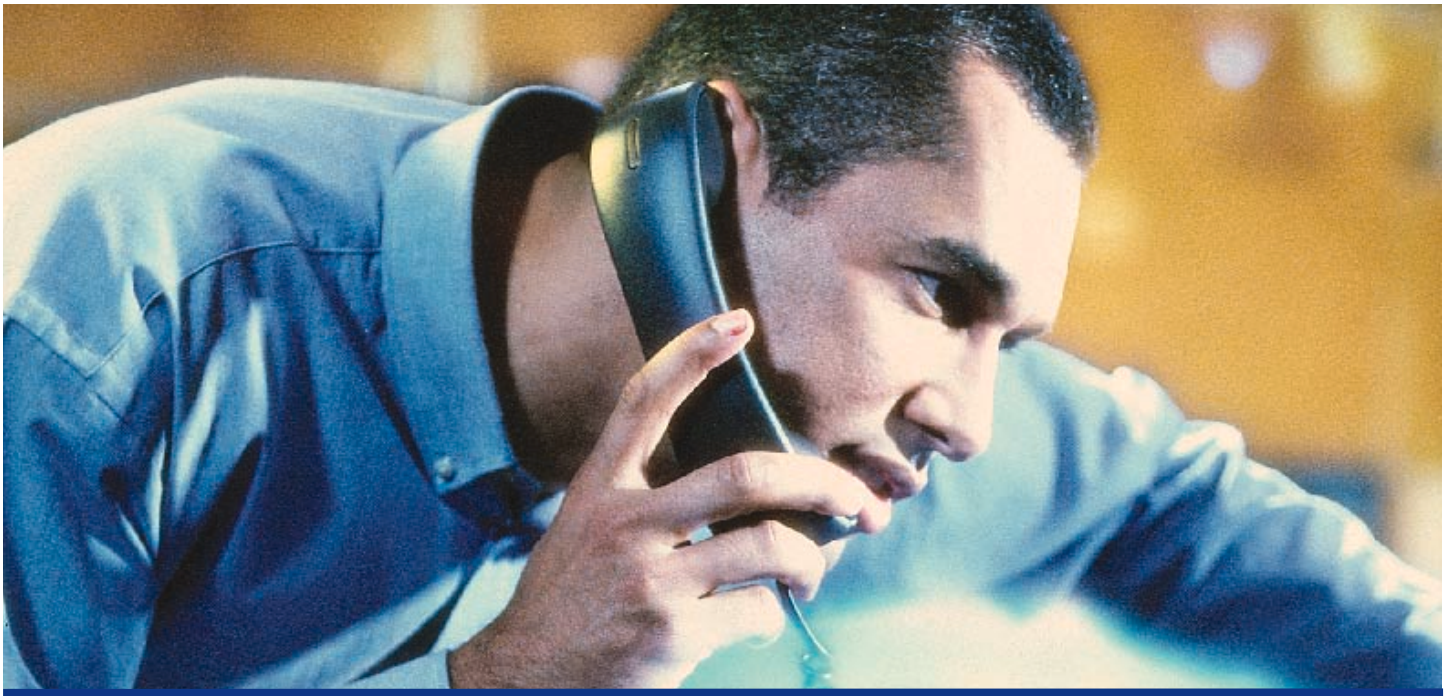
Cisco security certifications provide individuals and organizations with a metric to validate the skills and competencies of security professionals using best-of-class training and exams. The Cisco Certified Security Professional and the three focused certifications—Cisco VPN Specialist, Cisco Firewall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

Security Focused Authorized Cisco Learning Partners

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

The Cisco Powered Network Program

The service providers who display the Cisco Powered Network mark are telling you a lot about their services. They've earned the right to display this mark by maintaining high levels of network quality and by building their services with Cisco equipment—the same equipment on which virtually all Internet traffic travels today. The services provided, therefore, are reliable and secure.



Cisco Customer Services and Support

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

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

Optimization services are focused on personal, preventive, consultative support for IT organizations that anticipate rapid growth, struggle to close an expertise gap, or require maximum uptime and performance. Based on the Cisco Network Analysis Toolkit (NATkit), regular site visits, and continuous communication, your Advanced Services Engineer builds in-depth knowledge of your networking environment and business objectives.

Cisco: Building and Securing Your Network

The Cisco vision for security—empowering Cisco customers to safely improve their productivity —is what drives our commitment to your network security and to your long-term success. Today, Cisco delivers integrated security solutions that enable secure internetworking by embedding feature-rich security capabilities in Cisco infrastructure and providing a broad range of security-specific appliances, software, and consulting services. Cisco security solutions enable your business to cost-effectively take advantage of the Internet economy with the confidence you need to explore next-generation opportunities and the explosive growth they bring.

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.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

TS LW3818 11/02
Printed in the USA