

# Security Issues for Enterprise VPNs

## Cisco's Vision for Enterprise VPN security

Virtual private networks (VPNs) are, by definition, networks, and so require the end-to-end functionality, reliability, and scalability that any network requires. This functionality is delivered by the market-leading Cisco IOS® software and by VPN-ready Cisco platforms.

However, the challenge of using a shared service provider network to interconnect corporate sites (intranet VPNs), Access VPN, and suppliers and business partners (extranet VPNs) heightens the visibility of security issues. Enterprises need to be assured that their VPNs are secure from perpetrators observing or tampering with confidential data passing over the network, and from unauthorized users gaining access to network resources and proprietary information.

VPNs extend the corporation's network boundary and as such offer new business opportunities and support for many new networked applications, but this scenario increases still more the need for security. This document describes Cisco's enterprise VPN (E-VPN) security solution, which is a vital part of the Cisco five-point E-VPN strategy.

## Security Technologies Address Important E-VPN Issues

### Authenticating Users of Network Services

Accurately and positively identifying users of network services and resources is a critical component of any secure network, and is key to the successful deployment of VPNs. Cisco VPN solutions are built around authentication, authorization, and accounting (AAA) capabilities that provide the foundation to authenticate users, determine access levels, and archive all the necessary audit and accounting data. Such capabilities are paramount in dial access and extranet applications of VPNs.

### Providing Secure Network Perimeters

Controlling access to applications, services, and resources nonintrusively is one function of a properly designed network. The use of such network tools as access control lists, firewalls, content filtering tools (such as URL blockers), and virus scanning provides a method of securing the movement of data through the infrastructure.

### Transporting Confidential Data Over Shared Public Data Networks

As VPN services are deployed over shared network infrastructures, the tools used to ensure the authenticity and privacy of this data need to become more sophisticated, scalable, and manageable. Requirements for privacy range from mere separation of traffic with the use of tunnelling or encapsulation techniques, to sophisticated encryption as a method of guaranteeing confidentiality. A technology such as IPSec, with its authentication, key management, and encryption components, is, therefore, a very important enabler of VPNs.

Public

Copyright © 1999 Cisco Systems, Inc. All Rights Reserved.

Page 1 of 6

### **Monitoring and Responding to Network Intrusions and Suspicious Events**

Unfortunately, security looks the same whether it is working or not, unless you actively monitor and test for intrusions and vulnerabilities. Therefore, it is important to include vulnerability testing and intrusion detection capabilities in any VPN design.

### **Deploying Secure E-VPNs**

By delivering a comprehensive set of technologies, products, and services, Cisco can address all aspects of network security and help its customers to design, deploy, and manage successful VPNs. Recognizing that the unique security challenges posed by VPNs will require flexible solutions, Cisco offers products that include standalone software packages, network appliances, Cisco IOS software-based software solutions, and high-performance interface cards for Cisco hardware platforms. All these products work together to deliver comprehensive security solutions, but it is the successful partnerships with other technology vendors, systems integrators, service providers, and Cisco customers that allow Cisco to offer true end-to-end solutions.

## **Cisco's E-VPN Security Toolkit**

### **Authentication**

The use of protocols and technologies such as TACACS+, RADIUS, kerberos, one-time passwords, and Microsoft login enable today's network administrators to control access in a granular manner. For example, users logging in can be treated differently based on their IP address, domain membership, or location.

The CiscoSecure access control servers (ACSs) are used to determine who may access the network and what services they are authorized to use. An access control server can be used simultaneously with dialup access servers, routers, and firewalls.

In order to enable a more practical use of digital encryption, which relies on the accurate distribution of software "keys" for operation, Cisco has pioneered the use of X.509 digital certificates. Through the use of these certificates, which are essentially digital identity cards, Cisco VPNs can scale more efficiently and be managed more effectively. Cisco VPN products can use these digital certificates to confirm the identity of the end station dynamically, reducing the need for operator intervention.

### **Perimeter Security**


Cisco protects the network perimeter with firewalls that are high performance, flexible to deploy, and incorporate leading-edge firewall technology. Network administrators can choose to use a dedicated firewall appliance, an integrated firewall and router, or a combination of the solutions to meet the security needs of the network.

Cisco's PIX™ Firewall is a leading, dedicated security appliance that offers the industry's highest performance (according to KeyLabs' Firewall Shootout) with stateful packet filtering and security analysis. Using cut-through proxy, the PIX Firewall authenticates users against RADIUS or TACACS+ at very high speeds. NetPartner's WebSENSE Internet Access Management software is incorporated into the PIX Firewall to block outbound access to objectionable or unproductive content. With hardware-based encryption/acceleration and future support for standards-based IPSec, the PIX Firewall is an excellent solution for e-commerce over the Internet and for creating high-performance VPNs.

The Cisco IOS Firewall is a security-specific, value-add option to the most widely installed internetwork operating system in the world—the Cisco Internetwork Operating System (Cisco IOS software). The Cisco IOS Firewall enhances existing Cisco IOS software security capabilities, such as authentication, encryption, and fail-over, with state-of-the-art security. This security includes stateful, application-based filtering, defense against network attacks such as syn flooding, port scans, and packet injection, Java blocking, and VPNs based on Cisco IOS IPSec. Because it runs on a wide range of Cisco VPN-ready routers, the Cisco IOS Firewall Feature Set can be deployed extensively across a VPN, while the routers simultaneously provide multiprotocol routing, network services such as quality of service (QoS), plus the full breadth of standard Cisco software features.

### **Encryption**

IPSec is a framework of open standards for ensuring secure private communications over IP networks. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity, and authenticity of data communications across a public IP network. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.



Cisco offers IPSec in both Cisco IOS software and, in the future, on the PIX Firewall. Cisco is also working with industry partners to ensure that IPSec is available on a wide range of systems, including Windows NT, Windows 95, and UNIX.

#### **Intrusion Detection**

The Cisco NetRanger™ system is an enterprise-scale, real-time, intrusion detection system to detect, report, and terminate unauthorized activity throughout a network. The NetRanger system is the dynamic security component of Cisco's end-to-end security product line. With the NetRanger system, users can detect and terminate unauthorized network activity from both external and internal sources. Internal authorized users conducting unauthorized activity on the network—such as trying to transmit confidential documents over the Internet or illegally modifying network access privileges—can be detected in real time and stopped. An external intruder trying to break into the network could be handled in the same manner.

#### **Security Management**

A critical element of a comprehensive network security solution is centralized, coordinated security management. Cisco is addressing this need with Cisco Security Manager, a security policy management system for Cisco security technologies and network devices. In its upcoming V1.0 release, Security Manager will enable an administrator to define, enforce, and audit security policies for distributed Cisco PIX firewalls.

As the management cornerstone of Cisco's end-to-end security product line, Cisco Security Manager will be extended in the future to support Cisco's comprehensive security solutions, including Cisco IOS Firewall, IPSec encryption, user identity/authentication, intrusion detection, and vulnerability scanning technologies. These continuing efforts will result in a centralized, coordinated security management system for the enterprise, including support for VPNs.

### **Cisco's E-VPN Security Strategy**

#### **Providing End-to-End Security Capability**

Cisco is dedicated to providing security solutions that work together with other networking technologies in order to provide reliable, scalable secure networks. These solutions must consider client and server applications and services, as well as infrastructure capabilities. By delivering a comprehensive set of standards-based security products, technologies, and services that all work together, and by linking these security deliverables with technologies and products from industry partners, Cisco will remain the leader in network security solutions.

#### **Providing a Simple Migration Path to VPNs**

Cisco's VPN security solution can often be deployed using installed "VPN-ready" Cisco platforms. In this way, Cisco provides an easy, cost-effective migration path to virtual private networking, which extends and complements an organization's existing infrastructure. Cisco has installed nearly 10 million VPN-ready router ports, which can be enabled with the VPN capabilities of Cisco IOS software.

#### **Including Clients, Infrastructure, Hosts, and Applications**

Although a secure network infrastructure contributes to the value of a VPN, it is through the inclusion of all network components that a VPN reaches its greatest potential. By extending the VPN to include partner networks, remote clients, hosts, and applications, the VPN provides increased efficiency while reducing communications costs.

Through partnerships with such companies as Microsoft, Hewlett-Packard, and others, Cisco will deliver industry-standard and interoperable VPN solutions to operating systems and applications. These solutions will deliver VPN client capability and integration with such virtual private dial solutions as Layer 2 forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP), allowing service providers to participate more completely in VPN service offerings.

#### **Architecture-Based Solutions**

In order to address effectively the networking needs of customers, Cisco is developing its products and technologies to fit within an architectural model of efficiency. This model defines the critical functions that the VPN of the future must provide:

- Positively and granularly identify users, hosts, applications, and more
- Understand and act on data in context according to defined rules; this scenario might include denying access to, encrypting, or changing the priority of selected data, or recognizing and reporting anomalies or intrusions
- Configure, manage, audit, and centrally control the configuration of the network based on the relationship between these items

The products, technologies, and services Cisco delivers include dedicated appliances, capabilities integrated within Cisco IOS software, and high-performance interface cards for Cisco hardware platforms.

## **Cisco's E-VPN Security Roadmap**

Cisco has a comprehensive roadmap, which extends the four key areas of VPN security discussed in this paper.

### **Authentication**

More efficient and scalable methods of identifying network users, applications, and resources must be developed in order to handle the growth in VPNs and networks in general. Forward-looking network architects are envisioning a future in which authentication can be scaled to address orders of magnitude more users, and deliver an even more granular and secure set of solutions. Emerging technologies such as digital certificates and directory services enable a more scalable, flexible, and secure infrastructure for the authentication of network users.

Digital certificates are currently used to authenticate the encryption keys of IPSec end stations. In the future, these certificates are expected to carry more information about network users. The enhancement of these capabilities is being pursued under the Public Key Infrastructure (PKI) initiative in the Internet Engineering Task Force (IETF). Cisco is working with such industry leaders as VeriSign, Entrust, Microsoft, and Netscape to help in the development of these standards. In addition, digital certificates will be supported in the Cisco Security Manager.

It is also expected that network directory technologies and products such as Lightweight Directory Access Protocol (LDAP), Novell's NetWare Directory Services (NDS), and Microsoft's Active Directory and Directory-Enabled Network (DEN) initiatives will also play a large role in managing authentication and security policy information. These directories are a logical place to store user profiles, and will make the storage and management of digital certificates more efficient. Cisco continues to work with such partners as Microsoft and Novell to develop these directory technologies.

### **Perimeter Security**

As a leader in Internet security solutions, Cisco is at the forefront of access control and firewall technology development. Issues of price, performance, integration, and scalability are major concerns of today's VPN architects, and Cisco will continue to deliver leading-edge product solutions to customers.


Where it makes sense to deploy standalone solutions for operational reasons or otherwise, the Cisco PIX Firewall continues to evolve to meet the needs of customers. Planned enhancements to the PIX platform will offer increased performance, lower cost of ownership, and increased capabilities.

The Cisco IOS Firewall feature set will be ported to additional Cisco platforms. For example, it is now supported on Cisco 7200 Series routers. These scalability improvements, coupled with enhancements that address authentication, reporting, and flexible alerts, will continue to make the Cisco IOS Firewall feature set a very important part of the VPN infrastructure. These firewall solutions are complementary and are part of a complete security solution.

### **Encryption**

With VPNs gaining in popularity, the deployment of IPSec-based privacy and authenticity solutions is expected to grow significantly over the next several years. In order to accommodate this growth in VPNs, new solutions that provide increased encryption performance and scalability are required. IPSec capabilities in Cisco IOS software are scheduled to be augmented with high-performance encryption hardware adapters in mid-1999, beginning with the Cisco 7200 and 7500. These hardware adapters will deliver the ability to support large numbers of encryption sessions and provide higher-speed encryption data rates. Coupled with IPSec client software for workstations or IPSec-enabled access routers, these hardware accelerators will allow Cisco devices to serve as efficient encryption gateways or aggregation points in distributed VPN architectures.

In addition, as hackers and technology increase in sophistication, customers continue to demand more sophisticated and secure encryption technology for their VPNs. Although encryption based on 40- and 56-bit key lengths is generally accepted as sufficient today, tomorrow's VPNs will rely on longer keys and stronger encryption algorithms. Cisco will be ready in early 1999 with support for 3-Data Encryption Standard (DES), and, with the flexibility of Cisco IOS software, has developed Cisco VPN products with the capability to support future encryption algorithms.



## **Intrusion Detection**

As the threats to networks increase in sophistication and complexity, the ability to detect and react to these threats becomes critical. With the Cisco NetRanger intrusion detection products, Cisco has increased the ability of VPNs to operate securely. One important feature of the NetRanger system is its easily upgradable threat database. SMARTnet™ customers will be provided with updates to the threat database that include the latest threat profiles that the Cisco engineering labs have uncovered.

In order to increase the value and availability of intrusion detection in the network infrastructure, Cisco plans to introduce intrusion detection capability as an optional integrated feature in selected Cisco IOS software images. Additional efforts will focus on the integration of intrusion detection systems for switched internetworks and the development of high-performance hardware products.

The Cisco NetRanger system will also be enhanced with additional reporting tools that will allow the intrusion detection tools to more fully integrate with VPN management tools.

## **Management**

An extension to the enterprise network, VPNs must fit seamlessly into the overall enterprise management architecture for the current infrastructure. Enterprise customers require that the existing enterprise management environment be extended and enhanced with new VPN management capabilities that provide the administrator with control, security, and visibility from the wiring closet to the campus backbone, through the wide area and out to the VPN end user.

To meet these business requirements, Cisco is delivering a solution portfolio that meets the needs for comprehensive management of VPNs. Through Cisco Security Manager, Cisco will deliver a comprehensive, policy-based security management system that extends the existing management framework with additional capabilities to manage the unique aspects of the E-VPN. Security Manager, which initially focuses on the management of the PIX Firewall, will be extended to control Cisco's end-to-end security solutions (as mentioned above).

Cisco will also introduce ACL Manager, which provides administrators with an easy-to-use, Web-based application for the design and implementation of Cisco IOS services configured through access list statements. With ACL Manager, administrators can easily create, edit, archive, and delete ACLs for devices throughout the enterprise network.

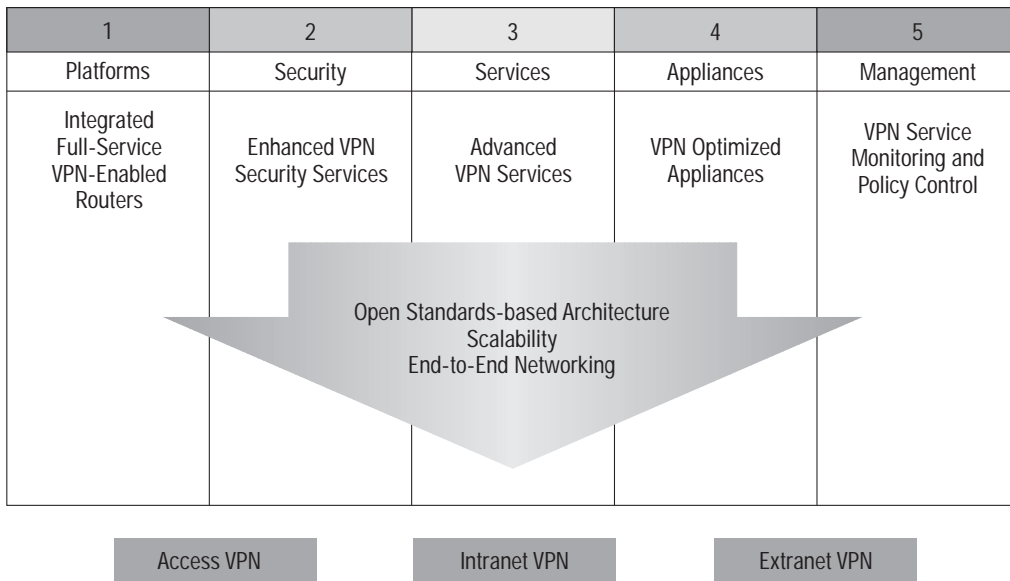
Both Security Manager and ACL Manager will be integrated into the CiscoWorks 2000 family of network management products. By consolidating configuration, reporting, and event information into CiscoWorks 2000 Resource Manager Essentials, Cisco will enable an administrator to view critical security and network management information from a single console.

## **Summary**

This document has shown that E-VPNs extend private enterprise networks but have an even greater need for security. Cisco's comprehensive security product suite, and VPN-enabled router family meet this need. They provide a smooth migration to a secure E-VPN environment, and integrate existing enterprise LANs and WANs with the new VPN infrastructure.

Going forward Cisco's five-point E-VPN strategy will build on the currently offered tool kit of E-VPN platforms, security, services, appliances, and management solutions, and offer greater functionality and performance in an open, standards-based approach.

Figure 1 Cisco's Five-point Enterprise VPN Strategy



**Corporate Headquarters**

Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
<http://www.cisco.com>  
 Tel: 408 526-4000  
 800 553-NETS (6387)  
 Fax: 408 526-4100

**European Headquarters**

Cisco Systems Europe s.a.r.l.  
 Parc Evolic, Batiment L1/L2  
 16 Avenue du Quebec  
 Villebon, BP 706  
 91961 Courtaboeuf Cedex  
 France  
<http://www-europe.cisco.com>  
 Tel: 33 1 69 18 61 00  
 Fax: 33 1 69 28 83 26

**Americas Headquarters**

Cisco Systems, Inc.  
 170 West Tasman Drive  
 San Jose, CA 95134-1706  
 USA  
<http://www.cisco.com>  
 Tel: 408 526-7660  
 Fax: 408 527-0883

**Asia Headquarters**

Nihon Cisco Systems K.K.  
 Fuji Building, 9th Floor  
 3-2-3 Marunouchi  
 Chiyoda-ku, Tokyo 100  
 Japan  
<http://www.cisco.com>  
 Tel: 81 3 5219 6250  
 Fax: 81 3 5219 6001

**Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at <http://www.cisco.com/offices>.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • 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 • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela