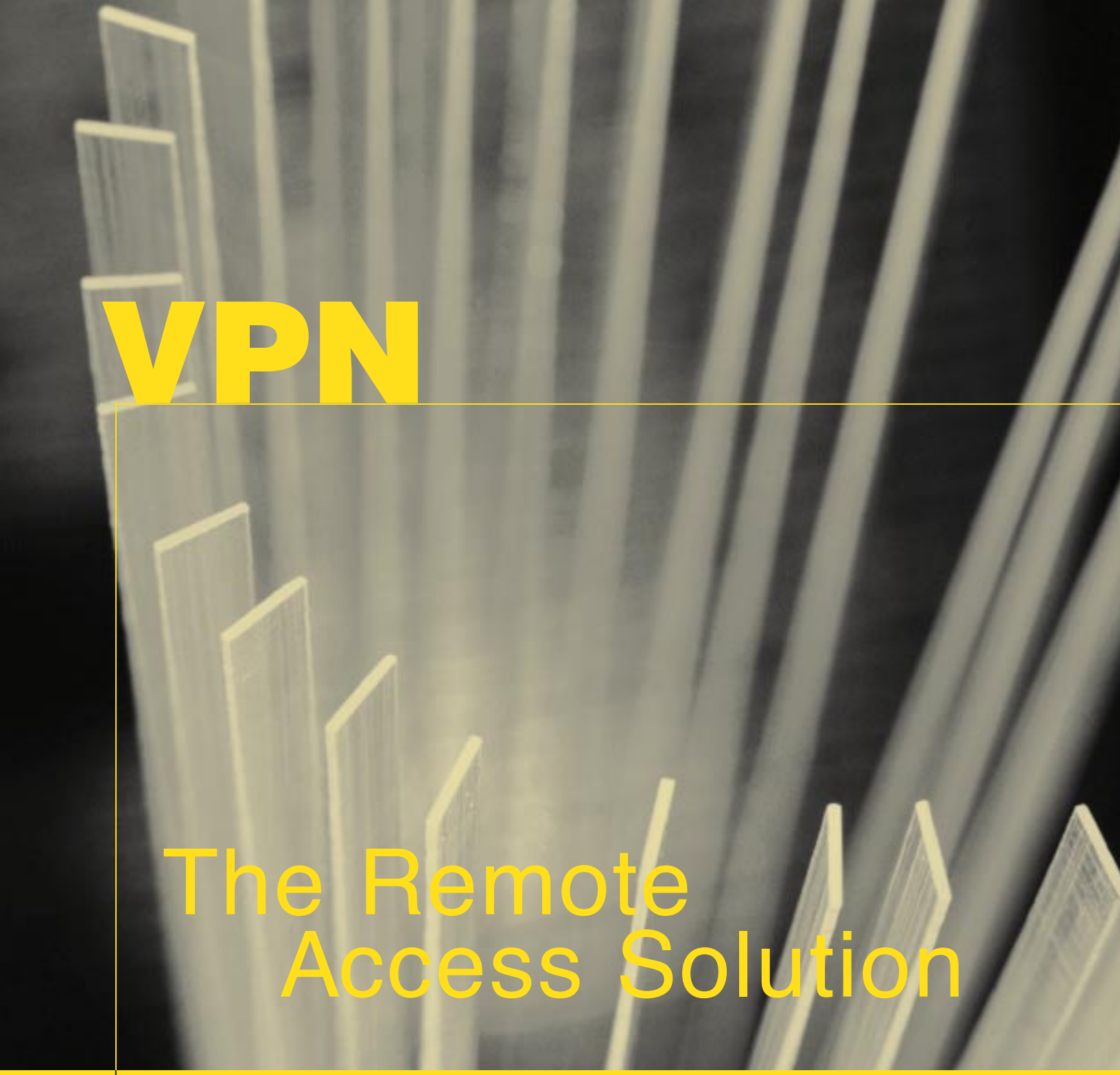


VPN

The Remote Access Solution

A Comprehensive Guide to Evaluating:

- Security
- Administration
- Implementation

Compatible Systems

the virtual leader

www.compatible.com

VPN:

The Remote Access Solution

Contents

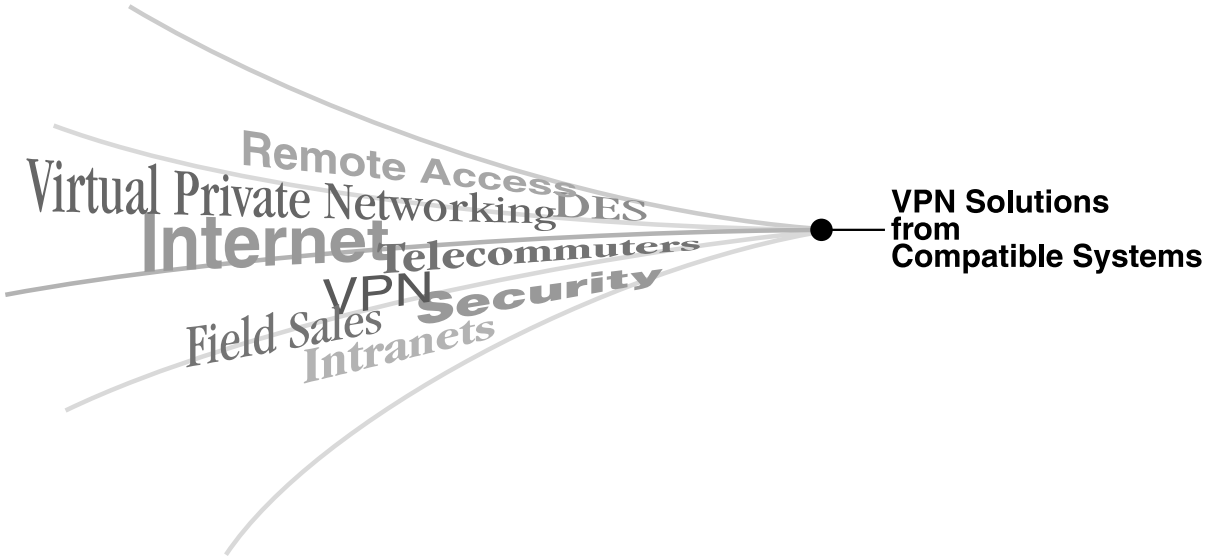
Compatible Systems

the virtual leader

The Promise of Virtual Private Networking

By now you know just about all there is to know about the Internet, right? You may already be maintaining e-mail servers, supporting e-mail lists, and managing internal and external web servers. But did you know you can give your remote users, telecommuters, and branch offices access to your private corporate network over the Internet? Do you know the real security issues involved? Are you writing off the Internet as a WAN backbone because it only supports TCP/IP? If you're not looking to the Internet as a vital part of your LAN/WAN infrastructure, you're missing out on one of the greatest opportunities to emerge from the networking world in years. Virtual Private Networking (VPN) technology is being implemented by leading-edge companies today, and the pace of implementation is accelerating.

VPN technology adds a new dimension of value to your Internet connection by allowing you to create highly secure point-to-point "tunnels" through the public Internet. At their end points, tunnels behave just like traditional dial-up or leased-line private network connections. Tunnels can be "nailed up," or created on demand and then torn down automatically when a session ends. Using encryption and packet authentication, you can protect both the data and session against intruders from the Internet. The result is a two-for-one use of your Internet connection. Not only can you employ the Net for marketing, research, and e-mail; you can also use it just as you would utilize an expensive, distance-based phone line or leased line. The result is lower administration overhead and lower line costs, along with greater security (yes, it's true, and we'll show you why), better access control, and easier access provision for your users and your LAN. That, in a nutshell, is the goal of VPN technology.



What Is VPN?

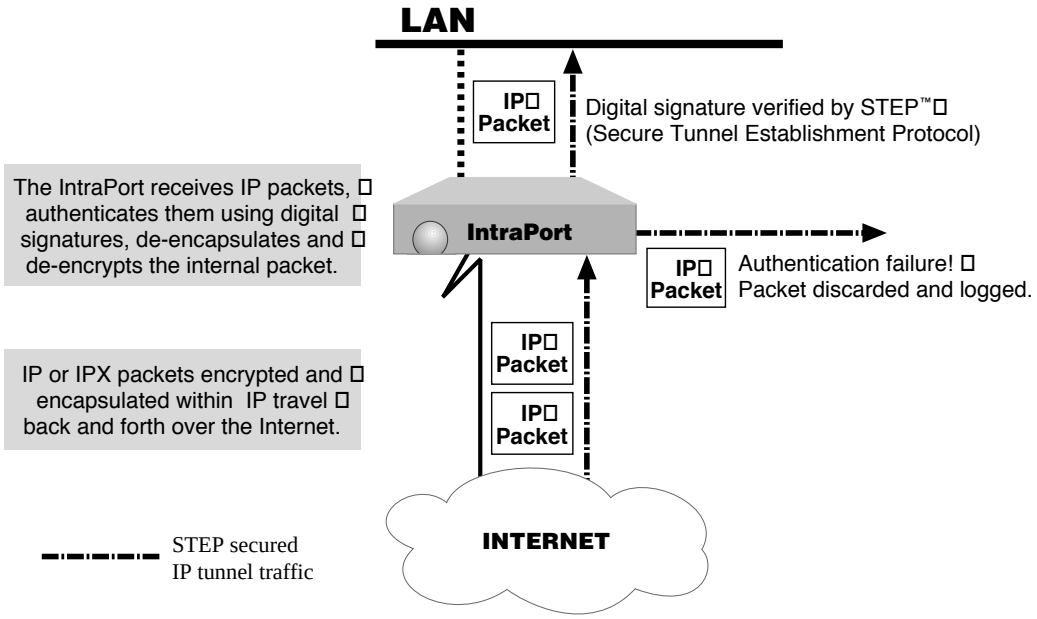
One of the difficulties of getting a handle on the various VPN alternatives is that there is no official set of guidelines a product must meet to call itself "VPN." But according to data communications analysts and network managers, a product must integrate these functions in order to call itself a true VPN solution.

Authentication: The VPN product must authenticate an incoming connection to confirm that the access is in fact legitimate. This is usually done through a series of shared "secrets." Upon completion of the authentication process, a tunnel is opened between the VPN product and the other end of the connection. The other end can be client software running on a PC, or a hardware-based device. More advanced VPN products authenticate the connection on a packet-by-packet basis for even greater end-to-end security.

Encapsulation: Once a tunnel is open, data packets must be encapsulated into other TCP/IP packets for transmission across the public Internet. Encapsulation allows private network packets such as IPX or AppleTalk to cross an IP network. In addition, products based on the IPSec standard encapsulate IP in order to provide packet-by-packet authentication. IPSec also helps make VPN solutions compatible with network firewall systems.

Encryption: Prior to transmission over the network, packets are scrambled to prevent theft by network "sniffers." There are dozens of "flavors" of encryption, and most VPN products support multiple options, allowing network managers to decide what level of protection their data requires.

Policy-Based Filtering: Although not strictly required for a product to be called a VPN solution, policy-based filtering allows fine-grained access control to network resources, based on the authenticated identity of the person or network address at the other end of the tunnel.



The Compatible Systems IntraPort™ provides full data and connection security through encryption, authentication, encapsulation and filtering.

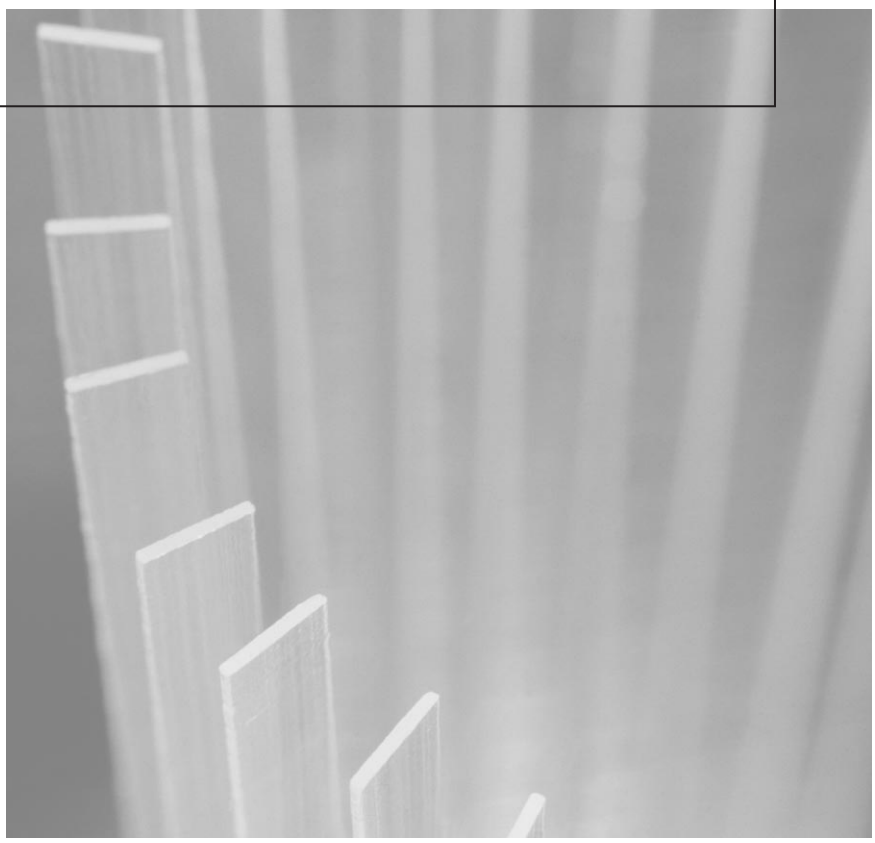
VPN solutions come in four types. The best one for you will depend on your application, your budget, and your technical expertise.

Hardware-based VPN: These products are generally stand-alone devices with a processor or processors dedicated solely to VPN functions such as authentication, encapsulation, encryption and filtering. Hardware-based products generally offer the greatest performance because they are designed exclusively for the tasks associated with VPN applications. Standalone hardware products include Virtual Access Servers and VPN-capable routers.

Software-based VPN: Many server platforms offer or plan to offer VPN modules to accompany existing remote access or routing modules. While these products provide basic VPN capabilities, they are severely limited in terms of performance because the processor must perform many functions in addition to VPN.

Firewall-based VPN: These are also software-based VPN products, except that the software modules are added onto a firewall package. Many firewall vendors have added IPSec (a VPN standard) support to their products in order to allow firewalls from different vendors to communicate with each other.

VPN Services from Internet Service Providers: Some Internet Service Providers (ISPs) provide "managed" VPN services. This is typically done using hardware-based or firewall-based VPN products which are owned and operated by the ISP. The biggest consideration with VPN services is that your company's security infrastructure will not be directly under your control.



How Can My Company Use VPN?

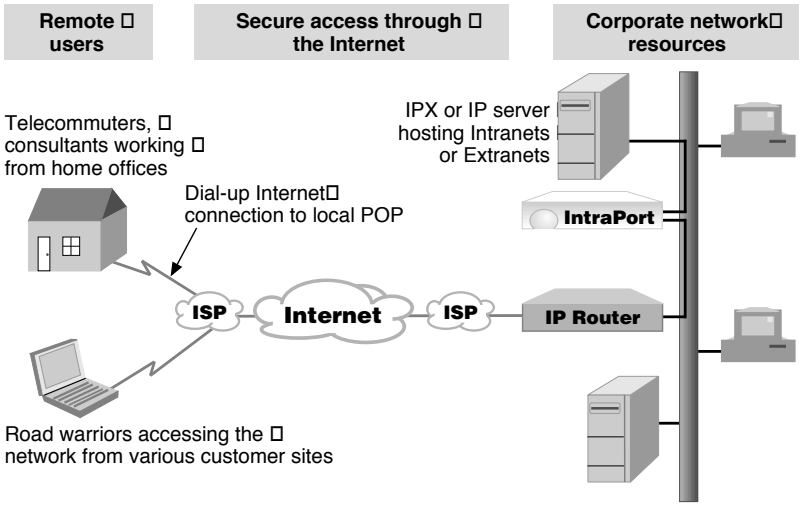
Virtual Private Networking can be used in almost any WAN application. VPN solutions provide secure network access for off-site users, including...

Road Warriors: You may have thought road warriors were just a figment of a science fiction moviemaker's dream, but anyone who works in today's corporate world knows how important it is to stay in touch when you're out of the office. Road warriors equip themselves with laptops and head out all over the world in search of sales or to provide customer services. For them, VPN means a simpler, more efficient and inexpensive way to connect to home base. All they need is a local access number for their Internet Service Provider, and away they go.

Telecommuters: Companies are turning to telecommuting for a variety of reasons. Employee flexibility, environmental concerns, and greater use of outside contractors are just a few of the forces driving the telecommuting revolution. These users often spend hours on the central network, paying distance-based phone charges the entire time. VPN simplifies their connection process and slashes the price of access.

Intranets and Extranets: The corporate network is constantly changing. Groupware applications and web-based intranets are vital players in many multi-vendor or consulting projects. A VPN solution enables companies to link the home office, consultants, suppliers, and customers. VPN gives everyone an easy way to work together.

Branch Office Personnel: LAN-to-LAN connectivity provides two-way access between a remote office LAN and a home office LAN. VPN is a secure and cost-effective way of providing this access, even in situations where it might have been cost-prohibitive using traditional WAN transport methods.



Virtual Private Networking solutions such as the Compatible Systems IntraPort provide full connectivity for access to extranets, intranets and other network resources to remote users and telecommuters.

The VPN Advantage

VPN technology allows companies to reduce remote access costs by removing the remote connection from the phone company and "outsourcing" it to the Internet. A remote user connects to corporate network resources by making a local phone call to an Internet Service Provider. A LAN-to-LAN connection is made over leased lines to ISPs. Outsourcing is a proven winner in many corporate Information Technology applications. And nowhere are the benefits of outsourcing more valuable than in remote access.

What does the VPN advantage mean to you?

Reduced administration overhead. Traditional remote access is a serious time drain, with modems and ports to configure, phone line problems to diagnose, and impatient users to support. Virtual Network Access allows you to "outsource" a majority of these configuration and support tasks to an Internet Service Provider.

No long-distance charges. Traditional remote access systems require a separate phone line for each user. Telecommuters and roving field users who must connect over long distances at peak periods can run up serious telco charges. With a VPN-based remote access system, users make a local call to an Internet Service Provider and generally pay a flat monthly usage fee, no matter how much time they spend on line. Savings on telco charges alone can add up to more than 60%.

	IntraPort	Traditional RAS
Line Costs for 50 users*	$35,970	$126,000
Administration of RAS connections**	$24,000	$108,000
Hardware costs***	$11,400	$13,500
Total Cost (capital equipment plus one year's line cost)	$71,370	$247,500

* One year's line costs includes monthly phone line + usage charges and Internet account for each user
** Administration charges based on figures from "The Real Costs of Remote Access" by Infonetics Research, Inc.
*** Assuming 16 ports/tunnel connections for 50 users (1:3 port/user ratio)

Under Lock and Key

Network security is the most important – and least understood – element of Virtual Private Networking. If you follow the lead of security professionals, who never rely on obscurity to protect sensitive corporate data, you'll find that, in fact, authenticated and encrypted VPN-based connections deliver much greater security and protection than traditional password-protected remote access systems.

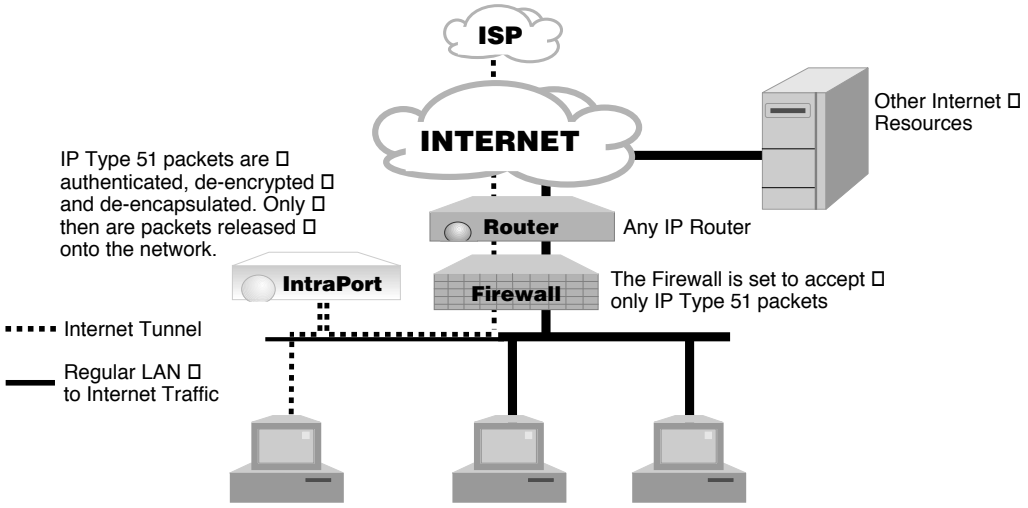
Think about it. Using traditional remote access, you can have dozens – even hundreds – of individual access ports into your network. Remote access servers generally offer little more than password protection. There is often no data encryption or filtering protection at all. Should an unauthorized person gain access to a port which isn't password protected, or discover a password, your network is at risk.

How do VPN devices help you protect your network?

Location, Location, Location: VPN servers attach directly to your central site network, behind the corporate firewall. With IPSec, a part of the TCP/IP standard, you can allow VPN traffic to penetrate the firewall via a single opening designed specifically for encapsulated IP. Then, when it reaches the VPN server, you can authenticate, de-encrypt and provide filter-limited access to services on the private LAN. This means that by the time the data reaches its final destination it has passed through a single controllable entry point, and undergone multiple security checks.

Cryptography, Another Layer of vbnkfgsklmc: In order to protect your data from eavesdropping as it travels over the public Internet, VPN products use encryption. The Data Encryption Standard (DES) provides encryption strong enough to be trusted by the military and other security-conscious governmental agencies. Cryptography also plays a role in the strongest authentication systems, which use MD5-based algorithms to create digital signatures for packet-by-packet verification of the identity of the data's originator.

Policy-Based Filtering – Your Greatest Safeguard: More than 80% of all network security breaches are inside jobs, according to computer security analysts. The password-based protections of traditional remote access systems are among the most insecure barriers in IT. A single compromised password can lead to havoc on your network. VPN solutions use packet filtering to dramatically heighten the controls you can place on remote users. With filters you can control access to specific sites or services on a user-by-user or group-by-group basis. Filtering lets you make sure that everybody can get the information they need – and nothing more.



Behind the Firewall: The IntraPort works with a firewall system to provide an additional layer of security.

The VPN Self-Test

Yes ☐ No ☐ **1.** Does your business rely on sales people who work in the field and require timely and accurate information from a central site?

Yes ☐ No ☐ **2.** Do your sales force-to-headquarters long-distance charges make up a significant portion of your monthly telco bill?

Yes ☐ No ☐ **3.** Do you have dedicated Internet access at your company's central network?

4. Does your company use telecommuters...

Yes ☐ No ☐ • on a part-time basis?

Yes ☐ No ☐ • on a permanent basis?

Yes ☐ No ☐ **5.** Do you have MIS staff dedicated to providing remote access and supporting remote access users?

6. Would you like to extend remote access to more users but are constrained by...

Yes ☐ No ☐ • number of ports on your existing remote access server?

Yes ☐ No ☐ • cost of hardware?

Yes ☐ No ☐ • cost of long-distance required by remote users?

Yes ☐ No ☐ • administration time required to support users?

Yes ☐ No ☐ **7.** Does your company have international offices that need cost-effective access to the central headquarters' computing resources?

Answers & Scoring

On questions 1, 2, 4, 5 and 6, give yourself 5 points for each "yes."

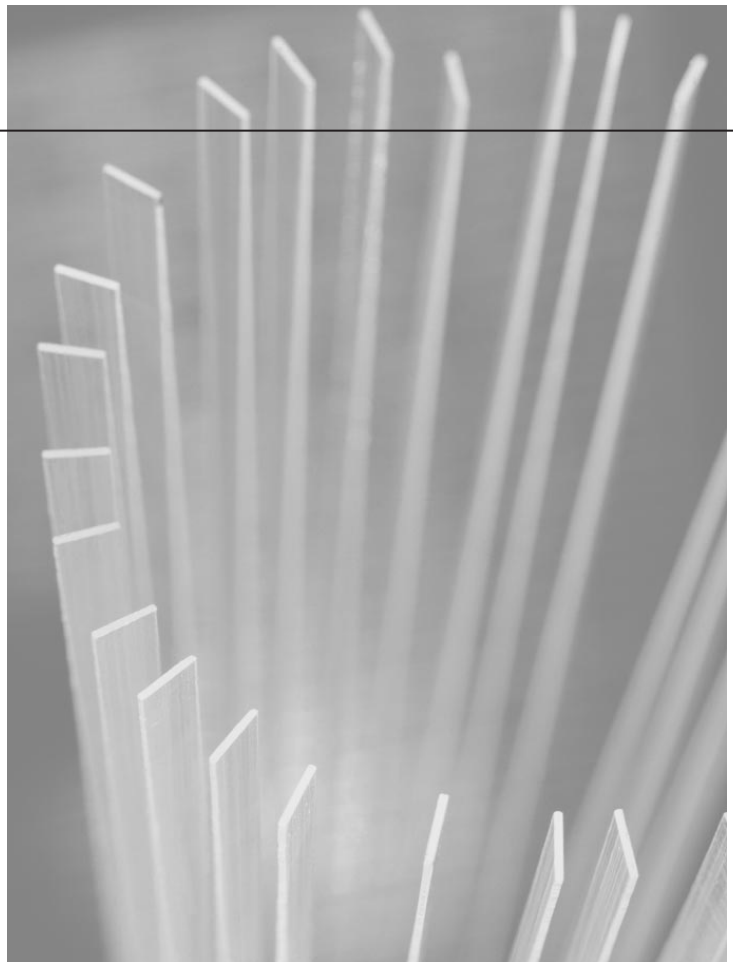
On questions 3 and 7, give yourself 10 points for each "yes."

Rate your need for VPN

40–50 points: Run, don't walk, to get a VPN access server installed on your system. You need it right now.

30–39 points: You should make VPN your next access server. If you're already providing remote access, it's time to bring the future to your network.

15–29 points: VPN is the simplest, most effective remote access technology you can buy. You know your employees, consultants, and partners need access. Give it to them with VPN.



Your VPN Checklist

While your VPN configuration and needs depend greatly on your specific application, there are a few guidelines you should always follow.

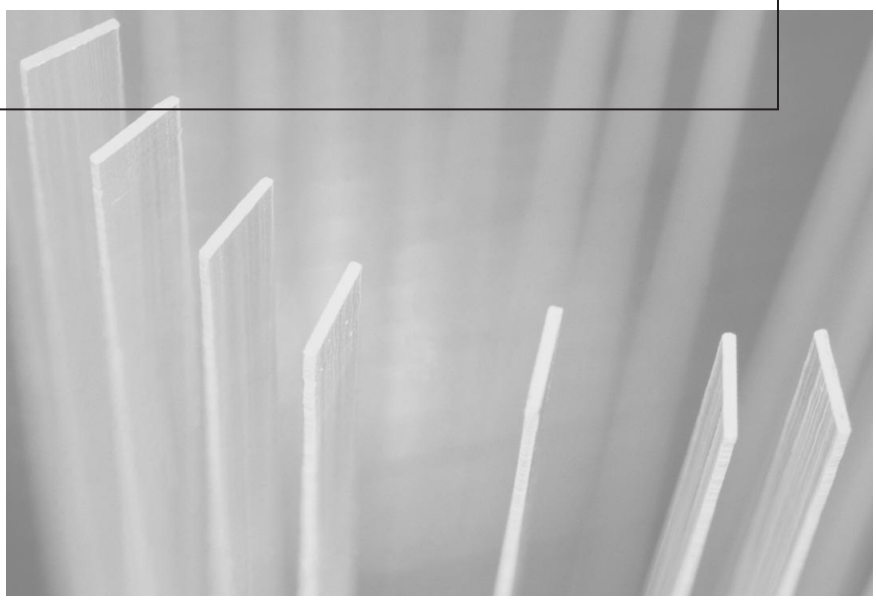
☑ **Choose an ISP with nationwide coverage.** A national ISP – or a regional one that provides access points nationwide – will allow you to take full advantage of local calling for remote access connection. You should also ask potential ISPs about technical support policies, internal network benchmarks and optional services such as bandwidth reservation.

☑ **Use filtering.** More than 80% of all network security breaches are caused by unauthorized access that proper filtering configuration would have prevented.

☑ **Assess the criticality of the data to travel the VPN link, configure for performance.** Know what kind of traffic your remote users will generate and ask your ISP for their recommendations in optimizing the network link. Set internal policies regarding the transfer of mission-critical or highly confidential data.

☑ **Integrate VPN into existing remote access systems.** VPN is the remote access technology of the future. If you already provide remote access, add VPN on a departmental basis. The experience you gain is invaluable.

☑ **Choose a VAR or Provider with full support capabilities.** Even an easy-to-use networking solution can be tough to configure and manage. Look for help from a reputable networking VAR in your area or from the service arm of your ISP.



Compatible Systems: The Virtual Leader

Tunneling has been a vital part of Compatible Systems internetworking products for almost 10 years, so we're no stranger to the world of VPN. We've used our extensive knowledge of routing and tunneling to produce the IntraPort VPN Access Server.

The IntraPort lets you run IP and IPX data over the Internet, cutting hardware, telco, and administrative costs by "outsourcing" these expenses to Internet Service Providers. The IntraPort utilizes MD5-based authentication and conforms to the IPSec standard. Two levels of encryption, including DES (Data Encryption Standard) technology, make sure your data is secure.

The IntraPort Client Software runs on Windows 95 and Windows NT (Q1 98) machines. Network administrators can configure client software at corporate headquarters and distribute it easily over the Internet or on disk to remote users. The IntraPort client may be used over PPP dial-up connections or Internet-attached Ethernet connections. The IntraPort VPN Access Server has the power you need to change the way you look at remote access.

For LAN-to-LAN applications, Compatible Systems delivers a full line of VPN Routers. These routers support TCP/IP, IPX and AppleTalk and include all the security features of the IntraPort. The routers operate at line speeds from 28.8 Kbps to full T1/E1.

Find out about the future of connectivity today. Contact your Compatible Systems sales representative at **800-356-0283.**

VPN Glossary

Authentication – A process that requires users to securely identify themselves through the use of passwords or, in the most secure VPN protocols, encrypted "secrets" prior to the establishment of a VPN connection.

Client – A computer or software program that requests a service of another computer system or processor (a "server"). For example, a workstation running a VPN client can create a network connection through a VPN server.

Digital Signature – A coded message added to a document or data that guarantees the identity of the sender. Used during authentication of some VPN links.

Encryption – The "scrambling" of data to prevent anyone other than the intended recipient from reading the information. Encryption protects data during actual transmission across the public network.

Firewall – A collection of components that supervises all traffic in and out of a network, permitting only traffic which is authorized by local security policy to pass.

IPSec – An IP security protocol that provides for encapsulation of IP packets into Type 51 IP, allowing firewalls to recognize and admit encapsulated, encrypted data.

Policy-Based Filtering – A process that determines who is given access to what services after an authenticated VPN link has been established.

Server – A computer or software that provides resources, such as files or other information, to client software running on other computers.

TCP/IP (Transmission Control Protocol/ Internet Protocol) – The U.S. Department of Defense developed TCP/IP in the 1970s to support the construction of world-wide internetworks. Today, millions of users are connected to the Internet with TCP/IP software.

Tunnel – A secured, private "path" connecting two points through a public network.

VPN (Virtual Private Network) – An Internet-based system for information communication and enterprise interaction. A VPN uses the Internet for network connections between people and information sites. However, it includes stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system.

Compatible Systems

the virtual leader

P.O. Box 17220 · Boulder, CO 80308
303/444-9532 · fax 303/444-9595
info@compatible.com · www.compatible.com