Virtual Private Networks

A Partnership Between Service Providers and Network Managers

Courtesy of:

VPNet®

INFONETICS RESEARCH

The Networking Information Source

255 West Julian Street, Suite 402
San Jose, California 95110-2406
Tel: 408-298-7999 Fax: 408-298-2073
www.infonetics.com

Copyright © 1997 by Infonetics Research, Inc.

Entire contents copyrighted by Infonetics Research, Inc. Unauthorized redistribution, electronic or otherwise, without prior written approval of Infonetics Research, Inc., is prohibited by law. Requests for permission to copy or distribute should be made to Infonetics Research, Inc.

Contents

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

Exhibits

II. Why Virtual Private Networks?

III. VPN Technology Choices

IV. VPN Implementation Issues

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

I. Conclusions

A. The VPN Opportunity

Virtual private networks (VPNs) provide excellent opportunities for both enterprises and service providers.

Enterprise network managers can provide reliable corporate dial-up access for the expanding numbers of road warriors, telecommuters, and day-extenders, and save costs and staff resources in the process.

Network managers can also replace leased line connections to remote offices and connect hitherto unconnected remote offices to the corporate network, and again save costs and staff resources in the process.

- Savings are typically 20–40% for site-to-site networks domestically, and more internationally
- Savings can be 60–80% for road warrior, telecommuter access

Internet service providers (ISPs, which offer Internet access) and network service providers (NSPs, which offer dedicated IP bandwidth on private backbones, in addition to Internet access)—together referred to as "service providers" or "SPs" in this paper—have a potentially huge revenue generator and service differentiator with VPNs. Listed in increasing value (and margin) for SPs, these are some of the new service revenue opportunities VPNs create:

1. Sell basic Internet access and bandwidth; the enterprise customer handles all VPN products and operations
2. Sell business-quality Internet or IP network services; the enterprise customer handles all VPN products and operations
3. Sell compulsory VPNs embedded in POP equipment
4. Offer VPN hardware and software bundled with VPN bandwidth and services
5. Design the customer's VPN solution
6. Operate the total VPN solution for the customer, including design, equipment installation and service, and helpdesk support (100% outsource)

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

B. VPN Technologies

Implementing VPNs across the Internet and other IP-based public networks depends on vendors, service providers, and other interested parties agreeing on standards through the Internet Engineering Task Force (IETF). The most popular emerging VPN standards are PPTP, L2TP, and IPSec.

- PPTP is a point-to-point tunneling mechanism originally created to support packet tunneling in Ascend's remote access server hardware and Microsoft's NT software.
- The backers of PPTP combined efforts with Cisco and its L2F protocol to produce a hybrid layer 2 tunneling protocol called L2TP (Layer 2 Tunneling Protocol).
- IPSec is a standard created to add security to TCP/IP networking; it is a collection of security measures that address data privacy, integrity, authentication, and key management, in addition to tunneling. It has been strongly supported by a user group consisting of manufacturers and suppliers.

Security is a critical component of VPNs, especially those implemented over the Internet. Encryption delivers the "private" in virtual private networking, and a basic aspect of encryption is the management of encrypted keys.

Neither PPTP nor L2TP specify inherent encryption or key management mechanisms in their published specifications. The current (July 1997) L2TP draft standard recommends that IPSec be used for encryption and key management in IP environments, and the next draft of the PPTP standard may do the same.

For these reasons, IPSec is the best VPN solution for IP environments, as it includes strong security measures, notably encryption, authentication, and key management, in its standards set. PPTP and L2TP are more suitable for multiprotocol non-IP environments.

Because of the computational power required to implement VPNs, hardware-based VPN products deliver the best performance. They also offer tighter physical and logical security. Software-based solutions are best-suited for lower-volume connections for small and medium businesses that have lower security requirements.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

II. Why Virtual Private Networks?

A. VPNs—A New Technology

Just as with most new technologies, there's confusion in the VPN marketplace:

- Network managers believe that VPNs can reduce costs for leased lines and remote access, but they also know that the Internet is not secure
- Major service providers are sure they will offer VPNs, but they're sorting through a bewildering array of options
- Security is but one of a list of VPN issues for corporate network and service provider managers—What is the role of PPTP, L2TP, IPSec, and other technologies? Which VPN functions should be kept in-house, and which should be outsourced

B. VPNs and Their Benefits

The purpose of this paper is to dispel some of the confusion, both for service providers and managers of enterprise networks.

VPNs use public IP networks to extend the reach of the enterprise network to remote sites, individual remote workers, and business partners. VPNs provide:

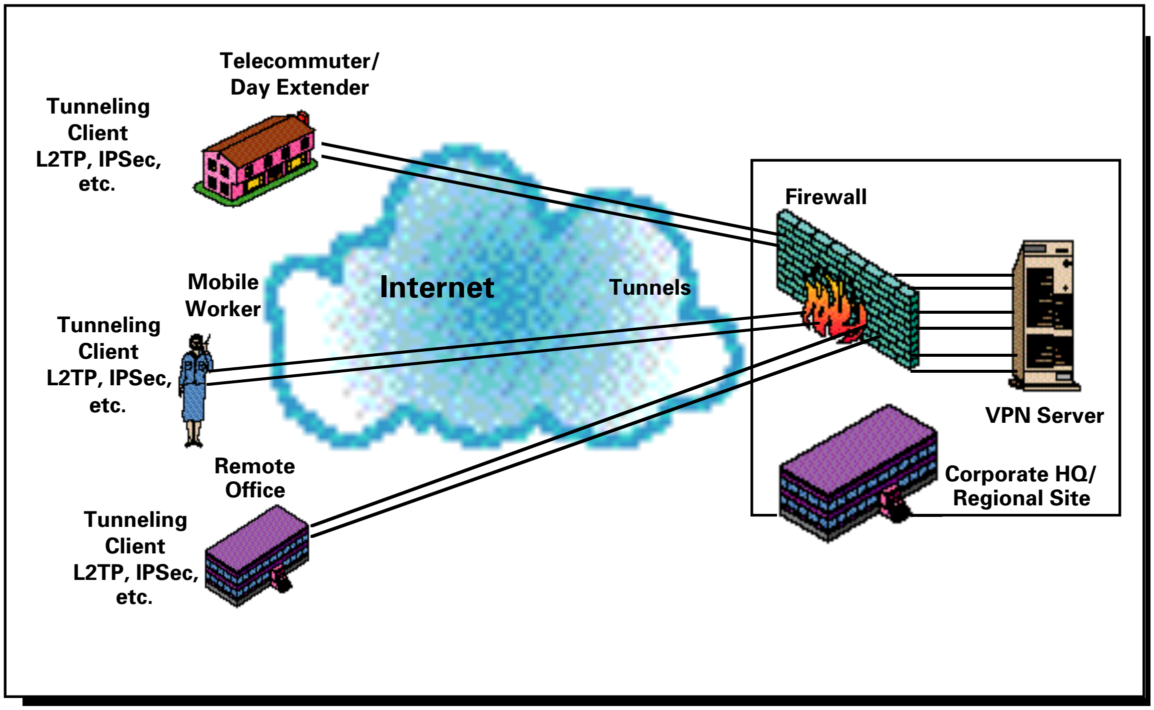
- Network managers with a reduced-cost means of increasing the effective span of the corporate network
- Network users with a convenient and secure means to remotely access their corporate network
- Corporations with a convenient, secure method for communicating with business partners
- Service providers with a great opportunity to grow their businesses by providing substantial incremental bandwidth with value-added services

VPNs provide an inexpensive way to extend the corporate network out to distant offices, home workers, and road warriors. Rather than using expensive dedicated leased lines to reach distant offices, VPNs make use of world-spanning IP network services, including the Internet, and service provider

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

backbone networks. Rather than dialing in at long distance rates, road warriors can make a local Internet connection. The cost savings in line charges alone can be substantial.

Exhibit 1 **VPNs Across the Internet**



© 1997 Infonetics Research, Inc.

As a VPN delivery transport, the Internet is the low-cost leader. But many service providers also offer VPN services over their private IP backbones. While these VPNs may be limited in scope to subscribers of the service provider network, they offer more predictable and controllable performance than is available from today's Internet. The public Internet offers ubiquitous access and low cost. Private IP backbones can provide VPNs with levels of quality of service (QoS). With the appropriate mix of services, enterprise network managers can develop an outsourced WAN strategy that meets a range of cost and performance needs.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

In addition to saving on line charges, VPNs are much less costly in terms of WAN operations costs such as personnel and equipment.

- According to a study authorized by Sun Microsystems, by replacing leased lines to remote sites with VPNs, corporations save from 20 to 47% of the WAN costs.
- Data from an upcoming Infonetics Research study shows VPNs saving users from 60 to 80% of their corporate remote access dial-up costs.

Besides lowering costs, VPNs provide access from wherever the Internet reaches. Internet POPs are available worldwide, providing potential VPN connection points in nearly every country, and in most of the commercially important cities of the world.

Perhaps most importantly, VPNs enable the establishment of rich, flexible communications relationships with customers, suppliers, and business partners via so-called extranets. By their nature, extranets allow users to establish interactive links with every business partner—not just a selected few. The expensive dedicated network is no longer a necessity. Instead, VPN technology creates a secure communication environment that members may join at a moment's notice. So beyond the tactical cost-savings, extranets are strategic—they will change the way businesses communicate as significantly as have fax, voicemail, and e-mail.

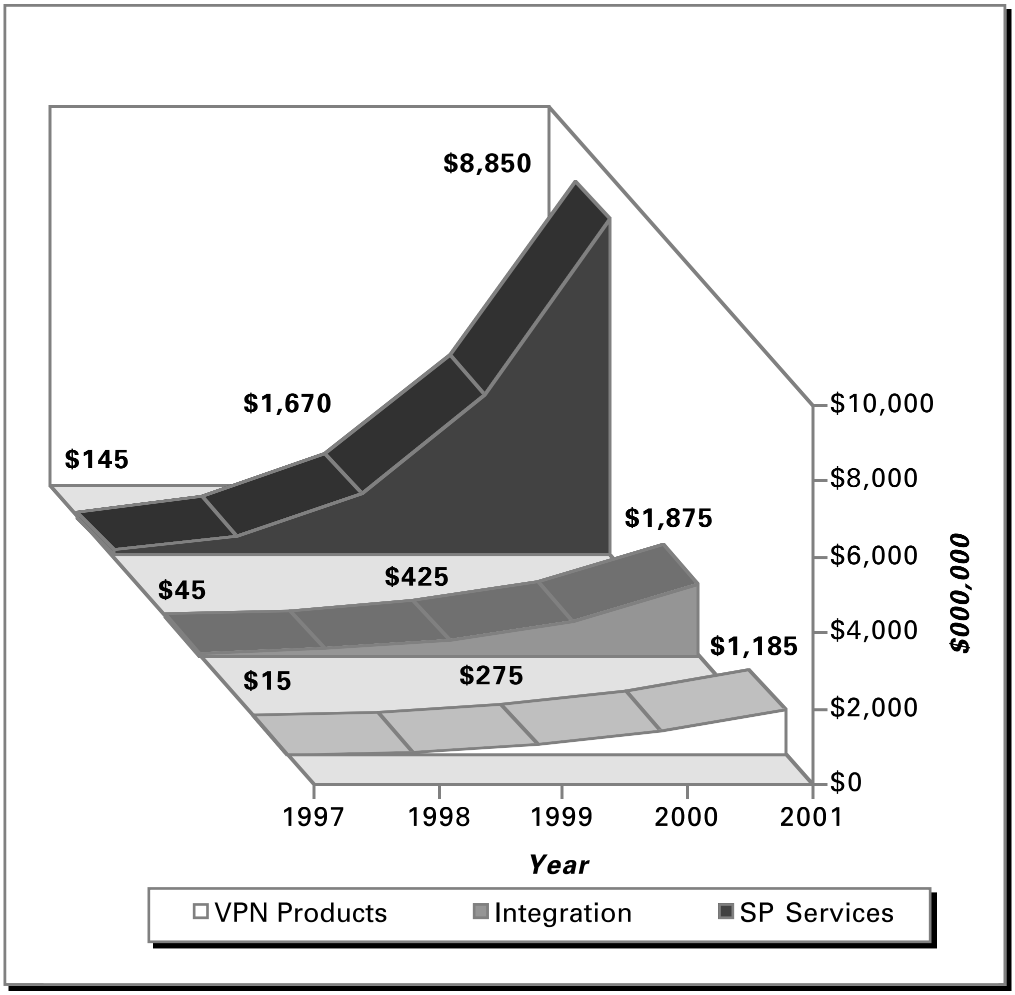
With all that going for them, why are VPNs only now at the take-off point?

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

C. VPN Market Growth

Infonetics Research estimates the VPN market was US$205M in 1997 and will grow over 100% per year through 2001 when it reaches US$11.9B. These estimates comprise 3 segments: VPN products, systems integration, and SP services as shown below.

Exhibit 2 **Worldwide VPN Expenditures, 1997–2001**

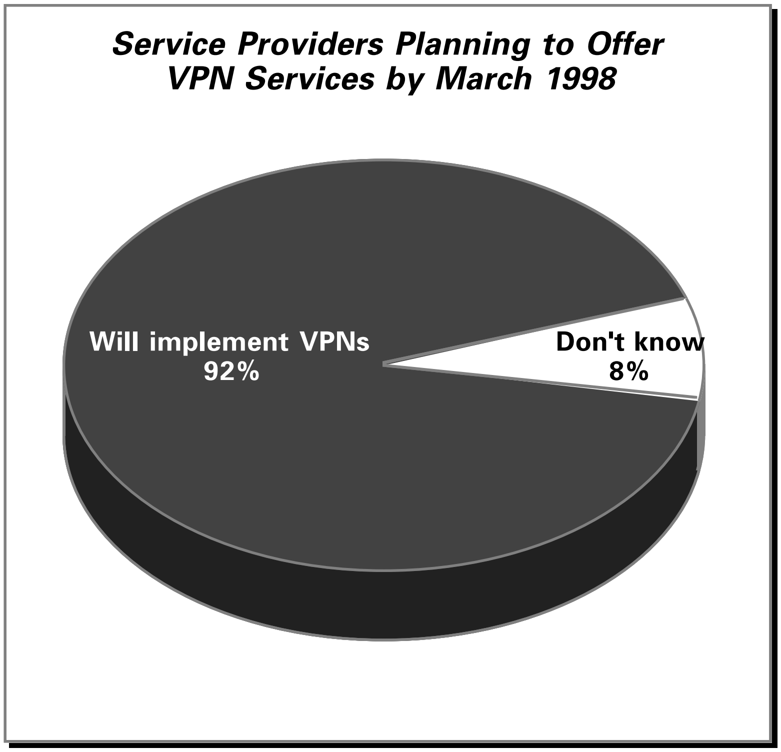


© 1997 Infonetics Research, Inc.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

Because of the large opportunity, VPNs are being offered by an increasing number of SPs. By March, 1998, 92% of large service providers plan to offer VPNs. Those with service offerings or stated plans include UUNET, BBN Planet, Internet MCI, Sprint, and PSINet, among others.

Exhibit 3 **Major Service Providers Are Offering VPNs**



© 1997 Infonetics Research, Inc.

Although many enterprise network and SP managers realize that they need VPNs, they may not realize that VPNs come in a variety of implementations, each with consequences for security, performance, convenience, cost, and manageability. Furthermore, the division of VPN responsibilities between the enterprise network staff and the service provider ranges from *completely in-house* to *totally outsourced.*

D. Caution: Emerging Market

There are a number of issues to resolve and decisions to make in order to implement VPNs in the real world.

- Some industry problems have been settled, some are being mastered as we write, and some are the subject of standards debates and the lengthy standards process.
- The Internet was not initially designed with high security in mind, which means that for corporations to entrust it with their most sensitive data, some additional work must be done both in assuring that the right people are accessing the corporation's networks (authentication) and that the data itself cannot be read by outsiders (encryption).
- The Internet was also not designed to deliver performance guarantees. Applications designed to work with a guaranteed network latency may not perform adequately on the Internet.
- Finally, there are several different technical approaches to implementing VPNs over the Internet. Three of the most popular are PPTP (Point-to-Point Tunneling Protocol), its kin L2TP (Layer 2 Tunneling Protocol), and IPSec (IP Security). These VPN technologies have very different capabilities, as described in the next chapter.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

III. VPN Technology Choices

All 3 VPN technology types we consider here—PPTP, L2TP, and IPSec—employ tunneling, in which data designed for point-to-point transmission is encapsulated inside IP packets. PPTP and L2TP are strictly tunneling protocols; IPSec is a collection of IP security measures that define standard ways for creating and managing encrypted tunnels for privacy, data integrity, and authentication. These tunneling mechanisms differ on what's done to the data (encryption, authentication), the headers that describe the data transmission and packet handling, and the OSI layer at which they operate.

A. The Issues

Being able to create VPN tunnels does not itself determine a useful VPN service. Many other ingredients are necessary, and several are discussed in the following paragraphs.

1. Security

Security is the central issue for many VPN applications. Some VPN technologies have security built in (as part of their IETF specification); others require one or more add-ons.

To meet corporate standards, VPN communications must be:

- Safe from prying eyes—outsiders must not be able to read the data
- Safe from tampering—outsiders must not be able to alter the data
- Safe from spoofing—outsiders must not be able to masquerade as insiders

Data privacy is provided using encryption. Data tampering is thwarted by using transformations called hashing functions, which create fingerprints that can detect altered data. User authentication prevents one user from masquerading as another.

Encryption involves a series of complex mathematical transformations, in which the original data is combined with a logical key and later decrypted by

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

the receiver using the same key and an inverse transformation at the receiving end. Managing the keys is the most critical and problematic issue associated with practical encryption systems. It requires that the sender and receiver, potential strangers, negotiate, agree upon, and exchange key information in a safe manner, even before the communicating parties have established a secure communications channel. If the keys are not safeguarded, the security of the data is compromised. As such, any viable VPN solution must have a key management mechanism to automatically negotiate and exchange secret encryption keys in a secure manner.

Encryption is especially computationally expensive. To avoid severe performance degradation all these security measures—encryption, hashing, authentication, and key management—must be performed on products that are optimized for these functions.

2. Performance

Performance of VPNs is a function of 2 factors:

- The speed of the transmissions through either the Internet or a public IP backbone network
- The efficiency of the VPN processing—establishing a secure session, encapsulating and securing packets—at each end of the connection

The public Internet cannot provide guaranteed levels of response time, reliability, and consistency. Many vital corporate networks cannot be subjected to the whim of Internet performance fluctuations and spotty access. For example, for sales people in the field to use VPNs rather than private facilities, they must have reliable access plus good performance, or the corporation's sales efforts get stymied.

Some service providers solve the transmission speed problem by offering quality-of-service agreements, guaranteeing bandwidth at specified levels. The most effective method of achieving QoS today is to send VPN traffic across the SP's own IP backbone (e.g., across the SP's frame relay or ATM circuits), not across the Internet.

Once the packet traverses the public network, the speed of decryption and tunnel destination processing further affects the ultimate throughput.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

Encapsulation requires adding data fields to each packet, which increases their size and also increases the likelihood that internetwork routers will find them oversized and fragment them in two, further degrading performance. Packet fragmentation and data encryption overhead can reduce dial-in system performance to unacceptable levels depending on the applications being used. Compression of the packet data before encapsulation can alleviate this problem, but there is a price to pay: the combination of compression and encapsulation requires additional computational power beyond that needed for security.

3. Convenience and Flexibility

In order to be useful, implementing and using VPNs should be as transparent as possible for users, corporate network management staff, and SPs. Users in particular should be able to connect as easily as they do over leased lines or by long distance dial-up. Network management staff require management and troubleshooting tools that enable them to outsource their WAN infrastructure with confidence.

4. Costs

One of the promises of VPNs is to save costs over leased line WAN connections and reduce the cost of corporate dial-up operations. The real cost of corporate dial-up connections includes a load on the network staff:

- Buying, installing, and configuring remote access servers and modem racks
- Working with telephone companies to install lines
- Keeping up with new client software, and installing it in laptops
- Monitoring traffic patterns on remote access ports
- Supplying sufficient ports for increasing numbers of telecommuters
- Monitoring and paying for dial-up telephone charges
- Keeping up with fast-changing technology (for example, knowing when to install how many ports for 56K modems or ISDN

The costs of implementing and managing VPNs should be viewed in relation to these "soft" costs, as well as the more obvious costs for lines and equipment.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

5. Management

VPNs must include tools for the network manager and SPs to manage security, performance, and costs. Both enterprise network managers and service providers must be able to manage:

- Installation and provisioning of equipment, in a secure fashion
- Scaling the VPN, when the requirements grow beyond its current capabilities
- Tracking of problems beyond their own borders—for the network manager this means across the outsourced WAN, and for the service provider this means across multiple subscriber networks
- Establishment of extranet relationships with a range of business partners, some highly trusted and some not

Another important factor is the security of the VPN management process itself and the tools it requires. Over time, the quality, completeness, and security of VPN management tools will play a dominant role in the effectiveness of any VPN implementation.

B. Technology Options

The PPTP, L2TP, and IPSec specifications are sets of requests for comment (RFCs) to the IETF that describe protocols to be used for tunneling. All are proposed for inclusion in the next-generation IP protocol, IPv6. IPSec is already being implemented in IPv4, the current IP protocol used in the Internet and elsewhere.

PPTP (Point-to-Point Tunneling Protocol) was initially driven by Microsoft and Ascend to support packet tunneling in Ascend's remote access server hardware and Microsoft's NT software. The backers of the PPTP protocol combined efforts with Cisco and its L2F protocol to produce a hybrid called L2TP.

IPSec is a general initiative to add security services to the IP protocol. A growing number of VPN, security, and major network companies—over 30 as of October 1997—either support or plan to support IPSec. It is also strongly supported by a user group consisting of manufacturers and suppliers. This group, the Automotive Network Exchange (ANX) is spearheading IPSec

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

interoperability testing. Of the 3 alternatives, IPSec is the only protocol being driven by major network users.

Another protocol, SOCKS v.5, operates at OSI layer 5, but it is supported by only a small number of vendors at this point, and is not considered here.

Exhibit 4 summarizes key aspects of the different VPN technologies' characteristics.

Exhibit 4 **VPN Technology Standards Compared**

	PPTP	L2TP	IPSec
Mode	Client-server	Client-server	Host-to-host
Purpose	Remote access via tunneling	Remote access via tunneling	Intranets, extranets, remote access via tunneling
OSI Layer	Layer-2	Layer-2	Layer-3
Protocols Encapsulated	IP, IPX, AppleTalk, etc.	IP, IPX, Appletalk, etc.	IP
Security:			
User authentication	None (use PAP, CHAP, Kerberos, Token ID, etc.)	None (use PAP, CHAP, Kerberos, Token ID, etc.)	None (use PAP, CHAP, Kerberos, Token ID, etc.)
Packet authentication	None[1]	None[3]	AH header
Packet encryption	None[2]	None[3]	ESP header
Key management	None[1]	None[3]	ISAKMP/Oakley, SKIP
Tunnel Services	Single point-to-point tunnel, no simultaneous Internet access	Single point-to-point tunnel, no simultaneous Internet access	Multipoint tunnels; simultaneous VPN and public access

Notes

1. Not in standard, not offered
2. Vendor-specific implementation only
3. Refers to IPSec for implementation

© 1997 Infonetics Research, Inc.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

Mode: The client-server model is based on a user-to-server paradigm for remote user dial-up over PPP. The host-to-host model is based on the more general computer-to-computer paradigm, which includes both site-to-site and remote user dial-up.

Purpose: PPTP and L2TP tunneling are aimed primarily at enabling Internet-based remote access. IPSec is a standard IP method for tunneling and security.

OSI layer: PPTP and L2TP operate at layer 2 of the OSI 7-layer network model, while IPSec operates at layer 3. Layer-2 tunneling has the advantage of simplicity, while layer-3 tunneling offers better scalability and security.

Protocols encapsulated: As PPTP and L2TP operate at layer 2 of the OSI model, they can encapsulate protocols from layer 3, such as IP, IPX, and Appletalk. IPSec is specific to layer 3 and must rely on other encapsulation protocols for non-IP traffic.

Security: The IETF PPTP drafts for 1996 and 1997 both delay discussion of security, which is to be covered in the next version of the specification. The PPTP draft may soon be revised to refer to IPSec for packet encryption. The L2TP specification refers to IPSec as the security method for encryption in environments (chiefly IP) that have IPSec. Security methods for L2TP in non-IP environments that lack IPSec are currently under draft review. IPSec includes specifications for packet-level encryption and authentication, and also defines robust means for key management.

Tunneling: Single point-to-point tunneling means there can be no simultaneous Internet access while using a VPN connection. With multipoint tunneling a user could have an Internet session at the same time as several VPN sessions.

Based on the above comparison, **IPSec is the preferred solution for IP environments, as it has security built in**. PPTP and L2TP are most appropriate for multiprotocol environments, but both require additional support to deliver data privacy, integrity, and authentication. Unless augmented with IPSec, PPTP and L2TP cannot support extranets, because extranets require keys and key management.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

IV.VPN Implementation Issues

The first question facing the enterprise network manager and their service provider is how they will share the various VPN operational tasks between them. The second question, for one or both of them, is which technology to implement.

A. Corporate Tasks and Outsourcing

Service providers can take many different approaches to their VPN offerings. For example, they may simply supply the Internet or IP network bandwidth needed to handle VPN traffic. Alternatively, SPs can offer more products and services, including design, management, service, and training for the corporate VPN. Flexible SPs will offer a range of VPN service options, so that the corporate network manager can outsource those functions for which they are not equipped.

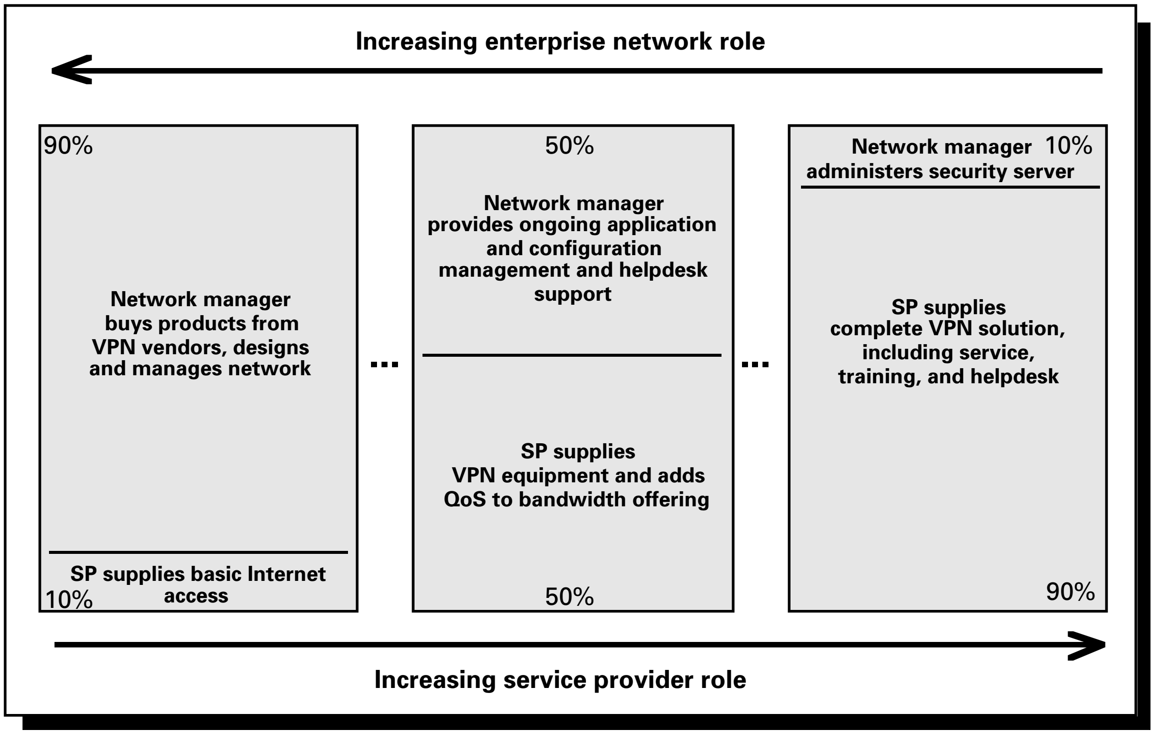
Some selected VPN service offerings for SPs:

1. Sell basic Internet access and bandwidth; the enterprise customer handles all VPN products and operations
2. Sell business-quality Internet or IP network services; the enterprise customer handles all VPN products and operations
3. Sell compulsory VPNs embedded in POP equipment
4. Offer VPN hardware and software bundled with VPN bandwidth and services
5. Design the customer's VPN solution
6. Operate the total VPN solution for the customer, including design, equipment installation and service, and helpdesk support (100% outsource)

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

Exhibit 5 graphs some of the varying degrees of VPN responsibility that can be shared between the enterprise network staff and the network service provider.

Exhibit 5 **Who Performs VPN Functions—Enterprise or SP**


Increasing enterprise network role
90%
Network manager buys products from VPN vendors, designs and manages network
SP supplies basic Internet access
10%
...
50%
Network manager provides ongoing application and configuration management and helpdesk support
SP supplies VPN equipment and adds QoS to bandwidth offering
50%
...
Network manager 10%
administers security server
SP supplies complete VPN solution, including service, training, and helpdesk
90%
Increasing service provider role

© 1997 Infonetics Research, Inc.

1. Implications for Network Managers

Network managers need to determine how much of the implementation tasks they want off-loaded to the service provider. Security, as a prime example, may be required to stay in-house, while costly helpdesk services may be gratefully off-loaded to the service provider. In-house security will probably require that the network management staff include a security expert, as the topic is highly technical and requires special expertise.

Some VPN implementations cannot be achieved without involving the service provider. IPSec and "voluntary" mode of PPTP handles all VPN operations at the end-points and are thus transparent to the service provider. PPTP requires SP participation to establish a VPN connection when compulsory mode is used. Compulsory tunneling requires service provider cooperation.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

2. Implications for Service Providers

Service providers need to determine how they will support VPNs. They may choose to support a single technology or multiple technologies, but they need to know and understand the issues.

When SPs have determined their VPN service offerings, they must make these services clear to corporate network managers, who are wrestling with operational decisions. We believe SPs can find markets for any level of VPN service, from basic Internet services to complete outsourcing, and should target those enterprises that are seeking a corresponding level of service.

B. Scaling the Solutions

Implementation solutions for creating VPNs range from software only, through hardware-assist, to dedicated hardware. Depending on the VPN application, the security required, and the desired performance, users may need hardware rather than software solutions. Encryption, authentication, and key management require intense computation power. Exhibit 6 presents some of the trade-offs between software, hardware-assist, and dedicated hardware solutions.

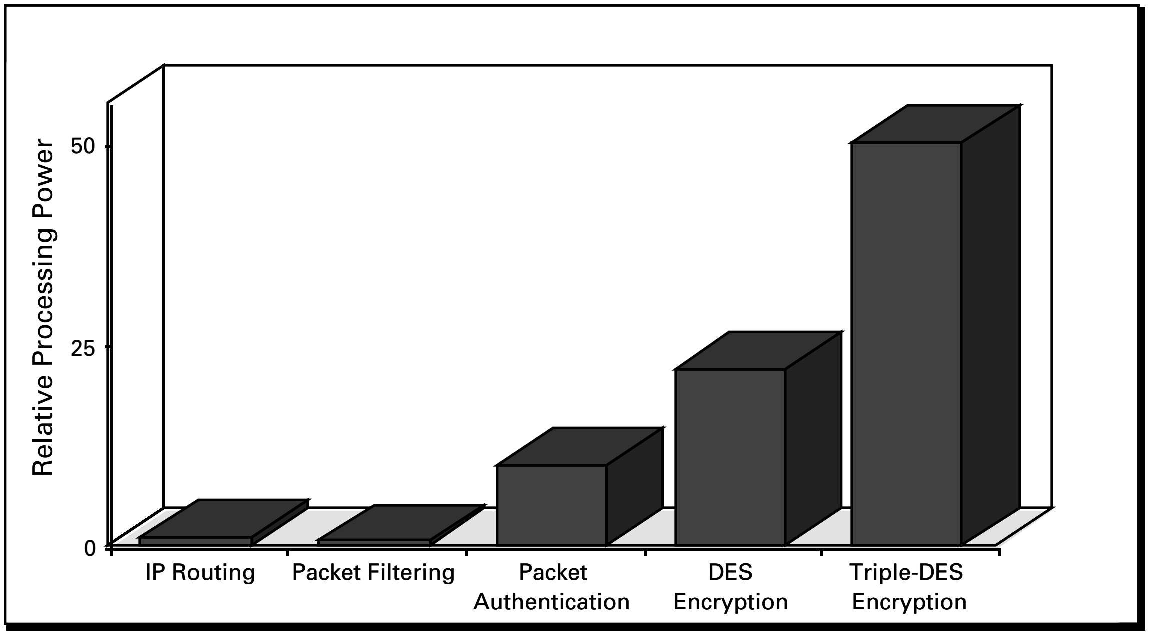
Exhibit 6 **VPN Solutions: Hardware/Software Trade-Offs**

	Software Only	Hardware Assist	Dedicated Hardware
Performance	Lowest	Low-medium	Highest
Security	Physically insecure (platform) Logically insecure (OS)	Physically insecure (platform) Logically insecure (OS)	Physically and logically secure
Suitable applications	Dial-up to ISDN data rate (128K), e.g., a single user or SOHO with no special security needs	ISDN through T1 speeds	Dial-up speeds to 100Mbps
Products	Firewalls Standalone VPN software	Encryption cards for routers, PCs	Standalone VPN devices

© 1997 Infonetics Research, Inc.

Encryption is heavily processor-intensive. Whereas a router generally need only process the packet header, an encrypting process operates on each byte in the packet. Triple DES encryption, for example, requires about 50–100 times more processing power than straight IP routing. For this reason, when performance is a concern, hardware-based VPN solutions provide a critical advantage. When data rates are low enough, for example 128Kbps or less, software-based encryption products deliver adequate throughput. And, while they offer limited performance, the cost of software-based VPN solutions can be much lower if companies already have the hardware platforms to run them on.

Exhibit 7 **Security Is Processor-Intensive**



© 1997 Infonetics Research, Inc.

Physical security requires a tamper-proof hardware enclosure. Logical security requires a closed, secure operating system to implement the security computations. Dedicated VPN hardware platforms offer the best support in these areas.

For small-scale situations in which privacy is not an issue, a software solution may work. Large traffic volumes and/or highly secure solutions call for dedicated hardware.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

1. Small-Scale Solutions

Because of the performance implications, encryption in software is typically limited to 56-bit DES at most (rather than Triple DES), so traffic cannot be of utmost sensitivity—and even DES encryption will consume many CPU cycles. Encryption via 40-bit and 56-bit DES may provide low-but-adequate security for most transactions; although crackable, the task isn't easy. For occasional connections for mobile and home-site workers, a software implementation may be all that's needed and is the most cost-effective.

2. Large-Scale Solutions

Replacing leased lines in a corporate WAN requires a high-performance VPN solution, which means adding hardware—either add-ons to existing devices (router, server), or adding standalone VPN devices. Costs are greater, but there are significant benefits: wire speed or close to it, and robust security.

Router and server add-ons, such as encryption cards, may be limited in performance range, as to some extent they depend on the performance of the device to which they attach. Standalone devices are typically designed to be more scalable, which means they can accommodate greater bandwidth—increased traffic, more VPNs, higher-speed lines—better than can add-ons.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

V. The Enterprise and Service Provider Partnership

VPNs provide both service providers and enterprise network managers with opportunities. The service provider can expand its service offerings, and resulting margins. The manager of the enterprise network can extend the network's reach to the full global extent of the Internet, and at the same time cut costs. For most businesses, VPNs are not a matter of "if," but a matter of "when" and "how."

For both service providers and enterprise network managers, the first implementation consideration is: Which VPN operational tasks do you want to offer/assume? The service provider must determine its strengths and where it can find good margins; the network manager must determine what the staff is good at, and how much they want to take on. Then each can seek out an appropriate VPN partner.

The network manager who wants to do it all should seek a service provider that can provide low-cost, high bandwidth at service levels that meet the corporate needs. If VPN services are to be outsourced, find a reliable full-service provider. If VPN implementation is to be shared between them, they must agree on the technology to be used (PPTP/L2TP or IPSec); the security, and hence computing power, required (software only, hardware assist, or dedicated hardware); and future needs (scalability). VPNs are ultimately about partnerships, and the most important VPN partnership for many organizations will be the one they establish with their VPN service provider.

© 1997 by Infonetics Research, Inc. All rights reserved. Reproduction is prohibited.

About Infonetics Research

Infonetics Research, Inc., provides network vendors with critical market and technology advice aimed at developing winning products—and the most effective messages to sell those products. Infonetics Research delivers advice through comprehensive market studies and one-on-one consulting. Our focus areas are campus LANs, remote access, Internet service providers, and network and systems management.

The research team frequently interviews all players in the network industry—product owners, network vendors and trade press. This in-depth research results in a thorough knowledge of both the supply and the demand sides of the network market. Time and again, market studies from Infonetics Research have made a critical difference to network vendors.

For more information on Infonetics Research multiclient studies and consulting services, call **Larry Howard** at **408-298-7999**.