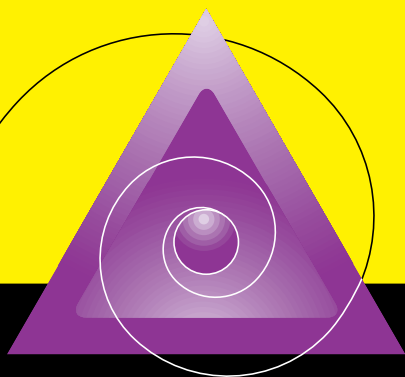


THE TECHNOLOGY GUIDE SERIES®

www.techguide.com™

A Practical Guide to the Right VPN Solution



This Guide has been sponsored by



Table of Contents

Summary.....	4
Introduction.....	5
VPN Overview and Benefits	8
VPN Implementation Alternatives.....	25
Key Features and Cost Elements for a VPN Solution	30
Selecting the Right VPN Solution.....	35
Conclusion.....	37
Case Study.....	38
Glossary of Terms.....	42

Visit ATG's Web Site
to read, download, and print
all the Technology Guides
in this series.

www.techguide.com

About the Editor...

Jerry Ryan is a principal at ATG and the Editor-in-Chief of techguide.com. He is the author of numerous technology papers on various aspects of networking. Mr. Ryan has developed and taught many courses in network analysis and design for carriers, government agencies and private industry. He has provided consulting support in the area of WAN and LAN network design, negotiation with carriers for contract pricing and services, technology acquisition, customized software development for network administration, billing and auditing of telecommunication expenses, project management, and RFP generation. Mr. Ryan has been a member of the Networld+Interop Program Committee and the ComNet steering Committee. He holds a B.S. degree in electrical engineering.

“The significant problems we face cannot be solved
by the same level of thinking that created them.”

Albert Einstein

The Guide format and main text of this Guide are the property of The Applied Technologies Group, Inc. and is made available upon these terms and conditions. The Applied Technologies Group reserves all rights herein. Reproduction in whole or in part of the main text is only permitted with the written consent of The Applied Technologies Group. The main text shall be treated at all times as a proprietary document for internal use only. The main text may not be duplicated in any way, except in the form of brief excerpts or quotations for the purpose of review. In addition, the information contained herein may not be duplicated in other books, databases or any other medium. Making copies of this Guide, or any portion for any purpose other than your own, is a violation of United States Copyright Laws. The information contained in this Guide is believed to be reliable but cannot be guaranteed to be complete or correct. Any case studies or glossaries contained in this Guide or any Guide are excluded from this copyright.

Copyright © 2001 by The Applied Technologies Group, Inc. 209 West Central Street, Suite 301, Natick, MA 01760, Tel: (508) 651-1155, Fax: (508) 651-1171
E-mail: info@techguide.com Web Site: <http://www.techguide.com>

Summary

This Technology Guide is written for Business and for IT Managers at small to medium-sized businesses who plan and implement the network infrastructure for their businesses. The Guide is primarily for IT and networking managers who are selecting VPN solutions. It is written to help the reader navigate the VPN swamp. This Guide assumes the reader is familiar with the Internet and with the distinction between intranets and extranets. It should help readers understand VPN applications, benefits, and implementation alternatives.

After reading this Guide, the reader should be able to evaluate features of a VPN solution relative to his/her requirements. Based on least cost of ownership, the reader will be able to select a VPN solution from a set of alternatives that is most suitable for their near- and long-term needs.

Introduction

E-business, e-commerce, e-marketplace, business-to-business (B2B), and business-to-consumer (B2C), are now common business parlance. Every organization is defining and implementing its e-strategy. The question is no longer whether to migrate to an e-environment, but what is the best way to migrate to a Web and Internet-based business model.

The Internet allows businesses to reach their customers, and vice versa, anytime and anywhere in the world. A US company need not deploy any resources or infrastructure in China, for example, to engage in business in China. A mom-and-pop e-business in a non-English speaking country has as good a probability of reaching a customer in the US as an American multi-billion dollar company. A common challenge to both companies is the use of the Internet to leverage their business.

One of the key technologies for using the Internet in a secure and private manner is the virtual private network (VPN). This Technology Guide explains VPN applications, benefits, and implementation alternatives. More importantly, it provides guidelines for selecting the right VPN solution.

The Guide focuses on needs of small and medium-sized businesses that do not have the technical and management resources to deploy, to maintain, or to operate their own VPNs. Many large enterprises will find the VPN deployment model discussed here to be the most cost-effective answer to their e-business and remote office requirements.

The Business Problem

Before the popularity of the Internet, large enterprises were building multi-million dollar private data networks (now called intranets), using telecommunications services such as leased lines, Frame Relay, and Asynchronous Transfer Mode (ATM) to communicate among geographically dispersed sites. These services were often supplemented with services, such as switched analog or ISDN, to connect smaller sites and mobile users. Small and medium-sized enterprises, who could not afford the cost of long-distance leased facilities, were limited to low-speed switched services.

These intranets were expensive and required hordes of support personnel. Intranets also had long planning, design, and implementation cycles, resulting in tremendous lost-opportunity costs. As the Internet became ubiquitous and as ISPs offered high-speed Internet access, enterprises reduced the cost and the time to deploy their intranets by off-loading them to the Internet.

As enterprises dabbled in e-commerce, whether as B2B or as B2C, it became clear that the Internet was the practical and cost-effective way to connect with customers and partners. The concept of connecting with external users or organizations came to be known as extranets.

As cost-effective as the Internet is, it introduces one major challenge—security. Though the Internet has emerged as the network foundation for e-endeavors, it is paradoxically a public, shared network of networks and is not suitable, in its natural state, for secure transactions or private communications.

Enterprises have recognized that e-business is more than just Internet connectivity or the exchange of e-mails and files. E-business needs real time exchange of data. This involves all of the enterprise-procurement, supply-chain management, sales and customer relationship management, online business transactions,

online dealings with financial institutions, etc. These requirements make security over the Internet paramount.

Virtual Private Network—The New Solution for E-Business

VPNs have emerged as the key technology for achieving security over the Internet. While a VPN is an inherently simple concept, early VPN solutions were geared towards large organizations and their implementation required extensive technical expertise. As a consequence, small and medium-sized businesses were left out of the e-revolution. Recently, VPN solutions have become available that focus specifically on the needs of small and medium-sized businesses.

Historically, the term VPN has also been used in contexts other than the Internet, such as in the public telephone network and in the Frame Relay network. In the early days of the Internet-based VPNs, they were sometimes described as Internet-VPNs or IP-VPNs. However, that usage is archaic and VPNs are now synonymous with Internet-VPNs.

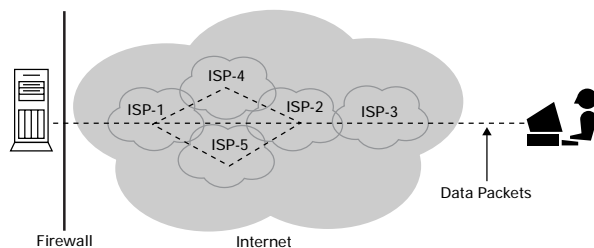


Figure 1a: Data flow through the Internet

VPN Overview and Benefits

Protection Beyond the Firewall

A firewall is an important security feature for Internet users. A firewall prevents data from leaving and entering an enterprise by unauthorized users. However, when packets pass through the firewall to the Internet, sensitive data such as user names, passwords, account numbers, financial and personal medical information, server addresses, etc. is visible to hackers and to potential e-criminals. Firewalls do not protect from threats within the Internet. This is where a VPN comes into play.

A VPN, at its core, is a fairly simple concept—the ability to use the shared, public Internet in a secure manner as if it were a private network. Figure 1a shows the flow of data between two users over the Internet when not using a VPN. As shown by the dotted lines, packets between a pair of users may go over networks run by many ISPs and may take different paths. The structure of the Internet and the different paths taken by packets are transparent to the two users. With a VPN, users encrypt their data and their identities to prevent unauthorized people or computers from looking at the data or from tampering with the data.

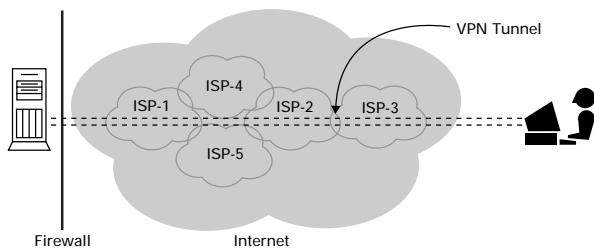


Figure 1b: VPN over the Internet

Figure 1b, shows the encrypted flow of packets—referred to as a tunnel in a VPN. The VPN tunnel is shown graphically as a line connecting the starting point and endpoint of the encryption. While the tunnel is shown in Figure 1b and in other literature as if the tunnel is a fixed path, packets associated with the tunnel may take different paths, like the ones in Figure 1a. In this example, the endpoints of the VPN tunnel are a client at the user station and a server or gateway at a central site. We need software or some other device at each end of the tunnel to initiate, authenticate, and terminate a VPN tunnel. In addition to encryption, VPN also allows for user- and data-authentication.

VPN Applications

A VPN can be used for just about any intranet and e-business (extranet) application. Examples on the following pages illustrate the use and benefits of VPN for mobile users and for remote access to enterprise resources, for communications between remote offices and headquarters, and for extranet/e-business.

Remote Access

In this application, when not using a VPN, mobile and remote users often use analog (dial-up modems) or ISDN switched services to connect to a headquarters data center. This is shown in figure 2a. These connections are used to access e-mail, to download files and to execute other transactions. This type of connection would also be used by small offices that do not have a permanent connection to the enterprise intranet.

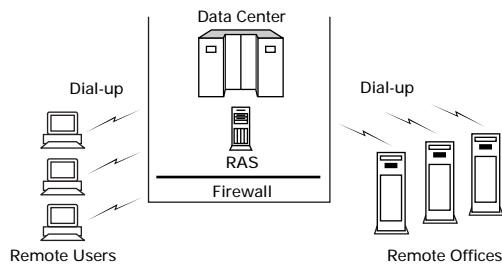


Figure 2a: Remote access using switched services

The cost elements for such an application include:

- Dial-up connection charges, especially for users making long-distance connections.
- A remote access server (RAS) at the central site to handle incoming calls.
- Technical personnel to support remote users and to configure, maintain, and support a RAS.

With a VPN, as shown in figure 2b, remote users and branch offices set up dial-up connections to local ISPs and connect via the Internet to a VPN server at headquarters.

VPN benefits include:

- Elimination of the RAS, of associated modems, and of technical support costs to install, configure, and maintain the RAS.
- Replacement of long-distance or 800-number services with local ISP connections at remote sites.
- Access to all enterprise data and applications (not just e-mail or file transfers) over the Internet.

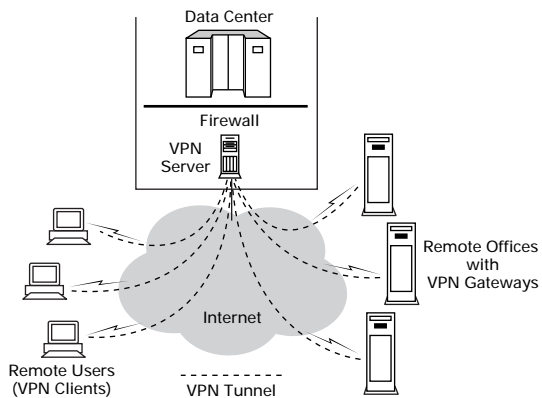


Figure 2b: Remote access using VPN

New costs for VPN include:

- Installation, support, and maintenance of a VPN server at the central site and of VPN clients for remote users.

Studies show that the cost savings in long-distance charges alone pay for the VPN setup costs within a few months, and substantial recurring savings follow.

Branch-to-Branch or Branch-to-Headquarters

In Figure 3a, a business has an intranet connecting remote locations with headquarters. Each campus has a router connecting the campus to a backbone router over a LAN or WAN link (smaller networks may not need backbone routers). A single router may be connected to both the campus LAN and to the other campuses with a WAN link. WAN routers are typically mesh-connected using leased lines or a Frame Relay service.

Primary cost elements for a branch-to-branch intranet include:

- Routers, both campus and backbone.
- Telecommunications services, in particular long distance. The cost of the intranet backbone,

depending on the traffic volume and geographical reach, can run from tens of thousands of dollars a month to hundreds of thousands of dollars a month. These costs are especially onerous for multi-national organizations.

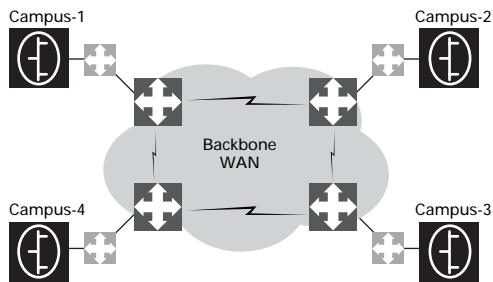


Figure 3a: Enterprise intranet without VPN

With a VPN, the intranet backbone WAN is replaced by the Internet. This is shown in Figure 3b. The new costs for this configuration include the deployment and maintenance of VPN gateways at remote campuses and the deployment and maintenance of a VPN server at the headquarters site. In addition, each location pays for an Internet connection.

VPN benefits include:

- Elimination of backbone routers.
- Elimination of system administration, configuration, and technical support for routers and elimination of the need to design and maintain routing tables.
- Elimination of long-distance services; as with the remote access case, this results in substantial savings. The amount of savings depends on the size of the intranet.
- Reduction in lost-opportunity cost due to the

elimination of long provisioning cycles for long-distance service and for international telecommunications services.

- Most likely, better performance than an intranet due to higher speed facilities inside the Internet.

The migration to VPN could pay for itself in a few months. There would also be substantial recurring savings.

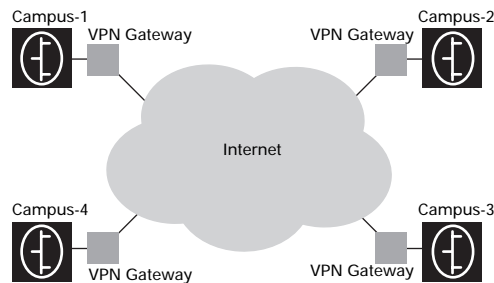


Figure 3b: Branch-to-branch and branch-to-headquarters over VPN

B2B, B2C, and Extranet

Before the availability of the Internet and VPNs, electronic transactions and communications between enterprises were particularly difficult since there was no standard or common way to enable these communications.

As shown in Figure 4a, there were numerous networks and architectures to enable inter-corporate commerce. For example, the banking industry has a long history of electronic transactions among banks and with central banks. The brokerage industry, similarly, has special systems for communicating with stock exchanges, with settlement bodies, and with depository companies. In addition, there were several custom-made networks with proprietary transaction formats for electronic data interchange (EDI). In some cases,

corporations or government agencies set up their own standards to execute transactions with their business partners and suppliers. Many organizations had to connect with multiple EDI networks because of the diverse nature of their business.

These historic approaches had numerous drawbacks:

- Very expensive to develop since everything is tailor-made for one industry.
- Long design and deployment time.
- Inability to adapt to new requirements.
- Lack of qualified personnel for narrowly used proprietary systems.
- Could not be easily extended to new locations and customers.
- High entry cost for new customers/members and lost opportunity cost for not being able to participate in e-commerce with non-members.

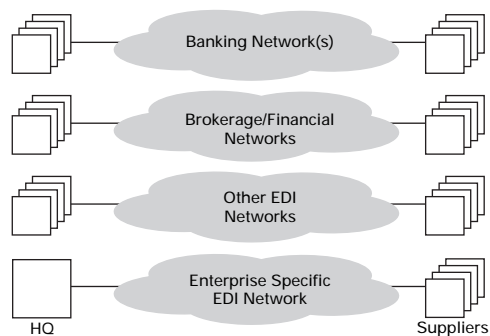


Figure 4a: E-Commerce before the Internet and VPN

The Internet, of course, has changed all that. Now, any organization or individual can engage in business transactions or other communications in a secure and private manner by using a VPN over the

Internet. Figure 4b shows an example of the new environment.

VPN benefits include:

- Open interfaces; anyone can use it without a major initial investment.
- Fractional cost compared to proprietary networks.
- Worldwide ubiquity built in; reach any customer anywhere without adding infrastructure at those sites.
- Low entry cost, narrowing the opportunity gap between large and small enterprises.
- Rapid deployment, flexibility, ease of modification.
- Choice of vendors in selecting a solution.
- Extensive availability of technical personnel and expertise.

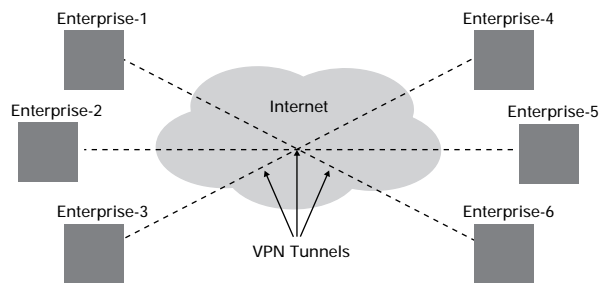


Figure 4b: E-Business and extranets with VPN

The three examples discussed in this section explain the benefits and versatility of VPNs for e-business. VPN has become a prerequisite for secure commerce or for secure communications over the Internet. In the following section, the Guide explains technologies underlying VPN and the applicable security standards for VPNs.

VPN—Technical Concepts and Enabling Technologies

A VPN is essentially a software technique to securely route private, un-routable traffic on the public Internet. Three functions form the basis of a VPN:

1. Packet encapsulation (“tunneling”)
2. Encryption
3. Authentication

(This section provides an overview of encapsulation, encryption, and authentication techniques used in a VPN. Knowing some basic VPN concepts will help the reader later understand trade-offs in selecting the right solution.)

People sometimes consider network Quality of Service (QoS) as another VPN requirement. This function refers to network performance, response time, availability, packet loss, etc. However, the implementation of the network QoS is a responsibility of the ISPs, and the user will have to monitor and manage QoS for any VPN that spans multiple service providers. Attaining end-to-end QoS is a complex task for the ISPs and, besides technology, also requires agreements among ISPs on QoS parameters. While there are some VPN products that claim QoS implementation through the customer-premise equipment, these devices have no impact on the network QoS. They essentially manage traffic priorities through queuing mechanisms that control the release of packets to the network. While this may be an important consideration for some customers (with under-capacity routers and low-speed links), this QoS has nothing to do with end-to-end network level QoS. Instead, if QoS is an important criterion for VPN selection, it's often best to actually separate the QoS requirement from the VPN requirements, thus obtaining the maximum flexibility while still guaranteeing the service levels needed. For example, if QoS is important, select a

single ISP that can provide an adequate SLA for network performance, and then select the most cost-effective, manageable, and flexible VPN solution separately.

The Scope of Encapsulation and Encryption

Figure 5 shows general layout of an IP packet. Each part of the IP packet has security exposures if sent in the “clear” over the Internet.

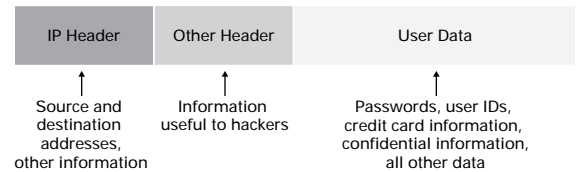


Figure 5: IP packet and security threats

1. IP Header: Among other information, it includes addresses of the source and destination of the packet. By capturing these addresses, a hacker can learn the addresses of target servers and try to set up unauthorized communications with them. A hacker can also learn the addresses of authorized users and use these addresses to act as an authorized user.

We can encrypt the addresses but that creates a problem on the Internet because routers look at these addresses to route packets to their correct destinations. We will see how encapsulation solves this problem.

Tunnel Mode: When the IP header above is encrypted and is encapsulated in another IP header, the mode of transmission is referred to as the tunnel mode in the IP Security (IPSec) standard.

2. Other Headers and User Data: Other headers contain information used by hackers to attack an enterprise's Web sites and, therefore, must be encrypted before traveling over the Internet.

The User Data part of the packet, of course, contains not only all of an organization's business data but also its user IDs and passwords.

Thus, we need to encrypt the entire packet when transmitting packets over the Internet.

Encryption Concepts

Virtual private networks ensure the privacy of information by using encryption. Encryption is a technique for scrambling and unscrambling information. The scrambled information is called cipher-text and the unscrambled information is called clear-text.

In a VPN, when information is sent from one location to another, the VPN Gateway at the sending location pulls information off the LAN and encrypts the information into cipher-text before sending the encrypted information on the Internet. The VPN Gateway at the receiving location decrypts the information into clear-text and puts the decrypted information on the LAN.

It used to be that encryption was made secure by keeping the encryption algorithm a secret. The problem with this approach is that once someone cracks the algorithm, that person has access to all the information that has ever been encrypted with that algorithm. Furthermore, since the encryption algorithm is a secret, it's hard to tell how good the algorithm is because only a few people test it.

Today, encryption algorithms are published so that everyone knows how they work. Popular published encryption algorithms include the Data Encryption Standard (DES) and Blowfish. If the algorithm isn't secret, how are secrets kept? The answer is keys.

Keys

A key is a secret code that is used by the encryption algorithm to create a unique version of the cipher-text. One way to think about it is that the encryption method is like a combination lock that is purchased at the hardware store and the key is the combination that comes with that lock. Even though many buyers each purchase the same lock, it doesn't mean that they have access to each other's tool shed.

So security is no longer dependent upon keeping the encryption algorithm a secret; it now depends on keeping the key a secret.

Key Lengths

When working with well-known encryption algorithms the security strength depends on the length of the keys used. An 8-bit key provides 256 combinations (two to the eighth power). A 16-bit key provides 65,536 combinations (two to the sixteenth power). And so on.

With a 16-bit key, someone could make 65,536 attempts before finding the combination that would unlock his/her cipher-text. With people, this would be impractical, but with computers, it wouldn't take long to run through the possible combinations. Many VPN products use 168-bit keys to encrypt data. A 168-bit key creates 374,144,419,156,711,000,000,000,000,000,000,000,000,000 possible combinations. Even fast computers would take years to try all these.

Still, it's not enough to use long keys. As with the encryption algorithm, once someone has the key, he/she has access to all the information that has ever been encrypted with it. Fortunately, with keys, one can routinely change the key so that even if someone has the key, it would only be useful for cipher-text encrypted with that key. The length of time a key is used is called a crypto-period.

Symmetrical or Private Keys

When the same key is used both to encrypt and to decrypt information, the key is called a symmetrical key. Symmetrical keys require users of a VPN to possess (share) the same key at each end of the connection. Because the key is shared, symmetrical keys are frequently referred to as shared secrets. As the name suggests, these keys work as long as it is only the authorized parties who know the key. These parties take the appropriate steps to keep the key secret. One of the problems with secret keys is distributing them to authorized users. Obviously, these keys cannot be sent over the Internet because of the public nature of the Internet.

Asymmetrical or Public Keys

Another class of keys allows information to be encrypted with one key and decrypted with a different key. Information encrypted with the first key cannot be decrypted with the same key and vice versa. These key-pairs are called asymmetrical keys.

With asymmetrical keys, one key is called the public key and the other is called the private key. The public key is made available to anyone—it is not secret. The private key is secret and it is only known by its owner. If someone wants to send information that only an intended person can see, the information is encrypted using the target's public key. That private key has the property that only it can decrypt the cipher-text created using the public key!

On the flip side, if a user wants to be certain that a message was from a known person, the message would have been encrypted using a private key. The message is then decrypted using the public key. If the message decrypts correctly, it must have come from the originator.

Asymmetrical keys get us around having to distribute and manage secret keys.

Authentication Concepts

Authentication answers the question “Are you really who you say you are?”

There are two types of authentication: User/System authentication and data authentication.

User/System Authentication: This is the way of verifying that the person or system is indeed who the person or system claims to be. A common technique for authentication is for each side to “challenge” the other side by sending a random number. The challenged side returns a value to the challenger by encrypting the random number using a key that should only be known to the challenged side. The challenger decrypts the returned value and if the decrypted value matches the original random number, the challenged party is treated as authentic.

Data Authentication: This verifies that a packet has not been altered during its trip over the Internet. A typical technique is for the sender to calculate a number, called a hash, based on the data content and to append the hash to the data packet. This is done prior to encryption. The receiver decrypts the packet. The receiver then calculates the hash independently and compares this receiver-calculated hash with the hash appended to the data. If the two hashes do not match exactly, the data was altered and the receiver rejects it. The hash is calculated using a mathematical function called a hash function. Hash functions have the property that they spit out a unique number (“hash”) for each unique bit string that is fed into them.

Encryption Algorithms

The Data Encryption Standard (DES) is a commonly used and thoroughly tested encryption algorithm. The DES system uses 56-bit symmetric keys to encrypt data in 64-bit blocks. The 56-bit key provides 72,057,594,037,927,900 possible combinations. A per-

sonal computer would take about 20 years to run through this many combinations. However, an organization with millions of dollars worth of computers could run through this many combinations in about 12 seconds. So DES makes information safe from casual attacks by hackers, but not from a focused attack by a well-funded organization.

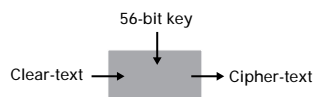


Figure 6: DES with 56-bit key

Triple-Pass DES is a DES system that encrypts information multiple times. With triple-pass DES, the data is encrypted once using a 56-bit key. The resulting cipher-text is then decrypted using a second 56-bit key. This results in clear-text that doesn't look anything like what was originally encrypted. Finally, the data is re-encrypted using the first key. This technique of encrypting, decrypting and encrypting is referred to as EDE. It effectively increases the key length from 56-bits to 112-bits.

3DES is an encryption algorithm that provides better security than triple-pass DES. With 3DES, the data is encrypted, decrypted and encrypted again (EDE), but with three different keys. This results in an effective key-length of 168-bits.

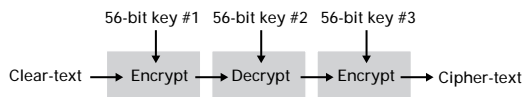


Figure 7: 3DES with 56-bit key yielding effective key length of 168-bits

VPN Protocols

This Guide has referenced the IPSec protocol as the Internet standard protocol for tunneling, encryption and authentication. IPSec is widely supported as the protocol for VPN implementations. There are two other protocols, available as alternatives to IPSec. These two protocols were developed as tactical solutions while the IPSec protocol was being developed. IPSec is widely available now but the other protocols are still used. Each of the three protocols is discussed below:

1. IP Security (IPSec)

IPSec is the security standard for the Internet. It allows for encryption and authentication. The general layout of IPSec-encoded packets is shown in Figure 8.

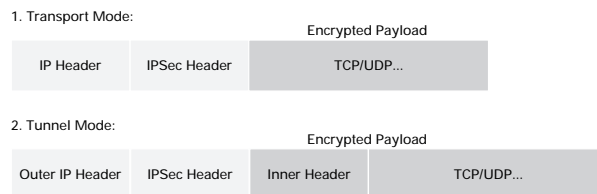


Figure 8: Encryption modes for IPSec

As shown in Figure 8, IPSec defines two modes of encryption: transport mode and tunnel mode. In transport mode, the original source and destination addresses of the header are used and are not encrypted. This makes transport mode appropriate for use over a LAN. Tunnel mode is more appropriate for use over the Internet. In particular, tunnel mode permits the routing of normally un-routable private addresses over the public Internet. In both cases, the IPSec header contains authentication information and other information needed to decrypt the packet.

2. Layer 2 Tunneling Protocol (L2TP)

L2TP was developed to merge two earlier protocols, the Layer 2 Forwarding (L2F) protocol and the Point-to-Point Tunneling Protocol (PPTP). L2TP is a protocol for putting a wrapping on non-Internet protocols such as IPX, SNA and AppleTalk, in an IP envelope, for encryption purposes. By itself, L2TP does not provide an encryption function and L2TP depends on IPSec (or some other scheme) for encryption.

3. Point to Point Tunneling Protocol (PPTP)

PPTP is a Microsoft proprietary encryption and authentication protocol. PPTP was supposed to have been replaced by L2TP, but Microsoft retains PPTP as its way of supporting VPNs in Microsoft Windows products. PPTP uses RSA instead of DES or 3DES for encryption. RSA is a weaker security algorithm than IPSec's 3DES.

Of the three protocols, IPSec, besides being the Internet standard for tunneling, encryption and authentication, has the most industry momentum and is implemented by the greatest number of vendors. There are numerous IPSec implementations available for all Windows environments. This Guide recommends IPSec as the preferred protocol for implementing VPNs.

What it all Means

While selecting and implementing a VPN solution, a user may get involved in selecting keys and encryption algorithms. At a minimum, they know the key types and encryption algorithms supported by a product. Some products require great involvement and great expertise in security details. Large businesses have complex security requirements and they benefit from the ability to customize and set every detail. Most small and medium-sized businesses do not have the need, the money, the skills, or the time to tweak every possible

VPN security setting. These businesses often prefer a solution that shields them from the internal operation of encryption algorithms and key structures.

With expanding business relationships, even smaller companies want to have e-business links with the broadest set of partners. And they want an easy way to do this. The solution these businesses pick should not require them to have certain types of network equipment (like firewalls and routers) and should not specify the type of Internet connections they use or require them to use a particular ISP.

VPN Implementation Alternatives

There are many VPN solutions available. They cover a range of price-performance, of capacity, and of installation and configuration complexity. Since VPNs are relatively new, the way of comparing products and solutions is not mature either. To provide a framework for evaluating VPNs, this Guide divides VPNs into the following categories:

1. Traditional or legacy VPN products
2. Outsourced VPNs
3. Low-end VPN/firewall products
4. Point-and-Click VPN services

Traditional or Legacy VPN Products

Most first generation VPN products fall in this category—The VPN function is typically an add-on to a router, to a LAN switch, or to a firewall. These include products from vendors such as Lucent, Cisco, Nortel, and Checkpoint. These products are optimized for

large businesses. When such a customer adds VPN functionality it often means an upgrade to a new router/switch/firewall model that supports VPN as an add-on feature. Once the customer buys the right model, the customer then physically installs and logically configures the router/switch/firewall. The customer then configures VPN configurations at central and at remote sites and for mobile and remote users.

The legacy VPN products category includes PC-based (Windows and Linux) software solutions targeted at smaller users. For these, a user installs the operating system and the networking support and then installs and configures the VPN support. Configuring the VPN support means defining security policies and key structures for VPN gateways and clients for mobile and remote users.

These VPN solutions need significant expertise to design, install, operate, support, and maintain.

Outsourced VPNs

There are three subcategories:

1. VPN service from an ISP or NSP
2. Managed VPN service from a reseller/solution provider
3. Consultant/Systems Integrators' VPN implementation services

VPN Services from an ISP or NSP

More and more ISPs and network services providers (NSPs) are providing VPNs as a service. With a managed service offering, the service components include installation of servers, installation of clients and ongoing technical support. The customer is involved with defining security policies and with the overall VPN design.

An important issue here is the availability of the managed VPN service in all the geographic areas where a customer wants to deploy their VPN. For example, regional Bell companies typically limit coverage to their operational and high-speed access providers. This may impose technological limitations. A DSL-based provider would exclude cable-users and vice versa. For example, AT&T's broadband access-services are based on cable-TV and most regional telephone companies and other providers are based on DSL. These restrictions could force one to use multiple service providers, each with its own systems administration, configuration, ordering, provisioning, and technical support. The customer would be responsible for identifying and resolving interoperability. For example, if one goes with a DSL-based ISP, how do employees with cable modems access the VPN? And with multiple ISPs one has to manage interoperability among the service providers.

Given the internal cost structure of these service providers, their services tend to be on the high end of the VPN price range and their services tend to focus on large customers. ISPs and NSPs are not known for rapidly adopting new technologies or for rapidly responding to changing customer needs.

Managed VPN Service from a Reseller/Solution Provider

These solution providers package services from multiple service providers to provide a solution covering all geographical areas. While these providers offer more flexibility than a single ISP/NSP solution, the fact remains that no single solution provider covers all possible geographic locations, covers the broad range of access technologies and maintains reasonable cost. Cost, availability in all desired locations, and technical support are the criteria for evaluating these total service solution providers.

Consultant/Systems Integrators' VPN Implementation Services

An enterprise may build their own VPN buying professional services from systems integrators and consultants. There are three phases in VPN deployment:

1. Needs-analysis, product evaluation and selection
2. Initial VPN design, configuration and rollout
3. Ongoing technical support

A business may outsource one or more of these phases. The cost of doing this and the number of new employees needed depends on the number of tasks outsourced. Small and medium-sized enterprises should contract all three phases. This could lead to high recurring charges for VPN deployment. There is also the challenge of finding the right consultant/systems integrator for the technology to be implemented.

Low-end VPN/Firewall Appliances

Low-end VPN firewall appliances are designed for small and medium-sized businesses and are purpose-built (dedicated to VPN gateway function). These appliances may use PC processors or specialized processors. Operating systems may be Microsoft Windows, Unix/Linux or a proprietary operating system. These appliances may incorporate co-processors for off-loading the encryption function to a separate chip.

These devices are called appliances due to their standalone nature. However, these appliances still have to be configured and maintained with the same level of resources as traditional VPN devices. These appliances may include additional functions such as a firewall, increasing their complexity. Appliance VPN boxes are simpler than router or firewall-based VPNs and, therefore, may be less prone to problems, easier to diagnose

and require less technical support. The recurring-costs model for appliances is similar to the cost model for traditional VPN products. Many appliance designs are based on proprietary chips and could run into future scalability problems due to the high cost and long development cycles for new chips.

Point-and-Click VPN Services

This is a relatively new category among VPN solutions. This solution is independent of the ISP and allows customers to use existing equipment or generic PCs as the hardware. One example of a service provider who delivers such solutions is OpenReach.

The key characteristic of this solution is that the customer does not have to get involved in designing, configuring, and supporting the VPN.

To deploy a VPN with this approach, for example, the customer simply logs onto the service provider's Web site and registers basic information about each site that is to be part of the VPN (such as site name and IP address). The Network Operations Center then automatically creates appropriate VPN configurations based on the user-provided information and downloads this information to a floppy disk that can be installed on a PC at each location. The user simply plugs the diskette at each site in a standard PC, reboots, and now has a VPN gateway that automatically registers itself with the Network Operations Center. The VPN administrator or user can then simply use a Web browser to "point and click" the connections among the registered VPN gateways, thereby creating secure, transparent IPSec tunnels among each remote location. In addition, the solution provider uses a Web-based control center that monitors the health of VPN gateways and provides technical support for the customer. The customer data does not flow through the vendor's network control center, but directly between the remote locations as needed. The customer billing is based on

the bandwidth required for the VPN connection (i.e., cable modem, DSL, T1, etc.) Since this type of solution uses standard PCs and free software, there is essentially no up-front investment required, and thus the potential risk is significantly less than many other types of VPN solutions. In addition, unlike most outsourced VPNs, “point and click” VPNs are not tied to a single service provider, allowing customers to mix and match Internet access types and ISPs (cable modems and DSL, for example).

Key Features and Cost Elements for a VPN Solution

There are two sets of criteria for evaluating VPN solutions: basic VPN functions and total cost of ownership (TCO). The basic VPN functions are for comparing products based on current technical requirements. However, the TCO criteria show long-term cost differences of one solution over the other.

Functional Evaluation

Table 1 lists criteria for functions of a VPN solution.

Security

IPSec Support: Is IPSec the primary security protocol supported? If IPSec is not supported, there may be future difficulties interoperating with locations and businesses using Internet standard protocols. Attention should be given to future locations and e-business partners.

Ease of Key Management: Are the types of keys, authentication techniques used and their management compatible with the customer’s security objectives? If a user has to deal with design and management of key

distribution, the solution may require technical personnel to support it. 3DES should be considered the minimum acceptable encryption level.

Performance

Packet Throughput Capacity: This is the capacity and performance data for the device. Another number often included in product specifications is the number of tunnels handled by the device. The theoretical number of tunnels handled by a device is typically very large but is not very useful in assessing the performance of the device. Packet throughput capacity, rather than the number of tunnels, is the true measure of a device’s performance.

Availability and Reliability: The device or service should be reliable enough to provide 99.9% or higher availability.

Hardware vs. Software Encryption: Encryption can be performed either through software or through hardware. While this is often considered important, it does not provide a direct measure of a product’s performance. Look instead at the product’s packet throughput capacity.

	Solution 1	Solution 2	Solution 3
Security			
IPSec Support			
Ease of Key Management			
Performance			
Packet Throughput Capacity			
Availability/Reliability			
Interoperability			
Access/Connectivity			
Service Coverage			

continued next page

	Solution 1	Solution 2	Solution 3
Platform Type			
Hardware/Appliance			
Add-on Feature to Firewall or Router/Switch			
Operation and Management			
Web-based Management System			
Management Reports			

Table 1: Functional criteria for selecting a VPN solution

Interoperability

Does the solution interoperate with any existing firewall that a customer might have? This will provide a secure mechanism for interoperating with current and future business partners.

Access/Connectivity: Does the solution handle a variety of connectivity choices, including dial-up, leased line, T1/E1, DSL, and cable to meet a customer's current and future needs? For many customers, wireless access is already important as well. The solution chosen must be flexible enough to support the types of Internet connectivity technology a customer needs at each location, and whatever type of connectivity technology the customer envisions deploying in the future.

Service Coverage

This issue applies to VPN as a service from ISPs/NSPs, and total service solution providers. Is the VPN service available in every location where the customer is conducting business or plans to conduct business, and in every location where the customer has partners or potential partners? The service levels and the time that it takes to make additions and changes to the service should be consistent with the customer's business objectives.

Platform Type

Hardware/Appliance: Is the internal hardware architecture transparent to the user? PC-based network appliances are not the same as an ordinary PC. Do not assume, for example, that one could employ a generic PC as a backup device for a PC-based network appliance. Also, the economies of scale of a generic PC are vastly different from that of a PC-based VPN appliance.

Add-on Feature to Router/Switch/Firewall: If VPN is an add-on feature to an existing platform, the reliability and the performance record of the platform should be known to the customer. This option allows the use of an existing device for the VPN. However, as discussed under TCO considerations, this may not be the optimal choice for a customer.

Operation and Management

The operation and management of the VPN is certainly the customer's responsibility for 'build-it-yourself' VPNs. Even for an outsourced solution, customers would certainly want to monitor the health and performance of their VPN. Certain outsourced solutions may require significant customer involvement with configuration details. This would add to the TCO of the solution.

A Web-based management and monitoring system is preferable over non-Web-based systems since it can be accessed from anywhere on the Internet. However, not all Web-based interfaces have equal ease of use. A customer certainly should go through a demonstration of the management system.

The quality of the reports from the management system is important. The reports should be easy to create, customize, and understand.

Total Cost of Ownership (TCO)

As pointed out, the functions discussed in the previous section provide a short-term view. Use TCO to

select a solution from a set of products with similar basic VPN capabilities. Table 2 lists the important elements for calculating TCO.

Basic Costs: These are calculated based on vendor fee and on equipment price. One item that warrants discussion is the additional cost of a hardware and software upgrade if the VPN is an add-on feature to an existing in-house router/switch/firewall. When an administrator adds another function to an existing platform, the complexity of maintaining that platform increases and the performance degrades. Multi-function platforms also are prone to more crashes and “glitches”. Make sure you account for these costs under additional costs for personnel, flexibility, and reliability.

Additional Costs: These include indirect costs but form the major part of the TCO.

Personnel costs should include loaded salaries and infrastructure (office space, furniture, telephone, desktop, and networking) and recruitment costs for technical people and management.

	Solution 1	Solution 2	Solution 3
Basic Costs			
Annual fee			
License fee, if hardware/appliance or software solution			
Service fee, if outsourced			
Annual software license/rental fee			
Cost of additional hardware and hardware upgrade (if add-on to firewall/router/switch)			
Additional Costs			
Personnel/professional services cost for initial design and deployment			

continued next page

	Solution 1	Solution 2	Solution 3
Annual personnel/professional services cost for ongoing management and maintenance of VPN			
Interoperability and Flexibility - Opportunity cost for not being able to connect with customers and business partners in a timely manner			
Reliability and Availability— Opportunity cost for downtime (planned and unplanned)			

Table 2: Total Cost of Ownership for a VPN

Interoperability and Flexibility: These costs include the cost of lost business if one cannot connect or interoperate with customers, business partners, and their systems in a timely manner.

Reliability and Availability: These are costs of unproductive employees and of lost transactions due to system unavailability.

Selecting the Right VPN Solution

The range of VPN solutions frustrate customers trying to compare the solutions. This is especially true for customers in small and medium-sized businesses. These businesses have neither the resources nor the time for a drawn-out evaluation. By focusing on the long-term IT and networking strategy and by using a TCO framework, customers can simplify and rationalize the evaluation and can eliminate the theoretical possibilities.

Build vs. Outsource

Before developing a detailed list of technical, functional, and other requirements, a customer must decide whether they want to build their own VPN solution or they want to outsource it. This needs to be answered even when customers have in-house installed firewalls and routers for which a VPN is available as an optional feature.

A build-your-own solution has the following characteristics:

- More control and customization
- Capital investment
- In-house IT and networking personnel and resources
- Long development cycles and greater lost-opportunity cost

An outsourced solution has the following characteristics:

- No capital investment
- No in-house personnel and other resources needed to manage the technology
- Ease of expansion and changes
- Ease of migration to new technologies

For small and medium-sized businesses and, increasingly, for large businesses too, the IT trend is towards outsourced services. Businesses want to focus on the “business-of-the-business” and providing internal IT services is becoming a distraction.

For VPNs, if a customer can find an outsourced solution that meets his/her functional requirements and is flexible enough to support their future needs, outsourcing is a better solution than a build-your-own solution.

For a more specific and detailed cost/benefits analysis of implementation alternatives, a user should use Tables 1 and 2.

Conclusion

The ability to use the Internet in a secure manner is the foundation of e-commerce. A VPN is the key to attaining that objective. Not only do VPNs provide security across the Internet, they can eliminate expensive intranets and EDI networks.

There are numerous solutions available for implementing a VPN. Small and medium-sized businesses will find that, more often than not, building their own solutions, even as add-on features to existing in-house solutions, will be more expensive and less compatible with their business objectives in the long run.

For the outsourced solutions, managed VPN services from network services providers are no longer the only option for customers. Customers should compare emerging services such as point-and-click VPN services and network service provider VPN solutions. A point-and-click solution may not only cost less than the alternatives, but also provide greater flexibility and more scalability to reach customers and business partners worldwide.

Glossary of Terms

Asymmetrical Keys—The use of a key pair. One key is used to encrypt the information, the other is used to decrypt it.

Authentication—Verification of the identity of specific users or systems.

B2B—Business-to-Business transactions over the Internet.

B2C—Business-to-Consumer transactions over the Internet.

Certificates—A unique private key which identifies a user or system to another user or system which also holds its own unique certificate.

Crypto Period (encryption period)—Length of time for which the encryption keys are held valid.

Data Encryption Standard (DES)—A commonly used standard for encrypting data over the Internet. DES, or Standard DES, has a 56-bit key length.

3DES—A variation of the DES algorithm which uses 3 keys. One to encrypt, a second to decrypt, and a third to encrypt again. The result is effectively a 168-bit key length.

Digital Subscriber Loop (DSL)—A digital telephone link to the user premises, which allows very high speed connections, 10 to 20 times greater than the 56 Kbps modem, to the Internet.

EDE—Encrypt, Decrypt, Encrypt. Method used in the Triple-Pass DES and 3DES encryption algorithms.

Electronic Data Interchange (EDI)—A technique for exchanging transaction-related and other data between businesses based on formats and standards defined by an industry group or a corporation. Most

EDI standards pre-date the Internet and are not based on the Internet standards.

Encryption—The use of a mathematical algorithm and keys to scramble and unscramble information so that it is not translatable by the naked eye.

Extranet—The extension of a private corporate network to allow connectivity with partners and customers.

Firewall—A device or piece of software which employs rules to specify that communication from a specific location or individual, or of a specific protocol, can or cannot enter the network.

Intranet—An organization's private network typically based on TCP/IP protocol.

Internet Protocol (IP)—The routing and addressing part of the TCP/IP protocol suite.

IP Security (IPSec)—The name of the standard for secure communications over the Internet. Defines framework for authentication, encryption and managing encryption keys.

ISP—Internet Service Provider

LAN—Local Area Network

Layer 2 Forwarding (L2F)—An earlier, proprietary Cisco protocol for secure communications over the Internet, replaced by L2TP.

Layer 2 Tunneling Protocol (L2TP)—An amalgamation of two proprietary protocols, L2F and L2TP, PPTP, for secure communications over the Internet. Proposed as an alternative to IPSec, but IPSec remains the dominant protocol for secure communications over the Internet.

Mesh-connected (fully meshed network)—A network whereas every entity in that network can access any other entity within that network.

Network Address Translation (NAT)—Used to convert, or translate, an address on one network to an address which will be usable on another network.

Network Services Provider (NSP)—Differs from an ISP in that it also provides services other than Internet access.

Packet Encapsulation—The placement of one packet into another packet, thereby hiding the original addressing information and data.

Point-to-Point Tunneling Protocol (PPTP)—A proprietary protocol used by Microsoft as an alternative to IPSec for secure communications over the Internet.

Public/Private Key Pair—The public key in a key pair is not kept secret. The private key, held by one individual, is kept secret.

Quality of Service (QoS)—Defines or measures the quality of expected Internet connectivity or services. QoS specifications typically include parameters such as network availability, restoration time, number of dropped packets, end-to-end delay.

Remote Access Server (RAS)—A device to support dial-in connections from remote users.

Symmetrical keys—The use of the same key to encrypt information and decrypt that same information.

Total Cost of Ownership (TCO)—Includes, in addition to initial purchase price of hardware and software, additional one-time and recurring costs such as installation, support, loss of productivity and opportunity costs. Reflects the true cost of product or service over a period of time.

Transmission Control Protocol (TCP)—A reliable protocol for application-to-application communications over the Internet.

Triple-Pass DES (Triple DES)—A variation of the DES algorithm which uses 2 keys. The first key encrypts the data, the second decrypts the data, and the first is used again to re-encrypt the data. The result is effectively a 112-bit key length.

Tunnel Mode—Mode of IPSec which enables the secure transfer of data across the wide area network inside a tunnel.

User Datagram Protocol (UDP)—An unreliable protocol for application-to-application communications over the Internet.

Virtual Private Network (VPN)—The use of the Internet as if it were a private network through the use of encryption and authentication techniques such as IPSec.

WAN—Wide Area Network

This **Technology Guide** is one in a series of topic-focused Guides that provides a comprehensive examination of important and emerging technologies.

This series of Guides offers objective information and practical guidance on technologies related to Communications & Networking, the Internet, Computer Telephony, Document Management, Data Warehousing, Enterprise Solutions, Software Applications, and Security.

Built upon the extensive experience and ongoing research of our writers and editorial team, these Technology Guides assist IT professionals in making informed decisions about all aspects of technology development and strategic deployment.

techguide.com is supported by a consortium of leading technology providers. OpenReach has lent its support to produce this Guide.

Visit our Web site at **www.techguide.com** to view and print this Guide, as well as all of our other Technology Guides.

This is a free service.

produced and published by



visit www.techguide.com™