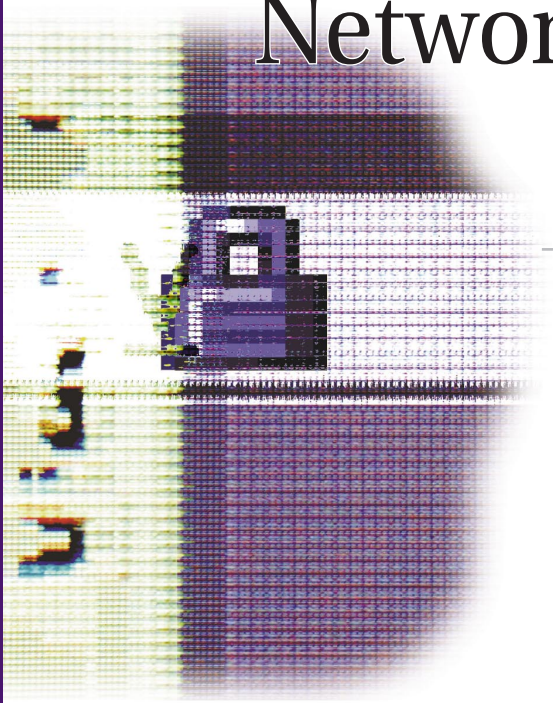
A Technology Guide from ADTRAN

Understanding

Virtual Private Networking

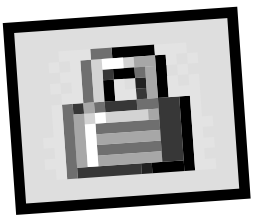


ADTRAN

Understanding

Virtual Private Networking

Introduction

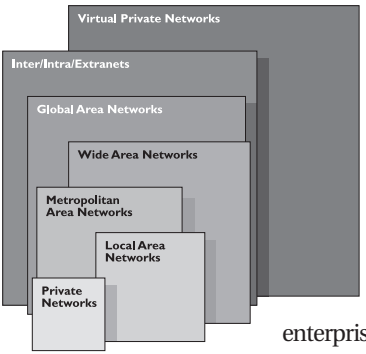


Enter another no-brainer application for the Internet environment: Virtual Private Networks (VPN). It's a no-brainer in terms of its low-cost, easy-to-implement, and convenient solution for mobile and remote business networking. However, the technology it employs is nothing short of brilliant.

This primer is written as a high-level overview of VPN to introduce less technical readers to this innovative WAN application. The publication is divided into four major sections: VPN History, VPN Technologies, VPN Applications, and VPN Products. Armed with this information, you should be well-poised for educated inquiry into the VPN service option for your own remote networking implementations.

VPN History

The term VPN has been associated in the past with such remote connectivity services as the public telephone network and Frame Relay PVCs, but has finally settled in as being synonymous with IP-based data networking. Before this concept surfaced, large corporations had expended considerable resources to set up complex private networks, now commonly called Intranets. These networks were installed using costly leased line services, Frame Relay, and ATM to incorporate remote users. For the smaller sites and mobile workers on the remote end, companies supplemented their networks with remote access servers or ISDN. At the same time, the small- to medium-sized enterprises (SMEs), who could not afford dedicated leased lines, were relegated to low-speed switched services.



Corporate networking has come a long way in a relatively short time.

As the Internet became more and more accessible and bandwidth capacities grew, companies began to offload their Intranets to the web and create what are now known as Extranets to link internal and external users. However, as cost-effective and quick-to-deploy as the Internet is, there is one fundamental problem – security.

Today's VPN solutions overcome the security factor. Using special tunneling protocols and complex encryption procedures, data integrity and privacy is achieved in what seems, for the most part, like a dedicated point-to-point connection. And, because these operations occur over a public network, VPNs can cost significantly less to implement than privately owned or leased services.

Although early VPNs required extensive expertise to implement, the technology has matured already to a level that makes its deployment a simple and affordable solution for businesses of all sizes, including SMEs who were previously being left out of the e-revolution.

Understanding

Virtual Private Networking

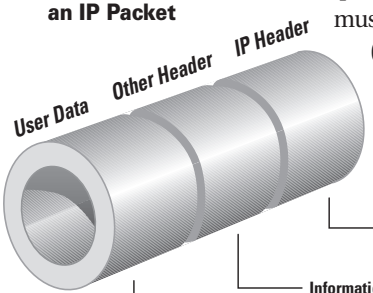
Using the Internet, companies can connect their remote branch offices, project teams, business partners, and e-customers into the main corporate network. Mobile workers and telecommuters can get secure connectivity by dialing into the POP (Point-of-Presence) of a local ISP (Internet Service Provider). With a VPN, corporations see immediate cost-reduction opportunities in their long distance charges (especially important to global companies), leased line fees, equipment inventories (like large banks of modems), and network support requirements.

VPN Technologies

Whether you implement your own VPN or outsource to your ISP (more about that later), you'll want to be familiar with the basic technologies involved.

The Internet is a shared public network of networks with open transmission protocols. Therefore, VPNs must include measures for packet encapsulation (tunneling), encryption, and authentication to ensure that sensitive data reaches its destination without tampering by unauthorized parties.

Anatomy of an IP Packet



Source and destination addresses, other information

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 impersonate authorized clients.

Information useful to hackers

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

Passwords, user IDs, credit card information, confidential information, all other data

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

Companies using an Internet VPN establish links to the local access points of their ISP. From here, they let the ISP ensure that the data is transmitted to the appropriate destinations via the Internet, leaving the rest of the connectivity details to the ISP's network and the Internet infrastructure.

Firewall:

A firewall is an important security feature for any Internet user. Available in software or standalone hardware forms, a firewall prevents unauthorized users and/or data from getting in or out of your network, using rules to specify acceptable communications from locations, individuals, or in certain protocols. However, firewalls do not protect your data from threats within the Internet network itself. Once the data gets outside your firewall, your user names, passwords, account numbers, server addresses, and other sensitive information are visible to hackers. VPN tunnels, enabled by encryption algorithms, give you the ability to use the public, shared Internet for secure data transmission after it leaves the protective custody of your firewall.

Tunnels:

The thing that makes a Virtual Private Network "virtually private" is a tunnel. Even though you access your network via the Internet, you're not really "on" the Internet, you are actually "on" your company network. Although the term "tunnel" feels like it's describing a fixed path through the Internet, this is not the case. As with any Internet traffic, your VPN tunnel packets may take different paths between the two endpoints. What makes a VPN transmission a tunnel is the fact that only the recipients at the other end of your transmission can see inside your protective encryption shell, sort of a "tunnel vision" idea.

Tunneling technology encrypts and encapsulates your own network protocols within Internet protocol (IP). In this way, you can route and bridge, enable filters, and

deploy cost-control features the same way as any of your other traditional WAN links. So, not only is the Internet-based VPN transmission transparent to your users, it is virtually transparent to your network management operations, as well.

Encryption:

Encryption Algorithm:
mathematical function that establishes the relationship between the encrypted message and the decrypted message.

Encryption is a technique for scrambling and unscrambling information. The unscrambled information is called clear-text, and the scrambled information is called cipher-text. At either end of your VPN tunnel sits a VPN gateway in hardware of software form. The gateway at the sending location encrypts the information into cipher-text before sending the encrypted information through the tunnel over the Internet. The VPN gateway at the receiving location decrypts the information back into clear-text.

In the early days of VPN tunneling, companies kept their encryption algorithms secret. Unfortunately, once it was cracked, all the information ever encrypted with that formula became vulnerable. Therefore, the industry began publishing well-known and well-tested encryption algorithms, such as the popular Data Encryption Standard (DES).

But, if everyone knows the encryption algorithm, how is the data kept secure? The answer: keys.

DES and 3DES

The Data Encryption Standard (DES) 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. This sounds impressive, and it would take up to 20 years for typical business computers to run this many combinations. But, more focused, well-funded hacker organizations with a bigger inventory of powerful computers could break it in about 12 seconds. DES has been developed even further with its 3DES ("triple-DES") system that encrypts information multiple times. For example, with 3DES, 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 a third 56-bit key. This technique of encrypting, decrypting, and encrypting (EDE) increases the key length from 56 bits to 168 bits.

Keys:

A key is the secret code that the encryption algorithm uses to create a unique version of cipher-text. To put it in simpler terms, two people might go to the hardware store and buy the same lock off the shelf, but their combinations are different. In VPN encryption, the method may be the same (like the lock), but our keys are different (like the combination).

Of course, VPN locks have a lot more than three numbers on the combination dial. As a matter of fact, transmission security strength depends on the length of the keys you use. Here's the formula:

- 8-bit keys = 256 combinations or two to the eighth power (2^8)
- 16-bit keys = 65,536 combinations or two to the 16th power (2^{16})
- 56-bit keys = 72,057,594,037,927,900 or two to the 56th power (2^{56})
- And so on…

In other words, if you used a 16-bit key, an intruder might have to make 65,536 attempts at cracking your combination. Obviously, this would be a quick and fairly simple task for computers. That's why a lot of VPN products on the market today are using 168-bit keys, creating 374,144,419,156,711,000,000,000,000,000,000,000,000,000,000,000,000 possible combinations. There are some enterprises out there going even higher. Even the fastest computers today would need extended time to crack a code that complex.

You might be tempted to make a policy of always using the highest-bit encryption method available, but keep in mind that processing such complicated cipher-text will require significant, dedicated CPU processing power. There are other ways to use keys to the utmost security to fit your needs. For example, it does, indeed, take time to crack the higher-bit keys. If you establish a policy of periodically changing your keys, the trespassers won't be able to keep up.

But what is a key and what does it look like?

Similar to Einstein's Theory of Relativity, there is only a handful of people who truly understand what keys fundamentally are. It involves such impressive math, that most of us just have to accept that they work. There's an entire world of standards and granularity out there that could fill libraries of technology primers. Bottom line, keys are software-generated encryption algorithms. Luckily, reliable hardware and software vendors are providing standards-based key-management features in their products that your current networking employees can be easily trained to maintain. Take care to partner with suppliers you trust.

The period of time you use a particular key is called a crypto-period. Some crypto-periods are changed at a particular volume-level of transmitted data. Some change at the beginning of each new session or even at a lull within the transmission. The danger in frequent key generation is that the likelihood of key-code disclosure increases the more you re-key. So, that's where another creative use of keys comes in handy. It involves what are called symmetrical and asymmetrical keys.

Symmetrical Keys

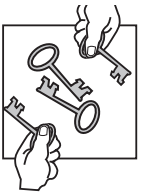
Symmetrical keys means the same key is used at each end of the tunnel to encrypt and decrypt information. Because a symmetrical key is being shared by both parties, there must be an understanding between the two to take appropriate steps to keep the key secret, which is why symmetrical keys are often referred to as "shared secrets." These keys become more difficult to distribute, since they must be kept confidential. A technique called "key splitting" may be employed to reduce the potential of key disclosure during transit. This allows participants to use public channels such as the Internet. More commonly, however, distribution of symmetrical keys is more of a manual operation using paper, removable media, or hardware docking.

Asymmetrical Keys

Asymmetrical keys are slightly more complicated, but, logistically, much easier to manage. Asymmetrical keys allow information to be encrypted with one key and decrypted with a different key. The two keys used in this scenario are referred to as private and public keys, or the ones you keep to yourself and the ones you distribute to your remote users.

Consider this example:

Let's call our businesses ACME and ABC. ACME has a set of two keys, a public key and a private key. His public key has been programmed to encrypt data so that only his own private key can decipher it. In order to communicate securely, ACME hands his public key to ABC and tells him to encrypt anything he sends with that code. Using this asymmetrical keying method, both are assured that only ACME will be able to read those transmissions because he retains the private decoder key. If the communication is to be bi-directional, ABC would share his public key with ACME in the same manner.



With asymmetrical keys, business partners trade their public keys but retain their private keys for secure two-way communications.

Key Management

Configuring pre-shared secrets in smaller VPNs does not necessarily require software automation or large infrastructure investments. However, larger networks might benefit from deploying a Public Key Infrastructure (PKI) to create, distribute, and track digital certificates on a per-user basis. You can use pre-shared keys or raw digital signatures if your equipment supports these authentication alternatives. However, if you decide to use certificates, there are options. For example, you may use third-party Certificate Authority services. Or, you may build your own Certificate Authority using software from Entrust, Xcert, or Baltimore Technologies. Either option will help you establish a comprehensive PKI, which is especially useful in large organizations needing to extend secure, limited network access beyond their own internal users to business partners and customers.

Digital Certificates:
a virtual security procedure that verifies an association between a user's public key and the user's identity and public privileges.

Authentication

The last bit of housekeeping involved in VPN transmission is authentication. At this step, recipients of data can determine if the sender really is who he says he is (User/System Authentication) and if the data was redirected or corrupted enroute (Data Authentication).

User/System Authentication

Consider, again, our two businesses named ACME and ABC. When ACME receives a message signed from ABC, ACME picks a random number and encrypts it using a key only ABC should be able to decode. ABC then decrypts the random number and re-encrypts it using a key only ACME should be able to decode. When ACME gets his number back, he can be assured it really is ABC on the other end.

Data Authentication

Hash functions create a fingerprint of your data that can be used for authentication.

In order to verify that data packets have arrived unaltered, VPN systems often use a technique involving "hash functions." A hash function creates a sort of fingerprint of the original data. It calculates a unique number, called a hash, based on fixed- or variable-length values of unique bit strings. The sender attaches the number to the data packet before the encryption step. When the recipient receives the data and decrypts it, he can calculate his own hash independently. The output of his calculation is compared to the stored value appended by the sender. If the two hashes do not match, the recipient can assume the data has been altered.

IPSec Protocol

IPSec (IP Security) is the Internet standard protocol for tunneling, encryption, and authentication. It was designed to protect network traffic by addressing basic usage issues including:

- access control
- connection integrity
- authentication of data origin
- protection against replays
- traffic flow confidentiality

The IPSec protocol allows two operational modes. In Transport mode, everything in the packet behind and not including the IP header is protected. In Tunnel mode, everything behind and including the header is protected, requiring a new pseudo IP header.

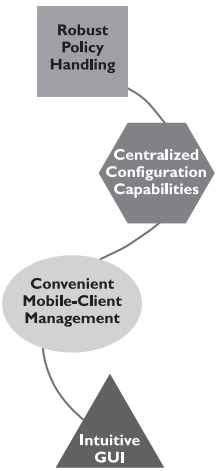
While the IPSec protocol was under development, two other protocols — L2TP and PPTP — arose as temporary solutions. L2TP (Layer 2 Tunneling Protocol) encloses non-Internet protocols such as IPX, SNA, and AppleTalk inside an IP envelope. However, L2TP has to rely on other protocols for encryption functions. PPTP (Point-to-Point Tunneling Protocol), is a proprietary Microsoft encryption and authentication protocol. Although originally developed as a temporary solution, Microsoft continues to deploy L2TP as its tunneling protocol instead of IPSec tunneling. When comparing the three, IPSec is, by far, the most widely used protocol, and the only one that addresses future VPN environments (such as new IP protocols).

Management

Understanding the operational technologies is only part of implementing a successful VPN, but the management of the devices you deploy can sneak up to be your largest investment in terms of the time and personnel required. As you can imagine, the bigger your VPN and the more granular your security policies, the more complex your management needs become.

For example, consider the seemingly simple addition of one new site to a 50-site meshed VPN. The network manager might have to manually configure each individual VPN tunnel establishing two-way communication between the new site and each of the other 50 boxes. That's 100 different policies to add a single node to a meshed network. And that's just creating the tunnel. But network managers have to plan for much more than just each workstation's IP address, they must also publish and enforce comprehensive security policies.

Security policies define acceptable access privileges, which may depend upon combinations of factors including job titles, special projects, need-to-know, and level of trust. In addition, policies should be granular enough to allow differentiation by organization, server, group, and even user levels. Keep in mind, however, that you're trying to walk a fine line between limited access and collaborative computing. Your policies should protect your resources at the highest level possible without jeopardizing employee productivity.



When evaluating VPN management software packages, look for the above.

In order to implement your VPN effectively and efficiently, device management is best handled with dedicated VPN management software. Several packages are available, but are typically associated with specific vendors' products. When evaluating these management platforms, be sure to look closely at auto-policy setting and configuration capabilities accommodating branch offices and remote clients, as well as intuitive GUI that clearly depicts your VPN map and the policies currently in place. You might also consider functionality that pulls user groups and authorizations from existing databases to reduce set-up time.

Element-Based or Policy-Based Management?

This is one area where you live by the rule, "The simpler the better." For smaller, site-to-site VPN implementations, the less expensive element-based (device-by-device) management and monitoring systems are adequate. You may even consider a hybrid middle-ground approach of element-based configuration with centralized reporting and monitoring functions. In other words, you may have to configure each individual tunnel and device one at a time. But, once established, you can centrally monitor intrusion attempts, VPN tunnel failures, concurrent tunnel reports, and software validations, without having to request the information manually, device by device.

For larger networks, centralized policy-based management is a must. With centralized policy-based systems, you have the ability to establish policies and then push them out to all the applicable devices with a single command. Not only does this save incredibly significant

amounts of time, it also prevents the increased likelihood of misconfigurations that can happen when administrators have to enter hundreds of individual commands.

Outsourced Management

Another way to deal with large-scale VPNs is to outsource managed VPN to your ISP or a Secure Application Service Provider (SASP). These services generally come in two packages: CPE-based VPNs or Network-based VPNs.

When your provider designs a VPN solution for you, installs a security gateway (firewall, router, and VPN device in some configuration) and then manages it on your behalf, it is called a CPE-based VPN. In contrast, a network-based VPN uses carrier-class VPN switches, embedded at ISP points of presence or telco central offices to support hundreds of thousands of high-speed tunnels. Creating a network-based VPN is accomplished by reconfiguring the switch instead of placing equipment at your site.

Some corporations prefer to outsource these services to providers with management infrastructures already in place. In this case, your cost lies more in recurring monthly fees rather than in capital investment. Because this is a relatively new service offering, managed services come in many shapes and prices. Shop carefully. (More information about Outsourced VPN begins on page 19.)

VPN Applications

Remote Access

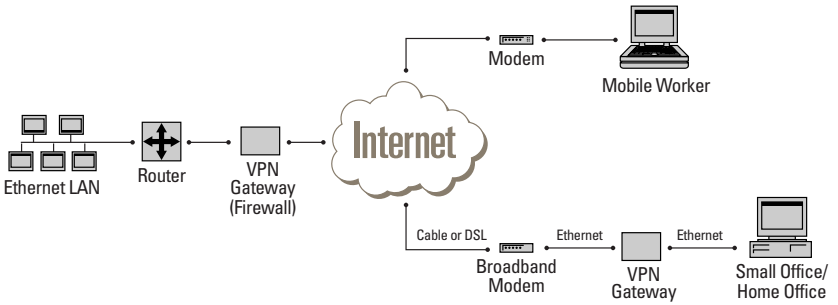
Business professionals who travel frequently or who often work at home after hours find this solution to be of great benefit to their ability to get things done. No matter where they are, secure access to their entire business is only a local telephone call away. This is also a useful solution for cases where key personnel need to be away from the office for an extended period of time.

Remote Access Before VPN

Connections for mobile and remote users have traditionally been achieved using analog or ISDN switched services. Small offices that could not afford permanent connections to the corporate Intranet would also use these dial-up technologies.

The long distance charges would be the largest cost of this type of remote connectivity. Other costs include investment in a Remote Access Server (RAS) at the central site as well as the technical support personnel necessary for configuring and maintaining the RAS.

Remote Access After VPN



Remote users can establish dial-up connections to local ISPs and connect, via the Internet, to a VPN server at headquarters. Using today's faster Internet connections (DSL or cable), employees access corporate resources at speeds well exceeding 500 kbps. Under most conditions, this is like being at a desk in the corporate headquarters building. VPN enables mobile and remote employees to work faster and more efficiently.

In this application, the VPN benefits include replacement of long-distance or 800-number services, elimination of the need for remote access servers and modems, and access to all enterprise data and applications (not just email or file transfer servers). 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.

Site-to-Site Connectivity

The global business village of today's marketplace often requires companies to establish regional and international branch offices. The options have traditionally been either to deploy dedicated leased-line services or to use the same dial-up technologies as mobile workers. In addition to the infrastructure costs attached to this scenario, businesses have also had to consider the lost-opportunity costs associated with inefficient or non-existent access to centralized information and applications.

Site-to-Site Before VPN

To connect branch offices to headquarters, businesses would previously outfit each remote location with a router that connected the campus to a backbone router over a LAN or WAN link. The remote routers also connected the branch office with the other remote locations. All these routers were often connected with a web of leased line or Frame Relay service.

The costs for this configuration included the campus and backbone routers as well as the charges for telecommunications services, most significantly, the long distance charges. The initial investment in an Intranet backbone alone might cost anywhere from $10,000 to $100,000, depending on the traffic and geographical reach.

Site-to-Site After VPN

Using a VPN solution for this application, the backbone WAN, and its associated hardware, is replaced by the Internet. Each remote location incurs the cost of an Internet connection, but even the fastest DSL, cable, and ISDN connections only cost approximately $40 per month (some ISP business rates vary and may be slightly higher). Using the Internet pipeline, you also eliminate the backbone routers and their system administration, configuration, technical support, and routing-table maintenance. Performance is also likely to be enhanced in this application thanks to the higher-speed facilities within the Internet network. The Return on Investment (ROI) for this application is quick and also provides for recurring savings.

VPN Products

You're sold, right? VPN sounds like the perfect solution for your remote connectivity. Now it's time to take a look at the shopping list. Before you make any purchases or adjustments in your operations, you'll need to investigate whether it's more appropriate for your company to implement its own VPN system or outsource it to your ISP or other network service provider.

Do-it-Yourself VPN

When implementing your own VPN, there are four basic areas to consider: the Internet service itself, a security policy server, a PKI system, and a VPN gateway solution.

Gateway products fall into two categories, standalone and integrated. Standalone VPN implementations incorporate purpose-built devices sitting between the source of the data and the WAN link. At the remote end, there may be VPN software for a mobile user's laptop, or a purpose-built encryption device between the modem and the data source at a remote office.

Integrated implementations add VPN functionality to existing devices such as the router and firewall, still complemented by remote client software.

VPN Gateway: The Router

Adding encryption support to a router can keep the upgrade costs of your VPN low. Depending on whether the functionality can be added to an existing router with software or special expansion boards, the cost might range from approximately $1,500 to $4,000.

VPN Gateway: The Firewall

Using firewalls to create a VPN is a workable solution for small networks with low traffic volume. However, because of the processing performed by firewalls, they can be ill-suited for tunneling on large networks with a great deal of Internet traffic. An integrated firewall can list from less than $1,000 up to $21,000, depending on the throughput performance you need.

VPN Gateway: The Internet Security Device

Standalone VPN devices specifically designed for tunneling, encryption, and user authentication are much easier to set up than installing software on a firewall or reconfiguring a router. Large enterprises have a variety of options in VPN devices for throughput and simultaneous

tunnel management. Small businesses or small offices without IT support staffs should look for turnkey products that incorporate VPN functions with firewall and other network services. Depending on the combinations of VPN features, Internet security device packages can cost as little as $500 or as much as $35,000 (for higher-capacity systems).

VPN Gateway: The Software

VPN software for creating and managing tunnels is available for use between a pair of security gateways or a remote client and a security gateway. These software VPN systems are good low-cost choices for relatively small tunnels that do not have to process a lot of traffic. The software can run on existing servers and share support resources with them. Software solutions are also a good stepping-off point for network managers wishing to be more familiar with VPNs. VPN software, again depending on the features included, may range from $21 per seat to $2,500 per server.

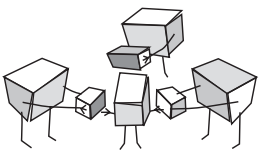
Outsourced VPN

Buying VPN service from a provider is a relatively new option. Companies without adequate support personnel, or who don't want to be distracted from the business-of-the-business, can outsource to their ISP. When researching this alternative, there are a few important considerations to remember:

- If you are connecting offices or workers in remote cities or countries, you'll need an ISP that offers POPs in those locations (keeping the Internet to a local call, rather than using toll-free connections).
- Look for providers with redundancy in equipment, connections, and people.

- Investigate your provider's policies, equipment/software, and employee qualifications for dealing with outside attacks.
- Inquire about on-site consulting assistance to help ensure you're getting the services you need based on your specific applications.

Pricing for this service is based on several factors, and different service providers package those differently. IDC published an analysis of VPN services (IP VPN Services: U.S. Market Assessment and Forecast, 1999-2004) outlining a number of pricing schemes from the leading ISPs. According to that report, pricing structures are developed based on flat-rate monthly fees, usage, and even a la carte offerings. Although the dollar amounts fluctuate with market conditions, here's a snapshot of how the prices have run and what determines them:



Outsourced VPN packages come in all shapes and sizes making the offerings a challenge to compare.

- *Provider A* offers VPN services for $10/month per user (including technical support). There is an $80 set-up fee per remote user, and the Internet connection is extra. Provider A also offers a three-year contract for T1 connection and managed VPN services for $2,300/month per site.
- *Provider B* offers a dial-up VPN plan for $2.50/hour to $4.25/hour with negotiable usage discounts.
- *Provider C* offers firewall service from $800/month for up to 25 users to $2,500/month for unlimited usage licenses. Encryption equipment rental costs approximately $250/month. A Quality of Service contract runs $1,500/month for 256-384 kbps services up to $35,000/month for T3 services. Installation fees are based on the cost of the truck roll, and DSL service costs between $129/month to $250/month.

- *Provider D* offers fully managed VPN service for $2,750/month per site. Installation costs $5,000 per U.S. site and $7,500 per international site. T1 rates were $995/month per U.S. site and $1,595/month per International site. The CPE rental fees were $995/month per site for up to 200 users and $3,300/month per site for T3 capacities.

- *Provider E* offers a variety of term contracts. The one-year VPN contract costs $950/month per site for low-capacity applications and $3,300/month per site for high-capacity applications. Connectivity port fees (e.g., $1,200/month for T1) and local loop charges are extra. Installation fees run from $500 to $1,500 per site.

QoS Note

The Internet is a complex environment with an enormous mixture of data and real-time applications moving in different paths through unknown infrastructures. You have to expect that there will be bottlenecks and congestion. QoS generally encompasses bandwidth allocation, prioritization, and control over network latency for network applications. But, the Internet is a "connectionless" technology that makes no guarantees. When you're transmitting mission-critical files that need to get to their destination without delay, QoS becomes an important part of your VPN implementation. IPv6, the next version of IP, is expected to change all that by including inherent provisions for QoS, but is not widely used as of this writing. That's why, if QoS is important for your VPN objectives, you should separate your QoS requirements from your VPN requirements. In other words, select an ISP that provides an adequate service level agreement (SLA) for your performance expectations, and then, select the most cost-effective, manageable, and flexible VPN service solution separately. As you've seen earlier, these services are available as separate products, so look closely at each requirement.

Making the Move

The question is no longer whether to migrate to an Internet-based business model, but what is the best way to set up your e-environment. With expanding business relationships, even small companies are defining and implementing their own e-strategies. In this process, they're finding that their IP communications are involving much more than just Internet access, email, and file transfer. Today, businesses need real-time exchange of mission-critical information such as procurement, supply-chain management, sales and customer relationship management, online business transactions, online access to financial institutions, etc. These applications make security over the Internet paramount. The technology that enables those objectives is VPN.

Money Drain

The average dollar amount lost per organization in the past year by type of security breach, according to a 2001 survey of 538 U.S. security professionals:

Financial fraud	**$8.0 million**
Theft of proprietary information	**$2.9 million**
System penetration by outsider	**$454,000**
Unauthorized insider access	**$276,000**
Viruses	**$244,000**
Denial-of-service attacks	**$122,000**
Laptop theft	**$62.000**

Source: Computer Security Institute/FBI, March 2001

When making your decision to move to a VPN structure, consider the key business benefits of VPN connectivity:

Lower costs

According to Infonetics, LAN-to-LAN connectivity costs are reduced 20 to 40 percent, and remote access costs up to 80 percent. For companies just setting up their remote networks, VPN also offers a low-cost alternative to investment in backbone equipment, in-house terminal equipment, and access modems.

For more information or for assistance in designing your own VPN solutions, call ADTRAN's highly-skilled pre-sales applications engineers at 800 615-1176.

Anywhere, anytime access

The ubiquitous public Internet offers remote users transparent access to central corporate systems such as email, directories, internal and external web sites, security, and other shared applications over round-the-clock local access services.

Connectivity Improvements

VPN-based links are easy and inexpensive ways to support changing business demands. Extending corporate network services to new offices or mobile workers, adding new vendors, or removing users are simple tasks that are quick to achieve.

VPN technology is maturing rapidly and represents the wave of the future for data communications. It is cost-effective and safe, and its high return on investment will likely outweigh any skittishness about investing in a new technology.

About ADTRAN®

Established in 1985, ADTRAN, Inc. is a leading provider of network deployment and access solutions for delivering today's digital telecommunications services over existing copper infrastructures.

VISIT US ON THE WEB AT:
www.adtran.com

Today, ADTRAN technologies support more than two million local loops worldwide. More than 500 ADTRAN products support all major digital technologies, including T3, T1, E1, Frame Relay, VPN, DDS, HDSL, xDSL, ISDN, and wireless transport. In the carrier network and enterprise markets, ADTRAN produces a complete end-to-end solution that provides the greatest network efficiency and lowest possible telecommunications costs.

According to Dataquest and IDC, ADTRAN holds revenue-leading positions in the Integrated Access, Frame Relay/DDS, ISDN Extension and HDSL/T1/E1 network and access markets. ADTRAN customers include the Regional Bell Operating Companies, interexchange carriers, GTE, domestic independent service providers, corporate end users, international customers and original equipment manufacturers.

CORPORATE OFFICE
ADTRAN, Inc.
901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000

800 9ADTRAN
256 963-8000
fax: 256 963-8699
fax back: 256 963-8200
e-mail: info@adtran.com
web site: www.adtran.com

REGIONAL OFFICES
Chicago, IL 800 436-4217
Seattle, WA 800 390-1573
Washington, DC 800 794-9798

FIELD OFFICES
Atlanta, GA 800 289-0966
Chicago, IL 800 471-8655
Columbus, OH 888 865-2237
Dallas, TX 800 471-8648
Denver, CO 800 471-8651
Irvine, CA 800 788-5408
Kansas City, KS 800 471-8649
Los Angeles, CA 888 223-7668
Nashville, TN 888 223-7657
New York, NY 800 471-8657
Portland, OR 888 223-7660
Richmond, VA 800 689-9915
San Jose, CA 888 223-7655

INTERNATIONAL CONTACTS
Beijing, China 8610 8529-8895
Canada 1 877 923-8726
Germany 49 6007 930-203
Hong Kong 852 2824-8283
Latin America 1 954 474-4424
London, U.K. 44 1252 626-730
Melbourne, Australia 61 3 9658-0500
Mexico/Caribbean 1 954 577-0357
Zürich, Switzerland 41 1 880-2777

EN286A September 2001

ADTRAN