



NETGEAR

Everybody's connecting.

Security & Savings with Virtual Private Networks

W h i t e P a p e r

In today's New Economy, small businesses that might have dealt with just local or regional concerns now have to consider global markets and logistics. Many companies even have facilities spread across the country or throughout the world. At the same time security concerns of their network from hackers, Denial-of-Service (DoS) attacks and sending data over the Internet have become more widespread. Whether companies have a local, national, or global presence, they all need one thing: a way to maintain fast, secure, and reliable communications wherever their offices and workers are located.

Until recently, such communications were only available by using leased telephone lines to maintain a Wide Area Network (WAN). Leased lines enabled companies to expand their private network beyond their immediate geographic area. Moreover, a WAN provided advantages over a public network like the Internet when it came to reliability, performance, and security. Unfortunately, leased lines are expensive to maintain, with costs rising as the distance between the offices increases.

As the popularity of the Internet grew, businesses turned to it as a cost-effective way to extend their networks. The continuing popularity with the Internet has led to the evolution of Virtual Private Networks (VPNs).

A VPN is a connection that allows private data to be sent securely over a shared or public network, such as the Internet. In fact, one of the driving forces behind VPNs is the Internet and its global presence. With VPNs, communication links between users and sites can be achieved quickly, inexpensively, and safely across the world. In this way, VPNs empower organizations to extend their network service to branch offices and remote users — such as traveling employees, telecommuters, and strategic partners — by creating a private WAN via the Internet.

With all these benefits, small businesses are also eager to reap the advantages afforded by VPNs. However, they're also eager to learn more first. This paper explains what a VPN is and how VPNs provide secure, private connections to network applications. By reading this paper, you will gain a fundamental understanding of VPNs, including their security mechanisms, benefits, and cost-saving advantages.

What is a VPN?

Internet technologies have changed the way that companies disseminate information to their employees, customers, partners, and suppliers. Initially, companies were conservative with the information they published on the Internet - product information, product availability, and other less business-critical items. More recently, using VPNs across the Internet has gained wider acceptance as a way to provide more cost-effective access to business-critical information.



NETGEAR

Everybody's connecting.

A VPN is a combination of software and hardware that allows mobile employees, telecommuters, business partners, and remote sites to use a public or "unsecured" medium such as the Internet to establish a secure, private connection with a host network. With a VPN deployed across the Internet, virtual private connections can be established from almost anywhere in the world.

From the user's perspective, a VPN connection is a point-to-point connection between the user's computer and the company's server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link. In this way, the secure connection across the internetwork appears to the user as a private network communication, despite the fact that this communication is occurring over a public internetwork — hence the name Virtual Private Network.

Figure 1 shows an example of a VPN.

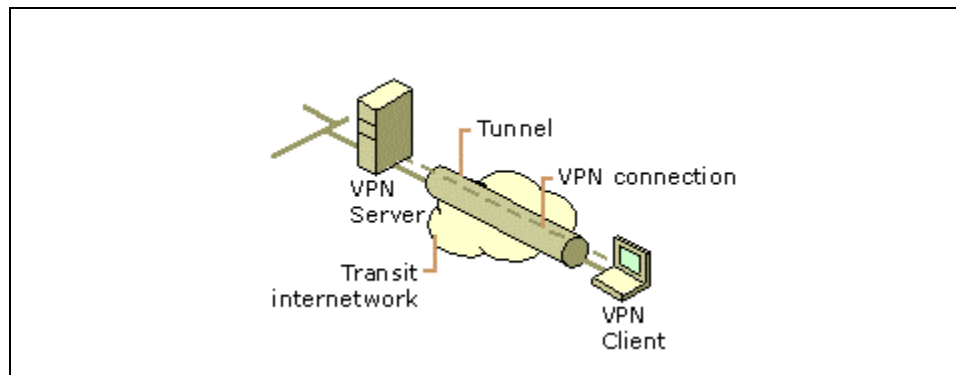


Figure 1. Example of a VPN

VPN Security

Because the Internet facilitates the creation of VPNs from anywhere, networks need strong security features to prevent unwelcome access to private networks and to protect private data as it traverses the public network. After all, companies that have expectations of privacy over their own networks have the same expectation when the Internet is involved. Unfortunately, as data travels between users and their remote offices, it can pass through 25 or more different servers around the world before reaching its final destination. With so many potentially prying eyes, the data should be secured through some form of encryption.

Encryption

A key component of a VPN solution is providing data privacy. Without an explicit way to provide data privacy, information traveling over an unsecured channel like the Internet is transmitted in clear text.

Data transmitted in clear text can be viewed — or even stolen — through common "sniffing" programs and/or devices that monitor data traveling



over a network. Tools such as a protocol analyzer or network diagnostic tools built into today's operating systems can easily "see" the clear-text information as it is transmitted.

Companies are also concerned that some private data may not be encrypted by the VPN before it is transmitted on the public wire. IP headers, for example, will contain the IP addresses of both the client and the server. Hackers may capture these addresses and choose to target these devices for future attacks.

To ensure data privacy and protect valuable transmitted data against "man-in-the-middle" attacks, encryption techniques are required to scramble clear text into cipher text. Encryption scrambles a message into cipher text. The cipher text is then sent to the recipient, who decrypts the message back into clear text again. This encryption/decryption process on the parts of the sender and receiver of the message combine to form a cryptosystem. There are two types of cryptosystems: private key (described below) and public key (described on page 4).

Private Key (Symmetric) Cryptosystems

A private key cryptosystem uses the same secret, fixed-length bit string as a key for both encryption and decryption. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the private key.

Figure 2 shows an example of how data flows in a private key cryptosystem. In this example, the originator encrypts the message "abc" using the secret key, transforming it into "!&#". Anyone that has the same secret key can then decrypt the message "!&#" back into the original message of "abc".

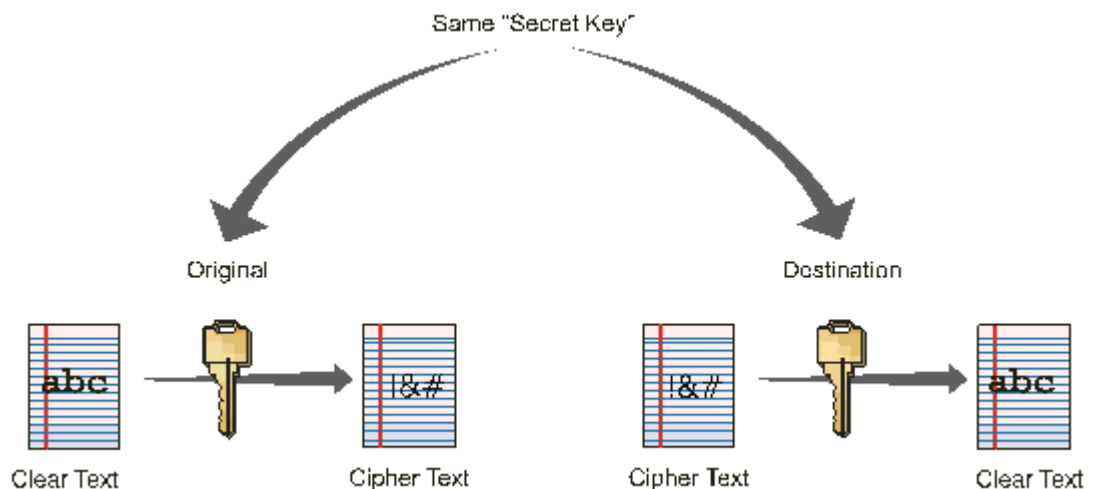


Figure 2. Example of a Private Key (Symmetric) Cryptosystem

Some common symmetric encryption algorithms include:



NETGEAR

Everybody's connecting.

- Data Encryption Standard (DES) — DES takes a 64-bit block of data and a 56-bit key and produces a 64-bit block of encrypted data.
- RC4 — an alternate to DES that uses the same key to scramble and descramble packets. RC4 uses either 40- or 128-bit encryption and is approximately 10 times faster than DES.
- Triple-DES (3-DES) — an even more highly sophisticated encryption mechanism that uses three keys instead of one, thereby providing a much higher level of security than DES.

Each of these algorithms differs in bit length (or "strength"). The strength of the algorithm establishes the amount of effort required to break the system. The longer the bit length, the "stronger" the encryption algorithm and the greater the effort required to break the system.

A private key cryptosystem suffers from the following drawbacks:

- Since the "secret key" is used for both encryption and decryption, anyone who steals the key can steal all the data that is currently or had already been encrypted, jeopardizing all present and past communications using the shared key.
- Because of this danger, the keys must be delivered in a protected manner such as a direct face-to-face negotiation or a telephone call exchange.
- Since the privacy of all data communications is based on the integrity of the secret key, it is important to replace keys periodically. Replacing keys on a frequent basis presents hackers with a very small window of access to the system, thereby providing a greater level of privacy.

Public Key (Asymmetric) Cryptosystems

A public key cryptosystem uses a pair of mathematically related keys:

- A private key that is kept secret within the system, and
- A public key that can be made known to the public.

Because one of the two elements — the public key — is made available to the general public, the initial creation and exchange of a "shared secret key" that is used for secure communications can be accomplished more easily than with a private key cryptosystem. Two public key cryptosystems that are commonly used within VPN solutions today are Diffie-Hellman (DH) and Rivest Shamir Adleman (RSA).

Figure 3 shows an example of a private key (symmetric) cryptosystem.

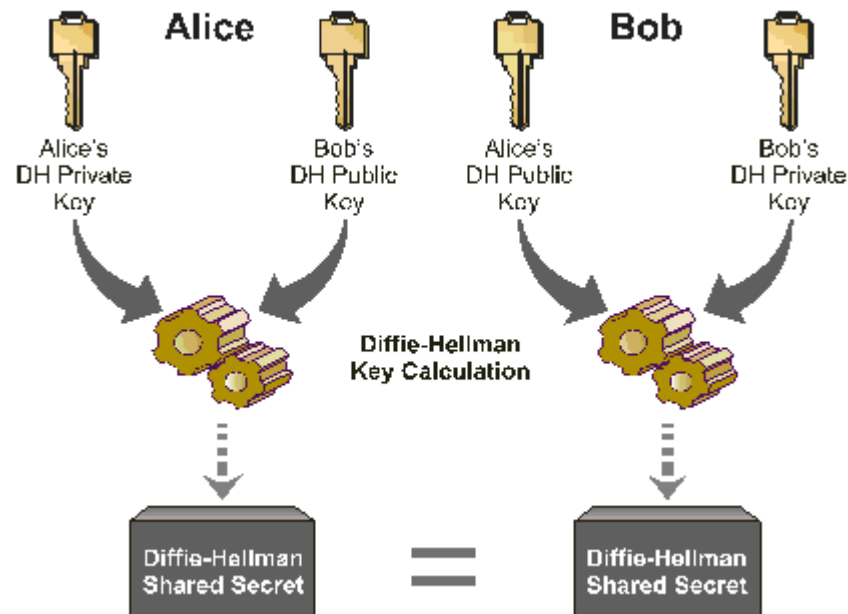


Figure 3. Example of a Private Key (Symmetric) Cryptosystem

User Authentication and Access Control

Up to this point, this paper has discussed the encryption aspects of VPNs. Equally as important is the process of ensuring that users are who they say they are. The following sections describe the steps taken to address and resolve these security concerns.

Internet Protocol Security

Internet Protocol Security (IPSec) is a framework of open standards developed by the Internet Engineering Task Force (IETF) to ensure data privacy, data authentication, and user authentication on public networks. It is a robust standard that has withstood extensive peer review and emerged as the clear industry standard for Internet VPNs.

One of the advantages of IPSec is that it operates at the network layer, whereas other approaches insert security at the application layer. The benefit of network layer security is that it can be deployed independently of applications running on the network. This means that organizations are able to secure their networks without deploying and coordinating security on an application-by-application basis.

Data and User Authentication

Data authentication methods can be used to verify that communications have not been modified in transit.

With user authentication, the identity of the remote user must be verified before that user is granted access to the corporate network.



NETGEAR

Everybody's connecting.

With this method, unauthorized individuals are denied access to the network. This process is arguably the most important element of any VPN solution.

There are a number of user-authentication methods. These include:

- **Pre-shared secrets**

Pre-shared secrets are passwords that are distributed to users "out of band," or independent of the VPN technology infrastructure. They offer an easy way to deploy VPNs quickly to a limited number of remote users. However, shared secrets do not provide robust scalability for large remote user environments.

- **Digital certificates**

Digital certificates are electronic credentials for proving user identity. These electronic credentials can be stored on the remote computer or on tokens carried by the user. Management of digital certificates, including distribution and revocation, is automated by a Public Key Infrastructure (PKI). PKIs offer a stronger and more scaleable authentication infrastructure than shared secrets, but are more expensive and complex to deploy.

Hybrid Mode Authentication

Hybrid Mode Authentication allows organizations to integrate legacy authentication schemes such as SecureID, TACACS+, and RADIUS with VPNs. Without Hybrid Mode Authentication, these schemes must be replaced by shared secrets or digital certificates to deploy a VPN, which can be a complex and costly process.

Goals and Types of VPNs

VPNs address the following three goals:

- They provide remote, traveling, and telecommuting workers with access to central network resources.
- They securely interconnect satellite offices to enable corporate intranets.
- They supply partners, suppliers, and customers with controlled access to selected network resources.

Historically, remote access has been the strongest of the three goals for VPN adoption, but this situation is changing. While remote access remains at the top of the list, the goals of establishing intranet and extranets have emerged. Today, an equal percentage of network managers are building VPN-based extranets and VPN-based remote-access solutions, with the goal of interconnecting internal offices close behind.

To achieve these objectives, VPNs have evolved into the following three classifications:



VPN Type	Description
Remote-access VPNs	Allow remote workers and telecommuters to connect to the company's corporate information resources inexpensively using the Internet or an Internet Service Provider's (ISP's) backbone.
Intranet-based VPN	An internal, TCP/IP-based, password-protected network that businesses use to share information with employees and others with authorization.
Extranet-based VPN	A network that allows controlled network access from external networks, such as from customers, trading partners, suppliers, partners, and business associates. When a company has a close relationship with other companies, it may want to build an extranet-based VPN that connects its LAN to the LAN of the other companies.

A key ingredient of VPN solutions is that the same network infrastructure can be used to support all three types of VPNs. A single VPN can support remote-access users, intranets, and extranets. The following sections describes these VPN types, and Figure 3 illustrates them.

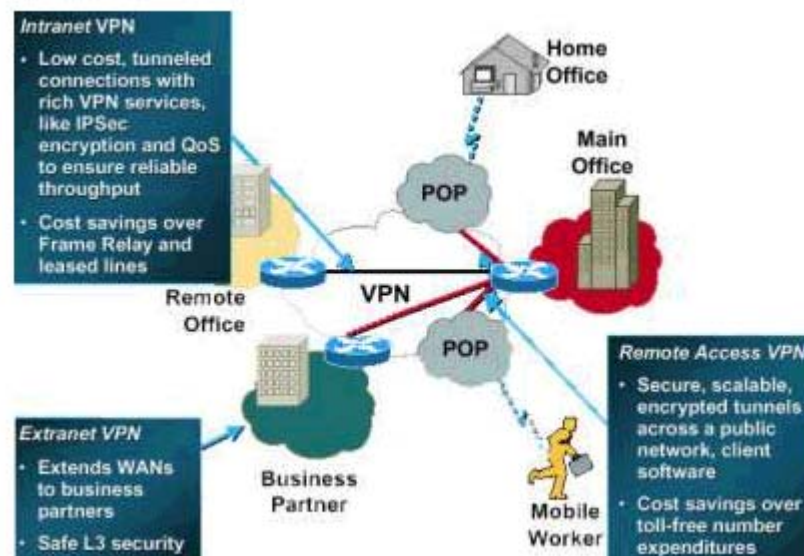


Image courtesy of Cisco Systems, Inc.

Figure 3. Examples of Three VLAN Types

Summary of VPN Benefits

A well-designed VPN can provide companies with significant advantages, including:



NETGEAR

Everybody's connecting.

- Extended geographic connectivity
- Improved security
- Reduced operational costs versus traditional WAN
- Reduced transit time and transportation costs for remote users
- Improved productivity
- Simplified network topology
- Global networking opportunities
- Telecommuter support
- Broadband networking compatibility
- Faster return on investment than traditional WAN technology
- Scalability that provides a comprehensive solution for cost-effective remote access, intranet, and extranet connectivity using public data services

Cost-Saving Advantages

In addition to the benefits mentioned above, VPNs enable small businesses to save from 30% to 70% over competing remote-access solutions. For connectivity outside the US, the savings can reach 90%. The following sections provide additional information about the cost savings that can be achieved with VPNs.

Eliminating Pricey Leased Lines

One way a VPN lowers costs is by eliminating the need for companies to procure expensive long-distance leased lines. With VPNs, an organization needs only a relatively short dedicated connection to an ISP. This connection can be a local broadband connection such as Digital Subscriber Line (DSL) service, cable service, or a local leased line (which is considerably less expensive than a long-distance leased line). This factor alone convinces many organizations to eliminate other remote-access methods in favor of VPN solutions.

Reducing Long-Distance Dependence

Another way VPNs reduce costs is by allowing remote employees to access the corporate LAN via the Internet by placing a local call into the nearest ISP's POP. This provides a three-fold cost savings.

Firstly, local Internet calls are significantly less expensive than pricey long-distance calls.

Secondly, companies do not have to support expensive toll-free 800 telephone numbers to accommodate their remote employees.



NETGEAR

Everybody's connecting.

Thirdly, remote employees located at international venues can be supported inexpensively (see "Reduced International Calling Expenses," next).

Reduced International Calling Expenses

VPNs can also slash communications costs significantly for companies that have many international sites. Typically, the cost to link a European site to a North American headquarters office can be high when using leased lines or data services such as frame relay. A VPN built around an ISP with POPs in countries where there are branch offices allows the international sites to pay only for dedicated Internet access to that POP. This method is much less expensive than paying for a long-distance link back to the United States. In fact, some studies show that international remote access VPNs can yield cost savings of between 60 and 90% over other remote-access solutions.

Obviating Multiple Access Lines

Some organizations that have multiple access lines: one to carry data back to headquarters and a second for Internet access. In fact, some industry studies have found that as many as 72% of sites have multiple access lines. Using a VPN, a branch office with multiple links can eliminate its data lines and move traffic over the existing Internet access connection, resulting in dramatic cost savings.

Reduced Equipment Costs

VPN equipment is much less expensive to deploy and maintain than equipment required for other remote-access solutions. According to a recent survey by Giga Information Group, domestic remote access VPNs can yield cost savings of 20 to 70% over other remote-access equipment.

Offloading Support Burden

Another, more subtle way that VPNs lower costs is by offloading the support burden. With VPNs, the ISP handles remote access rather than the organization. ISPs can, in theory, charge much less for their support than it costs a company internally, because the public provider's cost is shared among potentially thousands of customers. In addition, ISPs possess the knowledge and capabilities for maintaining remote access, which may exceed a company's own core expertise.

Scalability and VPNs

The cost to an organization of traditional leased lines may be reasonable at first but can increase exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations. If a third branch office needs to come online, just two additional lines will be required to directly connect that location to the other two.

However, as an organization grows and more companies must be added to the network, the number of leased lines required increases dramatically.



NETGEAR

Everybody's connecting.

Four branch offices require six lines for full connectivity, five offices require ten lines, and so on. In a traditional WAN, this explosion limits the flexibility for growth. VPNs that utilize the Internet avoid this problem by simply tapping into the geographically distributed access already available.

Additional Advantages

The real benefits of VPNs lie not in cost savings, but in coverage and openness. VPNs — particularly Internet-based VPNs — are unmatched in their potential for global coverage. No other network service offers the global footprint available by using the Internet.

The same can be said about the openness of the standards-based IP protocol. If there's an intranet or extranet in your company's future, no other network infrastructure will get you there more directly than a VPN.

VPN Tunneling

VPN technology is based on a tunneling strategy. Tunneling creates a private network that spans the Internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network. The protocol of the outer packet is understood by the network and the source and destination points (called *tunnel interfaces*) where the packet enters and exits the network.

Tunneling utilizes three different protocols:

- **Carrier protocol**
The protocol used by the network that is carrying the information.
- **Encapsulating protocol**
The protocol that is wrapped around the original data
- **Passenger protocol**
The original data being carried

To better understand how these components work, think of tunneling as a package delivered to you by an overnight-delivery service. The sender places the package (passenger protocol) in an envelope (encapsulating protocol), which is then put on a delivery truck (carrier protocol) at the sender's office (entry tunnel interface). The truck (carrier protocol) travels over the roads (Internet) to your home (exit tunnel interface) and delivers the package. You open the package (encapsulating protocol) and remove the contents (passenger protocol). Tunneling is just that simple.

Tunneling has significant implications for VPNs. For example, you can place a packet that uses a protocol not supported on the Internet (such as NetBeui) inside an IP packet and send it safely over the Internet. Furthermore, you can insert a packet that uses a private (non-routable) IP address inside a packet that uses a globally unique IP address to extend a private network over the Internet.



NETGEAR

Everybody's connecting.

NETGEAR Solutions

NETGEAR's FVS318 Cable/DSL ProSafe VPN Firewalls provide the ability to establish multiple VPN tunnels using IPSec DES or 3-DES encryption technology. These routers can be used together to establish and terminate a VPN tunnel, without the need for VPN client software. Conversely, they can be used in conjunction with standard VPN client software (Safenet), when using multiple routers is not practical. The latter example could apply to a mobile workforce, such as a salesperson, for example.

Other routers that support IPSec pass-through, such as NETGEAR's RP614 Cable/DSL Web Safe Router, can be used at a remote site and terminate a VPN tunnel, provided the PCs at the remote site are using a VPN client. Clearly, the most practical and easy-to-deploy method would be to have VPN-enabled FVS318s at both sites, which would eliminate the need for VPN client software on each computer.

Conclusion

This paper has shown that VPNs deliver tangible business benefits, with secure communications and significant cost savings versus other remote-access solutions. Moreover, end users do not need to know anything about VPN client software or hardware to establish a VPN tunnel and access the company LAN. When a user wants to check e-mail remotely, for example, the user simply opens his or her e-mail client and requests a download as if connected to the company LAN.

One of the most exciting aspects of VPNs is that everyone can benefit from these solutions. In the beginning days of the technology, early adopters were the largest and the smallest of companies.

- Large enterprises viewed VPNs as a way to contain escalating WAN costs, connect remote users, and integrate partners, suppliers, and customers into their networks.
- Very small companies adopted VPNs because they were the first real WAN or remote-access solutions they could afford.

Today, VPNs are equally appealing to companies of all sizes. Even small businesses are finding compelling reasons to implement VPNs. Many view VPNs as a competitive advantage, specifically because of their global coverage and the relative ease with which they can be extended to create extranets.

VPNs also have universal appeal across industry types. The earliest adopters included high-technology firms, computer services, and communications companies. Businesses in other industries — including insurance, real estate, manufacturing, and finance — have since found VPNs beneficial. As the technology continues to grow, success stories are coming from other industries as well, including education, health services, transportation, and government. Even the US military takes advantage of VPN benefits. With the decrease in the cost of VPN



NETGEAR

Everybody's connecting.

technology, it is not surprising to see small businesses taking advantage of the savings realized by embracing and deploying these networks.

With all of the interest in VPNs, analysts predict tremendous growth. By late 2001, nearly 70% of businesses with networking needs are expected to be testing VPNs or using them in a production environment.

Given the growing interest in — and increasing deployment of — VPNs, it is vital to scale that interest in terms of security. Possessing a better understanding of VPNs and their security mechanisms empowers companies to expand the borders of their business, without increasing the vulnerability of their information assets. It also enables you to make a well-informed decision when evaluating VPN solutions.

Information Links

IETF Web site	http://www.ietf.org/
IP Security Protocol (IPSec)	http://www.ietf.org/html.charters/ipsec-charter.html
Public Key Infrastructure (X.509 - PKIX)	http://www.ietf.org/html.charters/pkix-charter.html
Simple Public Key Infrastructure	http://www.ietf.org/html.charters/spki-charter.html
Point-to-Point Protocol Extensions	http://www.ietf.org/html.charters/pppext-charter.html
Socksv5	ftp://ftp.isi.edu/in-notes/rfc1928.txt
Search IETF Draft Database	http://search.ietf.org/search/brokers/internet-drafts/query.html