

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.

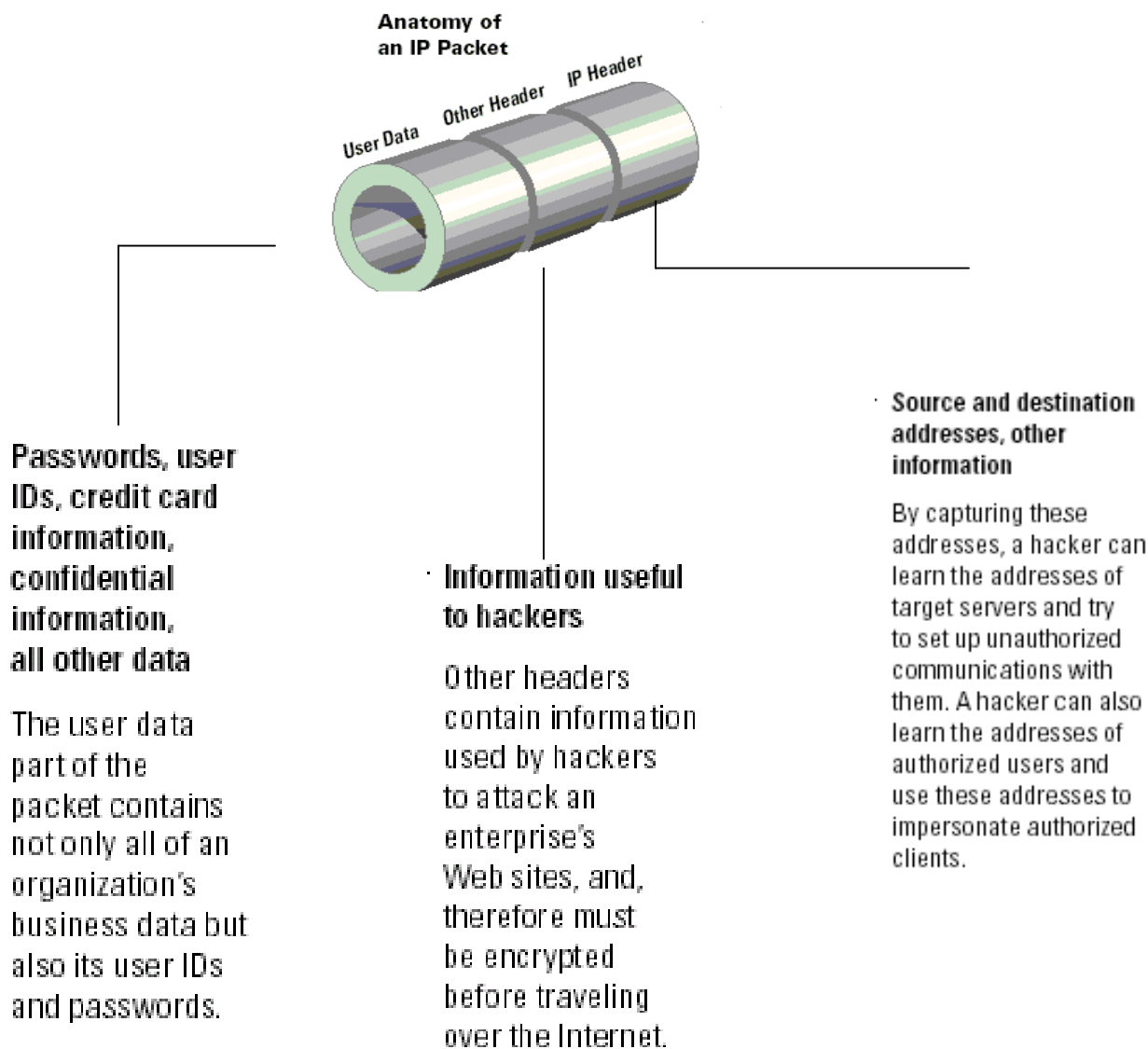
As the Internet became more and more accessible and bandwidth capacities grew, companies began to offload their Intranets to the web and create what are now known as Extranets to link internal and external users. However, as cost-effective and quick-to-deploy as the Internet is, there is one fundamental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

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

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.



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 Internetbased VPN transmission transparent to your users, it is virtually transparent to your network management operations, as well.

Encryption:

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 or software form. The gateway at the sending location encrypts the information into ciphertext 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

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 (28)
- 16-bit keys = 65,536 combinations or two to the 16th power (216)
- 56-bit keys = 72,057,594,037,927,900 or two to the 56th power (256)
- 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

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.

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 XYZ and ABC. XYZ 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, XYZ 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 XYZ 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 XYZ in the same manner.

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.

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 XYZ and ABC. When XYZ receives a message signed from ABC, XYZ 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 XYZ should be able to decode. When XYZ gets his number back, he can be assured it really is ABC on the other end.

Data 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).