Virtual private networks

Contents

Introduction
What is a VPN?
What does the term virtual private network really mean?
What types of VPN are there?
What does a VPN consist of?
How does a VPN work?
What are the advantages and disadvantages of a VPN solution?
Should a VPN use dedicated hardware or software?
How does a VPN keep the data secure?
What is an SSL VPN, and should it be used instead of IPSec?
Can a VPN be used to secure a wireless network?
What are the essential features of a VPN?
What alternatives are there?
The impact and benefits of VPNs
Other sources of information

Introduction

Virtual private networks (VPNs) offer low-cost, secure, dynamic access to private networks. Such access would otherwise only be possible by using an expensive leased line solution or by dialling directly into the local area network (LAN).

VPNs allow remote users to access private networks securely over the internet. A remote user in one part of the UK can establish a secure network connection using a VPN to a school LAN in another part of the UK and only incur the call cost for the local internet connection.

What is a VPN?

A virtual private network gives secure access to LAN resources over a shared network infrastructure such as the internet. It can be conceptualised as creating a tunnel from one location to another, with encrypted data travelling through the tunnel before being decrypted at its destination.

Remote users can connect to their organisation’s LAN or any other LAN. They can access resources such as email and documents as if they were connected to the LAN as normal. By using VPN technology it is possible to connect to a school LAN from anywhere in the world via the internet, and to access it securely and privately without incurring the large communication costs associated with other solutions.

Figure 1: two methods of connecting to a school’s LAN using a VPN

One user uses a 56 kilobits per second (Kbps) modem to dial their internet service provider (ISP) and connects to the central LAN with VPN software.

A remote site uses ADSL (asymmetric digital subscriber line) to connect to its ISP and a VPN router (a hardware solution) to carry out the VPN connection. Few changes are made to the PCs at the remote site and the VPN router carries out the encryption and decryption of data.

As both connect to their usual ISP, they only incur their normal ISP call tariffs.
What does the term virtual private network really mean?

**Virtual** – means that the connection is dynamic. It can change and adapt to different circumstances using the internet's fault tolerant capabilities. When a connection is required it is established and maintained regardless of the network infrastructure between endpoints. When it is no longer required the connection is terminated, reducing costs and the amount of redundant infrastructure.

**Private** – means that the transmitted data is always kept confidential and can only be accessed by authorised users. This is important because the internet's original protocols – TCP/IP (transmission control protocol/internet protocol) – were not designed to provide such levels of privacy. Therefore, privacy must be provided by other means such as additional VPN hardware or software.

**Network** – is the entire infrastructure between the endpoints of users, sites or nodes that carries the data. It is created using the private, public, wired, wireless, internet or any other appropriate network resource available.

What types of VPN are there?

There are many variations of virtual private networks, with the majority based on two main models:

- **Remote access, virtual private dial-up network (VPDN) or client-to-site**
  A remote access VPN is for home or travelling users who need to access their central LAN from a remote location. They dial their ISP and connect over the internet to the LAN. This is made possible by installing a client software program on the remote user's laptop or PC that deals with the encryption and decryption of the VPN traffic between itself and the VPN gateway on the central LAN.

- **Fixed, intranet and extranet or site-to-site**
  A fixed VPN is normally used between two or more sites allowing a central LAN to be accessed by remote LANs over the internet or private communication lines using VPN gateways. VPN gateways (normally a VPN-enabled router) are placed at each remote site and at the central site to allow all encryption and decryption and tunnelling to be carried out transparently.
What does a VPN consist of?
As VPN topologies can vary greatly there is no standard for a definitive VPN. However, it is possible to specify what each main component of a VPN does:

- **VPN gateways** – create the virtual tunnels that the data passes through, carrying out the encryption before transmission and decryption at the other end. Gateways can be software, or built into a firewall, or a server or router or a dedicated appliance.

- **Security servers** – maintain the access control list (ACL) and other user-related information that the security gateway uses to determine which traffic has authorised access.

- **Keys** – used for the encryption and decryption of data. Sites can choose to maintain their own database of digital certificates (keys) for users by setting up a certificate server, or they can use an external certificate authority.

- **Network** – there must be an internet infrastructure at both ends to provide the actual transmission medium.

Some of these components may be built into a single device or spread over many devices over several sites.

How does a VPN work?
A remote access solution works by the remote user first establishing an internet connection to an ISP in the normal way. The user activates the VPN client software to create a tunnel over the internet and to connect to the central LAN’s VPN gateway. The VPN client software then passes its authorisation to the VPN gateway. The VPN gateway checks that the user is authorised to connect and then ensures the encryption key from the remote client is valid. All VPN data is encrypted using the key before being transmitted over the internet using a tunnelling protocol. It is decrypted at the other end by the VPN gateway, which has an identical set of keys to decrypt the data. Data sent from the central LAN to the remote user is encrypted by the VPN gateway before transmission and decrypted by the remote user’s VPN client software.

![Figure 2: a remote access VPN solution](image)

A fixed solution works by first establishing a VPN gateway at each site. Each VPN gateway has the same key to encrypt/decrypt data and knows the IP addresses of the other sites, so they know where to transmit the data to, and where to expect secure VPN transmissions from. This flow of data is transparent to the users and requires little actual configuration on the PCs.

![Figure 3: a fixed VPN solution](image)

The choice of ISP is very important when implementing a VPN solution as it can have a major impact on VPN performance. It may be advisable for all VPN users and sites, including the central LAN, to use the same ISP for their internet connections. This will lessen the amount of
data that needs to cross into the networks of other ISPs, which could degrade performance. Most ISPs will offer a service level agreement (SLA) that agrees network uptime, latency, security and other functions. It is important to read the SLAs carefully before deciding which ISP will give the fastest and most reliable service.

What are the advantages and disadvantages of a VPN solution?
Virtual private networks have a number of advantages and disadvantages over direct dial or leased line solutions.

Advantages:

- VPNs authenticate all packets of data received, ensuring that they are from a trusted source. Encryption ensures that the data remains confidential.
- Most VPNs connect over the internet so call costs are minimal, even if the remote user is a great distance from the central LAN.
- Multiple telephone lines and banks of modems at the central site are not required.
- A reduction in the overall telecommunication infrastructure – as the ISP provides the bulk of the network.
- Reduced cost of management, maintenance of equipment and technical support.
- Simplifies network topology by eliminating modem pools and a private network infrastructure.
- VPN functionality is already present in some IT equipment.
- VPNs are easily extended by increasing the available bandwidth and by licensing extra client software.
- If a LAN uses NetBeui or IPX/SPX (both incompatible with the internet) instead of TCP/IP to transmit data to its clients, the VPN gateway can encapsulate these languages into an IP packet and transmit it over the web to another VPN gateway.

Disadvantages:

- If the ISP or internet connection is down, so is the VPN.
- The central site must have a permanent internet connection so that remote clients and other sites can connect at anytime.
- VPNs may provide each user with less bandwidth than a dedicated line solution.
- Existing firewalls, proxies, routers and hubs may not support VPN transmissions.
- The internet connection of the central site must have sufficient bandwidth to cope with VPN traffic, the internet connections originating from the central site and any other traffic such as email and FTP (file transfer protocol).
- VPN equipment from different manufacturers may comply with different standards.

Any institution that has users who connect to a LAN from a remote location, or which requires its users to connect to a central LAN, should consider implementing a VPN solution. It is considered to be a superior alternative to long-distance dial-in and leased lines; VPNs can be used securely.
to carry information at a fraction of the cost of other solutions. An institution can reduce its connection and maintenance costs by replacing banks of modems and multiple leased lines with a single link that carries remote access and fixed VPN traffic along with existing internet traffic.

**Should a VPN use dedicated hardware or software?**

Some VPN solutions use dedicated hardware appliances that are specifically designed for the tasks of tunnelling, encryption, and user authentication. These devices usually operate as encrypting bridges and they are often placed between the routers on the networks. Although most of these hardware tunnels are designed for fixed configurations, some products also support remote access tunnelling. Many of these products perform very well on throughput and when handling large numbers of simultaneous tunnels, which is crucial for supporting a large number of users. Hardware solutions are generally considered to be more secure and provide good logging and reporting options.

VPN client software can be installed on laptops and individual PCs for use by one user between a remote client and a security gateway. VPN software may be used on a server that will act as a VPN gateway for an entire site to create and manage tunnels between a pair of security gateways. These VPN software systems are often good low-cost choices for networks that are relatively small and which do not have to process a lot of traffic. Such solutions can run on existing servers, share resources with existing applications and serve as a good starting point for getting familiar with VPNs. Many of these systems are well suited for remote access connections. Software-based VPN solutions allow great flexibility in terms of implementation and usage, but flexibility brings extra management and support costs.

**Which VPN solution?**

There is no 'one size fits all' solution when choosing a VPN. Several basic questions should be asked before deciding on a solution:

**Do you need to connect sites together or individual remote users to a central LAN?**

Individual users are best connected with software installed on their PC/laptop and a hardware device or a VPN software server on the central LAN. Sites should be connected using hardware devices because of their faster throughput, with one device located at each site.

**What type of network equipment and operating systems do you already have?**

Existing equipment may have VPN functionality already built in and it may be worth attempting to configure this rather than purchasing a completely new solution. Some older and cheaper firewalls and proxy servers may not support VPN functionality and will require replacing or upgrading.

**What are the main features of a software solution?**

Software is cheaper, and it may be included with equipment already in use. Another advantage of the software approach is that the network does not change, no extra devices need to be installed and the management of the network remains the same. Single remote users tend to use software VPN solutions.

**What are the main features of a hardware solution?**

Hardware solutions are more expensive but remain more reliable and secure than software solutions, although the extra equipment brings with it extra support and management costs. Hardware solutions are generally used to connect 100 or more users, or fixed sites, or where users place a particularly heavy load on the VPN network.

It is cheaper to implement software VPNs, but the total cost of ownership (TCO) tends to be higher when compared with a hardware solution.
It is extremely common for hardware and software solutions to be mixed. Often institutions have hardware-based VPN solutions installed on their central and remote LANs, while remote or travelling users have VPN software clients installed on their laptops or home PCs.

**How many users require VPN access?**
If the number of users is less than 100 then a software solution is probably better than a hardware solution.

**Do your users only need access to one application that is, or can be, browser based such as webmail?**
If so, then consider a secure socket layer (SSL) VPN solution, which may be cheaper and easier to manage than a full internet protocol security (IPSec) solution.

**How secure does your data need to be during transmission?**
If you are transmitting data that is sensitive then software is possibly the best option; if the data is highly confidential then hardware offers the best security and encryption.

**Are you connecting remote sites with many users to a central LAN?**
Connecting remote sites with many users should be done with a hardware solution as it has performance and management benefits over a software solution.

**Do you need a flexible and scalable system?**
A software solution offers greater flexibility than a hardware solution, but there is a trade off. As flexibility and security compromise each other, it is difficult have a very flexible, fully secure system.

**What about a managed VPN solution?**
A managed VPN is one that is built and operated by a trusted third party, like an ISP or a secure application service provider (SASP). The third party designs the fixed or remote access VPN solution and manages it on your behalf. This may be more expensive than an internal solution but carries the benefits of reducing the burden on ICT co-ordinators and IT staff.

**How does a VPN keep the data secure?**
TCP/IP is not designed for security, so VPNs use a mix of IP protocols and systems to provide the best security solution for each type of connection. Some protocols encrypt the packets of data while other protocols protect the packet whilst it is being transmitted. Some of the more popular protocols and systems that a VPN uses to keep the data secure are:

- **PPTP (point-to-point tunnelling protocol)**
  Creates a virtual tunnel for connections which, along with L2TP (layer two tunnelling protocol) and L2F (layer two forwarding), is used mainly for remote access VPNs.

- **IPSec (internet protocol security)**
  Is becoming the most commonly used security option for fixed VPN solutions. Each packet of data is encrypted and has an authenticating stamp verifying its origin. This makes IPSec a very secure option. IPSec works in one of two ways:
    - In ‘transport mode’ only the payload portion of the packet is encrypted. (The payload consists of the actual data that is being transmitted.)
    - In ‘tunnel mode’ the entire packet, including the header is encrypted. (The header contains the source and destination IP addresses.)

- **Encryption standards**
  DES (data encryption standard) and 3DES (triple DES) secure the data to different levels ranging from 56- to 168-bit encryption.
Authentication systems
Prove that the sender of the packets is genuine and not a hacker attempting to deceive the receiver by intercepting and altering the packets before they arrive at their destination.

PKE (public key encryption)
PKE can be used with VPNs. Instead of manually entering encryption codes, internet key exchange (IKE) allows keys to be automatically exchanged – which is useful on larger networks.

There are many ways to protect the data during transmission. Most VPN solutions use either encryption or authentication for data security. As the security level increases so does the time required to process and assemble each packet. The typical overhead for VPN encryption during web browsing is 20 per cent; other user applications that run over VPNs may increase the overhead significantly more. To alleviate this problem some VPN systems compress data before sending to improve network performance.

What is an SSL VPN, and should it be used instead of IPSec?
SSL VPNs use existing web browser technology to create a secure VPN tunnel between a client and a server. Most, if not all, web browsers now have the capability to use SSL encryption to access secure websites and to transmit and receive secure or private information. SSL VPNs are limited to applications that can run in a browser window and therefore are not as popular as IPSec VPNs. While some might find the limitations of SSL-based VPNs a problem, these shortcoming may diminish as web-enabled or browser-based applications become more popular.

IPSec is application independent and is suitable for users who need to access all applications and resources as if they were physically connected to the LAN. SSL is suited to infrequent users who require webmail or browser-based application access.

Figure 4: a simplified example of an IPSec fixed VPN solution
A VPN gateway has been installed at site A and site B. These two devices are connected to the internet via an ISP’s ADSL package, with each VPN gateway having a unique IP address. Each VPN gateway is configured with the same shared key or code.

The original IP packets on the LAN only contain the receiver’s address (H1) called a header, the actual data being sent (payload) and sender’s address (T1) called a trailer.

Each individual packet of data that passes through the VPN gateway to be sent to site B is wrapped inside another packet that is encoded using the shared key. The original packet is encrypted and remains inside a wrapped layer of authentication, proving that it originated from site A.

When the packet of data reaches the VPN gateway on site B, the gateway checks to see if the packet originated from site A and that the packet has not been tampered with. Then, if the packet meets these criteria, it decodes the packet using the shared code before passing it on to its destination on the LAN.

If the packet becomes subject to a so-called ‘middleman attack’ and a hacker collects the packet before it reaches site B then it will be useless without the shared code. The hacker cannot break into the packet’s payload without first decrypting the code.

Can a VPN be used to secure a wireless network?
As a VPN encrypts data from one point to another it is ideal for use over a wireless local area network (WLAN). However, it is worth noting that the biggest cause of WLAN security problems...
is the network not being made secure at time of installation, either by bad installation practices or lack of knowledge of the product. Further information about installing and configuring WLANs can be found in Becta’s WLAN technical document [http://www.becta.org.uk/technicalpapers].
What are the essential features of a VPN?

VPNs should supply a certain amount of basic functionality for any given solution. However it is reasonable to expect that a fixed hardware VPN, which covers multiple sites, should have more features than a software remote access solution. Some of the main features are:

- **AAA** – authentication (who is the user), authorisation (what is the user allowed to do) and accounting (recording what the user actually does).
- **Security** – tunnelling support between sites with at least 128bit encryption of the data.
- **Scalability** – extra users and bandwidth can be added easily to adapt to new requirements.
- **Services** – quality of service features, including bandwidth management and traffic shaping, are important to avoid congestion.
- **Management** – reports on user activity, management of user policies and monitoring of the VPN as a whole.

There are many different VPN manufacturers and it is important to be aware that their products are sometimes incompatible because of the protocols used or the lack of standardised testing.

What alternatives are there?

When VPNs are used it is normally in place of other methods of communication. A VPN is designed to remove the need for fixed links, dedicated circuits and expensive long distance telephone calls. Remote access service (RAS) and leased lines are possible alternatives.

- **Remote access service** – via standard PSTN (public switched telephone network) or ISDN (integrated services digital network) lines requires the user and receiving site to have access to exclusive modems or similar devices, and different communication lines for each connection that is made. The caller may incur large telephone bills if they are a long distance from the network that they are accessing.

- **Leased line** circuits – can be very expensive (such circuits are normally charged by the mile) when compared to the cost of a VPN connection over the internet, although there is a high quality of service. With the current poor quality of service within a VPN run over a public network, leased lines provide a good solution for when a ‘guaranteed’ level of service is required.

The impact and benefits of VPNs

VPNs allow institutions to take advantage of the internet’s infrastructure for secure, private communications between schools, remote sites, and home-based workers. Access to a school’s LAN is entirely possible from home before, during or after school hours. A user can access all of resources on the LAN as if they were actually on site.

A VPN solution can reduce the need for dedicated equipment by using existing internet equipment. VPNs are scalable solutions which allow new users to be added without major restructuring.

Users are able to access an SSL VPN server from almost any internet-connected PC, even those in public locations. An SSL-based VPN does away with the need for VPN software to be installed on the users’ PCs, although the applications that can used are limited to those available in a web-enabled format.
Implementing a VPN solution for home/school links would be extremely beneficial, allowing a large number of users to access a school’s network from home while requiring very few changes to be made to the existing LAN infrastructure.

**Other sources of information**

**Becta**  
Remote access technical paper (Word or rich text format)  
or [http://www.becta.org.uk/technicalpapers](http://www.becta.org.uk/technicalpapers)

**Others**  
ActivSupport: VPN FAQ  

FindVPN: information on VPN providers  

VPN Labs: open source VPN community  