VIRTUAL PRIVATE NETWORKS

What is a VPN?

A VPN provides a way to connect a private *network* (such as a LAN in an office) to other computers over a public network such as the *Internet*. For example a VPN can be used to allow:

- Offices in separate locations to connect their networks together
- Remote access - e.g. staff working from home can connect their computers to the office network

Because the Internet is available globally, a VPN can be used to give staff access to the office network from any location in the world. Since a user would typically be using a local call to a local Internet Service Provider (*ISP*) rather than dialling into the office network directly, the cost of long distance phone calls or expensive dedicated leased lines is eliminated. VPNs have the added advantage that they can allow a Local Area Network (*LAN*) in an office to be managed and supported remotely. This means that many problems can be resolved without the network support provider having to physically visit the office.

Is a VPN safe?

Because information travelling across the Internet can potentially be intercepted, VPNs use a number of security features to help keep your data safe. These features include:

- Encryption
- Authentication
- Tunnelling

Encryption

A major concern for information passing over the Internet is that an unauthorised person may gain access to it. This problem can be solved by encrypting or encoding the data before putting it on the Internet. The information is then decrypted or decoded once it reaches its destination. This way, if the information is intercepted by an unauthorised user, it cannot be read.

Authentication

Authentication provides a means for authorised users only to access your office network. It is usually achieved by implementing a user name and password system.

Strong Passwords

It is important to enforce strong passwords and frequent password changes to maintain security as passwords can be guessed. Strong passwords contain at least 8 characters, with a mixture of upper and lower case letters, numbers, and special characters. This makes them much harder to guess. If a very high level of security is needed, one time password systems are available which use electronic gadgets that generate a new password very frequently (every minute or so). The authentication system in the office does the same so it recognises which password to accept.

Of course any authentication system can potentially be compromised if access details are revealed to unauthorised users. For example because a password is written down, easily guessed, or someone is looking over your shoulder as you login to your office network from your laptop in a public place.Once an authorised user has access to the network, you still want to restrict them only to the bits of the network they require so it is important to make sure user logins for the *VPN* restrict access to the network appropriatly. This means if a user's account is

compromised by an unauthorised person, the amount of the network available to the intruder is also restricted.

Tunnelling

Tunnelling is a way of bundling up the packets of data at the sender's end, transporting them over the Internet using IP, and unwrapping them at the destination. Tunnelling allows the Internet, a public network, to convey data on behalf of a private network. Tunnelling gets round the problem that different networks may use a different set of protocols to allow machines on the network to talk to each other. With a VPN you are connecting to an Internet *Protocol* (IP) network whereas the machines on your office network may be using a different protocol.

VPN Systems

2 main categories of VPN products are commonly used:

- Hardware systems
- Firewall-based systems

Hardware systems

Hardware systems typically use a device called a *router* to encrypt data. A router is a device (or sometimes a piece of *software* in a computer), that determines the next network point to which a unit of data should be forwarded toward its destination. Some hardware VPNs need special cards to be installed on each PC on the network.

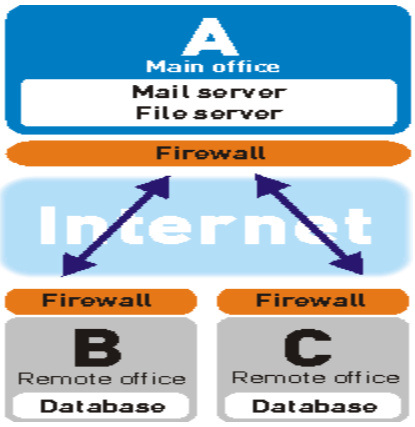
Firewall-based systems

Firewall based systems use the firewall's existing security mechanisms including restriction of access to the internal network. A firewall is a piece of hardware (or software) that protects a private network from unauthorised access by users of other networks such as the Internet. If you

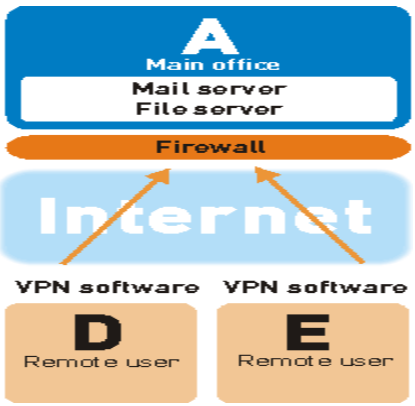
have a *broadband* connection to the Internet it is advisable to use a *firewall*. Your existing firewall product may well have VPN capability.

For more information on firewalls, see the knowledgebase articleFirewalls.

Typical VPN setups



Office A, the main office houses the mail server and main file server. Users at all locations can access their emails and other resources on the network such as calendars and files. Backing up files is also easier for all the users on the network. Office A needs access to the databases at offices B and C as well as these offices needing access the network at office A. Since this two way access is needed, offices A, B and C each need to have a firewall and a broadband connection to the Internet.



D and E are other remote users e.g. mobile workers needing only access to office A's network. Office A does not need access to computers at D and E. Since only one-way access is needed from D and E to office A, only VPN software needs to be installed at D and E. Locations D and E also do not ***need*** to have a broadband connection (if they do however, it would be advisable to install a firewall at D and E).

Performance issues

If two or more offices in separate locations are to be connected, broadband access such as *ADSL* in all the offices is likely to be the only feasible option when using a VPN. This is because it is likely that large amounts of data will need to be transferred between the locations and several people may be trying to access the network at the same time - anything other than broadband would be too slow. However, for individual staff accessing the network from home for example, a 56k *modem* connection may be adequate. As with any service, the Internet may not be available a hundred percent of the time. For example:

- Your ISP's equipment may break down, making their services unavailable for a period
- From time to time the Internet gets very busy and slows to a crawl (as on September 11th 2001) affecting access to the main office network from remote locations
- Very occasionally problems occur with the handful of servers that are at the heart of the Internet, causing system wide availability problems.

Obviously if your Internet connection is unavailable, then your network will be unavailable to remote users. However, these days, many ISPs are trying hard to improve the reliability of their networks and many now also offer VPN services.

Source: http://www.ictknowledgebase.org.uk/vpn