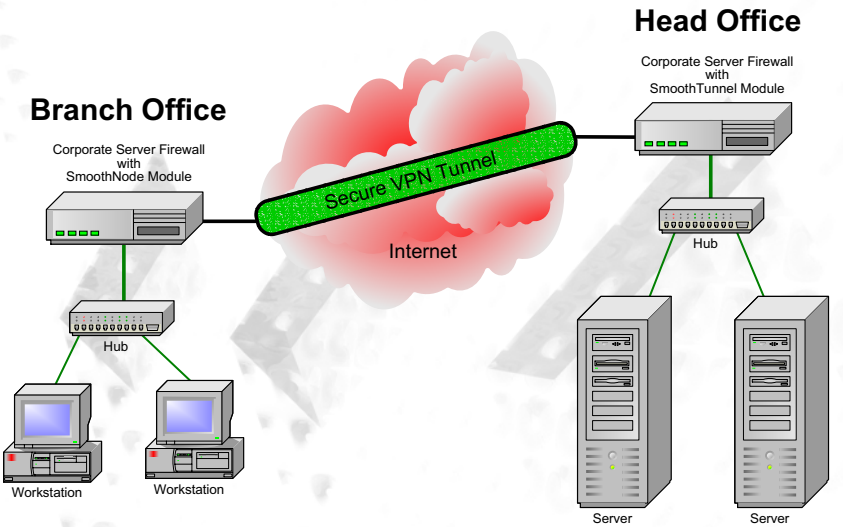
Introduction to VPN (Virtual Private Networks)

What is a Virtual Private Network (VPN)?

A Virtual Private Network allows an organisation to join the Local Area Networks at two or more locations together using an encrypted connection over the Internet. This allows users to securely access information wherever it may be located on the network.

The following illustration depicts a very simple VPN. This would allow remote users at an organisation's branch office to securely access the IT resources, such as servers and printers, at head office.



The principal advantages of a VPN over traditional computer network solutions are:

- **Security** - all data is encrypted, typically using a 168 bit key, making it extremely secure
- **Cost** - replacing private circuits (leased lines) can save a considerable amount of money on an annual basis
- **Flexibility** - almost all IP (Internet Protocol) traffic and hence applications can be routed through a VPN

Security

The Internet can be a dangerous place for confidential data. There are legions of hackers who enjoy nothing better than the challenge of penetrating other people's computer systems. Not all are malicious; their motives are very varied. However, even if information gained is not used for fraudulent purposes, the damage to company confidence and prestige can be significant. Many hackers like to leave their mark upon a system or deface it to show their prowess. Worse still they may create a "back door" into the system, allowing them or others to easily gain access again at a later date.

Data sent over the Internet between two computer systems will pass through many computers and network systems over which the end-user has absolutely no control. Unless the data is encrypted then it is extremely vulnerable to being eavesdropped on.

SmoothWall Corporate Server provides a secure Internet Gateway and Firewall to protect an organisation's Local Area Networks (LANs). The SmoothTunnel and SmoothNode Add-On module establish secure encrypted VPN connections (tunnels) between Corporate Server Systems.

Cost

Private Circuits are supplied by a Telecommunications Company (TelCo) for the sole use of the customer organisation. They are normally subject to both installation and annual charges. The charges are normally distance related, with high capacity long distance circuits normally being regarded as too expensive for all bar the richest corporations.

Using the Internet for the long haul portion of the route is an obvious money saving scheme. It may still be necessary to provide short distance private circuits between the customer locations and the TelCo, to provide a high-speed connection into the Internet backbone. However such a connection could handle multiple VPN connections, instead of the traditional pattern of a dedicated circuit to each location.

Flexibility

Internet Protocol (IP) is a family of protocols of which TCP/IP is the best known. Most VPNs conform to a standard known as IPSec that enables the VPN to carry almost all IP protocols. Web servers, file servers, email servers, FTP servers can all potentially be accessed from anywhere on a VPN network, thus allowing a company to rationalise its information and resources in order to prevent needles duplication. The availability of IPSec VPN client software for individual Microsoft Windows PC's means that mobile (Road Warrior) or home workers can participate in the company VPN, even it be from a dial-connection in an hotel bedroom.

How does a VPN Work?

Virtual Private Networking is an umbrella term that embraces all the technologies used to secure communications over the public Internet. A VPN creates "tunnels" between two VPN Gateways to protect the private data as it travels over the Internet. Tunnelling is the process of encapsulating private IP packets into an IPSec packet; ie the private data packet is wrapped up inside the IPSec packet like the filling in a sandwich.

'Data sent over the Internet between two computer systems will pass through many computers and network systems over which the end-user has absolutely no control. Unless the data is encrypted then it is extremely vulnerable to being eavesdropped on.'

A VPN Gateway is the software/hardware combination which controls the VPN tunnels, its primary functions being:

- Allow VPN tunnels to be configured
- Authenticate the other end of a VPN connection (ie ensure it can be identified/trusted)
- Route all data received from its own local network (LAN) to the correct VPN tunnel
- Encrypt all data presented to the VPN tunnel and encapsulate it in IPSec packets
- De-encapsulate the IPSec packets received from the VPN tunnel and de-crypt the data
- Route all data received from the tunnel to the correct computer on the local network (LAN)
- Allow VPN tunnels to be managed

Once the authentication between the VPN gateways has been established the tunnel is opened and the users can send and receive data across it. There are two principal authentication methods, Pre-Shared Key (PSK or Shared Secret) and x509 Digital Certificates (see below). A VPN Gateway can normally support many VPN tunnels (depending upon licencing issues, hardware performance and speed of the Internet connection.

What is IPSec?

The Internet Protocol Security (IPSec) protocol suite was developed by an international group organised under the auspices of the Internet Engineering Task Force (IETF). An IPSec tunnel through the Internet protects all data traffic passing through it, regardless of the application. Most firewall and VPN vendors support the IPSec standard although many have made their own custom extensions to the protocol. This can make it difficult to get their supposedly IPSec standard equipment to interoperate with other IPSec solutions from other vendors. Microsoft has traditionally used an alternative VPN system called Point to Point Tunnelling Protocol (PPTP). However there are a number of weaknesses with PPTP and it is not generally considered to be very secure; the reason why virtually everybody else uses IPSec. Corporate Server will allow PPTP traffic to pass through or be forwarded by the firewall but it will not act as a PPTP gateway or client.

What are x509 Certificates?

Each VPN tunnel will normally be individually authenticated using digital certificates (x509 certificates). The certificates come in two parts, the private and the public part. Each end of the VPN tunnel must have the public part of the other ends x509 certificate. The certificate, in the form of a computer file, is an electronic document that like a driving license identifies its owner. The certificate should be unique, eg the Miami branch office certificate. For Road Warriors this should be a personal certificate. So when the Miami office goes to establish and authenticate the VPN tunnel to the Head Office VPN Gateway in New York, it is looking to be receive the public part of the New York certificate and no other. Conversely New York will expect the Miami certificate. If the certificate exchange is not as expected then the tunnel will not be opened. This guarantees that each end can trust the other. Digital certificates can be leased from companies like Verisign or Thawte, can be created by Certificate Authorities such as the one included in Microsoft Windows 2000™, or more conveniently, using SmoothTunnel's in-built Certificate Authority (CA).

What is wrong with Pre-Shared Key (PSK, Shared Secret) Authentication?

PSK authentication basically pre-dates x509 certificate authentication. With PSK a pass phrase is configured at both ends of the VPN connection. The authentication basically consists of comparing the two pass phrases - if they match then the VPN tunnel has been authenticated and is opened. This is obviously nothing like as secure as the exchange of x509 certificate information, where the certificates (files) have to be created on the same Certificate Authority. A Pre-Shared Key can be dictated over the phone so is liable to being eavesdropped, plus like many passwords, people often choose easy to remember and hence insecure phrases.

PSK certainly works and almost all VPN solutions support it - so it is often used as away to connect systems from different manufacturers. X509 certificates are undoubtedly a more robust authentication method. X509 certificates can be re-issued when necessary and be rescinded if say an employee leaves the company. This is especially important for a VPN solution supporting Road Warriors. It is basically impracticable to construct a Road Warrior VPN system using PSK, principally as each Road Warrior would need the same shared-secret, thus if one person leaves the company then all users would need to change their shared-secret. Perhaps a secret shared so widely will not be secret for very long!

What are DES and 3DES?

DES is an acronym for the Data Encryption Standard. This is a US government standard for the encryption of commercial data. It uses a 64-bit key and is nowadays considered not to be particularly secure.

Most VPN solutions now use the Triple Data Encryption Standard (3DES, pronounced triple DES) which is defined by ANSI standard X9.52. The data is effectively encrypted three times, typically using a 168-bit encryption key. This means that it will require a huge amount of time and computer power to de-encrypt the data without knowing the key in advance. It must be accepted that nothing is totally secure, all that we can do is to take sensible and realistic precautions. If the CIA decides its wants to intercept your data and is prepared to put a considerable amount of time and money into doing so, it will succeed. However to make things more difficult for potential crackers, the keys are changed every few hours, so even if somebody should work out a key then it is only of use for a short period of time.

SmoothTunnel

SmoothTunnel is the VPN Gateway module for Corporate Server. It:

- Forms the central point of a small VPN network
- Incorporate a Certificate Authority (CA) to create and issue self-signed x509 certificates

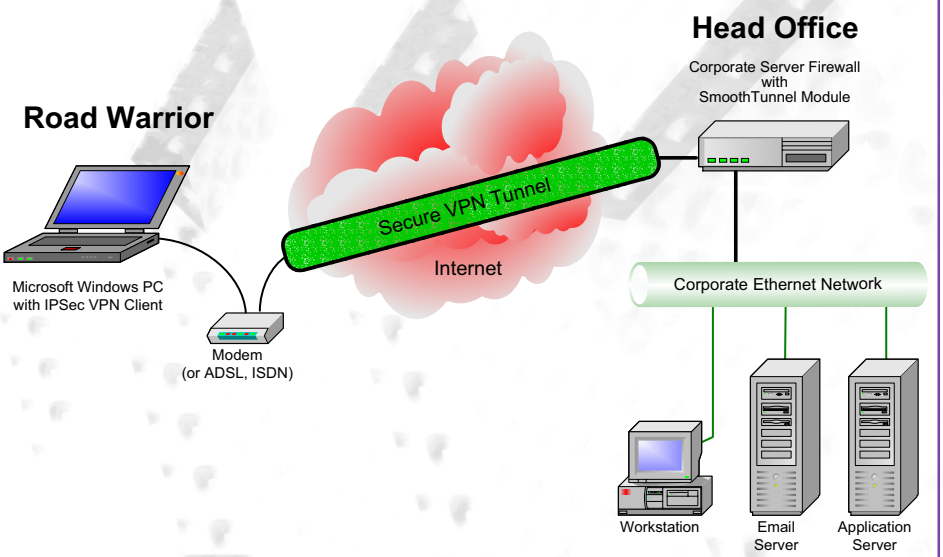
'Most firewall and VPN vendors support the IPSec standard although many have made their own custom extensions to the protocol. This can make it difficult to get their supposedly IPSec standard equipment to interoperate with other IPSec solutions from other vendors.'

'X509 certificates are undoubtedly a more robust authentication method.'

- Supports from 5 to 100 or more active VPN tunnels (depending upon hardware and Internet connections speed)
- Hosts VPN connections to SmoothNode Systems (single tunnel variant of SmoothTunnel)
- Can establish VPN connections to other SmoothTunnel Systems
- Supports VPN connections from Road Warriors using IPSec VPN Clients for Microsoft Windows™
- Can establish VPN connections to other IPSec compliant systems

There must be at least one SmoothTunnel module in a SmoothWall VPN network.

SmoothTunnel supports VPN connections from systems using Dynamic IP addresses, such as SmoothNode or Road Warrior VPN clients. SmoothTunnel itself can utilise a Dynamic DNS name to identify the VPN gateway instead of a fixed IP address, again facilitating the use of a Dynamic IP address or allowing the VPN gateway to be moved to another Internet connection in the event of a line/router failure.



In a more complex network with regional centres requiring VPN connections to both branch offices and a central Head Office, both Head Office and the regional centres would need SmoothTunnel to support the multiple VPN connections. SmoothNode would still adequately serve the branch offices, at the end of the VPN network.

SmoothConnection

SmoothConnection is a license to increase the number of VPN tunnels that can be configured on a SmoothTunnel VPN gateway. As standard SmoothTunnel allows five (5) VPN connections to be configured. This can be extended by the purchase of SmoothConnection License packs, which add another 5, 10, 20 or 50 tunnels each. The packs can be stacked, so that adding both a 10 and a 20 tunnel pack will raise the total tunnel count to 35 (including the five (5) that come as standard with SmoothTunnel).

SmoothNode

SmoothNode is in effect a cut-down derivative of SmoothTunnel for use where only a single VPN connection is required. A typical example of its use is in a branch office network. Each branch offices would be equipped with Corporate Server and the SmoothNode module, which will establish a single VPN tunnel back to SmoothTunnel VPN Gateway at Head Office. SmoothNode does not incorporate a Certificate Authority so cannot create x509 certificates; it must utilise a certificate created elsewhere, typically by SmoothTunnel's Certificate Authority. SmoothNode cannot support a Road Warrior Connection, only SmoothTunnel can do this. In all other respects SmoothNode offers the same functionality and performance as SmoothTunnel. SmoothNode can be used on a system that has a dynamic IP address, saving the need to provide a static (fixed) IP address.

Road Warriors

If only a single remote PC needs to connect to the VPN Gateway (SmoothTunnel) we class this as a Road Warrior. The term springs from travelling salesmen, managers - in fact anybody requiring computer access from a non-fixed location. However we encompass within this term most home workers, as typically they have only a single computer they use for work, rather that a small network (LAN) as would be found in a branch office.
Road Warrior/Home User PCs will need an IPSec VPN client for Microsoft Windows™. We recommend the SafeNet SoftRemote IPSec VPN client. It works well with SmoothTunnel and of the products we have tested has proved to be the easiest to set-up and get working. SoftRemote supports Windows 95, 98, ME, NT4, 2000 and XP. Although Microsoft Windows 2000™ and Windows XP™ include IPSec software we do not class this as a Road Warrior IPSec client. The reasons are that it does not support dynamic IP addresses and is generally considered to be too complex to set-up and use for Road Warriors. We class it as a VPN gateway, not a client.

Consideration must be given to protecting these Road Warrior PCs from hackers and viruses - the VPN tunnel to Head Office will be secure but if they communicate on the Internet outside of the VPN tunnel then there are risks to be borne in mind.

IP address is essential for use with multiple sub-net networks; otherwise the Road warrior would not be able to connect to servers on all sub-nets.

Having tested a number of IPSec clients for Microsoft Windows™, we have found SoftRemote from SafeNet Systems Inc. to be the easiest to install, configure and get working.

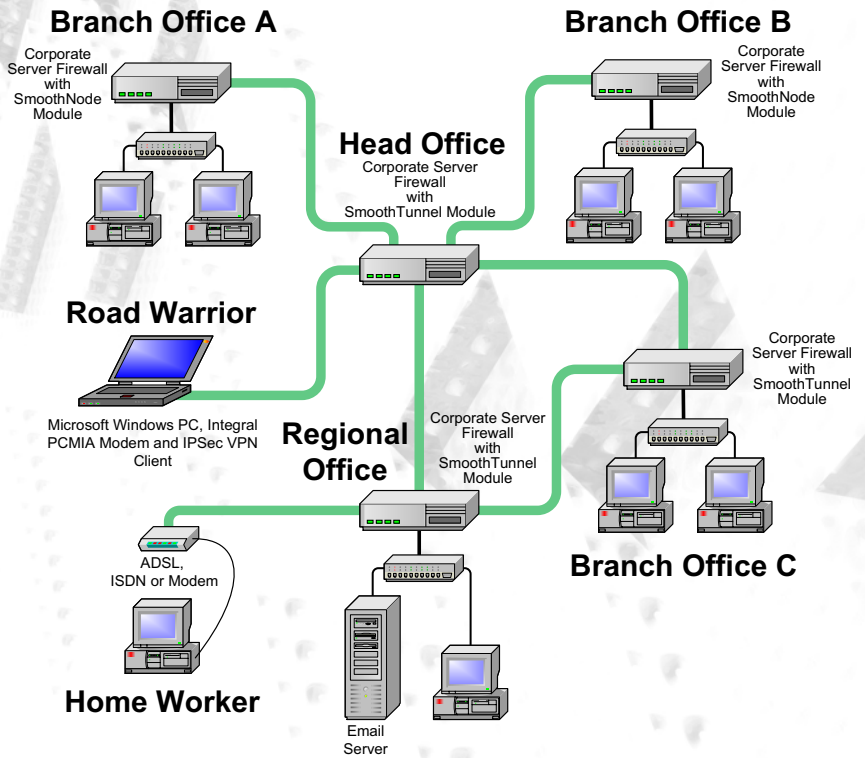
Example Network

The following diagram depicts part of a VPN for a large multi-office organisation.

The organisation's Head Office is at the centre of the diagram. It has direct VPN connections to two branch (remote) offices (A and B), at the top left and top right of the diagram. The users at these branch offices would be able to access the corporate IT services at Head Office, such as

'SmoothTunnel supports VPN connections from systems using Dynamic IP addresses, such as SmoothNode or Road Warrior VPN clients.'

email, Intranet, file and application servers. Effectively they can work and share data as though they were physically present at Head Office. The speed of operation would depend upon the speed of the Internet connections at both the Head Office and the Branch office. Normally such a Head Office would have a short distance private circuit



(leased line) to connect it to their Internet Service Provider (ISP). This will ensure that a fixed bandwidth (speed) available and is normally subject to a Service Level Agreement to guarantee uptime and time to repair if a fault develops. Failure of the Internet connection to Head Office would cause disruption to the entire organisation, whereas failure of the Internet connection to a branch office would have little effect upon the rest of the organisation. The Head Office supports multiple VPN connections so uses the SmoothTunnel module, which acts as the Certificate Authority (CA) for the entire network.

The branch offices may be connected to the Internet using ADSL, contending for bandwidth with the other users in their ADSL group (the TelCo will publish the contention ratios for its ADSL services). Thus there will be no performance guarantee, nor will the TelCo normally offer a Service Level Agreement. However ADSL normally costs a fraction of the price of a leased line connection so can be very cost effective.

The Head Office also connects to a Regional (Area) Office (bottom centre), which in turn connects to Branch Office C at the bottom right of the diagram. This, for example represents an international organisation, where branch (country) offices report to a regional office and in turn, the regional offices report back to Head Office. The Regional Office has the SmoothTunnel module, as it needs to support multiple VPN connections, ie to its branch offices and Head Office.

The network also illustrates a Road Warrior who can open a VPN connection from their notebook PC using a dial-up (modem) connection to the corporate data centre at Head Office. The organisation's network also supports Home Workers who connect to Regional Offices. ADSL would probably be the first choice for these connections with ISDN, satellite, wireless or analogue modem being the alternatives, mainly dependent upon geographic location. Depending upon how the VPN tunnels are configured, users can "tunnel through" one SmoothWall system to another network.

Depending upon how the VPN tunnels are configured, users can "tunnel through" one SmoothWall system to another network. Branch Offices A and B could for instance access the servers at the Regional Office, so there is no need to configure a VPN tunnel between each location which needs to share resources. However the two branch offices "tunnelling through" Head Office will obviously consume bandwidth (in and back out again) and increase the workload upon the Head Office Corporate Server. For occasional usage this is probably sensible but if frequently used then a direct VPN tunnel would probably be provided. It should also be borne in mind that "tunnelling through" can present a security risk, it may not be desirable for branch office users to gain access to the systems at other branch offices etc. Thus this aspect needs careful consideration to user limit access.

Branch Office C has a direct VPN tunnel back to Head Office to provide a degree of redundancy should the connection to its Regional Office fail. Although the above diagram represents a relatively simple star network, cross links can be added where required to provide both direct tunnels avoiding "tunnelling through" and increase redundancy in the event of failure somewhere in the network. As Branch Office C has two VPN tunnels it will need the SmoothTunnel module.

Hardware Requirements

Corporate Server will run on virtually any Pentium class machine. However in the case of a SmoothTunnel VPN gateway supporting several VPN tunnels, we normally recommend that the machine specification meets or exceeds a Pentium III 500 MHz, with 64 MBytes RAM and 4 GBytes hard disk. Reputable (branded) Ethernet cards are also strongly recommended. Such a specification should be capable of supporting 50 VPN tunnels. SmoothNode can operate on a minimum specification system, ie Pentium with 32 MBytes RAM and 250 MBytes hard disk.

SmoothWall Limited
Suite 325, 80 High Street
Winchester, Hampshire
SO23 9AT, UK
Tel: +44-(0)7092-377632
Fax: +44-(0)113-203-7352

Email:
sales@smoothwall.co.uk

WWW:
www.smoothwall.co.uk