Understanding VPNs And PPTP

A Virtual Private Network is an efficient and cost-effective way to set up a WAN by using the Internet for the long-distance communications.

By Kevin Townsend

If you manage anything more than the smallest of LANs, the question is probably not so much "Do I need a VPN?" as "How soon should I implement one?".

The business world is marching inexorably towards a paradigm that demands VPN (Virtual Private Network) technology. Telecommuting and e-commerce are growing and inevitable. And virtual private networks are the ideal solution for such a world.

Definition

So what exactly is a VPN? There are several answers to this question. Primarily, there are two types: voice-carrying and data-carrying.

Voice VPNs developed with the advent of increased telecommunications liberalization. They serve to simulate a private network at a considerably lower cost than the basic public switched network. They started primarily in the USA, but have become global over the last few years. Sprint, AT&T, Global One and Uniworld/World Partners are example providers.

There are several variants of data-carrying VPNs. One occurs when the entire network requirements are outsourced, probably to a carrier. A second variation occurs where two or more LANs are linked together using the Internet as the connecting medium. This would require the use of intranet technology at the two LAN sites, together with firewalls between each site and the Internet itself.

While this approach has some advantages, it is static. If you are not connected to one or other of the LANs, then you are not connected to the VPN. It furthermore operates best only where the intranet technology (use of Web browsers, Internet email and so on) is strongly woven into the operational organization of the company.

It is the third variant data-carrying VPN with which this article is primarily concerned. This is dial-up connection from a remote user to the corporate LAN across the Internet. Its primary advantage over other data VPN variants is its flexibility. New users can be added, and existing users are not tied to any specific geographic location.

So that's the basis for what follows: point-to-point VPNs using the Internet as the transmission medium. I shall be considering the arguments in favour of implementing such a VPN, the requirements for a successful VPN, and how the various elements work and should be combined.

Why Do It?

There are many reasons for implementing such a VPN. Fundamentally, the nature of business is changing. The notion of the office as a geographic and essential central location for all workers is shifting. More and more people are using computers to work from home, from customer sites, from hotel rooms, from the car or train or plane etc. It has been estimated by AT&T, for example, that home working can provide up to 45% productivity gains.

But what hasn't changed is that the central office remains the primary location of corporate data. To work to full capacity from remote locations we consequently need to network our remote PCs and the central server, and this needs to be done as easily, as transparently and as economically as possible.

Technically, this has long been possible but costly. You could dial into your office computers from almost anywhere in the world. But leased lines are costly and fixed, and the cost of long-distance PSTN calls can rapidly become excessive. And, of course, the vast banks of necessary modems are both costly and potential bottlenecks (not to mention security risks).

The primary argument given for implementing a VPN is thus usually cost. Vast savings (the usually quoted figures are between 40% and 50%) can be made by switching from PSTN dial-up with its high costs to the usually local charge for connecting to the Internet.

All you need are the right tools for a VPN and an Internet Service Provider (ISP) able to support VPNs and offer global roaming (ie, with local access numbers in the same parts of the world as your callers).

Cost is not the only argument - productivity is another. It is generally considered that users are more productive when working from home, or at least away from the main office. There are fewer social interruptions from workmates, and no loss of time spent commuting. But this requires turning the user's local environment, whether it be the home, a customer site, a hotel room or all three, into a virtual office. And this can only realistically be done by connecting the PC to the corporate network in as transparent a way as possible. That is, with a VPN. Without access to the central data, the type of work that the remote user can perform is limited.

There are other potential benefits

too. E-commerce will drive the world's economy in the next millennium - and it is already a force to be reckoned with. There seems little point in simply using your Web site to advertise your wares when it can also be used to actively sell them. And if you're selling goods over the Internet, perhaps you should also be buying them. And if your company is big enough, and your products and needs are multifarious and repetitive, then perhaps you should be allowing both your major customers and suppliers to order from and supply to your stock systems. It makes a lot of sense. It would be efficient and excellent for good customer relations. This is best done via a virtual private network, where major suppliers and customers (and partners and contractors) can directly access their accounts on your systems (suitably secured, of course). So there is little doubt that the arguments in favour of implementing a VPN are growing. If they are not yet overwhelming, they soon will be.

How To Do It

The Internet is the obvious choice of transmission medium because of its universal availability. This is where global roaming comes in. If your ISP's only access point is in Sydney and you're visiting California, you are still faced with long-distance telephone charges whenever you connect. Unless your ISP offers global roaming (or, like AOL and CompuServe, has access points all over the world).

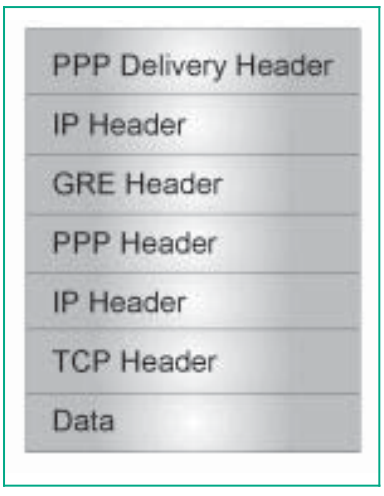

Figure 1 - The structure of the IP datagram.

Global roaming is a new concept, and as such you may have heard of it under a different name (some people simply call it "roaming service"). The two primary providers are iPass (http://www.ipass.com) and Aimquest's Global Reach Internet Connection (http://www.aimquest.com). A description of the iPass service will show how it works and its value to the VPN.

The iPass system is actually a network of ISPs. Provided that your own ISP delivers the iPass service, you can access the Internet via the nearest point of presence of any other iPass ISP anywhere in the world. For example, an Australian user visiting the UK would be able to use a UK ISP offering local call dial-up to get on to the Internet and thence to his own ISP to collect or send any email. The cost would simply be the local call charge plus any charge levied for the service by his Australian ISP. It would undoubtedly be cheaper than dialling Australia from the UK.

The iPass system itself claims to have more than 2500 Points Of Presence (POPs) in more than 150 different countries - and this number is increasing all the time. The service is transparent. You can use any platform, and can use the browser and email system of your own choice. Your ISP or company provides you with the iPass Dial Wizard or the Microsoft Connection Manager to install on your laptop. This is a simple client software tool that contains an international phone book of iPass access numbers.

From anywhere in the world, you need just point and click with the iPass client software to connect to a local Internet access number. You would then log in with the same userid and password that you usually use, but including your domain name after your userid (eg, yourname@yourdomain). The local ISP recognises that you are an "alien" and forwards your user name and password (encrypted) to your own ISP. Provided that everything is correct, you are then logged on to your own ISP account.

It is relatively easy to see that this process requires very little adaptation to provide roaming access to your own virtual private network. In principle, you simply need to connect your own corporate network to the Internet. Then, when working from home or travelling, you use a local ISP to provide access to the Internet and from there to your corporate Net. This can be done with tunnelling.

Tunnelling

Tunnelling, also known as encapsulation, is not a new technology. It is the process of encapsulating or enclosing one type of data packet (as used by your own LANs) inside the packet of another protocol, in this case TCP/IP as used by the Internet. Once the data has been enclosed within TCP/IP, it can be transmitted across the Internet.

But encapsulation is not all that is needed for a VPN. You also need user authentication to ensure that only authorised users can log onto your private network, and encryption to ensure the privacy of your data across the Internet. There are many proprietary products that can help you achieve this. Some use their own technologies, but the two standards are Microsoft's PPTP (Point-to-Point Tunnelling Protocol) and Microsoft/Cisco's L2TP (Layer 2 Tunnelling Protocol).

PPTP is an extension of the remote access Point-to-Point Protocol (PPP - which is defined and documented by the Internet Engineering Task Force in RFC 1171). PPTP technology encapsulates PPP packets into IP datagrams for transmission over TCP/IP-based networks. It is packaged with NT 4 server and workstation, and also within Win95's Dial Up Networking - so it has the advantage of being widely available.

Data is transmitted in IP datagrams containing PPP packets. The IP datagram is created using a modified version of the Generic Routing Encapsulation (GRE) protocol (GRE is defined in RFC 1701 and 1702). The structure of the IP datagram is shown in Figure 1.

Three systems would be involved in such a point-to-point VPN: the client, an ISP (for the Internet), and an Internet server on your private network.

VPNs And PPTP

For the sake of this example, the client could be a remote NT or Win95 workstation, while the ISP would be your chosen ISP (or indeed any local iPass ISP if you have implemented global roaming and your local ISP doesn't have international numbers).

Needless to say, the client must have PPTP installed, a modem, and the ISP connection. The first stage in connecting the client to your server is modem dial-up to the ISP using the PPP protocol. The second stage is a VPN connection using PPTP, over the modem and through the ISP. The second connection requires the first connection because the tunnel between the VPN devices is established using the modem and PPP connections to the Internet.

The exception to this two-step process is using PPTP to create a VPN between computers physically connected to a LAN. In this scenario the client is already connected to a network and only uses Dial-Up Networking with a VPN device to create the connection to a PPTP server on the LAN. You would use this approach if you were providing direct access for a remote but static user to your private intranet.

The overall process is thus threefold. The PPTP client uses PPP to connect to an ISP on the Internet and encrypt the data packets (we'll come back to the encryption later). Using this connection, the PPTP protocol then establishes a control connection to a PPTP server on the Internet (that is, your private network's Internet server). This is the PPTP Tunnel. The client then creates IP datagrams containing encrypted PPP packets and sends them through the PPTP Tunnel to the PPTP server. This server disassembles the IP datagrams and decrypts the PPP packets, and then routes the decrypted packet to its destination.

PPTP Security

A PPTP VPN is generally from Win95 or NT Workstation to NT Server. Consequently, it can and does use the authentication and encryption security available to computers running RAS under NT Server 4. PPTP can also protect the PPTP server and private network by ignoring all but PPTP traffic.

An initial dial-in authentication will probably be required by the ISP network access server. This is an additional level of security (often RADIUS-based, and probably a username and password) that is not part of PPTP. It will not be required if you are directly accessing a private intranet.

Your PPTP server is a gateway to your network. It will consequently require the standard NT-based logon procedures. The client must therefore provide a correct username and password. In theory, then, a remote access logon using a client running under NT or Win95 is as secure as logging on from a PC directly connected to your LAN. Authentication of remote PPTP clients is done by using the same PPP authentication methods used for any RAS client dialling directly into an NT server: it fully supports CHAP (Challenge Handshake Authentication Protocol), which uses the MD4 hash as well as earlier LAN Manager methods.

Following successful authentication, all access to the private LAN continues to use existing NT-based security structures. Access to resources on drives or to other network resources requires the proper permissions, just as if you were connected directly to the LAN.

For data encryption, PPTP uses the RAS "shared-secret" encryption process. It is referred to as shared-secret because both ends of the connection share the encryption key. Under Microsoft's implementation of RAS, the shared secret is the user password.

PPTP uses the PPP encryption and PPP compression schemes. The CCP (Compression Control Protocol) is used to negotiate the encryption used. The username and password is known to the server and supplied by the client. An encryption key is generated using a hash of the password stored on both the client and server. The RSA RC4 standard is used to create this 40-bit (128-bit inside the US and Canada is available) session key based on the client password. This key is then used to encrypt and decrypt all data exchanged between the PPTP client and server.

Network security against intruders can be enhanced by enabling PPTP filtering on the PPTP server. When PPTP filtering is enabled, the PPTP server on the private network accepts and routes only PPTP packets. This prevents all other packet types from entering the network.

Weaknesses Of PPTP

We can thus see that a PPTP-based VPN provides the three necessary basics: the tunnel, user authentication and data encryption. It is not, however, without its own problems. The first and most obvious is that encryption is limited to 40 bits outside the USA - and this is known to be insecure. Secondly, all Microsoft software is coming under intensive scrutiny for flaws and "hacker" exploits. One has already been found and published on the Internet.

NT 4.0 with SP3 and RAS PPTP is vulnerable to a denial of service attack. If you send a PPTP start session request with an invalid packet length in the PPTP packet header, it will crash an NT box and cause the NT server to do a core dump. [*You'll find the patch for this on your CD - Ed.*]It is generally expected that more flaws will be found.

A third problem can be found in the lack of any inherent key management within PPTP itself. The encryption is based on a "shared secret"; that is, both ends of the tunnel must know the encryption key (username and password). Since this is used for every

"If you send a PPTP start session request with an invalid packet length in the PPTP packet header, it will crash an NT box."

"Good password management demands that users' passwords are regularly changed. This in itself can cause administrative problems."

connection, if the key is stolen or broken it is compromised for all future transmissions.

Good password management demands that users' passwords are regularly changed. This in itself can cause administrative problems. However, if the VPN includes hundreds of different users, you will not only need to manage regular password changes, but will need to find some way of securely ensuring that both ends of the tunnel are aware of changes to the shared secret.

Finally, of course, PPTP will lock you into Microsoft Windows until a Unix implementation of PPTP is made available.

Alternatives

If the above warnings turn you off the idea, the primary alternative is L2TP (others include Mobile IP and SOCKS). L2TP is actually a convergence or combination of elements of Cisco's earlier L2F protocol with PPTP. In this sense, L2TP can be viewed as the successor to PPTP.

While PPTP is also an extension to PPP, L2TP is designed to tunnel the link level of higher level protocols over the Internet. Specifically, it is designed to tunnel PPP and SLIP sessions. One problem, however, is that an ISP must have L2TP-enabled hardware at each of its POPs in order for customers to take advantage of it, a problem for ISPs that is similar in nature and scale to deploying new 56 Kbits/sec modem support.

Another alternative would clearly be to implement a proprietary VPN from one of the leading VPN suppliers. This would have at least three strong advantages: it would reduce your development workload; it could provide stronger encryption than you would get using, say, PPTP outside of the USA; and it could include its own key management facilities. There are, however, dangers to this approach. You should, as always, avoid any supplier that supports only its own proprietary technologies. This is particularly relevant given that there are three primary protocols (PPTP/L2TP and IPsec) that are supported by Microsoft and the Internet Engineering Task Force respectively.

The universality of Microsoft and the importance of the IETF effectively guarantee that these protocols will dominate. And as support for the protocols is increasingly built into operating systems, it is likely that users will more and more develop their own VPN implementations. There must, therefore, be a question mark over the future of the market for VPN manufacturers - and you must be sure that you do not lock yourself into a costly mistake.

Having just mentioned IPsec for the first time, a brief explanation is called for. IP Security (IPsec) is the proposed IETF standard for IP security. It defines a set of standard security protocols that authenticate TCP/IP connections. It specifies encryption and authentication, but it does not include any method of access control other than packet filtering.

The goal of the IPsec protocol suite is to provide Layer 3 secure tunnelled transport of IP packets. Essentially, it takes private IP packets, performs data security functions such as encryption, authentication and integrity, then wraps these secured packets in other IP packets for transport across the Net.

Key management functions will also be a part of the IPsec protocol suite: Simple Key Management for Internet Protocol (SKIP) and Internet Security Association Key Management Protocol (ISAKMP).

The IETF has already issued five foundational requests for comments on the IPsec protocols - RFCs 1825 to 1829. An interesting note is that if IPv6 succeeds in replacing IPv4, IPsec will be the automatic Internet VPN standard since it is integrated into the IPv6 specifications.

Conclusion

So, to go back to the initial question: how soon should I implement a VPN? The answer is probably "As soon as I can develop one that is compatible with, and can evolve into, an IPv6 IPsec virtual private network".

If all this sounds appealing, the next step is to talk to your ISP (and a selection of other local ones) and find out about the VPN services on offer.

Note: *You will find some additional relevant documents on this month's CD, including a paper from a pair of researchers who claim to have found some security weaknesses in Microsoft's implementation of PPTP.*

PCNA

The Author

Kevin Townsend is a freelance writer, and editor of Information Security Bulletin. Educated at Oxford University, and a member of the ITSEC Industry Working Group, he specialises in information security matters. You can email him as kevin@oakworth.demon.co.uk.

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews
A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers
Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software
In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs
There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.