
Understanding VPNs

IP-based Virtual Private Networks (VPNs) across the Internet are swiftly overtaking the conventional technologies of remote access dial-up servers and expensive leased-line WANs, but can frequently be complex to configure and maintain.

By Andrew Ward
Technology Journalist

An ever-increasing reliance on IT, accompanied by a growing trend for people to work from home or while travelling, are together driving demand for provision of remote access to the corporate network. It's now widely accepted that using Virtual Private Networks (VPNs) over the Internet provides a cheaper, easier and more flexible means of delivering this access than the traditional technology of dedicated remote-access dial-in racks and servers. But there are many different ways to implement a VPN, and the right choice will depend on several factors, such as the number of users, the required scalability, what existing network infrastructure you have and the locations of any remote workers.

IP VPN WANs

IP VPNs are finding a second market, in addition to providing remote access. For organisations with more than one site, VPNs provide a low-cost means of interconnecting the networks at these premises to build a Wide Area Network (WAN). Sometimes known as intranet VPNs, their natural extension is to include partner organisations such as customers and suppliers in an extranet VPN.

For WAN use, the choice of topology is generally clear-cut. Since your corporate IT infrastructure will be reliant on the WAN, your best option is to use a single service provider to supply the Internet connections at each site. That way, you can obtain a Service Level Agreement (SLA) that specifies such parameters as the availability of the connections over a year. A service provider can issue such an agreement with confidence, because all your traffic will be travelling over the provider's own network backbone, rather than over the public Internet. The service provider thus has much greater control over the bandwidth and reliability of the service.

IP VPNs provide security by encrypting your network traffic as it crosses the public Internet. Therefore, you can take advantage of the low cost of Internet bandwidth compared with expensive leased lines for WAN use, while being confident that your data is safe from prying eyes.

Terminating A VPN

Even with the relatively straightforward WAN model, there are a number of different possible topologies. Encryption will normally be carried out by equipment on your premises, but you have the choice of whether this takes place within the router, the firewall, or on some other device. To terminate a VPN within an existing router or firewall will almost certainly entail upgrading the embedded software, and you'll probably need upgraded hardware to provide sufficient performance to carry out the required encryption and decryption. If you wish to avoid changing or upgrading an existing firewall or router to terminate your VPN, a drop-in dedicated VPN server can be used instead.

If your VPN server is outside the firewall, then traffic between it and the firewall will not be protected. If it is inside the firewall you may encounter problems with passing the encrypted traffic through the firewall, especially if you are using any form of Network Address Translation (NAT). For most purposes, termination of the VPN within the firewall itself will be the most practical solution, and firewalls do generally support VPNs as a standard feature. To overcome performance and scalability issues, some use hardware devices to perform encryption.

Remote Access

For remote access solutions, implementation of a VPN is a great deal more complicated. Users are connecting from a variety of different locations, using different

Internet service providers, myriad access devices such as modems and routers, and a variety of different desktop computers and operating systems. Your choice will also be partly dictated by whether you have the resources and desire to configure and support your own solution built using general-purpose components such as Windows 2000, or prefer to go for a fully-managed solution from a service provider.

Service Provider Models

Service provider models for remote access VPNs rely on the provider to encrypt data from remote users when it reaches their dial-up access nodes, and are therefore really only sensible where it is likely that all remote users will be able to connect using the same ISP. A distinct advantage of this solution, however, is that no additional software is required on the users' PCs. They simply connect to the appropriate dial-in access number, and the secure connection is taken care of thereafter. With the service provider model, decryption of data coming into the organisation, and encryption of outbound data, takes place within the service provider's network. This assumes that the link between your premises and the service provider is secure.

A variant of this model places the responsibility for terminating the VPN tunnels from remote users back with you, using a VPN server on your premises. This suffers from the same disadvantage as the service provider model, and also means responsibility for the VPN is split between your organisation and the ISP, which could make it more difficult to track down and resolve problems.

Enterprise Models

Remote users will frequently be accessing the Internet via some sort of router when connecting via ISDN, ADSL, a cable modem or even from a client or partner company's network. However, an edge-to-edge VPN - where the security tunnel terminates in an edge device at each end - would be impractical, because of the number of different devices in use. Not all of them will support VPNs - they will be incompatible - and many will also be managed by the service provider, making it difficult to change their configuration. Normally, therefore, a remote access VPN will start at the remote worker's client device, usually a PC. This necessitates either the installation of additional software, or configuration of the existing operating system if that provides any VPN support. Which of these you want to do is likely to significantly influence your choice of VPN protocol.

PPTP Or IPsec

The most fundamental decision to be made when considering a VPN is which protocol to use. There are now two major contenders - IPsec and PPTP. Previously, there were proprietary implementations by vendors such as Check Point and Shiva, but of course these were not interoperable. Now, IPsec support is widespread, and interoperability is starting to become more realistic.

PPTP is Microsoft's VPN support, built into Windows NT 4.0, Windows 2000 and Windows 95/98. Client software is included with each of these operating systems, but to implement a VPN server you'll need Windows NT 4.0 Server. Windows 2000 Professional does include support for a single VPN server, but that's all. In the Network And Dialup Connections control panel, select Make New. A wizard offers you the choice of Accept Incoming Connections, which will allow you to configure one VPN server. However, PPTP isn't as secure as IPsec. Although PPTP in some versions does provide 128-bit encryption using the RC4 algorithm, the key is derived from the user password and there's no key management. Standard brute-force techniques can be used to guess passwords and decrypt PPTP data. By contrast, IPsec uses public key cryptography, although this does have the attendant problems of key distribution.

In some cases, which protocol to use will be decided for you. If you use any non-IP protocol, IPsec won't be of any help, since it only works with IP. Although other alternatives exist, including L2F (Layer 2 Forwarding) and L2TP (Layer 2 Transport Protocol), they have practical limitations and don't provide native support for encryption anyway. You'll be stuck with PPTP. If you opt for PPTP and your users have Windows-based PCs, you won't need to add any software to their desktop systems. However, for IPsec, you'll need to install, configure and maintain IPsec

“For devices with hardware decryption and encryption circuitry, performance shouldn't be an issue; however, for software devices, any encryption will have a significant impact on the throughput”

client software. Vendors of remote access servers, including firewalls and routers, do usually include client software in the price of their products. However, this isn't always the case, so check exactly what you're being quoted for. There are also third-party IPSec client software products, such as Soft-PK from SafeNet. Designed to be standards-compliant, this can be used with VPN servers from RADGUARD and others, and in fact is sold by several VPN server vendors under their own brand names.

NAT

NAT is widely used to allow support for more than one PC at a single IP address, or to provide some additional security by hiding a network's IP addresses. However, there are several issues that stop PPTP and IPSec from working over NAT-based devices. Although in many cases there are upgrades or configuration workarounds, the sheer number of different devices that you might have to contend with when managing remote users makes the task distinctly daunting.

In the case of IPSec, the problems stem from the Encapsulating Security Protocol (ESP) used, which is IP Protocol 50. Normally, NAT or PAT (Port Address Translation) devices will only recognise TCP, UDP and ICMP, and therefore can't correctly translate ESP packets. However, many devices are now starting to add IPSec support. For example, the Linksys range of cable modem routers features IPSec pass-through to allow home users to connect with IPSec servers on corporate networks. Some IPSec implementations provide support for NAT gateways by encapsulating ESP traffic within UDP packets. For this to traverse a NAT gateway, you may have to ensure that the ports used (depending on what options you choose these can be UDP ports 259, 500, 1723 and 2746) are passed through to the PC running the VPN client software. You may also have to configure the device to permit packets with an invalid checksum, since applying NAT to AH packets (see box) can destroy the checksum. Where specific passthrough support is provided, you shouldn't have to enable any ports.

Similar problems occur with PPTP and, once again, the router vendors have responded. Recent products will therefore usually feature PPTP pass-through. For example, this is now a standard feature in WebRamp routers. For a specific router, you should consult the vendor's documentation. There is usually a workaround, although in some cases you may have to face restrictions. For example, to use the

“Note that both IPSec and PPTP can be used with dynamically-assigned IP addresses, which is what many remote users will have when they connect via the dial-up lines of various ISPs.”

IPSec - A Summary

IPSec uses three main protocols:

- IP Authentication Header (AH), IP protocol 51, provides authentication of the origin of the data, ensures data integrity, and protects against replay.
- IP Encapsulating Security Payload (ESP), IP protocol 50, protects data from viewing by third parties, and provides the same features as AH.
- The Internet Security Association and Key Management Protocol (ISAKMP) is a protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

IPSec can be used in two modes:

- Transport mode is normally used between the end points of a connection - for example, to establish a secure connection such as a VPN between a client device and a server.
- Tunnel mode is normally used between two systems where one or both of them are not the endpoint of the connection. For example, to communicate between a firewall and a VPN server on a LAN, or between a remote dial-in system and an edge device such as a router or gateway, you might use tunnel mode (or IPSec tunnelling).

Tunnel mode and transport mode are implemented in different ways. In transport mode, the IP header of a packet is modified, and has a trailing IPSec header added to it. In tunnel mode, the entire packet is wrapped with a new IP header that has a trailing IPSec header attached to it.

Check Point SecuRemote client, you firstly need FireWall-1 version 4.0 or later, and client software build 4003 or higher. Even then, with a many-to-one NAT translation, only one user at a time can use SecuRemote, unless you use UDP encapsulation. With older routers and other access devices you may encounter problems when trying to support PPTP or IPSec. It's always a good idea to update the device firmware to the latest available, but even that may not help you. Many users will be unable to reconfigure the devices in their homes, since they will be entirely under the management of their Internet service provider or telecommunications company. In that case, there's not much you can do about it.

Note that both IPSec and PPTP can be used with dynamically-assigned IP addresses, which is what many remote users will have when they connect via the dial-up lines of various ISPs. However, they do need the server to be located at a fixed IP address. In smaller companies or branch offices, where the server may be implemented in software (perhaps on a Windows NT machine) behind a router, this may present a problem in that the system won't have a fixed or public IP address. Some routers and proxy devices will allow you to overcome this by specifying that incoming PPTP traffic goes to a specific machine - the one running your VPN server software.

VPN Servers

Just as with a traditional remote access server, you'll need to pay attention to the number of concurrent users you want to support, both now and into the future. Pricing for standalone VPN Servers can range from a few thousand US dollars for models supporting 50-100 users, up to over US\$100,000 for models supporting tens of thousands of concurrent VPN tunnels. Generally speaking, larger devices such as these will use hardware for encryption and decryption in order to achieve the necessary performance. Where smaller devices (such as 3Com's OfficeConnect firewall) provide VPN support for up to 25 users, this is implemented in software for reasons of economy.

RADIUS Authentication

Many VPN solutions support the use of an external RADIUS authentication provider to check user credentials. A connection request is sent from the VPN server to the RADIUS server, which will either refuse or allow the request. The server will also have a central database of other user properties, such as access permissions and maximum session time. A RADIUS server can either fulfil these requests from its own database, or seek the information from another source, such as an enterprise directory using NDS (Novell Directory Service). Part of the workload of managing a VPN therefore includes the administration and maintenance of VPN fields within the user authentication database.

High Availability

Usually, when you've invested in a VPN for use by hundreds or even thousands of users, it's not merely to make it slightly more convenient for remote workers to collect their email, but because the applications they're running are mission-critical. As with any other IT system or infrastructure element, you'll want to ensure that it's sufficiently reliable. Two of the options you can consider are its balancing and clustering. Load-balancing VPN implementations are of necessity proprietary, since there is no provision within either PPTP or IPSec for such services. However, it is easier to achieve with PPTP than IPSec, since IPSec load-balancing requires sharing both state and IP identity information between the devices, but presenting an IPSec-compliant interface. Certain vendors such as RADGUARD provide failover support within their products so, if the device fails, the second unit takes over almost instantaneously. While this does provide good availability, it's at a price.

OS Support

PPTP is built into Windows as standard, but if you're implementing it on Windows 4.0 you'll need to ensure that you have the major RRAS (Routing and Remote Access Server) upgrade installed. However, there are also PPTP products available for Linux. If you want to use a Linux server to implement PPTP, it's worth looking at PopTop (on the Web at poptop.lineo.com). This works with Windows 2000 clients as well as Windows 95, 98 and NT 4.0. Anyone using Linux on a desktop PC can

“The most fundamental decision to be made when considering a VPN is which protocol to use. There are now two major contenders - IPSec and PPTP.”

still participate in a PPTP VPN with PPTP-Linux, available on the Web from cag.lcs.mit.edu/~cananian/Projects/PPTP/.

Windows 2000 includes IPsec as well as PPTP. Support for tunnelling is only provided where both tunnel endpoints have static IP addresses, so it's not suitable for client remote access VPN use. Client remote access VPN is provided using IPsec transport mode. Using PPTP requires extensive configuration at both ends of the VPN link (see box). One ingenious way to avoid this is to use built-in router PPTP client capabilities, such as those found in WebRamp products, for example. This technique is faster than using PPTP pass-through, and provides support for all users on the network. Of course, this means that anyone can use PPTP, regardless of their operating system.

Encryption Strength

Once you've decided on the security protocol, you then have a choice of encryption types and strengths. This decision will be a trade-off between security, performance and compatibility. For devices with hardware decryption and encryption circuitry, performance shouldn't be an issue; however, for software devices, any encryption will have a significant impact on the throughput of the device. Taking WebRamp as an example, even within IPsec there are several different security options. ARC4 has the least impact on performance, DES uses a 56-bit key length and has a very significant performance impact, and DES RFC1829 is an alternative encryption scheme provided for compatibility with Check Point FireWall-1. Finally, a scheme using HMAC MD5 for authentication will have the biggest impact of all on performance.

Configuring PPTP

To configure a PPTP VPN using Windows NT 4.0, you will need to allocate one Windows NT machine on the corporate network as the VPN server. You can choose to install two network interface cards, one for the Internet and one for the internal network. Remember also that, for PPTP to work, the server must have a legitimate fixed IP address presented on the public Internet.

Microsoft has implemented PPTP in such a way that it uses virtual devices called VPNs that you install and configure in RAS (Remote Access Service) as if they were physical devices like modems. Note that you only need install PPTP on the client and server machines, and not on any other machines on the network. The first step on the server is to add PPTP just as you would any other network protocol, using the Network control panel. You do need to specify the number of concurrent VPN client connections that you want to support. You must then select Add to add the VPN devices themselves to RAS. The Add RAS Device properties dialog box will appear, and will include a drop-down list of RAS Capable Devices that you must add one by one. Now, for each VPN port you must click Configure and check that the Receive Calls Only option is selected. This is the default setting, but you should check it. When you've finished checking all VPN ports, click OK to return to the Remote Access Setup properties dialog box, and then Continue. Close the Network control panel, and restart the machine.

To install the PPTP client on Windows NT 4.0, follow the same procedure as for the server to add PPTP as a new network protocol. Then create a RAS Phone Book entry for the VPN connection. This entry looks like any other Phone Book entry, with two exceptions: an IP address appears in place of a telephone number, and the Dial Using pull-down list includes a PPTP option. Where the user is connecting via a LAN modem, or an ISDN, cable or ADSL router, then all the user has to do is dial the appropriate phone book entry to establish the VPN connection over the Internet. If the user is also using RAS to connect to the Internet via a dial-up connection, then clearly that connection must be made first before the VPN entry can be activated. It's possible to activate both connections from one autodial phone book entry.

To install the PPTP client on a Windows 2000 system, go to the Network And Dialup Connections control panel, select Make New, and when the wizard starts up choose Connect To A Private Network Through The Internet. Then all you have to do is specify the IP address of the VPN server, and choose a convenient name for the connection. Remember that your VPN may well not work unless any other network devices in the path between the two systems, in particular firewalls, are sympathetic to PPTP and can be instructed to allow PPTP connections to pass through.

“IP VPNs provide security by encrypting your network traffic as it crosses the public Internet, and you can therefore take advantage of the low cost of Internet bandwidth.”

Solutions | Products | Ordering | Support | Partners | Training | Corporate

Cisco Enterprise Solutions

Virtual Private Networks

CISCO SYSTEMS

Home | What's New | How to Buy | Login | Register | Feedback | Search | Map/Help

Enterprise > Technology Solutions > Virtual Private Networks

SECTION HOME

Why Cisco?

Research & Plan

Technology Solutions

Business Solutions

Design & Build


Design Guidance

Choose Products

Purchase Products

Get Support

Virtual Private Networks (VPNs) use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets.



Benefits of VPN Include:

- **Cost Savings** - By leveraging third party networks, with VPN, organizations no longer have to use expensive leased or frame relay lines and are able to connect remote users to their corporate networks via a local Internet service provider (ISP) instead of via expensive 800-number or long distance calls

References

VPN Servers and clients:

Check Point
www.checkpoint.com

Shiva
www.shiva.com

RADGUARD
www.radguard.com

WebRamp
www.webramp.com

Nortel Networks
www.Nortel.com

3Com
www.3com.com

SafeNet
www.safenet-inc.com

IPSec further reading:

www.ibm.com/software/network/library/whitepapers/vpn/ipsec.html

IPSec and NAT:

IETF RFC 2709

Windows 2000 Knowledge Base Articles:

Q265112 IPSec and L2TP Implementation in Windows 2000

Q252735 How to Configure IPSec Tunneling in Windows 2000

For technical questions on VPNs try the following newsgroup:

news://comp.dcom.vpn

LAN Routing

If you have a VPN server implementation with two network cards, you will then need to configure routing so that packets from the PPTP client are sent to the correct destination computer. First, you need to enable IP forwarding, under the Routing Properties sheet for TCP/IP in the Network control panel. Then you need to prevent Windows NT placing a default route on each adapter in the computer. Add the registry entry DontAddDefaultGateway with a value of REG_DWORD 0x1 in the following registry key for each adapter: HKEY_LOCALMACHINE\SYSTEM\CurrentControlSet\Services\\Parameters\Tcpip\DontAddDefaultGateway. After the DontAddDefaultGateway entry is created you must stop and restart the computer, and then add static routes for each network adapter. These static routes must configure the PPTP server to route incoming data from the Internet to the correct server on the private network. Use the route command with the persistent (-p) option. For example, to add a route to a server at IP address 192.163.192.17, type the following command: `route add -p 192.163.192.17`. Do this for every computer or network that you want PPTP clients to have access to, otherwise the PPTP server would issue a broadcast for every address required by PPTP clients.

Configuring proprietary VPNs is sometimes much easier. For example, WatchGuard Technologies provides a wizard that has a point-and-click interface to select the home networks you want to allow clients access to, and the protocols they can use.

Conclusion

VPNs provide a convenient and cost-effective way for branch offices, remote workers and partner organisations to access your corporate network. But although the procedures outlined here appear straightforward, like dial-in remote access servers, VPNs are notorious for being difficult to configure. If just one thing is wrong, the VPN won't work and you'll receive precious little feedback as to exactly where the problem lies. Choosing a standards-based IPSec VPN gives you interoperability and thus the freedom to choose components from different vendors, while opting for a VPN server incorporated within your firewall should reduce configuration issues by removing the possibility of VPN and firewall interactions and incompatibilities.

PCNA

Copyright ITP, 2001