NEXTEP *Broadband* **White Paper**

Virtual Private Networks

Solutions for cost-effective, high-speed corporate extranets and wide-area networks.

A Nextep Broadband White Paper
May 2001

NEXTEP BROADBAND
Broadband Networks Group

Virtual Private Networks

EXECUTIVE OVERVIEW

Virtual private networks (VPNs) have been used increasingly since 1997 to allow businesses to link separate local area networks (LANs), build wide area networks (WANs), create extranets with suppliers, or provide secure remote access.

Because a VPN does not require dedicated E1 or DDN lines, this technology is a particularly attractive option to small and medium enterprises (SMEs) which need to link their computing resources.

However, there are many pitfalls to be negotiated in setting up a VPN, ranging from conflicts between security protocols and firewalls, to slow data transfer due to choice of access methods.

While this paper covers the basics of VPNs for readers who are new to the concept, its main focus is to examine the various options for creating a VPN to suit your business and data needs.

CONTENTS

VIRTUAL PRIVATE NETWORKING

A virtual private network (VPN) is the use of a secure data transfer protocol to connect computing resources over a shared or public infrastructure. This, in effect, creates a corporate wide-area network (WAN) or extranet, without installing or leasing dedicated lines.

By configuring a VPN, computers or networks can share data just the same as if they were connected via cable in a point-to-point local area network (LAN). The speed of data transfer between systems on the VPN depends on the type of shared or public infrastructure used, such as the Internet or a digital subscriber line (DSL) connection. For this reason, the choice of access method is of critical importance, as described later in this paper.

The security of the VPN is assured either by establishing virtual circuits, or by using tunnelling techniques which hide the source and destination addresses and encrypt the data. This prevents both the systems and the data from being accessed by third parties that also use the public or shared infrastructure.

The benefit of a VPN is it allows an organisation to have secure connections to geographically separated offices or suppliers using low-cost local lines, instead of expensive leased lines.

TYPES OF VPNS

VPNs can be placed in two broad categories based on the type of connection used – either a VLAN with virtual circuits, or an IP VPN with tunnelling. These are explained below.

NEXTEP Broadband uses a combination of both of these VPN technologies to suit the customer's requirements, configuration and budget.

VLAN with Virtual Circuits

A virtual LAN (VLAN) is a bridged connection between two or more LANs. This is different from an IP VPN because it uses virtual circuits, which means no firewalls or VPN devices are needed because the VLAN is shielded from other traffic in the system.

In the NEXTEP VLAN solution, permanent virtual circuits are used (i.e. always connected – always on). The systems using the VLAN identify each other using VLAN tags attached to each frame, which gives the network superior Layer 2 security.

Configuring the VLAN entails placing a high-speed DSL modem in the customer's premises. Plugged into a normal phone jack, the modem communicates to a DSL Access Multiplexer

(DSLAM) in the local telephone exchange. This is shown in the following diagram.

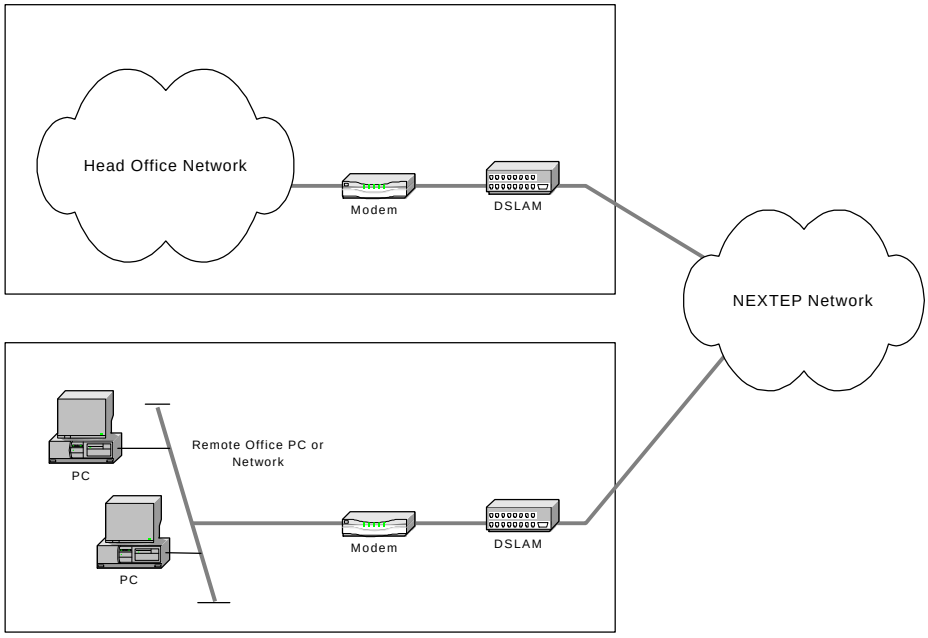

Figure 1: Virtual LAN

Advantages of a NEXTEP Broadband VLAN include:

- Geographically-separated systems can communicate as if they were on the same LAN.
- Easy administration of moves, adds, and changes in these systems
- Traffic between VLANs is restricted. Bridges forward traffic only on LAN segments to which the traffic belongs. This means the administrator can control the traffic to each remote office.
- VLANs maintain compatibility with existing bridges and end stations.
- In a corporate network environment, each VLAN is typically a Logical IP Subnet. Remote offices communicate at the IP layer.
- In the NEXTEP Broadband network, each customer is segregated into a separate VLAN, so they have total privacy of their traffic and have full access to the DSL bandwidth.
- VLANs are IP address independent, so private internal addresses are used instead of public IP addresses.

IP VPN with Tunnelling

The other type of VPN uses internet protocol (IP) tunnelling techniques. A high-speed DSL modem is placed in the customer premises and connected to a VPN-enabled firewall (e.g. a router or switch), as shown in the following diagram.

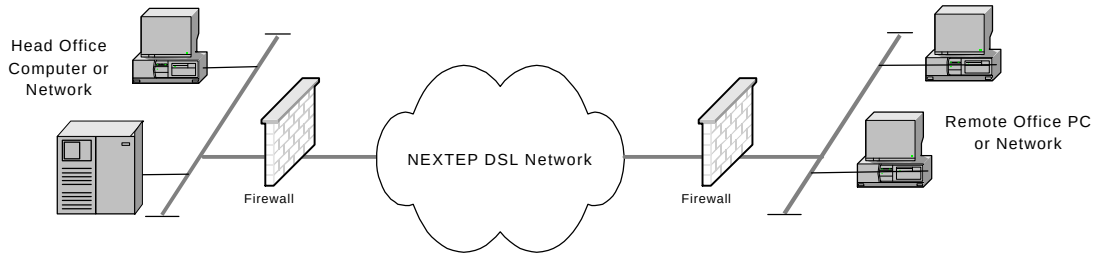

Figure 2: IP Virtual Private Network

Almost all shared or public infrastructure options use IP for data transmission. IP is adaptable, powerful, and allows data sharing between different operating systems. However, the extensive use of IP means that its transport method is well understood and is easily intercepted and tampered with.

Almost all shared or public infrastructure options use IP for data transmission. IP is adaptable, powerful, and allows data sharing between different operating systems. However, the extensive use of IP means that its transport method is well understood and is easily intercepted and tampered with.

Tunnelling is the use of encapsulation to hide the addresses of both the sender and receiver, and the use of encryption to hide the data being transmitted. Thus protected, even the most sensitive data can be sent across a vulnerable public network, such as the Internet, without fear of being breached.

Encapsulation involves taking the header and internal network address from an IP packet and placing it inside the data segment of another IP packet. This hides the internal address and replaces it with the external address of the VPN gateway (such as the firewall or router). This means any packets intercepted by a third party only reveal the network's public IP address.

When the encapsulated packet reaches the destination gateway, the VPN software extracts the original packet and address and forwards it to the final destination behind the firewall.

Encryption involves taking the payload data (the information being transmitted) and the encapsulated original address information and rendering it unreadable by using a random algorithm and a private deciphering key. Typically, the rules of the algorithm are transmitted as a public key, but the packet can only be decrypted by a system which has the private key.

USES OF VPNS

Before investing the time and resources necessary to configure and maintain a VPN, you need to consider why it is needed and how it will be used. If the only real usage will be remote email access, then a VPN is not very practical.

A VPN is best suited for business-critical applications, such as those discussed below.

Internal Office Networking

A NEXTEP VPN can be used wherever a secure point-to-point connection is required between office locations.

For example, a large hospital may have its central computer system in an administration building, while its patient facilities and laboratory are in other buildings – perhaps across the street or across town, or even interstate.

Rather than using conventional leased-line services to connect the computer systems in each building, a VPN can be created at a low cost and data can be exchanged securely over normal telephone lines.

Not only is a VPN the most affordable and secure method of building a site-to-site wide area network (WAN), but it can provide the same data quality and potentially faster speeds than traditional services.

In fact, the security and cost-efficiency of VPN technology makes it ideal even for internal data privacy. If corporate legal or financial data needs tight security, a VPN can be created between departments within the company LAN. A VPN device (e.g. a switch, router or server) is placed between the department computers and the main network backbone, as shown in the following diagram.

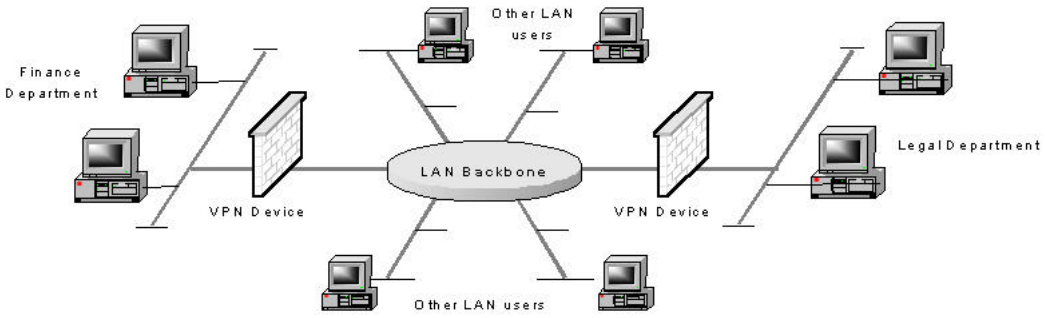

Figure 3: Inter-departmental VPN

External Office Networking

A company may have a small branch or remote employee that depends heavily on data from its main office, or it may have vendors or customers that it wants to give restricted data access.

In both cases, whether the parties are local, interstate or international, a VPN can be used to create a secure extranet environment. This allows each party immediate access to data when it is needed, rather than using slower or less secure means of communication.

In the case of remote access, the VPN connection can either be routed, such as a DSL line, or dial-up via an Internet service provider (ISP). The remote VPN client authenticates itself to the VPN server on the corporate network, and in return the VPN server must authenticate itself to the client. This establishes that communications are secure and enables a virtual point-to-site network.

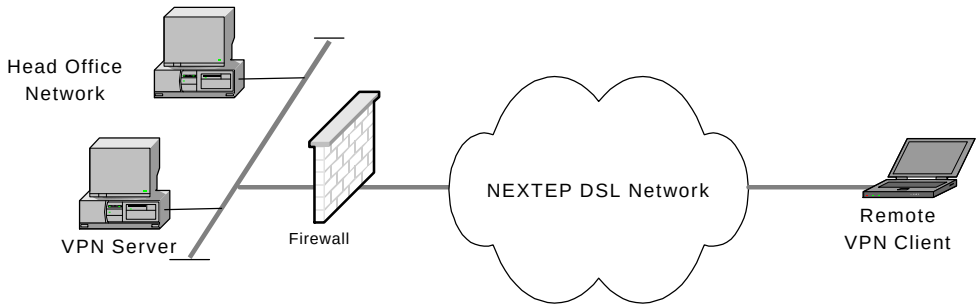

Figure 4: Remote Access VPN Connection

PROTOCOL OPTIONS

There are several different routing and addressing methods, or protocols, available for creating a VPN. Some are vendor-supplied proprietary methods which may not be interoperable or available on all platforms. Others, such as Layer 2 Forwarding (L2F) and Layer 2 Transport Protocol (L2TP) do not provide native support for encryption.

NEXTEP uses the most widely-supported and widely-available methods, which are the IP security protocol (IPSec) and the point-to-point tunnelling protocol (PPTP). Both have common strengths and limitations, including:

- Both IPSec and PPTP are widely used and accepted as industry standards.
- Router or modem gateways which use Network Address Translation (NAT) or Port Address Translation (PAT) cannot recognise IPSec or PPTP packets, although there are workarounds and newer devices are adding IPSec support.
- Both IPSec and PPTP can be used with dynamically-assigned IP addresses for the remote VPN client, but require a fixed public IP address for the VPN server. This can be a problem where the server is implemented

in software and sits behind a router or firewall without a fixed or public IP address.

- For reliability, you will need to employ load balancing and clustering services, as neither is provided by IPSec or PPTP.

Despite these commonalities, IPSEC and PPTP also have distinct differences. Because the choice of protocols may have a big impact on your VPN implementation, the pros and cons of both are discussed in the following paragraphs.

IPSec

The IPSec protocol was developed in 1998 by the Internet Engineering Task Force (IETF) to provide a universal standard for IP Layer 2 (network) security. By securing the IP, you secure the network and applications as well as the data transmissions.

Pros

- IPSec is backward and forward compatible. Only the VPN server and VPN client need to be IPSec compliant – to the rest of the network it looks just like normal IP packets.
- IPSec can be used wherever normal IP would be used, so all data transmissions on a LAN can be secured.
- IPSec is more secure than PPTP because it uses asymmetric public/private key encryption.
- IPSec services are configured on the network side to specify whether client connections must be secure. When a remote computer connects to the network and is properly identified by user-level security, then IPSec security is automatically negotiated in the background.
- IPSec and PPTP support are standard in Windows 2000.
- IPSec is the industry standard, so most new third-party VPN software is IPSec compliant.

Cons

- If you use any non-IP protocols (such as AppleTalk, IPX, NetBIOS, DECnet, etc.) you cannot use IPSec.
- If the VPN client computer does not have Windows 2000, you must install and configure IPSec-compliant software.

PPTP

PPTP is Microsoft's proprietary VPN protocol and was first included with Windows 95. This makes it the most widely available and most widely used VPN protocol.

Pros

- PPTP VPN client software is built into Windows versions 95 / 98 / 2000 / NT 4.0.
- Multiple VPN servers can be configured in Windows NT 4.0 or a single VPN server can be configured in Windows 2000.
- PPTP can be used with non-IP protocols.
- PPTP products are available for the Linux operating system.
- Using built-in router PPTP client capabilities allows anyone on the network to use PPTP regardless of their operating system.

Cons

- PPTP requires extensive configuration on both the VPN server and VPN client. You can avoid this by using built-in router PPTP clients.
- PPTP is less secure than IPSec because it uses single-key (symmetric) encryption, where the key is derived from the user's password.
- Although PPTP support is built into Windows, you need to install and configure the Routing and Remote Access Server (RRAS) major upgrade on the Windows VPN server.

IMPLEMENTATION METHODS AND LEVELS OF SERVICE

In addition to protocols, there are many different ways you can implement your VPN. The choices you make will have a direct impact on the quality of service experienced by users, and may either simplify or complicate the VPN set up.

Access through the public Internet

Wherever your head office, branch offices, customers, suppliers and remote employees are located, all will have access to public telephone lines and a local internet service provider (ISP).

Each VPN client can connect to your VPN server using their existing dedicated or dial-up access to their local ISP, rather than using long distance or leased line services.

The VPN client establishes a connection across the Internet to your VPN server, and then has transparent, secure, point-to-point access to your network.

The drawback of public Internet access is speed. The connection will only be as fast as the slowest component in the link between the client and the server, and will be further restricted by any traffic congestion encountered at any point in the link.

If your VPN connection is business-critical, this type of access will probably be unacceptable. In addition, this scenario usually means you are setting up and configuring the VPN yourself, which can be a difficult task best left to specialists.

Access through a single ISP backbone

You can significantly reduce your VPN complexity and greatly improve your data transmission speed by using a single ISP for both the VPN server and all VPN clients.

Using this type of outsourced access, you can place responsibility for all point-to-point encryption and decryption on the ISP, which means that neither your server nor your clients require any VPN software. Another advantage is you can negotiate a Service Level Agreement that specifies guaranteed network availability and transmission speed.

The danger of this configuration is that data does not have full security as it approaches and leaves the ISP. To overcome this you can have the ISP place a VPN server on your premises, or configure your clients and server for full VPN security.

Obviously this type of VPN access may be geographically impossible if the offices being connected are spread interstate or internationally.

Access through a DSL backbone

At this point you may be thinking that the easiest way to get data security and guaranteed service is by using dedicated leased lines, such as E1, ISDN, DDN, etc. However, one of the primary objectives of the VPN is to eliminate the expense of leased line services.

The issues of network availability, service quality, and transmission speed can all be resolved by using low-cost digital subscriber line (DSL) technology.

NEXTEP Broadband has already installed VPN-enabled equipment in telephone exchanges throughout Melbourne, Sydney and Brisbane, with further rollouts across the country. To connect to the NEXTEP network, all that is required is a high-speed DSL modem for your network server and remote clients.

When NEXTEP implements a VPN solution, we provide a Service Level Agreement and take responsibility for all point-to-point security, installation and configuration. Unlike an ISP

backbone, a NEXTEP Broadband DSL link provides point-to-point security.

By adding an optional splitter, NEXTEPs DSL technology enables you to have both normal telephone communications and broadband service on your existing phone lines, without interfering with the telephone signal.

NEXTEP Broadband can offer data transfer rates above 6 megabits per second (Mbps), which is 100 times faster than standard modem speeds of 56 kilobits per second (Kbps), and 50 times faster than ISDN combined channel speeds of 128 Kbps.

Actual performance of any DSL service is contingent on your line quality and distance from a local exchange, and whether you are paying for a single-user or shared DSL service.

There are also several variations of DSL, each based on different standards and service requirements. For more information about DSL, please refer to the following NEXTEP white papers:

- *Introduction to ADSL: A primer on Asymmetric Digital Subscriber Line transmission technology*
- *DSL Variations: Definitions and differences of Digital Subscriber Line variations*

Where to place the VPN device

VPN termination (where the data encryption/decryption and address encapsulation/extraction take place) can be positioned either within the firewall, at the firewall, or outside the firewall.

If a Windows-based VPN server is placed inside the firewall, you will probably have to upgrade the firewall firmware or hardware to enable passthrough of the IPSec or PPTP packets. In addition, software-based encryption and decryption is the slowest method, so consider the number of users and volume of data that will be passed across the VPN. Drop-in VPN hardware is available that will provide superior performance and ease of configuration.

To avoid upgrading or replacing your firewall, especially if you are using NAT or PAT, you can place your VPN server or drop-in VPN hardware outside the firewall. The danger here is that traffic between the VPN device and the firewall does not have full security.

To place the VPN termination at the firewall will require routing equipment or software that will perform both the VPN and firewall function. Again, you need to decide whether to use software or hardware-based encryption.

Providing failover redundancy

As with other business systems, you need to consider all the issues behind failover protection on your VPN.

- Is your VPN mission-critical, or accessed by hundreds of users?
- Do you need to install or configure a backup VPN server?
- Will your firewall backup system support the VPN?
- Do you need to provide alternative access routes to the VPN, such as IP addresses, dial-in access, etc.?

Having NEXTEP implement the VPN

If your business operations are going to be highly dependent upon the VPN, having NEXTEP handle the implementation and provide the connections at each site will give you peace of mind.

NEXTEP is experienced in making all the tough decisions outlined above, as well as handling the complexities of configuration. Our standard Service Level Agreement specifies guaranteed network availability and transmission speed.

NEXTEP Broadband has the resources to help build and configure your VPN using DSL technology. Please contact our sales department if you would like more information.

CONTRIBUTING COMPANIES

For over a year, two of Australia's leaders in DSL technology have worked together to perfect a cost-effective high speed broadband service for small and medium enterprises (SMEs).

The result is a new business enterprise, Nextep Broadband, bringing together the expertise of NEC Australia and xDSL Limited.

NEC Australia

NEC Australia has more than 7 years experience with broadband deployments in Australia, New Zealand, Spain, Venezuela, Japan and Hong Kong, and is the DSL Global Design Centre for NEC Corporation.

NEC's DSL-based system is a standards-based, fully managed, multi-service access platform designed for carrier and enterprise applications. System interoperability has been tested and confirmed with more than 20 major CPE vendors and a range of backend server, switch and transmission equipment.

xDSL Limited

xDSL Limited was established in 1999 to explore the commercialisation of DSL as a broadband technology in Australia. Its major shareholders include ASX-listed Sirocco Resources N.L., the RMB Ventures group and AIB investments.

xDSL has a 26.7% interest in VOD Pty Limited, a joint venture with the Sirocco group and Civic Video. VOD is currently deploying video-on-demand over the TransACT network in Canberra.

xDSL has considerable experience in deploying content and other broadband services in commercial environments. The success of xDSL is due in large measure to its highly focused and skilled team assembled from a broad mix of backgrounds and disciplines.

"Virtual Private Networks" Rev 1.1
Written by Michael C. Bouy for NEXTEP Broadband

This document is printed for informational purposes only and the information herein is subject to change without notice.

This document is written for installations where all items are supplied by Nextep Broadband and the system integration has been completed by Nextep Broadband personnel. Nextep Broadband is not responsible for overall system performance, thermal characteristics, EMC and safety issues where the customer uses third party equipment and the system integration has been completed by parties other than Nextep Broadband.

649-655 Springvale Road
Mulgrave, Victoria 3170 Australia

Phone: (03) 9271 4240
Fax: (03) 9271 4249