Windows 2000 Server

Chapter 6 - Expanding and Securing Remote Client Access

Microsoft Windows 2000 provides security enhancements and virtual private network (VPN) support that enable expansion of remote access connectivity to address your most critical global deployment requirements. You can use the Routing and Remote Access service, Internet Authentication Service, and Connection Manager components of Microsoft Windows 2000 Server to deploy security features and VPN support as part of your integrated, end-to-end remote access solutions. You can use the information in this chapter to plan, design, and implement the security and VPN features of these components.

This chapter is intended for network engineers and support professionals who are already familiar with TCP/IP, IP routing, Internetwork Packet Exchange (IPX) routing, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Windows Internet Name System (WINS), and wide area network (WAN) technology, and assumes that you have read "Providing Dial-Up Client Access," as well as the virtual private networking information in Windows 2000 Server Help.

Overview of Virtual Private Networking and Secure Connections

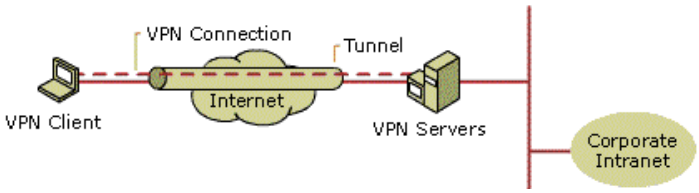
Security and cost-efficiency are critical to the deployment of any remote access solution. The expanding requirements of nonlocal users for remote access to a network can result in escalating long-distance costs. At the same time, the availability of Internet access has become so widespread that it is difficult to find a locality without Internet access capabilities. Now, rather than making a long distance or 1-800 call to an enterprise, a remote access client can call a local ISP to access the Internet, and then create a secure tunnel through the Internet to establish a virtual private network connection to the enterprise network. The ISP provides the infrastructure to support the dial-up portion of the connection, so the enterprise does not have to install and maintain components such as modem banks or network access servers (NASs).

When you move remote access from dial-up infrastructure to the Internet, security of the connection is a requirement and is more complex and difficult to deploy. Security features, such as smart cards and certificate services, can provide improved manageability and stricter access control for virtual private network–based remote access.

Windows 2000 provides support for the implementation of VPN remote access that can use the Internet to provide world-wide connections for remote users. Windows 2000 also provides extensive support for high-security features, such as certificate-based services, that can be implemented in both dial-up and VPN solutions. Before evaluating how Windows 2000 can best support your security or VPN requirements, it is important to understand the technologies used to implement such solutions.

Virtual Private Networking

Virtual private networking is the act of creating and configuring a virtual private network (VPN) by using a combination of tunneling, authentication, and encryption technologies. A virtual private network is the extension of a private network that encompasses links across shared or public networks like the Internet. Figure 6.1 shows the basic components of a VPN solution.



If your browser does not support inline frames, click here to view on a separate page.

Figure 6.1 Basic VPN components

Many organizations with extensive remote access requirements are implementing virtual private networking to reduce remote access expenses by using the Internet infrastructure to partially or entirely replace centralized in-house dial-up remote access infrastructures and legacy services. VPNs offer three primary benefits:

- Reduced costs

  One of the largest expenses an enterprise can have is phone cost. Using the Internet as a connection medium saves long distance phone expenses and requires less hardware.

- Reduced management overhead

  Because the local phone company and your Internet service provider (ISP) owns and manages the phone lines or wide area network (WAN) links that support your VPN connections, there is less management for network administrators.

- Added security

  The use of standard, interoperable authentication and tunneling protocols allows data to be hidden from the unsecured environment of the Internet but remain accessible to enterprise users through a VPN. In addition, with encryption, users on the Internet see only the external IP addresses, while the internal addresses are encrypted. It is extremely difficult for a hacker to interpret the data sent across a VPN connection.

VPNs are TCP/IP-based traffic, and therefore provide flexible medium support, including analog, ISDN, and dedicated broadband connections. Although the security risks of providing remote access over the Internet have traditionally been a deterrent to using VPNs, Windows 2000 offers complete VPN solutions using an integrated set of components that make VPN-based connections extremely secure and viable. This chapter focuses on client-to-server VPN solutions using Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP), both of which can provide highly secure connections.

Although the term VPN is used to cover an increasingly broad field of network implementations, the critical aspect of VPNs is that they support secure connections across a public or untrusted network infrastructure, including:

- Secure client-to-server connections, either over the Internet or within private or outsourced networks.
- Secure gateway-to-gateway, or router-to-router, connections across the Internet or across private or outsourced networks.

VPNs support Internet Protocol (IP) layer tunneling, which encapsulates data sent between a remote access client and a remote access server. VPNs enhance data security for a connection by:

- Authenticating remote access users prior to data exchange.
- Encrypting authentication credentials.
- Encrypting exchanged data.

Implementing a secure VPN solution requires setting up a perimeter network (also known as a demilitarized zone or DMZ). A perimeter network is positioned between the Internet and the intranet to protect the enterprise network from unauthorized traffic. The perimeter network includes servers, routers, and switches that maintain security by preventing the internal network from being exposed on the Internet. A firewall helps protect the perimeter network. Input and output filters can both be used to protect the security of the perimeter network. Deployment of a VPN solution with a secure perimeter network requires several key decisions, including which

tunneling protocol is most appropriate, whether to use voluntary or compulsory tunneling, and whether to use an in-house or outsourced support solution.

VPNs can be implemented using RADIUS to centralize management and administration of the VPN solution. The VPN server operates as a RADIUS client and is responsible for passing user connection information from the ISP to the appropriate RADIUS servers, and then acting on the response.

Tunneling Protocols

Network security is a concern for most organizations, and two protocols that can help to ensure secure communications across the Internet are Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP), both of which can support encrypted and plaintext authentication. It is possible to create a tunnel and send data by means of a tunnel without encryption. However, it is not a true VPN connection because the private data is sent across a shared or public network in an unencrypted form, which exposes the data to viewing or modification.

Although VPNs can be used within an enterprise's intranet to implement secure communications for very sensitive areas of a LAN, this chapter focuses only on the use of VPNs for remote client connections. Tunneling protocols used to implement VPNs include:

- Point-to-Point Tunneling Protocol (PPTP), which is a Request for Comments (RFC)-based tunneling protocol that was first supported in Microsoft Windows NT 4.0, based on an informational RFC. PPTP provides encapsulation of Point-to-Point Protocol (PPP) frames and employs the authentication, compression, and encryption mechanisms of PPP. Microsoft Point-to-Point Encryption (MPPE) is used to encrypt the PPP frames prior to encapsulation. Because the authentication process happens before the encryption is active and MPPE encryption does not provide data authentication and integrity services, PPTP is not as secure as L2TP used in conjunction with Internet Protocol security (IPSec). However, PPTP is supported by a more diverse client base.
- Layer Two Tunneling Protocol (L2TP), which is an RFC-based tunneling protocol that is still evolving but is already an industry standard. Like PPTP, L2TP encapsulates PPP frames and builds on the mechanisms of PPP. L2TP does not provide encryption. Rather than using MPPE to encrypt PPP frames, IP security (IPSec) is used to provide encryption for L2TP messages. IPSec provides encryption, data authentication, and data integrity services. Unlike PPTP, where the PPP frame is encrypted by MPPE before it is encapsulated by PPTP, L2TP encapsulates the unencrypted PPP frame and the entire L2TP message is secured by using IPSec. An L2TP tunnel using IPSec encryption services is known as L2TP over IPSec. When using L2TP over IPSec, two levels of authentication are required. To negotiate the use of IPSec, computer-level authentication with computer certificates is used to verify the identities of the two computers. To send data over the L2TP tunnel, user-level authentication using a PPP authentication protocol verifies the identity of the user making the connection. Because it is a newer technology, L2TP over IPSec is not supported by many operating systems earlier than Windows 2000.
- Internet Protocol security (IPSec), which is an RFC-based suite of cryptography-based protection services and security protocols that represent the long-term direction for secure networking. IPSec provides aggressive protection against private network and Internet attacks. IPSec provides advanced security for VPNs but was not designed to address critical remote access requirements such as user authentication and address assignment. In addition, it does not support multiprotocol or multicast (including some routing protocols) functions. It is applicable primarily to IP-only and unicast-only situations. Implementation of IPSec tunnels is recommended only in solutions for which PPTP and L2TP tunnels are not feasible.

For more information about IPSec tunnels, which are supported in Windows 2000 only for router-to-router connections, see "Connecting Remote Sites."

Tunnel Methods

The tunnel method is the way in which a VPN is created. There are two types of tunnels:

- Voluntary tunnels are ad-hoc connections that a dial-up user initiates. The appropriate tunneling protocol and client software must be installed on the client computer, but no intermediate remote access server support for tunneling is required. In this case, the user's computer is a tunnel endpoint and acts as the tunnel client. Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server. In a dial-up situation, the client must establish a dial-up connection to the internetwork before the client can set up a tunnel. If additional tunneling server-side restrictions are implemented to enforce appropriate use of tunnels, voluntary tunneling can prevent security exposures.
- Compulsory tunnels are preconfigured device-initiated connections for which a provider's NAS initiates the tunnel connection on the client's behalf. Client support for VPNs in a compulsory tunneling configuration is not required, and the user's computer is not a tunnel endpoint. The provider NAS between the user's computer and the tunnel server is the endpoint, acting as the tunnel client. Compulsory tunnels can provide security for client-to-server connections, but are generally only used when clients do not support voluntary tunnels.

Outsourced Support

Deploying remote access solutions for a large number of remote users, especially a large number of users who connect from outside of the local calling area, can be very costly. Although the use of VPNs can significantly reduce remote access costs, organizations can still have significant challenges to cost-effective implementation of remote access solutions. Two of the most costly items include:

- Providing the network infrastructure to support dial-up client access.
- Providing Internet connectivity for VPN users.

Enterprises with extensive remote access requirements can obtain significant cost and implementation advantages by establishing wholesale contracts with third-party service providers for VPN access. Outsourcing the remote access infrastructure and connectivity to a single ISP on a wholesale contract basis can minimize both setup and operation costs. Many Internet service providers provide guaranteed levels of service that rival those of dial-up WAN connections.

Outsourced support for remote access can include providing extensive networks of access points across a broad geographical area, even worldwide, as well as providing the technology, infrastructure, and services to implement and manage high-availability external access to an enterprise network.

Expanding Security for Remote Access Solutions

Both VPN and dial-up remote access solutions can provide high levels of security, but managing and maintaining tight security can challenge complex enterprise solutions. Some of the best ways to provide better security include the use of certificates to validate identity and access rights, smart cards to provide secure authentication of remote clients, token cards for increased password security, and filters to restrict access to specific areas of a network.

Firewalls and Filters

The firewall is designed to provide protection for the computers on the perimeter network (also called a demilitarized zone or DMZ) by filtering traffic. Its use is critical in VPN solutions, where ineffective implementation can expose the enterprise network to a variety of attacks or other unwanted access from the Internet.

Filters include one or more conditions that can be applied to incoming and outgoing network traffic to limit access to specific resources. Filters are especially useful when providing access to external partners or other entities that are not generallyallowed access to an enterprise's entire network or for preventing communication with unauthorized computers.

Public Key Infrastructures and Extended Authentication Support

A public key infrastructure (PKI) is a system of digital certificates, certification authorities (CAs), and other registration authorities that use public key cryptography to verify and authenticate the validity of each user and computer involved in an electronic transaction. Standards for public key infrastructure are still evolving even as they are being widely implemented as a necessary element of electronic commerce.

Certificates

A certificate binds a public key to the identity of a person, computer, or service that holds the corresponding private key. Certificates are used by a variety of public key security services and applications that provide authentication, data integrity, and secure communications across networks such as the Internet. These are especially useful for situations where users require transient access to a system and are entities about which you have limited knowledge, but that require access to some of your information resources. Certificates are also useful for providing easy access in environments where users are required to have multiple passwords, each specific to a distinct network or application. Certificates can provide strong security, simplified administration, and support for new components that use PKI technology.

Both the remote client and the VPN server need to have both a certificate issued to them and the ability to trust each other's certificate. The remote client needs to have a certificate installed to negotiate a trust relationship with the VPN server. Typically, a user's computer receives a certificate from a Windows 2000 certification authority (CA) when the computer joins the domain. The computer receives a Group Policy setting containing instructions for enrolling in the domain certification authority called a certificate auto-enrollment policy. The certificate policy of the public key infrastructure (PKI) also specifies that the client can trust the certificate server that issued a certificate to the VPN server. The VPN server is configured to trust the certificate server that issued certificates to remote access clients.

Smart Cards

Smart cards are physical cards that store certificates used for authentication and access for a specific network. Smart cards are a tamper-resistant and portable way to provide security for tasks such as network access and e-mail access. Smart cards provide secure storage for private keys and other forms of personal information and isolation of security-critical computations involving authentication, digital signatures, and key exchange.

Token Cards

Token cards from different vendors work in a variety of ways, but they are all basically hardware-based password generators. Token cards provide for increased security by implementing algorithms for generating one time passwords (OTP). For example, some cards have a small LCD display and a keypad like a calculator; the user enters a numeric personal identification number (PIN) and the card displays a numeric passcode that can be used as a password. Normally, token cards are designed so that they only produce a particular passcode once.

Planning for VPNs and Secure Remote Access

Planning for deployment of virtual private networking and expanded security support requires the same type of decision-based steps as the deployment of a basic dial-up client access solution, including:

- Analyzing your user, business, and information technology (IT) requirements for VPN access.
- Assessing VPN and expanded security solutions.
- Doing project planning for a VPN or expanded security deployment project.

Many companies find that the integration of dial-up and VPN solutions is most effective for meeting remote access needs, and that a combined dial-up and VPN deployment plan is required to provide a complete solution. As you complete the planning steps discussed in this section, evaluate how VPN and dial-up solutions might be combined to meet your enterprise's needs and objectives.

Analyzing VPN and Expanded Security Requirements

Basic dial-up client access can meet specific business needs for remote access, particularly for local connectivity and occasional access. However, the costs of providing long-distance connectivity and supporting multiple remote locations might be excessive when using basic dial-up access. In addition, some enterprises require more extensive security than is provided by a basic dial-up client access implementation. Use the information in this chapter to determine whether expanded security features or VPNs are appropriate for meeting your remote access requirements.

VPN Access

After analyzing your remote access requirements, consider deploying VPN solutions if:

- Remote access by individual users requires connections from outside of the local calling area, where long-distance charges might be prohibitive.
- Remote users require connections with a high-level of security that cannot be met by other access methods.
- The organization's connection to the Internet supports the aggregate throughput required for the maximum number of concurrent remote access clients.
- The variability of Internet bandwidth does not adversely impact client response times, especially if guaranteed levels of service can be negotiated with the ISP.
- Users require worldwide access points to support roaming, telecommuting, or other noncentralized activities.
- Users require support for high-speed Internet connections, such as a broadband connection.

If cost, quality, or manageability factors are issues that detract from the use of service providers for VPN access, outsourcing VPN support can be an optimal solution. Outsourcing, which includes negotiation of wholesale rates and managed levels of service, can be very cost-effective.

For additional cost and support benefits, consider deploying a VPN solution using outsourced support if:

- A volume discount can be negotiated with an ISP.
- Remote users (including those who require a high-level of security) cannot connect effectively by means of dedicated lines or basic dial-up access.
- Remote users need a guaranteed level of quality and availability.
- It is not cost-effective to maintain and manage modem banks internally.
- Client software does not support voluntary tunneling and a contractual obligation to provide compulsory tunneling is an acceptable option.

Although the focus of the above requirements is on the use of VPNs for remote client access, VPNs can also be very effective for connecting remote sites. For more information about using VPNs for router-to-router remote site connectivity, see "Connecting Remote Sites."

Expanded Security for Dial-Up and VPN Solutions

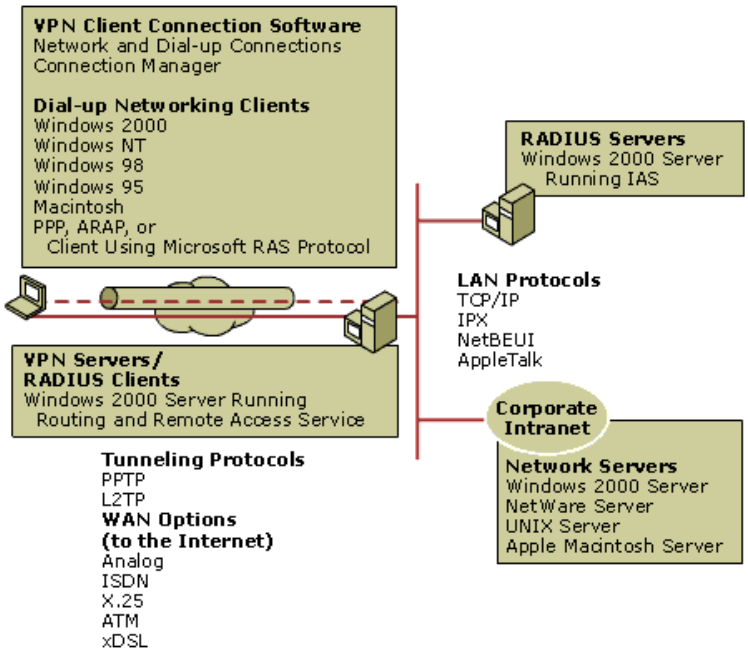
Whether deploying VPN or dial-up remote access, enhancing security by using add-ons and filtering techniques can provide additional protection for more sensitive requirements. Consider implementing expanded security support (such as smart cards, token cards, and multiple filters), if any of the following is true:

- Remote users are mobile, with increased potential for theft of a portable computer.
- Remote users are limited to very specific areas of a network.
- Remote users are accessing extremely sensitive data.
- Network penetration by unauthorized users is an unacceptable risk for the enterprise.
- The cost of implementing additional security features, which can be significant for security solutions requiring additional third-party hardware, is not prohibitive.

Assessing Windows 2000 VPN and Expanded Security Solutions

Windows 2000 Server and its remote access components and features support deployment of an end-to-end VPN solution or the upgrade of an existing remote access solution to provide additional security capabilities.

Figure 6.2 provides an overview of the primary support provided in Windows 2000 for VPN solutions.



If your browser does not support inline frames, click here to view on a separate page.

Figure 6.2 Windows 2000 support for VPN solutions

In addition to the basic support shown in Figure 6.2, Windows 2000 also provides support for expanded security, such as smart cards (and other certificate-based support) and token cards.

Use the information in this section to determine how to plan effective solutions that meet your VPN and additional security needs using Microsoft virtual private networking, Certificate Services, Routing and Remote Access service, Internet Authentication Service (IAS), and Connection Manager components.

VPN Support

A VPN solution can include a variety of protocols, connection options, and optional security-based features. The components that you select to implement your solution must be tailored to the security, availability, and cost objectives for specific user groups, but every VPN solution must provide at least a basic level of support. At a minimum, a VPN solution must provide all of the following:

- User authentication

  The solution must verify the user's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who created connections and when they were created.

- Address management

  The solution must assign an IP address on the private network and ensure that private addresses are kept private.

- Data encryption

  Data carried on the public network must be rendered unreadable to unauthorized clients on the network.

- Key management

  The solution must generate and refresh encryption keys for the client and the server.

- Multiprotocol Support

  The solution must handle common protocols used in the public network. Such as IP, and Internetwork Packet Exchange (IPX).

The standards-compliant services in Windows 2000 meet all of these requirements, supporting the use of the Internet to provide secure remote access to a private network, dramatically reducing dial-in administrative and long distance service costs. A computer running Windows 2000 Server and configured as a VPN server is a remote access router, providing both remote access and routing services to VPN clients.

Windows 2000 TCP/IP with PPTP or L2TP over IPSec provides high levels of security. Both PPTP and L2TP are components of the Windows 2000 Routing and Remote Access service.

Tunneling Protocols

To deploy a VPN remote Client access solution, first determine which tunneling protocol best meets your requirements. Windows 2000 supports two tunneling protocols:

- Layer Two Tunneling Protocol over IPSec (L2TP over IPSec), in which L2TP provides encapsulation and tunnel management for any type of network traffic and IPSec in transport mode provides the security for the L2TP tunneled data.
- Point-to-Point Tunneling Protocol (PPTP) using Microsoft Point-to-Point (MPPE) for data encryption.

Windows 2000 also supports IPSec in tunnel mode, in which IPSec itself does the encapsulation for IP traffic only, but only for limited router-to-router connections. IPSec tunnel mode is not supported for remote access client connections. For more information about router-to-router VPN solutions, see "Connecting Remote Sites."

L2TP over IPSec

In Windows 2000, secure, remote communication is achieved by combining the Layer Two Tunneling Protocol (L2TP) and IPSec. L2TP is used to build the tunnel through which the data travels and computer-level certificates use IPSec to secure the data. L2TP creates the necessary IPSec security policy to secure tunnel traffic. You do not need to assign or activate your own IPSec policy on either computer. If the computer already has an active IPSec policy, L2TP simply adds a security rule to protect L2TP tunnel traffic to the existing policy.

L2TP over IPSec is the most flexible, interoperable, and secure tunneling option for both client remote access VPN tunnels and gateway-to-gateway VPN tunnels. However, both the VPN client and the VPN server must support both L2TP and IPSec. L2TP allows IP, IPX, or NetBEUI traffic to be encapsulated, and then sent over any medium that supports point-to-point datagram delivery, such as IP, X.25, Frame Relay, or asynchronous transfer mode (ATM). L2TP does not require that the transit network be based on IP, but only that it provides point-to-point connectivity. For an L2TP over IPSec connection to occur, you need to install computer certificates on the VPN client and VPN server computers. It requires more central processing unit (CPU) power than PPTP (which can be offset with the addition of an offload card). L2TP in combination with IPSec is the only standards-based technology that addresses remote access VPN requirements while building on IPSec for encryption. L2TP currently retains the same IETF standards-track status as IPSec.

Deploying IPSec provides strong security and requires no changes to existing applications or operating systems. Other security mechanisms that operate above the network layer, such as Secure Sockets Layer (SSL), only provide security to applications that know how to use SSL, such as Web browsers. Protecting communications with SSL requires modifying all other applications. Security mechanisms that operate below the network layer, such as data-link layer encryption, only protect the link, but not necessarily all links along the data path. This makes link layer encryption unsuitable for end-to-end data protection on Internet or routed intranet scenarios.

The implementation of IPSec at the network layer provides protection for all IP and upper-layer protocols in the TCP/IP protocol suite, such as TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and even custom protocols that send traffic at the IP layer. The primary benefit of securing information at this layer is that all applications and services that use IP for transport of data can be protected with IPSec, without any modification to those applications or services. (To secure protocols other than IP, the packets must be encapsulated by IP.) Unlike PPTP, L2TP over IPSec provides an authenticity method to ensure that packet content is not changed in transit.

IPSec configuration is contained in an IPSec policy that the administrator creates and applies on the local computer or using Group Policy in Active Directory, the directory service included with Windows 2000. To resolve the difficulty of manually configuring IPSec policy, Windows 2000 has IPSec support built into L2TP so that you only need to create a VPN connection (that uses L2TP) from the remote computer to the VPN server.

When L2TP uses IPSec for security:

- The required IP filter and filter action lists are dynamically set in the IPSec Policy Agent for the duration of the connection.
- The authentication method is certificate-based, which requires a computer certificate to be installed on the VPN client and the VPN server.
- Default key exchange settings are in effect.

The level of Internet Protocol security that is used for the duration of the connection is dependent upon the remote access policy profile settings that specify whether data encryption is required.

IPSec tunnel mode, as originally specified, only supports user authentication by means of user certificates or preshared keys. However, most IPSec tunnel-mode implementations only support use of computer-based certificates or preshared keys. L2TP uses PPP as the method of negotiating user authentication. As a result, L2TP can provide PPP-based, password-based authentication by using Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). It can also support advanced authentication services through Extensible Authentication Protocol (EAP), which offers a way to plug in different authentication services without having to invent additional PPP authentication protocols. Because L2TP is encrypted inside of an IPSec transport mode packet, these authentication services are strongly protected as well. Most importantly, by means of integration with Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP)-based directories, L2TP supports interoperability requirements by using authentication services that most customers and vendors already have in place.

Consider using L2TP over IPSec for Windows 2000 Server–based VPN solutions if your clients are using Windows 2000 (or another operating system that supports L2TP and IPSec) and you need:

- A higher level of security than PPTP provides. However, computer-level certificates are required, and a computer-based certificate infrastructure must be in place and certificates issued prior to connecting.
- The requirement for stronger security outweighs the potential cost and/or performance impacts of implementing processor-intensive IPSec support. The performance impacts can be mitigated by deploying more powerful computers or providing offload encryption cards.

  Note Before deploying IPSec, make sure you have a thorough understanding of its functionality and how it is implemented. For more information about IPSec, see "Internet Protocol Security" in the *Microsoft Windows 2000 Server Resource Kit TCP/IP Core Networking Guide*.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is an excellent solution to the tunneling needs of remote clients. It is relatively simple to set up when compared to L2TP over IPSec, and it provides good security when used with strong passwords.

PPTP uses user-level Point-to-Point Protocol (PPP) authentication methods and Microsoft Point-to-Point Encryption (MPPE) for data encryption. The PPP frame is encrypted with MPPE by using encryption keys generated from the MS-CHAP (version 1 or version 2) or the Extensible Authentication Protocol-Transport Level Security (EAP-TLS) authentication process. PPTP clients must use either the MS-CHAP or EAP-TLS authentication protocol in order to encrypt PPP payloads. PPTP does not provide encryption services. PPTP encapsulates a previously encrypted PPP frame.

PPTP allows Internet Protocol (IP), Internetwork Packet Exchange (IPX), or NetBIOS Extended User Interface (NetBEUI) traffic to be encrypted and then encapsulated in an IP header to be sent across an enterprise IP internetwork or a public IP internetwork such as the Internet. PPTP also requires that the transit network be based on IP.

PPTP was the earliest widely supported VPN protocol. PPTP supports both multiprotocol and multicast environments. Developed before the existence of IPSec and public key infrastructure (PKI) standards, PPTP provides for automated configuration and supports legacy authentication methods. PPTP combines standard user password authentication with MPPE encryption without requiring the complexity

and expense of PKI. Recent PPP authentication protocols enhance its security while preserving its other useful properties, through the addition of support for MS-CHAP v2 and Extensible Authentication Protocol (EAP). These latest enhancements provide stronger authentication and the ability to use smart cards and public key certificates. This strengthens protection against both user impersonation and brute-force decryption of intercepted packets.

PPTP can provide a lower-cost VPN security alternative or complement to L2TP over IPSec solutions. Consider using PPTP (using MPPE as the data encryption method) for Windows 2000 Server–based VPN implementations, if:

- The client supports PPTP and MPPE. Windows 2000, Windows NT 4.0, Microsoft Windows 98, and Microsoft Windows 95 support PPTP with MPPE.

  Note Microsoft Windows 95 requires installation of Windows Dial-Up Networking version 1.3 (or later) Performance & Security Upgrade for Windows 95.
- Either the client or server does not support L2TP or IPSec. Windows-based clients other than Windows 2000-based clients, and many clients running other operating systems do not support L2TP or IPSec.
- Support for MS-CHAP (version 1 or 2) or EAP-TLS authentication protocols is required.
- User-based authentication is required, the added security of computer-based authentication is not required, and a public key infrastructure (PKI) does not exist.
- VPN connections must pass through Network Address Translators (NATs) that are capable of translating PPTP traffic. NATs are incompatible with any IPSec implementation.

RADIUS Support for VPNs

If you have multiple VPN servers running Windows 2000, each VPN server requires configuration. You can lower management costs by centralizing administration, authentication, and logging of VPN servers. If you want to take advantage of centralized management, including centralized control of remote access policies and logging, you can configure the VPN servers as Remote Authentication Dial-In User Service (RADIUS) clients to a RADIUS server,running Windows 2000 Server and Internet Authentication Service (IAS).

One of the benefits of using IAS for VPN connections is that IAS can be configured to direct the traffic from the client through a tunnel to a particular location. Depending on the category of the authenticating user, a tunnel can be created to different parts of the enterprise network.

IAS supports both voluntary and compulsory tunneling as follows:

- Voluntary tunneling

  IAS can be used to authenticate users and to control access to voluntary tunnels. You can use IAS to enforce tunneling by configuring remote access policies to restrict incoming calls to the appropriate VPN protocols.
- Compulsory tunneling

  Using IAS, the tunnel endpoint (the VPN server at which the tunnel is terminated) can be changed based on conditions in a remote access policy. For example, the tunnel endpoint can be changed based on user credentials or the groups to which the user belongs.

IAS can provide compulsory tunneling connection attributes for NASs that support compulsory tunneling. The Windows 2000 Routing and Remote Access service does not support compulsory tunneling.

If you have VPN servers running Windows NT 4.0 with Routing and Remote Access Service (RRAS), you can use IAS to take advantage of Windows 2000 remote access policies on the VPN servers that are set up as RADIUS clients. (You cannot configure VPN servers running Windows NT 4.0 as RADIUS clients, unless they are running RRAS.)

An enterprise can outsource VPN support by contracting with an ISP to provide compulsory tunneling by supplying the tunnel client (tunneling-enabled remote access server). These ISP tunnel clients can receive calls from remote access clients and then establish compulsory tunnels across the Internet to a tunnel server connected to the enterprise's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the enterprise network. Clients can also use voluntary tunnels to establish connections by means of outsourced ISP connections. RADIUS proxy servers at the ISP location act as RADIUS clients to forward authentication requests from the ISPs remote access servers to the enterprise IAS servers.

For more information about the authorization and authentication process used in voluntary and compulsory tunneling, see "Internet Authentication Service" in the *Microsoft Windows 2000 Server Resource Kit Internetworking Guide*.

Expanded Security Features for Remote Access

Windows 2000 Server and the Routing and Remote Access service supports the Extensible Authentication Protocol (EAP), allowing new authentication methods to be used for PPP authentication. EAP is the infrastructure that allows third-party authentication modules to plug in to the Windows 2000 Point-to-Point Protocol (PPP) implementation. This is especially important for deployment of security based on smart cards. It is also important for deployment of other certificate services and token cards.

In addition to EAP support, Windows 2000 Server provides extensive filtering support to provide maximum security for remote access connections.

Certificate Services and Smart Card Support

Windows 2000 Certificate Services includes a variety of templates to be used to implement certificates for the authentication of users, computers, and services. Some of the most useful ones for remote access include:

- Computer certificates that can be issued to remote access computers for L2TP over IPSec connections
- Smart Card certificates that can be issued to remote users

If you are using L2TP or smart cards, determine how to implement the required certificates. For more information about using public key infrastructure (PKI) to manage certificates, see Windows 2000 Server Help.

Guideline Although EAP-TLS works with registry-based certificates, for security reasons it is highly recommended that you only use EAP-TLS with smart cards.

Token Card Support

EAP supports the implementation of token cards to provide increased security for authentication. Independent software vendors (ISVs) can use EAP to supply new authentication modules for clients and servers that support token cards. When used as part of a Windows 2000 VPN solution, with the data encryption support provided in PPTP and L2TP solutions, a token-card implementation can be highly secure. Token cards are not as convenient as preprogrammed public key smart cards, but they are less expensive and are currently more widely implemented.

Note Token cards are not recommended for Integrated Services Digital Network (ISDN)-based dial-up connections because a separate password is required for each channel (so the B channel has to generate a password every time it is bonded).

Other EAP Support

In addition to EAP-TLS, Windows 2000 Server supports EAP-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5) CHAP and the passing of EAP messages to the RADIUS server. Windows 2000 Server also supports third-party EAP plug-ins for

emerging authentication methods, including those that support implementation of smart cards and biometric devices.

Filtering Support

For VPN connections, Windows 2000 with Routing and Remote Access service supports the following IP packet filters:

- PPTP or L2TP over IPSec packet filters for VPN servers

  To secure the VPN server from sending or receiving any traffic on its Internet interface except VPN traffic, you must configure IP input and output packet filters on the perimeter network interface of the VPN server to discard all traffic except PPTP or L2TP over IPSec traffic.

- Remote access policy profile packet filters

  To define the specific types of IP traffic that are allowed in to and out of a remote access VPN connection (sent or received within the PPTP or L2TP tunnel), you can configure IP packet filters on the profile for the remote access policy that is used for the remote access VPN connections. For example, for business partner remote access VPN connections, you can configure IP packet filtering on a remote access policy that allows connections to and from only a specific subnet in your organization.

Note When deploying business partner connections, it is recommended that you limit these dial-up clients to traffic only from specific addresses and not allow the traffic to be routed onto the enterprise network.

Account Lockout

Windows 2000 Server also supports account lockout for remote access, which can be used to thwart dictionary attacks on remote user accounts. With account lockout enabled, a dictionary attack is foiled after a specified number of failed attempts. You implement account lockout for remote access clients by customizing the registry. This is different than the setting of the account lockout policy for domain or local user accounts (using the **Account locked out** setting on the **Account** tab on the properties of a user account). For more information about remote access account lockout, see "Remote Access Server" in the *Internetworking Guide*.

Connection Software for Remote VPN Clients

Implementing Connection Manager on a client provides the required support for voluntary tunneling. By using a Connection Manager service profile, users can use worldwide Internet access points to establish secure tunnels to firewall-protected VPN servers as easily as local users can use dial-up access to connect to the enterprise network. Connection Manager supports both non-persistent (dial-up) and persistent connections (direct, pre-established ISP connection). If you specify support for both persistent and non-persistent connections, users have the option at connection of choosing which type of connection is most appropriate.

Connection Manager support for VPN connections provides additional capabilities not available for dial-up connections, including support for high-performance solutions using technologies such as Asynchronous Digital Subscriber Line (ADSL).

Connection Manager support for merging phone books and other features is useful if you outsource support, especially when outsourcing to multiple ISPs. The replication support provided in Connection Point Services (CPS) also makes it easy to distribute phone books to other locations and enterprises. For instance, an ISP that markets to local Internet access providers (IAPs) might also provide phone books to each IAP to support travel requirements of IAP subscribers.

Operating Systems for Remote VPN Clients

Computers running Windows 2000, Windows NT 4.0, Windows 95, and Windows 98 can create remote access VPN connections to a VPN server running Windows 2000. VPN clients can also be any other Point-to-Point Tunneling Protocol (PPTP) client or Layer Two Tunneling Protocol (L2TP) client with IPSec. Clients running Windows 2000 support the widest range of secure connections, including VPN connections, of all Windows operating systems. Consider using Windows 2000-based clients for VPN or other secure connections if:

- Clients require connections using L2TP over IPSec.
- Clients require smart card access.
- You require Connection Manager features that are not supported by other operating systems, such as support for EAP or the PPP Multilink Protocol.

VPN Project Planning

Your VPN project plan can build upon a project plan for dial-up remote access or can be a stand-alone plan. When doing project planning for VPN solutions, it is recommended that you:

- Address how to coordinate multiple solutions (such as dial-up and VPN).
- Provide for completion of testing and piloting of any dial-up solutions before starting deployment of the VPN solution.
- Deploy PPTP first, if deploying both PPTP and L2TP solutions.
- Document requirements for your ISP, especially if you are outsourcing access.
- Include representatives from your security team and at least one ISP representative on the deployment team to help clarify all interdependencies.
- Have your domain and Certificate Services infrastructure (as appropriate) in place before starting deployment of any remote access solutions.
- Maintain a dial-up access point (800 number or other) throughout the rollout as a backup for VPN access.

Designing the VPN and Security Infrastructure

To design a VPN client access infrastructure that meets the needs of your environment, you need to:

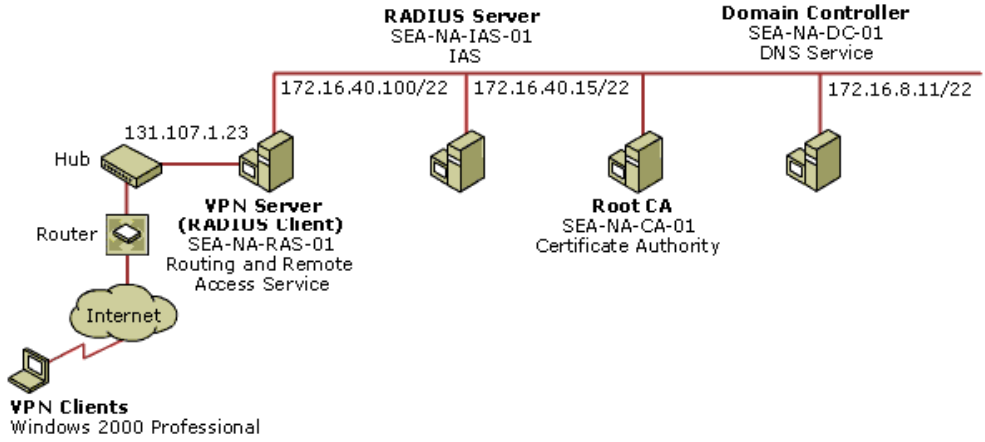
- Design the network infrastructure showing the components and physical layout for your VPN remote access solution.
- Develop specifications showing implementation details for all aspects of your VPN solution.
- Test your design and use the results to refine your VPN solution.

The design process for a VPN solution is more complicated than designing a dial-up solution, especially if the VPN solution includes outsourced support, because the design must take into consideration the additional requirements for implementing ISP support.

Designing the Network Infrastructure

A network diagram for your VPN solution is critical for ensuring a properly designed VPN network infrastructure, including the perimeter network. If you also provide support for dial-up client access, the network diagram for your VPN solutions overlaps the dial-up access topology. Integration of the two might be appropriate, depending on the size and complexity of your deployment.

Figure 6.3 shows a sample network diagram containing initial network information. The information in this figure is based on the VPN (L2TP) scenario covered at the end of this chapter.



If your browser does not support inline frames, click here to view on a separate page.

Figure 6.3 VPN network infrastructure

To complete the network diagram, additional information should be added, including WAN and LAN connections, subnet masks, gateways, and any information required to clarify location of servers and relationships to other components and networks. Depending on whether you outsource your support and, if so, how, you might also need to incorporate specifics of the ISP support in your network diagram.

Defining WAN Connections in the Perimeter Network

WAN connections are critical elements of your VPN design. The WAN infrastructure must support your business and user requirements for remote access. Some ISPs now provide their own Internet infrastructure, which provides access across the Internet using advanced technology, such as fiber optics. If performance is critical to your VPN connections, select an ISP that provides the appropriate Internet backbone.

The firewall at the edge of a perimeter network is a router. You can use a Windows 2000–based computer running the Routing and Remote Access service as a firewall on a perimeter network. You can also use most existing routers with a Windows 2000-based VPN solution.

To attach a VPN server to your internal network as well as to the Internet, connect one network adapter in the VPN server to your enterprise network and connect another network adapter to the perimeter network.

The connection to the Internet from the firewall computer running Windows 2000 Server is a dedicated connection — a WAN adapter installed in the computer. The WAN adapter is typically a DDS, T1, fractional T1, or Frame Relay adapter. For a large enterprise, the WAN connection to the Internet should be a T3 or DS3 line operating at 44.7 megabits per second (Mbps). The connection between the router and the servers in the perimeter network can be any high-speed LAN connection, but gigabit Ethernet or ATM are recommended to support heavy Internet traffic.

Note Windows 2000 remote access servers support direct connections to X.25 networks only when using an X.25 smart card for VPN connections. Connection Manager does not support X.25 or ATM connections. If X.25 or ATM support is required, users should use a Dial-Up and Networking connection instead of Connection Manager. Windows 2000 L2TP does not support native tunneling over X.25, Frame Relay, or ATM networks.

PPP Over ATM

Using ATM over a broadband connection service preserves high-speed characteristics, and QoS guarantees availability in the core networking layer, without changing protocols. This creates the potential for an end-to-end ATM network to the residence or small office. This network model provides several advantages, including:

- Support for multiple classes of ATM QoS with guarantees
- Bandwidth scalability
- An evolution path to newer DSL technologies

Adding Point-to-Point Protocol (PPP) over this end-to-end architecture adds functionality and usefulness. PPP provides the following additional advantages:

- User-level connection authentication
- Network-layer address assignment
- Multiple concurrent sessions to different destinations
- Network-layer encryption and compression

If each virtual circuit (VC) carries only one Point-to-Point (PPP) session, each destination has its own authenticated PPP session, providing authentication for each VC. This provides an extra measure of security and guaranteed bandwidth as if you had a dedicated line. Using Null Encapsulation over ATM Adaptation Layer 5 (AAL5) can further reduce overhead because PPP provides protocol multiplexing.

Adapter Configurations

It is recommended that the network adapter that connects the VPN server to the private network have a statically configured IP address that is excluded from the DHCP address pool. Before setting up the hardware, determine the TCP/IP settings to be set on the LAN adapter:

- IP address and subnet mask assigned by the network administrator.
- DNS and WINS name servers of enterprise intranet name servers.

Additionally, determine the TCP/IP settings on the WAN adapter:

- IP address and subnet mask assigned by the network administrator.
- Default gateway of the firewall, if the VPN server is on the perimeter network, and not directly connected to the Internet.

PPTP and L2TP Ports

Determine the number of ports for the WAN miniport (PPTP) and WAN miniport (L2TP) devices on each VPN server. The maximum

number of ports is subject to licensing restrictions: 1,000 ports for Windows 2000 Server, 5,000 ports for Windows 2000 Advanced Server.

For a PPTP-only or L2TP-only VPN server, specify for the unused protocol that neither remote access nor demand-dial connections are supported.

Defining Servers

The type, number, and location of servers required for your VPN infrastructure are some of the most important decisions for deploying a VPN solution, especially decisions about the servers in your perimeter network. These decisions impact the performance, security, and manageability of your network.

VPN Servers and Firewalls

When designing your VPN solution, remember that the VPN server resides in the perimeter network and that the VPN server is responsible for enforcing user access policy decisions that might be configured on the user account in the Windows 2000–based domain controller and in remote access policies.

Firewalls filter IP traffic based on fields and values in an IP packet such as the source and destination IP address and source and destination TCP port number of the packet. A single default route points to the perimeter network firewall interface so that all Internet locations are reachable. To make all private network locations reachable, either configure routing protocols on the private network interface of the VPN server or configure static routes on the VPN server summarizing all private network locations pointing to a local private network router.

Guideline A server running Windows 2000 with the Routing and Remote Access service enabled can be a virtual private networking server for both PPTP and L2TP. Remote access and VPN servers can share resources with other services and applications on the same physical computer but, for security and performance reasons, it is not recommended.

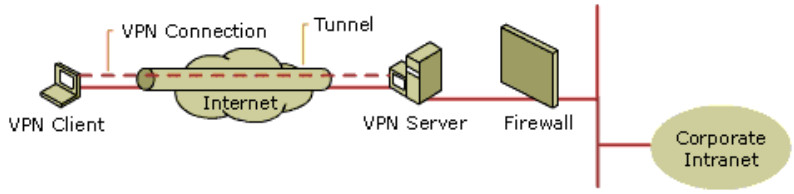
There are two approaches to using a firewall with a VPN server:

- Place the VPN server in front of the firewall.
- Place the VPN server behind the firewall.

Proper placement of the VPN server relative to the firewall can help achieve the functionality, availability, and performance goals of the design without compromising the security aspects of the design.

VPN Server in Front of the Firewall

If you position the VPN server in front of the firewall, it is connected to the Internet and the only traffic that is crossing the VPN server is from authenticated VPN clients. Packet filtering on the VPN server is used to restrict traffic to and from the IP address of the VPN server's interface on the Internet. Figure 6.4 shows a network design with the VPN server in front of the firewall.



If your browser does not support inline frames, click here to view on a separate page.

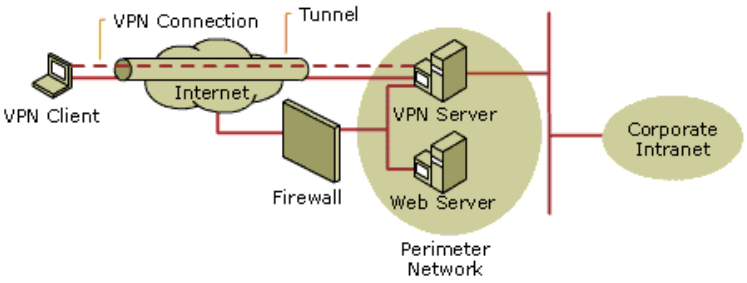
Figure 6.4 VPN server in front of the firewall

VPN Server Behind the Firewall

When multiple resources require connection to the Internet, a perimeter network protected by a firewall is required to protect the corporate intranet from unauthorized traffic. In this instance, the VPN server has no direct connection to the Internet and the firewall is configured with input and output filters that allow the passing of tunnel maintenance traffic and tunneled data to the VPN server. Additional filters allow the passing of traffic to other resources on the perimeter network, such as Web servers and File Transfer Protocol (FTP) servers.

Note The firewall needs to have the appropriate ports open to allow VPN traffic through the firewall.

Figure 6.5 shows a network design with the VPN server on the perimeter network behind the firewall.



If your browser does not support inline frames, click here to view on a separate page.

Figure 6.5 VPN server behind the firewall

Because the firewall does not have the encryption keys for each VPN connection, it can only filter by the plaintext headers of the tunneled data, so all tunneled data passes through the firewall. However, the VPN server authentication process prevents unauthorized access beyond the VPN server.

IAS Servers

The firewall should be set up between the Internet connection and your IAS server. If your IAS server on the perimeter network needs to be accessed by servers on the Internet, specify firewall conditions that explicitly permit access to packets that meet all of the following conditions:

- The packet is coming from or going to the IP address of the IAS server.
- The packet is coming from or going to the RADIUS UDP port.

If you know the IP address of the RADIUS client sending the packets through the firewall, you can provide additional security by

restricting incoming access to packets received from only that IP address. For more information about filtering, see "Specifying Authentication and Other Security Elements for VPN Access" later in this chapter.

Certification Authority

Using smart cards or other certificates, including for L2TP over IPSec, requires a certification authority (CA). If you require certificate support and do not already have an enterprise root CA, include one in your remote access network design. To support smart cards and other remote access certification requirements, implement an enterprise subordinate CA online. For more information about setting up certificate-based authentication for VPN connections, see Windows 2000 Server Help.

Phone Book Servers

The Phone Book Service (PBS) server can be located on the perimeter network of the enterprise or, if you outsource phone book support, in the ISP's perimeter network. Ensure that the PBS server is using Microsoft Internet Information Services (IIS) to run FTP and Web services. This is necessary for PBS servers to receive posts from the Phone Book Administrator (PBA) and to download updated files to clients.

Or, if distributing the phone book to multiple locations (such as an ISP distributing to multiple IAPs), install PBS on a staging server within the perimeter network and on host servers residing outside of the perimeter network. Phone book updates are posted to the staging server. Using content replication, phone book updates are then copied from the staging server through the firewall to the host servers. Additional information about outsourcing phone book support is covered later in this chapter.

Designing the IP Infrastructure

Creating a VPN server-side infrastructure that provides the best balance between security and resource optimization is critical to deploying an effective VPN solution. The core elements of this infrastructure include the IP routing and addressing and the DHCP Relay Agent.

IP Routing and Address Assignment

To enable IP routing and allow IP-based remote access, determine how you want to assign IP addresses.

If a DHCP server allocating intranet IP addresses is available, you can specify that it be used to obtain IP addresses assigned to VPN clients.

If a DHCP server is not used, specify a static pool or pools of IP addresses that are assigned to VPN clients.

If the static IP address pool represents a separate subnet, add a static IP route that consists of the remote access address pool for the routers within the intranet or enable an IP routing protocol on the remote access server. If the static IP routes are not added, then VPN clients cannot receive traffic from resources on the intranet.

Guideline If you use DHCP servers, configure the VPN server to use DHCP to assign IP addresses for VPN clients. If you did not install a DHCP server and you have a single subnet, configure the VPN server with a static IP address pool that is a subset of addresses for the subnet to which the VPN server is attached.

If you did not install a DHCP server and you have multiple subnets and a routed infrastructure, configure the VPN server with a static IP address pool that is a separate subnet from the subnet to which the VPN server is attached. Then either add the static IP routes to the routing tables of neighboring routers or enable the routing protocol of your routed infrastructure on the VPN server. For more information about how to create a static IP address pool, see Windows 2000 Server Help.

DHCP Relay Agent

Windows 2000 and Windows 98 remote access clients send DHCPInform messages to obtain configuration parameters beyond those assigned during PPP negotiation. For the VPN server to forward the DHCPInform messages between VPN clients and DHCP server, the VPN server must be configured with the DHCP Relay Agent component of the Routing and Remote Access service. The DHCP Relay Agent is automatically added when the Routing and Remote Access Server Setup wizard is run.

If the VPN server is using DHCP to assign IP addresses to VPN clients, no further configuration is necessary. If the VPN server is using a static pool of addresses and a DHCP server is present, then the DHCP Relay Agent must be configured with at least one IP address of a DHCP server.

Optimizing the RADIUS-based VPN Infrastructure Design

In a proper design of remote access and VPN servers, the maximum data rate of the Internet or intranet connection must be the limiting factor in accessing resources. To optimize the availability and performance for RADIUS clients in a VPN solution, determine how you want to implement functionality across your VPN servers, implement load balancing to maximize existing resources, and fine-tune the hardware and software design as needed to provide the required level of service.

Load Balancing

Create VPN server designs by adding multiple servers in a load-balancing configuration. These redundant servers distribute the remote access clients in a manner that divides total resource usage across all of the servers. Spread VPN functions over multiple servers with hardware acceleration and fallback defenses. Use the following methods to provide load balancing for a VPN solution:

- Round-robin DNS entries

  Use round robin DNS entries to distribute remote access VPN clients across multiple VPN servers to provide load balancing. To do this, register all the IP addresses of your VPN servers under the same host name in DNS. DNS uses round-robin rotation so that each address appears at the top of the list in sequence.

- Network Load Balancing

  Use Network Load Balancing (available on Microsoft Windows 2000 Advanced Server) to distribute remote access VPN clients across multiple VPN servers, to provide immediate failover in the event of a VPN server failure, and to provide load balancing.

  Note Network Load Balancing is only supported for PPTP, not L2TP or IPSec.

  When using Network Load Balancing with VPN servers and PPTP clients, it is important to configure the TCP/IP properties correctly to ensure compatibility with clients running earlier versions of Windows (such as Windows 98 and Windows NT 4.0). To do this, assign only a single virtual IP address to the network adapter used by Network Load Balancing, and do not assign another IP address to any network adapter on this subnet. This virtual IP address to the network adapter used by Network Load Balancing ensures that network traffic returning from the VPN server to the client originates from the virtual IP address to which the client sent the request.

  Set bindings so that Network Load Balancing is enabled for the cluster network adapter (the network adapter with the cluster's virtual IP address).

  Note If a particular VPN server fails, client sessions handled by that server handle also fail. Clients are prompted to log on again; their new session is handled by one of the remaining hosts.

  To provide load balancing for VPN clients, use the default port rule for all hosts, as follows:

  - Set the port range to 0-65535 (the default). Setting the range to the default covers all of the ports, so the port rule remains

valid even if there is a change in the port numbers that you want to cover.

- Accept the default filtering mode, load weight/equal load distribution, and affinity settings.

Hardware and Software Optimization

Additional optimization of a VPN solution can be accomplished by:

- Configuring multiple RADIUS servers for each VPN server.
- Registering redundant RADIUS clients with RADIUS servers to ensure proper authentication and accounting.
- Increasing the data rate of the connections between the remote access VPN client and the private network.
- Adding VPN servers.
- Upgrading the hardware resources of existing VPN servers.
- Replacing existing VPN servers with higher performance servers.
- Incorporating support for direct connections, such as ADSL.

Designing Outsourced Components

One of the primary benefits of outsourcing is that the ISP can provide many of the components required to support VPN access, including NASs for access from various geographical access points, RADIUS proxy servers for secure routing of access requests to the enterprise without exposing enterprise data, and phone book support for delivering the latest access numbers either to the enterprise or directly to the client.

Outsourced NASs

VPN users dial first to a NAS. Unless you have an outsourcing agreement that specifies the support required from the ISP's NASs, including connection speeds, device support, and levels of service, the ISP's NASs can be the weak link in your VPN solution. If outsourcing support, ensure that the NASs implemented by the ISP meet your access requirements.

Outsourced RADIUS Proxies

If you outsource your VPN solution, you can contract with an ISP to provide authentication services, or you can ask the ISP to provide a RADIUS proxy to the enterprise. Use of a RADIUS proxy is recommended for security purposes, to enable authentication without divulging employee data to third parties.

If you want to use a Windows-based RADIUS proxy, you can use Internet Connection Services for Microsoft RAS, Commercial Edition for Windows NT 4.0. Windows 2000 IAS does not support the RADIUS proxy functionality.

Outsourced Phone Book Support

If you outsource your VPN solution, you can contract with an ISP to provide phone book maintenance and support. To maintain phone book data in the enterprise, specify that the ISP must provide a list of access numbers in a format that can be imported into the enterprise-maintained phone book, such as a phone book created and maintained by using Microsoft Connection Point Services (CPS). You can then integrate the ISP access numbers as appropriate. For instance, you can:

- Integrate multiple lists of access numbers (including lists from multiple ISPs) into a single phone book to be distributed to all users.
- Split out access numbers by location to provide individual access lists to users in specific regions or other geographic areas.
- Create custom phone books that contain access points that support a specific access medium (such as ADSL).

Determine the best structure for your phone book support before negotiating an agreement with your ISP. The structure of your phone books should determine the requirements you place on your ISPs for the content and format of access number data.

You might also decide to have the ISP do all maintenance and updates for a phone book. This is advantageous if you are using a single ISP, do not have additional access numbers to be merged, and do not want to incur the expense of setting up and maintaining phone book servers within the enterprise. To enable automatic updating of phone books, implementation of this type of phone book support requires client connection software (such as Connection Manager) that supports implementation of pre-tunnel actions, as well as support of the ISP for automatic updates.

Developing Specifications for VPN Access and Expanded Security

Most of the considerations for creating detailed specifications for dial-up client access are also valid for VPN access (such as the maximum number of simultaneous connections, etc.). Additionally, consider the following when developing your specifications:

- What are your quality and reliability requirements for Internet access?
- What are your ISP costs?
- What is required to support the infrastructure (for the enterprise and the ISP)?

Identifying the Administrative Model for a VPN Solution

To establish specific authorization and authentication requirements for VPN users that are different than for dial-up users, use an access-by-policy administrative model. If you want to use a single solution for everyone (for instance, only VPN is supported), you can use access-by-user model to establish specific restrictions. You do not need to create user accounts just for VPN connections. VPN servers use the user accounts specified in the available user accounts databases, according to Windows 2000 Server security.

If you want to deploy multiple VPN and dial-up solutions and you are using Windows 2000 VPN servers, but need to restrict access of individual groups, you can use groups with universal scope to define different authorization and authentication restrictions for each solution. This is only supported when using the access-by-policy administration model in a Windows 2000 native-mode domain.

For examples using the access-by-policy model for VPN access, see Windows 2000 Server Help.

Determining How to Set Up Remote Access Policies for Secure VPNs

Some elements of VPN deployment can affect the way in which you structure your remote access policies and the way in which security is controlled. The remote access policies you use for VPN and expanded security should be separate from other dial-up remote access policies.

VPN Remote Access Policy Structure

By using remote access policies, you can create a policy that requires remote access VPN connections to use a specific authentication method and encryption strength.

For example, you can create a Windows 2000 group called VPN Users whose members are the user accounts of the users creating remote access VPN connections across the Internet. Then, you create a policy with two conditions on the policy: **NAS-Port-Type** is set to **Virtual (VPN)** and **Windows-Group** is set to **VPN Users**. Finally, you configure the profile for the policy to select a specific authentication method and encryption strength.

You can also structure remote access policies to force the use of strong authentication and encryption for VPN users and a different set of authentication and encryption constraints for dial-up users.

Conditions for Granting or Denying VPN Access Permission

VPN access requires that your VPN servers can recognize and process requests from NASs or, if applicable, RADIUS proxy servers at the ISP locations. If IAS receives an access request from a RADIUS proxy, IAS cannot detect the manufacturer of the NAS that originated the request. This can cause problems if you plan to use authorization conditions based on the client vendor and have at least one client defined as a RADIUS proxy.

The friendly name that you provide for your RADIUS clients, including the RADIUS proxy, can be used in remote access policies to restrict access.

Defining RADIUS Support for VPNs

If your network design includes RADIUS support, specify how this support is to be implemented. This is done in much the same way as a dial-up solution. This section covers considerations that are focused on VPN deployment and build on the information in "Providing Dial-Up Access".

RADIUS Client Properties

RADIUS client properties are specified for VPN servers in the same manner as they are for remote access servers in dial-up client access solutions. When specifying the friendly name, designate the tunneling protocol in the name to clarify the role of the server to administrators.

RADIUS Realms

You can use RADIUS realm names, either a prefix or suffix to the user name, to support outsourced VPN support. This is useful for situations in which a service provider supplies access points without providing authentication and authorization, but uses a RADIUS proxy to forward logon requests to the enterprise. In this case, a realm name is essential to routing the logon request to the appropriate location and servers for validation of logon credentials. Realms are also useful for tracking usage for accounting purposes.

If outsourcing VPN support, especially if outsourcing to multiple ISPs who use RADIUS proxies to forward access requests to the enterprise network for authentication, specify for the outsource vendor the RADIUS realm prefixes or suffixes to be used to route the requests to the RADIUS servers on the enterprise perimeter network.

User names in RADIUS messages must be converted before authentication processing begins. To do this, specify the rules to use for realm stripping, including the pattern (realm suffix or prefix) to find and the pattern to be used to substitute for it (which can be blank if realm stripping is all that is required). You cannot replace a realm suffix with a realm prefix or vice versa.

Advanced Settings for RADIUS Attributes

If outsourcing VPN support, the ISP can provide NAS-specific information about vendor-specific attributes required to set up RADIUS standard attributes and vendor-specific attributes (VSAs) appropriately in the remote access profiles on the IAS server. For more information about specifying these attributes, see "Providing Dial-Up Client Access."

Specifying Authentication and Other Security Elements for VPN Access

Implementing VPNs using Windows 2000 provides the basis for establishing secure connections if appropriate specifications are enforced in the network. In addition to establishing secure passwords, you must specify how security is to be enforced, including authentication, encryption, filtering, and other security requirements.

Authentication Providers for VPNs

For each VPN server, determine whether to authenticate the credentials of the VPN client locally or centrally:

- Specify Windows authentication to authenticate the credentials locally by using Windows 2000 authentication credential verification mechanisms. This usually involves contacting a domain controller to verify the credentials of the VPN client.
- Specify RADIUS to authenticate the credentials centrally on a RADIUS server, such as the Windows 2000-based IAS server. Ensure that the shared secret between the RADIUS server and the VPN servers follows secure password guidelines.

For more information about specifying the authentication provider, see "Providing Dial-Up Client Access."

Authentication Methods

The authentication of VPN clients by the VPN server is a critical security concern. Authentication takes place at two levels:

- Computer-level authentication

  When Internet Protocol security (IPSec) is used for an L2TP over IPSec connection, computer-level authentication is performed through the exchange of computer certificates during the establishment of the IPSec security association (SA). An SA is a combination of policy and keys that define the common security services, mechanisms, and keys used to protect communication from end to end. The security parameters index is a unique, identifying value in the SA used to distinguish among multiple security associations that exist on the receiving computer, such as when a remote access server serves multiple clients. Internet Security Association and Key Management Protocol (ISAKMP) centralizes SA management, reducing connection time, while the Oakley key generation protocol generates and manages the authenticated keys used to secure the information.
- User-level authentication

  Before data can be sent over the PPTP or L2TP tunnel, the user or demand-dial router that requests the VPN connection must be authenticated. User-level authentication occurs by means of a Point-to-Point Protocol (PPP) authentication method using an authentication protocol, such as MS-CHAP version 2, that is negotiated during the connection establishment process.

Support for authentication protocols by virtual private networking clients is outlined in Table 6.1.

Table 6.1 Authentication Protocol Support

Virtual Private Networking Client	Supported Windows 2000 Remote Access Authentication Protocols	Unsupported Windows 2000 Remote Access Authentication Protocols
Windows 2000	MS-CHAP, CHAP, Shiva Password Authentication Protocol (SPAP), PAP, MS-CHAP v2, and EAP	
Windows NT version 4.0	MS-CHAP, CHAP, SPAP, PAP, and MS-CHAP v2 (with the Windows NT 4.0 Service Pack 4 and later)	EAP
Windows 98	MS-CHAP, CHAP, SPAP, PAP, and MS-CHAP v2 (with the Windows 98 Service Pack 1 and later)	EAP

Windows 95	MS-CHAP, CHAP, SPAP, PAP, and MS-CHAP v2 (with the Windows Dial-Up Networking version 1.3 Performance and Security Upgrade for Windows 95)	EAP

Use the strongest authentication scheme possible for your VPN connection, such as EAP-TLS with certificates. Otherwise, use the MS-CHAP version 2 authentication and enforce the use of strong passwords on your network.

Windows 95, Windows 98, and Windows NT 4.0 clients running the latest service pack can force the use MS-CHAP v2 for PPTP connections by setting the Secure VPN flag in the registry. For more information, see the release notes for Dial-Up Networking 1.3 Security Upgrade.

Certificates

Creating L2TP over IPSec remote access VPN connections requires installation of computer certificates on the VPN client and the VPN server.

Note When used as a client VPN connection (using EAP), a computer certificate authenticates the user, not the computer. When used as a gateway-to-gateway connection, the computer is assigned a user ID and is authenticated.

Creating certificates requires an enterprise root certification authority (CA). If you do not have a root CA, determine how you want to set it up.

You have two options for implementing the certificates you specify:

- Automatic allocation of computer certificates to computers in a Windows 2000 domain, known as auto-enrollment.
- Manual enrollment of computer certificates by using Microsoft Internet Explorer to obtain the certificate and Certificate Manager to import the certificate.

For more information about computer certificates for L2TP over IPSec VPN connections, see Windows 2000 Server Help.

The Enrollment Agent certificate does not have to be issued by the same CA issuing certificates for smart cards. The issuing CA for the Enrollment Agent certificate only needs to be a trusted enterprise CA in the domain. In that case, make sure that there is an enterprise CA in your domain capable of issuing Enrollment Agent certificates.

For more information about specifying support for certificates, see Windows 2000 Server Help.

Smart Cards

The use of smart cards for user authentication is the strongest form of authentication in Windows 2000. Using smart cards for remote access VPN connections requires the use of EAP with the smart card or another certificate (TLS) EAP type, also known as EAP-Transport Level Security (EAP-TLS), which supports secure authentication and strong encryption-key generation. Determine which type of certification is required:

- Certification for smart card logon

  Specify this to use the smart card for logging on to Windows-based computers only.

- Certification for smart card users

  Specify this to use the smart card for secure e-mail as well as for logging on to Windows-based computers.

Smart card implementation is not supported on a stand-alone remote access server.

For more information about specifying support for smart cards, see Windows 2000 Server Help.

Token Cards and Other Third-Party EAP-based Security

If token card or other EAP support is required for your enterprise, specify the third-party EAP plug-in that you want implemented. Specify this EAP plug-in for each remote access policy that requires this third-party EAP support. The components for an EAP type must be installed on every remote access client and every computer that is performing authentication. If a Windows 2000–based computer is running the Routing and Remote Access service and is configured for Windows authentication, install the EAP type on the Windows 2000–based computer. If configured for RADIUS authentication and the RADIUS server is also an IAS server, install the EAP type on the IAS server.

EAP-MD5 CHAP

EAP-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP) is a required EAP type that uses the same challenge handshake protocol as PPP-based CHAP, but the challenges and responses are sent as EAP messages.

A typical use for EAP-MD5 CHAP is to authenticate the credentials of remote access clients by using user name and password security systems. You can also use EAP-MD5 CHAP to test EAP interoperability. Specify this only if EAP-TLS authentication is not appropriate, for example, if implementing EAP on a stand-alone remote access server and data encryption is not required.

Data Encryption for PPTP and L2TP

For virtual private networking connections, you protect your data by encrypting it between the ends of the virtual private network (VPN) connection. Always use data encryption for VPN connections when private data is sent across a public network such as the Internet, where there is always a risk of unauthorized interception. For VPN connections, Windows 2000 uses MPPE with the Point-to-Point Tunneling Protocol (PPTP) and Internet Protocol security (IPSec) encryption with the Layer Two Tunneling Protocol (L2TP).

Note It is possible to have either a non-encrypted PPTP connection (where the PPP payload is sent in plaintext) or a non-encrypted non-IPSec-based L2TP connection (where the PPP frame is sent in plaintext). However, a non-encrypted connection is not recommended for VPN connections over the Internet because communications of this type are not secure.

The encryption and decryption processes depend on both the sender and the receiver using a common encryption key. The length of the encryption key is an important security parameter, especially over public networks. You can use computational techniques to determine the encryption key. However, such techniques require more computing power and computational time as the encryption keys get larger. Therefore, it is important to use the largest key size to ensure data confidentiality.

For encryption, you can use either link encryption or end-to-end encryption:

- Link encryption encrypts the data only on the link between the VPN client and the VPN server. For PPTP connections, you must use Microsoft Point-to-Point Encryption (MPPE) in conjunction with either MS-CHAP or EAP-TLS authentication. For L2TP over IPSec connections, IPSec provides encryption on the link between the VPN client and the VPN server.
- End-to-end encryption encrypts the data between the source host and the destination host. After a VPN connection is made, IPSec can be used to provide end-to-end encryption.

When data encryption is performed between the VPN client and VPN server, it is not necessary to use data encryption on the communication link between a dial-up client and its Internet service provider (ISP). For example, a mobile user uses a dial-up networking connection to dial in to a local ISP. After the Internet connection is made, the user creates a VPN connection with the enterprise VPN server. Because the VPN connection is encrypted, there is no need to use encryption on the dial-up networking connection between the user and the ISP.

Data encryption for PPTP connections is available only if MS-CHAP (v1 or v2) or EAP-TLS is used as the authentication protocol. Data encryption for L2TP connections relies on IPSec, which does not require any specific authentication protocol. In either case, if data encryption is specified as required, IPSec enforces the encryption and, if the server declines data encryption, the connection is denied.

For each remote access policy that supports PPTP or L2TP connections, determine the levels of encryption supported:

- No Encryption

  Allow connections that don't use data encryption.

- Basic

  Allow connections using IPSec 56-bit (Data Encryption Standard) DES or MPPE 40-bit data encryption.

- Strong

  Allow connections using IPSec 56-bit DES or MPPE 56-bit data encryption.

- Strongest

  Allow connections using IPSec Triple DES (3DES) or MPPE 128-bit encryption.

IPSec encrypts data for an L2TP connection. IPSec uses computer-based certificates for computer-level authentication, thereby reducing the ability of an unauthorized computer to impersonate an authorized computer.

The level of IPSec that is used for the duration of the connection is dependent upon the encryption settings on the profile for the remote access policy used for L2TP connections.

Guideline Use IPSec in all solutions where security is a top priority.

VPN clients that use PPTP or L2TP over IPSec and that do not run Windows-based operating systems can access a remote access server running Windows NT 4.0 (PPTP only) or Windows 2000. No special configuration of the remote access server is required for other virtual private network clients. However, if these clients require secure VPN connections, make sure that other VPN clients support the proper encryption. For PPTP, Microsoft Point-to-Point Encryption (MPPE) must be supported. For L2TP, IPSec encryption must be supported. Windows 95, Windows 98, and Windows NT 4.0 clients running the latest service pack and dial-up networking upgrade that support 128-bit MPPE encryption can force the use of strongest encryption for all connections by setting a flag in the registry. For more information, see the release notes for the dial-up networking security upgrade.

IP Addressing and Filtering

Windows 2000–based servers can be configured to filter incoming and outgoing traffic, based on source and destination addresses and the type of traffic. Both server-level and policy-level filtering are supported by the Routing and Remote Access service. Two of the most common types of filters are RADIUS packet filters and VPN packet filters.

Note Only RADIUS and VPN packet filters are covered in this section. You can also implement other filters. Define as many filters as required to provide all required filtering. For more information about filtering, see Windows 2000 Server Help.

RADIUS Packet Filters

If you must allow access to an IAS server on the perimeter network from the Internet and you have a firewall, set up the firewall with packet filters to allow RADIUS traffic to and from the IAS server. For example, if the IAS server on the perimeter network is using the public IP address of 131.107.255.17 and UDP ports 1812 (for RADIUS authentication) and 1813 (for RADIUS accounting), you should set up the firewall with packet filters that allow the following IAS traffic:

- Traffic from the Internet to the IAS server:
  - To the destination of 131.107.255.17 and with a UDP destination port of 1812.
  - To the destination of 131.107.255.17 and with a UDP destination port of 1813.
- Traffic from the IAS server to the Internet:
  - From the source of 131.107.255.17 and with a UDP source port of 1812.
  - From the source of 131.107.255.17 and with a UDP source port of 1813.

    Note These filters do not specify the inbound source or outbound destinations corresponding to the RADIUS clients or proxies on the Internet. You can create more specific filters that allow RADIUS traffic from only your RADIUS clients, however, this requires two filters (one for inbound traffic and one for outbound) for each RADIUS client or proxy on the Internet.

VPN Packet Filters

To protect your intranet so that the only traffic that is forwarded to the intranet is the traffic that is sent and received over secure VPN connections, configure PPTP or L2TP over IPSec filters on the interface of the VPN server that is attached to the perimeter network. To use additional IP packet filters to restrict traffic for VPN connections, determine which of the following types of filtering are appropriate for your VPN solutions:

- **PPTP or L2TP over IPSec filtering for VPN servers** - To secure the VPN server from sending or receiving any traffic on its Internet interface except VPN traffic, you must configure IP input and output packet filters to discard all traffic except PPTP or L2TP over IPSec traffic. These filters must be configured on each interface that corresponds to the connection to the Internet.
- **Remote access policy profile packet filtering** - To define the specific types of IP traffic that are allowed into and out of a remote access VPN connection (sent or received within the PPTP or L2TP tunnel), you can configure IP packet filters on the profile for the remote access policy that is used for the remote access VPN connections. The filters are defined in the same way as the IP packet filters for dial-up remote access connections. To implement remote access policy profile packet filters, determine which remote access policies require filters and then, for each policy, which packet filters are required.

To implement these filters by using Windows 2000 Server either at the VPN server level or for specific remote access policies, specify whether the packet filters are to be applied to PPTP or L2TP connections (or both) and then determine:

- Whether filters are to be applied to traffic to the client (source network) or from the client (destination network).
- Whether the filters define traffic that is allowed, or denied.
- The IP address and subnet mask of the source network or destination network being filtered.
- The protocol being filtered (including protocol qualifiers, such as source port and destination port, specific to the protocol).

The information in Table 6.2 shows the information required to configure an interface to discard all packets except those that represent PPTP connections.

Table 6.2 Input and Output Filter Settings for PPTP Connections

Filter Type and Sequence	IP Address	Subnet Mask	Protocol	Source Port	Destination Port
First input filter	Destination of 131.107.1.23 (for example)	255.255.255.255	Other: 47		

Second input filter	Destination of 131.107.1.23 (for example)	255.255.255.255	TCP	0	1723
Third input filter (optional)	Destination of 131.107.1.23 (for example)	255.255.255.255	TCP [established]	1723	0
First output filter network	Source of 131.107.1.23 (for example)	255.255.255.255	Other: 47		
Second output filter network	Source of 131.107.1.23 (for example)	255.255.255.255	TCP	1723	0
Third output filter network	Source of 131.107.1.23 (for example)	255.255.255.255	TCP [established]	0	1723

Note The optional input and output filters are only configured if the PPTP server is also used as a PPTP client. For example, if the PPTP server is creating PPTP-based demand-dial connections, it is acting as a PPTP client. For more information about demand-dial connections, see "Connecting Remote Sites" in this book.

Table 6.3 shows the information required to configure an interface to discard all packets except those that represent L2TP over IPSec connections.

Table 6.3 Input and Output Filter Settings for L2TP over IPSec Connections

Filter type and sequence	IP Address	Subnet Mask	Protocol	Source Port	Destination Port
First input filter	Destination of 131.107.1.23 (for example)	255.255.255.255	UDP	500	500
Second input filter	Destination of 131.107.1.23 (for example)	255.255.255.255	UDP	1701	1701
First output filter	Source of 131.107.1.23 (for example)	255.255.255.255	UDP	500	500
Second output filter	Source of 131.107.1.23 (for example)	255.255.255.255	UDP	1701	1701

Note There are no filters required for IPSec ESP traffic using the IP protocol of 50. The Routing and Remote Access service filters are applied after IPSec removes the ESP header.

Dial-up Constraints for VPN Solutions

You can use dial-up constraints to modify how a remote access policy implements PPTP and L2TP connections, as well as how to implement dial-up backup connections.

PPTP and L2TP Constraints

For each remote access policy that supports only VPN access, you can specify in the profile for that policy that only connections using specific dial-up media are allowed VPN access.

If you do not want to support extended connections, you can specify maximum connection time limitations to reduce costs associated with unproductive connection times. This includes specifying the maximum idle time and maximum session time. For example, specify that the connection is to be disconnected if idle for more than 30 minutes to limit costs. Or restrict the maximum session time to 600 minutes to prevent connections from remaining active overnight.

Backup Access Constraints

If you support dial-up access as a backup for VPN access, you can set up a policy to specify limitations for dial-up access. For instance, you can restrict dial-up access to a specific dial-up media (such as asynchronous modems) and only one phone number.

Account Lockout

In addition to IP filtering, you can use the account lockout of remote users feature to help prevent unauthorized access attempts. When deciding whether to deploy this feature, remember that if you enable the account lockout feature, a malicious user can deliberately force an account to be locked out by attempting multiple authentications until the user account is locked out, thereby preventing the authentic user from being able to log on.

To implement the account lockout feature, specify:

- The number of failed attempts before future attempts are denied.

  The default is 0, which means that account lockout is disabled.

- How often the failed attempts counter is reset.

  When account lockout is enabled, the default is 2,880 minutes (48 hours). A successful authentication resets the failed attempts counter when its value is less than the configured maximum. Set up account lockout carefully to avoid unnecessarily impeding access by legitimate users. Although a user account can be manually reset before the failed attempts counter is automatically reset, implementing the account lockout feature can cause productivity problems for the user if the maximum number of denials is too low or the reset time is too high.

Enable the account lockout feature by changing settings in the Windows 2000 registry on the computer that provides the authentication. If the remote access server is configured for Windows authentication, modify the registry on the remote access server. If the remote access server is configured for RADIUS authentication, and Windows 2000 Internet Authentication Service (IAS) is being used, modify the registry on the IAS server. For more information about specifying this registry entry, see Windows 2000 Server Help.

Note Remember that this account lockout method is implemented in the registry, which is different from the account lockout policy for domain or local user accounts.

If using smart cards, the smart card manufacturer controls account lockout for PINs that are not valid. Recovery from account lockout due to PINs that are not valid requires replacement of the smart card.

Specifying Extended Support for PPP Clients

Implementation of some demand-dial designs may require the customization of PPP client features. Determine how these features affect your VPN design and what customization is required to meet your requirements.

Multilink for PPP Clients

Multilink supports the combination of multiple physical connections into a single logical connection, but not virtual connections. To avoid conflicts with other protocols, ensure that Multilink is not configured in remote access policies that provide VPN support.

LCP Extensions for PPP Clients

Link Control Protocol (LCP) extensions are enabled by default but can cause problems with NASs running older PPP software, so you might need to disable them on each VPN server if problems occur and you do not require the extensions.

Software Compression for PPP Clients

Support for Microsoft Point-to-Point Compression (MPPC) is enabled by default on Windows 2000–based VPN servers. Generally, use this compression unless you are supporting the connection of VPN clients that do not support MPPC.

Defining VPN Accounting and Logging Methods

Specifying VPN accounting and logging methods requires the same decisions that are made for dial-up client access. This section provides information about VPN-specific considerations.

Accounting Providers

You can specify for each VPN server where to log access attempts received by the VPN client:

- Specify Windows 2000 to log records locally on the Windows 2000-based VPN server.
- Specify RADIUS to log records centrally on a RADIUS server, such as the Windows 2000–based IAS server.

Remote Access Logging and Accounting

The remote access logging functionality is useful for tracking VPN usage by enterprise users and groups. This is especially useful for tracking and analyzing usage of outsourced connections to determine when specific negotiated thresholds must be adjusted.

Event Logging

As with dial-up client access, use event logging sparingly to prevent unnecessary use of system resources. If outsourcing support, ensure that your service provider supports the level of event logging and reporting that you require for your users.

Defining Connection Manager Support for VPNs

VPN support and many expanded security features can be implemented by using Connection Manager, especially if Windows 2000 is the operating system running on the client. A single Connection Manager service profile can support both dial-up and VPN connections. Implementation of a service profile to support VPN provides more options than implementation of a dial-up service profile, including support for broadband connections.

Note The decisions covered in this section about how to specify Connection Manager support are in addition to the other decisions documented in "Providing Dial-Up Client Access," such as naming conventions, how phone books are to be implemented, branding options, and custom functionality required to support your solution.

Client-Side WAN Connections

Connection Manager provides expanded support for VPN connections, beyond that which is available for dial-up access. Specify the support to be implemented in your Connection Manager service profiles, including:

- Whether the service profile is to support persistent connections. Unless you outsource access support and have negotiated ISP RADIUS proxy support for dial-up connections, you must specify support for direct (persistent) connections to enable users to use pre-established connections to ISPs that establish voluntary end-to-end connections.
- If you want to support both dial-up and VPN connections. You can specify that VPN access is to be used for all connections, for some connections, or for no connections. Supporting only VPN connections is useful for outsourced VPN support, especially if contracting for unlimited access for all users. A mixture of VPN and dial-up access is useful for reducing service provider costs for some deployments.
- Whether PPTP or L2TP is to be used. The default for Connection Manager is to try L2TP first and then PPTP. This sequence is significant because trying an unsupported protocol first can cause significant authentication delay (possibly several minutes, depending on your environment). Using advanced customization techniques, you can specify to try only PPTP or L2TP or to try both (and which to try first).

Client Access Support

The service profiles you create can provide ease-of-use and security features that improve the VPN logon experience for the user. Specify the client-access support you want to provide in your Connection Manager service profiles, including:

- Whether a single-click logon process can be supported. Because a VPN connection requires establishing a connection with an ISP and then establishing a tunneled connection to the enterprise, logon credentials are required for each. If matching credentials can be implemented for the ISP connection and enterprise connection, users see only a single set of logon credentials. If you implement this option, disable the saving of the enterprise password to protect the security of the credentials. If the user name and password used to connect to the ISP is the same as that used to connect to the enterprise, simplify the user logon process by specifying that Connection Manager automatically uses the same credentials for both parts of the VPN connection.
- Whether you want users to save passwords. You have the option of using advanced customization techniques to disable the saving of the enterprise password, the Internet password, or both. If you want to provide single-click connectivity and cannot use the same credentials for both connections, do not disable the Internet Logon password in the service profile (leave the HideInternetPassword option in the service provider (.cms) file set to the default of 0). However, as with dial-up connections, disable the save password feature (use advanced customization techniques to edit the .cms file and set the HidePassword option to 1). This combination of settings supports single-click access without jeopardizing the security of the enterprise credentials. Then users can save the Internet password so that they only have to manually enter the enterprise credentials.
- The VPN server address, specified either as a DNS name or as a TCP/IP address for the end-point server. If you do not want to let the server assign addresses, you can specify the DNS or Windows Internet Name Service (WINS) addresses to be used, including:
  - A primary and secondary DNS IP address for the end-point server.
  - A primary and secondary WINS IP address for name-resolution on the network of the end-point server.

Service Providers and Outsourced Support

When implementing VPN connections, you might need to integrate some elements of the service provider's infrastructure with the enterprise's infrastructure and reflect this integration in your Connection Manager service profile. Specify how these elements are implemented in Connection Manager components, including:

- Who should provide the support for developing and maintaining Connection Manager service profiles and CPS phone books. For security reasons, at least portions of these are best retained in-house. For example, if you integrate a dial-up solution with an ISP solution, you might contract with the ISP to develop and provide to you a phone book containing all of their access points, but you

might then develop your own phone books with your internal dial-up numbers.

- If you want to merge service profiles. When you merge service profiles, a single VPN server address is used for all access. You can merge dial-up and VPN access numbers into a single profile to control VPN costs, especially if VPN access is charged by the minute. For example, if you want users to dial-in directly to the enterprise when in the local calling area, but use VPN connections when out of the local area, put the list of access numbers provided by the ISP in one service profile, then merge it with a top-level (referencing) profile that contains your organization's dial-up access numbers. Users see only a single phone book that contains a complete list of all access numbers and can select the connection method that is most cost-effective for their location. Using merged profiles to support multiple phone books can be especially useful if you outsource to multiple ISPs. All ISPs create their own phone books and provide their own PBS servers. Connection Manager, however, merges the phone books into a single list of access numbers, so the remote user views the multiple phone books as a single entity. Furthermore, depending on the contractual agreement between the enterprise and the ISP, the ISP might leverage the development and administration time required to set up and maintain the CPS-based phone book by offering it to other enterprise clients.
- If you want to require realm names to connect VPN users through the Internet to the enterprise by using a RADIUS server for authentication. The realm prefix or suffix specified in the service profile must match that specified on the RADIUS server.

Specifying Third-Party Client-Side Security Features

Additional security features, such as the use of smart cards, require additional client-side component installation and configuration. Specify the security features to be installed at the client, including smart card readers or token cards. Although Connection Manager can be configured to support these features, by implementing EAP support (as specified earlier), the third-party hardware determines the specific implementation requirements. Ensure that all third-party client-side security components are compatible with Windows 2000 Server before finalizing your design.

Developing Specifications for VPN and Security Support Tools

A variety of tools are available to support implementation, administration, and management of your remote access solution, including Windows 2000-based and third-party tools. Determine the tools that are most appropriate to your environment and how these tools are to be used in the implementation of your VPN solution. The Windows 2000-based tools include:

- Software development kits (SDKs) for IAS and Routing and Remote Access.
- Routing and Remote Access and Internet Authentication Service snap-ins.
- Netsh command-line tool.
- Connection Manager Administration Kit (CMAK).
- Phone Book Administrator (PBA) and Phone Book Service (PBS) of Connection Point Services.
- Network Monitor.
- Logging and tracing tools included with Windows 2000 Server.

For more information about these support tools, see "Providing Dial-up Client Access." Additionally, third-party software that supports implementing EAP plug-ins can be valuable for deploying secure remote access solutions. For more information about third-party tools used for implementing token cards, see the valuadd folder on the Windows 2000 Server operating system CD.

Testing YourVPN and Security Designs

This phase of your deployment includes individual testing of VPN access, as well as comprehensive testing of the entire external connectivity design. If you are implementing both dial-up and VPN solutions, test the dial-up solution before the VPN solution. If implementing both PPTP and L2TP, test PPTP first. If multiple remote access solutions are to be integrated, test them together after testing them individually.

Because of vulnerabilities that might be introduced from exposure to the Internet, be sure to isolate your network perimeter from your intranet during testing. Do not integrate your network perimeter with your intranet until you are confident that all security issues have been appropriately addressed.

During testing, ensure that the ISP infrastructure is tested sufficiently, including the RADIUS proxy server (if applicable) and a representative sampling of access points.

Provide the final VPN-specific troubleshooting procedures to your customer support center to use in the pilot and rollout phases of your VPN deployment.

Implementing Your VPN and Security Design

To successfully implement external connectivity solutions in your environment, your network administrators must:

- Prepare the environment for implementation of VPNs and security.
- Develop custom software to support VPN access and security.
- Install and configure VPN and security solutions.
- Implement VPN and security tools.
- Validate the VPN and security deployment.
- Stabilize the VPN and security environment.

Members of your organization might go through these steps multiple times to successfully implement (pilot and roll out) a VPN solution. For example, you might pilot PPTP, then L2TP. You might pilot VPN separately from your other solutions, and then again as part of your final integrated solution.

Preparing for VPN and Security Implementation

As with dial-up client access, preparing for implementation requires that your core networking environment is stable, including DHCP, WINS, DNS, and Active Directory. Before you start implementation efforts, ensure that the plans and design (including network diagrams) are complete and that all accounts and domains are set up in the enterprise network. Obtain the IP addresses from the appropriate network administrator and your ISP, as appropriate.

Ensure that your ISP contract has begun, that ISP user accounts have been established, and that the ISP infrastructure (including RADIUS proxy server, if appropriate) are ready for deployment.

Ensure that the appropriate physical wiring to your premises is in place and working.

Verify the compatibility of all hardware in the VPN solution (including ISP NASs and RADIUS proxy servers).

If implementing L2TP, review the IPSec policy concepts (including IPSec policy properties). For more information about IPSec, see Windows 2000 Server Help.

Developing Custom VPN Access and Security Software

As with dial-up remote client access, develop the custom software that you identified as appropriate during the design phase. To develop software for VPN client access or security features, do the following:

- Develop any SDK extensions for IAS or Routing and Remote Access service required to support your VPN solution.
- Install and run the CMAK wizard to create the required Connection Manager service profiles for VPN access, based on the worksheet completed during the design phase. If your ISP is maintaining the phone books and providing support for automated updates to the phone book, set up a pretunnel connect action to check for phone book updates. Your ISP should be able to provide the required script to support this connect action.
- Install and run Phone Book Administrator (PBA) to create the required phone books for VPN access so that it is ready to be posted to the server. Also remember to build the phone book, but not to post it yet. For more information about preparing the phone book for implementation, see the guidelines in "Providing Dial-Up Client Access" in this book.
- Develop any Connection Manager extensions required to support VPN access.

Installing and Configuring VPN and Security Components

It is recommended that you first pilot a VPN solution without smart card or other extended security features. Add additional security components after functionality of the VPN solution has been verified.

Preparing Network Components

Before installing and configuring Routing and Remote Access, IAS, and other Windows 2000 components of your VPN solution, install the server-side components required to create the basic network infrastructure for your VPN solution. These components include all server hardware and operating systems, as well as the drivers, adapters, and connections required to enable network connections.

Server Components

Install the hardware, operating systems, and drivers for the following components:

- IAS servers.
- VPN servers (remote access servers).

  Note If using the Windows 2000 mixed-mode administrative model, you must configure support for remote access servers running Windows NT 4.0. For more information about providing support for Windows NT 4.0–based remote access server in a Windows 2000 domain, see Windows 2000 Server Help.
- Phone book servers.
- Clients.
- Routers.
- Local area network (LAN) adapters with certified Network Driver Interface Specification (NDIS) drivers.
- WAN adapters.
- Multiport adapters for acceptable performance with multiple remote connections.
- WAN connections.
- Windows 2000 High Encryption Pack containing 128-bit and 3DES encryption, if appropriate.

  Note You can download the Windows 2000 High Encryption Pack from http://www.microsoft.com

Start with a clean installation of Windows 2000, use NTFS partitions, and only install the minimum components required by the server. Disable services and permissions that are not required. See your enterprise security plan for specific security measures to be implemented to lock down the network perimeter before establishing Internet access.

Verify that the IAS server is a member of the forest against which it authenticates remote users (because a trust relationship is required and all domains in Active Directory forests automatically have trust relationships with each other.) If the IAS server and the user account are not in the same forest, the domain for the user account must have a trust relationship with the domain of which the IAS server is a member. For more information about trust relationships, see Windows 2000 Server Help.

WAN Connections

The WAN adapter includes drivers that are installed in the Windows 2000 operating system so that the WAN adapter appears as a network adapter. On each WAN adapter that you installed for your VPN solution, configure the following TCP/IP settings:

- IP address and subnet mask from the InterNIC or ISP.
- Default gateway of the ISP router.

Connections to the Intranet

On each LAN adapter that you installed in the remote access and IAS servers, configure the following TCP/IP settings:

- IP address and subnet mask from the network administrator.
- DNS and WINS names servers.

Do not configure a default gateway.

Configuring the Servers

Install and configure the required software on all servers. This includes servers in the VPN infrastructure, such as VPN and IAS servers. This also includes configuring all enterprise servers that are required to support the VPN infrastructure, including the domain controllers. This does not include configuring the CA, which is done later.

VPN Servers

To configure and start a VPN server, you must be logged on with local administrator privileges. When you install Windows 2000 Server, the remote access component is automatically installed but in a disabled state. If you have not previously enabled the Routing and Remote Access service for dial-up connections, enable it by opening **Routing and Remote Access** from the **Administrative Tools** menu, right-clicking the server name, and then clicking **Configure and Enable Routing and Remote Access**. Complete the Routing and Remote Access Setup wizard to set up the protocols and IP addresses, as well as to specify the use of RADIUS. Do not configure the remote access policies yet.

Note If you need to install more protocols, install them from the Network and Dial-up Connections folder in **Local Area Connection Properties**.

All of the VPN ports are listed as separate WAN miniports (PPTP or L2TP) under **Ports** in the Routing and Remote Access snap-in. When you use the wizard to configure a VPN server, the default configuration is 128 PPTP and 128 L2TP ports.

Note When running the wizard, if you specify that the server is to be a remote access server instead of a VPN server, the default is 5,

not 128 mini-ports for each protocol.

You can change the configuration of these ports manually by obtaining properties of **Ports** in the console tree of the Routing and Remote Access snap-in. For a PPTP-only or L2TP-only VPN server, configure the **Ports Properties** for the unused port type (PPTP or L2TP) to support neither remote access nor demand-dial connections. For more information about how to configure ports on a remote access server (VPN server), see Windows 2000 Server Help.

After configuring the ports, configure the appropriate interface to provide input and output filters that support only PPTP or L2TP over IPSec connections.

Note If you go through the "VPN server" path of the wizard, PPTP and L2TP packet filters are configured, but they are not specific to the IP address of the VPN server interface. The IP routing configuration for the interface might need to be modified manually to individually specify the appropriate IP addresses for each input and output filter. For more information about setting PPTP packet filters or L2TP over IPSec packet filters, see Windows 2000 Server Help.

IAS Servers

To set up the primary IAS server, you must be logged on with local administrator privileges, install IAS, and then configure the following as appropriate:

- IAS properties, including ports and realm stripping.
- RADIUS clients (adding one for each VPN server).

  Note Ensure that the authentication and accounting shared secrets in IAS match those specified for the VPN servers.
- Remote access policies, adding one for each user or group to be supported.
- Filters
- Reversibly encrypted passwords (if using CHAP).
- Logging for user authentication and accounting.
- Event logging for IAS.

For more information about how to configure each of the above items, see Windows 2000 Server Help. Use the Netsh tool to copy the client configurations, remote access policies, registry, and logging configuration to the backup IAS server.

For more information about how to copy the IAS configuration to another server, see Windows 2000 Server Help.

Domain Controllers

If this server is a member of a Windows 2000 Active Directory domain and you are not a domain administrator, instruct your domain administrator to add the computer account of this server to the **RAS and IAS Servers** security group in the domain of which this server is a member. The domain administrator can add the computer account to the **RAS and IAS Servers** security group by using the Active Directory Users and Computers snap-in or by using the **netsh ras add *registeredserver*** command.

Verify that groups have been created for the remote VPN users, that the VPN users are in the appropriate groups, and that the computer running IAS has permission to read the user objects in the domain. Then verify that the user names and passwords are valid by testing their logon capabilities on the LAN. Verify that the user accounts have the remote access permission (by user or policy) set appropriately and that the administrative mode (native or mixed) is correct.

To support CHAP, you need to configure support for reversibly encrypted passwords. For more information about CHAP and reversibly encrypted passwords, see Windows 2000 Server Help.

RADIUS Clients

Log on to the remote access server using domain administrator credentials, and then open the Routing and Remote Access snap-in. Verify that the RADIUS accounting and authentication properties for each remote access server are correct.

Phone Book Servers

If you have outsourced maintenance and updating of phone books, verify that the ISP has set up the required phone book support.

If you provide phone book maintenance and updating internally, install and configure the Connection Point Services (CPS) Phone Book Service (PBS) as a Windows 2000 Server optional component and then post your phone books, including access numbers provided by your ISP, from PBA to the server. To do this, set up an administrative account for your PBS host and set permissions, including administrative permissions for the PBS folder, FTP accounts for known users, and write permissions for the FTP virtual directory.

Note Before anyone attempts to post to the server, verify that you have set the Write permission for the FTP virtual directory. Set this permission immediately before posting a phone book and clear it immediately after posting the phone book.

For more information about how to install and configure PBS and PBA, including how to set permissions and create and manage phone books, see Windows 2000 Server Help.

Configuring Addressing and Routing

Configure the methods of obtaining IP addresses and any static routes, as appropriate. Verify all routing before implementing the client-side components.

IP addressing

If the remote access server is using a static IP address pool to obtain IP addresses for remote access clients, optionally configure the DHCP Relay Agent with the IP addresses of at least one DHCP server. Configure starting and ending IP addresses to create a static IP address access pool for the required number of remote access clients. For more information about how to configure the DHCP Relay Agent properties, see Windows 2000 Server Help.

Note If the remote access server is using DHCP to obtain IP addresses for remote access clients, then the remote access server uses the DHCP Relay Agent to forward DHCPInform messages to the DHCP server of the selected LAN interface. In this case, the DHCP Relay Agent does not require configuration.

Routing

To reach intranet locations, configure a static route on the remote access servers. If the static address pool for remote access clients is not on the same subnet as the remote access server, configure a static route on the router to reach remote access clients.

Setting Up Certificates

If you will be using L2TP, the list of authentication methods must include certificates, and at least one computer-level public key certificate must be configured on each peer (remote client or remote access server). These should be implemented as part of an overall deployment of certification authorities (CAs) and public key infrastructure in your organization. The set up of Certificate Services for remote access should build upon the infrastructure already implemented in your enterprise.

To auto-enroll computer certificates, the Windows 2000 domain must be configured. To create a computer certificate for the VPN server

that is a member of the domain for which auto-enrollment is configured (as well as other computers that are members of the domain), restart the computer or type **secedit /refreshpolicy machine_policy** at the command prompt. For more information about configuring a domain for automatic certificate allocation from an enterprise CA, see Windows 2000 Server Help.

Note To manually enroll computer certificates, use Certificate Manager to install the CA root certificate. For more information about how to manage certificates for a computer and to request a certificate, see Windows 2000 Server Help.

Implementing Client Components

After server-side components are installed, distribute, install, configure, and test client-side components. This includes the client connection software and any additional components required to implement enhanced security features.

Client Connection Software

Distribute client connection software (such as Connection Manager service profiles) and verify that the remote VPN clients can use the software to access the intranet.

Note If implementing high encryption, ensure that clients have the required software to support the specified encryption method.

Smart Cards and other Enhanced Security Components

If using smart cards, token cards, or other EAP-based security, install the required EAP plug-ins. If installing certificate-based services, install the certificates. Use third-party instructions to complete installation of third-party components. In general, installing smart cards requires the following:

- Configure remote access on the remote access router.
- Install a computer certificate on the remote access router.
- Enable a smart card logon process for the domain.
- Enable EAP and configure the **Smart card or other certificate (TLS)** EAP type on the remote access router computer.
- Enable smart card authentication on the VPN connection on the remote access client.

For more information about setting up certificate-based authentication for VPN connections, see Windows 2000 Server Help.

Validating VPN and Security Deployment

As with dial-up client access, successfully managing VPN access requires ongoing tracking of implementation status and identifying changes required to meet evolving requirements, including continued capacity planning, performance optimization, and planning for future.

If outsourcing your VPN solution, verify that any negotiated levels of service are being provided.

It is recommended that enhanced security features, such as smart cards, token cards, and certificates, are validated by the security team.

Stabilizing the VPN and Security Environment

To stabilize the environment and to create the basis for future deployment efforts, determine the best ways for:

- Ensuring the stability of the network perimeter.
- Migrating users to L2TP, as appropriate.
- Effectively implementing emerging ISP services without disrupting service.

VPN Scenarios

The Microsoft Windows 2000 Resource Kit Deployment Lab Scenarios include two VPN scenarios:

- Connecting Remote Users Across the Internet Using L2TP
- Connecting Remote Users Across the Internet Using PPTP

The following objectives and criteria support both scenarios, because the primary difference between the two is the support for legacy clients. If both are deployed, higher security is provided for Windows 2000–based clients (using L2TP), but support for other Windows–based clients (using PPTP) is maintained.

Note A variety of additional scenarios are available. For information about deploying VPNs in various scenarios, see Windows 2000 Server Help.

This scenario shows how a specific set of requirements and objectives might be met by Windows 2000 remote client access solutions. In this scenario, a mid-size organization has identified the enterprise requirements for remote access that can be summarized as shown in Table 6.4.

Table 6.4 General Requirements and Goals in this Scenario

Area	General Requirements and Goals in this Scenario
Business	Provide a method for specific user groups to work remotely without negatively impacting their productivity or quality of their work products. The long-term goal is to enable: • Enterprise personnel to use portable computers to connect remotely while traveling. • Enterprise telecommuters who reside outside the local calling area to connect remotely from home. Ensure security of all external information and applications accessed remotely, especially research and development information, by allowing only encrypted passwords and data to be sent.
User	Provide 500 members of the sales team with the software and portable equipment required to access sales order data bases, reporting tools, product information, and e-mail from local and non-local locations. Provide 10,000 enterprise personnel with the software and home computers required to access the central network, including all applications used in-house, whether the personnel are located in the local calling area or anywhere in North America. Provide telecommuters with the computers required to connect from home. Provide each department with portable computers for employees to use while traveling. Ensure that remote access client software does not require users to be technically competent.
IT	Provide sufficient bandwidth and performance to support real-time requirements of all users. Provide fully staffed technical support 24 hours per day. Implement a system that can be centrally managed.

Table 6.5 shows sample measurable objectives developed to reflect the enterprise's implementation requirements. Table 6.6 shows additional sample objectives for a single group, specifically a group of sales representatives with local territories. Table 6.7 shows

objectives for establishing negotiated levels of service with the service provider.

Table 6.5 Remote Client Access Objectives for the Organization in the Scenario

Area	Objectives
Functionality	Support 2,000 simultaneous connections, with a minimum connection speed of 33.6 kilobits per second (Kbps). Log 100 percent of access attempts, and analyze all data within 24 hours of logging to determine inappropriate access attempts. Use existing remote access servers where possible. Use Active Directory to control user access.
Security	Require a minimum of 40-bit encryption for 100 percent of remote communications. Provide access to the network strictly on an "as needed" basis; not all remote client access users need access to all areas of the network. For users with access to sensitive areas within the network, allow access only if using 128-bit encryption. Provide real-time analysis of access logs to alert support personnel within 10-minutes of any significant unauthorized access attempts.
Availability	Provide access 24 hours per day, 365 days per year. Ensure that reliability is 98 percent or greater.
Performance	Ensure that access can be established within two minutes, and wait times for completion of any single transmission are less than 30 seconds for 95 percent of activities. Provide dial-up access support for up to 10,000 users, with up to 10,000 simultaneous remote clients accessing the system at any time.
Management	Ensure that ninety-five percent of users can install and run the client software with no calls for assistance and a maximum of 10 minutes for setup and initial connection. Manage ninety percent of enterprise NAS administration from a single central location. Enforce account lockout any time that three successive attempts to make a remote connection to a user account fail. Provide reports of access problems daily and summaries of problem areas to management weekly. Maintain and update client software with only minimal user involvement.

Table 6.6 Remote Access Objectives for Roaming Users (Traveling Employees)

Area	Objectives
Functionality	Support local sales reps' and traveling employees' access to the network using portable computers and PSTN technology for dial-up connections to a contracted ISP. Support remote access to shared folder resources on Windows 2000 and Novell NetWare 3.*x*–based servers, and to Web-based applications and files.
Security	Provide 128-bit encryption for all roaming connections.
Availability	Support remote access to enterprise resources, regardless of a single server failure, for at least 300 remote staff members, with 99.9 percent or greater reliability.
Performance	Provide support equal to local connections.
Management	Update phone book access numbers within 24 hours of availability of new access points, with daily user access.

Table 6.7 Negotiated Levels of Service for ISP Operations

The ISP guarantees the following levels of service:

Area	Objectives
Availability	Ninety-seven percent busy-free dial.
Data rates	26.4 Kbps ninety-nine percent of the time or beat industry average.
Reliability	Ninety-nine and nine-tenths percent averaged over ten or more sites; ninety-nine and eight-tenths percent reliability averaged over three to nine sites.
Packet latency	125 milliseconds (ms) or less between VPN devices or 120 ms or less between customer-premise routers within Northa America or Europe, 300 ms or less inter-region.

Sample VPN Design

To meet these objectives, the enterprise decides to implement the following:

- Windows 2000 Server–based VPN servers, each running the Routing and Remote Access service and connected to the LAN.
- Primary and backup IAS servers, each running Windows 2000 Server and connected to the local area network.
- L2TP and PPTP packet filters to provide security for the perimeter network.
- Connection Manager connection software set up to support standard dial-up access capabilities using Point-to-Point Protocol (PPP) and a Connection Point Services phone book.
- Windows–based clients with all roaming users using Microsoft Windows 2000 Professional.

Access is outsourced to a national ISP with points of presence across North America. The ISP provides the access infrastructure (NASs with no RADIUS proxy server support required), but the enterprise decides to retain in-house phone book support to prevent divulging employee data to the ISP.For more information about how an IAS-based VPN solution that supports the above objectives, see "Connecting Remote Users Across the Internet Using L2TP" and "Connecting Remote Access Users Across the Internet Using PPTP" in the Microsoft Windows 2000 Resource Kit Deployment Lab Scenarios at http://www.reskit.com .

The design and implementation for any VPN client access solution is dependent on the requirements of the environment and the decisions made to support those requirements. See Windows 2000 Server Help for additional scenarios.

Related Information in the Resource Kit

- For more information about virtual private networks, see "Virtual Private Networking" in the *Internetworking Guide*.

- For more information about Internet Protocol Security, see "Internet Protocol Security" in the *TCP/IP Core Networking Guide*.
- For more information about public key technology, certificates, and smart cards, see the chapters under "Distributed Security" in the *Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide*, as well as "Planning Distributed Security" and "Planning Your Public Key Infrastructure" in the *Microsoft Windows 2000 Server Resource Kit Deployment Planning Guide*.
