Selecting an Authentication Protocol

Because L2TP/IPSec user authentication occurs after the VPN client and the VPN server have established a secure channel of communication, your choice of authentication protocol has no effect on VPN security if you use L2TP/IPSec. However the use of MS-CHAP v2 and EAP-TLS is recommended.

To use encryption on a PPTP connection, you must use one of the following authentication protocols:

- MS-CHAP
- MS-CHAP v2
- EAP-TLS

Authentication Protocols for PPTP VPN Connections

PPTP VPN connections require the use of the MS-CHAP, MS-CHAP v2, or EAP-TLS authentication protocols. Only these three authentication protocols provide a mechanism to generate the same encryption key on both the VPN client and the VPN server. MPPE uses this encryption key as a basis for encrypting all PPTP data sent over the VPN connection.

MS-CHAP and MS-CHAP v2 MS-CHAP and MS-CHAP v2 are password-based authentication protocols. In the absence of certificates or smart cards, use MS CHAP v2, a stronger authentication protocol than MS CHAP, which provides mutual authentication. With *mutual authentication*, the VPN server authenticates the VPN client, and the VPN client authenticates the VPN server.

Note

- If you must use a password-based authentication protocol, enforce the use of strong passwords on your network. A strong password has more than eight characters and a random mixture of uppercase and lowercase letters, numbers, and punctuation marks. For example, "f3L*q02~>xR3w#4o" is a strong password. In an Active Directory domain, use Group Policy settings to enforce strong user passwords.

EAP-TLS The EAP-TLS authentication protocol is designed for use with a certificate infrastructure and either certificates or smart cards. With EAP-TLS, the VPN client sends its user certificate for authentication, and the authenticating server for the VPN server sends a computer certificate for authentication. This is the strongest authentication method, because it does not rely on passwords. For more information about EAP-TLS authentication, see "Connecting Remote Sites" in this book.

You can use Certificate Services in Windows Server 2003 as the CA for your organization, or you can use a third-party CA when you deploy EAP-TLS as your authentication method. For information about certificate requirements with Certificate Services, see "Network access authentication and certificates" in Help and Support Center for Windows Server 2003.

Using a third-party CA requires the following setup:

- The certificate in the computer store of the authenticating server must contain the Server Authentication certificate purpose in Enhanced Key Usage (EKU) extensions. A certificate purpose is identified with an object identifier (OID). The object identifier for Server Authentication is 1.3.6.1.5.5.7.3.1.
- The Subject Alternative Name property of the computer certificate must contain the fully qualified domain name (FQDN) of the computer account of the authenticating server.
- The cryptographic service provider for the computer certificates on the authenticating server must support the secure channel (Schannel) security package. Without support for Schannel, the authenticating server cannot use the certificate, and the certificate will not be available for use in the remote access policy.
- The certificate installed on a remote access client that is running Windows Server 2003 must contain the Client Authentication certificate purpose (OID 1.3.6.1.5.5.7.3.2).
- The Subject Alternative Name property of the user certificate must contain the FQDN of the user account of the VPN client.
- Both the certificate in the computer store of the authenticating server and the user certificate of the remote access client must contain a private key.

Authentication Protocols for L2TP/IPSec Connections

For L2TP/IPSec connections, you can use any user authentication protocol, because the authentication occurs after the VPN client and VPN server have established a secure channel of communication. This is referred to as an *IPSec security association (SA)*. It is strongly recommended that you use either MS-CHAP v2 or EAP-TLS to provide the most secure user authentication that is available.

Guidelines for Selecting Authentication Protocols

Consider the following factors when choosing an authentication protocol for VPN connections:

- If you use smart cards or have a certificate infrastructure that issues user and computer certificates, use the EAP-TLS authentication protocol for both PPTP and L2TP connections. EAP-TLS is supported by VPN clients running Windows 2000, Windows XP, or Windows Server 2003.

- If you must use a password-based authentication protocol, use MS-CHAP v2, and enforce strong passwords using Group Policy. MS-CHAP v2 is supported by VPN clients running Windows XP, Windows Server 2003, Windows 2000, Windows NT Workstation 4.0 with Service Pack 4 (SP4) and later, Windows Millennium Edition, or Windows 98.

- Use the most secure protocols that your network access servers and clients can support. If you need a high level of security, configure the remote access server and the authenticating server to accept only a few very secure authentication protocols. Alternatively, if flexibility is more important than maintaining a high level of security, configure the authenticating server to accept less secure authentication protocols. For more information about designing and deploying IAS, see "Deploying Internet Authentication Service (IAS)" in this book.