Global Information Assurance Certification Paper

An Evaluation of Windows 2000's Virtual Private Networking (VPN): Microsoft's Implementation of the standards and the implications for network security

---

This paper was written by Matt Morton to complete the requirements of the SANS GIAC Windows NT Security Administrator certification

Introduction

Microsoft really "threw in the kitchen sink" when it created its very ambitious new operating system, Windows 2000. It would seem Microsoft was attempting to make an operating system to meet every possible need and then some. There are many, many new features in this operating system. This paper is an attempt at a detailed evaluation of the remote access Virtual Private Networking features in Windows 2000 Advanced Server and Professional Workstation. Virtual private Networks are used to encrypt data and authenticate packets between computers. For the many administrators who have long tired of the numerous interoperability headaches of having to make multiple different vendor implementations of a particular type of VPN work together, the new VPN features in Windows 2000 sounded like they might provide a quick and much needed solution. Since Microsoft dominates the business desktop operating systems market, a standards based VPN client bundled with their workstation (at no extra charge) operating system should greatly ease many of these headaches. At least you would be able to standardize on one VPN client, or so the thinking / marketing went….

Unfortunately, as with most new Microsoft features, rather than being a perfect implementation of a standard, the Microsoft's VPN solution is a Microsoft interpretation of the standards with added Microsoft features to improve operation in a Microsoft centric environment. What was finally shipped was a suite of protocols for creating VPN tunnels, including two that can be used for creating remote access VPN connections. Conspicuously absent from Windows 2000 was the industry leading standard which everyone was hoping would be natively supported, Internet Protocol Security (IPSec). NOTE: IPSec support is included in Windows 2000 but not for remote access VPNs. Given that the industry leading option is missing and numerous other security and deployment issues exist with the options Microsoft has settled on, we are left with a less than perfect solution.

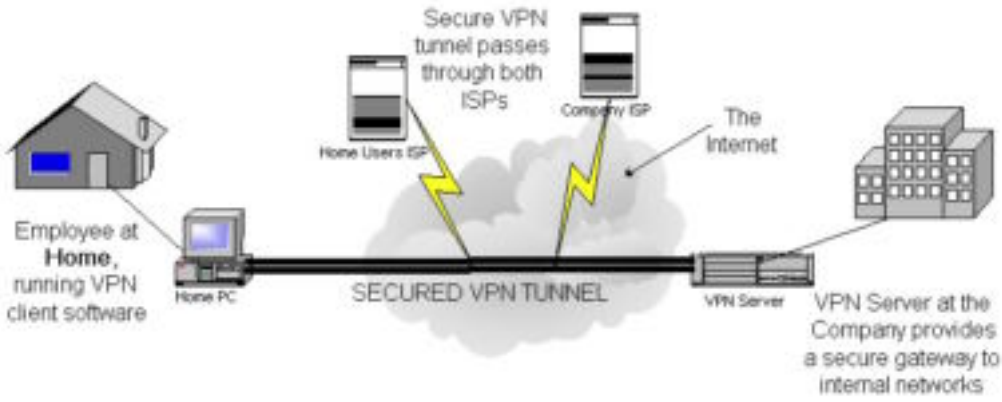
Given all of this, the new VPN options include many updated features and new security options that previous version of Windows did not offer. These feature are worth a detailed examination but should not be implemented hastily or without a full understanding of all the issues. This paper will provide an overview of Virtual Private Networks (VPNs). It will then provide a brief overview of the industry leading protocol IPSec and what its absence may mean for Windows 2000. Next, an evaluation of the two remote access VPN options in Windows 2000 will be covered.

Virtual Private Networking Overview (VPN)

Virtual Private Networks are secured, private networks created across unsecured, public network links usually to save the costs of dedicated, point-to-point connections. Point-to-point connections are inherently secure because, as they imply, there are usually only two connections on the network, one at each end point of the connection. There are no systems in between to eavesdrop or interfere with the data as it is passed over the connection. Many VPNs are created across the internet, allowing companies to leverage their existing internet connections to create secure channels for other business purposes

This can result in significant savings of cost that would have been needed for expensive leased lines (leased lines are commercial point-to-point links that can be purchased in a variety of sizes and types).

Figure 1: Typical Remote Access VPN



As you can see from the diagram above, creating a VPN provides a virtual point-to-point connection over unsecured connections. By encapsulating or wrapping the packets with a new header that provides routing, endpoint and other information and then encrypting the packets, they can be sent over the un-secure link with confidentiality and privacy. Even if some of the packets are intercepted along the way, they are indecipherable without the encryption keys needed to un-encrypt them. The two most common uses for VPNs today are for remote access, allowing company employees working away from the office to obtain secure remote access connections to the company and site-to-site, allowing branch or remote offices or networks to connect into main offices and networks. These two options often have very different configuration, security and implementation requirements. For this paper, I will focus solely on remote access VPNs and their security implications. With the ever-increasing availability and options of high-speed Internet access for home users, this is becoming a more and more important security consideration.

Minimal Requirements of Remote Access VPN Technology Today:

VPN connections minimally require the following in order to provide full security to the packets transmitted through them and maximum interoperability with other VPN equipment:

Encapsulation:
Support for standard and secure of encrypting the entire original packet, including the headers, and placing (encapsulating it) it within a new larger packet

Authentication:
Support for standard and secure methods to determine who the user and machine that is trying to establish the VPN connection are and to determine if that user and machine have appropriate permissions to establish the connection (minimally, most support machine

authentication only as user authentication requires integration with a Directory service or other authentication mechanism). This also include packet level authentication to verify that packets originate only on one of the VPN endpoints.

Data Encryption:
Support for standard and secure methods to encrypt the data for shipment across the virtual point-to-point connection

Additional Common Security Features Available in Remote Access VPN Technology Today:

The following features are also commonly sought to better integrate VPN technology into existing networks and to increase the level of security available: Most are commonly available in most products on the market today.

Standard Key Exchange:
Support for standard and secure methods of allowing endpoint VPN partners to exchange the security parameters (shared keys, etc) they need to create the VPN.

Extensibility of Supported Protocols
The ability of vendors to add new encryption and authentication algorithms as they are created. Since encryption algorithms are broken all the time, this provides the ability to keep the VPN strong regardless of the specific algorithm used.

Certificate Authority Support:
The ability to link into or to provide additional repositories of authentication data or certificates. This is an improved method of allowing machine authentication but it has some major implementation issues

Interoperability with Directories and Proprietary Databases:
This is support for RADIUS, TACACS(+), Microsoft Active Directory, Novell NDS, and other types of authentication and Token authentication such as RSA Security's SecureID.

Support for Network Address Translation:
Methods to allow VPN connectivity amongst one or more end points which is using Network Address Translation

Built in Client Controls:
These include the ability for the VPN administrator to lock down the client system, disable routing, disable split-tunneling, and otherwise remotely secure the remote VPN clients.

Centralized Management of VPN tunnels:
The ability to manage from a central console without multiple user databases, and multiple configurations, etc.

Address Management:
The ability to assign VPN clients addresses using standard methods such as Network Address Translation (NAT), static pools and DHCP

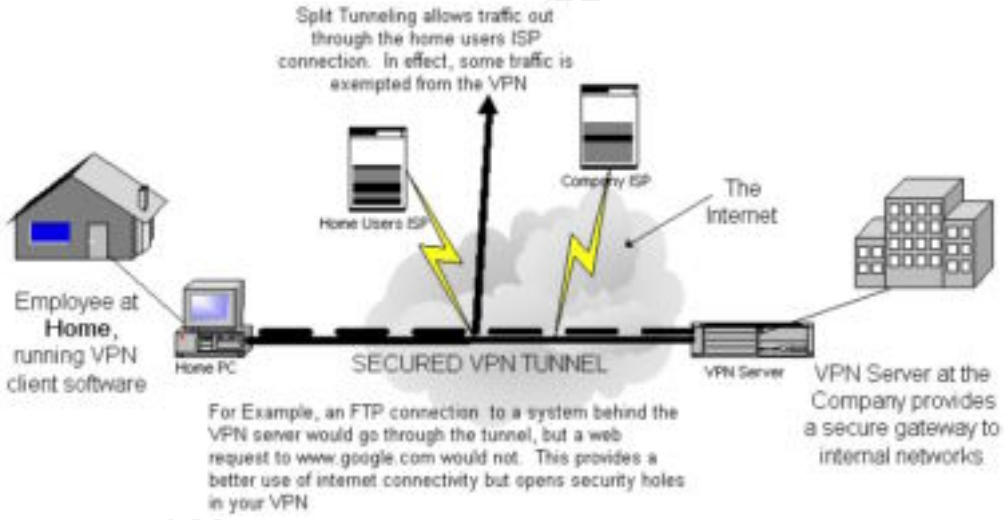
Security Issues Which Need to Be Considered When Providing Remote Access VPNs

Besides finding a solid VPN solution that hopefully encompasses the best of all the features and options above, setting up remote access VPNs will open your network to many new security concerns. These include, but are not limited to the following:

Split Tunneling:

Split tunneling is an option on the VPN server and / or the VPN client that determines which traffic should be sent through the encrypted tunnel. Only traffic destined for specific networks will be tunneled (sent through the VPN); all other traffic goes directly through the clients local ISP to its destination. Some VPN clients allow the user to decide whether or not to allow split tunneling! This opens a security hole into your VPN connection and limits control over outside influences. Spit tunneling appears as follows:

Figure 2: Split Tunneling



Remote VPN Clients Configured as Routers:
Remote VPN clients should be configured to control routing, otherwise an attacker may be able to take over the system and redirect traffic over the VPN connection.

Vulnerabilities of the Remote VPN client operating systems:
Administrators need to worry about securing remote VPN clients or they may be used to break into the network. Service packs and patches will need to be kept up to date.

Personal Firewalls and other Client Protections should be considered:
Because of the issues above and more, a person firewall or client profile should be enforced from the home network. This will limit the ability of the remote VPN client to bypass security measures and to protect always-on home connections from attackers.

Antivirus Software with up-to-date signatures should be Required on all VPN clients:
Otherwise you will be opening new pathways for viruses to enter the company network.

An important thing to remember with VPNs is that just because the tunnel itself is encrypted using a highly secure cipher, doesn't mean that your overall access method is secure. There are many, many factors involved in a secure end-to-end VPN solution, make sure you are aware of what these are before implementing any type of VPN.

Overview of the VPN capabilities Included in Windows 2000

In the end, Microsoft chose to ship Windows 2000 with several VPN tunneling protocols; Point-to-Point Tunneling Protocol (PPTP), layer Two Tunneling Protocol L2TP, and Internet Protocol Security IPSec. However, only PPTP and L2TP/IPSec, a combination of L2TP and IPSec, are available for use in creating remote access VPNs. Pure IPSec was included in Windows 2000 but only in tunnel mode, which can only be used with static IP addresses and between gateways. But the reason why Microsoft chose not to provide native (non-L2TP) support for IPsec remote access has to do with limitations of L2TP and IPsec. L2TP, a hybrid evolving from PPTP and Cisco's L2F, provides dial-up user authentication and IP address assignment for PPP sessions. However, L2TP doesn't offer any type of data encryption. On the other hand, IPSec standards offer strong encryption but do not support (non-certificate-based) user authentication or tunnel endpoint address assignment (such as using DHCP). "But Microsoft didn't stop with a recommendation, "**Microsoft eliminated support for native IPSec between client and gateway**" (Phifer, 2001, pg1).

Regardless of what Microsoft has done, IPSec is moving to become an international open standard and it is currently the leading choice for VPN deployment, so it will be covered along with the Microsoft VPN options. Besides, a clear understanding of IPSec is integral to understanding L2TP/IPSec. Rather than native IPSec support, Microsoft's Windows 2000 implementation of IPSec includes embedded Layer Two Transport Protocol (L2TP) for the following reason: According to Microsoft, "Embedding L2TP in IPSec provides the best standards-based solution for multi-vendor, interoperable client to –gateway VPN scenarios" (Microsoft, Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability, 2001 pg.2).
This is not necessarily a bad thing from a security point of view, but it is too bad that Microsoft again chose to stray from a leading standard. For VPN vendors working towards interoperability, this has caused them to have to do an about face and add last minute support for L2TP in their products. Many have also complained that L2TP adds

un-needed burden by adding 40-50 bytes of per-packet overhead to a VPN. L2TP/IPSec is Microsoft's recommended for all security minded remote access VPNs. This solution does offer many security improvements over Microsoft's legacy VPN option PPTP but it also brings some new issues. Finally, Point-to-Point Tunneling Protocol (PPTP) is Microsoft's legacy, backward-compatibility option for VPN. This solution has been around a long time and has suffered from numerous security issues and problems, not with the PPTP protocol itself, but always in the Microsoft implementation of this protocol. This solution may be appropriate in low security situations, that require Network Address Translation, or for VPNs that must support non-Windows 2000 clients. However, it should only be used as a last resort when all other solutions will not work.

A Detailed Look at IPSec and Comparisons to Microsofts Windows 2000 VPN Options

You can't help but look into these protocols with an eye for security issues, after all a VPN that doesn't provide security is no VPN at all. However, my definition of security here is quite broad as there are an awful lot of factors that play a role in overall security. For example, as we know, if a security solution is too difficult to use or too cumbersome to use then users will circumvent it anyway, destroying the benefits of using it in the first place. My discussions of each of the protocols will attempt to take an open approach considering all facets of security, from ease of use to strength of encryptions methods and everything in between.

IPSec, The Leader that Microsoft Left Out of its Remote Access VPNs

Overview:

Interestingly enough, Internet Protocol Security (IPSec) is according to Microsoft,

> "The long-term direction for secure networking"
> (Microsoft, Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability, 2001 pg.1).

For the rest of the world, it is the most standard method used to create VPNs today. Many recent and on-going studies and market analysis are showing time and time again that IPSec is currently the most heavily implemented VPN type. According to Lucent's recent State of VPN Survey 2000, nearly three quarters of the respondents to this survey have implemented or plan to implement IPSec VPNs (for more information please see: http://www.lucentnps.com/knowledge/surveys/00vpn/). IPSec was developed by the Internet Engineering Task Force (IETF) as a set of protocols to provide security to IP version 6, but also applies to IP version 4 (widely used today). One important thing to note about IPSec is that it only addresses security at the IP layers, or layer 3 of the OSI model. As such, it can be used to secure all the layers above the IP layer, but cannot be used to protect other protocols such as IPX or AppleTalk because these reside at lower layers of the OSI model (Layer 2).

Goals For IPSec:
(From RFC 2401)
"IPSec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols."

What IPSec Provides:
Internet Protocol (IP) does not inherently provide any protection to your transferred data. It does not provide authentication, or the ability to determine that the sender is who you think it is. IPSec attempts to add these security features to IP by adding the following:

Confidentiality
Encryption, so that only the intended recipients will be able to obtain the data

Integrity
Provides a guarantee that the data did not get changed during transmission.

Authenticity
The ability to determine, without a doubt, who sent the data

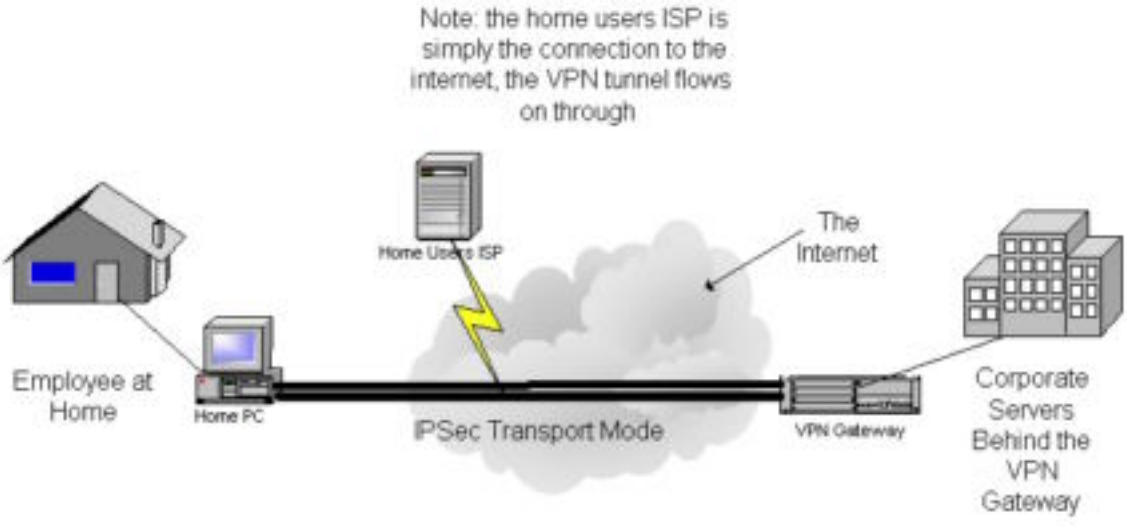
Replay protection
Provides methods to ensure that a transaction can only happen once unless authorization is given to repeat it.

Key Management
Standard methods for the sharing and maintenance of encryption keys between encryption partners

How IPSec Works

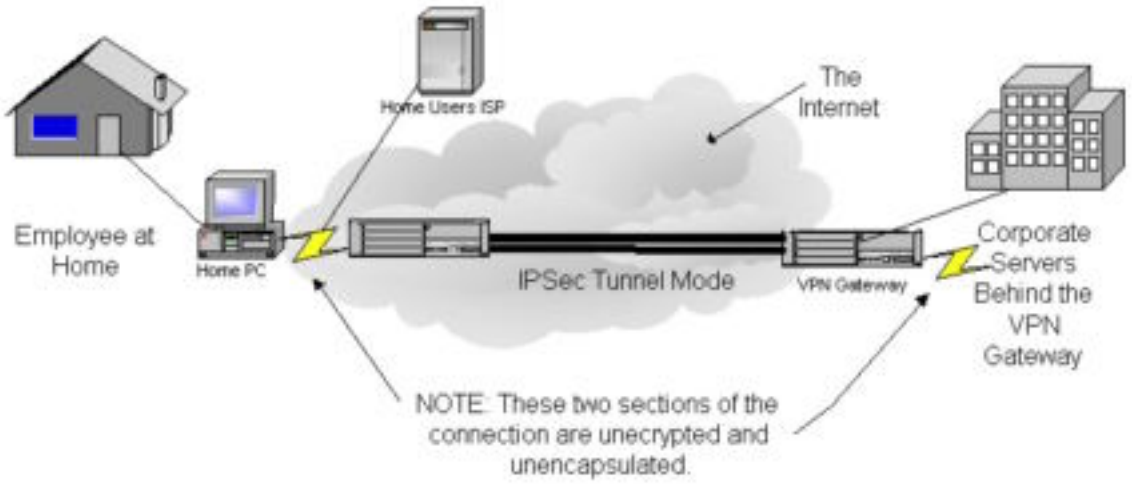
IPSec operates in two distinct modes. The first, transport mode, (or client to gateway) is the native mode for IPsec. As shown in Figure 3, it is the direct relaying of IPSec protected data from host to host. It is used in devices that incorporate IPSec into the way they stack TCP/IP data: for example a laptop outfitted with a VPN client. This is the mode of IPSec which Microsoft left out of Windows 2000. This mode provides end-to-end encryption and encapsulation and is the mode commonly used for remote access VPNs.

Figure 3: IPSec Transport Mode



The second method is tunnel mode (or gateway-to-gateway). In this mode, the end point doesn't have IPSec capabilities but simply transmits IP traffic onto the wire that is captured from the wire by a security device, or gateway. As shown in Figure 4 below, the gateway encapsulates the entire IP packet with IPSec encryption, including the original IP header. It then adds a new IP header to the data packet and sends it across the public network to a second gateway, where the information is decrypted and sent in its original form to the designated recipient. The data is in the clear before it reaches the first gateway and after it leaves the second gateway (in this situation these must be trusted networks). For this reason and others, tunnel mode is typically used to connect to networks together such as a branch office network to the headquarters of a company. This mode only supports router-to-router VPN connections today because the current standards don't specify a method for providing user authentication or address assignment for remote clients.

Figure 4: IPSec Tunnel Mode



IPSec Protocols:

Security Associations and Key Management
Before IPSec may operate in either of the above two modes, an IPSec Security Association must be established. This is done when the two hosts authenticate each other as well as negotiate an encryption method to use for the connection. The SAs are stored on each IPSec computer in a special database called the SPD. SAs are identified within the SPD by a Security Parameter Index (SPI) which is always a part of IPSec headers. The most common method used to create SAs is using the Internet Key Exchange protocol (IKE). IKE handles the creation of SAs and the generation of shared keys needed for the encryption of the VPN traffic between end points. IKE specifically uses the Diffie-Hellman (DH) key exchange protocol to securely generate and manage the encryption keys used to encrypt and decrypt data. IKE provides a secure channel for DH to create encryption keys.

AH and ESP
Besides the protocols used for key management, IPSec uses two protocols to provide traffic security, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides connectionless integrity, data origin authentication, and an optional anti-replay service. ESP may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay protection. These protocols may be applied alone or in combination with each other to provide a desired level of security. This is one of the ways in which IPSec allows the user (or system administrator) to control the granularity of security services offered. Normally, AH is used to provide integrity and authentication and the optional anti-replay services and ESP is used to provide data encryption.

AH- IP Protocol 51
AH provides authentication, integrity and anti-replay for the entire IP packet, this includes the IP header and the data carried in the packet. AH signs the entire packet to provide this level of security. It does not encrypt the data; it remains readable, but protected from modification. AH uses the HMAC algorithms to sign and authenticate the packet. HMAC is a mechanism for message authentication which uses cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function such as, MD5 or SHA-1, in combination with a shared secret key. The cryptographic strength of the HMAC depends on the properties of the underlying hash function. If MD5 is used it produces a 128-bit key and if SHA1 is used this results in a 160-bit key.
In addition, AH provides two way authentication which allows the client and the server to both verify each other's identity.

ESP- IP Protocol 50
ESP is used to provide confidentiality, data integrity, data source authentication and Protection from anti-replay attacks. Given all these options for ESP, its main function is to encrypt the entire original packet, including headers, and places it into a new, larger packet. The full set of options implemented depends on choices selected at the time of SA establishment and the mode which IPSec is operating in (tunnel or transport). Confidentiality may be selected independent of all other options. However, it is not possible to create an SA that does not provide for AH or ESP, this is illegal, as it does not provide for any VPN security at all. The authentication algorithms of ESP are the same as those used for AH. The data encryption algorithm employed is specified by the SA. All encryption algorithms used with ESP must operate in cipher block chaining mode (CBC). CBC requires that the amount of data to encrypt be a multiple of the block size of the cipher. ESP is designed for use with symmetric encryption algorithms. Two common choices for ESP encryption are Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Because IP packets may arrive out of order, each packet must carry any data required to allow the receiver to establish cryptographic synchronization for decryption.

Remote Access VPN Authentication Options:

- IPSec also makes use of Digital Certificates to provide a more robust way to authenticate users.
- It also allows for shared secrets, agreed to ahead of time and set on the server and client.

Benefits of IPSec

- IPSec gives IT managers flexibility in how VPN sessions are secured
- Extensibility- the ability to add new authentication and encryption algorithms as they become available
- Support for open, and widely tested encryption and authentication algorithms
- Support for Certificate Authorities
- Support for RADIUS, TACACS+ and Tokens

- Open international standard which is being developed in a very public environment
- Support for Public Key Cryptography and longer key lengths

Issues with IPSec

- Interoperability- the standard is so open that it is possible to have two VPN systems which implement the standard but do not interoperate completely
- No built-in authentication methods for users, default is machine authentication
- IP only, does not support multiple protocols such as IPX and AppleTalk
- ESP, by creating larger packets may go over the TCP/IP packet size limits causing fragmentation. This could affect throughput for applications

L2TP/ IPSec and PPTP: Comparing and Contrasting Microsoft's Windows 2000 VPN Options with IPSec

L2TP/IPSec, Improvements to IPSec with Strings…

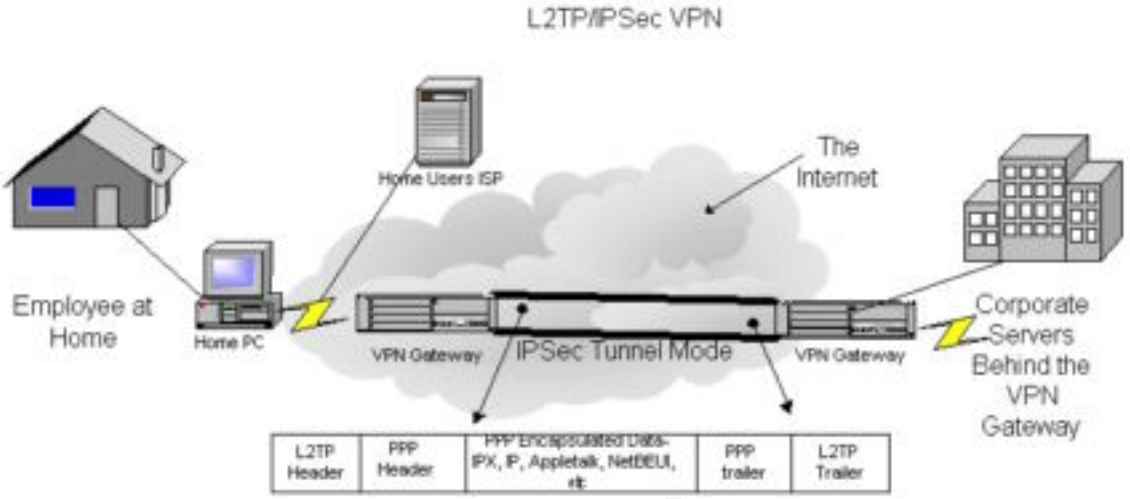
It is clear that Microsoft felt it needed to improve on IPSec when it released L2TP/IPSec support in Windows 2000, instead of supporting native IPSec and working to make changes to this standard. As per Microsoft, "For advanced security requirements, IPSec has emerged as a key technology. However, IPSec tunnel mode by itself does not support legacy authentication methods, tunnel IP address assignment and configuration, and multiple protocols—all critical requirements for remote access VPN" (Windows 2000 –Based Virtual Private Networking: Supporting VPN Interoperability). One major area of concern for Microsoft and other is the lack of for non-IP protocols in IPSec. These include: Novell's IPX and Apple's AppleTalk and, though rarely mentioned, Microsoft's netBEUI. Since L2TP operates as layer 2 of the OSI model, it can allow for multiple protocols which IPSec cannot. Also, Microsoft has expressed worry over authentication options using IPSec. Since IPSec only knows about IP addresses, it's built –in authentication methods to the machine level only, not the user level. Although IPSec has wide support for external authentication services, such as RADIUS, TACACS+, tokens and Certificates which can add user authentication, there is no direct support for Microsoft's Active Directory. Again, according to Microsoft, "By placing L2TP as payload within an IPSec packet, communications benefit from the standards-based encryption, integrity and replay protection of IPSec, while also benefiting from the user authentication, tunnel address assignment and configuration, and multi-protocol support of PPP-based tunneling" (Windows 2000 –Based Virtual Private Networking: Supporting VPN Interoperability). I don't disagree with what Microsoft has attempted, but issues related to L2TP/IPSec have also made this a less that perfect solution.

A Brief Overview of L2TP and What it Brings to L2TP/IPSec

L2TP has been defined by the PPP extensions working group of the IETF as a way to tunnel layer 2 data. Based on Layer two Forwarding 9L2F) and Point to Point Tunneling Protocol (PPTP), L2TP is used to setup tunnels across intervening networks. L2TP encapsulates Point-to-Point Protocol (PPP) frame, which can in turn encapsulate various other protocols including IP, IPX or NetBEUI. L2TP does not provide any security.

Since L2TP runs over IP, it is possible to use IPSec to secure the tunnel. See an example configuration below:

Figure 5: L2TP/IPSec VPN



The IPSec is used to provide encryption, integrity and replay protection to the L2TP/IPSec VPN. The methods used to do this are the same as those discussed for native IPSec. DES and 3DES encryption are supported, however you must have the Windows 2000 High Encryption Pack installed on all VPN endpoints in order to use 3DES encryption.

Authentication:
What IPSec doesn't provide in L2TP/IPSec is authentication. Authentication is provided by L2TP using the following Microsoft authentication options:

Password Authentication Protocol (PAP):
Legacy authentication protocol using plaintext (unencrypted) passwords and is the least sophisticated authentication protocol. Provides no data encryption.

Shiva Password Authentication Protocol (SPAP):
For Shiva clients connecting to Windows 2000 servers, or for Windows 2000 clients dialing into Shiva servers. Similar to PAP this authentication method provides no data encryption.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP):
Integrates encryption and hashing algorithms used on Windows networks. It uses a challenge- response mechanism with one-way encryption on the response. This protocol allows support for older Windows clients such as Windows 95/98 and NT.

Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP V2):
Repairs many of the well-known security issues in MS-CHAP and is also a mutual authentication protocol, which means that both the client and the server prove their identities.

Extensible Authentication Protocol (EAP):
The Extensible Authentication Protocol is an extension to the Point-to-Point protocol (PPP). EAP was developed in response to an increasing demand for remote access user authentication using add on security devices. EAP provides this support for additional authentication methods within PPP. Using EAP, support for the following add-on authentication schemes can be supported:

- Token cards
- One-time passwords
- Public key authentication using smart cards
- Certificates
- Others

Tunnel Address Assignment and configuration (DHCP):
In addition to providing the above authentication methods, L2TP also adds the ability for the VPN devices to dynamically provide IP addresses for tunnel partners using Dynamic Host Configuration Protocol (DHCP). DHCP is the desktop standard for IP addressing and allows pools of IP addresses to be configured ahead of time and handed out automatically as they are needed.

Multi-Protocol Support:
As has been stated before, because L2TP encapsulates PPP frames, which are capable of encapsulating multi-protocol traffic, L2TP provides a method to deliver IPX, AppleTalk and NetBEUI traffic across VPNs. This is necessary if your network hasn't been migrated to an IP only environment, or if you are unable to migrate because of legacy applications which will not function across TCP/IP.

Benefits to Using L2TP/IPSec over native IPSec for Remote Access VPNs:

- Multi-protocol Support (although this is less and less of an issue)
- Tunnel address assignment and configuration using DHCP
- Ability to authenticate directly to Active directory
- Relatively low initial cost involved (however, many hidden cost may exist)
- May allow for better integration into a Microsoft centric environment than native IPSec solutions

Security and Other Issues which Need to be Considered Before Using L2TP/IPSec over native IPSec for Remote Access VPNs:

- **High Encryption Pack is required for 128-bit encryption**
  DES has been cracked successfully many times, each time requiring less and less time to complete. Because of this VPN security minimum should be 128-bit

encryption. Adding the High Encryption pack to all systems will be difficult to administer and maintain

- **Encryption Keys are based on Passwords**
  In some configurations, VPN encryption keys are based on user passwords. If this is the case, even a 128-bit key is not secure; most passwords do not provide enough entropy (randomness) to produce strong encryption keys.

- **Client and Server Certificates are Required for authentication of L2TP over IPSec**
  Setting up a certificate server and maintaining and administering certificates to all your users is no small feat. Setting up VPNs can be difficult enough without this added burden. Plus most people won't be ready for certificates until they have converted to Active Directory and this is an enormous task. It is unfortunate that this is a prerequisite to L2TP/IPSec Remote Access VPNs.

- **Microsoft proprietary and /or weakly secured authentication schemes**
  PAP, SPAP, and MS-CHAP are all weak authentication protocols with numerous well-known vulnerabilities and security holes. Unless you can afford to add EAP add-on authentication methods, this leaves you with only MS-CHAP V2 as an authentication option, and it's not even an open standard. Also, by default, Windows 2000 will step down to lower authentication methods when necessary. For more information please see:
  http://www.windows.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_RASS_MSCHAPv2.htm

  http://windows2000experience.com/Articles/Index.cfm?ArticleID=135
  http://www.26thcentury.com/~buc/Info/Security/protocol/chap/conf.txt

- **Setting must be changed in the Registry or Windows 2000 systems will default to NTLM authentication which will in turn weaken VPN passwords**
  By default Windows 2000 system support compatibility with legacy windows versions by allowing NTLM, Microsoft's legacy authentication protocol from NT version 4. Since this password may be used to generate your VPN keys, this may leave you even more susceptible to password attacks.

- **Default VPN settings are not secure**
  As is the usual with Microsoft software, the default settings for authentication and encryption of Microsoft VPNs are not secure; they step down to weak and insecure algorithms on demand.

Point-to-Point Tunneling Protocol (PPTP): too many security problems in the Microsoft Implementation

PPTP Overview:
PPTP is not a standard, it was created by a consortium of vendors which included Ascend, 3Com and U.S. Robotics and Microsoft. PPTP is Microsoft's legacy VPN

protocol and was available before the advent of certificates and PKI in Windows 95/98 and NT. PPTP was eventually submitted to the Internet Engineering Task Force (IETF) to be considered as a standard. The IETF took PPTP and Cisco's Layer Two Forwarding protocol and combined them into L2TP which did become a standard. Because PPTP is one of the precursors to L2TP, the protocol works in much the same way as L2TP. PPTP is extensively deployed in Internet service-provider networks. ISPs have had PPTP support built into their networks from day one because many of the vendors in the consortium sold their products to mostly ISPs. Also, Microsoft bundled support for PPTP into the Windows client and server environments making it an even easier choice. But there have also been numerous security issues with PPTP and after researching this paper I don't feel that it is a viable VPN solution in today's security environment. For this reason, I am not going to cover PPTP except to point out Microsoft's official position on it and to point you to more information about the numerous security problems with this protocol. Finally, I will leave you with information from a recent article talking about PPTP.

Microsoft's Current Position on PPTP:

Microsoft's VPN Directions

"Note For remote access, Microsoft strongly recommends customers deploy only L2TP/IPSec due to the authentication security vulnerabilities and non-standard implementations of IPSec tunnel mode. Microsoft also recommends L2TP/IPSec for multi-protocol, multi-cast gateway-to-gateway configurations

Microsoft's customers, the press, and analysts have told Microsoft that they prefer if Microsoft creates the single standard VPN client for Windows because it allows for easier deployment, better Windows integration, and better reliability.

Microsoft is supporting L2TP/IPSec as its only native remote access VPN protocol based on IPSec because it remains the only existing interoperable standard that addresses real customer deployment issues. In addition, Microsoft continues to support PPTP for both remote access VPN scenarios and site-to-site scenarios—in order to meet special-needs situations that can not be addressed with any IPSec-based solution." (Microsoft, Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability, 2001 pg.2)

More Information on PPTP Security Issues:

http://ciac.llnl.gov/ciac/bulletins/i-087.shtml
http://www.counterpane.com/pptp-pressrel.html
http://www.counterpane.com/pptp-faq.html
http://www.counterpane.com/pptp.html
http://www.cticomm.com/pptpfinal.htm
http://www.cs.dal.ca/~little/Courses/4171/FinalProject4171.htm
And many more, just do some searching….

Article: Windows 2000's VPN-Related Security Issues: ISP Planet
http://www.isp-planet.com/technology/vpn_windows2000a.html

> **"If you use PPTP** Finally, any ISP that uses PPTP in a remote access VPN service should start working on a transition plan. Vendors like IndusRiver and Nortel have verified interoperability with Windows 2000 PPTP; upward compatibility issues appear to be minimal. Microsoft's official position: 'PPTP provides simple-to-use, lower-cost VPN security' for customers who "do not require the sophistication of IPSec, who do not want to deploy PKI, or who require a NAT-capable VPN protocol." But PPTP is considered weak by many security experts. Industry advances like embedding PKI and IPSec in Windows 2000 will eventually bring down the cost and complexity of IPSec deployment. Expect to migrate PPTP users to L2TP/IPsec, and you won't be caught by surprise when users demand an upgrade or Microsoft finally pulls the plug on PPTP" (Phifer, 2001, pg1).

Conclusions, What does it all Mean for Remote Access VPNs?

Ultimately, the best standard should win out and I believe that standard will be IPSec. IPSec is the most open of the standards available for remote access VPNS and it is also the most flexible. It has been developed over a long period of time with complete public scrutiny from the beginning. It also supports algorithms, which have been created in the same ways. IPSec is not without its issues and it has a way to go before it is fully developed and easy to integrate. However, it is the best solution available today for creating secure VPNs. As for Microsoft's new VPN options, there are many strong reasons that a company with a mostly Microsoft Windows 2000 network will want to consider L2TP/IPSec. Price alone should be a very large driving factor. But as I have stated before, Microsoft has added so many new feature to Windows 2000 that I believe corporations will end up taking much longer than they planned for implementation. Since the VPN and other features are tightly tied in with Active Directory and other Windows 2000 features, this could force companies to look elsewhere for VPN solutions. Overall, L2TP/IPSec is probably the second best option for remote access VPNs available today, but it shouldn't be considered without a thorough understanding of the issues it presents. The new security features are better than any which Microsoft has provided before, and much better than PPTP. Yet, they open new holes unless they are properly configured and maintained.

Bibliography:

Fraser, Moye, SANS Institute –Information Reading Room (2001). Understanding Virtual Private Networks (VPN). URL http://www.sansa.org/infosecFAQ/encryption/understanding_VPN.htm

Ciolek, Gregory J., SANS Institute –Information Reading Room (2001). Virtual Private Network (VPN) Security. URL http://www.sans.org/infosecFAQ/encryption/VPN_sec.htm

Rogers, Timothy J., SANS Institute –Information Reading Room (2001). IP Security in Windows 2000: Step-by-Step. URL http://www.sans.org/infosecFAQ/win2000/ipsec_w2k.htm

RFC 2401: IETF. Security Architecture for Internet Protocol. URL http://sunsite.dk/RFC/rfc/rfc2401.html

RFC 2402: IETF. IP Authentication Header (AH). URL http://andrew2.andrew.cmu.edu/rfc/rfc2402.html

RFC 2406: IETF. IP Encapsulating Security Payload (ESP). URL http://sunsite.dk/RFC/rfc/rfc2406.html

RFC 2637: IETF. Point-to-Point Tunneling Protocol (PPTP). URL http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2637.html

RFC 2661: IETF. Layer Two Tunneling Protocol "L2TP". URL http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2661.html

Phifer, Lisa, ISP Planet. Windows 2000's VPN-Related Security Issues. URL http://www.isp-planet.com/technology/vpn_windows2000a.html

Salamone, Salvator, Internet Week Online (1999). PPTP is the Tunnel Most Traveled. URL http://www.internetwk.com/VPN/vpnsupp062199-4.htm

Salamone, Salvator, Internet Week Online (1999). IPSec the Flexible Protocol. URL http://www.internetwk.com/VPN/vpnsupp062199-5.htm

Microsoft, Microsoft Tech Net. (2001). Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability. URL http://www.microsoft.com/technet/win2000/vpninter.asp

FirstVPN Enterprise Networks. (2000). Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources. URL http://www.firstvpn.com/research/papers6.html

Doraswamy, Naganand and Harkins, Dan, Prentice Hall (1999). IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks.