Operating System

Microsoft Privacy Protected Network Access:
Virtual Private Networking and Intranet Security

White Paper

Abstract

The Microsoft® Windows® operating system includes technology to secure communications over private and public networks. Current products from Microsoft provide tools to provide security services at the link and transport layers, as well as providing application-layer security for electronic mail. Link layer security encrypts data in transit within remote access sessions as well as within branch network connections. Transport layer security permits protection of TCP-based protocols, including World Wide Web sessions. Windows 2000 will, in addition, provide end-to-end network layer security services through Internet Protocol (IP) Security, or IPSec, which permits security services to be applied on internal networks.

This paper focuses on link layer and end-to-end security. It explains the Microsoft commitment to support Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IPSec protocol to address diverse customer requirements. The paper also details Microsoft plans for implementing these protocols on the Windows operating systems.

CONTENTS

INTRODUCTION

Network security is increasing in importance for companies of all sizes. Whether to protect information in transit in remote access sessions, branch network connections, or internal networks, solutions for this form of security are essential. In general, security is not a single product or technology but an integration of several technologies combined with management policy that provides protection balanced with acceptable risks. Microsoft takes security seriously and is working on a number of initiatives to provide customers with the technology and tools needed to easily define and manage security policy.

Security services include confidentiality, integrity protection, authentication, authorization, and replay protection. Among these tools are network encryption services that help minimize risks associated with transmitting sensitive information over public and privately managed networks. Microsoft also takes total cost of ownership seriously and is committed to providing standards based solutions that maximize communications interoperability and flexibility using the Windows platform.

There are three major models for securing the network and Microsoft supports each of these:

- Today, many applications are hosted for access across public and privately managed networks, secured through *transport layer security* technologies such as HTTPS, SOCKS, or SSL. Transport layer security as provided by SSL/TLS means that TCP-based applications are written specifically to use these security services. Microsoft supports SSL/TLS extensively across its products. However, SSL/TLS applications are not well suited to centralized management because these services are frequently applied on a page-by-page basis. SOCKS is an authenticated firewall traversal protocol that provides for extensible authentication, as well as granular authorization for both incoming and outgoing sessions. SOCKS V, which is not supported by Microsoft, applies both to TCP and UDP-based protocols, and is amenable to centralized management. As a result, SSL/TLS, and SOCKS technologies are complementary and can be used together to provide transport layer security within virtual private networks and extranets.
- Many companies use *private or trusted network infrastructures* including internal and outsourced cable-plants and wide area networks, which offer a level of privacy by virtue of physical security. Alone, these networks do not protect against inadvertent or intentional viewing of information as it passes over a network. With most security breaches occurring within a company network, additional technology is required to protect information from theft and attack.
- *End-to-end network security* consists of security techniques and protocols that transparently secure communications requiring application awareness. Careful network design and configuration is required to achieve this security. These tools are generally managed through administrative policy so that communications are safely protected as they travel across a network, without the knowledge or involvement of applications or end users.

All three models have been discussed in the industry under the broad category of *Virtual Private Networking* (VPN). While it is true that each model provides some level of private networking, this broad definition is a bit confusing. As such, Microsoft has adopted a more restricted definition of the term, and uses "VPN" to refer to providing security across a public or untrusted network infrastructure. This includes:

- Secure remote access from client-to-gateway, either through Internet connections or within private or outsourced networks
- Secure gateway-to-gateway connections, across the Internet or across private or outsourced networks.

Additionally, Microsoft is leading the industry with the first operating system–integrated, solution for securing end-to-end communications within a private network. Windows 2000 integrates IPSec with the Active Directory™ directory service to deliver central control of policy based security administration.

This paper discusses the Microsoft direction for both the VPN and end-to-end models for secure networking. It describes the key differences between the leading network protocols, discusses the Microsoft position relative to these protocols, and explains how Microsoft is supporting these protocols in its operating systems.

Over the past few years, a number of protocols have emerged that are categorized as VPN protocols and that encrypt communications. These include:

- *Internet Protocol Security* (IPSec)—an architecture, protocol, and related Internet Key Exchange (IKE) protocol, which are described by IETF RFCs 2401-2409.
- *Layer 2 Forwarding* (L2F)—created by Cisco Systems.
- *Layer 2 Tunneling Protocol* (L2TP)—a combination of PPTP and L2F, which evolved through the IETF standards process.
- *Point-to-Point Tunneling Protocol* (PPTP)—Created by the PPTP Industry Forum (US Robotics(now 3Com), 3Com/Primary Access, Ascend, Microsoft, and ECI Telematics).

While IPSec, L2TP, and PPTP are viewed by many as competing technologies, these protocols offer different capabilities that are appropriate for different uses. To understand this, it is useful to consider the design goals and technical differences of the protocols.

IPSec Design Goals and Overview

IPSec provides integrity protection, authentication, and (optional) privacy and replay protection services for IP traffic. IPSec packets are of two types:

- IP protocol 50 called the *Encapsulating Security Payload* (ESP) format, which provides privacy, authenticity, and integrity.
- IP protocol 51 called the *Authentication Header* (AH) format, which only provides integrity and authenticity for packets, but not privacy

IPSec can be used in two modes; *transport mode* which secures an existing IP packet from source to destination, and *tunnel mode* which puts an existing IP packet inside a new IP packet that is sent to a tunnel end point in the IPSec format. Both transport and tunnel mode can be encapsulated in ESP or AH headers.

IPSec transport mode was designed to provide security for IP traffic end-to-end between two communicating systems, for example to secure a TCP connection or a UDP datagram. IPSec tunnel mode was designed primarily for network midpoints, routers, or gateways, to secure other IP traffic inside an IPSec tunnel that connects one private IP network to another private IP network over a public or untrusted IP network (for example, the Internet). In both cases, a complex security negotiation is performed between the two computers through the Internet Key Exchange (IKE), normally using PKI certificates for mutual authentication.

The IETF RFC IPSec tunnel protocol specifications did not include mechanisms suitable for remote access VPN clients. Omitted features include *user* authentication options or client IP address configuration. To use IPSec tunnel mode for remote access, some vendors chose to extend the protocol in proprietary ways to solve these issues. While a few of these extensions are documented as Internet drafts, they lack standards status and are not generally interoperable. As a result, customers must seriously consider whether such implementations offer suitable

multi-vendor interoperability.

L2TP Design Goals and Overview

L2TP is a mature IETF standards track protocol that has been widely implemented. L2TP encapsulates Point-to-Point Protocol (PPP) frames to be sent over IP, X.25, frame relay, or asynchronous transfer mode (ATM) networks. When configured to use IP as its transport, L2TP can be used as a VPN tunneling protocol over the Internet. L2TP over IP uses UDP port 1701 and includes a series of L2TP *control* messages for tunnel maintenance. L2TP also uses UDP to send L2TP-encapsulated PPP frames as the tunneled *data*. The encapsulated PPP frames can be encrypted or compressed. When L2TP tunnels appear as IP packets, they take advantage of standard IPSec security using IPSec transport mode for strong integrity, replay, authenticity, and privacy protection. L2TP was specifically designed for client connections to network access servers, as well as for gateway-to-gateway connections. Through its use of PPP, L2TP gains multi-protocol support for protocols such as IPX and Appletalk. PPP also provides a wide range of user authentication options, including CHAP, MS-CHAP, MS-CHAPv2 and Extensible Authentication Protocol (EAP) that supports token card and smart card authentication mechanisms. L2TP/IPSec therefore provides well-defined and interoperable tunneling, with the strong and interoperable security of IPSec. It is a good solution for secure remote access and secure gateway-to-gateway connections.

PPTP Design Goals and Overview

PPTP was designed to provide authenticated and encrypted communications between a client and a gateway or between two gateways—without requiring a public key infrastructure—by using a user ID and password. It was first delivered in 1996, two years before the availability of IPSec and L2TP. The design goal was simplicity, multiprotocol support, and ability to traverse a broad range of IP networks. The Point-to-Point Tunneling Protocol (PPTP) uses a TCP connection for tunnel maintenance and Generic Routing Encapsulation (GRE) encapsulated PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted and/or compressed. The use of PPP provides the ability to negotiate authentication, encryption, and IP address assignment services.

Table 1 summarizes some of the key technical differences between these three security protocols.

Table 1. Network Security Protocol Differences

Feature	Description	PPTP/ PPP	L2TP/ PPP	L2TP/ IPSec	IPSec Xport	IPSec Tunnel
User Authentication	Can authenticate the user that is initiating the communications.	Yes	Yes	Yes	WIP[1]	WIP
Machine Authentication	Authenticates the machines involved in the communications.	Yes[2]	Yes	Yes	Yes	Yes
NAT Capable	Can pass through Network Address Translators to hide one or both end-points of the communications.	Yes	Yes	No	No	No
Multiprotocol Support	Defines a standard method for carrying IP and non-IP traffic.	Yes	Yes	Yes	No	WIP
Dynamic Tunnel IP Address Assignment	Defines a standard way to negotiate an IP address for the tunneled part of the communications. Important so that returned packets are routed back through the same session rather than through a non-tunneled and unsecured path and to eliminate static, manual end-system configuration.	Yes	Yes	Yes	N/A	WIP
Encryption	Can encrypt traffic it carries.	Yes	Yes	Yes	Yes	Yes
Uses PKI	Can use PKI to implement encryption and/or authentication.	Yes	Yes	Yes	Yes	Yes
Packet Authenticity	Provides an authenticity method to ensure packet content is not changed in transit.	No	No	Yes	Yes	Yes
Multicast support	Can carry IP multicast traffic in addition to IP unicast traffic.	Yes	Yes	Yes	No	Yes

[1] Support is not yet provided; however, there is work in progress (WIP) by the IETF IPSec working group.

[2] When used as a client VPN connection, it authenticates the user, not the computer. When used as a gateway-to-gateway connection, the computer is assigned a user ID and is authenticated.

IPSec

By design, IPSec transport mode is ideal for delivering end-to-end authenticity and encryption within corporate networks. Microsoft is working closely within the IETF and with leading networking vendors to ensure interoperability within the specified IPSec standards that support this scenario.

In most client-to-gateway VPN situations, user authentication and internal address configuration are critical aspects of security and management. Multicast support and defined methods for carrying multi-protocol traffic are also essential, particularly in gateway-to-gateway scenarios. To address this, many vendors have implemented proprietary and/or weakly adopted extensions to IPSec that inhibit multi-vendor interoperability. The IETF IPSec working group is currently exploring ways to address these issues, while minimizing packet overhead and leveraging the IETF IP framework. However, because IPSec tunnel mode does not have defined standard methods for extensible user-based authentication and address assignment for accomplishing these aspects yet, Microsoft has concluded that *by itself*, IPSec tunnel mode is unsuited to most client-to-gateway VPN situations. For gateway-to-gateway VPN scenarios, IPSec tunnel mode is fine—although interoperability problems for specific networking configurations may arise due to the varying number of IKE options supported, as well as the level of interoperability testing provided in products today.

L2TP/IPSec

L2TP is a well-defined, interoperable protocol that addresses the current shortcomings of IPSec-only client-to-gateway and gateway-to-gateway scenarios (user authentication, tunnel IP address assignment, and multiprotocol support). L2TP has broad vendor support, particularly among the largest network access equipment providers, and has verified interoperability. By placing L2TP as payload within an IPSec packet, communications benefit from the standards-based encryption and authenticity of IPSec, while also receiving a highly interoperable way to accomplish user authentication, tunnel address assignment, multiprotocol support, and multicast support using PPP. This combination is commonly referred to as L2TP/IPSec. Lacking a better pure IPSec standards solution, Microsoft believes that L2TP/IPSec provides the best standards based solution for multi-vendor, interoperable client-to-gateway VPN scenarios. Microsoft is working closely with key networking vendors including Cisco, 3Com, Lucent and IBM, to support this important combination.

It should be noted that due to incompatibilities between the IKE protocol and Network Address Translation, it is not possible to use L2TP/IPsec or IPSec tunnel mode through a Network Address Translator while taking advantage of automated key exchange.

Recently proposed work for L2TP specifies a header compression method for L2TP/IPSec. This work is important because it helps reduce protocol overhead dramatically while retaining the benefits of the rest of L2TP. Microsoft believes this

header compression work represents an important direction for L2TP and supports the progression of this capability along the standards track. Microsoft also supports the continued development of standards-based, interoperable, and well-integrated solutions for IPSec tunnel mode in client-gateway applications. In particular, Microsoft believes that such solutions must not compromise the integrity of the IKE protocol by introducing excessive complexity. Additionally, IPSec Remote Access (IPSRA) solutions must be well integrated with existing network infrastructure, such as DHCP, and with existing IETF standards for extensible authentication, such as EAP and GSS_API.

PPTP

PPTP is broadly used today in both client-to-gateway and gateway-to-gateway scenarios. With mutual client/server authentication based on users' passwords and encryption keys seeded by the authentication process, PPTP is easy and inexpensive to set up and simple to administer. By virtue of its design, PPTP can also be passed through Network Address Translators (NAT). This NAT capability eliminates the requirement that each PPTP end-point have a registered IP address when used across the Internet.

While L2TP/IPSec is an excellent solution for multi-vendor interoperability in both client-to-gateway and gateway-to-gateway scenarios, its usage of IPSec does require a PKI to be scalable. Also, because of incompatibilities between IKE And NAT, neither L2TP/IPSec, nor IPSec pure tunnel mode, nor IPSec transport can pass through typical NATs. Microsoft believes that PPTP will remain an important protocol choice for customers who do not require the sophistication of IPSec-based communications, who do not want to deploy a PKI, or who require a NAT-capable VPN protocol. As such, Microsoft is committed to on-going support and advancement of PPTP.

IPSec

The Microsoft Windows 2000 operating system simplifies deployment and management of network security with Windows IP Security, a robust implementation of IPSec. IPSec protocol is an integral part of the TCP/IP protocol stack. Microsoft and Cisco Systems, Inc., have jointly developed IPSec and related services in Windows 2000. Interoperability is tested with Cisco and a number of other vendors for each of the examples below.

Using IPSec, you can provide privacy, integrity and authenticity for network traffic in the following situations.

- End-to-end security for IP unicast traffic, from client-to-server, server-to-server and client-to-client using IPSec transport mode
- Remote access VPN client and gateway functions using L2TP secured by IPSec transport mode.
- Site-to-Site VPN connections, across outsourced private WAN or Internet-based connections using L2TP/IPSec or IPSec tunnel mode.

Windows IP Security builds upon the IETF IPSec architecture by integrating with Windows 2000 domains and the Active Directory service. Active Directory delivers policy-based, directory-enabled networking. IPSec policy is assigned and distributed to Windows 2000 domain members through Windows 2000 Group Policy. Local policy configuration is provided, so membership in a domain is not required.

An automatic security negotiation and key management service is also provided using the IETF-defined Internet Key Exchange (IKE) protocol, RFC 2409. The implementation of IKE provides three authentication methods to establish trust between computers:

- ***Kerberos v5.0 authentication*** is provided by the Windows 2000 domain that serves as a Kerberos version 5.0 Key Distribution Center (KDC). This provides easy deployment of secure communications between Windows 2000 computers that are members in a domain or across trusted domains. IKE only uses the authentication properties of Kerberos, as documented in draft-ietf-ipsec-isakmp-gss-auth-02.txt. Key generation for IPSec security associations is done using IKE RFC2409 methods.
- ***Public/Private key signatures using certificates*** is compatible with several certificate systems, including Microsoft, Entrust, Verisign, and Netscape. This is part of RFC 2409.
- ***Passwords***, termed *pre-shared authentication keys*, are used strictly for establishing trust between computers. This is part of RFC 2409.

Once configured with an IPSec policy, peer computers negotiate using IKE to establish a main security association for all traffic between the two computers. This involves authenticating using one of the methods above and generating a shared *master key*. The systems then use IKE to negotiate another security association for the application traffic they are trying to protect at the moment. This involves generating shared *session keys*. Only the two computers know both sets of keys.

The data exchanged using the security association is very well-protected against modification or interpretation by attackers who may be in the network. The keys are automatically refreshed according to IPSec policy settings to provide constant protection according to the administrator defined policy.

For customers familiar with technical details of IPSec, Windows 2000 supports DES (56-bit key strength) and 3DES (168-bit key strength) encryption algorithms, and SHA-1 and MD5 integrity algorithms. These algorithms are supported in all combinations in the ESP format. Because the AH format provides only integrity and authenticity, only MD5 and SHA-1 are used.

L2TP

Windows 2000 includes L2TP support when used with IPSec for client-to-gateway and gateway-to-gateway configurations. In these configurations, all traffic from the client to a gateway, and all traffic between two gateways is encrypted. This implementation has been tested with a variety of other vendor implementations of L2TP/IPSec.

PPTP

Windows 2000 includes PPTP support for client-to-gateway and gateway-to-gateway configurations. This implementation is consistent with the PPTP services available for the Microsoft Windows NT® Server, Windows NT Workstation, Windows 98, and Windows 95 operating systems. Customers can take advantage of their existing investment in Windows operating system–based platforms by using PPTP. Windows 2000-based systems can interoperate with Windows NT–based PPTP servers, and today's Windows–based systems interoperate with Windows 2000–based PPTP servers. In addition to password-based authentication, Windows 2000 PPTP can support public key authentication through the Extensible Authentication Protocol (EAP).

Remote Access Policy Management

Another dimension of security policy management that goes beyond encryption policy is *access policy*. In client-to-gateway and gateway-to-gateway situations, Windows 2000 provides a rich set of administrative policies that can be implemented to control user access through direct-dial, PPTP, and L2TP/IPSec connections. These access policies allow administrators to grant or deny access based upon a combination of user ID, time-of-day, protocol port, encryption level, and more. While available natively within a Windows 2000 Active Directory environment, these access policies can also be enforced on non-Windows 2000 environments through the use of RADIUS. For example, an existing Windows NT–based PPTP server can be configured to use a Windows 2000 Server to authenticate users through RADIUS. When used in this way, the Windows 2000 Server can be configured to enforce access policies and apply them to the Windows NT–based PPTP server. This is an example of how Windows 2000 can

simplify and strengthen central administration during a transition to Windows 2000, and demonstrates one of the many benefits of using Windows 2000 for authentication in heterogeneous environments.

Client Management

As previously mentioned for IPSec, Active Directory is used to define and control IPSec policy. Installation of the PPTP, L2TP, and IPSec protocols is inherent in the installation of Windows 2000. Client configuration of these protocols for client-to-gateway scenarios can be accomplished in two ways:

- On end systems, a New Connections wizard prompts the user through a simple set of screens to set configure the connection.
- In larger scale installations, the Connection Manager Administration Kit and Connection Point Services can be used together to deliver a customized remote access direct-dial and VPN client to corporate systems.

With these tools the administrator can provide the client with a specially configured profile that:

- Brands the dialer consistent with corporate remote access programs.
- Integrates customize help files and corporate remote access use licenses.
- Integrates applications and other tools for automatic launch at various stages of the connection process.
- Administers a central phonebook of remote access numbers.
- Contracts with Internet Service Providers (ISPs) for management of point-of-presence (POP) phone numbers.
- Configures clients to automatically update, and collates phonebooks from the ISP and the corporate phonebook servers.

The resulting profile can be distributed centrally to clients through Microsoft System Management Services, Web downloads, file transfers, e-mail, floppy disks, or CDs. This lets administrators centrally manage clients while users get a single interface that:

- Connects, regardless of type of protocol or connection (direct dial or VPN protocol).
- Hides the complexity of the connection process (single click access).
- Provides single sign-on using company user IDs (no separate ISP account required).

Based on customer feedback, Microsoft considers this to be one of the most important components for deploying VPN services.

PLATFORM SUPPORT FOR SECURE NETWORK COMMUNICATIONS

Because IPSec and its related policy management, Kerberos authentication, PKI support, and hardware acceleration are integrated tightly into the Windows 2000 operating system and the Active Directory directory service, Windows-based desktop and server systems must be upgraded to Windows 2000 to take advantage of IPSec for end-to-end scenarios. Microsoft has no plans to deliver IPSec-only based services for the Windows NT, Windows 98, Windows 95, or Windows 3.x operating systems. Windows CE is under investigation at this time.

L2TP/IPSec support is being delivered first in Windows 2000 Server and Windows 2000 Professional. Microsoft has no work planned for L2TP/IPSec on Windows NT or Windows 95 or Windows 3.x. Microsoft is working with customers to understand the specific requirements with regard to L2TP/IPSec and IPSec tunnel mode on Windows 98 and Windows CE. However, Microsoft has no work planned for L2TP/IPSec or IPSec tunnel mode on Windows 3.x.

In addition to being an integral part of Windows 2000, PPTP continues to be supported on Windows NT, Windows 98, and Windows 95 operating systems. PPTP support for Windows CE is under investigation at this time. Microsoft intends to continue its leadership in the development of PPTP to address key customer scenarios that are unmet by IPSec and L2TP/IPSec standards.

FOR MORE INFORMATION

For the latest information on Windows 2000, visit our World Wide Web site at http://www.microsoft.com/windows/. For the latest information on Windows NT, visit our Web site at http://www.microsoft.com/ntserver and the Windows NT Server Forum on MSN™, and The Microsoft Network online service (GO WORD: MSNTS).