



*Operating System*

## Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability

---

### **Abstract**

Multi-vendor interoperability for virtual private networking (VPN) is essential in today's networking environment due to the nature of business acquisitions, the need to extend corporate networks to contractors and partners, and the diverse equipment within company networks. The Microsoft® Windows® operating system has integrated VPN technology that helps provide secure, low-cost remote access and branch office connectivity over the Internet. Windows 2000 virtual private networking has been designed to interoperate with VPN software and devices that support Internet-industry standards for secure remote access.

By supporting industry standards, Microsoft delivers a solution that will work with other standard-compliant devices or software, helping to lower the cost and complexity of supporting proprietary solutions. Customers who plan to deploy VPNs for remote access should seriously evaluate long-term interoperability issues and invest in standards-based solutions. This paper explains Microsoft's commitment to support VPN interoperability through standards such as Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol with IPSec protocol (L2TP/IPSec).

© 2000 Microsoft Corporation. All rights reserved.

*The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*Microsoft, Windows, the Windows logo and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.*

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA*

*01/00*

---

## CONTENTS

<b>CONTENTS .....</b>	<b>1</b>
<b>MICROSOFT VPN INTEROPERABILITY .....</b>	<b>2</b>
Executive Summary	2
Introduction	3
Remote Access VPN Requirements and IPSec-based Implementations	4
User Authentication	4
Address Assignment	5
PPTP: An Alternative and/or Complement to IPSec-Based VPN	6
<b>MICROSOFT'S VPN DIRECTIONS .....</b>	<b>7</b>
What Customers Should Do	7
Recommendations to VPN Vendors	7
<b>FOR MORE INFORMATION.....</b>	<b>8</b>

---

## MICROSOFT VPN INTEROPERABILITY

### Executive Summary

Microsoft® Windows® 2000-based virtual private networking (VPN) supports Internet-industry standards technology to provide customers with an open interoperable VPN solution. Microsoft is committed to IETF (Internet Engineering Task Force) standards-track-based technology such as Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP) as well as Point-to-Point Tunneling Protocol (PPTP)—a proven published informational RFC that is supported in multiple interoperable third-party products.

- PPTP provides simple-to-use, lower-cost VPN security. Unlike IPSec technology, PPTP is compatible with Network Address Translators (NAT) and supports both multi-protocol and multicast environments. It also combines standard user password authentication with strong encryption without requiring the complexity and expense of public key infrastructure (PKI).
- IPSec provides advanced security for VPN but was not designed to address critical remote access requirements such as User Authentication and Address Assignment. In addition, it does not support multi-protocol or multicast (including some routing protocols). It is applicable primarily to IP-only, unicast-only situations.
- L2TP in combination with IPSec is the **only** standards-track technology that addresses these remote access VPN requirements while leveraging IPSec for encryption. L2TP currently retains the same IETF standards-track status as IPSec.
- Third-party IPSec-only implementations that do not use L2TP with IPSec are using non-standard proprietary technologies that can lock customers into closed solutions.

Lacking a better pure IPSec standards solution, Microsoft believes that L2TP with IPSec provides the best standards-based solution for multi-vendor, interoperable client-to-gateway VPN scenarios.

Customers should prioritize VPN solutions that are based on interoperable standards and which support user-based authentication, authorization and accounting. If proprietary implementations of IPSec Tunnel Mode are being considered, carefully evaluate the near-term availability of solutions based on L2TP/IPSec to support interoperability. Customers should also consider how their L2TP/IPSec solution might be complemented by PPTP-based solutions.

Microsoft encourages VPN gateway vendors to provide support for L2TP/IPSec for remote access VPN and as an option to complement IPSec tunnel mode for gateway-to-gateway situations, in which multi-protocol and multicast considerations come into play. By supporting L2TP/IPSec and/or PPTP, Windows 2000 Professional can connect directly to the vendor's gateway and other VPN solutions without customers having to change client-side code.

---

## Introduction

Multi-vendor interoperability for virtual private networking (VPN) is essential in today's networking environment due to the nature of business acquisitions, the need to extend corporate networks to contractors and partners, and the diverse equipment within company networks. To ensure customers have an open solution, Microsoft Windows 2000-based VPN technology is based on Industry standards.

By supporting IETF industry standards, Microsoft delivers a VPN solution that will work with other standard-compliant devices or software systems, helping to lower the cost and complexity of supporting proprietary solutions. Customers who use standards-based technology are not locked into any given vendor's proprietary implementations. Microsoft supports the IETF efforts to standardize VPN technology. To date, two major technologies have reached IETF Proposed Standard status:

- Layer 2 Tunneling Protocol (L2TP)—a combination of PPTP and Cisco's Layer 2 Forwarding, which evolved through the IETF standards process.
- Internet Protocol Security (IPSec)—an architecture, protocol, and related Internet Key Exchange (IKE) protocol, which are described by IETF RFCs 2401-2409.

In addition to IETF standards-track technologies, Microsoft supports PPTP, created by the PPTP Industry Forum (US Robotics (now 3Com), 3Com/Primary Access, Ascend, Microsoft, and ECI Telematics.) PPTP is a published informational RFC and has many companies shipping third-party implementations.

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. To provide a truly interoperable solution, Windows 2000 uses L2TP in combination with IPSec to provide an interoperable, secure VPN solution.

L2TP has broad vendor support, particularly among the largest network access equipment providers, and has verified interoperability in a series of vendor-sponsored testing events. 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. 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.

---

## Remote Access VPN Requirements and IPSec-based Implementations

Remote access VPN solutions require User Authentication (not just machine authentication), Authorization, and Accounting to provide secure client-to-gateway communication and Tunnel Address Assignment and Configuration to provide manageability. IPSec-based implementations that do not use L2TP are using non-standard proprietary methods to address these key remote access VPN requirements.

### User Authentication

Many IPSec-tunnel mode implementations do not support user-based authentication with certificates. When machine-based authentication is used by itself, it is impossible to determine who is accessing the network in order to apply proper authorization. With today's multi-user operating systems, many people may use the same computer, and without user-based authentication, IPSec tunnel mode cannot distinguish between them. Thus, using IPSec tunnel mode without user authentication is inappropriate for use in remote access VPNs.

Third-party IPSec tunnel mode implementations based on XAUTH, a non-standards-track proprietary technology, attempt to address this issue by supporting proprietary user authentication technologies along with group pre-shared keys. As a result, a group pre-shared key introduces a "man-in-the-middle" vulnerability, allowing anyone with access to the group pre-shared key to act as a "go-between," impersonating another user on the network.

IPSec tunnel mode was designed for gateway-to-gateway VPN, in which user authentication and tunnel addressing is less of an issue. Because gateway-to-gateway VPNs are usually between routers, fewer boxes simplify address assignment. And since routers often do not have user-level authentication, machine authentication may be sufficient in many cases. Microsoft supports IPSec tunnel mode in Windows 2000 for gateway-to-gateway configurations that require IP-only, unicast-only communications. Here user authentication is not an issue and interoperability is good.

**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.**

While many customers are interested in eventually deploying smart card authentication, in most cases it remains necessary to support legacy authentication methods such as passwords or token cards during the transition period. Some customers may also want support for advanced authentication technologies such as biometrics (such as retinal scans, fingerprint, and so forth.) There needs to be a standard way to accommodate both legacy authentication as well as authentication methods emerging in the future.

---

IPSec tunnel mode, as originally specified, only supports user authentication via user certificates or pre-shared keys. However, most IPSec tunnel-mode implementations only support use of machine certificates or pre-shared keys. L2TP uses PPP as the method of negotiating user authentication. As a result, L2TP can authenticate with legacy password-based systems through PAP, CHAP, or 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, via integration with RADIUS and LDAP-based directories, L2TP gives the industry a common way to authenticate in an interoperable way while supporting the authentication services that most customers and vendors already have in place.

While there are vendors working on and proposing other authentication services for IPSec only, these alternatives are not on an IETF-standards track. Rather than supporting existing IETF standards for extensible authentication, these proposals introduce yet another authentication framework—with serious known security vulnerabilities. Microsoft believes that customer needs are best served by keeping implementations standards-based.

#### **Address Assignment**

Currently many IPSec tunnel mode implementations use proprietary methods for address assignment and configuration, rather than supporting IETF standards such as DHCP. Microsoft, along with Sun Microsystems, Intel, and RedCreek, has proposed using DHCP to address and configure IPSec tunnels, allowing integration with enterprise class IP address management solutions. IPSec tunnel mode clients that support proprietary address assignment methods are incapable of supporting the wide range of configuration options already supported by DHCP, and in addition, these clients cannot use advances in DHCP technology, such as DHCP Failover, address pool management, or DHCP authentication. They therefore represent a dead-end for IP address management.

Because L2TP uses PPP, it can easily be integrated with existing IP address management systems. PPP clients can use IPCP for address assignment and DHCPINFORM for configuration, while PPP and L2TP servers can integrate with IP address management and configuration systems via DHCP and RADIUS. As a result, L2TP provides good interoperability based on existing standards.

At the past two Network+Interop conferences (<http://www.interop.com>), Microsoft has:

- Included partners in technology demonstrations of L2TP/IPSec, illustrating the interoperability in remote access and gateway-to-gateway configurations.
- Participated in the technology demonstration by InteropNetLabs showing Windows 2000 with up to 15 simultaneous tunnels to other IPSec-pure tunnel mode vendors in a gateway-to-gateway configuration. See: <http://www.interop.com/LasVegas/InteropNet/LabsDesign.html#VPN>

---

### **PPTP: An Alternative and/or Complement to IPSec-Based VPN**

PPTP was the earliest widely supported VPN protocol. Developed before the existence of IPSec and PKI standards, PPTP provides for automated configuration and supports legacy authentication methods. Because PPTP does not require a PKI, it can be much more cost-effective and easier to deploy in situations that do not require the most sophisticated security. PPTP may also be the only viable option when VPN connections must pass through Network Address Translators (NATs), which are incompatible with any IPSec implementation. With Windows 2000, it is possible to use IPSec transport mode within a PPTP tunnel to get extremely powerful encryption services while also passing through NATs. Recent updates to the PPTP specification 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 the ability to use smart cards and public-key certificates to strengthen both user authentication and encryption keys. This strengthens protection against both user impersonation and brute-force decryption of intercepted packets. As a result, PPTP can be a useful alternative or complement to IPSec-based VPNs.

---

## **MICROSOFT'S VPN DIRECTIONS**

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.

### **What Customers Should Do**

Customers who plan to use an IPSec-based VPN solution for remote access should seriously evaluate interoperability issues. Due to many factors—the nature of business acquisitions, the need to let contractors and partners access your corporate networks, and the diverse equipment within company networks—multi-vendor interoperability for VPN is very important. While proprietary solutions may work, it's important to consider how VPN will be used over the next one to two years and how your VPN solution choice today affects your overall direction in the future.

Customers planning to use VPNs for business partnering or to support remote access by contract employees who own their own equipment should prioritize VPN solutions that are based on interoperable standards and which support user-based authentication, authorization, and accounting. If proprietary implementations of IPSec Tunnel Mode are being considered, carefully evaluate the near-term availability of solutions based on L2TP/IPSec to support interoperability. Customers should also consider how their L2TP/IPSec solution might be complemented by PPTP-based solutions.

### **Recommendations to VPN Vendors**

Microsoft encourages gateway vendors to implement L2TP/IPSec for remote access VPN so that the Windows 2000 Professional operating system can connect directly to the vendor's gateway and other VPN solutions without customers having to change client-side code.

For gateway vendors that support other IPSec-based access methods, Microsoft encourages vendors to provide support for L2TP/IPSec as an option to complement IPSec tunnel mode for gateway-to-gateway situations, in which multi-protocol and multicast considerations come into play.

Microsoft also recommends that vendors implement or update their PPTP implementations to ensure compatibility with the most recent PPTP security enhancements as well as maintain interoperability both with Windows 2000 and the older Dial-up Networking version 1.3 clients.

---

## FOR MORE INFORMATION

### VPN Resources

- Microsoft VPN Position White Paper:  
<http://www.microsoft.com/windows2000/library/howitworks/communications/remoteaccess/nwpriv.asp>
- Windows Communications: <http://www.microsoft.com/communications>
- Compaq/Microsoft Network Security Briefings: <http://www.securitybriefing.com/>
- Windows 2000 Server: <http://www.microsoft.com/windows/server/>
- 3DES support in IPSec is obtained by installing the High Encryption Pack at:  
<http://www.microsoft.com/windows/server/beta/downloads/128bit/default.asp>
- Windows 2000 IPSec Interop external Web site:  
<http://w2kipsec-pub.rte.microsoft.com>
- IETF specifications:
  - RFC 2637 (PPTP)
  - RFC 2661 (L2TP)
  - <http://www.ietf.org/internet-drafts/draft-aboba-ipsra-req-00.txt>
  - <http://www.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-security-05.txt>
  - <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-dhcop-04.txt>

For the latest information on Windows 2000, visit our World Wide Web site at <http://www.microsoft.com/windows2000/>.

For the latest information on the Windows NT® operating system, visit our Web site at <http://www.microsoft.com/ntserver> and the Windows NT Server Forum at <http://computingcentral.msn.com/topics/windowsnt>.