PPTP − Point−to−Point Tunneling Protocol

PPTP es un protocolo de red creado por Microsoft que permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet. En el escenario típico de PPTP, el cliente establecerá una conexión *dial−up* con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP. Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP (necesariamente Windows NT Server 4.0) el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada.

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido. Por el momento, PPTP únicamente soporta los protocolos de red IP, IPX, y NetBEUI. El protocolo PPTP especifica además una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP. Estos mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. De este modo, los paquetes de control almacenan la cabecera IP, la cabecera TCP, el mensaje de control PPTP y los trailers apropiados.

La autenticación PPTP está basada en el sistema de acceso de Windows NT, en el cual todos los clientes deben proporcionar un par login/password. La autenticación remota de clientes PPTP es realizada empleando los mismos métodos de autenticación utilizados por cualquier otro tipo de servidor de acceso remoto (RAS). En el caso de Microsoft, la autenticación utilizada para el acceso a los RAS soporta los protocolos CHAP, MS−CHAP, y PAP. Los accesos a los recursos NTFS o a cualquier otro tipo, precisa de los permisos adecuados, para lo cual resulta recomendable utilizar el sistema de ficheros NTFS para los recursos de ficheros a los que deben acceder los clientes PPTP.

En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el estándar RSA RC−4 a partir del password del usuario. La longitud de dicha clave puede ser 128 bits (para usuarios de Estados Unidos y Canada) o 40 bits (para el resto de usuarios).

Por último, PPTP puede ser utilizado conjuntamente con cortafuegos y routers, para lo cual deberá habilitarse el paso del tráfico destinado al puerto TCP 1723 (tráfico PPTP) y protocolo 47 (IP).

Comparativa global entre las diferentes tecnologías VPN

Tecnología	*Puntos fuertes*	*Puntos débiles*	*En desarrollo*
IPSEC	• Opera independiente de las aplicaciones de niveles superiores • Subconjunto de IPv6 • Ocultación de direcciones de red sin emplear NAT • Acoplamiento con las técnicas	• No proporciona la gestión de usuarios • Interoperabilidad entre los fabricantes. • No estandarizado	• Estandarización de todas las facetas de PKI, incluyendo los protocolos de intercambio de certificados y el formato de éstos. • El IETF está en su desarrollo

	criptográficas existentes y futuras		
Cortafuegos	• Gestión centralizada de los parámetros de seguridad, autenticación y acceso. • Disponibilidad de una interfaz común para la modificación de las reglas del túnel. • Disponibilidad de ACLs para usuarios remotos.	• Reducción del modo de operación debida a la encriptación software. • Precisa un alto control con los cambios al añadir nuevas reglas VPN.	• Mismos objetivos que IPSec. • Soluciones capaces de realizar la encriptación por medio del hardware
PPTP	• Soporta tunneling extremo a extremo y entre servidores. • Posibilidad de valor añadido para el acceso remoto. • Proporciona una capacidad multiprotocolo. • Empleo de encriptación RSA RC−4	• No proporciona encriptación de datos para los servidores de acceso remoto • Precisa un servidor NT como terminador del túnel. • Sólo usa encriptación RSA RC−4	• Integración con IPSec
L2F	• Habilita el tunneling multiprotocolo • Soportado por la gran mayoría de fabricantes	• No posee encriptación • Autenticación débil • No dispone de control de flujo sobre el túnel	• Implementaciones que empleen el nombre de usuario y dominio en el establecimiento del túnel
L2TP	• Combina L2F y PPTP. • Necesidad de únicamente una red de paquetes para operar bajo X.25 y Frame Relay.	• Aún no implementado	• Estandarización y operación en proceso • Será adoptado por los fabricantes para el acceso remoto una vez completo
VTCP/Secure	• Mecanismos de encriptación y autenticación fuerte.	• Protocolo propietario. • Las configuraciones LAN−LAN no están permitidas.	• Compatibilidad con IPSec.

	• Proporciona seguridad extremo a extremo. • Tunneling basado en nombre de dominio.	• No es multiprotocolo.	