Microsoft®

Windows NT® Server

Sistema operativo

Red privada virtual: Una descripción general

Resumen

Este documento proporciona una descripción general de redes privadas virtuales (VPNs), describe sus requerimientos básicos y analiza algunas de las tecnologías clave que permiten la conexión de redes privadas en redes públicas.

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

TABLA DE CONTENIDOS

INTRODUCCION

Una red privada virtual (VPN) conecta los componentes de un red sobre otra red. Las VPNs logran esto al permitir que el usuario *haga un túnel* a través de Internet u otra red pública de tal forma que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas (véase la Figura 1).

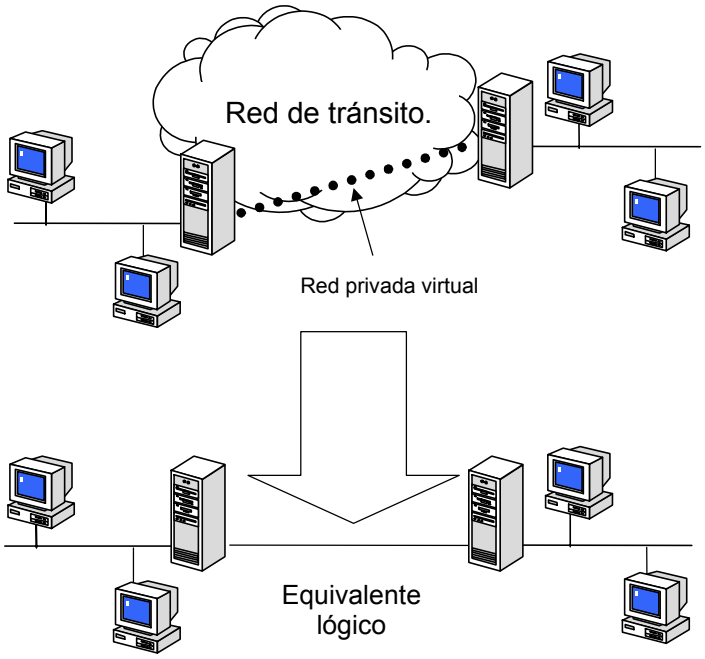


Figura 1: Red privada virtual

Las VPNs permiten a los usuarios que trabajan en el hogar o en el camino conectarse en una forma segura a un servidor corporativo remoto utilizando la infraestructura de enrutamiento que proporciona una red pública (como Internet). Desde la perspectiva del usuario, la VPN es una conexión de punto a punto entre la computadora del usuario y un servidor corporativo. La naturaleza de la red intermedia es irrelevante para el usuario, debido a que aparece como si los datos se estuvieran enviando sobre un enlace privado dedicado.

La tecnología VPN también permite que una compañía se conecte a las sucursales o a otras compañías (Extranets) sobre una red pública (como Internet), manteniendo al mismo tiempo comunicaciones seguras. La conexión de la VPN a través de Internet opera de manera lógica como un enlace de Red de área amplia entre los sitios.

En ambos casos, una conexión segura a través de la red aparece ante el usuario como una comunicación de red privada, a pesar del hecho de que esta comunicación sucede sobre una red pública, de ahí el nombre *Red Privada Virtual*.

La tecnología de la VPN está diseñada para tratar temas relacionados con la tendencia actual de negocios hacia mayores telecomunicaciones, operaciones globales ampliamente distribuidas y operaciones con una alta interdependencia de socios, en donde los trabajadores deben poderse conectar a recursos centrales y comunicarse entre sí.

Para proporcionar a los empleados la capacidad de conectarse a recursos de cómputo corporativos sin importar su ubicación, una compañía debe instalar una solución de acceso remoto que sea confiable y escalable. Típicamente las compañías eligen una solución basada en: 1. Un departamento de sistemas que está encargado de adquirir, instalar y mantener los conjuntos de módems corporativos y la infraestructura de red privada; ó 2. Eligen una solución de Red de valor agregado (VAN), en donde contratan a una compañía externa para adquirir, instalar y mantener los conjuntos de módems y una infraestructura de telecomunicaciones.

Ninguna de estas soluciones proporciona la escalabilidad necesaria en términos de costo, flexibilidad de la administración y gestión, así como demanda de conexiones. Por lo tanto, tiene sentido encontrar un terreno intermedio en donde la organización complemente sus inversiones actuales en conjuntos de módems y su infraestructura de red privada con una solución menos costosa basada en tecnología de Internet. De esta forma, las empresas se pueden enfocar a su negocio principal con la garantía de que nunca se comprometerá su accesibilidad y que se instalen las soluciones más económicas. La disponibilidad de una solución de Internet permite pocas conexiones a Internet (a través de Proveedores independientes de servicio ISPs) y la implementación de varias computadoras de servidor VPN en el borde de la red para dar servicio a las necesidades remotas de red de cientos o hasta miles de clientes y sucursales remotas, como se describe a continuación.

Usos comunes de las VPNs

Las siguientes secciones describen situaciones comunes de la VPN con mayor detalle.

Acceso remoto al usuario sobre Internet

Las VPNs proporcionan acceso remoto a recursos corporativos sobre Internet público, manteniendo al mismo tiempo la privacidad de la información. La Figura 2 muestra una VPN utilizada para conectar a un usuario remoto a una Intranet corporativa.

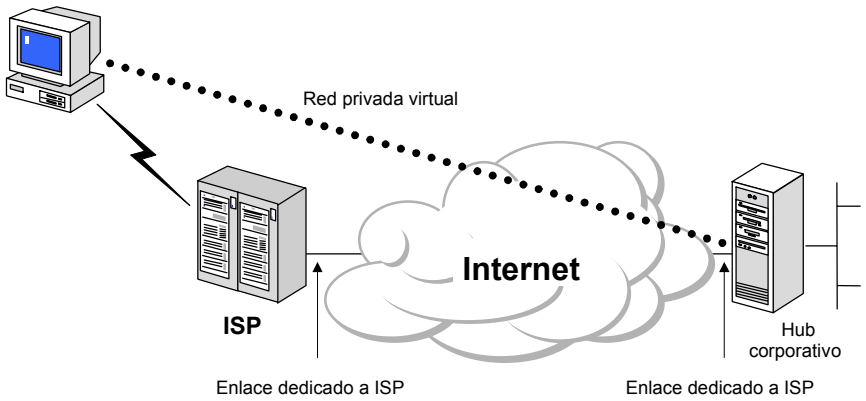


Figura 2: Uso de una VPN para conectar a un cliente remoto con una LAN privada

En lugar de hacer una llamada de larga distancia (ó 1-800) a un Servidor de acceso de red (NAS) corporativo o externo, el usuario llama al ISP local. Al usar la conexión local al ISP, el software de la VPN crea una red privada virtual entre el usuario que marca y el servidor VPN corporativo a través de Internet.

Conexión de las redes sobre Internet

Existen dos métodos para utilizar VPNs para conectar redes de área local a sitios remotos:

- ***Uso de líneas dedicadas para conectar una sucursal a una LAN corporativa***. En lugar de usar un circuito dedicado de arrastre largo entre la sucursal y el *hub* corporativo, tanto los ruteadores del *hub* de la sucursal como el corporativo pueden usar un circuito dedicado local e ISP local para conectarse a Internet. El software VPN utiliza las conexiones ISP locales y el Internet público para crear una red privada virtual entre el ruteador de la sucursal y el ruteador del *hub* corporativo.
- ***Uso de una línea de marcación para conectar una sucursal a una LAN corporativa***. En lugar de que el ruteador en la sucursal realice una llamada de larga distancia (ó 1-800) a un NAS corporativo o externo, el ruteador en la sucursal puede llamar al ISP local. El software VPN utiliza la conexión al ISP local para crear una red privada virtual entre el ruteador de la sucursal y el ruteador del *hub* corporativo a través de Internet.

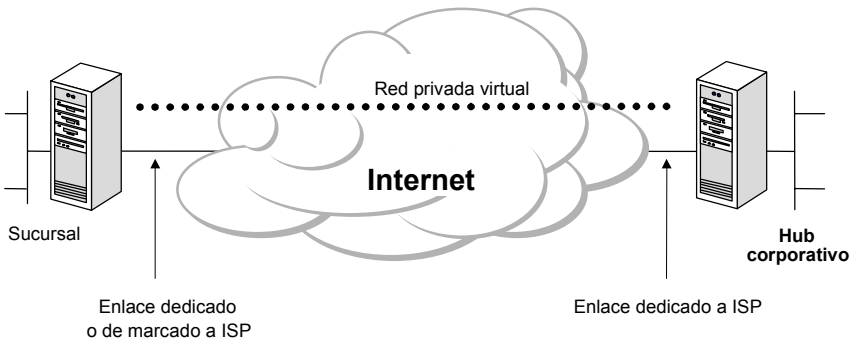


Figura 3: Uso de una VPN para conectar dos sitios remotos

Nótese que en ambos casos, las facilidades que conectan la sucursal y la oficina corporativa al Internet son locales. Se recomienda que el ruteador del *hub* corporativo que actúa como un servidor VPN se conecte a un ISP local con una línea dedicada. Este servidor VPN puede estar listo 24 horas al día para tráfico VPN entrante.

Conexión de computadoras sobre una Intranet

En algunas redes corporativas, los datos departamentales son tan sensibles que la LAN del departamento está físicamente desconectada del resto de la interred corporativa. Si bien esto protege la información confidencial del departamento, crea problemas de accesibilidad a la información para otros usuarios que no están conectados físicamente a la LAN separada.

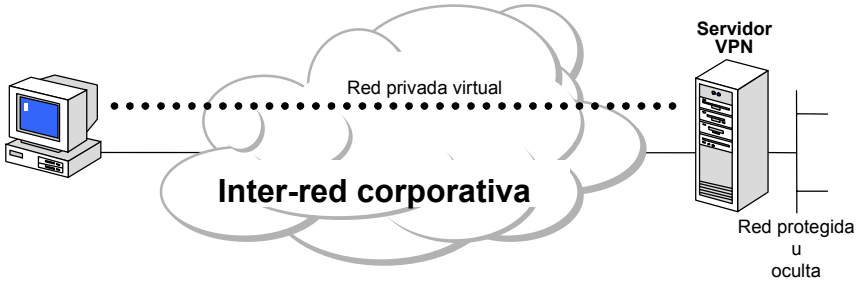


Figura 4: Uso de una VPN para conectar dos computadoras en la misma LAN

Las VPNs permiten que la LAN del departamento esté físicamente conectada a la interred corporativa, pero separada por un servidor por VPN. Nótese que el servidor VPN NO está actuando como un ruteador entre la interred corporativa y la LAN del departamento. Un ruteador interconectaría las dos redes, permitiendo que todo mundo tuviera acceso a la LAN sensible. Al utilizar una VPN, el administrador de la red puede asegurar que sólo aquellos usuarios en la interred corporativa que tienen el nivel adecuado (basado en una política de lo que necesiten saber dentro de la compañía) puede establecer una VPN con el servidor VPN y tener acceso a los recursos protegidos del departamento. Adicionalmente, todas las comunicaciones a través de la VPN pueden encriptarse para efectos de confidencialidad de datos. Aquellos usuarios que no tienen el nivel adecuado no podrán ver la LAN del departamento.

Requerimientos básicos de la VPN

Típicamente, al implementar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la compañía. La solución deberá permitir la libertad para que los clientes *roaming* o remotos autorizados se conecten fácilmente a los recursos corporativos de la red de área local (LAN), y la solución también deberá permitir que las oficinas remotas se conecten entre sí para compartir recursos e información (conexiones de LAN a LAN). Finalmente, la solución debe garantizar la privacidad y la integridad de los

datos al viajar a través de Internet público. Las mismas cuestiones aplican en el caso de datos sensibles que viajan a través de una red corporativa.

Por lo tanto, como mínimo, una solución de VPN debe proporcionar todo lo siguiente:

- ***Autenticación de usuario***. La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados. Además, la solución deberá proporcionar registros de auditoría y contables para mostrar quién accedió a qué información y cuándo.
- ***Administración de dirección***. La solución deberá asignar una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan así.
- ***Encriptación de datos***. Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.
- ***Administración de llaves***. La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.
- ***Soporte de protocolo múltiple***. La solución deberá poder manejar protocolos comunes utilizados en las redes públicas. Estos incluyen Protocolo de Internet (IP), Central de paquete de Internet (IPX), etc.

Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto (PPTP) o un Protocolo de túnel de nivel 2 (L2TP) cumple con todos estos requerimientos básicos y aprovecha la amplia disponibilidad de Internet a nivel mundial. Otras soluciones, incluyendo el Protocolo de seguridad IP (IPSec), cumplen con algunos de estos requerimientos, y siguen siendo útil para situaciones específicas.

El resto de este documento analiza los conceptos, protocolos y componentes de la VPN en mayor detalle.

ASPECTOS BASICOS DE TUNELES

Trabajar en un sistema de túnel es un método de utilizar una infraestructura de la red para transferir datos de una red sobre otra. Los datos que serán transferidos (o carga útil) pueden ser las tramas (o paquetes) de otro protocolo. En lugar de enviar una trama a medida que es producida por el nodo originador, el protocolo de túnel encapsula la trama en un encabezado adicional. El encabezado adicional proporciona información de enrutamiento de tal manera que la carga útil encapsulada pueda viajar a través de la red intermedia.

Entonces, se pueden enrutar los paquetes encapsulados entre los puntos finales del túnel sobre la red. La trayectoria lógica a través de la cual viajan los paquetes encapsulados en la red se le llama un *túnel.* Una vez que las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final. Nótese que este sistema de túnel incluye todo este proceso (encapsulamiento, transmisión y desencapsulamiento de paquetes).

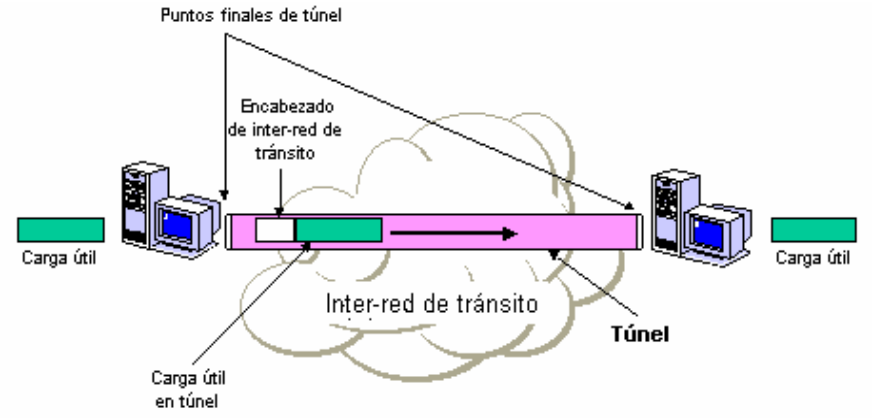


Figura 5: Túneles

Nótese que la interred de tránsito puede ser cualquier interred, el Internet es una interred pública y es el ejemplo del mundo real más conocido. Existen muchos otros ejemplos de túneles que pueden realizarse sobre interredes corporativas. Y si bien Internet proporciona una de las interredes más penetrantes y económicas, las referencias a Internet en este documento se pueden reemplazar por cualquier otra interred pública o privada que actúe como una interred de tránsito.

Las tecnologías de túnel existen desde hace tiempo. Algunos ejemplos de tecnologías maduras incluyen:

- ***Túneles SNA sobre interredes IP***. Cuando se envía tráfico de la Arquitectura de la red del sistema (SNA) a través de una interred IP corporativa, la trama SNA se encapsula en un encabezado UPN e IP.
- ***Túneles IPX para Novell NetWare sobre interredes IP***. Cuando un paquete IPX se envía a un servidor NetWare o ruteador IPX, el servidor o ruteador envuelve el paquete IPX en un encabezado UDP e IP, y luego lo envía a través

de una interred IP. El ruteador IP a IPX de destino quita el encabezado UPD e IP, y transmite el paquete al destino IPX.

Además, se han introducido en los últimos años nuevas tecnologías de sistemas de túneles. Estas tecnologías más nuevas, que son el enfoque principal de este documento, incluyen:

- ***Protocolo de túnel de punto a punto (PPTP)***. PPTP permite que se encripte el tráfico IP, IPX o NetBEUI y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP, como Internet.
- ***Protocolo de túnel de nivel 2 (L2TP)***. L2TP permite que se encripte el tráfico IP, IPX o NetBEUI y luego se envíe sobre cualquier medio que dé soporte a la entrega de datagramas punto a punto, como IP, X.25, *Frame Relay* o ATM.
- ***Modo de túnel de seguridad IP (IPSec)***. El modo de túnel IPSec permite que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP como Internet.

Protocolos de túneles

Para que se establezca un túnel tanto el cliente del túnel como el servidor del túnel deberán utilizar el mismo protocolo de *túnel.*

La tecnología de túnel se puede basar ya sea en el protocolo del túnel de Nivel 2 ó de Nivel 3. Estos niveles corresponden al Modelo de referencia de interconexión de sistemas abiertos (OSI). Los protocolos de nivel 2 corresponden al nivel de Enlace de datos, y utilizan *tramas* como su unidad de intercambio. PPTP y L2TP y el envío de nivel 2 (L2F) son protocolos de túnel de Nivel 2; ambos encapsulan la carga útil en una trama de Protocolo de punto a punto (PPP) que se enviará a través de la red. Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan *paquetes.* IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de Nivel 3. Estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red IP.

Cómo funcionan los túneles

Para las tecnologías de túnel de Nivel 2 como PPTP y L2TP, un túnel es similar a una sesión; los dos puntos finales del túnel deben estar de acuerdo respecto al túnel y deben negociar las variables de la configuración, como son asignación de dirección o los parámetros de encriptación o de compresión. En la mayoría de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas. Se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.

Por lo general, las tecnologías del túnel de Nivel 3 suponen que se han manejado fuera de banda todos los temas relacionados con la configuración, normalmente por medio de procesos manuales. Sin embargo, puede no haber una fase de

mantenimiento de túnel. Para los protocolos de Nivel 2 (PPTP y L2TP), se debe crear, mantener y luego dar por terminado un túnel.

Una vez que se establece el túnel, se pueden enviar los datos a través del mismo. El cliente o el servidor del túnel utilizan un protocolo de transferencia de datos del túnel para preparar los datos para su transferencia. Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor del túnel, el cliente del túnel adjunta primero un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la cual lo enruta al servidor del túnel. El servidor del túnel acepta los paquetes, quita el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo. La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar.

Los protocolos del túnel y los requerimientos básicos del túnel

Debido a que se basan en protocolos PPP bien definidos, los protocolos de Nivel 2 (como PPTP y L2TP) heredan un conjunto de funciones útiles. Como se señala más adelante, estas funciones, y sus contrapartes de Nivel 3 cubren los requerimientos básicos de la VPN.

- ***Autenticación de usuario***. Los protocolos de túnel Nivel 2 heredan los esquemas de autenticación del usuario de PPP, incluyendo los métodos EAP que se comentan a continuación. Muchos de los esquemas de túnel de Nivel 3 suponen que los puntos finales han sido bien conocidos (y autenticados) antes de que se estableciera el túnel. Una excepción es la negociación IPSec ISAKMP, la cual proporciona una autenticación mutua de los puntos finales del túnel. (Nótese que la mayor parte de las implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios. Como resultado, cualquier usuario con acceso a uno de los equipos de punto final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de seguridad cuando se conjunta el IPSec con un protocolo de Nivel 2 como el L2TP.)
- ***Soporte de tarjeta de señales***. Al utilizar el Protocolo de autenticación ampliable (EAP), los protocolos de túnel Nivel 2 pueden dar soporte a una amplia variedad de métodos de autenticación, incluyendo contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define la Autenticación de los certificados de llaves públicas en su negociación ISAKMP/Oakley.
- ***Asignación de dirección dinámica***. El túnel de Nivel 2 da soporte a la asignación dinámica de direcciones de clientes basadas en un mecanismo de negociación de Protocolo de control de la red (NCP). Por lo general, los esquemas de túnel de Nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel. Los esquemas para la asignación de direcciones en el modo de túnel IPSec están actualmente en desarrollo y no

están disponibles aún.

- ***Compresión de datos***. Los protocolos de túnel Nivel 2 dan soporte a esquemas de compresión basados en PPP. Por ejemplo, las implementaciones de Microsoft tanto de PPTP como L2TP utilizan Microsoft Point-to-Point Compression (MPPC). La IETF está investigando mecanismos similares (como la compresión IP) para los protocolos de túnel Nivel 3.
- ***Encriptación de datos***. Los protocolos de túnel Nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. La implementación de Microsoft de PPTP da soporte al uso opcional de Microsoft Point-to-Point Encription (MPPE), basado en el algoritmo RSA/RC4. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define varios métodos de Encriptación opcional de datos que se negocian durante el intercambio ISAKMP/Oakley . La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.
- ***Administración de llaves***. MPPE, un protocolo de Nivel 2, se basa en las claves iniciales generadas durante la Autenticación del usuario y luego las renueva periódicamente. IPSec negocia explícitamente una llave común durante el intercambio ISAKMP y también las renueva periódicamente.
- ***Soporte de protocolo múltiple***. El sistema de túnel de Nivel 2 da soporte a protocolos múltiples de carga útil, lo cual hace más fácil para los clientes de túnel tener acceso a sus redes corporativas utilizando IP, IPX, NetBEUI, etc. En contraste, los protocolos de túnel Nivel 3, como el modo de túnel IPSec, típicamente dan soporte sólo a redes objetivo que utilizan el protocolo IP.

Protocolo de punto a punto (PPP)

Debido a que los protocolos de Nivel 2 dependen principalmente de las funciones originalmente especificadas para PPP, vale la pena examinar este protocolo más de cerca. PPP se diseñó para enviar datos a través de conexiones de marcación o de punto a punto dedicadas. PPP encapsula paquetes de IP, IPX y NetBEUI dentro de las tramas del PPP y luego transmite los paquetes encapsulados del PPP a través de un enlace punto a punto. El PPP se utiliza entre un cliente de marcación y un NAS.

Existen cuatro fases distintivas de negociación en una sesión de marcación del PPP . Cada una de estas cuatro fases debe completarse de manera exitosa antes de que la conexión del PPP esté lista para transferir los datos del usuario. Estas fases se explican más adelante.

Fase1: Establecer el enlace del PPP

PPP utiliza el Protocolo de control de enlace (LCP) para establecer, mantener y terminar la conexión física. Durante la fase LCP inicial, se seleccionan las opciones básicas de comunicación. Nótese que durante la fase de establecimiento de enlace

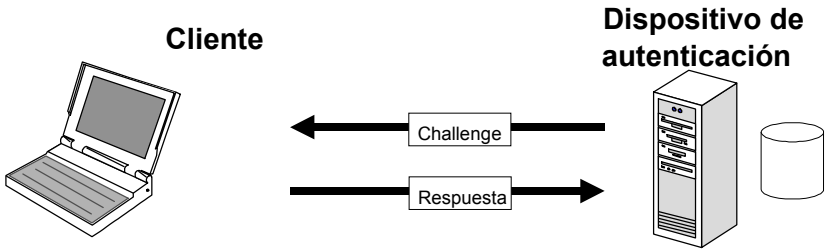
(Fase 1), se seleccionan los protocolos de Autenticación, pero no se implementan efectivamente hasta la fase de Autenticación de conexión (Fase 2). De manera similar, durante el LCP, se toma una decisión en cuanto a que si dos iguales negociarán el uso de compresión y/o encriptación. Durante la Fase 4 ocurre la elección real de algoritmos de compresión/encriptación y otros detalles.

Fase 2: Autenticar al usuario

En la segunda fase, la PC cliente presenta las credenciales del usuario al servidor de acceso remoto. Un esquema seguro de Autenticación proporciona protección contra ataques de reproducción y personificación de clientes remotos. (*Un ataque de reproducción* ocurre cuando un tercero monitorea una conexión exitosa y utiliza paquetes capturados para reproducir la respuesta del cliente remoto, de tal manera que pueda lograr una conexión autenticada. La *personificación del cliente remoto* ocurre cuando un tercero se apropia de una conexión autenticada. El intruso espera hasta que se haya autenticado la conexión y luego atrapa los parámetros de conversación, desconecta al usuario autenticado y toma control de la conexión autenticada.)

La mayoría de las implementaciones del PPP proporcionan métodos limitados de Autenticación, típicamente el Protocolo de autenticación de contraseña (PAP), el Protocolo de autenticación de saludo Challenge (CHAP) y Microsoft Challenge Handshake Authentication Protocol (MSCHAP).

- ***Protocolo de autenticación de contraseña (PAP)***. El PAP es un esquema simple y claro de autenticación de texto. El NAS solicita al usuario el nombre y la contraseña y el PAP le contesta el texto claro (no encriptado). Obviamente, este esquema de autenticación no es seguro ya que un tercero podría capturar el nombre y la contraseña del usuario y utilizarlos para tener un acceso subsecuente al NAS y todos los recursos que proporciona el mismo. PAP no proporciona ninguna protección contra ataques de reproducción o personificación de cliente remoto una vez que se ha escrito la contraseña del usuario.
- ***Protocolo de autenticación de saludo Challenge (CHAP)***. El CHAP es un mecanismo de autenticación encriptado que evita la transmisión de contraseñas reales en la conexión. El NAS envía un *Challenge*, que consiste de una identificación de sesión y una extensión *challenge* arbitraria al cliente remoto. El cliente remoto deberá utilizar el algoritmo de control unidireccional MD5 para devolver el nombre del usuario y una encriptación del *challenge*, la identificación de la sesión y la contraseña del cliente. El nombre del usuario se envía sin verificar.



Challenge = Identificación de sesión extensión Challenge
Respuesta = Hash MD5 (Identificación de sesion, extensión Charllenge, contraseña de usuario),Nombre de usuario

Figura 6: El proceso CHAP

El CHAP es una mejora sobre el PAP en cuanto a que no se envía la contraseña de texto transparente sobre el enlace. En su lugar, se utiliza la contraseña para crear una verificación encriptada del *challenge* original. El servidor conoce la contraseña del texto transparente del cliente y por lo tanto puede duplicar la operación y comparar el resultado con la contraseña enviada en la respuesta del cliente. El CHAP protege contra ataques de reproducción al utilizar una extensión *challenge* arbitraria para cada intento de autenticación. El CHAP protege contra la personificación de un cliente remoto al enviar de manera impredecible *challenges* repetidos al cliente remoto a todo lo largo de la duración de la conexión.

- ***Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)***. El MS-CHAP es un mecanismo de autenticación encriptado muy similar al CHAP. Como en el CHAP, el NAS envía un *challenge*, el cual consiste en una identificación de sesión y una extensión *challenge* arbitraria, al cliente remoto. El cliente remoto debe devolver el nombre del usuario y una verificación MD4 de la extensión *challenge*, el identificador de sesión y la contraseña MD4 verificada . Este diseño, que manipula una verificación del MD4 de la contraseña, proporciona un nivel adicional de seguridad debido a que permite que el servidor almacene las contraseñas verificadas en lugar de contraseñas con texto transparente. MS-CHAP también proporciona códigos adicionales de error, incluyendo un código de Contraseña ha expirado, así como mensajes adicionales cliente-servidor encriptados que permiten a los usuarios cambiar sus contraseñas. En la implementación de Microsoft del MS-CHAP, tanto el Cliente como el NAS generan de manera independiente una llave inicial para encriptaciones subsecuentes de datos por el MPPE. El último punto es muy importante, ya que explica la forma en que se requiere la autenticación del MS-CHAP para poder permitir la encriptación de datos con base en MPPE.

Durante la fase 2 de la configuración del enlace del PPP, el NAS recopila los datos de autenticación y luego valida los datos contra su propia base de datos del usuario o contra un servidor central para la autenticación de base de datos, como el que mantiene un Controlador del dominio primario Windows NT, un servidor de Servicio remoto de usuario con marcación de autenticación (RADIUS).

Fase3: Control de rellamado del PPP.

La implementación de Microsoft del PPP incluye una Fase opcional de control de rellamado. Esta fase utiliza el Protocolo de control de rellamado (CBCP) inmediatamente después de la fase de autenticación. Si se configura para rellamado, después de la autenticación, se desconectan tanto el cliente remoto como el NAS. Entonces, el NAS vuelve a llamar al cliente remoto en el número telefónico especificado. Esto proporciona un nivel adicional de seguridad a las redes de marcación. El NAS permitirá conexiones partir de los clientes remotos que físicamente residan sólo en números telefónicos específicos.

Fase 4: Invocar los protocolo(s) a nivel de red

Una vez que se hayan terminado las fases previas, PPP invoca los distintos Protocolos de control de red (NCPs) que se seleccionaron durante la fase de establecimiento de enlace (Fase1) para configurar los protocolos que utiliza el cliente remoto. Por ejemplo, durante esta fase el Protocolo de control de IP (IPCP) puede asignar una dirección dinámica a un usuario de marcación. En la implementación del PPP de Microsoft, el protocolo de control de compresión se utiliza para negociar tanto la compresión de datos (utilizando MPPC) como la encriptación de datos (utilizando MPPE) por la simple razón de que ambos se implementan en la misma rutina.

Fase de transferencia de datos

Una vez que se han terminado las cuatro fases de negociación, PPP empieza a transferir datos hacia y desde los dos iguales. Cada paquete de datos transmitidos se envuelve en un encabezado del PPP el cual quita el sistema receptor. Si se seleccionó la compresión de datos en la fase 1 y se negoció en la fase 4, los datos se comprimirán antes de la transmisión. Si se seleccionaron y se negociaron de manera similar la encriptación de datos, los datos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

Protocolo de túnel de punto a punto (PPTP)

El PPTP es un protocolo de Nivel 2 que encapsula las tramas del PPP en datagramas del IP para transmisión sobre una red IP, como la de Internet. También se puede utilizar el PPTP en una red privada de LAN a LAN.

El PPTP se documenta en el RFC preliminar, “Protocolo de túnel de punto a punto” (pptp-draft-ietf-ppext-pptp-02.txt). Este proyecto se presentó ante el IETF en junio de 1996 por parte de las compañías miembros del Foro PPTP incluyendo Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics y US Robotics (ahora 3Com).

Nota: *Se deberá considerar los documentos proyecto de Internet como trabajos en proceso. Véase* www.ietf.org *para copias de proyectos de Internet.*

Protocolo de túnel de punto a punto (PPTP) utiliza una conexión TCP para mantenimiento del túnel y tramas del PPP encapsuladas de Encapsulación de

enrutamiento genérico (GRE) para datos de túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas del PPP encapsulado. La Figura 7 muestra la forma en que se ensambla el paquete del PPTP antes de la transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño de la trama final muestra la encapsulación para un cliente de marcación (controlador de dispositivo PPP).

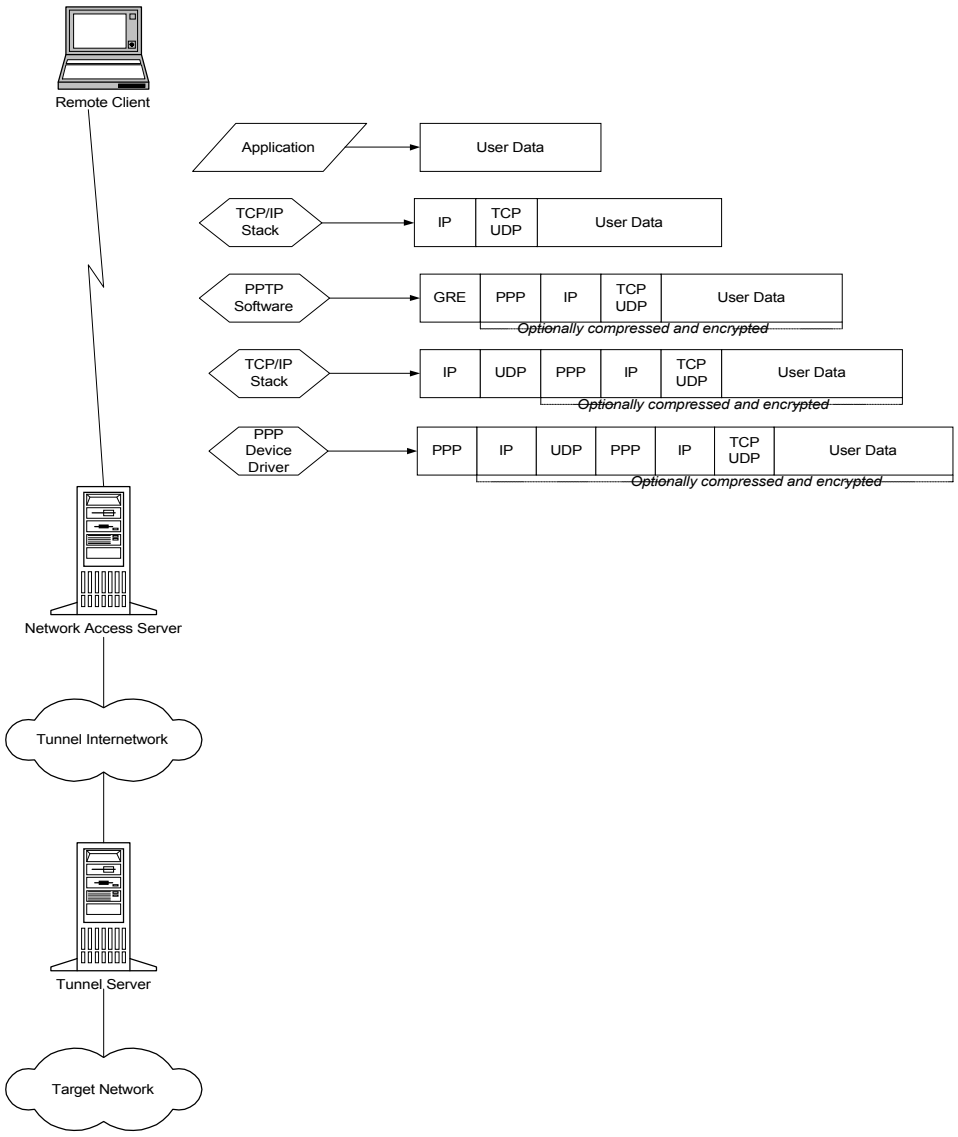


Figura 7. Construcción de un paquete PPTP

Reenvío de nivel 2 (L2F)

L2F, una tecnología propuesta por Cisco, es un protocolo de transmisión que permite que los servidores de acceso de marcación incluyan el tráfico de marcación

en el PPP y lo transmitan sobre enlaces WAN hacia un servidor L2F (un ruteador). El servidor L2F envuelve entonces los paquetes y los inyecta en la red. A diferencia del PPTP y L2TP, L2F no tiene un cliente definido. Nótese que L2F funciona sólo en túneles obligatorios. (Para un análisis detallado de los túneles voluntarios y obligatorios, véase la sección “Tipos de túneles”, más adelante en este documento.)

Protocolo de túnel de nivel 2 (L2TP)

L2TP es una combinación del PPTP y L2F. Sus diseñadores esperan que el L2TP represente las mejores funciones del PPTP y L2F.

L2TP es un protocolo de red que encapsula las tramas del PPP que se enviarán sobre redes IP, X.25, *Frame Relay* o Modo de transferencia asíncona (ATM). Cuando está configurado para utilizar al IP como su transporte de datagrama, L2TP se puede utilizar como un protocolo de túnel sobre Internet. También se puede utilizar al L2TP directamente sobre varios medios WAN (como *Frame Relay*) sin nivel de transporte IP.

El L2TP se documenta en el proyecto del RFC, el *Protocolo de túnel nivel 2 “L2TP”* (draft-ietf-pppext-l2tp-09.txt). Este documento se presentó al IETF en enero de 1998.

Nota: Los documentos del proyecto sobre Internet deberán considerarse como trabajos en proceso. Véase www.ietf.org para copias de los proyectos de Internet.

El 2TP sobre las redes IP utilizan UDP y una serie de mensajes del L2TP para el mantenimiento del túnel. El L2TP también utiliza UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas PPP encapsuladas. La Figura 8 muestra la forma en que se ensambla un paquete L2TP antes de su transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

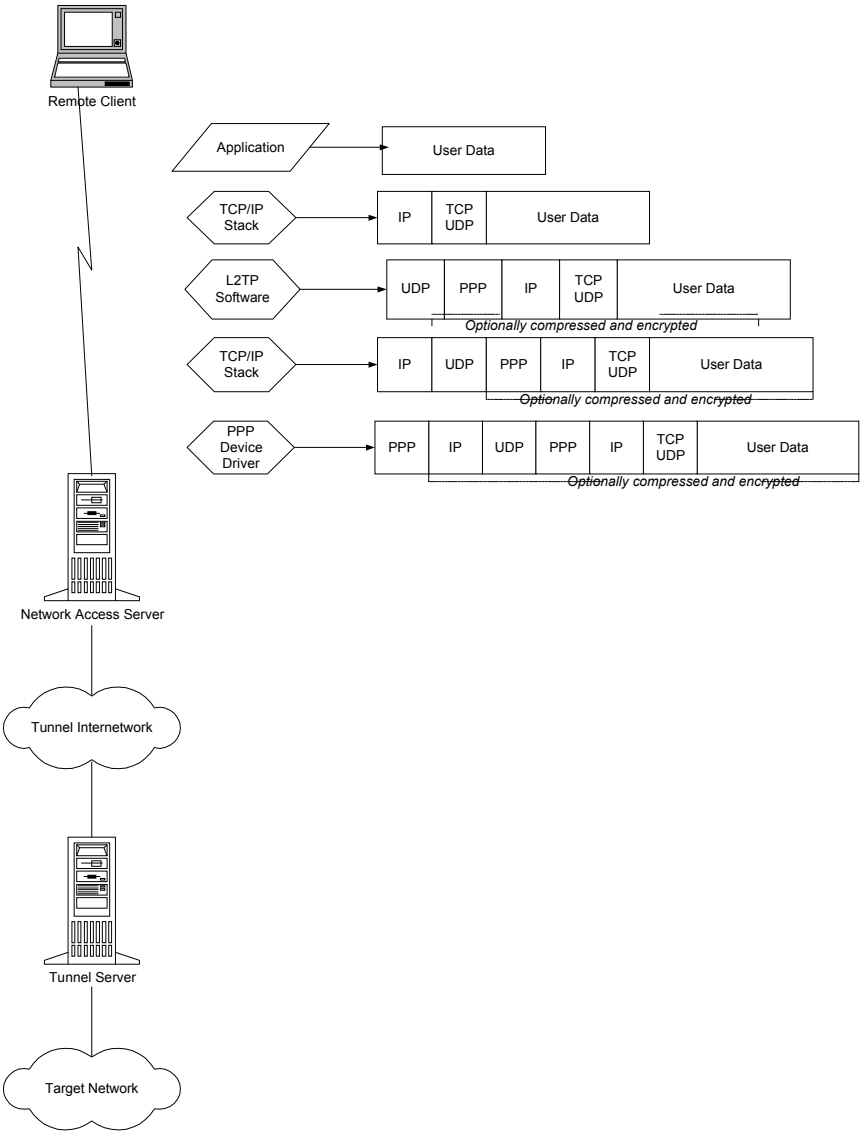


Figure 8. Construcción de un paquete L2TP

PPTP comparado con el L2TP

Tanto el PPTP como L2TP utilizan el PPP para proporcionar una envoltura inicial de los datos y luego incluir encabezados adicionales para transportarlos a través de la red. Los dos protocolos son muy similares. Sin embargo, existen diferencias entre el PPTP y L2TP:

- El PPTP requiere que la red sea de tipo IP. El L2TP requiere sólo que los medios del túnel proporcionen una conectividad de punto a punto orientada a paquetes. Se puede utilizar L2TP sobre IP (utilizando UDP), circuitos virtuales permanentes (PVCs), circuitos virtuales X.25 (VCs) o VCs ATM.
- El PPTP sólo puede soportar un túnel único entre puntos terminales. El L2TP permite el uso de varios túneles entre puntos terminales. Con el L2TP, uno

puede crear diferentes túneles para diferentes calidades de servicio.

- L2TP proporciona la compresión de encabezados. Cuando se activa la compresión de encabezado, el L2TP opera sólo con 4 bytes adicionales, comparado con los 6 bytes para el PPTP.
- L2TP proporciona la autenticación de túnel, mientras que el PPTP no. Sin embargo, cuando se utiliza cualquiera de los protocolos sobre IPSec, se proporciona la autenticación de túnel por el IPSec de tal manera que no sea necesaria la autenticación del túnel Nivel 2.

Modo del túnel de seguridad de protocolo para Internet (IPSec)

El IPSec es un estándar de protocolo de Nivel 3 que da soporte a la transferencia protegida de información a través de una red IP. En su conjunto se describe con mayor detalle en la sección de Seguridad avanzada más adelante. Sin embargo, hay un aspecto del IPSec que debe analizarse en el contexto de los protocolos de túnel. Además de su definición de mecanismos de encriptación para tráfico IP, IPSec define el formato de paquete para un modo de túnel IP sobre IP, generalmente referido como un *modo de túnel IPSec*. Un túnel IPSec consiste en un cliente de túnel y un servidor de túnel, ambos configurados para utilizar los túneles IPSec y un mecanismo negociado de encriptación.

El modo del túnel del IPSec utiliza el método de seguridad negociada (de existir) para encapsular y encriptar todos los paquetes IP para una transferencia segura a través de una red privada o pública IP. Entonces, se vuelve a encapsular la carga útil encriptada con un encabezado IP de texto y se envía en la red para su entrega a un servidor de túnel. Al recibir este datagrama, el servidor del túnel procesa y descarta el encabezado IP de texto y luego desencripta su contenido para recuperar el paquete original IP de carga útil. Entonces, se procesa el paquete IP de carga útil de manera normal y se enruta su destino en la red objetivo.

El modo de túnel IPSec tiene las siguientes funciones y limitaciones:

- Sólo da soporte a tráfico IP.
- Funciona en el fondo de la pila IP; por lo tanto, las aplicaciones y protocolos de niveles más altos heredan su comportamiento.
- Está controlado por una *política de seguridad*—un conjunto de reglas que se cumplen a través de filtros. Esta política de seguridad establece los mecanismos de encriptación y de túnel disponibles en orden de preferencia y los métodos de autenticación disponibles, también en orden de preferencia. Tan pronto como existe tráfico, los dos equipos realizan una autenticación mutua, y luego negocian los métodos de encriptación que se utilizarán. En lo subsecuente, se encripta todo el tráfico utilizando el mecanismo negociado de encriptación y luego se envuelve en un encabezado de túnel.

Para más información sobre el IPSec, refiérase a la sección “Seguridad Avanzada“

más adelante en este documento.

Tipos de túnel

Se pueden crear túneles en diferentes formas.

- ***Túneles voluntarios:*** Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente del túnel.
- ***Túneles obligatorios***: Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del túnel.

A la fecha, los túneles voluntarios han probado ser el tipo más popular de túnel. Las siguientes secciones describen cada uno de estos tipos de túnel en mayor detalle.

Túneles voluntarios

Un túnel voluntario ocurre cuando una estación de trabajo o un servidor de enrutamiento utiliza el software del cliente del túnel para crear una conexión virtual al servidor del túnel objetivo. Para poder lograr esto se debe instalar el protocolo apropiado de túnel en la computadora cliente. Para los protocolos que se analizan en este documento, los túneles voluntarios requieren una conexión IP (ya sea a través de una LAN o marcación).

En una situación de marcación, el cliente debe establecer una conexión de marcación para conectarse a la red antes de que el cliente pueda establecer un túnel. Este es el caso más común. El mejor ejemplo de esto es el usuario de Internet por marcación, que debe de marcar a un ISP y obtener una conexión a Internet antes de que se pueda crear un túnel sobre Internet.

Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un enrutamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este sería el caso para un cliente en una LAN corporativa que inicia un túnel para alcanzar una sub-red privada u oculta en la misma LAN (como sería el caso de la red de Recursos Humanos que se analizó previamente).

Es una equivocación común que las VPNs requieran una conexión de marcación. Sólo requieren de una red IP. Algunos clientes (como las PCs del hogar) utilizan conexiones de marcación al Internet para establecer transporte IP. Esto es un paso preliminar en la preparación para la creación de un túnel, y no es parte del protocolo del túnel mismo.

Túneles obligatorios

Varios proveedores que venden servidores de acceso de marcación han

implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora del cliente es conocida de varias maneras como: Procesador frontal (FEP) en PPTP, un Concentrador de acceso a L2TP (LAC) en L2TP o un *gateway* de seguridad IP en el IPSec. Para los propósitos de este documento, el término FEP se utilizará para describir esta funcionalidad, sin importar el protocolo de túnel. Para llevar a cabo esta función, el FEP deberá tener instalado el protocolo apropiado de túnel y deberá ser capaz de establecer el túnel cuando se conecte la computadora cliente.

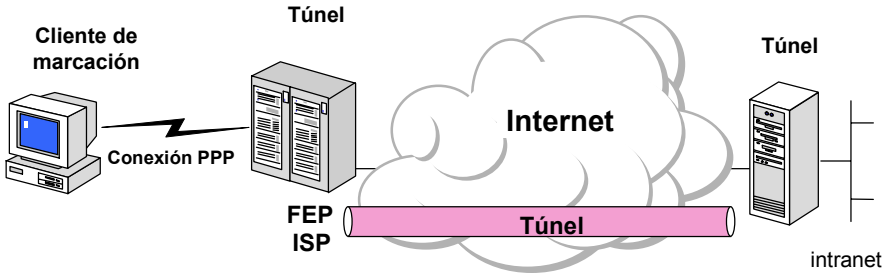


Figura 9: Túneles obligatorios

En el ejemplo de Internet, la computadora cliente coloca una llamada de marcación al NAS activado por los túneles en el ISP. Por ejemplo, una empresa puede haber contratado con un ISP para instalar un conjunto nacional de FEPs. Estos FEPs pueden establecer túneles a través de Internet a un servidor de túnel conectado a la red privada de la empresa, consolidando así las llamadas de diferentes ubicaciones geográficas en una conexión única de Internet en la red corporativa.

Esta configuración se conoce como “túnel obligatorio” debido a que el cliente está obligado a utilizar el túnel creado por FEP. Una vez que se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel. En los túneles obligatorios, la computadora cliente realiza una conexión única PPP y, cuando un cliente marca en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de éste. Se puede configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel. De manera alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el FEP y servidor del túnel puede estar compartido entre varios clientes de marcación. Cuando un segundo cliente marca al servidor de acceso (FEP) para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el FEP y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

FUNCIONES DE SEGURIDAD AVANZADAS

Debido a que Internet facilita la creación de VPNs desde cualquier lugar, las redes necesitan fuertes funciones de seguridad para evitar el acceso no deseado a redes privadas y proteger los datos privados cuando viajan a través de redes públicas. Ya se ha analizado la autenticación de usuario y la encriptación de datos. Esta sección proporciona un breve análisis de capacidades más sólidas de autenticación y encriptación que estarán disponibles con EAP e IPSec. Empezaremos con una descripción general de la encriptación de llaves públicas y certificados basados en llaves públicas, ya que éstos jugarán un papel importante en las nuevas funciones de seguridad EAP e IPSec que se encuentran ahora en desarrollo por Microsoft y otros proveedores de software.

Encriptación simétrica vs. encriptación asimétrica (Llaves privadas vs. llaves públicas)

La encriptación simétrica o de llave privada (también conocida como encriptación convencional) está basada en una llave secreta que comparten ambas partes que se comunican. La parte emisora utiliza la llave secreta como parte de la operación matemática para encriptar (o codificar) texto plano a texto cifrado. La parte receptora utiliza la misma llave secreta para desencriptar (o descifrar) el texto cifrado a texto plano. Ejemplos de los esquemas de encriptación simétrica son el algoritmo RSA RC4 (que proporciona la base de Microsoft Point-to-Point Encription (MPPE), el Estándar de encriptación de datos (DES), el Algoritmo de encriptación de datos internacional (IDEA) y la tecnología de encriptación Skipjack propuesta por el gobierno de Estados Unidos (e implementada en el *Chip* Cliper).

La encriptación asimétrica o de llave pública utiliza dos llaves diferentes para cada usuario: una es una llave privada conocida sólo por este usuario; la otra es una llave pública correspondiente, que es accesible para todos. Las llaves privadas públicas están matemáticamente relacionadas con el algoritmo de encriptación. Se utiliza una llave para encriptación y la otra para la desencriptación, dependiendo de la naturaleza del servicio de comunicación que se esté implementando.

Además, las tecnologías de encriptación de llaves públicas permiten que se coloquen firmas digitales en los mensajes. Una firma digital utiliza la llave privada del remitente para codificar alguna parte de los mensajes. Cuando se recibe el mensaje, el receptor utiliza la llave pública del remitente para descifrar la firma digital como una manera de verificar la identidad del remitente.

Certificados

Con la encriptación simétrica, tanto el remitente como el destinatario cuentan con una llave secreta compartida. La distribución de la llave secreta debe ocurrir (con la protección adecuada) antes de cualquier comunicación encriptada. Sin embargo, con la encriptación asimétrica, el remitente utiliza una llave privada para encriptar o firmar digitalmente los mensajes, mientras que el receptor utiliza una llave pública para descifrar estos mensajes. La llave pública puede distribuirse libremente a todos los que necesiten recibir mensajes encriptados o firmados

digitalmente. El remitente necesita proteger cuidadosamente sólo la llave privada.

Para garantizar la integridad de la llave pública se publica con un *certificado*. Un certificado (o certificado de llave pública) es una estructura de datos que está firmada digitalmente por una autoridad certificadora (CA); una autoridad en la que los usuarios del certificado pueden confiar. El certificado contiene varios valores, como el nombre y el uso del certificado, la información que identifica al propietario de la llave pública, la llave pública misma, una fecha de expiración y el nombre de la autoridad certificadora. La CA utiliza su llave privada para firmar el certificado. Si el receptor conoce la llave pública de la autoridad certificadora, el receptor puede verificar que el certificado sea, en efecto, de esa CA y, por lo tanto, que contiene información confiable y una llave pública válida. Los certificados se pueden distribuir de manera electrónica (a través de acceso al Web o correo electrónico), en tarjetas inteligentes o en discos flexibles.

En resumen, los certificados de llaves públicas proporcionan un método conveniente y confiable para verificar la identidad de un remitente. IPSec puede utilizar de manera opcional este método para la autenticación de extremo a extremo. Los servidores de acceso remoto pueden utilizar certificados de llave pública para la autenticación de usuarios, como se describe en la sección "Seguridad a nivel de transacción (EAP-TLS)", más adelante.

Protocolo ampliable de Autenticación (EAP)

Como se señaló anteriormente en este documento, la mayor parte de las implementaciones del PPP proporcionan métodos de autenticación muy limitados. El EAP es una extensión propuesta por el IETF al PPP que permite que se empleen mecanismos arbitrarios de autenticación para la validación de una conexión PPP. El EAP se diseñó para permitir la adición dinámica de módulos conectables de autenticación tanto en el extremo del cliente como del servidor de una conexión. Esto permite que los proveedores cuenten con un nuevo esquema de autenticación en cualquier momento. El EAP proporciona la más alta flexibilidad en cuanto a autenticaciones únicas y variación de las mismas.

El EAP se implementará en Microsoft® Windows® 2000.

Seguridad a nivel de transacción (EAP-TLS)

La EAP-TLS ha sido presentada ante el IETF como una propuesta proyecto para un fuerte método de autenticación basado en certificados de llaves públicas. Con la EAP-TLS, un cliente presenta un certificado de usuario a un servidor de marcación, mientras que al mismo tiempo, el servidor presenta un certificado de servidor al cliente. El primero proporciona una sólida autenticación de usuario al servidor; el segundo proporciona la garantía de que el usuario ha llegado al servidor que esperaba. Ambos sistemas dependen de una cadena de autoridades confiables para verificar la validez del certificado ofrecido.

Se puede almacenar el certificado del usuario en la PC del cliente de marcación, o se puede almacenar en una tarjeta inteligente externa. En ambos casos, no se

puede tener acceso a certificados sin alguna forma de identificación de usuario (número NIP o intercambio de nombre/contraseña) entre el usuario y la PC cliente. Este enfoque cumple con el criterio de “algo que sabes más algo que tienes” que recomiendan la mayoría de los expertos en seguridad.

La EAP-TLS es un método EAP específico que se implementará en Microsoft Windows 2000. Al igual que MS-CHAP, EAP-TLS devolverá una llave de encriptación para activar la encriptación de datos subsecuentes por MPPE.

Seguridad IP (IPSec)

La Seguridad de protocolo de Internet (IPSec) fue diseñada por el IETF como un mecanismo de extremo a extremo para garantizar la seguridad de los datos en comunicaciones basadas en IP. Se ha definido a IPSec en una serie de RFCs, especialmente RFCs 1825, 1826 y 1827, las cuales definen la arquitectura global, un encabezado de autenticación para verificar la integridad de los datos, y Carga útil de seguridad de encapsulación tanto para la integridad de los datos como para la encriptación de los mismos.

La IPSec define dos funciones que aseguran la confidencialidad: encriptación de datos e integridad de datos. Como lo definió Internet Engineering Task Force, IPSec utiliza un Encabezado de autenticación (AH) para proporcionar la autenticación e integridad de la fuente sin encriptación, y la Carga útil de seguridad encapsulada (ESP) para proporcionar la autenticación y la integridad junto con la encriptación. Con la Seguridad IP, sólo el remitente y el receptor conocen las llaves de seguridad. Si los datos de autenticación son válidos, el receptor sabe que la comunicación provino del remitente, y que no se cambió en su tránsito.

Se puede considerar que IPSec es un nivel inferior a la pila TCP/IP. Este nivel está controlado por una política de seguridad en cada equipo y una asociación negociada de seguridad entre el remitente y el receptor. La política consiste en un conjunto de filtros y comportamientos de seguridad asociados. Si la dirección IP, el protocolo y el número de puerto de un paquete corresponde con un filtro, entonces el paquete está sujeto al comportamiento de seguridad asociado.

Asociación de seguridad negociada

Este primer paquete acciona una negociación de seguridad entre el remitente y el receptor. ISAKMP/Oakley es el protocolo estándar para esta negociación. Durante un intercambio ISAKMP/Oakley los dos equipos acuerdan sobre el método de autenticación y de seguridad de los datos, realizan una autenticación mutua y después generan una llave compartida para una encriptación subsecuente de los datos.

Después de que se ha establecido una asociación de seguridad, se puede proceder con la transmisión de datos para cada máquina aplicando el tratamiento de seguridad de datos a los paquetes que se transmitan al receptor remoto. El tratamiento puede simplemente asegurar la integridad de los datos transmitidos o puede encriptarlos también. A continuación se analizan estas opciones.

Encabezado de autenticación

La integridad de los datos y la autenticación de los mismos para las cargas útiles IP pueden proporcionarse por medio de un encabezado de autenticación localizado entre el encabezado IP y el encabezado de transporte. El encabezado de autenticación incluye los datos de autenticación y un número de secuencia, los cuales se usan conjuntamente para verificar el remitente, asegurar que el mensaje no se haya modificado en el tránsito y evitar un ataque de reproducción.

El encabezado de autenticación IPSec no proporciona encriptación de datos; se pueden enviar mensajes de textos transparentes y el encabezado de autenticación asegura que se hayan originado en un usuario específico y no se hayan modificado en el tránsito.

Encabezado de seguridad de encapsulación

Tanto para la confidencialidad como para la protección de los datos de la captura de un tercero, la Carga útil de seguridad de encapsulación (ESP) proporciona un mecanismo para encriptar la carga útil IP. La ESP también proporciona servicios de autenticación e integridad de los datos; por lo tanto, los encabezados de la ESP son una alternativa a los encabezados AH en los paquetes IPSec.

ADMINISTRACION DEL USUARIO

Al seleccionar una tecnología VPN, es importante considerar los asuntos administrativos. Las redes grandes necesitan almacenar información de directorios por usuario en un almacenamiento centralizado de datos, o *servicio de directorio*, de tal manera que los administradores y las aplicaciones puedan agregar, modificar o consultar esta información. Cada servidor de acceso de datos o túnel podría mantener su propia base de datos interna de propiedades por usuario, como nombres, contraseñas y atributos de permisos de marcación. Sin embargo, debido a que administrativamente no es posible mantener cuentas múltiples de usuarios en servidores múltiples y mantenerlas actualizadas de manera simultánea, la mayoría de los administradores establecen una base de datos de cuenta maestra en el Servidor del directorio o en el Controlador de dominio primario, o un servidor RADIUS.

Soporte en RAS

Microsoft Remote Access Server (RAS) está diseñado para trabajar con la información por usuario almacenada en el controlador de dominio o en un servidor RADIUS. Al usar un controlador de dominio se simplifica la administración del sistema debido a que los permisos de marcación son un subconjunto de la información por usuario que el administrador ya está manejando en una base de datos única.

Microsoft RAS fue diseñado originalmente como un servidor de acceso para los usuarios de marcación. RAS es también un servidor de túnel para las conexiones PPTP y L2TP. Por consiguiente, estas soluciones VPN de Nivel 2 heredan toda la infraestructura de administración que ya se encuentra en las redes de marcación.

En Windows 2000, RAS aprovechará los nuevos Servicios de directorio, una base de datos duplicada en toda la empresa con base en el Protocolo de acceso de directorio ligero (LDAP). El LDAP es un protocolo estándar de la industria para tener acceso a los servicios de directorio, y fue desarrollado como una alternativa más simple al protocolo X.500 DAP. El LDAP es ampliable, independiente del proveedor y se basa en estándares. Esta integración con el DS permitirá que un administrador asigne una variedad de propiedades de conexión para las sesiones de marcación o VPN a usuarios individuales o grupos. Estas propiedades pueden definir filtros por usuario, métodos de autenticación o encriptación requeridos, limitaciones por hora del día, etc.

Escalabilidad

La redundancia y el balance de carga se logran utilizando DNS *round-robin* para dividir las solicitudes entre un número de servidores de túnel VPN que comparten un perímetro común de seguridad. Un perímetro de seguridad cuenta con un nombre DNS externo—por ejemplo, vpnx.support.bigcompany.com—y varias direcciones IP, y las cargas se distribuyen de manera aleatoria a través de todas las direcciones IP. Todos los servidores pueden autenticar solicitudes de acceso contra una base de datos compartida, como un Controlador de Dominio Windows

NT. Nótese que las bases de datos del dominio Windows NT se duplican por diseño.

RADIUS

El protocolo del Servicio del usuario de marcación de autenticación remota (RADIUS) es un método popular para administrar la autenticación y autorización de usuarios remotos. El RADIUS es un protocolo muy ligero, basado en UDP. Los servidores RADIUS se pueden localizar en cualquier lugar de Internet y proporcionan autenticación (incluyendo PPP PAP, CHAP, MSCHAP y EAP) a su NAS cliente.

Además, los servidores RADIUS pueden proporcionar un servicio *proxy* para transferir las solicitudes de autenticación a servidores RADIUS distantes. Por ejemplo, muchos ISPs se han unido a los consorcios para que los abonados de *roaming* utilicen servicios locales desde el ISP más cercano para acceso de marcación a Internet. Estas "alianzas de *roaming*" aprovechan el servicio *proxy* del RADIUS. Si un ISP reconoce el nombre de un usuario como el de un abonado a la red remota, el ISP utiliza un *proxy* RADIUS para enviar la solicitud de acceso a la red adecuada.

CONTABILIDAD, AUDITORIA Y ALARMAS

Para administrar adecuadamente un sistema VPN, los administradores de red deberán poder rastrear quiénes utilizan el sistema y cuántas conexiones se realizan, actividades inusuales, condiciones de error y situaciones que puedan indicar fallas en el equipo. Esta información se puede utilizar para propósitos de facturación, auditoria y alarma o notificación de errores.

Por ejemplo, un administrador pude necesitar conocer quién se conectó al sistema y durante cuánto tiempo para poder preparar los datos de facturación. La actividad inusual puede indicar un uso inapropiado del sistema o recursos inadecuados del mismo. Un monitoreo en tiempo real del equipo (por ejemplo, una actividad inusualmente alta en un módem e inactividad en otros) puede generar alertas que notifiquen al administrador de la falla de un módem. El servidor de túnel pude proporcionar toda esta información, y el sistema proporcionará los registros de eventos, reportes y una facilidad para almacenaje de datos que maneje los datos de manera adecuada.

Microsoft Windows NT 4.0 proporciona soporte de contabilidad, auditoría y notificación de errores en el RAS.

El protocolo RADIUS define un conjunto de solicitudes de contabilidad de llamadas que son independientes de las solicitudes de autenticación que hemos analizado anteriormente. Estos mensajes del RAS al servidor RADIUS solicitan a este último la generación de registros contables al inicio de una llamada, la terminación de la misma y a intervalos predeterminados durante una llamada. Windows 2000 generará estas solicitudes de contabilidad RADIUS a partir de las solicitudes de autenticación de acceso (las cuales podrían ir al Controlador de dominio o a un servidor RADIUS). Esto permitirá que un administrador configure un servidor RADIUS de contabilidad ya sea o no que se utilice RADIUS para autenticación. Entonces, un servidor de contabilidad puede recopilar registros para cada conexión VPN para un análisis posterior. Varios terceros han preparado ya paquetes de facturación y auditoría que pueden leer estos registros de contabilidad RADIUS y producir varios reportes útiles.

CONCLUSION

Como se explica en este documento, los servicios VPN permiten que los usuarios o las empresas se conecten de manera confiable a servidores remotos, sucursales u otras compañías sobre redes públicas y privadas, mientras mantienen una comunicación segura. En todos estos casos, la conexión segura se muestra ante el usuario como una comunicación de red privada—a pesar del hecho de que la comunicación ocurre sobre una red pública. La tecnología VPN está diseñada para abordar asuntos relacionados con la actual tendencia de los negocios hacia operaciones globales cada vez mayores de telecomunicación y de amplia distribución, en donde los trabajadores deben poder conectarse a los recursos centrales y en donde los negocios deben poder comunicarse entre sí de manera eficiente.

Este documento estratégico proporciona una descripción general de redes privadas virtuales y describe los requerimientos básicos de tecnologías VPN útiles: autenticación de usuario, administración de dirección, encriptación de datos, administración de llaves y soporte de protocolos múltiples. Analiza la forma en que los protocolos de Nivel 2, específicamente el PPTP y L2TP, cumplen con estos requerimientos y la forma en que IPSec (un protocolo de Nivel 3) cumplirá con estos requerimientos en el futuro.

Para mayores informes

Para información más reciente sobre Windows NT Server, revise nuestro sitio Web en http://www.microsoft.com/communications y el Foro de Windows NT Server en Microsoft Network (GO WORD: MSNTS).