Redes Privadas Virtuales

(Virtual Private Network)

VPN

Introducción.

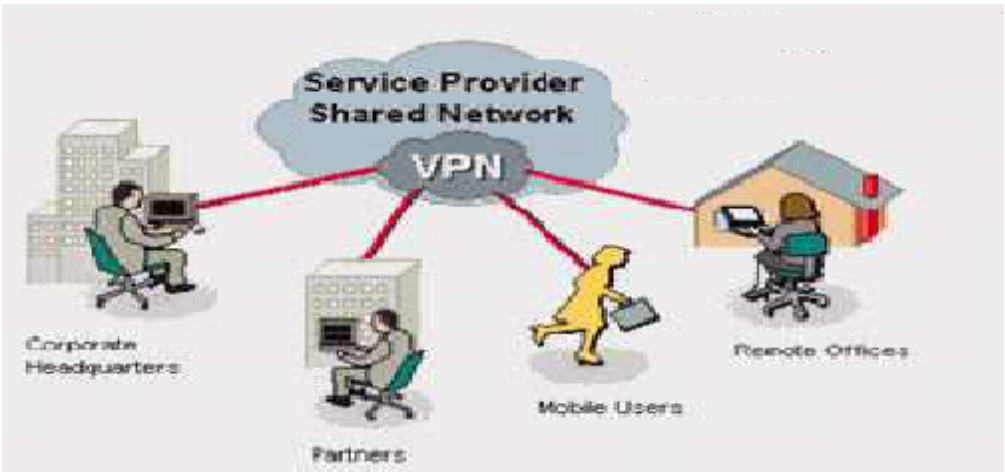
Ante la necesidad de comunicar puntos remotos, y lo costoso que significaría tener una WAN (Wide Area Network) que significaría tirar líneas entre cada sucursal de una empresa X se ideo la forma de utilizar redes publicas para comunicar estas sucursales.

Para poder habilitar redes privadas distribuidas para comunicar de forma segura cada uno de los nodos de una red pública hay una necesidad de aplicar algún sistema de seguridad, debido a que los datos de la empresa son valiosos, y no deben ser interceptados.

Con una Red Privada Virtual (VPN), los usuarios remotos, que pertenecen a una red privada, pueden comunicarse de forma libre y segura entre redes remotas a través de redes públicas.

Una VPN normalmente usa la red Internet como transporte para establecer enlaces seguros, extendiendo las comunicaciones a oficinas aisladas. Significativamente, decrece el coste de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante Acceso Remoto a Servidores.

Una Red Privada Virtual (VPN) transporta de manera segura por Internet por un túnel establecido entre dos puntos que negocian un esquema de encriptación y autentificación para el transporte. Una VPN permite el acceso remoto a servicios de red de forma transparente y segura con el grado de conveniencia y seguridad que los usuarios conectados elijan. Las VPN están implementadas con firewalls, routers para lograr esa encriptación y autentificación.



Descripción de VPN

Una Red Privada Virtual (VPN) consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el *Point−to−Point Protocol*, también conocido como PPP, un protocolo de acceso remoto, y posteriormente enrutados o encaminados

sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP.

Una Red Privada Virtual es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

Un escenario típico de uso de VPN es una compañía que tiene una serie de trabajadores remotos a los que quiere permitir el acceso a sus servicios. Si esto es lo único que se desea hacer, no hace falta una VPN: basta con utilizar tecnologías como Firewalls o proxys. Ahora bien, una VPN permite, además que la comunicación se realice por un canal seguro. Por seguro se entiende que la comunicación cumpla estos requisitos:

Confidencialidad: Los datos que circulan por el canal sólo pueden ser leídos por emisor y receptor. La manera de conseguir esto es mediante técnicas de encriptación.

Autentificación: Emisor y receptor son capaces de determinar de forma inequívoca sus identidades, de tal manera que no exista duda sobre las mismas. Esto puede conseguirse mediante firmas digitales o aplicando mecanismos desafío−respuesta.

Integridad: Debe garantizarse la integridad de los datos, esto es, que los datos que le llegan al receptor sean exactamente los que el emisor transmitió por el canal. Para esto se pueden utilizar firmas digitales.

No repudio: Cuando un mensaje va firmado, el que lo firma no puede

negar que el mensaje lo emitió él.

Existen varias formas de garantizar la existencia de un canal seguro entre emisor y receptor. Algunas de ellas pueden ser el uso de extranets, o bien proteger los servidores propios mediante passwords utilizando mecanismos de autentificación de terceras partes, o incluso utilizar líneas privadas para todas las comunicaciones que requieran un canal seguro. Sin embargo, utilizar tecnología VPN tiene una serie de ventajas con respecto a otras soluciones, como pueden ser:

Ahorro en costes de comunicaciones. En el caso de usuarios remotos, cuando quieren utilizar los servicios de la compañía no necesitan conectarse directamente a los servidores de la compañía, sino que se conectan directamente por su conexión a Internet. Por otro lado, la compañía puede utilizar sus líneas de conexión a Internet para realizar transmisiones de datos, sin necesidad de contratar líneas privadas adicionales.

Ahorro en costes operacionales. Usando VPN para dar acceso a los usuarios, la compañía puede deshacerse de los bancos de módems y de los servidores para acceso remoto, de manera que ya no habrá que administrar

esos dispositivos.

Entorno de trabajo independiente de tiempo y lugar a un coste reducido. Mediante el uso de una VPN, los trabajadores remotos pueden acceder a los servicios de la compañía sin necesidad de realizar llamadas a larga distancia ni utilizando líneas privadas.

Los servicios de la compañía están disponibles siempre. Una VPN permite a las compañías ofrecer servicios globales. Los trabajadores remotos pueden conectarse a la red interna sin importar dónde estén situados físicamente. Esto implica que pueden utilizar los servicios de la LAN de la compañía, como impresoras o archivos compartidos, sin problemas.

Una compañía puede ofrecer servicios a sus socios mediante una VPN, ya que la tecnología VPN permite accesos controlados y proporciona un canal seguro para compartir información de negocios.

Así, las VPN constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y lo escalable del acceso a través de Internet. Esta combinación hace de las Redes Privadas Virtuales o VPNs una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier organización.

Las VPNs permiten:

- La administración y ampliación de la red corporativa al mejor costo−beneficio.
- La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas.

Los requisitos indispensables para esta interconectividad son:

- Políticas de seguridad.
- Requerimiento de aplicaciones en tiempo real.
- Compartir datos, aplicaciones y recursos.
- Servidor de acceso y autentificación.
- Aplicación de autentificación.

Implementación

En una primera aproximación, se puede implementar una VPN mediante *mecanismos hardware.* Éstos se basan normalmente en routers con encriptación, que tienen la ventaja de ser lo más parecido a equipos "plug&play". Su única tarea es encriptar y desencriptar las tramas que pasan a través de ellos, por lo que tienen buenas prestaciones y no introducen demasiado retardo en la red. Ahora bien, no tienen tanta flexibilidad como los sistemas basados en software. Otra aproximación son *sistemas basados en Firewalls*. Estos sistemas aprovechan las ventajas del firewall como la restricción de acceso a la red o generación de registros de posibles amenazas, y ofrecen además otros como traducción de direcciones o facilidades de autentificación fuerte. Ahora bien, el hecho de insertar el servicio de VPN dentro de un firewall puede afectar en mayor o menor medida al rendimiento del sistema, lo que puede o no ser un problema dependiendo de nuestras necesidades. Si esto se convierte en un problema, algunos fabricantes de firewalls ofrecen procesadores dedicados a encriptación para minimizar el efecto del servicio VPN en el sistema. Por último, los *sistemas puramente software* son ideales en los casos en los que los dos extremos de la comunicación no pertenecen a la misma organización, o cuando aun estando dentro de la misma organización, las tecnologías de routers y/o firewalls difieren. Esta solución permite mayor flexibilidad en cuanto a la decisión de qué tráfico enviar o no por el túnel seguro, pudiendo decidir por protocolo o por dirección, a diferencia de los sistemas hardware, que normalmente sólo permiten decidir por dirección. Puede ser conveniente en situaciones donde la VPN es útil en algunos casos (consultas a una base de datos) pero irrelevante en otros (navegación normal por la web). También es útil en los casos en los que la conexión se realiza por líneas

lentas. Ahora bien, no todo son ventajas. Los sistemas software son difíciles de administrar, ya que requieren estar familiarizados con el sistema operativo cliente, la aplicación VPN y los mecanismos de seguridad adecuados. Y algunos paquetes VPN requieren cambios en las tablas de encaminamiento y los esquemas de traducción de direcciones. Sin embargo, las fronteras entre estas tres aproximaciones se van diluyendo conforme pasa el tiempo. Existen fabricantes que proporcionan soluciones basadas en hardware, pero que incluyen clientes software para VPN e incluso características que sólo se encontraban en los sistemas basados en firewalls. Por otro lado, la introducción del protocolo IPSec está facilitando la mezcla de distintos productos VPN.

En cuanto a los *algoritmos de encriptación*, se puede utilizar prácticamente cualquiera: desde la encriptación de 40 bits que lleva W9x por defecto a algoritmos más elaborados como triple DES.

La *autentificación de usuarios* se realiza utilizando cualquier técnica, desde métodos software a passwords dinámicos tanto software como hardware.

Problemas de VPN

VPN puede provocar una sobrecarga en la conexión de red debido a la encriptación utilizada. La mayoría de dispositivos VPN, tanto software como hardware podrán manejar encriptación para velocidades de conexión 10baseT. Para conexiones más lentas, como los módems, el procesamiento puede ser más rápido que la latencia de la red. Muchas veces las bajas prestaciones dependen más de la pérdida de paquetes provocada por una mala conexión a Internet que por la sobrecarga debida a la encriptación.

Requisitos

Para poder establecer una VPN, ya sea entre varias subnets o entre una LAN y un host "móvil", son necesarios algunos requisitos:

Requisitos Hardware: Es necesario tener un encaminador o router a internet, que va a ser la pieza

clave de la VPN. Cualquier tipo de encaminador, en principio, sería suficiente. Por supuesto, también es necesario el soporte físico para la comunicación entre las dos subnets o entre la LAN y el host "móvil".

Requisitos Software: Se debe tener un sistema de transporte `opaco' entre los dos puntos a unir

por la VPN. Esto es, que debe actuar sólo como transporte, sin `mirar' dentro de los datos que va a transportar. El transporte debe asegurar una cierta calidad de servicio, si esto es posible, y debe proporcionar seguridad (encriptación) a los datos. Además será necesario que junto con los encaminadores (ya comentados en los requisitos hardware) se disponga de algún tipo de encapsulamiento disponible para que la red de transporte intermedio (ya sea dialup, Internet u

otro tipo de red) sea capaz de entregar los paquetes entre los desencaminadores de la VPN, sin tener que `mirar' dentro de los datos de la transmisión que, además, podrían estar encriptados. Otro de los requisitos más importantes a la hora de construir una VPN es el hecho de que las aplicaciones deberían seguir funcionando perfectamente como hasta ahora habían funcionado. Es decir, la creación de la VPN debería ser *transparente a las aplicaciones* que se estén usando o se puedan usar en cualquiera de las redes que forman la VPN.

Tipos de conexión VPN

Crear una VPN es muy similar a establecer una conexión de acceso telefónico a una red punto a punto. Hay dos tipos de conexiones VPN: la conexión de acceso remoto VPN y la conexión router to router.

Conexión de Acceso Remoto.

Una conexión de acceso remoto es realizada por un cliente de acceso remoto, o un usuario de un computador que se conecta a una red privada. El servidor de VPN provee de acceso a los recursos del servidor VPN, o a la red completa a la cual el servidor VPN esta conectado. Los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto. El cliente de acceso remoto (cliente VPN), se autentifica al servidor de acceso remoto (el servidor VPN), y para una mutua autentificación, el servidor se autentifica ante el cliente.

Conexión VPN Router−to−Router

Una conexión VPN router−to−router Es realizada por un router, y este conecta 2 porciones de una red privada. El servido VPN provee una conexión ruteada hacia la red en la cual el servidor VPN esta conectado. En una conexión VPN router to router, los paquetes enviados desde cualquier router a través de la conexión VPN típica, no se origina en los routers. El router que realiza la llamada (Cliente VPN), se autentifica ante el router que responde (El servidor VPN), y para una autentificación mutua el router que responde, se autentifica ante el router que realiza la llamada.

Propiedades de la Conexión VPN

La conexión VPN, tiene las siguientes partes.

Encapsulacion

Autentificación

Encriptación de datos

Asignamiento de servidor de nombres y dirección.

Encapsulación

La tecnología VPN, provee una vía de encapsulamiento datos privados con encabezados que permiten a los datos pasar por el tráfico inter−redes.

Autentificacion

La autentificación para conexiones VPN, toma dos formats

Autentificacion de usuario

para que la conexión VPN sea establecida, El servidor VPN autentifica al cliente VPN intentando la conexión y verificando que el cliente VPN tiene los permisos apropiados. Si se acepta, se usa la autentificación mutua, el cliente VPN también autentifica al servidor VPN proveyendo una protección ante servidores VPN enmascarados

Autentificación e integración de datos

Para verifica que los datos enviados en la conexión VPN, son originados al otro lado de la conexión y no han sido modificados en el camino, los datos contienen una suma de comprobación criptográfica basaba en un código conocido solo por el emisor y el receptor.

Encriptación de datos

Para asegurar la confiabilidad de los datos que son enviados a través del transito inter redes compartido o publico, este es encriptado por el emisor, y desencriptado por el receptor. El proceso de encriptación y desencriptación depende de que el emisor y el receptor tengan conocimiento de una llave de encriptación conocida por ambos

Los paquetes interceptados a lo largo de la conexión VPN en el transito inter red, son ilegibles para quien no conozca la llave de encriptación. La longitud de la llave de encriptación es un parámetro importante de seguridad. Técnicas computacionales puedes ser usadas para determinar la llave de encriptación, como estas técnicas requieren mayor poder computacional y tiempo de cálculos mientras mas larga sea la llave de encriptación, por lo tanto, es muy importante usar una llave lo mas larga posible. Además mientras más información es encriptada con la misma llave, es mas facial de descifrar los datos encriptados. Con algunas técnicas de encriptación, se le da la opción de configurar cuan a menudo las llaves de encriptación son cambiadas durante una conexión.

Asignamiento servidor de nombres y dirección

Cuando un servidor VPN es configurado, se crea una interfaz virtual que representa la interfaz en la cual todas las conexiones VPN son hechas. Cuando un cliente VPN establece una conexión, una interfaz virtual es creada en el cliente VPN que representa la interfaz conectada al servidor VPN.

La interfaz virtual en el cliente de VPN se conecta con la interfaz virtual en el servidor de VPN creando una conexión VPN punto a punto.

Las interfaces virtuales del cliente VPN y del servidor VPN se deben asignar direcciones IP. La asignación de estas direcciones es hecha por el servidor de VPN. Por defecto, el servidor de VPN obtiene a las direcciones IP para sí mismo y a clientes de VPN usando Dynamic Host Configuration Protocol (DHCP). También se puede configurar una unión estática de las direcciones IP definidas por una identificación de la red IP y una mascara de subred.

Conexiones VPN basadas en Internet e Intranet

Las conexiones VPN pueden ser utilizados siempre que una conexión segura punto a punto necesite conectar otros usuarios o redes. Típicamente las conexiones vpn son basadas en Internet o en Intranet.

Las conexiones VPN basadas en Internet

Usando una conexión Internet−basada de VPN, usted puede evitar llamadas larga distancia y 1−800 mientras que se aprovecha de la disponibilidad global del Internet.

Acceso remoto sobre Internet

Antes que un cliente de acceso remoto tenga que hacer una llamada distancia o 1−800 a un corporativo o el servidor del acceso de red (NAS), el cliente puede llamar al ISP local. Usando la conexión física establecida a la ISP local, el cliente del acceso remoto inicia una conexión de VPN a través del Internet al servidor de VPN de la organización. Cuando se crea la conexión de VPN, el cliente del acceso remoto puede tener acceso a los recursos del Intranet privado.

fig. Conexión VPN, conectando un cliente remoto a una red privada.

Conectando redes sobre Internet

Cuando las redes están conectadas sobre Internet, router reenvía los paquetes a otro router a través de una conexión de VPN. Hacia los routers la VPN funciona como vinculo de capa data link

fig. Conexión VPN de dos sitios remotos a través de Internet.

Conectando redes, usando enlaces WAN dedicados

Antes que usar un costoso enlace dedicado larga distancia WAN entre las oficinas, los routers de la oficina están conectadas a Internet usando enlaces dedicados locales WAN a una ISP local. Una conexión VPN router to router por cualquier router a través del Internet. Cuando están conectadas, los router pueden remitir tráfico dirigido o trafico de protocolo de ruteo hacia otro usando la conexión VPN.

Conectando redes, usando enlaces WAN acceso telefónico

Antes que tener un router de la sucursal realizando llamadas larga distancia o 1−800 a un corporativo, el router de la sucursal, puede llamar a su isp local. Usando la conexión establecida al ISP local, una conexión router to router es iniciada por el router de la sucursal al router de la oficina corporativa a través de Internet. El router de la sucursal que actúa como servidor de VPN se debe conectar con un ISP local usando un enlace WAN dedicado. Es posible tener ambas oficinas conectadas con el Internet usando un enlace WAN de marcado manual. Sin embargo, esto es solamente factible si la ISP soporta el ruteo a los clientes según requerimientos de llamada, El ISP llama al router del cliente cuando un IP DATAGRAM debe ser entregado al cliente. El ruteo a los clientes según requerimientos de llamada no es apoyado extensamente por los ISPs.

Conexiones VPN basadas en Intranet

Las Conexiones VPN basadas en Intranet aprovechan la conectividad del IP en un Intranet de la organización.

Acceso Remoto sobre Intranet

en algunos intranets de una organización, los datos de un departamento, tales como los del departamento de recursos humanos, es tan delicado que el segmento de la red del departamento este desconectado físicamente del resto del Intranet de la organización. Mientras que esto protege los datos del departamento, crea problemas de accesibilidad hacia la información para el resto de los usuarios no conectados físicamente con el segmento de la red separada. Las conexiones de VPN permiten que el segmento delicado de la red del departamento sea conectado físicamente con el Intranet de la organización pero separado por un servidor VPN. El servidor de VPN no proporciona una conexión ruteada directa entre el Intranet corporativo y el segmento de la red separada. Los usuarios en el Intranet corporativo con los permisos apropiados pueden establecer una conexión de acceso remoto VPN con el servidor de VPN y pueden acceder a los recursos protegidos de la red delicada del departamento. Además, toda la comunicación a través de la conexión de VPN se cifra para confidencialidad de los datos. Para esos usuarios que no tengan permisos de establecer una conexión de VPN, el segmento de la red separada esta oculto para ellos.

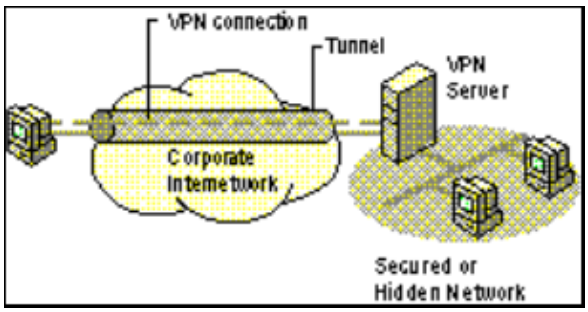


fig. Conexión VPN, permitiendo el acceso remoto a una red segura sobre Intranet

Conectando redes sobre un Intranet

Se puede también conectar dos redes sobre un Intranet usando una conexión router to router VPN. Este tipo de conexión VPN puede ser necesario, por ejemplo, para dos departamentos en lugares separadas, en que los datos son altamente delicados a comunicarse con uno a. Por ejemplo, el departamento de finanzas puede necesitar comunicarse con el departamento de los recursos humanos para intercambiar la información de la nómina de pago. El departamento de finanzas y el departamento de los recursos humanos están conectados a una Intranet común con las computadoras que pueden actuar como clientes de o servidores VPN. Cuando se establece la conexión VPN, los usuarios en las computadoras en cualquier red pueden intercambiar datos sensibles a través del Intranet corporativo.

fig. Conexión VPN conectando dos departamentos sobre Intranet

Conexión combinada VPN Internet e Intranet

Una VPN es una herramienta de red que puede proporcionar una conexión segura punto a punto cualquier manera usted ve ajuste. Una conexión combinada menos común del Internet y del Intranet VPN, llamada una conexión del paso VPN, permite a cliente del acceso remoto conectarse con una Intranet de la compañía para tener acceso a los recursos de otra Intranet de una compañía usando el Internet. En este panorama con, una conexión de acceso remoto VPN pasa por una Intranet y el Internet para tener acceso a una segunda Intranet.

fig. Conexión VPN de paso

Protocolos de VPN

Han sido implementados varios protocolos de red para el uso de las VPN. Estos protocolos intentan cerrar todos los hoyos de seguridad inherentes en VPN. Estos protocolos continúan compitiendo por la aceptación, ya que ninguno de ellos ha sido más admitido que otro.

Estos protocolos son los siguientes:

Point−to−Point Tunneling Protocol (PPTP): PPTP es una especificación de protocolo desarrollada por varias compañías. Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP. La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su fallo a elegir una única encriptación y autentificación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

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 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 Canadá) o 40 bits (para el resto de usuarios).

Layer Two Tunneling Protocol (L2TP): El principal competidor de PPTP en soluciones VPN fue L2F, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP. L2TP existe en el nivel de enlace del modelo OSI. L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

L2TP encapsula datos de aplicación, datagramas de protocolos Lan e información de tramas punto a punto dentro de un paquete que, además contiene una cabecera de entrega, una cabecera IP y una cabecera Generic Routing Encapsulation (GRE).

La cabecera de entrega mantiene la información de tramas necesaria para el medio a través del cual se establece el túnel, sea una red Frame Relay o IP. La cabecera IP contiene, entre otros datos importantes, las direcciones IP de fuente y destino. GRE, finalmente, incluye extensiones como, por ejemplo, la de señalización de llamada, que añaden inteligencia de conexión.

Para formar un túnel, L2TP emplea dos funciones básicas: LAC y LNS. LAC (L2TP Concentrador de acceso) realiza funciones de servidor de línea para el cliente, mientras que LNS (L2TP servidor de red), como su nombre indica, actúa como servidor de red en el lado del servidor.

En un escenario en el cual L2TP resida en el concentrador de accesos de un punto de presencia del operador, la función LAC iniciará un túnel cuando un usuario remoto active una conexión PPP con un proveedor de servicios Internet. Después de realizar la autenticación inicial, LAC acepta la llamada, añade las diferentes cabeceras comentadas a la carga útil (payload) de PPP, y establece un túnel hacia el dispositivo de terminación LNS del extremo de la red corporativa. Este dispositivo puede tratarse de un servidor de acceso remoto, un conmutador VPN especializado o un router convencional.

Una vez establecido el túnel, un servicio de nombres de seguridad, como ACE/Server de Security Dynamics o el servicio de nombres y seguridad integrado en Windows NT, autentifica las identidades del usuario y del punto final. LNS acepta el túnel y establece una interfaz virtual para el payload PPP. A las tramas entrantes se les elimina la información de cabecera de L2TP y se las procesa como si fueran tramas PPP normales. Entonces se asigna a la sesión un dirección IP corporativa local.

Internet Protocol Security (IPsec): IPsec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec existe en el nivel de red en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet.

Válido tanto para IPv4 como para IPv6, permite definir los protocolos de seguridad, los algoritmos criptográficos y las claves manejadas entre los sistemas que se comunican.

Una de las características más importantes de IPSec es su compatibilidad con las redes IP actuales.

IPSec puede dividirse básicamente en IP Security Protocols, mecanismos de gestión de claves, mecanismo de creación de asociaciones seguras y algoritmos criptográficos para autenticación y cifrado. Los primeros son los protocolos de seguridad propiamente dichos que definen la información que se ha de añadir a la cabecera de un paquete IP para proporcionar los servicios de seguridad requeridos. Dichos protocolos son AH (Authentication Header) y ESP (Encapsulating Security Payload).

La gestión de claves puede ser manual o automática. La gestión automática de claves se realiza mediante IKE (Internal Key Exchange).

Los mecanismos criptográficos que emplea IPSec son intercambio de claves basado en el algoritmo Diffie−Hellman, criptografía de clave público, algoritmos simétricos de cifrado de datos (como DES, IDEA...), algoritmos hash con clave (HMAC, por ejemplo), junto con otros más tradicionales (como MD5 y SHA), para proporcionar autenticación de paquetes, y manejo de certificados digitales.

IPSec combina estos mecanismos criptográficos para ofrecer confidencialidad, integridad y autenticidad a los datagramas IP. Es importante hacer notar que IPSec no define los algoritmos específicos a utilizar, sino que proporciona un mecanismo para que las entidades negocien aquellos que emplearán en su comunicación. Por otro lado, según recoge el estándar, todas las implementaciones de IPSec deberán soportar un conjunto mínimo de algoritmos que garantice la interoperatividad entre fabricantes.

Paquetes IPSec

IPSec define un nuevo conjunto de cabeceras que se añaden al datagrama IP. Esas nuevas cabeceras se colocan después de la cabecera IP y antes de la de nivel de transporte. Existen dos tipos de cabeceras:

- Authencation Header (AH): cuando es añadida asegura la integridad y la autenticidad de los datos que transporta el datagrama IP y de los campos invariables de la propia cabecera IP. AH no proporciona confidencialidad.
- Encapsulating Security Protocol (ESP): esta cabecera, cuando se añade al datagrama IP, proporciona confidencialidad, integridad y autenticidad de los datos transmitidos.
- IPSec propociona dos modos de operación:
    - ♦ Modo transporte: en este modo la cabecera IP del paquete original no se modifica. Este modo es utilizado entre dispositivos finales de una comunicación que cumplen el estándar IPSec.
    - ♦ Modo túnel: en este caso el datagrama IP entero es encapsulado dentro de otro datagrama IP. Este modo permite que un dispositivo actúe como proxy IPSec en beneficio de máquinas que no soporten el estándar.

Los dos sistemas comunicantes deben ponerse de acuerdo en los algoritmos a usar y en la clave de sesión que han de compartir. Una vez realizado este proceso se puede decir que se ha creado una asociación segura entre las dos entidades. Durante este proceso se crea un túnel seguro entre los dos sistemas y después se negocia la asociación segura para IPSec. El proceso de crear un túnel seguro consiste en una autenticación mutua y el establecimiento de una clave compartida. Existen diversos mecanismos de autenticación, entre ellos se encuentran:

- Pre−shared key: en este caso la misma clave es preinstalada en ambos sistemas. La autenticación se realiza basándose en este secreto compartido.
- Criptografía de clave pública.
- Firma digital

mppe (Microsoft Point−to−Point Encryption): protocolo que sirve para encriptar los datos de las transmisiones.

mschap: tanto la versión 1 como la número 2, que sirve para establecer la conexión segura y el intercambio de las claves. En la versión 1 se descubrió una vulnerabilidad, que todavía no ha sido confirmada, que le obligó a evolucionar hasta la versión 2 (actual).

IPIP: protocolo de encapsulamiento de IP sobre tramas IP. Este protocolo, que puede parecer poco útil, nos sirve para hacer el tunneling que se marca como uno de los requisitos de VPN.

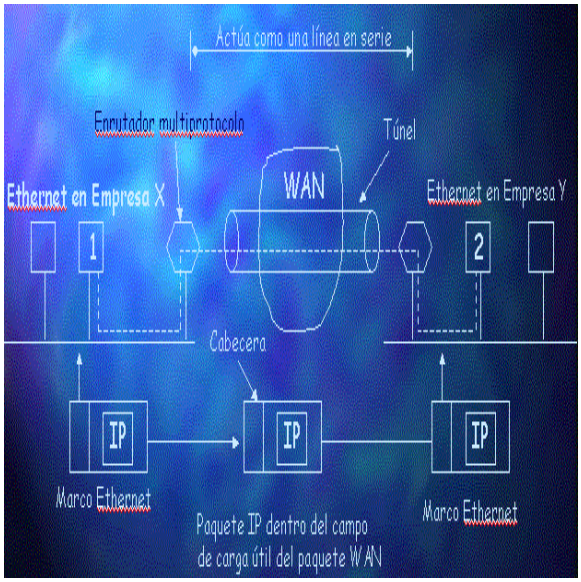
IP−GRE: protocolo de encapsulamiento de otros protocolos sobre IP. En un principio el tráfico que

puede encapsular IP−GRE sería cualquiera. Es útil en el sentido de que podemos tener redes de otro tipo además de IP (como por ejemplo IPX) y funcionar con una VPN de igual manera. Más adelante se verá como IPSec sirve para este mismo fin (a la vez que proporciona otros muchos servicios).

SOCKS Networks Security Protocol: El sistema SOCKS proporciona otra alternativa a los protocolos de VPN. SOCKS se aloja en el nivel de sesión de OSI. Como SOCKS trabaja en un nivel OSI más alto que los protocolos anteriores, permite a los administradores limitar el tráfico VPN.

Tunneling

El manejo del caso general de lograr la interacción de dos redes diferentes es difícil. Sin embargo, hay un caso especial común que puede manejarse. Este caso es cuando el host de origen y el de destino están en la misma clase de red, pero hay una red diferente en medio. Como ejemplo, piense en una empresa X con una ethernet basada en TCP / IP, otra ethernet de una empresa Y basada igualmente en TCP / IP y una WAN PTT en medio, como lo ilustra la figura 1.



El principio de funcionamiento para el proceso túnel es el siguiente: para enviar un paquete IP al host 2, el host 1 construye el paquete que contiene la dirección IP del host 2, lo inserta en un marco ethernet dirigido al router multiprotocolo que enlaza la empresa X, y lo pone en el ethernet. Cuando el router multiprotocolo recibe el marco, retira el paquete IP, lo inserta en el campo de carga útil del paquete de capa de red de la WAN, y dirige este último a la dirección de la WAN del router multiprotocolo que enlaza con la empresa Y. Al llegar ahí, el router retira el paquete IP y lo envía al host 2 en un marco ethernet.

La WAN puede visualizarse como un gran túnel que se extiende de un router multiprotocolo al otro. El paquete IP simplemente viaja de un extremo del túnel al otro. No tiene que preocuparse por lidiar con la WAN. Tampoco tiene que hacerlo los hosts de cualquiera de los ethernet. Sólo el router multiprotocolo tiene que entender los paquetes IP y WAN.

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos.

El proceso de comunicación en las tecnologías de túneles

El túnel lleva datagramas entre PAC Y PNS. Muchas sesiones son multiplexadas sobre un mismo túnel.

PAC: (PPTP ACCESS CONCENTRATOR) Concentrador de acceso PPTP. Dispositivo que asocia una o mas líneas capaces de soportar PPP (point to point protocol) y manejo del protocolo PPTP. PAC necesita solamente TCP/IP para pasar sobre el tráfico de una o mas PNS.

PNS: (PPTP Network Server) Es el servidor para red de PPTP. Sirve para operar sobre computadoras de propósito general y plataformas de servidores. PNS dirige la parte del servidor del protocolo PPTP m

ientras PPTP confía completamente TCP/IP y es independiente de la interfaz de Hardware, el PNS puede usar cualquier combinación de hardware de interfaz IP, incluyendo dispositivos LAN y WAN.

PPTP está implementado para PAC y PNS. Existen actualmente relacionados muchos PAC Y PNS, un PAC puede proveer servicio a muchos PNS. Por ejemplo un proveedor de servicio internet puede elegir PPTP para un número de clientes de red privada y crear VPNs para ellos. Cada red privada podrá operar uno o mas PNSs. Un PNS podrá asociarse con muchos PACs para concentrar el tráfico desde muchos sitios de diferente ubicación Geográfica.

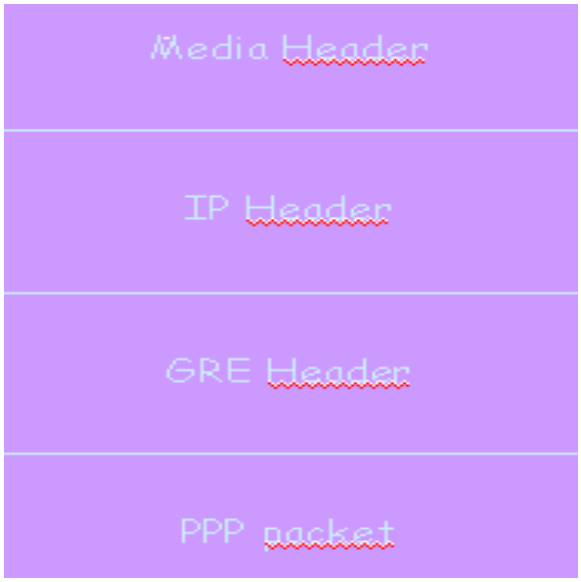
PPTP usa una forma parecida a GRE (Generic Routing Encapsulation) para llevar los paquetes PPP de usuario. Permite a bajo nivel controlar la congestión y flujo que va a llevarse a través de los túneles usados para llevar los datos de usuario entre PAC y PNS. Este mecanismo permite la eficiencia del uso del ancho de banda disponible para los túneles y evita retransmisiones innecesarias y desbordamiento en los buffers.

PPTP requiere el establecimiento de un túnel para cada comunicación PNS−PAC. Este túnel es usado para llevar todos los paquetes PPP de sesión de usuario participando un par determinado de PNS y PAC. Una llave está presente en el encabezado GRE indicando a cual sesión en particular pertenece el paquete PPP. De esta manera los paquetes PPP son multiplexados y demultiplexados sobre un túnel simple entre el PNS y PAC dado. El valor a usar en el campo de la llave es establecido por la llamada, estableciendo el procedimiento mediante el cual toma el control de la conexión.

El encabezado GRE también contiene la secuencia de información que ha sido usada para desempeñar algún nivel de control de congestión y detección de errores sobre el túnel. Luego la conexión de control es usada para determinar la tasa y los parámetros de almacenamiento temporal que han sido usados para regular el flujo de paquetes PPP para una sesión particular sobre el túnel.

Estructura de los paquetes IP transmitidos a través de los túneles

Los Paquetes IP transmitidos sobre los túneles entre PAC y PNS tienen la siguiente estructura General:



VPN Dinámicas

Conceptos de las VPN Dinámicas

Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios. Entonces, ¿Cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo para permitir un acceso libre a la información?, es decir, ¿Cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperatibilidad y facilidad de uso?

La respuesta apropiada se encuentra en la utilización de **VPNs Dinámicas**. A diferencia de una VPN tradicional, una VPN Dinámica proporciona, además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs Dinámicas pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información.

Alguna de las características que se proporciona son las siguientes:

Proporciona una seguridad importante para la empresa.

Se ajusta dinámicamente al colectivo dispar de usuarios.

Permite la posibilidad de intercambio de información en diversos formatos.

El ajuste que hace para cada usuario lo consigue gracias a los diferentes navegadores, aplicaciones, sistemas operativos, etc...

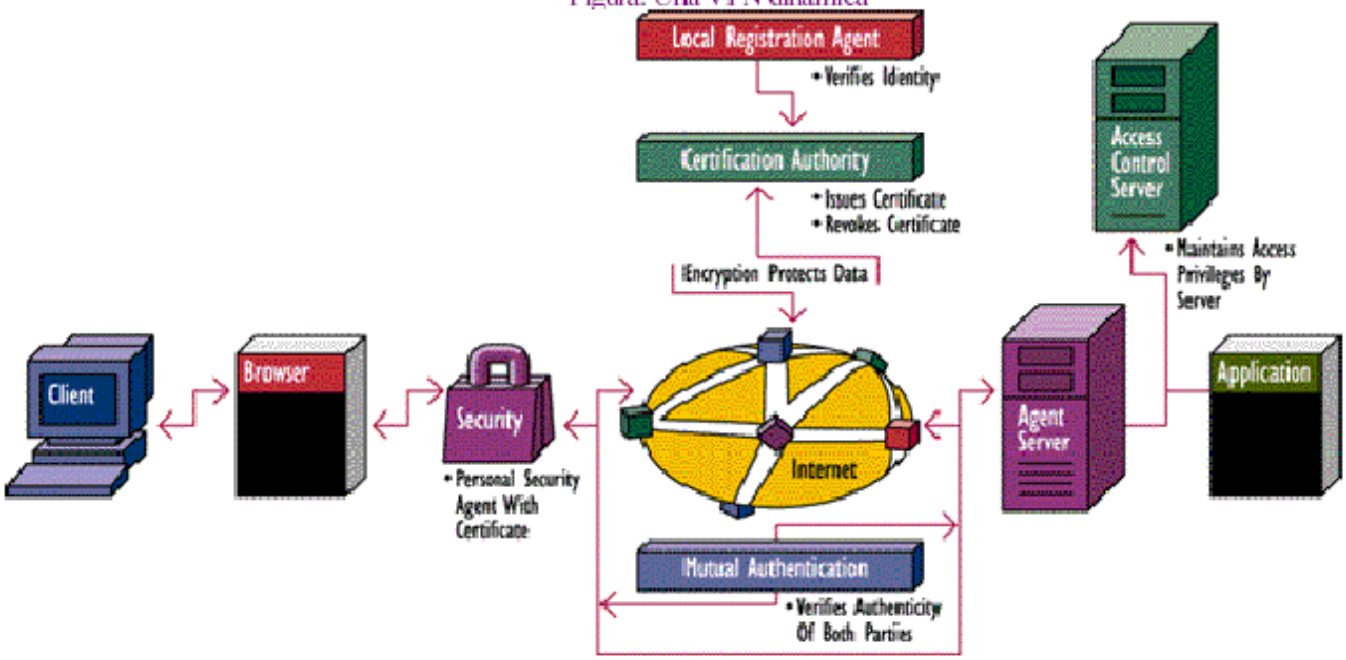
Permite a los usuarios unirse a distintos grupos, así como a los administradores asignar identidades en un entorno simple pero controlado.

Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

Funcionamiento de las VPN Dinámicas

Las VPNs Dinámicas constan de una plataforma de seguridad de red y un conjunto de aplicaciones para usar en la plataforma de seguridad.

Figura: Una VPN dinámica



Siguiendo los pasos ilustrados en la figura, un usuario realiza una petición de información a un servidor, por ejemplo, pulsando con su ratón en un hipervínculo. Los pasos seguidos se pueden describir en los siguientes puntos:

Un usuario solicita información usando una aplicación tal como un navegador de Internet, desde un ordenador de sobremesa: El intercambio de información comienza cuando un usuario envía información a otro usuario o solicita información al servidor. En el supuesto de que un usuario haya accedido a un hipervínculo desde dentro de algún documento Web, dicho hipervínculo será seguro y solamente podrá ser accedido por usuarios autorizados.

La aplicación envía y asegura el mensaje: Cuando un cliente y un servidor detectan que se necesita seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectan en un mutuo protocolo de autentificación. Este paso verifica la identidad de ambas partes antes de llevar a cabo cualquier acción. Una vez que se produce la autentificación se asegura el mensaje encriptándolo. Adicionalmente, se puede atribuir un certificado o firma electrónica al usuario.

El mensaje se transmite a través de Internet: Para que la petición alcance el servidor debe dejar la LAN y viajar a través de Internet, lo cual le permitirá alcanzar el servidor en algún punto de la misma. Durante este viaje, puede darse el caso de que atraviese uno o más firewalls antes de alcanzar su objetivo. Una vez atravesado el firewall, la petición circula a lo largo del pasillo Internet hasta alcanzar el destino.

El mensaje recibido debe pasar controles de seguridad: El mensaje se transfiere al servidor. El servidor conoce la identidad del usuario cliente cuando recibe la petición.

Durante la petición, se verifican los derechos de acceso de los usuarios: En una VPN dinámica, el sistema debe poder restringir que usuarios pueden y no pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de información. Esto lo hace usando mecanismos de control, alojados en el *Servidor de Control de Acceso*. De este modo, incluso si un usuario presenta un certificado válido, puede ser que se le deniegue el acceso basándose en otros criterios.

La petición de información es devuelta por Internet, previamente asegurada: El servidor de información encripta la información y opcionalmente la certifica. Las claves establecidas durante los pasos de autentificación mutua se usan para encriptar y desencriptar el mensaje. De esta forma, un usuario tiene su documento asegurado.

Equipos para Redes privadas virtuales

VPN gateway: Dispositivos con un software y hardware especial para proveer capacidad a la VPN.Varias funciones son optimizadas sobre varios componentes de software y hardware.

Algunos ejemplos de esto tenemos Alcatel 7130,Altiga C10, VPN−1 Gateway, Lucent VPN Gateway, Intel Shiva Lan Rover VPN Gateway Plus, TimeStep Permit/Gate 4620 y VPNet VPNware VSU−1010, las cuales incluyen el software y hardware necesario para realizar y administra VPN.

Acatel 7130 Gateways de VPN

Sólo Software: El software está sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN. Algunos ejemplos de esto el Sistema Operativo Windows 9x, ME, NT, 2000 y XP

Basado en Firewall: Funciones adicionales son agregadas al firewall para habilitar capacidades de VPN. Algunos ejemplos de esto son los modelos PIX de Cisco como 506, 515, 525 y 535.

Cisco 535 Secure PIX Firewall 535

Basado en Router: Funciones adicionales son agregadas al router para habilitar capacidades de VPN, las cuales se encuentran en el IOS de los router de Cisco como los modelos 804, 806, 827, 905, 1710, 1720, 1750, 2611, 2621, 2651, 3620, 3640, 3660, 7120, 7140 y 7200.

router cisco serie 7200

Aunque los router son mejores que los concentradores, existen algunos capaces de realizar VPN como los modelos 3005, 3015, 3030, 3060 y 3080.

Concentrador Cisco serie 3000

Bibliografía

Se han revisado las siguientes links de internet para lograr realizar este trabajo.

http://www.vpnlabs.org/

http://www.vpnlabs.org/all−vpn−categories.html

http://www.iec.org/

http://www.microsoft.com

http://www.gulp.org.mx/articulos/vpn.html

http://www.howstuffworks.com

http://www.cisco.com

http://atenea.udistrital.edu.co/egresados/xsepulveda/temas/hernan/

http://www.infor.uva.es/~jvegas/docencia/ar.html

http://lovecraft.die.udec.cl/~jorge/apuntes/

http://www.redes.upv.es/

Conclusiones

Las redes VPN proporcionan principalmente dos ventajas:

- Bajo coste de una VPN:

Una forma de reducir coste en las VPN es eliminando la necesidad de largas líneas de coste elevado. Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio.

Otra forma de reducir costes es disminuir la carga de teléfono para accesos remotos. Los clientes VPN sólo necesitan llamar al proveedor del servicio más cercano, que en la mayoría de los casos será una llamada local.

- Escalabilidad de las VPNs: Las redes VPN evitan el problema que existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet. Internet simplemente deriva en accesos distribuidos geográficamente.

Las redes VPN contraen cuatro inconvenientes:

- Las redes VPN requieren un conocimiento en profundidad de la seguridad en las redes públicas y tomar precauciones en su desarrollo.
- Las redes VPN dependen de un área externa a la organización, Internet en particular, y por lo tanto depende de factores externos al control de la organización.
- Las diferentes tecnologías de VPN podrían no trabajar bien juntas.
- Las redes VPN necesitan diferentes protocolos que los de IP.

Se estima que una solución VPN para una determinada empresa puede reducir sus costes entre un 30% y un 50% comparada con las conexiones punto a punto.