Red privada virtual

«VPN» redirige aquí. Para otras acepciones, véase VPN (desambiguación).

Una **red privada virtual** (RPV), en inglés: ***Virtual Private Network*** (**VPN**), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.[1] Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

La conexión VPN a través de Internet es técnicamente una unión *wide area network* (WAN) entre los sitios pero *al usuario le parece* como si fuera un enlace privado—de allí la designación "virtual private network".[2]

Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación.

- Autentificación y autorización: ¿quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: de que los datos enviados no han sido alterados. Para ello se utilizan funciones de *Hash*. Los algoritmos de hash más comunes son los *Message Digest* (MD2 y MD5) y el *Secure Hash Algorithm* (SHA).
- Confidencialidad/Privacidad: dado que solamente puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como *Data Encryption Standard* (DES), Triple DES (3DES) y *Advanced Encryption Standard* (AES).
- No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.
- Control de acceso: se trata de asegurar que los participantes autenticados tiene acceso únicamente a los datos a los que están autorizados.
- Auditoría y registro de actividades: se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio: se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

Requisitos básicos

- Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- Cifrado de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados. Esta tarea se realiza con algoritmos de cifrado simétrico como DES, 3DES o AES (Advanced Encryption Standard, en sus opciones AES128, AES192 o AES256) que únicamente pueden ser leídos por el emisor y receptor.
- Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.
- Nuevo algoritmo de seguridad SEAL.

Tipos de VPN

Básicamente existen cuatro arquitecturas de conexión VPN:

VPN de acceso remoto[editar]

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones deCABLE físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o *tunneling*.

Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios *multicast*, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de *tunneling*, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil. Se maneja de manera remota.

VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que solamente el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

Implementaciones

El protocolo estándar de facto es el IPSEC, pero también están PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

- Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Fortinet, SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link, Mikrotik, etc.

- Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, GNU/Linux y los Unix en general. Por ejemplo productos de código abierto como OpenSSH, OpenVPN y FreeS/Wan.

En ambos casos se pueden utilizar soluciones de *firewall* («cortafuegos» o «barrera de fuego»), obteniendo un nivel de seguridad alto por la protección que brinda, en detrimento del rendimiento.

Ventajas

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.

Tipos de conexión

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN *router* a *router* es realizada por un *router*, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier *router* no se originan en los *routers*. El *router* que realiza la llamada se autentifica ante el *router* que responde y este a su vez se autentifica ante el *router* que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN *firewall* es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

VPN en entornos móviles

La VPN móvil se establece cuando el punto de terminación de la VPN no está fijo a una única dirección IP, sino que se mueve entre varias redes como pueden ser las redes de datos de operadores móviles o distintos puntos de acceso de una red Wifi.[3] Las VPNs móviles se han utilizado en seguridad pública dando acceso a las fuerzas de orden público a aplicaciones críticas tales como bases de datos con datos de identificación de criminales, mientras que la conexión se mueve entre distintas subredes de una red móvil.[4] También se utilizan en la gestión de equipos de técnico y en organizaciones sanitarias[5] entre otras industrias. Cada vez más, las VPNs móviles están siendo adaptadas por profesionales que necesitan conexiones fiables.[6] Se utilizan para moverse entre redes sin perder la sesión de aplicación o perder la sesión segura en la VPN. En una VPN tradicional no se pueden soportar tales situaciones porque se produce la desconexión de la aplicación, time outs[7] o fallos, o incluso causar fallos en el dispositivo