

Los principios básicos de las redes privadas virtuales

Resumen

El siguiente documento presenta el concepto de red privada virtual (VPN, *Virtual Private Network*), y proporciona una acercamiento inicial a la forma en que se utilizan estas herramientas en el contexto de un marco de seguridad global.

Introducción

La expresión “red privada virtual” se ha vuelto muy frecuente en estos días, pero probablemente muchas personas tengan apenas una idea de su significado.

A menudo se lo asocia con la conectividad de la empresa, cuando trabajadores remotos acceden a la red corporativa, pero actualmente el concepto está ganando popularidad entre los usuarios caseros y las pequeñas organizaciones.

Con una red privada virtual, dos o más ordenadores o redes remotas pueden conectarse entre sí, de forma segura, para formar una red local virtual que utiliza una infraestructura pública como Internet, como medio para transmitir datos internos.

Se denomina red privada virtual porque no se trata de una red física, pero tiene todas las características de una red de área local (LAN, *Local Area Network*).

Este tipo de estructuras benefician a las personas y a las organizaciones, pues les permiten establecer conexiones de red de confianza y utilizar herramientas cooperativas y convencionales, tales como compartir impresoras y archivos, realizar conferencias en red y demás, desde cualquier punto donde haya acceso a Internet.

Además de proporcionar conectividad, las redes privadas virtuales tienen un impacto muy importante en la seguridad: pueden mantener los datos privados, a pesar de estar utilizando puntos de conexión a Internet inseguros, tales como proveedores de servicios de red desconocidos, o acceso inalámbrico en sitios públicos.

Existen muchas maneras de configurar una red privada virtual, y utilizarla para proporcionar acceso compartido e intercambio de datos de forma segura:

- **Acceso punto a punto (*peer to peer*):**

Todos los miembros participan de una red de confianza y utilizan los recursos compartidos que esta ofrece. Los usuarios pueden estar a miles de kilómetros de distancia, y sin embargo podrán ver los archivos de sus colegas como si estuvieran en un ordenador local.

Habitualmente, para ello es necesario que cada miembro de la red tenga acceso a Internet, y ejecute una aplicación especial para redes privadas virtuales que permita el trabajo remoto a través de Internet.

Las redes privadas virtuales pueden usarse de esta forma para, por ejemplo, acceder de forma remota a los documentos guardados en el ordenador del trabajo desde la comodidad del hogar.

- **Redes privadas virtuales con acceso cliente:**

En este caso, el empleado de la compañía se conecta a la red corporativa desde una ubicación remota, por ejemplo, durante un viaje de negocios.

Para ello es necesario implementar un servidor de red privada virtual en la puerta de enlace de la empresa, y ejecutar la aplicación cliente en el ordenador portátil del empleado.

- **Red privada virtual sitio a sitio (*site to site*):**

Las redes de trabajo remotas de múltiples sucursales, por ejemplo, pueden conectarse para crear una única red amplia y homogénea.

- **Red privada virtual interna:**

Los ordenadores pertenecientes a la misma red física se incluyen dentro de una red privada virtual protegida para asegurar los datos en tránsito, o para asignar privilegios específicos a un grupo de usuarios en particular.

Principios

Internet es una red transparente. Esto significa que si una persona tiene las herramientas y el conocimiento adecuados, cualquier comunicación no cifrada puede ser interceptada y leída por terceros no autorizados. Para transmitir datos privados a través de redes públicas de forma segura, los protocolos de la red privada virtual cifran las comunicaciones en el extremo emisor, y las descifran en el extremo receptor, de modo que no puedan ser leídas mientras se encuentran en tránsito.

Esta técnica de encapsulado (*tunneling*) de los datos, es el principio fundamental de las redes privadas virtuales, y amerita una explicación más detallada. El término inglés *tunneling*, se refiere al establecimiento de un canal de transmisión seguro sobre Internet, que permite que los datos viajen a través de un túnel aislado e imaginario, donde no pueden ser accedidos por terceros no autorizados.

Este proceso implica una sucesión de etapas:

1. El paquete de datos original está listo para ser enviado. Se lo denomina paquete viajero, porque será transmitido a través del túnel.
2. Un protocolo de encapsulado, usualmente IPSec (*Internet Protocol security*, Protocolo de seguridad en Internet) o L2TP (*Layer 2 Tunneling Protocol*, Protocolo de encapsulado de capa 2) se aplica al paquete original, para recubrirlo con un nuevo paquete (externo) que lo almacenará y transportará a través del túnel. El proceso de encapsulado es similar a colocar una carta dentro de un sobre, para protegerla mientras está viajando por el sistema postal.
3. En el proceso de encapsulado, el paquete es cifrado utilizando uno de los métodos criptográficos tradicionales. El estándar más poderoso actualmente disponible es AES-256.
4. El paquete es transmitido a través de una red pública, comúnmente Internet, y es descifrado y desencapsulado en el extremo receptor.

Los protocolos de red privada virtual proporcionan una amplia variedad de métodos de autenticación para verificar las identidades de los emisores y receptores de los paquetes en tránsito, de modo que los datos sean transmitidos a los destinos correctos. El método de autenticación más poderoso actualmente es SHA – 512 bit.

Beneficios de una red privada virtual

Desde la perspectiva de un usuario casero, los beneficios principales de una red privada virtual son:

1. Transmisión de datos segura sobre una infraestructura insegura.

El uso de [redes inalámbricas](#) e inseguras representa un riesgo enorme para la confidencialidad de la información que viaja a través de ellas. Este riesgo, puede eliminarse con la implementación y el uso de una red privada virtual. Si bien los datos pueden ser visibles ante miradas curiosas, tales como aplicaciones especialmente diseñadas para capturar la información que circula por la red (*sniffers*) y otras herramientas similares, nadie podrá acceder a ellos excepto el receptor especificado, debido a los requerimientos del cifrado y la autenticación. Terceras partes no autorizadas, solo verán el envoltorio externo (el paquete exterior), y no podrán saborear el dulce (el paquete original) que está dentro de él.

En este caso, la red privada virtual es la red interna protegida, donde los datos inalámbricos se transmiten a través del enlace seguro de un túnel VPN, dentro de una red física insegura (la red inalámbrica).

Existen muchos servicios comerciales que ofrecen seguridad VPN de redes internas para usuarios de conexiones inalámbricas, por ejemplo [JWire](#).

2. La habilidad para crear una red de confianza y compartir recursos.

Internet permite conectar personas, y una red privada virtual puede complementar esta función, proporcionando una forma segura y conveniente para implementar una red privada y acceder a los datos almacenados desde cualquier parte del mundo. Existen muchas soluciones gratuitas y fáciles de usar que permiten establecer y compartir una red privada virtual con amigos, tales como [Hamachi](#) y [OpenVPN](#).

Conclusiones

Las redes privadas virtuales ofrecen seguridad, escalabilidad y conectividad a un medio de comunicación inherentemente inseguro como Internet, creando un canal cifrado y aislado que pueden utilizar tanto los usuarios particulares como las empresas. Sin embargo, hay que tener en cuenta que las aplicaciones indeseadas pueden llegar tan lejos como los datos legítimos. Por lo tanto, es necesario utilizar cortafuegos y soluciones contra códigos maliciosos, además de seguir las prácticas de seguridad recomendadas para navegar por Internet.