

Redes Privadas Virtuales

Resumen

Este artículo permite dar un vistazo a una de las herramientas que esta revolucionando el mundo de las comunicaciones en lo que a redes se refiere. Esta herramienta son las Redes Privadas Virtuales, que son redes que ofrecen alta seguridad y bajos costos usando la infraestructura de redes públicas como Internet e Intranet.

Palabras claves:

PPP: Protocolo Punto-Punto

PPTP: Protocolo de Tunelado Punto-Punto

RPV: Redes Privadas Virtuales

Tunelado

Virtual Private Network

Abstract

This article shows one of the tools that represents a turning point in the world of communications regarding networks. This tool is the Virtual Private Networks, which are networks that offer high security and low-cost infrastructure using public networks such as Internet and Intranet.

Keywords:

PPP: Point-Point Protocol

PPTP: Point-Point Tunneling Protocol

VPN: Virtual Private Network

Tunneling

Introducción

Hoy en día, las empresas y gobiernos usan la red Internet como una herramienta más, confiándole información importante.

El problema está en que no es una red segura y es 'fácil' acceder a información confidencial que en malas manos puede ser peligrosa. Por este motivo, en los últimos años se le da mucha importancia a la seguridad, el uso de la encriptación es común y las empresas buscan soluciones lo más eficaces y baratas posibles a la inseguridad de Internet. Para dar solución a estas demandas surgieron las Redes Privadas Virtuales. [1]

Una red privada virtual 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 Protocolo Punto a Punto (en Inglés Point to Point Protocol: PPP), un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP (Protocolo de tunelado Punto-Punto) [2] [3].

De esta forma una Red Privada Virtual ofrece conexiones transparentes y seguras a través de Internet. Se trata de una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas IP. Estas redes permiten conectar tele-trabajadores, empleados móviles, oficinas y delegaciones separadas geográficamente, socios y clientes, de una forma relativamente barata y muy segura. Las empresas obtienen de esta manera reducción de gastos, aumentan su seguridad y ven facilitada la compartición de recursos entre delegaciones. [1]

¿Qué es una Red Privada Virtual?

Una Red Privada Virtual (RPV) 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. [3]

De esta forma, una RPV consiste de un conjunto de sistemas o dispositivos interconectados a través de canales seguros, sobre una red pública, permitiendo el acceso remoto de los recursos y servicios de la red de forma transparente y segura como si los usuarios estuvieran conectados de forma local.

Ofrece una alternativa sobre el acceso remoto tradicional y líneas dedicadas ya que utiliza los canales de comunicación ya existentes de la red de redes (Internet) permitiendo conectar usuarios remotos mediante el uso de servidores de RPV habilitando el uso compartido de los recursos ya que diferentes usuarios y conexiones pueden establecerse en diferentes momentos y compartir la misma infraestructura. [4]

Una RPV debe brindar:

Seguridad

Ahorro de Costos

Ubicuidad

Incremento de Ingresos [5]

Tipos de redes privadas virtuales

RPV de acceso remoto

Este 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, hotel, 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 basada en módems y líneas telefónicas, aunque por razones de contingencia todavía conservan sus viejos modems.

RPV punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor RPV, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel RPV. 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, sobre todo en las comunicaciones internacionales.... Es más común el punto anterior, también llamado tecnología de túnel o tunelado.

RPV interna WLAN

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 RPV, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información. [6]

Privacidad y Confidencialidad

Una de las características principales de las RPs es la confidencialidad de los datos transmitidos, los cuales sólo pueden ser manejados y accedidos por los usuarios validados para ese fin, generando privacidad en la conexión sobre una red como Internet, la cual por sí sola no posee, a la fecha, esa característica. [7]

La comunicación entre sitios a través de Internet es vulnerable a ataques de "escuchas". El uso de una red privada virtual garantiza que todo el tráfico existente entre diferentes puntos de comunicación remotos interconectados mediante una red pública sea privado. [4]

Cómo aumenta la seguridad:

Un RPV permite crear un perímetro de seguridad de operación. Incorpora routers y corta fuegos como base, y por encima utiliza mecanismos de seguridad como son:

- ❖ Encriptación de datos: se utilizan varias técnicas: DES, 3DES, RSA
- ❖ Compresión de datos.
- ❖ Autenticación: el servidor RPV autentica al cliente para asegurarse que tienen los permisos necesarios. Si además el cliente autentica al servidor se protege contra la suplantación de servidores.
- ❖ Administración distribuida de claves.
- ❖ Tunelado (Tunneling): para establecer las conexiones punto a punto

❖ Acceso desde el exterior controlado por ser acceso remoto a un servidor seguro

Los protocolos empleados en estas redes son: PPTP (tunelado Punto-Punto), IPSec (Protocolo de Internet de Seguridad), L2TP (Protocolo de tunelado de Capa 2), GRE y SSH (Secure Shell) como recomendado si empleamos la administración distribuida de llaves.

También se utiliza el certificado digital para autenticar servidores, sitios remotos, empleados, socios y clientes, de forma que se garantice que sólo accedan a la organización usuarios autorizados y que cada uno sólo acceda a la información para la que tiene autorización. [8]

Efectividad y Economía

Una RPV es realmente efectiva en términos de intercambio de información crítica entre empleados que trabajan en oficinas remotas, en el hogar, o en la vía pública. Puede distribuir información en forma segura entre vendedores, proveedores o socios, aún habiendo una distancia enorme entre ellos. Debido a que las compañías no tienen que invertir en gran infraestructura, pueden reducir sus costos operativos tercerizando los servicios de red a proveedores. RPVs también reducen costos al eliminar la necesidad de llamados telefónicos de larga distancia, combinando RPVs con Voz sobre IP (VoIP). [9]

Como reducen gastos:

Con estas redes podemos reducir gastos de varios tipos: costos de telecomunicaciones por el mantenimiento de muchas líneas de acceso, costos en la administración del equipo de acceso remoto. Las compañías suelen tener contratadas dos tipos de líneas de acceso: unas de alta velocidad de acceso a Internet y otras del tipo Frame Relay o ISDL.

Con las redes RPV sólo necesitamos un tipo de línea ya que podremos utilizar una red pública IP para transportar todo tipo de datos. Ahorro de gastos operativos. Se permite tener un acceso a una red vía una RPV de manera que la compañía no tiene que preocuparse del mantenimiento y problemas de administración de un banco de módems y servidores de acceso remoto. [8]

Mejora en las comunicaciones

Las RPV se abren paso a través de la red pública IP o por redes compartidas IP creando una conexión que emula las propiedades de un enlace punto a punto privado. Para el usuario es como si realizase una conexión dentro de una LAN (red de área local).

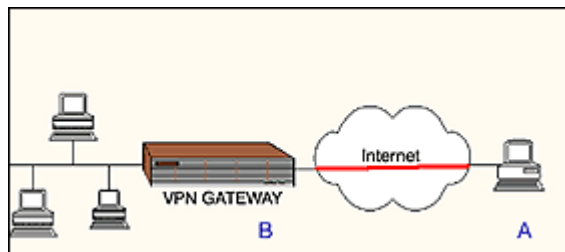
Para conseguir esto se emplean técnicas de tunelado en las que se crea un túnel que conecte a ambos extremos y por los que se transmite la información. Los datos se encapsulan con una cabecera que contenga la información para su encaminamiento a través de los túneles con previa encriptación de los datos. Cuando los datos salen a la red IP su seguridad está garantizada ya que sin la clave de desencriptación no se puede conocer su contenido. [8]

Desventajas

- ❖ El tiempo de respuesta no está garantizado y, por lo tanto, no son recomendables para aplicaciones críticas.
- ❖ Si eventualmente, el ISP de algunos de los puntos pierde la conexión, la conectividad del enlace deja de existir entre esos puntos.
- ❖ Los anchos de banda reales son inferiores a los teóricamente contratados, pues no existe calidad de servicio.
- ❖ No todos los equipos actualmente instalados poseen facilidades para realizar RPVs. Además, se rigen por distintas normas y estándares y no son compatibles entre ellos. [7]

RPV puede provocar una sobrecarga en la conexión de red debido a la encriptación utilizada. La mayoría de dispositivos RPV, 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. [10]

Cuando usar una RPV (VPN en Ingles)



Deberíamos considerarlas cuando los tiempos de respuesta no sean críticos. Por ejemplo, si estamos obteniendo un tiempo de respuesta variable en la RPV de 4 a 5 segundos, que esto no sea un impedimento para la aplicación que pudiera dejar de operar con ese tiempo de latencia.

Su uso también es recomendado cuando se requiere dar acceso a una gran cantidad de usuarios, como, por ejemplo, para aplicaciones de "telecommuting", trabajo en el hogar, oficinas remotas, mantención de redes de

áreas locales, instalación de nuevas aplicaciones, manejo de inventarios, etc.

Asimismo, un punto interesante de analizar aquí es la ventaja que pudiera tener una RPV sobre otras redes privadas o cuál será la tendencia en cuanto a ellas y otras redes, ya sea FR, ISDN, IP, IP/MPLS, Wire-less, etc. El hecho es que las redes RPVs vienen a complementar las posibilidades de conexión dentro de todas las anteriores. Deben funcionar óptimamente para aquellos proyectos donde existen las condiciones para su implementación y las expectativas de sus resultados sean aceptables como producto final obtenido. [7]

Funcionamiento general

En primer lugar es necesario instalar la RPV detrás del Corta fuegos corporativo y el router.

El segundo paso es iniciar el intercambio de llaves y autenticación de servidores y sitios de forma que el administrador consiga un servidor seguro.

Los routers deben ser configurados para que envíen al servidor seguro la información a encriptar, dejando seguir su ruta normal al resto de tráfico. En el Corta fuegos se configura un puerto por el que pase la información al servidor seguro sin filtrarla.

Cuando el RPV recibe un paquete TCP/IP lo comprime y encapsula en un nuevo paquete especial para enviarlo por un túnel hasta su destino. El receptor desencapsula el paquete original, lo descifra y lo envía a su destino dentro de la LAN. [8]

Conclusiones

Las Redes Privadas Virtuales están en rápido crecimiento, ofrecen flexibilidad, bajo costo y alta seguridad. Las Redes Privadas Virtuales enriquecen las comunicaciones, permiten flexibilidad de comunicación entre clientes, proveedores, socios de negocio y otros.

Referencias

1. <http://asignaturas.diatel.upm.es/seguridad/RPV.htm>
 2. <http://www.pc-serveis.com/soporte/windows95-98/Consultas%20m%C3%A1s%20frecuentes%20PPTP%20y%20Redes%20Privadas%20Virtuales.htm>
 3. <http://mashard.perublogs.com/2006/12/Que-es-una-red-privada-virtual.html>
 4. <http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/redes-privadas-virtuales>
 5. <http://www.sistemasunbosque.edu.co/archivos/revista/REDES%20P.pdf>
 6. http://es.wikipedia.org/wiki/Red_privada_virtual
 7. <http://www.emb.cl/gerencia/articulo.mv?sec=3&num=96>
 8. <http://tecun.cimex.com.cu/tecun/software/Soporte%20Tecnico%20de%20Redes/Cisco/Doc-Cisco/Security/RPVirtuales.pdf>
 9. <http://www.logiclinux.com/content/view/35/64/lang.es/>
 10. <http://zip.rincondelvago.com/?00033712>
-

Autores

Lucia Rodríguez García, Ingeniera en Ciencias Informáticas, Instructora Recién Graduada, Universidad de las Ciencias Informáticas

Jorge Hernández Roselló, Ingeniero en Ciencias Informáticas, Instructor Recién Graduado, Universidad de las Ciencias Informáticas