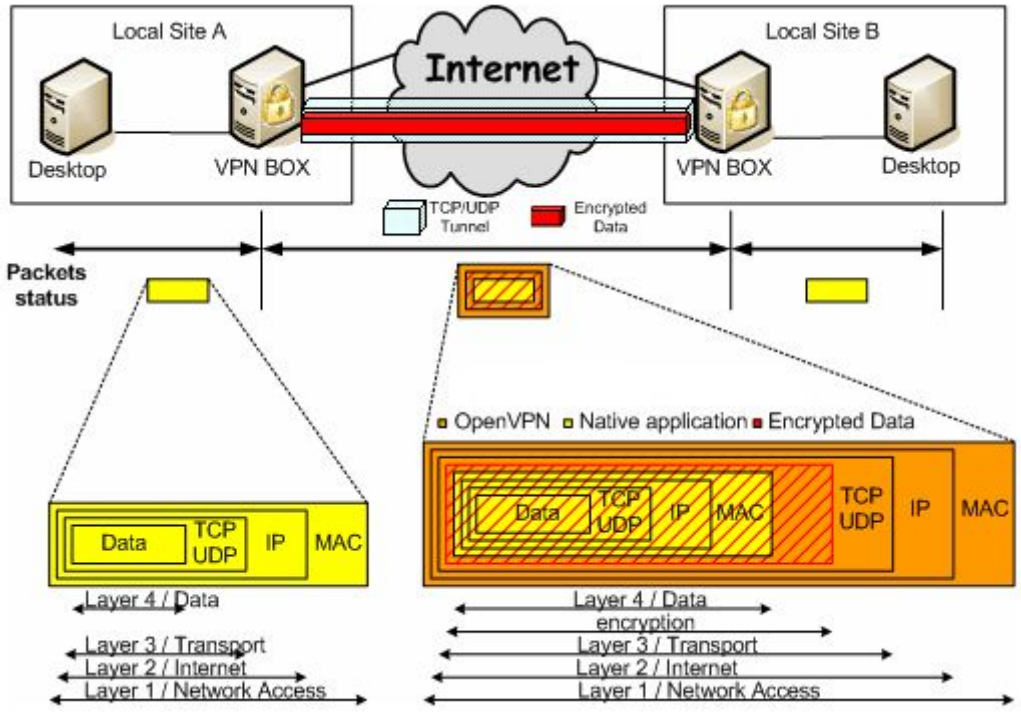
VPN - Introducción

¿Que es una VPN?

Según Wikipedia, una Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.” Si tomamos esta descripción como ejemplo podemos deducir que una VPN es una “red TCP/IP dentro de otra red TCP/IP”. Esta deducción es completamente válida inclusive en sus aspectos técnicos.

Aspecto técnico de una VPN

Si miramos a una Red VPN en su aspecto técnico la describiremos como el transporte de la capa de RED y los datos de una red privada LAN, dentro de los datos de otra red pública o privada completamente diferente. Para comprender mejor vemos el gráfico:



En la Imagen podemos comprender claramente la aplicación técnica de esta solución.

Si analizamos la figura vemos como la información de la red del “Sitio A” es enviada a la red del “Sitio B” encapsulada dentro de la red pública INTERNET. Analizando más en detalle vemos como los datagramas de la red “A” de forma completa (inclusive el encapsulado MC) es enviado dentro de la red Pública.

Esta implementación hace que los equipos dentro de la red “B” “Crean” que los equipos de la Red “A” se encuentran físicamente dentro de su red “B”, además podemos ver que los datos de la Red “A” van encriptados, y esto no es despreciable si entendemos que dicha información atraviesa redes de acceso público e inseguras.

Encriptación

Debido al uso y aplicación de las redes VPN sobre redes públicas, estas son obligatoriamente encriptados (existe la posibilidad de establecer túneles que no sean encriptados, pero en estos casos no se los llama VPN). O sea que la solución suministra seguridad al transporte de la información, creando un túnel de datos ilegibles que puede realizarse aplicando diferentes metodologías.

Por medio de esta encriptación las redes VPN nos brindan:

Confidencialidad y Privacidad

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

Autenticación

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no hubiese algún tercer participante que se haya entrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos.

Integridad

Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Protocolos de VPN

Para implementar una VPN los equipamientos requeridos para interpretar los datos encapsulan los paquetes dentro de paquetes para acomodar protocolos incompatibles, y por supuesto para entenderse entre ambos extremos estos equipos utilizan protocolos para enviar y recibir la información. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Forwarding Protocol (L2FP) y el modo túnel de IPSec.

Topologías de VPN

Las implementación de redes VPN dependen del requerimiento y del servicio a brindar, pero existen esencialmente dos tipos de implementación topológicas.

- LAN to LAN (Red a Red)

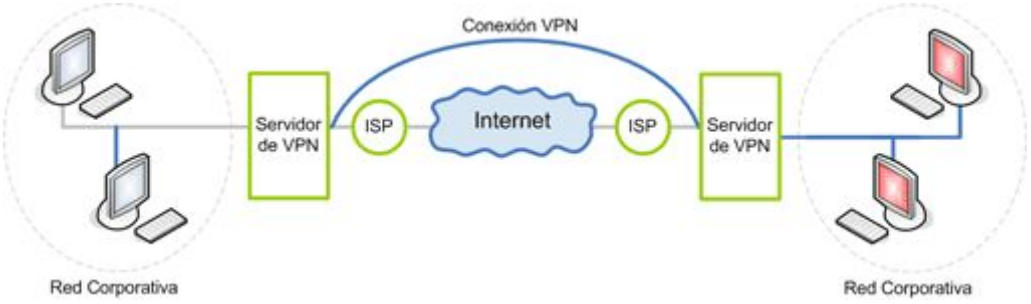
- Host to Host (Máquina a Máquina)
- Host to LAN (Máquina a Red)

LAN to LAN

Las implementaciones del tipo LAN to LAN son realizadas cuando se pretende unificar la información de dos redes del tipo LAN situadas en distintos lugares geográficos.

Para esta solución se requiere la instalación de dos servidores VPN que controlan la red VPN implementada entre ellos y las redes privadas que están detrás de ellos, uniéndolas de manera tal, que ambas redes pretenden coexistir como una única RED.

Esta arquitectura es realizada generalmente para unir sucursales de establecimientos donde todo el equipamiento de cada sucursal es miembro de una única red global. En la figura podemos comprender mejor el ejemplo.



Se ve claramente la necesidad de instalar dos equipos servidores de VPN

Host to LAN

Es muy similar a la arquitectura LAN to LAN, con la diferencia de que la conexión se utiliza únicamente por los dos servidores VPN. Es decir, que los servidores VPN no comparten dicha conexión con otros equipos.

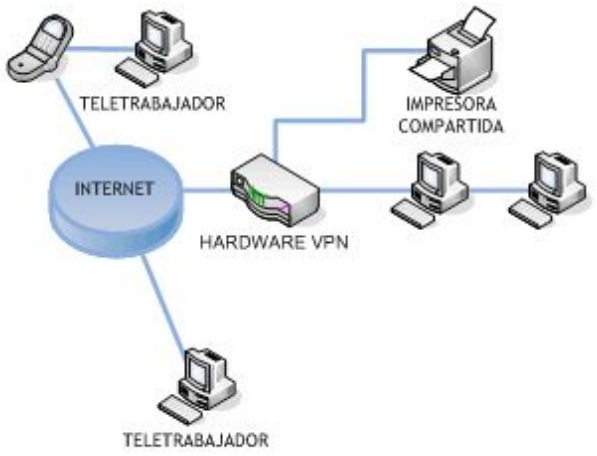
Esto es muy útil porque requiere una menor cantidad de configuración, por lo que puede establecerse relativamente rápido y puede servir para que dos equipos intercambien información de forma segura. Incluso puede crearse una VPN Host to Host entre dos equipos que pertenezcan a la misma LAN, lo que les permite evitar muchos de los ataques que se presentan en este tipo de redes.

NOTA: Debemos recordar que las redes LAN son susceptibles a algunos ataques, como el envenenamiento ARP (ARP Poisoning), que, en el caso de utilizar una VPN Host to Host, quedarían sin efecto.

Host to LAN

Las implementaciones Host to LAN son realizadas para conectar una máquina específica a una red privada mediante el uso de una red pública. Para esta topología no se requiere la implementación de dos servidores de VPN, sino simplemente, la utilización de un software

que comprenda el protocolo de VPN utilizado y sea el que realice la conexión hacia el servidor VPN de la red corporativa. Generalmente esta topología es utilizada para conectar agentes externos de una entidad hacia la red corporativa, por ejemplo para brindar el servicio de empleado ambulante, donde el agente puede conectarse a la red LAN desde cualquier lugar de la red Pública utilizando el software brindado.



Como podemos observar en el diagrama este tipo de implementación no requiere de dos hardware dedicados de VPN y los clientes se conectan directamente desde sus estaciones de trabajo.

Diferencias de las topologías

Ambos tipos de implementaciones topológicas son usadas en diferentes situaciones, pero cada una de ella presenta ventajas y desventajas de aplicación. Obviamente la tecnología LAN to LAN tiene la capacidad de unir dos Redes, pero posee la desventaja de requerir la implementación de dos equipos Servidores VPN para su instalación. Y por consiguiente es más costosa, más compleja de administrar, más difícil de configurar y requiere mayor mantenimiento.

En cambio la implementación Host to LAN no requiere de este hardware anexo, pero presenta la desventaja de requerir la instalación de la aplicación de cliente VPN en cada equipo. Otra ventaja que podemos señalar con esta implementación, es la capacidad de transporte que posee. Debido a que el cliente está instalado en la máquina del usuario, este puede conectarse a la red VPN desde cualquier punto de la red pública. Y como ventaja de la tecnología LAN to LAN podemos observar que los clientes de ambas redes VPN no requieren la instalación de un software adicional.

Autor: Fabian Martinez Portantier

Fuentes:

- www.microsoft.com

- www.openmaniak.com
- "Cortafuegos. Comparativa entre las Distintas Generaciones y Funcionalidades Adicionales " (Versión 1.1), escrito por José María Morales Vázquez