UD 3:
“Implantación de técnicas de seguridad remoto. Seguridad perimetral.”

Redes privadas virtuales. VPN

Luis Alfonso Sánchez Brazales

Redes privadas virtuales. VPN

- ***Beneficios y desventajas con respecto a las líneas dedicadas.***

En años pasados si una oficina remota necesitaba conectarse a una computadora central o red en las oficinas principales de la compañía significaba arrendar líneas dedicadas entre las ubicaciones**.** Estas líneas dedicadas arrendadas proveen relativamente rápidas y seguras comunicaciones entre los sitios, pero son muy costosas.
Una VPN crea un tunel virtual conectando dos terminales. El tráfico dentro del tunel VPN está encriptado, así que otros usuarios de la red pública de Internet no pueden fácilmente mirar comunicaciones interceptadas.
Implementando una VPN, una compañía puede proveer acceso a la red interna privada a clientes alrededor del mundo en cualquier ubicación con acceso al Internet público. Esto elimina los dolores de cabeza financieros y administrativos asociados con una tradicional línea arrendada de red de área amplia (WAN = Wide Area Network) y permite a usuarios móviles y remotos ser más productivos. Lo mejor de todo si está bien implementado, lo hace sin impacto a la seguridad e integridad de los sistemas de cómputo y datos en la red privada de la compañía.

VPN´s tradicionales se basan en IPSec (Internet Protocol Security) para construir un tunel entre dos terminales. IPSec trabaja sobre la capa de red (Network layer) en el modelo OSI asegurando todos los datos que viajan, a través, de dos terminales sin una asociación con alguna aplicación específica. Cuando se conectan sobre una VPN IPSec la computadora cliente es virtualmente un miembro pleno de la red corporativa – capaz de ver y potencialmente acceder a la red completa.

Redes privadas virtuales. VPN

VPN puede ser una buena solución con importantes ventajas:

Ventajas

- Una de las ventajas más significativas es el hecho de que las VPN permiten la integridad, confidencialidad y seguridad de los datos.
- Reducción de costes, frente a líneas dedicadas.
- Sencilla de usar, una vez conectados a la VPN, se trabaja como si fuera una LAN.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnóstico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.

Desventajas

El uso de redes VPN no tiene apenas desventajas, sin embargo cabe señalar que como toda la información se envía a través de Internet, es necesario tener una buena conexión.

- ***Tipos de conexión VPN:***

➢ VPN de acceso remoto

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).

Redes privadas virtuales. VPN

- VPN sitio a sitio (tunneling)

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 puntos tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

- VPN sobre 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 sólo 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.

Redes privadas virtuales. VPN

- ***Protocolos que generan una VPN: PPTP, L2F, L2TP***

- PPTP (Protocolo de túnel punto a punto) es un protocolo de capa 2 desarrollado por Microsoft, 3Com, Ascend, US Robotics y ECI Telematics.
- L2F (Reenvío de capa dos) es un protocolo de capa 2 desarrollado por Cisco, Northern Telecom y Shiva. Actualmente es casi obsoleto.
- L2TP (Protocolo de túnel de capa dos), incluye todas las características de PPTP y L2F. Es un protocolo de capa 2 basado en PPP.

- Protocolo PPTP

El principio del PPTP (Protocolo de túnel punto a punto) consiste en crear tramas con el protocolo PPP y encapsularlas mediante un datagrama de IP.
Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de IP.
De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan dentro de un mensaje PPP, que a su vez está encapsulado dentro de un mensaje IP.

Redes privadas virtuales. VPN

- Protocolo L2F

El protocolo L2F (Layer 2 Forwarding) se creó en las primeras etapas del desarrollo de la red privada virtual. Como PPTP, L2F fue diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas. La principal diferencia entre PPTP y L2F
es que, como el establecimiento de túneles de L2F no depende del protocolo IP, es capaz de trabajar directamente con otros medios, como Frame Relay o ATM. Como PPTP, L2F utiliza el protocolo PPP para la autenticación del usuario remoto, pero también implementa otros sistemas de autenticación como TACACS+ y RADIUS. L2F también difiere de PPTP en que permite que los túneles contengan más de una conexión.
Hay dos niveles de autenticación del usuario, primero por parte del ISP, anterior al establecimiento del túnel, y posteriormente, cuando se ha establecido la conexión con la pasarela corporativa. Como L2F es un protocolo de nivel de enlace de datos según el Modelo de Referencia OSI, ofrece a los usuarios la misma flexibilidad que PPTP para manejar protocolos distintos a IP, como IPX o NetBEUI.

- Protocolo L2TP

L2TP es un protocolo de túnel estándar (estandarizado en una RFC, solicitud de comentarios) muy similar al PPTP. L2TP encapsula tramas PPP, que a su vez encapsulan otros protocolos (como IP, IPX o NetBIOS).