Redes Privadas Virtuales

Feis Aguilar Amado. M.Sc.Empresa de Telecomunicaciones de Cuba SA, ETECSA, Guantánamo, Cuba.
Email: feis@enet.cu
Héctor R. Sánchez Paz Ph.D. Profesor Titular. Departamento de Telecomunicaciones. Universidad de Oriente, Cuba.
Email: hsanchez@fie.uo.edu.cu

Resumen

Los cambios experimentados en el campo de las telecomunicaciones desde comienzos de la década pasada, con la explosión de la red INTERNET entre otros, han hecho posible que los proveedores de estos servicios evalúen nuevas estrategias y formas de operar en función de evacuar las necesidades de conectividad, flujo informativo y prestaciones, en la era de la información y el conocimiento. Ante estas condiciones, se presenta a continuación las principales características de las Redes Privadas Virtuales (VPN) de datos.

Introducción

Durante la última década las redes de datos han experimentado cambios profundos, en lo fundamental por el rápido crecimiento de los servicios relacionados con el acceso a INTERNET. Se espera que para los próximos años exista un fuerte crecimiento de las aplicaciones basadas en el Protocolo de Internet (IP). Para poder soportar estos incrementos en materia de aplicaciones, las Redes de Datos deben sufrir grandes e importantes cambios. En un futuro cercano las redes basadas en el protocolo IP, muchas veces pocos fiables e inseguras con encaminamiento del tipo "el mejor posible" y las redes Frame Relay (FR) y ATM, ya establecidas y muy confiables, deberán evolucionar para ofrecer a los usuarios redes de datos confiables y seguras.

Estas redes proporcionarán a los proveedores soluciones con un costo inferior a las actuales, las cuales hacen un uso ineficiente de los recursos de red disponibles y requieren grandes esfuerzos operacionales. En este sentido, las redes en el futuro deberán incrementar la calidad y disponibilidad y para ellos tendrán que cumplir con varios aspectos:

Escalabilidad: Permite a los proveedores de redes de datos dosificar las inversiones en sus infraestructuras de acuerdo con el crecimiento de la demanda.

Fiabilidad: Se estima que la exigente cifra de 99,999% corresponde a cinco minutos de interrupción al año, lo que pronto se convertirá en una norma para las redes de datos.

Prestaciones: El mantenimiento de extremo a extremo del ancho de banda y de la calidad de servicio (QoS), en este aspecto las redes de datos basadas en ATM, FR están muy avanzadas lo que no ocurre con VPNs IP, lo que se estima que en un futuro deban transportar a la vez más tráfico a tiempo real y otros.

Seguridad: En el pasado, el problema de los ataques maliciosos sobre las redes y los servicios se consideraban que incumbía a los usuarios finales y a las empresas. Sin embargo, las cosas han cambiado, los ataques son cada vez más fuertes y las redes de datos en este sentido no tienen la envergadura suficiente.

Redes Privadas Virtuales (VPN)

Una Red Privada Virtual (VPN), es una forma de compartir y transmitir información entre usuarios separados geográficamente. Para ello se crea un canal dinámico a través de la Red de INTERNET, éstas transmisiones se realizan a través de tecnologías de encriptación y encapsulamiento para lograr un nivel de seguridad en los datos enviados.

En la Figura 1 se muestra el esquema general de una Red Privada Virtual, esta una vez establecida es capaz de transportar datos a través del canal público de INTERNET y los mismo tendrán la seguridad que pueda suministrarle el protocolo escogido para la aplicación en específico. Estos protocolos serán tratados en un acápite del presente trabajo.

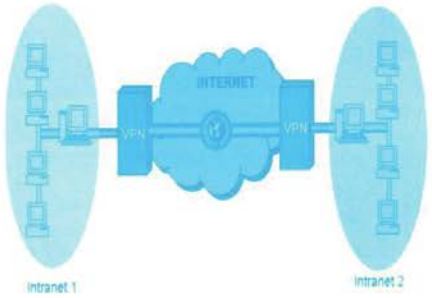

Figura 1. Estructura General de VPN.

Características de las VPN

Las VPN deben garantizar para su buen funcionamiento las siguientes características generales:

- Confidencialidad: Previene que los datos que viajan por la red sean leídos correctamente.

- *Integridad:* Asegura que los datos de origen corresponden a los de destino.

- *Autentificación:* Asegura que quien solicita la información exista.

- *Control de acceso:* Restringe el acceso a usuarios no autorizados que quieran infiltrarse en la red.

Ventajas de una VPN

- La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red, con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un ordenador en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc; a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a INTERNET desde el ordenador cliente VPN se realizarán usando los recursos y conexiones que tenga la red privada.

- Reducir los costos frente a otras soluciones de conectividad como arriendo de líneas dedicadas u otros. Las VPN tienen un funcionamiento similar al de las Redes de Área Amplia WAN, pero su costo es inferior ya que utiliza la red de INTERNET para comunicarse entre sí, permitiendo de esta manera tener comunicaciones rápidas y seguras entre sus oficinas o desde cualquier lugar exterior de ellas. La conexión WAN es posiblemente la solución más estable y segura para una red de cualquier tamaño. Las conexiones son totalmente privadas y usan tecnología estándar.

- Las redes privadas virtuales son una nueva tecnología, ejecutándose sobre una tecnología poco fiable, INTERNET. Realizando transacciones a través de Internet, comunicaciones entre varias plataformas, procesos de encriptación y similares se consigue un sistema menos fiable que en el caso de una conexión WAN. Sin embargo, el mundo se mueve más hacia una sociedad interconectada y como van apareciendo nuevos estándares reales (protocolos, hardware, etc.), las VPNs tendrán una base estable sobre la que debe operar.

- No requiere de grandes inversiones en infraestructura. Los enlaces punto a punto implican que la organización debe realizar una cuantiosa inversión inicial en equipamiento para conectar cada una de las sucursales u oficinas que posea. Sin embargo, con las VPN tanto la inversión inicial como las tareas de instalación, operación y mantenimiento son mucho más pequeñas. Las diferencias reales entre las VPN y las WAN aparecen cuando se considera la escalabilidad de ambas. Una gran WAN requiere una cuantiosa inversión en equipamiento, especialmente cuando se añaden múltiples redes a lo largo de la zona de actuación de la organización. Con VPN, inicialmente se necesita una red central que sólo tenga una actualización del ancho de banda aunque se aceptarán conexiones desde múltiples redes.

- Proporciona seguridad e integridad en la transmisión de datos

Inconvenientes de las VPN

- Mayor carga en el cliente VPN, puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una mayor demora de la mayoría de conexiones.

- También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).

- La fiabilidad es menor que en una línea dedicada.

- Se pueden producir ataques por denegación de servicio.

- Es delicada y laboriosa la gestión de claves de acceso y autenticación.

Protocolos en VPN: IPSec

Las siglas IPSec corresponden en inglés con "Internet Protocol Security". IPsec es un grupo de extensiones de la familia del protocolo IP y provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. Es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de IPsec para poder usarlo. Puede usar cualquier protocolo IP sobre IPSec y puede crear túneles cifrados (VPN), o simple cifrado entre computadoras. De un modo lógico, IPsec funciona en cualquiera de estos tres modos:

- Usuario-a-Usuario
- Usuario-Red
- Red-a-Red

Problemas con IPSec

La incorporación a IPSec con rasgos necesarios para desarrollar VPN's seguros sobre Internet, todavía es un trabajo en proceso. A continuación se comentan algunos problemas que pueden afectar al despliegue de IPSec:

- Todos los paquetes procesados IP con IPSec incrementan su tamaño debido a la adicción de cabeceras IPSec, las cuales pueden llegar a incrementar la fragmentación de paquetes y disminución del procesamiento.

- IPSec está solamente diseñado para manejar tráfico del IP. Si está corriendo en una red multiplataforma, puede tener que utilizar uno de los otros protocolos, como PPTP o L2TP.

- La computación sobrecargada asociada con muchos de los algoritmos criptográficos usados en IPSec pueden todavía tener problemas con viejas estaciones de trabajo y computadoras, solo el despliegue de IPSec sobre el nivel de escritorio puede afectar considerablemente el funcionamiento.

- La distribución de software y hardware criptográfico está todavía sujeta a las restricciones gubernamentales. Estas restricciones pueden requerir derechos de administración adicional si es de una organización internacional. Por último, usar IPSec para encaminamiento permite tener una dirección de IP ilegal y también comunicarse con otros.

PPTP

Las siglas PPTP corresponden en inglés con "Point-to-Point Tunneling Protocol". PPTP se diseñó para proporcionar comunicaciones autenticadas y cifradas entre un cliente y una puerta de enlace o entre dos puertas de enlace, utilizando un Id. de usuario y una contraseña. El objetivo del diseño era la simplicidad, la compatibilidad multiprotocolo y la capacidad de cruzar una amplia gama de redes IP.

El protocolo de túnel punto a punto utiliza una conexión TCP, por el puerto 1723, para el mantenimiento del túnel y tramas PPP en tramas IP encapsuladas mediante encapsulación de enrutamiento genérico GRE "Generic Routing Encapsulation" para los datos del túnel. Las cargas, partes de datos útiles, de las tramas PPP encapsuladas se pueden cifrar o comprimir. Actualmente este protocolo, aunque muy popular en el mundo de Microsoft, está siendo sustituido por el L2TP.

L2TP

Las siglas L2TP corresponden en inglés con "Layer 2 Tunnelling Protocol". L2TP es un protocolo maduro en la senda de los estándares IETF que ha sido ampliamente implementado. L2TP encapsula las tramas del protocolo punto a punto (PPP) que van a enviarse a través de redes IP, X.25, FR, o modo de transferencia asíncrona ATM "Asynchronous Transfer Mode". Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet. L2TP sobre

IP utiliza el puerto UDP 1701 e incluye una serie de mensajes de control L2TP, para el mantenimiento del túnel L2TP. También utiliza UDP para enviar tramas PPP encapsuladas en L2TP como datos del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPSec estándar mediante el modo de transporte IPSec para obtener una fuerte protección de integridad, reproducción, autenticidad y privacidad.

L2TP se diseñó específicamente para conexiones cliente a servidores de acceso a redes, así como para conexiones puerta de enlace a puerta de enlace. Mediante la utilización del protocolo PPP, L2TP gana compatibilidad multiprotocolo para protocolos como IPX y Appletalk. PPP también proporciona una amplia gama de opciones de autenticación de usuario, incluidos CHAP, MS-CHAP, MS-CHAPv2 y el Protocolo de autenticación extensible EAP "Extensible Authentication Protocol" que admite mecanismos de autenticación de tarjetas token y tarjetas inteligentes. L2TP/IPSec, por lo tanto, proporciona túneles bien definidos e interoperables, con la seguridad de alto nivel e interoperabilidad de IPSec. Es una buena solución para conexiones seguras de acceso remoto y de puerta de enlace a puerta de enlace.

Conclusiones

El nacimiento de la red de INTERNET a pesar de tener un crecimiento amplio, no preveé a largo plazo la sustitución de las redes ya establecidas.

El equilibrio tecnológico de las redes de datos a través de protocolos orientados a conexión (FR, X25, ATM), con el protocolo IP, y con este, las aplicaciones tales como VPNs IP es necesario, pues se impone el factor económico y otros aspectos relacionados con el servicio.

A pesar que las redes VPN prometen ser las redes del futuro es bueno destacar que en estos momentos no cuentan con la madurez suficiente en cuanto a seguridad, por lo que en conexiones donde se requiera un riguroso tratamiento a la seguridad, aún las redes de Datos punto a punto (X25, FR, ATM, etc) son necesarias.

Bibliografía

B. Levis. "Punto de vista de un operador sobre las telecomunicaciones". En: *Telecomunicaciones de ALCATEL*, 3er *trimestre*. p. 154-157. 2002.

F. Aguilar. "Propuesta de Red de Datos para la provincia Guantánamo". En: *Tesis de Maestría en Sistemas de Telecomunicaciones*. Universidad de Oriente, Cuba. 2003.

H. Rosaval. "Informatización: objetivo estratégico". En: *Mensuario de Informática y Comunicaciones*. No 6. Enero. 2003.

M. Aissaoui. "Fundamentos de una Arquitectura QoS Escalable para los Servicios VPN IP". En: *Telecomunicaciones de ALCATEL*, 3er trimestre 2002. P 154-157.

R. Collado; M. Montserrat, "Redes Privadas Virtuales". Abril. 2003. http://www.comexperu.org.pe/pdfs/rni/agosto01/portada.pdf.

R. M. Wernik. "Pilares de las redes de Datos Seguras". En: Telecomunicaciones de ALCATEL, 3er trimestre 2002. P. 158-160.