GUIA PRÁCTICA SOBRE REDES PRIVADAS VIRTUALES

VIRTUAL PRIVATE NETWORK (VPN)

LAURIE PAILLIER VASQUEZ

KAREN ROCIO ARZUAGA ARAUJO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

REDES Y COMUNICACIONES

CARTAGENA, DT Y C

2004

GUIA PRÁCTICA SOBRE REDES PRIVADAS VIRTUALES

VIRTUAL PRIVATE NETWORK (VPN)

LAURIE PAILLIER VASQUEZ

KAREN ROCIO ARZUAGA ARAUJO

Monografía para optar el titulo de

Ingeniero de Sistemas

Director

Giovanny Vásquez

Magíster en Ciencias Computacionales

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

REDES Y COMUNICACIONES

CARTAGENA, DT Y C

2004

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

A Dios por darme fortaleza
A mis padres Edwin y Glenis por creer en mí,
A mis hermanos Edwin y Gae para que sigan adelante,
A mis amigos Pedro Luis, Karen, Marianella y Efraín
por levantarme el ánimo en los momentos difíciles,
a mis abuelas Tulita y Olimpia por sus valiosas enseñanzas,
y a Alex por animarme a seguir
Los quiero mucho a todos.
Laurie

_____

A Dios por darme Entendimiento y Sabiduría
A mis padres Erasmo y Luga por su apoyo incondicional
A mis hermanos por su constante motivación
A mi novio Carlos por estar siempre a mi lado
A Laurie y a Marianella por apoyarme en los momentos más difíciles
Los quiero Mucho
Karen

AGRADECIMIENTOS

Agradecemos especialmente a:

Giovanny Vásquez, Ingeniero de Sistemas por su valiosa orientación para realizar este proyecto.

A todo el cuerpo docente de la Universidad Tecnológica de Bolívar por su constante motivación.

Al ing. Gonzalo Garzón por su invaluable apoyo a lo largo de nuestra carrera.

RESUMEN

Las Redes privadas virtuales o VPN son una tecnología nueva que a generado gran expectativa a nivel mundial y se puede decir que ha revolucionado el concepto de acceso remoto a Lan a bajo costo es así como este tema ofrece mucha expectativas a la hora de hablar de seguridad en redes corporativas, seguridad en los datos de nuestra empresa y ampliación del área de cobertura de la misma utilizando un medio publico como lo es el Internet, por este y muchos motivos mas consideramos este tema de gran interés e importancia para las nuevas generaciones en Redes y por tanto apto para ser desarrollado como trabajo investigativo en el marco de este Minor.

Actualmente el tema de las redes privadas virtuales ha llamado la atención de muchas empresas que desean ampliar sus redes de manera segura a bajo costo y la información que se conoce al respecto es bastante amplia y variada por tanto algunas veces resulta bastante complicado tomar la decisión correcta al implementar esta tecnología es decir establecer que es lo que realmente nos interesa y cuales son los pasos a seguir, es así, como lo que se pretende es ayudar a las empresas a conocer todo lo relacionado con la aplicación integral de las seguridad en las redes privadas virtuales (VPN) de manera clara, actualizada y resumida convirtiendo este en un manual efectivo para la solución de problemas y la toma de decisiones.

La metodología que se utilizo para el desarrollo de esta investigación fue la consulta del estado del arte de la tecnología VPN utilizando diferentes herramientas bibliograficas reconocidas, así como el análisis de la información publicada en Internet obteniendo como resultado una información veraz, concisa y objetiva, es así, como se presenta en tres capítulos que pretenden facilitar su comprensión.

Se desarrollo de una página Web utilizando la herramienta de diseño Macromedia Dreamweaver MX con el fin de facilitar el acceso a la información expuesta en esta monografía.

Le sugerimos al lector tener en cuenta las recomendaciones hechas al fina de este documento.

CONTENIDO

Pág.

LISTA DE FIGURAS

INTRODUCCIÓN

Cuando hablamos de expansión de nuestra red corporativa, conectividad en Internet, y de seguridad, el concepto de redes privadas Virtuales o Virtual Private Network (VPN) hace su aparición indiscutible, esta es quizás una de las tecnologías con mayor auge en los últimos años y su gran popularidad aumenta cada día, desafortunadamente para muchas de la empresas que desean incursionar en el ambiente VPN resulta muchas veces confuso tomar la decisión correcta, es así como este trabajo investigativo pretende facilitar estar labor brindándole a los ejecutivos, jefes de área y personal técnico la información y herramientas necesaria para elegir la solución mas acertada de acuerdo a las necesidades de su empresa; además de servir como material de consulta para la comunidad académica.

Las redes privadas virtuales VPN como tecnología de internetworking nos sugieren tres aspectos fundamentales: la expansión de la red, bajos costos y seguridad. Lo que se pretende analizar es si en realidad las VPN ofrecen todas las ventajas que predicen, es decir, mostrar cuales son la necesidades que suplen, dar herramientas para escoger la mejor solución VPN dependiendo de dichas necesidades y además brindarle al usuario una serie de

recomendaciones de seguridad que le serán de gran utilidad si desea optar por la implementación de esta tecnología. Para tal efecto es necesario que el lector este familiarizado con los conceptos de encripción y encapsulación de datos que asumimos posee, de igual forma no es objeto de esta investigación adentrarse en estos temas pero si dejarlos claros para facilitar la compresión de la misma.

Capitulo 1. REDES PRIVADAS VIRTUALES – VIRTUAL PRIVATE NETWORK (VPN)

1.1. Conceptos generales

Anteriormente las grandes compañías gastaban enormes cantidades de dinero configurando sus redes privadas (Intranets), estas eran instaladas utilizando costosos servicios de líneas dedicadas Frame Relay o ATM para unir sus sucursales con la oficina central y comunicaciones “dial-up” usando servidores de acceso remoto (RAS) basados en llamadas conmutadas (RTC, RDSI) con determinado número de *dialers* o dispositivos de establecimiento de llamadas para incorporar a sus usuarios remotos, era así como este proceso ofrecía ciertas desventajas como:

- El número de accesos simultáneos a la red corporativa estaba limitado por el número de *dialers* (modems RTC, RDSI) disponibles en el servidor RAS.
- El costo del acceso era el de una llamada conmutada entre los dos extremos de la comunicación (usuario - servidor RAS), por lo que en ocasiones era elevado (llamadas nacionales e internacionales).

Además que para las medianas y pequeñas empresas el pensar en implementar estas tecnologías era prácticamente imposible teniéndose que conformar con servicios mucho más inferiores.

Con el crecimiento de la accesibilidad a Internet, el aumento considerable del ancho de banda y el abaratamiento del costo de acceso (llamada metropolitana) se abrió un mundo de posibilidades, las extranets, que permitían comunicar a los usuarios internos y externos a más bajo costo y de manera rápida, sin embargo presentaban un inconveniente: la seguridad.

Actualmente las corporaciones tienen la posibilidad de crear una red privada virtual (VPN) que demanda una inversión relativamente baja utilizando Internet para la conexión entre diferentes localidades o puntos.

1.1.1 Concepto de VPN

Este concepto ha sido motivo de gran atención; el sector empresarial la considera como: "una tecnología que permite la extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet", por su parte la comunidad académica sugiere el siguiente concepto : [1] "Un proceso de comunicación cifrado o encapsulado que transfiere datos desde un punto hacia otro de manera segura; la seguridad de los datos se logra gracias a una tecnología robusta de cifrado, y los datos que se transfieren pasan a través de una red abierta, insegura y enrutada", ambas definiciones nos conllevan a reducir y entender este concepto de manera sencilla como:

[1] Steven, Brown Implementación de Redes Privadas Virtuales

Una red privada virtual o VPN es una tecnología que nos permite expandir nuestra red corporativa a través de una red publica como Internet, cerciorando la transferencia e integridad de nuestros datos en forma segura mediante la utilización de técnicas de encripción y cifrado.

Es así como las soluciones actuales de VPN ofrecen una gran cantidad de servicios mejorados que incorporan las ventajas de tener una red extendida que permite la comunicación interna y externa de los usuarios con la red privada de la empresa a bajo costo y con el beneficio de la seguridad integral, este concepto de VPN se logra gracias a la incursión de técnicas criptográficas y protocolos que nos garantizan la integridad de los datos y privacidad de las conexiones punto a punto.

Las características que deben garantizar todas las VPN son:

- *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.

Estas características son ofrecidas gracias a tecnologías y protocolos de seguridad y encriptación que proporcionan seguridad en la transmisión de los

datos independientemente de las redes involucradas y de sus medidas de seguridad:

La privacidad de los datos debe ser garantizada mediante la encriptación de los mismos. La encriptación usa complejas transformaciones matemáticas en la cual los datos se combinan con una llave lógica y luego son desencriptados por la persona que lo recibe usando la misma clave. Administrar estas claves es el aspecto más crucial para la encriptación.

Aplicar transformaciones matemáticas en los datos para crear una marca digital y evitar que no sea alterada ni modificada en el transporte.

La autenticación de los usuarios evita que un usuario pueda ser confundido por algún otro y de esta manera le otorgue privilegios sobre la red que no le corresponden. La habilidad de realizar una Autenticación positiva de un usuario es vital para la seguridad de las VPDN. La protección mediante password es fácilmente violable y por lo tanto insegura, es así como aparece en concepto de certificados digitales y la firma digital.

1.1.2 Como funciona una VPN

Una VPN (Virtual Private Network) es una estructura de red corporativa implantada sobre una red de recursos de transmisión y conmutación públicos, que utiliza la misma gestión y políticas de acceso que se utilizan en las intranets. En la mayoría de los casos la red pública es Internet, pero también puede ser una red ATM o Frame Relay. Como se menciono anteriormente una red privada virtual VPN ofrece una conexión segura entre los usuarios internos o remotos con la compañía asegurando la integridad de los datos a través del Internet.

Esto es posible gracias al concepto de “Tunneling”, esta es una técnica que nos permite construir un “túnel” virtual entre el emisor y el receptor asegurando que los datos transiten encapsulados y encriptados por este, en su paso a través de Internet.

Los paquetes de datos de una VPN viajan por medio del “túnel” definido en la red pública, estableciendo una conexión entre dos puntos en modo similar a como lo hacen los circuitos en una topología WAN, a diferencia de los protocolos orientados a paquetes, capaces de enviar los datos a través de una variedad de rutas antes de alcanzar el destino final, un túnel representa un circuito virtual dedicado entre dos puntos. Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen en uno nuevo que incluya

los campos de control necesarios para crear, gestionar y deshacer el túnel, tal como se muestra en la Figura 1. Asegurando la seguridad de estos.

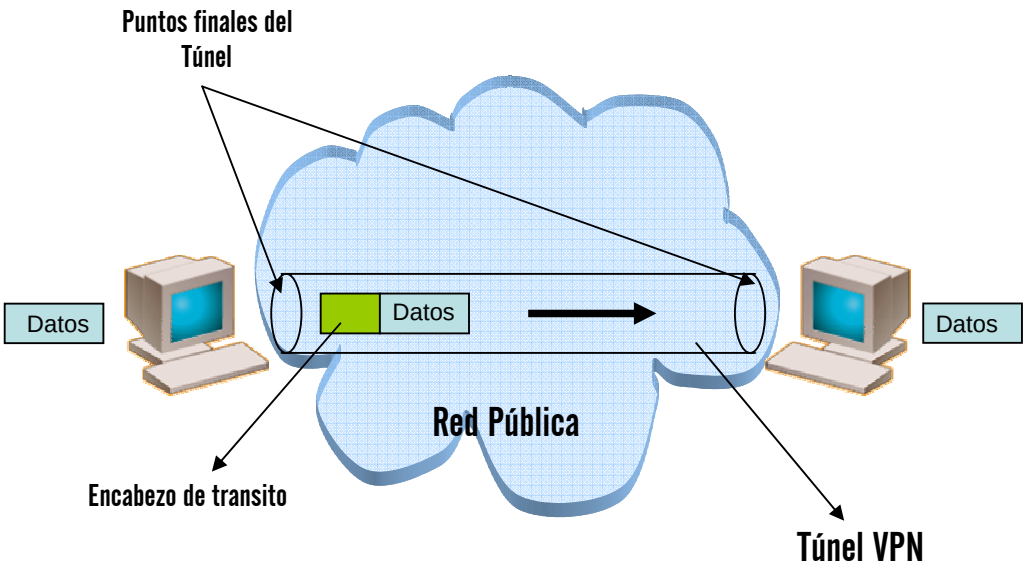


Figura 1. Túnel en una VPN

Es así como los datos realizan el siguiente proceso:

1. Se utiliza inicialmente funciones de cifrado o encripción de los datos, la encripción es una técnica que codifica la información de un modo que hace difícil o imposible su lectura, y la decodifica de modo que pueda ser leída nuevamente. A la información codificada se la llama texto cifrado y a la información sin codificar, texto claro.

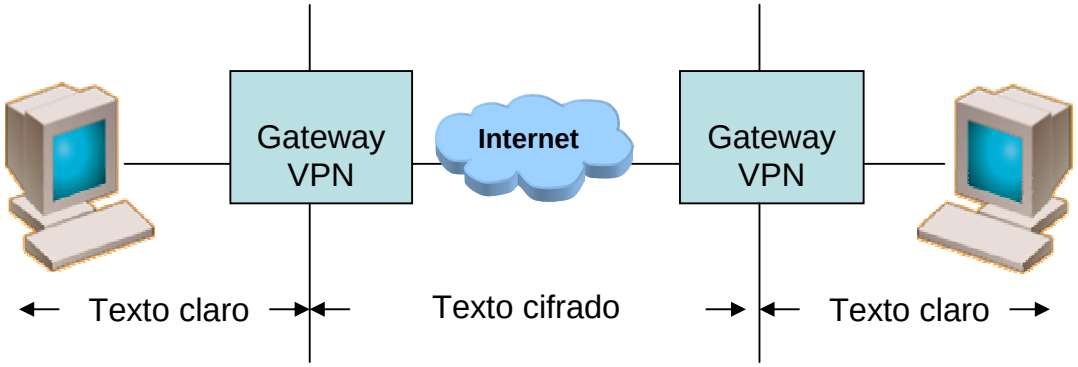


Figura 2. Proceso de Cifrado en una VPN

Cuando en una VPN se transmite información de un punto a otro, el Gateway de la VPN del punto de origen encripta la información en texto cifrado antes de enviarla. En el otro punto, el Gateway receptor desencripta la información, es decir se vuelve texto claro, y luego la envía a la LAN, este proceso se ilustra en la figura 2.

2. Luego se procede a la autenticación, esta tecnología nos garantiza la identidad de los participantes de la VPN, es decir, que los gateways y clientes estén autorizados para establecer la conexión.

La autenticación en VPNs es conceptualmente parecido a “logearse” o ingresar a un sistema con un nombre de usuario y una contraseña, pero con necesidades mayores de aseguramiento de validación de identidades, es así, como actualmente las técnicas de autenticación mas usada es la de certificados digitales, lo que permite autenticar e identificar tanto a personas

como a sistemas sin el uso de usuarios y contraseñas de manera mas confiable.

3. Después se encapsulan en paquetes IP (Internet Protocol) para este proceso es necesario la utilización de protocolos especiales entre los que se encuentran PPTP, L2TP e Ipsec, este proceso se describe mas adelante.

4. los paquetes transitan encriptados por el túnel VPN.

5. Posteriormente los paquetes son descifrados en su destino.

1.2 Tipos de VPN

Una VPN 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.

Existen actualmente varias formas de clasificar las VPN, pero generalmente se pueden dividir en tres categorías, es decir las implementaciones para los cuales son comúnmente utilizadas estas son::

1.2.1 VPN de Acceso Remoto

Este tipo de implementación se utiliza para conectar usuarios remotos o móviles de nuestra compañía con la red interna de la misma, es decir, aquellos usuarios que no poseen un sitio de trabajo “estático”, pero que por la características de sus actividades deben mantener un contacto directo con lo servicios que ofrece nuestra red interna, tal es el caso de vendedores, asesores externos, etc, la figura 3 muestra este tipo de conexión.

Este tipo de conexión por lo general consiste en proporcionar acceso desde una red pública, con las mismas políticas de la red privada a nuestro usuraos remotos, manteniendo las políticas de seguridad correspondientes y aplicando cada una de las técnicas de cifrado, encripción instaladas en la maquina del cliente. Los accesos pueden ser tanto sobre líneas analógicas, digitales, RDSI o DSL.

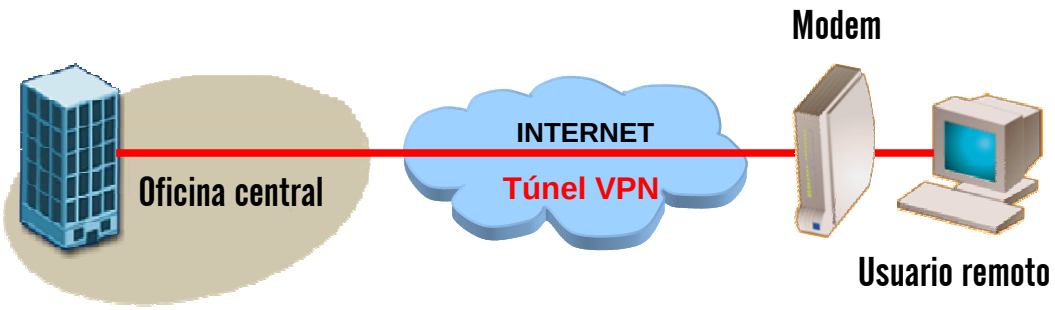


Figura 3. Conexión VPN de usuarios remotos

1.2.2 VPN de Intranet

Este tipo de implementación nos permite conectar localidades fijas a la red corporativa usando conexiones dedicadas, es decir, nos permite conectar nuestra oficina central con suscursales remotas estableciendo un canal logico que nos permite ver ambas como si fueran una sola, como se muestra en la figura 4.

También se le conoce con el nombre de conexión LAN-LAN o punto-punto y se utiliza dentro del entorno de la compañía permitiendo el acceso solo a los empleados de la misma.

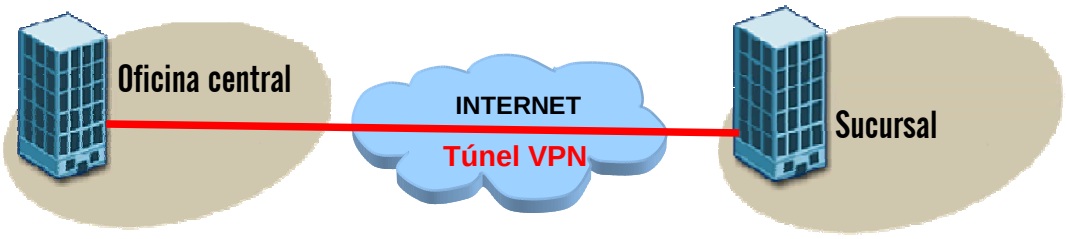


Figura 4. Conexión VPN Lan-Lan

1.2.3 VPN de Extranet

Una VPN de extranet se crea entre la empresa y sus clientes o proveedores, nos permite proporciona acceso limitado a los recursos de la corporación a nuestros aliados comerciales externos como proveedores y clientes, facilitando el acceso a la información de uso común para todos a través de una estructura de comunicación pública.

Es en esta implementación donde el comercio electrónico e-commece tiene su mayor impacto ya que nos permite realizar transacciones de manera segura y efectiva.

1.3 Seguridad de los Datos

Las redes de computadores están jugando un papel cada vez más vital en las operaciones cotidianas de las empresas sin importar su tamaño o la industria a la que pertenezcan. Desde e-commerce y correo electrónico hasta los archivos que se comparten día con día, los empresarios del siglo XXI saben que una red de área local rápida y confiable y el acceso a Internet, son la clave para poder trabajar eficientemente, comunicarse con los empleados y llevar a cabo transacciones con los clientes y socios de negocios.

La conectividad, sin embargo, tiene sus riesgos. Las deben hacer de la seguridad de la red un tema prioritario o no podrán aprovechar los beneficios de estar conectadas con un mundo más amplio. Más que un tema exclusivamente técnico, la seguridad es ahora una necesidad competitiva. Hoy en día, toda empresa luchando por ser cada vez mayor, debe satisfacer estándares corporativos de comunicaciones seguras. Una vez que una compañía comienza a tomar órdenes con tarjetas de crédito, a almacenar direcciones de clientes o a manejar información confidencial de sus clientes, proveedores y socios, los datos deberán protegerse de ojos no autorizados. Un hacker malicioso o un mensaje infectado con un virus podrían causar estragos en archivos valiosos; y, más importante aún, en la capacidad de una empresa de prosperar y crecer.

1.3.1 Amenazas de seguridad

Existen amenazas a la seguridad de una red contra las cuales se deberá proteger una empresa.

1. Intrusiones no autorizadas

Los hackers buscan rutas desprotegidas en las redes y computadoras individuales. Una vez dentro de la red, pueden robar datos, dañar archivos y aplicaciones, o prevenir el uso de la red por los usuarios legítimos: Todas estas situaciones podrían resultar desastrosas. La mejor defensa en contra de los ataques de hackers es un Firewall.

Un Firewall se interpone entre la red interna y el “mundo desprotegido” externo, e inspecciona todo el tráfico que intente entrar a la red interna. Sin importar si está basado en hardware o software, el Firewall reconoce, registra y bloquea toda actividad sospechosa en la red que pueda apuntar hacia algún intento inautorizado de acceso.

En las compañías pequeñas, el perímetro de la red es muchas veces una línea de cable o de DSL (Digital Subscriber Line) que se conecta a la LAN. Para ello, un Firewall basado en hardware provee la mejor protección y es lo más económico, cuando se implementa como un gateway seguro instalado entre un módem de cable o DSL y la LAN. Un gateway seguro ofrece protección óptima

en situaciones donde la seguridad de datos es esencial. Los firewalls de hardware deberán incluir las siguientes funciones avanzadas:

· Inspección de paquetes stateful, que inspecciona los datos al llegar al Firewall para determinar si se les permitirá entrar en la LAN.

· Control de tráfico, que admite los datos que entran en orden de importancia.

· Tecnología VPN (Virtual Private Network) de alta velocidad, que permite que los usuarios se conecten a la LAN rápida y seguramente.

· Control en los servicios de Internet que usan los empleados. Esto puede aumentar la productividad y reducir los riesgos de detección de su red por algún hacker.

· Registros completos de todos los eventos de seguridad que ocurran y la capacidad de enviarlos a un servidor central de registros.

Una empresa que se preocupa por el uso personal de Internet por parte de los empleados durante horas hábiles puede configurar su Firewall, o software de filtración Web, para controlar el acceso a la Web. El gerente de la red puede seleccionar lugares específicos en la Web que estén fuera de límites, bloquear sitios que contengan palabras clave en particular o inclusive denegar acceso a

todos los sitios con la excepción de algunos cuantos que estarán autorizados.

2. Virus

Aunque algunos hackers lanzan deliberadamente ataques de virus para destruir datos, la mayoría de los virus se propagan por contingencia, generalmente cuando los empleados abren algún archivo adjunto en el e-mail o bajan algún archivo que no saben está infectado. Los virus tienden a moverse de una computadora individual a otra, haciéndolos difíciles de detectar en un punto central.

La manera más segura y económica de inocular a una red, sin importar su tamaño, es instalando software anti-virus en todas las computadoras de la red y actualizando las definiciones de virus regularmente. Algunos de los nombres de mayor confianza en protección de virus incluyen a: Symantec, Norton y McAfee.

3. “Olfateo” de datos

Algunas Empresas necesitarán alguna forma de prevenir la intercepción de datos confidenciales, tales como números de tarjetas de crédito; mientras viajan de o hacia sitios de terceros. El uso de encriptación es la mejor forma de asegurar que nadie espíe en los datos transmitidos para obtener algún tipo de

información. La encriptación transforma los datos en códigos que sólo pueden ser leídos por los destinatarios autorizados.

Al conectar sitios remotos o de terceros con datos que viajan a través de Internet, la mejor forma de agregar encriptación es por medio de la tecnología VPN. Una VPN es una conexión remota segura en un “túnel” encriptado de o hacia la red de la compañía, por el cual pueden viajar con seguridad los datos. Los túneles VPN pueden establecerse entre dos empresas por medio de Internet; o algún usuario remoto puede establecer una conexión VPN a la LAN, como un medio para acceder seguramente a los datos corporativos.

4. Seguridad interna de la red

La protección con contraseña de ciertos archivos o aplicaciones limita el acceso sólamente a usuarios autorizados. Por ejemplo, se le podría bloquear al personal de ventas todo acceso a la información de contratación. Sin embargo, la mayoría de las pequeñas y medianas empresas prefieren no establecer este nivel de seguridad; entre más pequeña sea la compañía, más importante es que todos puedan desempeñar todas las funciones. Sin embargo, si una empresa está considerando un crecimiento rápido en el futuro cercano, valdría la pena considerar algún tipo de seguridad interna de su red.

5. E-commerce (comercio electrónico)

Una PYME puede manejar mejor los temas de seguridad de su e-commerce de manera muy simple, al subcontratarlos a algún Proveedor de Servicios de Internet (ISP, por sus siglas en inglés) reconocido que ofrezca tecnología SSL (Secure Socket Layer) para gozar de transacciones en línea seguras y privadas. El ferozmente competitivo mercado de ISPs garantiza que los servicios adecuados de e-commerce estén disponibles para presupuestos de casi todos los tamaños

Capitulo 2. PROTOCOLOS Y ARQUITECTURAS VPN

2.1 Protocolos

A continuación se describen los protocolos mas usados para la interconexión de redes privadas virtuales- Virtual Private Network - VPN

2.1.1 PPTP (Point-to-Point Tunneling Protocol)

Este un protocolo desarrollado por Microsoft y normalizado por la IETF (*Internet Engineering Task Force)* como RFC 2637 para el acceso a redes privadas virtuales (VPN). Este protocolo de red nos permite la realización de transferencias desde clientes remotos a servidores localizados en redes privadas. Para ello emplea tanto líneas telefónicas conmutadas como Internet.

PPTP es una extensión de PPP que soporta control de flujos y túnel multiprotocolo sobre IP.

El acceso a una red privada remota empleando PPTP dispone de dos componentes que trabajan en paralelo:

- Control de la conexión a la red privada, empleando el protocolo TCP, entre el equipo (host) remoto y el servidor de túneles.
- Funcionamiento del túnel IP entre el equipo remoto y el servidor de túneles.

En el control de la conexión, se establece una conexión TCP entre el equipo remoto y el puerto 1723 (reservado para este uso en el documento RFC 1700) del servidor de túneles. Esta conexión tiene como objetivo el establecimiento y la gestión de las sesiones que el usuario establece en la red privada y son transportadas por el túnel. El formato de los paquetes en el control de la conexión será como se ilustra en la figura 5:

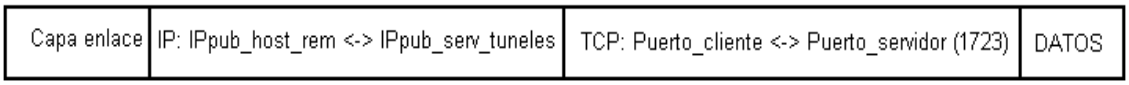


Figura 5. Encabezado de trama usando PPTP

La capa de enlace será la que proporciona el ISP (Internet Service Provider) al equipo remoto. En el caso de Windows 9x, 2000, XP se emplea el protocolo PPP en la fase de establecimiento de la conexión punto a punto entre el ISP y el equipo remoto, seleccionando a continuación como capa de enlace Ethernet aunque en la fase de establecimiento y liberación de la conexión se emplea PPP. La capa de red y transporte gestionan el establecimiento de una conexión TCP desde el cliente (equipo remoto) al puerto 1723 del servidor (servidor de túneles, router de la red corporativa), empleando el direccionamiento público que proporciona el ISP al equipo remoto y que posee el servidor de túneles para el acceso a Internet.

El funcionamiento del túnel IP permite el envío de paquetes IP con direccionamiento privado, empleando un protocolo de control del túnel (GRE,

Generic Routing Encapsulation) y un protocolo de control del enlace entre el equipo remoto y el servidor de túneles. El efecto de este túnel para el usuario del equipo remoto será proporcionarle un acceso a la red LAN corporativa a nivel de red, con una dirección de la red privada. El servidor de túneles se encarga del traspaso de los paquetes de la red LAN que vayan dirigidos a la dirección IP del equipo remoto o a la de broadcast. El protocolo de nivel de enlace entre el equipo remoto y el servidor de túneles es PPP, pues permite un control de establecimiento de sesiones y de autenticación (PAP, CHAP o MS-CHAP). El formato de los paquetes que circularán por el túnel será como se muestra en la figura 6:

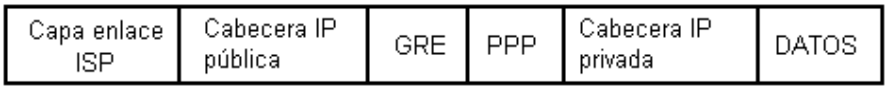


Figura 6. Formato del paquete IP que transita por el túnel

La parte de la cabecera correspondiente a la cabecera de enlace del ISP, cabecera IP pública, cabecera GRE y cabecera PPP se interpretan entre el equipo remoto y el servidor de túneles para el transporte del paquete de la red privada. La parte correspondiente a la cabecera IP privada y datos se interpreta entre el equipo remoto y la LAN corporativa para el acceso a los sistemas de información.

2.1.2 L2TP Layer Two Tunneling Protocol)

Anteriormente se describió cada una de las características del protocolo PPTP, pero para ver como funciona L2TP es necesario hablar de L2F (Layer 2 Forwarding) este protocolo propietario de cisco, tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace: HDLC, PPP, SLIP, etc. El proceso de tunneling involucra tres protocolos diferentes: el protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (IP); el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación (L2F); y el protocolo portador será el encargado de realizar el transporte de todo el conjunto (PPP).

L2TP (Layer 2 Tunneling Protocol) es un protocolo usada para conectar redes privadas a través de Internet de una manera segura por medio de las VPN, combinando los protocolos PPTP de Microsoft y el L2F de Cisco resolviendo los problemas de interoperatividad entre ambos protocolos, proporcionando así un mejor acceso y mayor seguridad. Este Permite el túnel del nivel de enlace de PPP, de forma que los paquetes IP, IPX y AppleTalk enviados de forma privada, puedan ser transportados por Internet.

L2TP encapsula las tramas del protocolo punto a punto (PPP) que van a enviarse a través de redes IP, X.25, frame relay, 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 su 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.

La implementación de L2TP ofrece:

- Soporte de Entornos multiprotocolo L2TP que puede transportar cualquier protocolo enrutado, incluyendo IP, IPX y Appletalk.
- Independiente del medio, éste opera sobre cualquier red con capacidad de distribuir tramas IP. Soporta cualquier tecnología backbone WAN, incluyendo Frame Relay, ATM , X.25 o SONET. Soporta también medios LAN como Ethernet, Fast Ethernet, Token Ring y FDDI.

Para comprender mejor este protocolo es necesario identificar los términos de:

- Access Concentrator (LAC). Es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. También se le conoce como el servidor de acceso a la red en el protocolo Layer 2 Forwarding (L2F).

- Network Server (LNS)

-Network Access Server (Servidor de acceso a la red) NAS. Este dispositivo proporciona a los usuarios acceso temporal a la red bajo demanda. Este acceso es punto a punto, de uso típico en líneas de la red telefónica convencional o RDSI. En la implementación Cisco, un NAS sirve como LAC.

En un entorno de conexiones telefónicas, un túnel L2TP puede iniciarse desde un servidor de acceso de red (NAS) (como un túnel iniciado NAS) o desde software cliente (como un túnel iniciado por el cliente) hacia un router que actúa como un punto de terminación del túnel.

En un entorno xDSL, la conmutación por canal virtual ATM de usuario se extiende desde el CPE a una función NAS centralmente localizada, la cual origina los túneles L2TP a los LNS.

Encapsulación en L2TP

La encapsulación de L2TP sobre paquetes IPSec consta de dos niveles:

1. Encapsulación L2TP : Una trama PPP (un datagrama IP, un datagrama IPX o una trama NetBEUI) se empaqueta con un encabezado L2TP y un encabezado UDP.

El mensaje L2TP resultante se empaqueta a continuación con un encabezado y un finalizador de Carga de seguridad de encapsulación (ESP, Encapsulating Security Payload) de IPSec, un finalizador de autenticación IPSec que proporciona autenticación e integridad de mensajes y un encabezado IP final. El encabezado IP contiene las direcciones IP de origen y de destino que corresponden al cliente VPN y al servidor VPN.

La figura 7 muestra la encapsulación L2TP e IPSec para un datagrama PPP

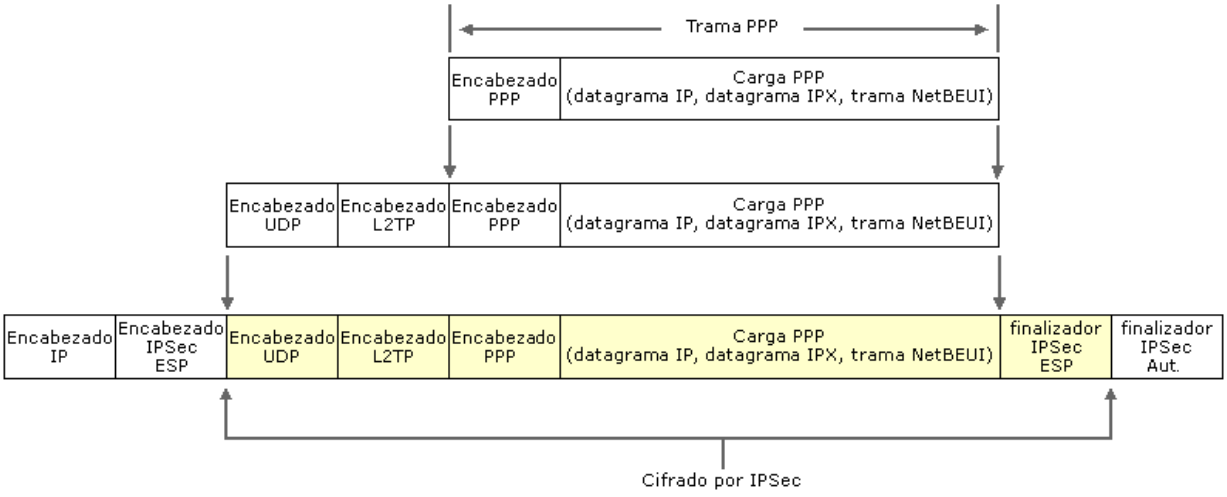


Figura 7. Formato del paquete IP cifrado en L2TP

L2TP es una solución que ofrece una larga lista de ventajas a los usuarios de empresa: Estas ventajas incluyen:

1. Seguridad y prioridad garantizada para la mayoría de las aplicaciones esenciales de trabajo.
2. Una mejor conectividad, costes reducidos y libertad para redistribuir los recursos en núcleos de funciones
3. Un entorno de acceso de red remota flexible y ampliable sin comprometer la seguridad corporativa o poner en peligro las aplicaciones esenciales.

2.1.3. IPSEC (Ip secure)

Las siglas IPSec corresponden en ingles con "*Internet Protocol Security*". IPsec es un grupo de extensiones de la familia del protocolo IP. IPSec provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. IPsec provee servicios similares a SSL, pero a nivel de redes, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto.

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 computadores. Debido a que dispone de tantas opciones, IPsec es un poco complejo.

De un modo lógico, IPsec funciona en cualquiera de estos tres modos:

- Anfitrión-a-Anfitrión
- Anfitrión-a-Red
- Red-a-Red

En cualquier escenario en el que haya una red, el concepto de enrutador está implícito, como en Anfitrión-a-Enrutador (y este enrutador controla y cifra el tráfico para una *Red* particular).

Como se puede ver, IPsec se puede usar como túnel de tráfico para conexiones de VPN. Sin embargo, su utilidad va más allá de las VPN. Con un registro central de "intercambio de claves de Internet" IKE, *Internet Key Exchange*, cada máquina en Internet podría comunicarse con otra y usar cifrado y autenticación de alto grado.

IPSec define el formato de paquetes para una modalidad de túnel IP-sobre-IP, llamada *IPSec Túnel Mode*. Un túnel IPSec consiste en un cliente túnel y un servidor túnel, los cuales están configurados para usar tunneling IPSec y algún mecanismo de cifrado.

IPSec Tunnel Mode utiliza un método de seguridad para encapsular y encriptar paquetes IP para transmitirlos de forma segura a través de una red IP privada o publica (Redes Internet).

Los datos encriptados son vueltos a encapsular en un encabezado IP y enviados a la red para ser entregados al otro extremo del túnel.

Una vez recibido el datagrama, el servidor túnel descarta el encabezado IP y desencripta el contenido del paquete para recuperar el paquete IP original. Este paquete, a su vez, es procesado normalmente y enrutado a su destino final.

IPSec soporta únicamente trafico IP los paquetes IP cifrados viajan como datos de usuario dentro de paquetes IP convencionales.

IPSec provee encripción y autenticación al nivel de IP en la pila de protocolos de red, por lo que protege todo tipo de tráfico transportado sobre IP y puede ser utilizado en routers, firewalls, servidores de aplicaciones e incluso desktops y laptops.

Se utilizan tres protocolos:

- AH(Authentication Header)
- ESP(Encapsulating Security Payload)
- IKE(Internet Key Exchange)

El protocolo IKE prepara las conexiones IPSec (ESP o AH) tras negociar ciertos parámetros (algoritmos a utilizar, claves, etc). Esto se realiza intercambiando paquetes en el puerto 500/UDP entre ambos gateways. IKE se encuentra definido en RFC2409.

AH brinda un servicio de autenticación a nivel de paquetes. Esta autenticación se brinda en forma separada a la encripción agregando un header de autenticación (AH) entre el header IP y el resto. Los detalles pueden encontrarse en RFC2402. Los datos de autenticación del header dependen tanto de una clave simétrica como de cada byte de los datos que son autenticados. La técnica utilizada es HMAC (RFC2104). Los algoritmos involucrados son SHA y MD5. AH utiliza el protocolo 51.

El protocolo ESP brinda encripción y autenticación de paquetes. Puede usarse con o sin AH.

La autenticación se realiza en forma similar a AH. Los algoritmos de encripción pueden variar de acuerdo a la implementación (los RFCs requieren únicamente DES y encripción nula). FreeS/WAN, la implementación de IPSec para Linux utiliza 3DES actualmente, aunque existen patches para agregar soporte de otros, como AES (Rijndael), Blowfish y CAST. Pese al requerimiento de DES, FreeS/WAN no lo implementa, ya que como anteriormente se dijo es inseguro. ESP utiliza el protocolo 50.

Este protocolo de seguridad que opera en la capa de red del modelo OSI, nos proporciona un canal seguro, ofreciendo aspectos importantes para el envío de paquetes IP por Internet, tales como:

- Confidencialidad: Los datos enviados a través de la red solo los pueden entender los participantes que hacen parte de la sesión.
- Integridad de Paquetes: Garantiza que en el trayecto de comunicación los datos no sean modificados.
- Autenticidad de Origen: Valida el remitente de los datos.
- Protección a Repeticiones: Verifica que una sesión no sea grabada y repartida, excepto que tenga autorización para hacerlo, esto se hace

mediante dos protocolos: Authentication Protocol, (AH) y Encapsulated Security Payload (ESP).

Pueden realizarse conexiones IPSec de dos modos diferentes: modo de transporte y modo de túnel.

El modo de transporte es una conexión de host a host y sólo involucra dos máquinas. Cada equipo realiza su propio procesamiento de IPSec y routea paquetes en forma acorde (algunos via IPSec).

El modo de túnel es una conexión entre gateways, los cuales proveen túneles para ser utilizados por máquinas clientes detrás de cada gateway. Las máquinas clientes no realizan ningún procesamiento de IPSec, tan sólo routean a los gateways.

El siguiente cuadro muestra una comparación entre los diferentes protocolos descritos.

Característica	Descripción	PPTP/ PPP	L2TP/ PPP	L2TP/ IPSec	Transporte IPSec	Túnel IPSec
Compatibilidad multidifusión	Puede transmitir tráfico multidifusión IP además del tráfico IP de difusión simple.	Sí	Sí	Sí	No	Sí

Característica	Descripción	PPTP/ PPP	L2TP/ PPP	L2TP/ IPSec	Transporte IPSec	Túnel IPSec
Autenticación de usuario	Puede autenticar al usuario que está iniciando las comunicaciones.	Sí	Sí	Sí	WIP[1]	WIP
Autenticación del equipo	Permite autenticar los equipos implicados en las comunicaciones.	Sí[2]	Sí	Sí	Sí	Sí
Compatible con NAT	Puede pasar por traductores de direcciones de red para ocultar uno o ambos extremos de las comunicaciones.	Sí	Sí	No	No	No
Compatibilidad multiprotocolo	Define un método estándar para transmitir tráfico IP y no IP.	Sí	Sí	Sí	No	WIP
Asignación dinámica de direcciones IP de túnel	Define una forma estándar de negociar una dirección IP para la parte de túnel de las comunicaciones. Es importante para que los paquetes devueltos se enruten de vuelta a través de la misma sesión en vez de a través de una ruta sin túnel e insegura y para eliminar la configuración manual estática del sistema final.	Sí	Sí	Sí	No disponible	WIP
Cifrado	Puede cifrar el tráfico que transmite.	Sí	Sí	Sí	Sí	Sí
Utiliza PKI	Puede utilizar PKI para implementar el cifrado y/o la autenticación.	Sí	Sí	Sí	Sí	Sí
Autenticidad de paquetes	Proporciona un método de autenticidad para asegurarse de que el contenido del paquete no se modifica mientras se transmite.	No	No	Sí	Sí	Sí

Cuadro comparativo entre los protocolos PPTP, L2TP e Ipsec.

2.1.3.1 Firma Digital

La firma digital garantiza que la información recibida es auténtica y no ha sido alterada en modo alguno.

La creación de una firma digital es un procedimiento de dos pasos. Primero, el mensaje transmitido es procesado por un algoritmo de encripción particular: la función de hash, que transforma un mensaje de largo arbitrario en un número único de longitud fija. Este número creado por la función hash es llamado el digest del mensaje. Si se cambia en cualquier forma el mensaje original, el digest de este cambia también. Las funciones de hash son muy conocidas, como SHA (Secure Hash Algorithm) y MD5(Message Digest 5). El segundo paso para crear la firma digital, es encriptar el digest del mensaje utilizando la clave privada. Esto da como resultado la firma digital la figura 8 muestra este proceso.

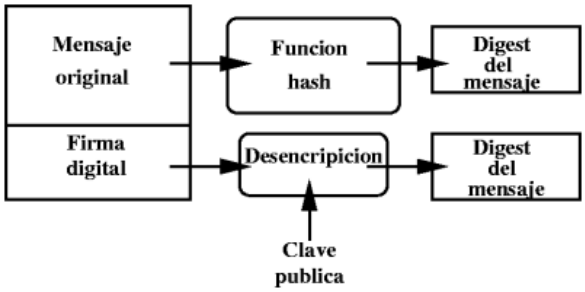


Figura 8. Firma Digital

Para garantizar la autenticidad de un mensaje, se crea una firma digital para el mismo y se incluye en el. El recipiente comprueba la autenticidad mediante:

1. La desencripción de la firma digital utilizando la clave pública del remitente (esto genera el digest del mensaje original)
2. Cálculo del digest del mensaje utilizando la función de hash (esto genera un nuevo digest del mensaje basado en los datos recibidos)
3. Comparación de resultados

Si los resultados son idénticos, entonces el mensaje es auténtico y no ha sido alterado. Un mensaje que incluye una firma digital es un mensaje firmado.

Entonces, un certificado digital es un tipo especial de mensaje firmado que asocia a una persona, organización o computadora con una clave pública. Una entidad certificadora, llamada CA (*Certificate Authority*), acepta claves públicas con una prueba de identidad y crea certificados digitales dejándolos disponibles para otras personas. La entidad certificadora es un organismo confiable por ambas partes, el cual declara que efectivamente una clave pública pertenece a una persona, organización o sistema. Esta entidad puede utilizar protocolos de directorio como X.500 o LDAP para brindar sus servicios, o puede estar implementada haciendo uso de protocolos propietarios.

PKI (*Public Key Infrastructure*: Infraestructura de claves públicas) es una serie de servicios de seguridad para administrar claves, certificados digitales y

políticas de seguridad. Las PKIs están diseñadas para dar soporte a grupos abiertos, a fin de manejar interacciones entre personas y sistemas que no se conocen previamente. Por ejemplo, en un sistema de compras a través de Internet. En particular, las PKIs posibilitan la coordinación entre múltiples CAs, dado que distintas personas o sistemas puede poseer certificados emitidos por distintas CAs.

2.2 Tipos de Arquitecturas y Soluciones VPN

2.2.1 VPN Proporcionas por un PSI (Proveedor de Servicios de Internet)

[2]Las RPV de proveedor de servicios son una buena alternativa para las compañías que desean que un proveedor de servicio se encargue de su infraestructura de Internet.

Aun cuando un proveedor de servicio no sea la única manera de lograr este modelo de consultoría externa, es conveniente, el PSI probablemente controlara el acceso a Internet de su empresa, lo cual facilitara la solución del problema.

En una solución de proveedor este llevara a cabo todas las tareas de servicio mientras que al mismo tiempo hará recomendaciones valiosas y ofrecerá

[2] Steven Brown. Implementación de Redes Privadas Virtuales

lineamientos sobre la seguridad si es necesario. El centro de operaciones de red por lo general llamado COR es un equipo de individuos altamente capacitados que se ocupa de las comunicaciones, de transporte de Internet y la seguridad las 24 horas del día los 7 días a la semana liberando así a la compañía para que se centre en sus negocios principales, es así como el PSI se encargara de todo lo relacionado con la VPN proveerla, mantenerla y asegurar su correcto funcionamiento y seguridad en las misma.

2.1 2 Soluciones Basadas en Firewall

[3]Las VPN basadas en Firewall probablemente son las más comunes hoy en día y muchos proveedores ofrecen este tipo de configuración. Esto no significa que las VPN basadas en Firewall sean superiores a otras formas de VPN, sino que más bien se trata de una base establecida a partir de la cual se puede crecer. Actualmente sería difícil de encontrar una organización conectada a Internet que no utilice ningún tipo de Firewall. Debido a que estas organizaciones ya están conectadas a Internet, todo lo que se necesita es añadir software de cifrado. Lo mas probable si su organización a adquirido recientemente un Firewall, es que incluya la capacidad para implementar tecnología de cifrado de VPN cuando decimos tecnología VPN nos estamos refiriendo a algún tipo de esquema de cifrado proporcionado con el dispositivo. Si usted desea un cifrado

[3] Steven Brown. Implementación de Redes Privadas.

distinto, lo más probable es que necesite comprar alguno. Muchos proveedores incluyen su tecnología de cifrado propietaria sin costo adicional del producto.

Existen muchos proveedores entre los cuales elegir cuando se considera una VPN basada en Firewall, y los productos están disponibles en todas las plataformas. Un aspecto importante de la seguridad es el sistema operativo subyacente, no existe un dispositivo que sea 100 por ciento seguro, así que si se crea la VPN en ese dispositivo, necesitará asegurarse de que el sistema operativo subyacente sea seguro.

Si decide que una solución VPN basada en Firewall es el camino correcto a seguir, sería conveniente observar algunas encuestas recientes sobre los productos de Firewall, de esta manera será más fácil comparar subjetivamente distintos Firewall.

Podría presentarse una confusión respecto a lo que queremos decir con una solución Firewall. Cuando decimos que debe añadir tecnología VPN a su Firewall, usted podrá suponer que nos referimos a cualquier tecnología de Firewall. Esto es incorrecto, ya que hasta el momento existen tres tipos de implementaciones de Firewall entre las cuales elegir: inspección de estados, Proxy y filtrado de paquetes. Cuando decimos “añada tecnología VPN a un Firewall”, nos estamos refiriendo a añadir tecnología VPN únicamente a un Firewall de inspección de estados. De la misma manera que la tecnología VPN en si misma se ejecuta en los niveles mas bajos de la pila de OSI, el Firewall

debe hacerlo o puede caer en problemas de desempeño importantes. Un servidor Proxy se ejecuta en el nivel 7, el nivel de aplicaciones del modelo OSI, y el Firewall de filtrado de paquetes también tiene que examinar el paquete completo cada vez que pasa. Un Firewall de inspección de estados se ejecuta en los niveles 2 y 3 debido a este requisito de procesamiento, usted solo deberá añadir tecnología VPN a un Firewall de inspección de estados.

2.2.2.1 Elegir el Firewall Adecuado

El Firewall debería ser considerado como parte de una solución corporativa de seguridad, pero desafortunadamente por sí mismos no son suficientes para crear una VPN, esto es debido a que un Firewall no puede monitorear o prevenir los cambios de datos que ocurren en un paquete a través de Internet, es decir, asegurar la integridad de los mismos.

Si se instala encriptación basada en host en todos los computadores (usando IPSec, por ejemplo), se hace necesaria la instalación de Firewalls en la organización para reforzar la política de seguridad de la red de la empresa ya que estos son parte de un perímetro de defensa.

IPSec en cada escritorio provee privacidad y autenticación, pero no asegura que la política de seguridad esté reforzada completamente.

Los firewalls son considerados, a menudo, para ser puntos de terminación VPN porque pueden administrar la política de seguridad de la red completa a través de un solo punto. Sin embargo, los firewalls son dispositivos complejos de instalar y gestionar debido a la posibilidad de conflicto entre reglas si no se tiene cuidado al establecer o modificar las reglas base. Adicionalmente, tener firewalls desempeñando servicios VPN incrementa el riesgo en caso de que e Firewall falle o se vea comprometido. Sin tener en cuenta que protocolo es usado para la VPN, es necesario considerar cómo el Firewall se integra con el resto de sistemas de administración de seguridad y red.

Si ya se está usando un sistema particular para la autenticación de usuarios remotos, entonces se puede simplificar la transición mediante la instalación de un Firewall que sea compatible con el sistema actual.

Si se planea usar un sistema de autenticación basado en certificados digitales, se debe pensar en cómo se distribuirán y verificarán los certificados. Es muy probable que los firewalls sean instalados en más de un sitio. Si el Firewall soporta administración sincronizada de sitios, será más capaz de mantener una política de seguridad más consistente. Esta administración puede involucrar intercambio de ficheros, o algunas otras formas de gestión remota. Si las capacidades de administración están incluidas en el producto, se asegura que el acceso remoto al Firewall es seguro. Debido a que los firewalls parecen ser

la localización lógica para la terminación de una VPN y refuerzan las políticas de seguridad, hay firewalls más compatibles con VPN que cualquier otra clase de dispositivo VPN.

Usar firewalls para construir una VPN es una solución factible para algunas redes. Las VPNs basadas en firewalls son, probablemente, lo más adecuado para pequeñas redes que transfieren pequeñas cantidades de datos y permanecen relativamente estáticas. Si se busca un mayor rendimiento, existen otras soluciones mejores.

2.2.3 Soluciones de Software

Una red privada virtual implementada mediante software, no es más que establecer una conexión cliente/servidor entre el software VPN del cliente y el software VPN instalado en el servidor.

Esta solución nos permite crear un túnel VPN iniciado con una petición del cliente al servidor de nuestra compañía que se encargara de determinar las características de la sesión tales como: el tipo de cifrado que se utilizara, los algoritmos de autenticación y otros datos también requeridos.

Para este tipo de implementación se hace necesaria la administración de claves adecuada y posiblemente una autoridad emisora de certificados con el objeto de mantener la seguridad y autenticidad de las sesiones.

Las ventajas que ofrece este tipo de solución es que nos permite ser usada en una amplia variedad de plataformas, lo que facilita la instalación y el manejo de la misma.

Las posibles desventajas que se pueden presentar son problemas tonel desempeño NAT, además que algunas de estas soluciones tiene tecnologías de cifrado antigua y son propietarias, algunos no se pueden administrar remotamente y no presentan capacidades de supervisión.

2.2.3.1 VPN en Windows

Para configurar una VPN bajo Windows se necesita lo siguiente:

- Conexión a Internet tanto para el servidor local de NT como para las máquinas remotas.
- Una dirección IP estática para el servidor NT.
- Proxy que se ejecute en el servidor NT, para evitar el acceso desautorizado al sistema.
- Direcciones IP para los recursos a compartir.

- Adaptador virtual de la red instalado en la máquina remota o cliente.

La secuencia de pasos es:

- Hacer una lista de las direcciones IP de los recursos que serán compartidos a través de Internet.
- Instalación y ejecución del proxy.
- En el servidor NT, se deben configurar los archivos del usuario NT para que pueda llamar y conectarse al servidor, garantizando su acceso al sistema con los permisos de la VPN.
- Luego de estos pasos, se deberá instalar el adaptador privado de la red en la máquina cliente, como se indica:
- Dentro del Diálogo de Red, que se muestra debajo, y al cual se accede a través de la opción Propiedades del icono Entorno de Red, se presiona el botón Add.

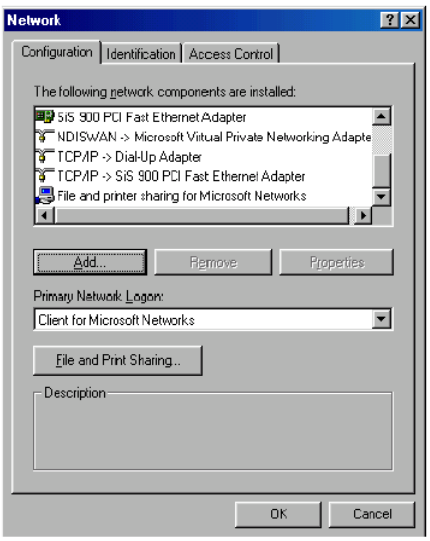


Figura 9. Dialogo de Red

Aparecerá la siguiente pantalla, se deberá seleccionar Adapter y luego presionar el botón Add

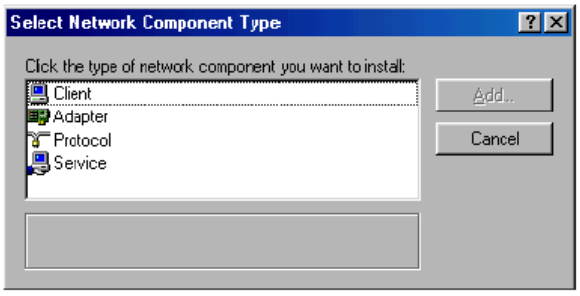


Figura 10. Componentes de Red

Aparece el cuadro Select Network adapters, donde se deberá elegir el fabricante y el adaptador como se muestra en la siguiente figura:

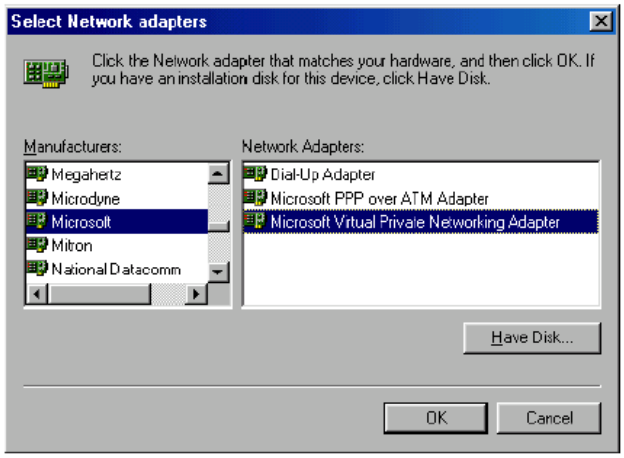


Figura 11. Adaptadores de Red

Posteriormente, para instalar la conexión a la LAN, se deberá acceder al Acceso Remoto a Redes

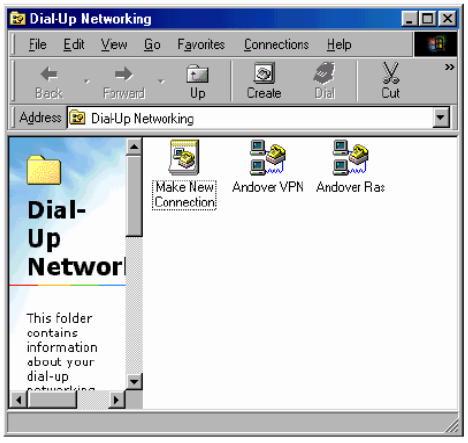


Figura 12. Ventana de "Dial-Up"

Se selecciona Make a New Connection, apareciendo la siguiente pantalla, donde se podrá elegir el adaptador de VPN:

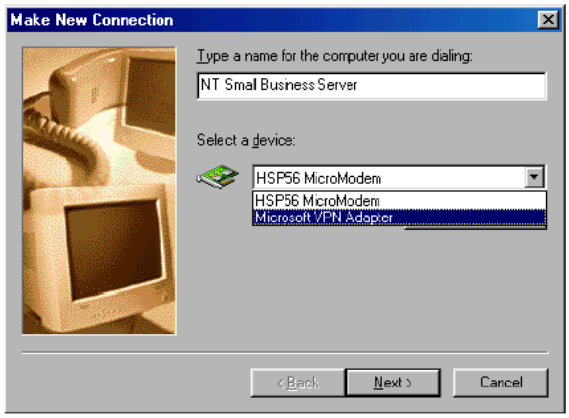


Figura 13. Ventana de Nueva Conexion

Luego de presionar el botón Next, se deberá introducir la dirección IP del servidor VPN en la siguiente pantalla:

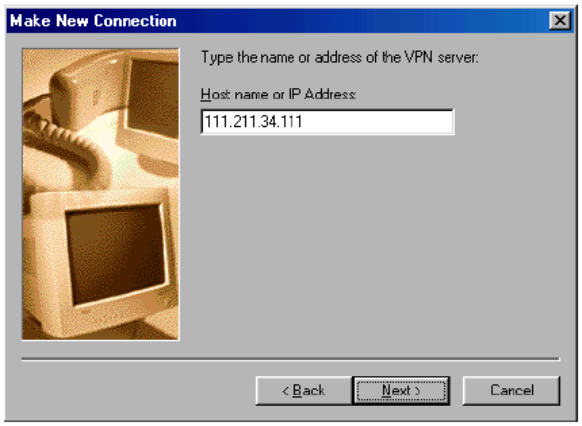


Figura 14. Ventana de Nueva Conexión

Así se finaliza la creación de la nueva conexión:

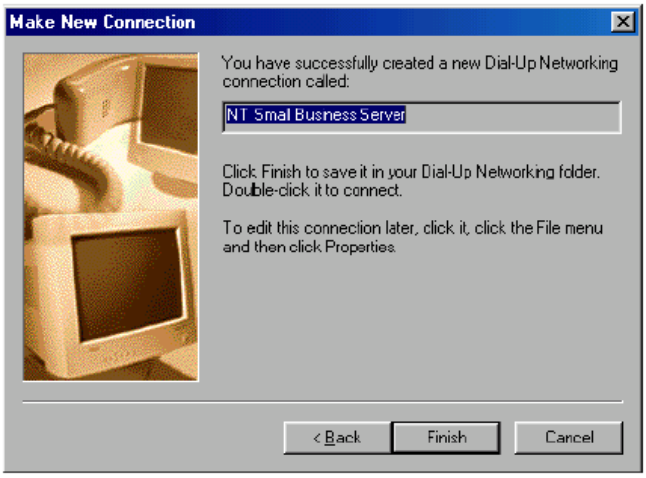


Figura 15. Ventana de Nueva Conexión

Para acceder al servidor NT, se abre el Acceso Remoto a Redes:

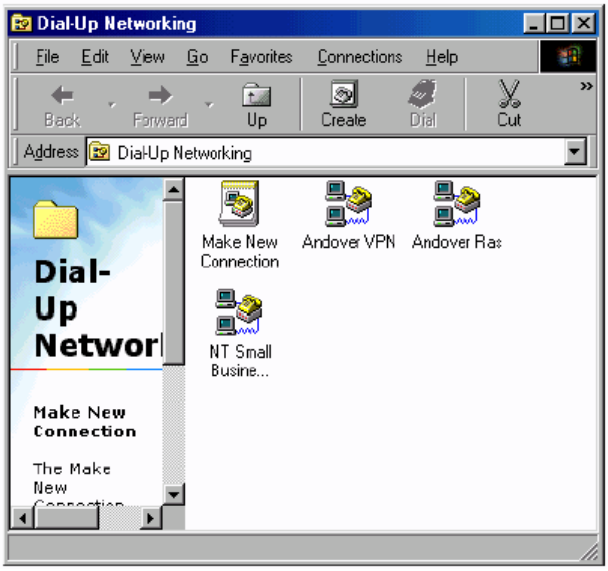


Figura 16. “Dial- Up Network”

Al hacer doble-click en el icono de la conexión VPN, aparecerá la siguiente pantalla, donde se debe introducir el nombre de usuario, la contraseña y la dirección IP del servidor NT:

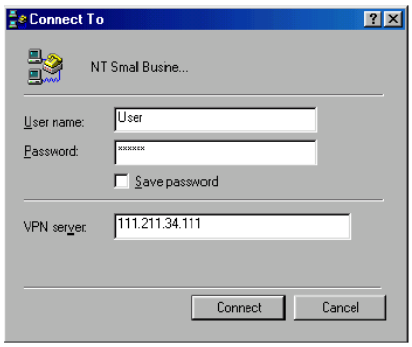


Figura 17. Conexión de VPN

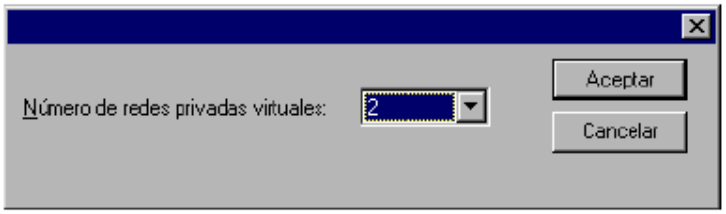
Para configurar el servidor VPN, se deberá configurar PPTP, activar el filtro PPTP y activar el soporte PPTP en los clientes.

Para configurar PPTP en el servidor RAS y en los clientes que vayan a utilizarlo, se deberán realizar los siguientes pasos:

Dentro de Red en el Panel de Control, seleccionando Protocolos, se deberá presionar el botón Agregar:

Se selecciona Point to Point Tunneling Protocol, y, luego de copiados los archivos, aparecerá el cuadro de diálogo Configuración de PPTP. El campo

Número de redes privadas virtuales indica el número de conexiones PPTP admitidas. En el ejemplo, se establecen 2 VPN:



Luego, se inicia la herramienta de configuración RAS, donde se deben añadir los puertos virtuales que darán servicio a las redes privadas virtuales que se deseen establecer. Al presionar el botón Agregar, se accede al dialogo Agregar dispositivo RAS:

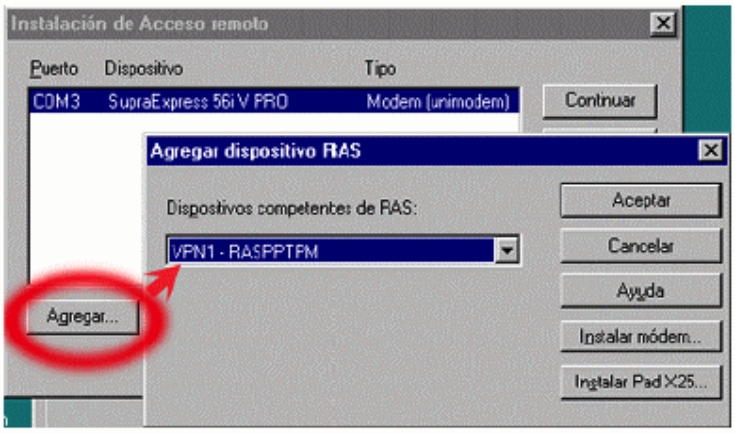


Figura 18. Protocolo de Red

Después de ingresadas las entradas, se presiona Aceptar. Luego se podrá seleccionar cada entrada del diálogo Instalación de Acceso Remoto, para configurar el uso del puerto. Las opciones son: Sólo recibir llamadas o Hacer y recibir llamadas.

Después de añadir todos los dispositivos virtuales, se podrá cerrar este diálogo para volver a la ficha Protocolos. Al reiniciar la computadora, ya estará configurado el server.

Para la activación del filtro PPTP, se debe selecciona la solapa Protocolos de Panel de Configuración / Red. Dentro de esta pantalla, se elige Protocolo TCP/IP, luego Propiedades. En la solapa Dirección IP, se selecciona el adaptador de red sobre el que se aplicará el filtro. Luego de presionar el botón Avanzadas, se marca la casilla Activar filtro PPTP y, por último, se reinicia la máquina para activar la configuración.

Cuando un cliente se conecta a Internet, el procedimiento para establecer un túnel VPN consta de dos pasos:

Establecimiento por parte del cliente mediante una conexión de acceso telefónico a través de un ISP.

Establecimiento de una conexión PPTP con el servidor RAS.

Cuando un cliente se conecta directamente a Internet, no es necesario establecer una conexión de acceso telefónico. Sin embargo, el procedimiento para iniciar la conexión PPTP con el servidor RAS es idéntico. Para establecer una conexión PPTP es necesario crear una entrada especial en la guía telefónica. Esta entrada se distingue por dos características:

El campo Marcar utilizado tiene uno de los dispositivos virtuales VPN añadidos a la configuración RAS al instalar PPTP. Esta lista sólo muestra los VPN configurados para hacer llamadas.

El campo Presentación preliminar de número telefónico contiene el nombre DNS o la dirección IP del servidor PPTP.

La creación de una conexión PPTP implica también dos pasos:

Se abre la aplicación Acceso telefónico a redes, utilizando la guía telefónica que permite acceder al ISP a través de un número de teléfono y un modem.

Establecida la conexión, se debe abrir la entrada de la guía telefónica que se conecta al túnel PPTP mediante un nombre DNS o una dirección IP.

Si el cliente está conectado directamente a Internet, sólo es necesario el segundo paso

2.2.3.2 VPN en Linux

El demonio VPND permite crear enlaces seguros sobre TCP/IP con claves de hasta 512 bits y algoritmo de encriptación BLOWFISH, montando una interfaz virtual serie que proporciona la posibilidad de enrutamiento de IP entre redes. Los pasos a seguir son:

- Dar soporte SLIP en el kernel LINUX, recompilándolo y probando que funcione.
- Instalación del paquete vnpd, que, en Debian, se puede hacer con '**apt-get install vpnd**'.
- Creación de una clave de sesión, utilizando '**vpnd –m /etc/vnpd/vpnd.key**', que debe ser pasada al otro extremo de la VPN mediante un medio seguro, ya que es la clave que ambos extremos de la VPN comparten.
- Configuración de los extremos de la VPN, siguiendo la estructura Cliente/Servidor. A continuación, se muestran el contenido de los archivos **vpnd.conf** de configuración para el servidor y el cliente.

Archivo **/etc/vpn/vpnd.conf** para el servidor:

```
mode server

# Direccion IP y puerto del servidor

server a.b.c.d 2001
```

```
# Direccion IP y puerto del cliente

client w.x.y.z 2001

# Direccion IP privada del servidor

local a.b.c.d

# Direccion IP privada del cliente

remote w.x.y.z

# Opciones generales

autoroute

Keepalive 10

noanswer 3

keyfile /etc/vnpd/vnpd.key

pidfile /var/run/vpnd.pid

keyttl 120

ramdomdev /dev/urandom

mtu 1600
```

Archivo **/etc/vpn/vpnd.conf** para el cliente:

```
mode client

# Direccion IP y puerto del servidor

client w.x.y.z 2001

# Direccion IP y puerto del cliente

server a.b.c.d 2001

# Direccion IP privada del servidor

local w.x.y.z

# Direccion IP privada del cliente

remote a.b.c.d

# Opciones generales

autoroute

Keepalive 10

noanswer 3

keyfile /etc/vnpd/vnpd.key
```

pidfile /var/run/vpnd.pid

keyttl 120

ramdomdev /dev/urandom

mtu 1600

Una vez creados estos archivos, se podrá levantar la VPN, iniciando los demonios con '**/etc/init.d/vpnd start**'. Para comprobar el correcto funcionamiento, se puede hacer *pings* a las direcciones privada y del otro extremo y verificar con '**ifconfig –a**' que exista una nueva interfaz como la siguiente:

sl0 Link encap: VJ Serial Line IP

[4]Inet addr: 10.0.0.1 P-t-P: 10.0.0.2

Mask : 255.255.255

UP POINTOPOINT RUNNING NOARP

MULTICAST MTU: 1600 Metric: 1

Rx packets:0 errors: 0 dropped:0

overruns: 0 frame: 0

Compressed: 0

[4] KOLESNIKOV OLEGHATCH. Brian Redes Privadas Virtuales con LINUX

Tx packets:0 errors: 0 dropped:0

overruns: 0 carrier: 0

Collisions: 0 compressed: 0

txqueuelen: 10

RX bytes: 0 (0.0 b) TX bytes; 0 (0.0 b)

2.3 Soluciones de Hardware

Uno de los mercados de mayor crecimiento para proveer soluciones VPN consiste en ofrecer soluciones VPN integradas en el hardware, las cuales en una única caja incluye toda la funcionalidad requerida para VPN, eliminando la necesidad de añadir software y hardware a un Firewall existente o un router y, en la mayoría de los casos, cualquier hardware para la conexión WAN.

Uno de los propósitos de estos productos VPN es no cargar las funciones VPN desde un Firewall o router que no tienen potencia computacional para sostener funciones como la encriptación.

No todos los productos ofrecen las mismas características. Algunos productos están dirigidos a proveer una solución “turnkey” para la seguridad, incluyendo un Firewall.

Otras soluciones VPN hardware abarcan desde cajas centradas en la encriptación hasta sistemas que sostienen todos los aspectos de una conexión a Internet, incluyendo conexiones WAN, routing, VPNs, DNS, y servicios e-mail, entre otros. Integrar varias funciones en un producto simple puede ser particularmente atractivo para los negocios que no tienen los recursos necesarios para instalar y mantener diferentes servicios de red y que tampoco quieren fuentes externas para sus operaciones VPN.
Incluso, puede resultar algo muy positivo, debido a que esta caja pasa a ser ahora el único punto de fallo. Esta acepta que todas las funciones de seguridad controlando las

Comunicaciones con Internet pueden fallar cuando un único servicio se cae; pero al menos, un enlace de comunicación roto no significa que los atacantes pueden entrar en la Intranet a través de ese enlace. Sin embargo, es completamente diferente poner un servidor de mail o un servidor Web en la misma caja, ya que si esta falla, entonces los empleados pueden perder algunos servicios internos también.

Como ya hemos indicado en la figura anterior, las funciones importantes de cualquier VPN son: encriptación, autenticación, túneles, y gestión de claves. Dependiendo de que protocolo se planee usar para la construcción de la VPN, se hace un énfasis diferente en cada una de estas funciones. PPTP, por ejemplo, se centra en tunelización e incluye encriptación débil, y L2TP soporta autenticación fuerte de usuarios; por otro lado, IPSec soporta encriptación y gestión de claves, pero todavía necesita trabajar más para ser usado con autenticación fuerte de usuario.

La principal diferencia entre los productos es el número de túneles simultáneos que pueden soportar y los servicios añadidos que son introducidos en los productos. Por ejemplo, el número de túneles puede variar desde 8 hasta 2000. Algunos productos incluyen gestión de ancho de banda y soporte extensivo para sistemas de autenticación de usuario, y otros productos han incluido servidores Web y e-mail.

Algunos de los servicios están disponibles en más de un producto. Si no se necesitan todos los servicios listados para un producto particular, es buena idea comprobar si existen soluciones parciales, es decir, productos que ofrezcan servicios separados e independientes; por ejemplo, Radguard ofrece de forma separada unidades Firewall y encriptación.

Para la gestión de claves, muchos de los productos dependen de un servidor de certificados que se ha instalado en una estación Windows o Unix y debería ser seguro contra manipulaciones y tener un acceso muy restringido para el personal interno. Incluso, para una mayor seguridad, una pieza adicional de hardware dedicado puede se instalada para la gestión de claves, permitiendo a la VPN continuar su ejecución incluso sin la Autoridad Certificadora.

Generalmente, se espera que estas soluciones hardware mejoren las funciones VPN, especialmente la encriptación, más rápido que su software homólogo. Sin embargo, determinar el rendimiento actual de estos productos es difícil.

A pesar de que muchos de los dispositivos hardware ofrecen el mejor rendimiento posible para la VPN, es necesario decidir cuantas funciones se quieren integrar en un único dispositivo. Para pequeños negocios o pequeñas oficinas sin un número elevado de personal, especialmente aquellas con experiencia en seguridad de redes, se beneficiarían de productos que integran todas las funciones VPN así como un Firewall y quizás uno o dos servicios de red. Algunos productos, normalmente los más caros, incluyen suministro dual de potencia y características de recuperación para asegurar fiabilidad. Pero se necesita determinar que servicios de red son cruciales para las operaciones de la compañía; después de priorizar estos servicios, se puede tomar la decisión de si debería ser instalado en un único producto.

¿Debería adquirirse hardware VPN en lugar de instalar software y/o hardware adicional en las routers o firewalls? Esto depende. Si se está buscando una solución final de bajo nivel que no tenga que procesar una gran cantidad de tráfico, entonces productos como routers y firewalls pueden hacer la trampa. Si no se tiene un Firewall o si se está planeando añadir capacidades VPN a las oficinas, entonces algunas de las cajas integradas descritas pueden reducir la necesidad de un especialista en seguridad o al menos minimizar alguna de las tareas de gestión de claves.

No se debe pasar por alto la importancia de integrar el control de otras funciones de red, como reserva de fuentes o control de ancho de banda. Algunas compañías ya incluyen estas características en sus productos, y es un paso que ganará mayor soporte en el futuro.

Si se están buscando prestaciones, los productos hardware para VPN normalmente ofrecen un mejor rendimiento que los productos software. Las versiones más básicas de estos productos incluyen paquetes de autenticación, túneles, encriptación y gestión de claves así como los sistemas de autenticación de usuarios. Productos más avanzados ofrecen otros servicios dentro del mismo paquete y soportan miles de túneles simultáneos.

Las soluciones hardware destacan por su facilidad de configuración e instalación, sin embargo, pueden resultar algo inflexibles. Resultan adecuadas para interconectar oficinas remotas, y además existen soluciones híbridas que permiten a clientes software conectarse con servidores hardware.

Capitulo 3. COMO ELEGIR CORRECTAMENTE UNA VPN

3.1 Etapas para la elección de una solución VPN

Actualmente, las VPNs pueden aportar grandes beneficios a las empresas, por la diversidad de servicios que ofrecen y que ayudan a fortalecer los objetivos del negocio, desafortunadamente las organizaciones que han intentado implementar una solución VPN han tenido relativo éxito, esto se debe a que las empresas que han tenido mayor éxito le han dado un enfoque analítico y lógico a la solución y por el contrario las empresas que han fracaso ha sido básicamente porque intentaron implementar la solución sin tener en cuenta un enfoque.

Una estrategia de VPN debe estar basada en función a las necesidades de la empresa, es ese precisamente el primer paso para elegir correctamente la mejor solución.

Usted como ejecutivo de sistemas de su empresa se ve en la obligación de escoger la mejor opción al menor costo, esto implica entonces un análisis conciente de sus necesidades ahora, y sus necesidades futuras.

Algunas de las demandas actuales de las organizaciones que nos conllevan a buscar una solución VPN se muestran en la Figura 19.

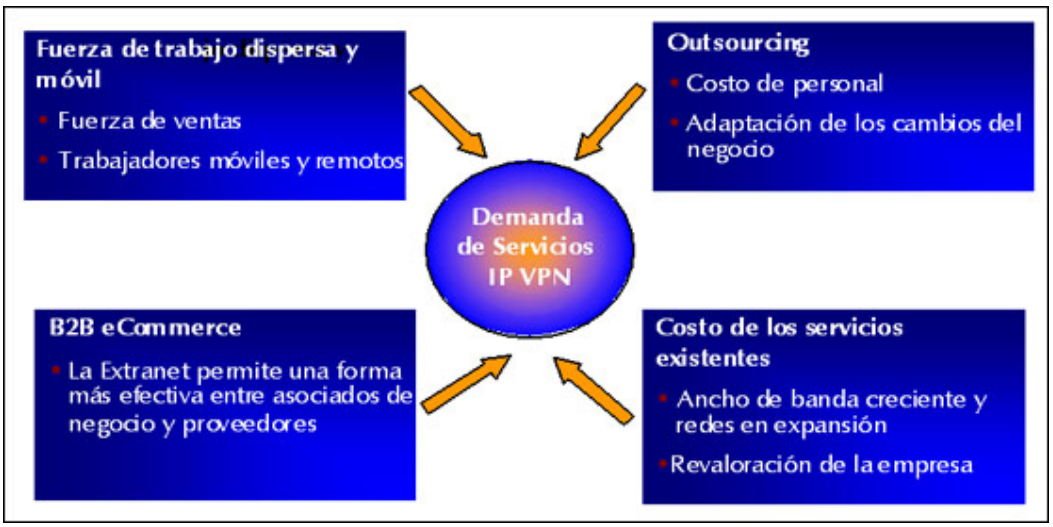


Figura 19.Demanda de servicios VPN

Sin embargo, las empresas que deseen implementar una VPN, deben tener en cuenta tres etapas importantes: planeacion, implementación y administración, en cada una de cuales se presentan aspectos de gran importancia que nos facilitaran la labor en cada una de ellas.

3.1.1 Planeación

Esta es quizás una de las etapas mas importantes, implementar una VPN es similar a implementar una nueva red desde cero, aunque muchas personas no lo admitirían ahora, la mayoría simplemente compraba algunos componentes: cable, núcleos, routers, etc., los conectaban entre si para formar una red

rudimentaria y luego buscaban la forma para que funcionara, se desempeñara mejor y estuviera más protegida.

Las empresas que se atreven a utilizar este método con las VPN tienen más probabilidad de fracasar. Incluso si las hacen funcionar, es probable que la seguridad obtenida sea inferior a la esperada y a la sugerida por el distribuidor que les vendió la solución.

La planeación es la parte clave para implementar una VPN segura. Sin planeación, la VPN no estará óptimamente protegida; es más puede estar desprotegida o no funcionar.

En esta etapa se sugiere tener en cuentas los siguientes aspectos fundamentales: Funcionalidad, Interoperabilidad, Cifrado y administración de claves, Políticas, Desempeño, Seguridad (que incluye tolerancia a las fallas, redundancia y punto único de fallas), Usuarios independientes y Facilidad de uso.

1. Funcionalidad

Cuando la empresa decide utilizar la tecnología VPN, es muy importante que no considere únicamente el requerimiento inmediato, sino también que considere los futuros usos potenciales de las VPN; de lo contrario, la empresa puede verse relegada al utilizar una tecnología que tendrá que desechar en un año o dos.

Existen básicamente 4 escenarios típicos de las VPN:

1. De oficina a oficina.
2. Al interior de la oficina.
3. De usuario por acceso telefónico a la oficina.
4. Proveedor y socio de la oficina.

En los primeros dos casos, las VPN simplemente forman parte de la red existente aunque una parte más segura. El asunto fundamental es donde posicionar los extremos de la VPN, por ejemplo, los gateways que son responsables de cifrar y descifrar los contenidos de los paquetes. Puesto que en muchos casos el diseño y estructura de la red estarán abiertos hasta que se implemente la VPN, no habrá el requerimiento de ocultación de la red. Si lo hay, aplicaría más la solución descrita para los dos últimos escenarios en el listado anterior.

En el caso del usuario por acceso telefónico a la oficina o del socio / proveedor de oficina, se deben considerar los siguientes aspectos importantes:

- La cantidad de VPN individuales que se necesitan así como cuántos usuarios o compañías individualmente necesitarán VPN individuales y no compartidas.
- El tipo de tráfico, abierto o controlado, que se permitirá a través de la VPN.

- Si se requiere ocultación de la red interna o traslado de direcciones.
- La profundidad de la VPN permitida para alcanzar la red empresarial: si se detiene en el perímetro o en la subred interna.
- La forma cómo se administra la autenticación del usuario.
- Las consecuencias de los extremos de la VPN que no están disponibles por tolerancia a las fallas y redundancia.
- La cantidad de información que se espera que fluya por las VPN
- La facilidad o dificultad de utilizar la solución.
- La posición en cuanto a la seguridad por parte de las estaciones de trabajo, socios o proveedores externos.

2. Capacidad

Para definir la capacidad de un gateway para las VPN la empresa debe determinar la cantidad de usuarios simultáneos, bien sea individuos u otras empresas, que ésta requiere para que pueda estar conectada simultáneamente, así como la velocidad de conexión requerida por los usuarios. Estos dos factores, junto con los requerimientos en materia de recursos para la solución de gateways para las VPN, determinan las características de desempeño para la computadora de gateways requerida.

3. Cifrado y administración de claves

Todas las implementaciones VPN usan ciertas claves como parte del proceso de cifrado que protege los datos en tránsito.

- Algunas VPN utilizan la misma clave para crear el túnel de las VPN y luego para cifrar los datos por todo el tiempo de duración del túnel de las VPN.
- Otras implementaciones utilizan una clave compartida fija para la inicialización de las VPN y luego crean una clave de sesión única que se utiliza para cifrar los datos durante todo el tiempo de vida de ese túnel.
- Un mejoramiento en comparación con los métodos anteriores es negociar y cambiar la clave de la sesión a solicitud de alguna de las partes que conforman la VPN o a un intervalo normal. Esta es la base de las implementaciones de intercambio de claves ISAKMP/Oakley y muchas otras.

Cualquiera que sea la solución VPN que se escoja, deben ser factores principales la fortaleza del cifrado utilizado y la metodología soportada de administración de claves.

4. Tolerancia a las fallas y deterioros

Si se requiere la tolerancia a las fallas, deterioro o redundancia, esto además repercute en las características de desempeño del sistema de gateways y potencialmente en la configuración de la infraestructura de comunicaciones requerida para respaldar la solución. Así, lo anterior podría suponer el uso de Proveedores de Acceso a Internet (ISP) duales, canales de línea telefónica terrestre y de comunicaciones microondas, provisión de suministros de energía ininterrumpidos, etc.

4. Autenticación del usuario

Después de considerar estos aspectos, una empresa debe analizar la manera de autenticar a los usuarios o si los usuarios se deben autenticar para utilizar una VPN. Si no se requiere autenticación para iniciar la aplicación de las VPN, cualquier persona podría enviar cualquier información por la VPN, lo que realmente entorpece el objetivo de la mayoría de VPN empresariales, que es utilizarlas para transmitir información confidencial. El gateway receptor de las VPN requiere la segunda parte del mecanismo de autenticación para que sepa que el gateway de iniciación es en efecto el gateway autorizado. Una vez que así se establece, los dos gateways inician el canal cifrado entre ellos.

5. Derechos de acceso al servicio y a las aplicaciones

Otro aspecto que se debe tener en cuenta es a lo qué tiene acceso un usuario determinado, además de las aplicaciones y protocolos que se permiten para llegar a ese destino. Este aspecto es ante todo un asunto de políticas empresariales, aunque tiene mucha relación con la solución VPN que la empresa seleccionará y cómo se implementará.

Implementar una VPN sin un control del contenido bien sea a nivel del protocolo o a nivel de los paquetes internos, proporciona acceso directo mediante un protocolo para el sistema de destino. La única protección que tiene el sistema de destino es su propia configuración de seguridad. En la práctica, es altamente conveniente y ampliamente recomendable agregar un segundo nivel de protección a ese sistema por medio del filtrado de las VPN.

6. Ocultación de la red

Algunas implementaciones VPN suministran funciones de traslado de direcciones de la red que efectivamente oculta la red interna empresarial para que no sea visible al otro lado del gateway. Aunque proporcionan un grado de seguridad al eliminar la visualización de la red, también pueden en algunos casos ocasionar problemas complejos de enrutamiento que se deben resolver.

7. Facilidad de uso

Por lo general el comportamiento del usuario es inestable. Por lo tanto, si una empresa ofrece una solución que es difícil de utilizar e implementar, tanto los usuarios como los administradores tendrán la tendencia a buscar una alternativa para realizar el trabajo, incluso si esto implica reducir la seguridad total de la empresa. Es primordial encontrar una solución que sea fácil de utilizar para que obtenga rápida aceptación y uso a largo plazo.

8. Usuarios externos

Cuando una empresa vincula a personas externas a su infraestructura de informática, está creando una relación de confianza implícita entre las dos empresas. La empresa asume lo siguiente

- Un usuario externo está protegido o más protegido que la empresa.
- Un usuario externo no compromete la seguridad empresarial.
- Nadie al interior de su propia empresa comprometerá la seguridad de un usuario externo.
- Muchos usuarios externos intentarán no involucrarse en una situación comprometedora a través de la infraestructura comúnmente utilizada.

Estos son aspectos importantes que necesitan ser revisados desde un punto de vista técnico y comercial para que todas las partes involucradas estén protegidas de conductas inescrupulosas o poco éticas.

9. Administración de claves e interoperabilidad

La administración de claves asociada a la implementación de las VPN no es un asunto trivial. Si los túneles de las VPN están bajo el control total de la empresa que las implementa, desaparecen muchos problemas. Sin embargo, si diferentes empresas de diferentes sistemas de administración intentan conectarse por medio de una VPN, los problemas pueden ser graves.

Aparte de escoger la tecnología VPN y las claves utilizadas por esa tecnología, los problemas con la administración de claves y de interoperabilidad pueden volverse un asunto de cooperación. Una VPN solo puede ser creada por las dos partes que se comprometen a lo siguiente:

- Utilizar un enfoque común
- Intercambiar métodos comunes para la administración de las claves relacionadas con las VPN.

Sin este grado de cooperación, es poco probable que la VPN entre las partes funcione. Un aspecto que no se refiere estrictamente a la administración de claves, pero que está relacionado es la fortaleza del cifrado. Debido a la legislación de diferentes países, la fortaleza del cifrado de un país puede no estar disponible para ser utilizado en el país del socio. Esto conduce inevitablemente a una reducción en la fortaleza del cifrado si ambas partes desean comunicarse por la VPN.

10. Configuración

Es de vital importancia recordar que las VPN ofrecen conexiones entre dos localidades y que ambos puntos del enlace se deben configurar para que funcionen conjuntamente. Para las empresas que quieren utilizar pocas VPN resulta inconveniente el trabajo adicional que implica la coordinación de los dos puntos de cada VPN. Si se espera que una empresa implemente una gran cantidad de VPN, se requiere un gran esfuerzo adicional y se debe prestar atención durante el proceso de selección de la solución VPN a los recursos suministrados en la solución por parte del distribuidor con el fin de reducir el esfuerzo de configuración cuando se implementan muchas VPN.

Independientemente del tamaño de la implementación propuesta de VPN, es importante incluir recursos suficientes para la implementación en la etapa de planeación.

3.1.2 Implementación

En esta segunda etapa se le recomienda tener en cuenta los siguientes aspectos: Mano de obra, Automatización, Tolerancia a las fallas, Redundancia, Administración de claves, Administración de usuarios iniciales

1. Mano de obra

Si una organización ha terminado con éxito el ciclo de planeación, la implementación de las VPN debe ser relativamente un asunto sin incidentes excepto por las usuales dificultades asociadas a la implementación de otro tipo de red. Quizás el aspecto más intrigante de implementar una VPN es que por lo general es muy difícil determinar lo que no está funcionando puesto que todo el tráfico que fluye por la ruta VPN está cifrado.

Se pueden presentar dos situaciones:

- Si la información no llega a su destino, no sería obvio saber a donde fue.
- Si el gateway en el extremo de las VPN no está configurado adecuadamente, la información puede llegar al gateway y luego parecer que está perdida.

Estas dos situaciones pueden parecer obvias, aunque en la ardua y compleja instalación de las VPN, algunas veces lo obvio está muy bien escondido.

Algunos distribuidores de las VPN proporcionan herramientas para ayudar a depurar estos problemas, mientras que otros no. En cualquiera de los casos es quizá prudente que la organización invierta en una clase de tecnología de husmeo (sniffing) de paquetes que ayuden en la depuración de un problema en las VPN. Dotado de un husmeador (sniffer) de paquetes y conocimiento sobre la estructura de paquetes VPN (suministrado por el distribuidor de la tecnología

VPN), depurar un problema en una VPN se vuelve una tarea ardua antes que una dificultad. El técnico de reparaciones de las VPN no será capaz de leer los contenidos del paquete y solo podrá identificar las direcciones fuente y destino de los paquetes.

Los distribuidores de las VPN no discuten el asunto de la mano de obra para la implementación de las VPN puesto que le resta importancia a la presentación de ventas, mostrarle a la organización por ejemplo cómo puede realizar negocios en un ambiente electrónico de manera segura por medio de una red pública como la Internet. Sin embargo, en el mundo real, donde la mano de obra calificada es escasa y es por lo general costosa, no es un asunto que se puede dejar pasar a la ligera. Las destrezas requeridas para implementar la tecnología VPN son básicamente las siguientes:

- Una red excelente y excelentes destrezas de depuración de redes (incluyendo el nivel de paquetes)
- Una mente muy analítica para resolver algunos de los problemas aparentemente abstractos que pueden surgir de las instalaciones de las VPN.

2. Automatización

El suministro de configuraciones automatizadas para la implementación de VPN no es un aspecto importante para las soluciones actuales debido a la complejidad y variedad de formas cómo se pueden configurar las VPN. Sin embargo, una vez que se selecciona la solución, se debe implementar un programa piloto para la solución en un entorno de laboratorio de pruebas y el proceso utilizado para configurar ese entorno debe ser documentado en detalle por el equipo de implementación.

3. Implementación de redundancia y tolerancia a las fallas

Un aspecto importante que con frecuencia se ignora hasta que surge el problema es el de la tolerancia a las fallas y la redundancia. En muchas implementaciones de VPN, toda la infraestructura de las VPN de una organización se centra en un solo sitio y por lo general dentro de un solo gateway que casi siempre es un Firewall. Esto significa inevitablemente que si este dispositivo sufre un imperfecto o avería que incapacite al dispositivo temporal o permanentemente, toda la herramienta VPN repentinamente no estará disponible.

Por lo tanto, la organización se enfrenta a la decisión de realizar negocios. Debe decidir si se arriesga a permitir la transmisión de información de texto en

lenguaje claro o si espera. En cualquiera de los casos, debe hacer una evaluación financiera para tomar la decisión más acertada.

4. Administración de claves

La Implementación de la administración de claves seguras es vital para que la implementación de las VPN sea segura. Si las claves se revelan inadvertidamente ante usuarios no autorizados, se pone en duda la seguridad de la implementación. A la luz de esta situación es importante tener mucho cuidado con este aspecto de la implementación de las VPN.

5. Administración inicial de usuarios

Cuando una organización configura una gran cantidad de usuarios para que use las herramientas VPN, es muy tentador expedir una contraseña estándar de inicio puesto que simplifica todo el proceso. Desde el punto de vista de la seguridad, no se trata de un ejercicio profesional adecuado y se debe evitar en lo posible. Si la implementación de las VPN soporta el uso de expiración de contraseñas, se debe utilizar esta herramienta para obligar a los usuarios a que cambien su contraseña de inicio de la aplicación VPN suministrada por el equipo de implementación tan pronto como llamen la aplicación.

Mientras que muchos usuarios pueden requerir acceso a los recursos corporativos a través de los túneles de las VPN, otros no utilizarán la herramienta. Por lo tanto, como medida preventiva la organización debe revisar periódicamente el uso del túnel y cancelar los túneles que no se han utilizado durante un largo periodo de tiempo. Por supuesto que se necesitará el respaldo de las políticas de seguridad de las organizaciones.

La capacitación de usuarios es un aspecto que no se debe pasar por alto aunque con frecuencia sucede. Las organizaciones no deben esperar que los usuarios, bien se trate de individuos, grupos, socios o estaciones de trabajo, deben ser capaces de utilizar instintivamente una nueva tecnología. Estos usuarios deben ser entrenados tanto en el manejo de la tecnología como en las responsabilidades que conlleva el uso de esa tecnología.

3.1.3 Administración

En esta es la ultima etapa, es importante fijar nuestra atención en aspectos como: Administración de usuarios a largo plazo, Modificación de la solución y diseño de una VPN, y enfatizarnos en la seguridad de las misma evitando Ataques de piratas a través del túnel de las VPN.

1. Administración de usuarios a largo plazo

Es posible que el aspecto más difícil de administrar usuarios de las VPN a largo plazo sea la indiferencia que sienten hacia el uso de las herramientas que se les han proporcionado. Los usuarios comienzan a suponer que la herramienta no es legítima e incluso empezarán a abusar de ella. Esta actitud puede ser eliminada a través de programas periódicos de concientización sobre la seguridad de la información que enfaticen las responsabilidades que tienen los usuarios para administrar la seguridad de la información a la que tienen acceso. Por supuesto que este enfoque debe estar respaldado por las políticas de seguridad de la información de las empresas.

En una empresa cambiarán los usuarios, sean individuos, grupos, socios o estaciones de trabajo. Cuando suceden estos cambios, es importante que el equipo a cargo de la administración de la solución VPN esté informado sobre estos cambios para que se puedan eliminar los túneles obsoletos que ya no se requieren y las identidades de usuario asociadas a ellos. La eliminación de las credenciales y cuentas de usuario obsoletas es una función que algunas veces se realiza inadecuadamente en las organizaciones. Sin embargo, en el caso de las implementaciones de las VPN, si no se logra realizar esta función, los intrusos afectarán gravemente el entorno computacional de la organización generando pérdidas.

2. Modificación del diseño y función de la solución VPN

Cuando se implementa una solución VPN en la organización, los cambios que se producen, diferente a agregar o eliminar usuarios o túneles, implicarán una significativa cantidad de trabajo. El enfoque más seguro sería comenzar todo el proceso de nuevo, no toda la implementación, puesto que la mayoría de empresas tendrán que continuar realizando sus operaciones existentes durante los cambios. De esta forma, se pueden identificar problemas potenciales en la etapa de Planeación y podrán resolverse antes de que efectúen cambios en el entorno operativo existente que se está implementando.

3. Ataques de piratas a través del túnel de las VPN

Simplemente por el hecho que una organización implemente una VPN no significa necesariamente que esté protegida contra todos los ataques de piratas. Que un pirata ataque una VPN establecida no es por si mismo un hecho trivial, aunque si el pirata informático es capaz de atacar una VPN durante o antes de que se inicialice, la empresa que está al otro extremo de la VPN creerá que el usuario está autorizado. Por esta razón es imperativo controlar la información que está autorizada para ingresar o salir de la empresa a través de los enlaces de las VPN.

También es vital que una empresa que utiliza las VPN, implemente una solución sofisticada de detección de intrusos para controlar a los intrusos no autorizados y tomar las medidas adecuadas.

.

3.2 Ventajas y Desventajas de las redes privadas virtuales- Virtual private network (VPN)

Algunas de las ventajas que ofrecen las VPN frente a otras tecnologías son:

Escalabilidad

Las VPNs son arquitecturas de red más escalables y flexibles que las WAN tradicionales, debido a que permiten a las corporaciones agregar o eliminar sus sistemas localizados remotamente, “teletrabajadores” o aliados comerciales de forma fácil y poco costosa en función de las necesidades del negocio.

Seguridad

Bajo el esquema de VPN la conexión a través de Internet es cifrada. El servidor de acceso remoto exige el uso de protocolos de autenticación y cifrado. Los datos confidenciales quedan ocultos a los usuarios de Internet, pero los usuarios autorizados pueden tener acceso a ellos a través de la VPN.

Diseño de red simplificado

Un diseño de red con tecnología VPN se simplifica en términos de diseño de arquitectura, flexibilidad y mantenimiento, debido a que se reducen los costos asociados a la gestión de red.

Compatibilidad

Como se aceptan la mayor parte de los protocolos de red más comunes (incluidos TCP/IP, IPX y NetBEUI), las VPNs puede ejecutar de forma remota cualquier aplicación que dependa de estos protocolos de red específicos.

Administración centralizada

Algunos proveedores soportan la característica de administración centralizada de sus productos VPN. Esto representa una fuerte característica de seguridad y un buen mecanismo para la resolución de problemas.

Prioridad de Tráfico

Algunos proveedores ofrecen la funcionalidad de priorizar tráfico en sus productos VPN. Esto agrega gran flexibilidad a la corporación en cuanto a la utilización de los enlaces de Internet, debido a que se puede decidir en qué orden se preserva el ancho de banda según el tipo de tráfico permitido y de acuerdo a su importancia.

Algunas de las desventajas que ofrece la tecnología VPN son:

- 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 ralentización 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 una línea dedicada.

- Se pueden producir ataques por denegación de servicio.

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

Se recomienda usar el servicio de VPN en aquellos casos en que, teniendo una conexión a un proveedor de acceso a Internet ajeno a la organización, se quiera disponer de un servicio sólo autorizado a los ordenadores de la

organización o una salida a Internet que sea más conveniente usando las líneas de salida de la organización.

3.3. RECOMENDACIONES

Una Red Privada virtual o VPN, es la contribución de un conjunto complementario de elementos tecnológicos integrados que aprovecha Internet para crear una solución de comunicación empresarial eficiente, permitiendo la integración de empleados, clientes y proveedores.

Hoy en día existen múltiples soluciones como se menciono anteriormente y en esta parte pretendemos recalcar las recomendaciones más importantes a la hora de elegir la solución correcta:

1. Verifique sus necesidades

Es importante centrarse mucho en la etapa de planeación de nuestra solución VPN, para ello debemos tratar de ubicar nuestra empresa en varios aspectos que son de relevancia a la hora de tomar una decisión, es por esto que usted como ejecutivo de sistemas deberá elaborar una lista teniendo en cuenta los siguientes criterios[5]:

[5] LEON Clark, David. Guía para el administrador de redes privadas virtuales.

- Implementación General: muchas de las soluciones del mercado incorporan tres estrategias para implementar una VPN: Lan a Lan, cliente a Lan o Cliente a Cliente, (o alguna combinación de las tres). Muchos proveedores de soluciones de VPN no soportan la implementación Cliente a cliente, por esto es importante que reconozca sus necesidades y se situé en las que quiera suplir.

  Si su desafío se relaciona con la conexión de una serie de redes geográficamente dispersas, y cada red soporta varios usuarios, una conexión de Lan a Lan seria su solución ideal, también seria una estrategia apropiada si sus usuarios remotos no se comunican a través de líneas telefónicas por el contrario si el objeto de su negocio le exige una comunicación de del personal remoto o móvil con su Lan y además estos se encuentran en una sucursal remota y en algunas ocasiones requieran conectarse inclusive con otros usuarios remotos la solución acertada es una red cliente a cliente o la integración de ambas, es así como usted entraría a considerar otros aspectos relevantes ya que este tipo de implementación a diferencia de la Lan a Lan no es transparente al usuario ya que este deberá aprender a manejar el software VPN instalado en su maquina portátil, es así como se requiere una curva de aprendizaje para sus usuarios y la duración de esta dependerá de la cultura empresarial y de su experiencia en general en el trabajo con tales sistemas.

Otro punto a considerar es la capacidad del usuario de activar o desactivar funciones de VPN como encripción y validación de datos, usted como administrador debe preocuparse porque sus usuraos no dejen huecos de seguridad al deshabilitar ciertas funciones ya que esto podría acarrearle consecuencia fatales a sus sistemas de información, es por esto que usted deberá elegir aquellos sistemas que no permitan a los clientes activar o desactivar la seguridad de VPN o establecer políticas de seguridad claras en aquellos que si las ofrecen y capacitar a los usuarios sobre este aspecto.

- Requisitos de seguridad: Es importante establecer políticas de seguridad claras y establecer niveles de seguridad que sean los suficientemente flexibles para asegurar varios servicios y recursos de la red a nivel de aplicación ante Ipsec y servidores de seguridad esto debería ser una prioridad, sin embargo si tiene una red basada en Ip, la integración de componentes y estándares de VPN y la tecnología adecuada harán que mantener la seguridad sea una tarea mucho mas sencilla.

- Autenticación de usuario deseada: Existen varias formas de autenticación de usuraos VPN, entre las cuales se citan la autenticación débil a través de contraseñas y la autenticación sólida entre esta ultima se incluyen los sistemas de contraseña de una sola vez y los sistemas

de autenticación de tres niveles como RADIUS, los certificados digitales también hacen parte de este proceso.

No existen unas reglas establecidas en cuanto a la autenticación de usuarios, sin embargo usted como administrador de la red esta en la obligación de verificar con certeza la autenticidad de los mismos, si su principal fuerza de trabajo son los usuarios móviles un sistema de dos factores como el de ficha seria la solución correcta, este escenario nos permite establecer una autenticación sólida para cada persona, por otra parte un sistema como RADIUS funciona junto con puertas de enlace de seguridad VPN para validar usuarios y esta solución es recomienda altamente cuando se manejan una gran base de usuarios ya que estos sistemas facilitan la administración del proceso de autenticación de cada uno para los sistemas de VPN.

- Consideraciones de cliente/ servidor: En general, los productos y servicios de VPN son compatibles con plataformas de uso común como Unix, Windows NT y Linux, por esta razone este tema no debe ser de gran preocupación para los usuarios de estos sistemas sin embargo es importante que se asegure de que la versión de la solución VPN y la versión o el nivel de la plataforma de operación de selección para su organización sean compatibles, a veces existe mas de una versión para

una solución VPN determinada en una plataforma de sistema determinado.

2. Verifique Su Presupuesto:

Aunque la gran popularidad de las VPN se basa en su bajo costo es importante que a la hora de tomar una decisión revise su presupuesto, ¿Cuanto esta dispuesto a invertir en determinada solución? y con cuales equipos cuenta actualmente en su red, ¿Que tipo de topología posee? y cual seria la solución mas factible teniendo en cuenta las características de su red privada, todo esto con el objeto de crear la solución mas acertada a mas bajo costo.

3. Busque Accesoria

Informarse bien puede ser la clave para elegir la mejor solución, por tanto le recomendamos investigar, leer o asesorarse con personal experto en el área, se dará cuenta que muchas veces es mas fácil cuando se conocen los pro y los contra de la situación y cuando se cuenta del personal con la experiencia y la capacidad para ayudarlo a elegir.

CONCLUSIONES

Mediante las investigaciones del estado del arte de la tecnología de Redes privadas Virtuales- Virtual Private Network VPN podemos concluir lo siguiente:

Actualmente la integración de los servicios en las empresas hacen evidente una búsqueda de nuevas formas para mantener una comunicación constante entre cada uno de los miembros de su organización, proveedores y clientes, estas necesidades de comunicación son suplidas satisfactoriamente por la implementación de la tecnología VPN, esta, nos permite hacer una extensión de nuestra red privada corporativa de manera segura mediante el uso de técnicas criptográficas a mas bajo costo ya que utiliza un medio publico (Internet) como estructura física.

Las VPN utilizan múltiples protocolos que nos permiten crear un túnel virtual en la Internet por el cual transitaran seguros nuestros datos, estos protocolos tales como PPPTP, L2TP e Ipsec nos ofrecen todas las condiciones de seguridad necesarias para mantener nuestro datos de manera confidencial.

Además en el mercado existe gran variedad de soluciones que son ofrecidas para que las empresas escojan las que mas adecuada para sus necesidades, entre las más comunes de implementación de VPN están: VPN de Intranet,

VPN de acceso remoto y VPN de extranet, para implementar estas soluciones existen diversas arquitecturas que nos facilitan esta labor estas son

- VPN proporcionadas por un PSI (proveedor de servicios de Internet)
- VPN basadas en Firewall
- VPN basadas en software
- VPN basadas en Hardware

Cada una con ventajas y desventajas que se resumen en el siguiente cuadro.

Arquitectura VPN	Ventajas	Desventajas
PSI	Menor gasto en infraestructura; fácil de instalar, costo relativo.	Perdida de control de administración de la VPN
Firewall	Soporta amplia variedad de plataformas, nos permite utilizar el hardware existente en nuestra compañía, soporta balance de cargas y Firewall redundantes; utiliza Ipsec lo que sugiere bajo costo.	Posibles problemas de seguridad debido al sistema operativo; no todos son completamente interoperables con soporte para RADIUS; algunos tiene problemas de licencias,
Software	Amplia variedad de plataformas; facilidad de instalación; es las solución mas recomendable para una amplia gama de compañías.	Problemas de desempeño con el soporte NAT; algunos tienen tecnologías de cifrado viejas; propietario; algunas carecen de capacidad de administración remota sin capacidades de supervisión.

Hardware	Buen desempeño; buena seguridad ampliable; carga de cifrado mínima para paquetes grandes; un poco de soporte para balanceo de cargas.	Flexibilidad limitada; precio alto; sin internas ATM, Token Ring y FDDI la mayoría son semiduplex; se necesita reiniciar para que los cambios tengan efecto; algunos tienen problemas de desempeño importante con paquetes pequeños(64 bytes); funcionalidad de subred limitada.

Para finalizar podemos decir que la elección de una solución correcta de VPN esta ligada a tres etapas importante: planeación, implementación y administración que depende del ejecutivo de sistemas identificar cual es su mejor alternativa después de analizar sus necesidades, verificar su presupuesto y buscar accesoria, este puede ser un trabajo arduo o sencillo, todo depende de usted.

GLOSARIO

Autenticación: Es una verificación de determinado usuario o proceso para tener acceso a cierto sistema, o realizar una operación en específico. La autenticación por lo general se realiza por medio de una función criptográfica. La tecnología de autenticación garantiza:

1. La identidad de los participantes de la VPN (los gateways y clientes son quienes dicen ser)
2. La integridad de la información recibida (no ha sido alterada en el camino)

ATM: Es una tecnología orientada a conexión, en contraste con los protocolos de base LAN, que son sin conexión. Orientado a conexión significa que una conexión necesita ser establecida entre dos puntos con un protocolo de señalización antes de cualquier transferencia de datos. Una vez que la conexión está establecida, las celdas ATM se auto-enrutan porque cada celda contiene campos que identifican la conexión de la celda a la cual pertenecen.

Centro de Información de redes de Internet (InterNIC): Compañías privadas, con el permiso de la Fundación Nacional de Ciencias (NSF), que asignan nombres de dominio de segundo nivel.

Encabezado de autenticación (AH): Una de las normas IPSec que considera la integridad de los paquetes de datos.

Privada: La privacidad es típicamente considerada como el hecho de ocultar información. Indica la seguridad y garantía que debe tener la información que se envía por la red y la disponibilidad de esta para los usuarios autorizados.

Protocolo Internet (IP): El protocolo de Internet es la norma de protocolos para enviar datos.

Traducción de direcciones de red (NAT): Proceso de convertir una dirección IP en otra dirección IP; las NAT disponibles son uno a uno, varios a varios y varios a uno.

Sistemas de nombre de dominio (DNS): Protocolo de normas de Internet para relacionar nombres y direcciones IP.

Proveedor de servicios de Internet (PSI): Compañía comercial que proporciona acceso a Internet.

Punto de acceso a red (NAP): Uno de los principales puntos de la columna vertebral de Internet donde los PSI transfieren datos entre si.

Protocolo simple de administración de redes (SNMP): Protocolo utilizado para administrar dispositivos de red desde una estación central de monitoreo.

Compresión: Proceso de hacer un paquete más pequeño que su tamaño original. La compresión de datos es útil en la norma IPSec, donde sin el modo de túnel, el tamaño del paquete aumenta por los protocolos de cifrado y autenticación.

Firewall: Una máquina que conecta el perímetro de la red confiable de una compañía a una red no confiable. Proporciona protección contra ataques al utilizar filtración en puertos, traducción de direcciones y tecnologías para inspección.

Protocolo de autenticación de reconocimiento de pruebas (CHAP): Utiliza una función de transformación de código de un solo sentido para proporcionar la autenticación de los usuarios; algunas implementaciones PPTP utilizan CHAP.

Protocolo punto a punto (PPP): Protocolo que permite establecer el protocolo TCP/IP en líneas telefónicas de marcación serial y en líneas dedicadas como ISDN.

Propietario: Término utilizado para describir cualquier diseño informático cuyas especificaciones técnicas no son publicadas y por tanto no son fáciles de obtener. Estas especificaciones de propiedad dificultan o imposibilitan a

terceros fabricar dispositivos auxiliares que funcionen correctamente con una máquina de arquitectura cerrada. Por lo general, sólo el fabricante original podrá construir periféricos y productos complementarios para este tipo de máquinas.

BIBLIOGRAFIA

Libros de Referencia

BROWN, Steven. Implementación de Redes Privadas virtuales. México D.F. Editorial Mc Graw Hill, 2000.

LEON, Clark David. Guía para el administrador de redes privadas virtuales. Mexico D.F. Editorial Mc Graw HILL, 2000

KOLESNIKOV OLEGHATCH. Brian Redes Privadas Virtuales con LINUX. México D.F. Editorial Alahmbra - Longman, 2003.

LEON-GARCIA, Alberto y Widjaja, Indra. Redes de Comunicación: Conceptos Fundamentales y Arquitecturas Básicas, Madrid España, Editorial MC Graw Hill, 1999.

Paginas Web

>http://www.uv.es/ciuv/cas/vpn/ Una interesante pagina sobre redes privadas virtuales, muestra ejemplos de implementación.

>http://www.kriptopolis.com/index.php?id=P178 Página sobre criptografía y seguridad.

>http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml

> http://www.cyclades.com.pe/Soporte/PRx000/Bulletin111.htm

>Seguridad en Redes. Redes Privadas Virtuales.

http://www.rediris.es/rediris/boletin/54-55/ponencia2.html>

>http://www.viptel.com/redes.html

>http://www.lafacu.com/apuntes/informatica/Redes_Virtuales_Privadas/

default.htm>

RECOMENDACIONES

Para facilitar el uso adecuado de este trabajo de investigación le sugerimos tener en cuenta el siguiente perfil:

- Sino posee ningún conocimiento empiece desde el capitulo 1.
- Si desee ampliar sus conocimientos y ahondar en la tecnología vaya al capitulo 2.
- Si usted tiene conocimiento acerca de la tecnología VPN y desea conocer como elegir correctamente una solución dirijase al capitulo 3.

Para mejorar este trabajo de investigación sugerimos:

- Brindar soporte en línea Incluyendo un servicio de FAQ o Chat en la página Web de tal manera que los usuarios que ingresen puedan colocar sus inquietudes o esperar recibir sugerencias personalizadas de acuerdo a la implementación de su VPN.
- Incluir ejemplos o estudios de caso de empresas que poseen actualmente la implementación de esta tecnología.

CONTENIDO DEL CD ROM

Adicional a este trabajo se encuentra un CD que contiene los siguientes archivos:

Tipo	Nombre	Contiene
Documento	Monografía VPN.doc	Documento final de la Monografía VPN 106 paginas
Carpeta	Capitulo 1	Capitulo1.doc
Carpeta	Capitulo 2	Capitulo2.doc
Carpeta	Capitulo 3	Capitulo3.doc
Carpeta	Apoyos	Graficas y páginas de consulta.
Carpeta	Pagina final	Pagina Web