INDICE

INTRODUCCIÓN

Sin duda alguna, una red es una colección de estándares, basada en dispositivos que encadenan todo lo referente a la compañía, como computadoras de escritorio, anfitriones y recursos, sin sacrificar velocidad, costo o maniobrabilidad. La tecnología en nuestros días avanza muy rápidamente y con ello la inseguridad en las redes, por ello surge la tecnología en software y hardware que nos proporcionan ayuda en cuanto a velocidad y seguridad de la información.

Surge entonces el término Red Privada Virtual (VPN, del inglés *Virtual Private Network*) y ya forma parte del glosario común a la industria de las telecomunicaciones y redes de servicios, aunque su significado puede variar según cómo se lo utilice. Una definición simple es que se trata de una red de comunicaciones privada implementada sobre una infraestructura pública. En base a esta definición, se puede decir que las redes públicas de X.25, ATM o Frame Relay son VPNs. Esto es cierto y este tipo de VPN es denominada de Nivel 2.

Sin embargo, la tecnología emergente de redes privadas virtuales se basa en los protocolos de Nivel 3 (Nivel de Red del modelo OSI), más específicamente en IP. Esta tecnología busca implementar redes de servicios privadas particionando redes públicas o compartidas de IP, donde la red pública IP más conocida y difundida mundialmente es Internet.

1. REDES PRIVADAS VIRTUALES

En una red privada virtual todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia.

Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas: primero, deben ser capaces de pasar paquetes IP a través de un *túnel* en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública; la solución debe agregar *encriptación*, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado; y por último, la solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación, de modo que un adversario no pueda acceder a los recursos del sistema.

Una definición simple es que se trata de una red de comunicaciones privada implementada sobre una infraestructura pública.

Las razones que impulsan al mercado en ese sentido son, fundamentalmente, de costos: es mucho más barato interconectar filiales utilizando una infraestructura pública que despliega una red físicamente privada. Por otro lado, como es lógico, es necesario exigir ciertos criterios de privacidad y seguridad, por lo que normalmente debemos recurrir al uso de la criptografía.

Una red privada virtual conecta los componentes de una red sobre otra red. Las VPN logran esto al permitir que el usuario haga un túnel a través de Internet u otra red pública, de manera que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas

Las VPN permiten a los usuarios que trabajan en el hogar o en el camino conectarse en una forma segura a un servidor corporativo remoto, mediante la infraestructura de entubamiento que proporciona una red pública(como Internet).

Desde la perspectiva del usuario la VPN es una conexión de punto a punto entre la computadora del usuario y un servidor corporativo. Por su parte, la naturaleza de la red intermedia es irrelevante para el usuario, debido a que aparece enviando como si los datos se estuvieran enviando sobre un enlace privado dedicado.

La tecnología VPN también permite que una compañía se conecte a las sucursales o a otras compañías (extranets) sobre una red pública (como Internet), manteniendo al mismo tiempo comunicaciones seguras.

La tecnología de la VPN está diseñada para tratar temas relacionados con la tendencia actual de negocios hacia mayores telecomunicaciones, operaciones globales ampliamente distribuidas y operaciones con una alta interdependencia de socios, donde los trabajadores deben conectarse a recursos centrales y entre sí.

Para proporcionar a los empleados la capacidad de conectarse a recursos de computo corporativos sin

importar su ubicación, una compañía debe instalar una solución de acceso remoto que sea confiable y escalaba. Por lo común, las compañías eligen una solución basada en un departamento de sistemas que está encargado de adquirir, instalar y mantener los conjuntos de módems corporativos y la infraestructura de red privada; también eligen una solución de Red de valor agregado (VAN), donde contratan a una compañía externa para adquirir, instalar y mantener los conjuntos de módems y una infraestructura de telecomunicaciones.

Sin embargo, ninguna de estas soluciones proporciona la escalabilidad necesaria en términos de costo, la flexibilidad de la administración y gestión, así como la demanda de conexiones. Por tanto, tiene sentido encontrar un terreno intermedio donde la organización complemente sus inversiones actuales en conjuntos de módems y su infraestructura de red privada, con una solución menos costosa basada en tecnología de Internet. De esta manera, las empresas se pueden enfocar a su negocio principal con la garantía de que nunca se comprometerá su accesibilidad y que se instalen las soluciones más económicas.

La disponibilidad de una solución de Internet permite pocas conexiones a Internet (a través de Proveedores independientes de servicio, PSI) y la implementación de varias computadoras de servidor VPN en el borde de la red, a fin de dar servicio a las necesidades remotas de red de cientos o miles de clientes y sucursales remotas.

1.1 Conexión de las redes sobre Internet

Existen dos métodos para utilizar VPN a fin de conectar redes de área local a sitios remotos:

Uso de líneas dedicadas para conectar una sucursal a una LAN corporativa. En lugar de utilizar un circuito dedicado de arrastre extenso entre la sucursal y el hub corporativo, tanto los ruteadores del hub de la sucursal corno el corporativo pueden emplear un circuito dedicado local e ISP local para conectarse a Internet. El software VPN utiliza las conexiones ISP locales y el Internet público, con el propósito de crear una red privada virtual entre el ruteador de la sucursal y el del hub corporativo.

Uso de una línea de marcación para conectar una sucursal a una LAN corporativa. A cambio de que el ruteador en la sucursal realice una llamada de larga distancia (0 1800) a un NAS corporativo o externo, el ruteador en la sucursal puede llamar al ISP local. El software VPN utiliza la conexión al ISP local para crear una red privada virtual entre el ruteador de la sucursal y el del hub corporativo, a través de Internet.

Note que en ambos casos las facilidades que conectan la sucursal y la oficina corporativa a Internet son locales; se recomienda que el ruteador del hub corporativo que actúa como un servidor VPN se conecte a un ISP local con una línea dedicada. Este servidor VPN puede estar listo 24 horas al día para tráfico VPN entrante.

1.2. Conexión de computadoras sobre una intranet

En algunas redes corporativas los datos departamentales son tan sensibles, que la LAN está físicamente desconectada del resto de la intranet corporativa. Aunque esto protege la información confidencial del departamento, crea problemas de acceso a la información para otros usuarios que no están conectados en forma física a la LAN separada.

Las VPN permiten que la LAN del departamento esté físicamente conectada a la intranet corporativa, pero separada por un servidor. Nótese que el servidor VPN no está actuando como un ruteador entre la intranet corporativa y la LAN del departamento.

Un ruteador interconectaría los dos redes, lo que permitiría que todos tuviera acceso a la LAN sensible. Pero al utilizar una VPN el administrador de sólo los la red puede asegurar que solo los usuarios en la intranet

corporativa, que tienen el nivel adecuado (basado en una política de lo que necesiten saber dentro de la compañía), pueden establecer una VPN con el servidor VPN y tener acceso a los recursos protegidos del departamento. Además, todas las comunicaciones a través de la red efectos VPN pueden encriptarse hay que de confidencialidad de datos. tornar en cuenta que los usuarios que no tienen el nivel adecuado no podrán ver la LAN del departamento.

1.3. ¿POR QUÉ USAR UNA VPN?

Las redes privadas virtuales surgen como una alternativa a los servicios de comunicaciones tradicionales de red amplia (WAN) de enlaces dedicados.

Este tipo de comunicaciones presentan múltiples ventajas y beneficios para los usuarios:

Bajo costo. Reduce el costo del servicio de comunicación o del ancho de banda de transporte, y también el de la infraestructura y operación de las comunicaciones.

Flexibilidad. Se puede optar por múltiples tecnologías o proveedores de servicio. Esa independencia posibilita que la red se adapte a los requerimientos de los negocios, y se puede elegir el medio de acceso más adecuado. Por ejemplo, si se trata de una pequeña oficina remota, se puede utilizar acceso discado, ISDN, xDSL o cable módem.

Implementación rápida. El tiempo de implementación de un "backbone" de WAN para una empresa es muy alto frente a la implementación de una red privada virtual sobre un "backbone" ya existente de un proveedor de servicio. Más aún, la flexibilidad de esta arquitectura permite implementar nuevos servicios de manera muy rápida, que concuerdan con los tiempos del negocio de la empresa.

Escalabilidad. El desarrollo masivo de redes como Internet permite que la empresa tenga puntos de presencia en todo tipo de lugares. Por otro lado, la independencia con respecto a la tecnología de acceso posibilita escalar el ancho de banda de la red de acuerdo con el requerimiento del usuario. Además, la escalabilidad de la red no incide en la operatoria y gestión de ésta, dado que la infraestructura de la WAN es responsabilidad del proveedor del servicio.

1.3.1. REQUERIMIENTOS BASICOS DE LAS VPN

Por lo general, al implementar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la misma. La solución deberá permitir la libertad para que los clientes roaming o remotos autorizados se conecten con facilidad a los recursos corporativos de la red de área local (LAN) así como las oficinas remotas se conecten entre si para compartir recursos e información (conexiones de N). Por último, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet público. Lo mismo se aplica en el caso de datos sensibles que viajan a través de una red corporativa. Por lo tanto, como mínimo, una solución de VPN debe proporcionar lo siguiente:

Autenticación de usuario. La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados. Además, deberá proporcionar registros de auditoría y contables para mostrar quién accedió a qué información y cuándo.

Administración de dirección. La solución deberá asignar una dirección al cliente en la red privada, y asegurarse de que las direcciones privadas se mantengan así.

Encriptación de datos. Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

Administración de llaves. La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

Soporte de protocolo múltiple. La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen Protocolo de Internet. Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto (PPTP) o un Protocolo de túnel de nivel 2 (L2TP) cumple con todos estos requerimientos básicos, y aprovecha la amplia disponibilidad de Internet a nivel mundial.

2. TIPOS DE REDES VIRTUALES PRIVADAS

Las redes privadas virtuales se dividen en 3 categorías de acuerdo con el servicio de conectividad que brinden:

2.1. VPN de Acceso Remoto.

(Remote Acces VPNs). Provee acceso remoto a la intranet o extranet corporativa a través de una infraestructura pública, conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada. Permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o IP para la conexión segura de usuarios móviles, *telecommuters* o sucursales remotas a los recursos corporativos (ver figura1 "VPN de acceso").

Características:

- Outsourcing de acceso remoto

- llamadas locales o gratuitas (n° 900)
- ubicuidad del acceso

- Instalación y soporte del PS (Proveedor de servicio)
- Acceso único al nodo central (elimina la competencia por puertos)
- Tecnologías de acceso RTC, ISDN, xDSL
- Movilidad IP
- Seguridad reforzada por el cliente

− AAA en el ISP proporciona 1° y posiblemente 2° nivel de seguridad.

2.2. VPN de Intranet.

Vincula la oficina remota o sucursal a la red corporativa, a través de una red pública, mediante enlace dedicado al proveedor de servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio y disponibilidad, entre otras (ver figura 2. "Intranet VPN").

Característica:

- Extiende el modelo IP a través de la WAN compartida.

2.3. VPN de Extranet.

Permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública (ver figura "Extranet VPN").

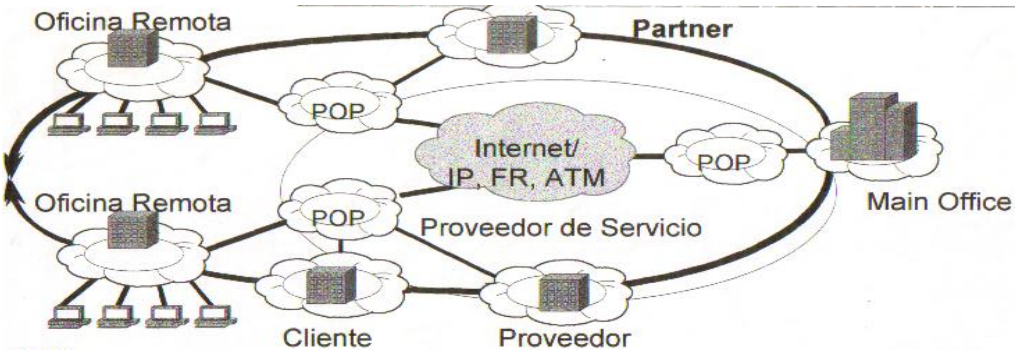
Características:

- Extiende la conectividad a proveedores y clientes

- sobre una infraestructura compartida
- usando conexiones virtuales dedicadas

- Los pharters tienen diferentes niveles de autorización

- accses control lists, firewalls, filtros, según decida la empresa



3. TECNOLOGÍA DE LAS REDES PRIVADAS VIRTUALES

La arquitectura de las VPNs se debe basar en elementos esenciales de la tecnología para proteger la privacidad, mantener la calidad y confibilidad, y asegurar la operatoria de la red en toda la empresa. Estos elementos son:

Seguridad: uso de túneles, encripción de datos, autenticación de usuarios y paquetes, control de acceso.

Calidad de Servicio: uso de colas, manejo de congestión de red, priorización de tráfico, clasificación de paquetes.

Gestión: implementación y mantenimiento de las políticas de seguridad y calidad de servicio a lo largo de la VPN.

3.1. Seguridad en las VPNs

Un punto fundamental es el particionamiento de las redes públicas o de uso compartido para implementar las VPN que son disjuntas. Esto se logra mediante ***el uso de túneles que no son ni más ni menos que técnicas de encapsulado del tráfico.*** Las técnicas que se utilizan son: GRE, que permite que cualquier protocolo sea transportado entre dos puntos de la red encapsulado en otro protocolo, típicamente IP; **L2TP** que permite el armado de túneles para las sesiones PPP remotas, y por último **IPSec** para la generación de túneles con autenticación y encriptado de datos.

La calidad de servicio permite la asignación eficiente de los recursos de la red pública a las distintas VPNs para que obtengan una performance predecible. A su vez, las VPNs asignarán distintas políticas de calidad de servicio a sus usuarios, aplicaciones o servicios. Las componentes tecnológicas básicas son:

Clasificación de Paquetes: asignación de prioridades a los paquetes basados en la política corporativa. Se pueden definir hasta siete clases de prioridades utilizando el campo de *IP precedence* dentro del encabezado del paquete IP.

Committed Access Rate (CAR): garantiza un ancho de banda mínimo para aplicaciones o usuarios basándose en la política corporativa.

Weighted Fair Queuing (WFQ): determina la velocidad de salida de los paquetes en base a la prioridad asignada a éstos, mediante el encolado de los paquetes.

Weighted Random Early Detection (WRED): complementa las funciones de TCP en la prevención y manejo de la congestión de la red, mediante el descarte de paquetes de baja prioridad.

Generic Traffic Shaping (GTS): reduce la velocidad de salida de los paquetes con el fin de reducir posibles congestiones de la red que tengan como consecuencia el descarte de paquetes.

4. ASPECTOS BASICOS DE TUNELES

Trabajar en un sistema de túnel es un método de utilizar una infraestructura de la red para transferir datos de una red sobre otra; los datos que serán transferidos (o carga útil) pueden ser las tramas (o paquetes) de otro protocolo.

En lugar de enviar una trama a medida que es producida por el nodo promotor, el protocolo de túnel la encapsula en un encabezado adicional. Éste proporciona información de entubamiento de manera que la carga útil encapsulada pueda viajar a través de la red intermedia.

De esta manera, se pueden enrutar los paquetes encapsulados entre los puntos finales del túnel sobre la red (la trayectoria lógica a través de la que viajan los paquetes encapsulados en la red se denomina túnel). Cuando las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final; nótese que este sistema de túnel incluye todo este proceso (encapsulamiento, transmisión y desencapsulamiento de paquetes).

Existen muchos otros ejemplos de túneles que pueden realizarse sobre intranets corporativas. Y aunque la Red de redes proporciona una de las intranets más penetrantes y económicas, las referencias a Internet en este artículo se pueden reemplazar por cualquier otra intranet pública o privada que actúe co*mo* de tránsito. Las tecnologías de túnel existen desde hace tiempo.

Algunos ejemplos de tecnologías maduras incluyen:

Túneles SNA sobre intranets IP. Cuando se envía tráfico de la Arquitectura de la red del sistema (SNA) a través de una intranet IP corporativa, la trama SNA se encapsula en un encabezado UPN e ¡P. Túneles IPX para Novell NetWare, sobre intranets IP. Cuando un paquete IPX se envía a un servidor NetWare o ruteador IPX, el servidor o ruteador envuelve el paquete IPX en un encabezado UDP e IP y luego lo envía a traves de una intranet IP.

EL ruteador IP a IPX de destino encabezado UPD e IP, el paquete al destino se han introducido en los últimos años nuevas tecnologías de sistemas de túneles, mismas que son el enfoque principal de este artículo. Incluyen:

Protocolo de túnel de punto a punto (PPTP). Permite que se encripte el tráfico IP, IPX o NetBEUI, y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP, como Internet.

Protocolo de túnel de nivel 2 (L2TP). Permite que se encripte el tráfico IP, IPX o NetBEUI, y luego se envíe sobre cualquier medio que dé soporte a la entrega de datagramas punto a punto, como IP, X.25, Frame Relay o ATM.

Modo de túnel de seguridad IP (IPSec). Deja que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP, para enviarse a través de una red corporativa IP o una red pública IP como Internes

4.1. PROTOCOLOS DE TUNELES

Para que se establezca un túnel, tanto el cliente de éste como el servidor deberán utilizar el mismo protocolo de túnel.

La tecnología de túnel se puede basar en el protocolo del túnel de Nivel 2 o e Nivel 3; estos niveles corresponden al Modelo de referencia de interconexión de sistemas abiertos (OSI).

Los protocolos de nivel 2 corresponden al nivel de Enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP y el envío de nivel 2 (L2F) son protocolos de túnel de Nivel 2, ambos encapsulan la carga útil en una trama de Protocolo de punto a punto (PPP) que se enviará a través de la red.

Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan paquetes. IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de Nivel 3; éstos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos a través de una red IP.

4.2. COMO FUNCIONAN LOS TUNELES

Para las tecnologías de túnel de Nivel 2 como PPTP y L2TP, un túnel es similar a una sesión; los dos puntos finales deben estar de acuerdo respecto al túnel, y negociar las variables de la configuración, como asignación de dirección o los parámetros de encriptación o de compresión.

En la mayor parte de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas; se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.

Por lo general, las tecnologías del túnel de Nivel 3 suponen que se han manejado fuera de banda todos los temas relacionados con la configuración, normalmente a través de procesos manuales; sin embargo, quizá no exista una fase de mantenimiento de túnel. Para los protocolos de Nivel 2 (PPTP y L2TP) se debe crear, mantener y luego concluir un túnel.

Cuando se establece el túnel, es Posible enviar los datos a través de¡ mismo. El cliente o el servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para su transferencia.

Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor, primero adjunta un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la que lo enruta al servidor del túnel. Este último acepta los paquetes, elimina el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo. La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar.

Los protocolos y los requerimientos básicos del túnel

Puesto que se basan en protocolos PPP bien definidos, los protocolos de *Nivel* 2 (como PPTP v L2TP) heredan un conjunto de funciones útiles. Como se señala adelante, estas funciones y sus contrapartes de Nivel 3 cubren los requerimientos básicos de la VPN

Autenticación de usuario. Los protocolos de túnel Nivel 2 hereda los esquemas de autenticación del usuario de PPP.

Muchos de los esquemas de túnel de Nivel 3 suponen que los puntos finales han sido bien conocidos (y autenticados) antes de que se estableciera el túnel. Una excepción es la negociación IPSec ISAKMP que proporciona una autenticación mutua de los puntos Finales del túnel. (Nótese que la mayor parte de las

implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios; como resultado, cualquier usuario con acceso a uno de los equipos de punto final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de seguridad cuando se conjunta el IPSec con un protocolo de Nivel 2, como el L2TP.)

Soporte de tarjeta de señales. Al utilizar el Protocolo de autenticación ampliable (EAP), los protocolos de túnel Nivel 2 pueden ofrecer soporte a una amplia variedad de métodos de autenticación, incluidas contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define la Autenticación de los certificados de llaves públicas en su negociación ISAKMP/Oakley.

Asignación de dirección dinámica. El túnel de Nivel 2 da soporte a la asignación dinámica de direcciones de clientes basadas en un mecanismo de negociación de protocolos de control de la red en general los esquemas del túnel de nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel. Cabe mencionar que los esquemas para la asignación de direcciones en el modo de túnel IPSec están actualmente en desarrollo, por lo que aún no están disponibles.

Compresión de datos. Los protocolos de túnel Nivel 2 proporcionan soporte a esquemas de compresión basados en PPP Por ejemplo, las implementaciones de Microsoft tanto de PPTP como L2TP utilizan Microsoft Point to Point Compression (MPPC). La IETF está investigando mecanismos similares (como la compresión IP) para los protocolos de túnel Nivel 3.

Encriptación de datos. Los protocolos de túnel Nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. Por su parte, la implementación de Microsoft de PPTP da soporte al uso opcional de Microsoft Point to Point Encription (MPPE), basado en el algoritmo RSA/RC4. Los protocolos de túnel Nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define varios métodos de Encriptación opcional de datos que se negocian durante el intercambio ISAKMP/Oaklev.

La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.

Administración de llaves. MPPE, un protocolo de Nivel 2, se basa en las claves iniciales generadas durante la Autenticación del usuario y luego las renueva en forma periódica. IPSec negocia explícitamente una llave común durante el intercambio ISAKMP y también las renueva de manera periódica.

Soporte de protocolo múltiple. El sistema de túnel de Nivel 2 da soporte a protocolos múltiples de carga útil, lo que facilita a los clientes de túnel tener acceso a sus redes corporativas utilizando IP, IPX, NetBEUI, etc.

En contraste, los protocolos de túnel Nivel 3, como el modo de túnel IPSec, por lo común dan soporte sólo a redes objetivo que utilizan el protocolo IP.

PROTOCOLOS DE PUNTO A PUNTO

Debido a que los protocolos de Nivel 2 dependen principalmente de las funciones especificadas para PPP, vale la pena examinar este protocolo más de cerca.

PPP se diseñó para enviar datos a través de conexiones de marcación o de punto a punto dedicadas. Encapsula paquetes de IP, IPX y NetBEUI dentro de las tramas del PPP, y luego transmite los paquetes encapsulados del PPP a través de un enlace punto a punto. Es utilizado entre un cliente de marcación y un NAS.

Existen cuatro fases distintivas de negociación en una sesión de marcación del PPP, cada una de las cuales debe completarse de manera exitosa antes de que la conexión del PPP esté lista para transferir los datos del

usuario. Estas fases se explican posteriormente.

FASE 1:

ESTABLECER EL ENLACE DEL PPP

PPP utiliza el Protocolo de control de enlace (LCP) para establecer, mantener y concluir la conexión física. Durante la fase LCP inicial, se seleccionan las opciones básicas de comunicación.

Nótese que durante la fase de establecimiento de enlace (Fase i), se seleccionan los protocolos de Autenticación, peto no se implementan efectivamente hasta la fase de Autenticación de conexión (Fase 2). De manera similar, durante el LCP se toma una decisión respecto a que si dos iguales negociarán el uso de compresión y/o encriptación. Durante la Fase 4 ocurre la elección real de algoritmos de compresión/encriptación y los otros detalles.

FASE 2:

AUTENTICAR AL USUARIO

En la segunda fase, la PC cliente presenta las credenciales del usuario al servidor de acceso remoto. Por su parte, un esquema seguro de Autenticación proporciona protección contra ataques de reproducción y personificación de clientes remotos. (Un ataque de reproducción ocurre cuando un tercero monitoriza una conexión exitosa y utiliza paquetes capturados para reproducir la respuesta del cliente remoto, de manera que pueda lograr una conexión autenticada.

La personificación del cliente remoto ocurre cuando un tercero se apropia de una conexión autenticada.

La gran parte de la implementaciones del PPP proporcionan métodos limitado, de Autenticación, típicamente el Protocolo de autenticación de contraseña (PAP), el Protocolo de autenticación de saludo Challenge (CHAP) Y Microsoft Challenge Handshake Authentication Protocol (MSCHAP).

Protocolo de autenticación de contraseña (PAP). El PAP es un esquema simple y claro de autenticación de texto: el NAS solicita al usuario el nombre y la contraseña y el PAP le contesta el texto claro (no encriptado).

Obviamente, este esquema de autenticación no es seguro ya que un tercero podría capturar el nombre y la contraseña para tener seña del usuario Y útil os un acceso subsecuente al NAS y todos los recursos que proporciona el mismo cuando se ha escrito la contraseña del usuario, PAP no proporciona protección contra ataques de reproducción o personificación de cliente remoto.

Protocolo de autenticación de saludo Challenge (CHAP). El CHAP es un mecanismo encriptado que evita la transmisión de contraseñas reales en la conexión. El NAS envía un Challenge, que consiste de una identificación de sesión y una extensión arbitraria al cliente remoto. Por su parte, el cliente remoto deberá utilizar el algoritmo de control unidireccional MD5 para devolver el nombre i del usuario y una encriptación del challenge, la identificación de la sesión y la contraseña del cliente.

El CHAP es una mejora sobre el PAP en cuanto a que no se envía la contraseña de texto transparente sobre el enlace. En su lugar, se utiliza la contraseña a fin de crear una verificación encriptada del challenge original. El servidor conoce la contraseña del texto transparente del cliente

y, por tanto, puede duplicar la operación y comparar el resultado con la contraseña enviada en la respuesta del cliente.

El CHAP protege contra ataques de reproducción al utilizar una extensión challenge arbitraria para cada intento de autenticación. Asimismo, protege contra la personificación de un cliente remoto al enviar de manera impredecible challenges repetidos al cliente remoto, a todo lo largo de la duración de la conexión.

Microsoft ChallengeHandshake Aut 1 identicatíon Protocol (MSCHAP).

Es un mecanismo de autenticación encriptado muy similar al CHAP. Al igual que en este último, el NAS envía un challenge, que consiste en una identificación de sesión y una extensión challenge arbitraria, al cliente remoto. El cliente remoto debe devolver el nombre del usuario y una verificación MD4 de la extensión challenge, el identificador de sesión y la contraseña MD4 verificada.

Este diseño, que manipula una verificación del MD4 de la contraseña, proporciona un nivel adicional de seguridad, debido a que permite que el servidor almacene las contraseñas verificadas en lugar de contraseñas con texto transparente.

MSCHAP también proporciona códigos adicionales de error, incluido un código de Contraseña ya expirado, así como mensajes adicionales cliente−servidor encriptado que permite a los usuarios cambiar sus contraseñas. En la implementación de Microsoft del MSCHAP, tanto el Cliente como el NAS, de manera independiente, una llave inicial para encriptaciones posteriores de datos por el MPPE.

El último punto es muy importante, ya que explica la forma en que se te quiere la autenticación del MSCHAP, a fin de permitir la encriptación de datos con base en MPPE.

Durante la fase 2 de la configuración del enlace del PPP, el NAS recopila los datos de autenticación y luego valida los datos contra su propia base de datos del usuario o contra un servidor central para la autenticación de base de datos, como el que mantiene un Controlador del dominio primario Windows NT, un servidor de Servicio remoto de usuario con marcación de autenticación (RA, DIUS).

FASE 3:

CONTROL DE ITERACIÓN DEL PPP

La implementación de Microsoft del PPP incluye una Fase opcional de control de interacción. Esta fase utiliza el protocolo de control de iteración (CBCP) inmediatamente después de la fase de autenticación .

Si se configura para iteración, después de la autenticación, le desconectan tanto el cliente remoto como el NAS. En seguida, el NAS vuelve a llamar al cliente remoto en el número telefónico especificado, lo que proporciona un nivel adicional de seguridad a las redes de marcación.

El NAS permitirá conexiones partir de los clientes remotos que físicamente residan sólo en números telefónicos específicos.

FASE 4:

INVOCAR LOS PROTOCOLOS A NIVEL DE RED

Cuando se hayan terminado las fases previas, PPP invoca los distintos Protocolos de control de red (NCP), que se seleccionaron durante la fase de establecimiento de enlace (fase i) para configurar los protocolos que utiliza el cliente remoto. Por ejemplo, durante esta fase el Protocolo de control de IP (IPCP) puede asignar una dirección dinámica a un usuario de marcación.

En la implementación del PPP de Microsoft, el protocolo de control de compresión se utiliza para negociar

tanto la compresión de datos (utilizando MPPC) como la encriptación de éstos (utilizando MPPE), por la simple razón de que ambos se implementan en la misma rutina.

Fase de transferencia de datos

Una vez que hayan concluido las cuatro fases de negociación, PPP empieza a transferir datos hacia y desde los dos iguales. Cada paquete de datos transmitidos se envuelve en un encabezado del PPP, que elimina el sistema receptor. Si se seleccionó la compresión de datos en la fase 1 y se negoció en la fase 4, los datos se comprimirán antes de la transmisión.

Pero si se seleccionó y se negoció de manera similar la encriptación de datos, éstos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

4.3. MODO DEL TUNEL DE SEGURIDAD DE PROTOCOLOS PARA INTERNET

El IPSec es un estándar de protocolo de Nivel 3 que da soporte a la transferencia protegida de información a través de una red IR En su conjunto se describe con mayor detalle en la sección de Seguridad avanzada.

Hay un aspecto del IPSec que debe analizarse en el contexto de los protocolos de túnel: además de su definición de mecanismos de encriptación para tráfico IP, IPSec define el 1 formato de paquete para un modo de túnel IP sobre IP, generalmente referido como un modo de túnel IPSec.

Un túnel IPSec consiste en un cliente de túnel v un servidor de túnel, ambos configurados para utilizar los túneles IPSec y un mecanismo negociado de encriptación. El modo del túnel del IPSec utiliza el método de seguridad negociada (de existir) para encapsular y encriptar todos los paquetes IP, para una transferencia segura a través de una red privada o pública IP. Así, se vuelven a encapsular la carga útil encriptada con un encabeza do IP de texto Y se envía en la red para su entrega a un servidor de túnel. Al recibir este datagrama, el servidor del túnel procesa y descarta el encabezado IP de texto y luego desencripta su contenido, a fin de recuperar el paquete original IP de carga útil. En seguida, se procesa el paquete IP de carga útil de manera normal y se en ruta su destino en la red objetivo.

El modo de túnel IP tiene la siguientes funciones y limitaciones:

- Solo da soporte a tráfico IP
- Funciona en el fondo de la pila IP por tanto, las aplicaciones y los protocolos de niveles más altos hereda su comportamiento.
- Está controlado por una Política de seguridad (un conjunto de reglas que se cumplen a través de filtros). Esta política de seguridad establece los mecanismos de encriptación y de túnel disponibles en orden de preferencia, así como los métodos de autenticación disponibles, también en orden de preferencia. Tan pronto como existe tráfico, ambos equipos realizan una autenticación mutua, y luego negocian los métodos de encriptación que se utilizarán. Posteriormente, se encripta todo el tráfico de encriptación, y luego se envuelve en un encabezado de túnel.

PROTOCOLO DE TUNEL DE PUNTO A PUNTO

El PPTP es un protocolo de Nivel 2 que encapsula las tramas del PPP en datagramas del IP para transmisión sobre una red IP, como la de Internet. También se puede utilizar en una red privada de LAN a LAN.

El Protocolo de túnel de punto a punto (PPTP) utiliza una conexión TCP, para mantenimiento del túnel y tramas encapsuladas del PPP de Encapsulamiento de entubamiento genérico (GRE) para datos de túnel. Se

pueden encriptar y/o comprimir las cargas útiles de las i tramas del PPP encapsulado.

La forma en que se ensambla el paquete del PPTP antes de la transmisión (el dibujo exhibe un cliente de marcación que crea un túnel a través de una red). El diseño de la trama final muestra la encapsulamiento para un cliente de marcación (controlador de dispositivo PPP).

REENVIO DE NIVEL 2 (L2F)

Una tecnología propuesta por cisco, es un protocolo de transmisión que permite que los servidores de acceso de marcación incluyan el tráfico de marcación en el PPP, y lo transmitan sobre enlaces WAN hacia un servidor L2F (un ruteador). Luego, el servidor L2F envuelve los paquetes y los inyecta en la red; a diferencia del PPTP y L2TP, L2F no tiene un cliente definido. Nótese que L2F funciona sólo en túneles obligatorios (para un análisis detallado de los túneles voluntarios y obligatorios, véase la sección "Tipos de túnel", más adelante en este artículo).

PROTOCOLO DE TÚNEL DE NIVEL 2 (L2TP)

Es una combinación del PPTP y L2F. Sus diseñadores esperan que el L2TP represente las mejores funciones del PPTP y L2E, L2TP es un protocolo de red cápsula las tramas de] PPP que viajan sobre redes IP, *x.25*, Frame Relay, o modo de transferencia ATM.

Cuando está configurado para utilizar al IP como su transporte de datagrama, L2TP se puede utilizar como un protocolo de túnel sobre Internet. También se Puede utilizar directamente sobre varios medios WAN (como Frame Relay), sin nivel de transporte IP.

El L2TP sobre las redes IP utiliza UDP y una serie de mensajes para el mantenimiento de túnel. Asimismo, emplea UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel; se pueden encriptar Y/O comprimir las cargas útiles de las tramas PPP encapsuladas.

PPTP COMPARADO CON EL L2TP

Tanto el PPTP como L2TP utilizan el PPP para proporcionar una envoltura inicial de los datos, y luego incluir encabezados adicionales a fin de transportarlos a través de la red. Aunque ambos protocolos son muy similares, existen diferencias entre ellos:

El PPTP requiere que la red sea de tipo IP, y el L2TP requiere sólo que los medios del túnel proporcionen una conectividad de punto a punto orientada a paquetes. Se puede utilizar L2TP sobre IP (utilizando UDP), circuitos virtuales permanentes (PVC), circuitos virtuales X25 (VC) o VC ATM.

El PPTP sólo puede soportar un túnel único entre puntos terminales, y el L2TP permite el uso de varios túneles entre puntos terminales. Con el L2TP es posible crear diferentes túneles para diferentes calidades de servicio.

L2TP proporciona la compresión de encabezados. Cuando se activa la compresión de encabezado, el L2TP opera sólo con 4 bytes adicionales, comparado con los 6 bytes para el

PPTP.

L2TP proporciona la autenticación de túnel, no así el PPTP. Sin embargo, cuando se utiliza cualquiera de los protocolos sobre IPSec, se proporciona la autenticación de túnel por el IPSec, de manera que no sea necesaria la autenticación del túnel Nivel 2.

4.4. TIPOS DE TUNEL

Se pueden crear túneles en diferentes formas.

Túneles voluntarios: Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora de¡ usuario es un punto termina¡ de¡ túnel y actúa como un cliente de éste.

Túneles obligatorios: Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con uno de éstos, la computadora de¡ usuario deja de ser un punto termina¡ de¡ túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora de¡ usuario y el servidor del túnel, es el punto termina¡ del túnel y actúa como el cliente del mismo.

A la fecha, los túneles voluntarios han robado ser el tipo más popular de túnel. Las siguientes secciones describen cada uno de estos tipos con mayor detalle.

4.4.1. TUNELES VOLUNTARIOS

Un túnel voluntario ocurre cuando, una estación de trabajo o un servidor de entubamiento utiliza el software del cliente del túnel, a fin de crear una conexión virtual al servidor del túnel objetivo; para lograr esto se debe instalar el protocolo apropiado de túnel en la computa*dora cliente. Para los* protocolos que se analizan en este artículo, los túneles voluntarios requieren una conexión IP (ya sea a través de una LAN o marcación).

En determinadas situaciones, el cliente debe establecer una conexión de marcación con el objeto de conectarse a la red antes de que el cliente pueda establecer un túnel (éste es el caso más común). Un buen ejemplo es el usuario de Internet por marcación, que debe marcar a un ISP y obtener una conexión a Internet antes de que se pueda crear un túnel sobre Internet..

Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un entubamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este sería el caso para un cliente en una LAN corporativa, que inicia , un túnel para alcanzar una subred privada u oculta en la misma LAN (como sería el caso de la red de Recursos Humanos).

Es falso que las VPN requieran una conexión de marcación, pues sólo requieren de una red IP. Algunos clientes (como las PC del hogar) utilizan conexiones de marcación 1 Internet para establecer transporte IP; esto es un paso preliminar en la preparación para la creación de un túnel, y no es parte del protocolo del túnel mismo.

4.4.2. TÚNELES OBLIGATORIOS

Diversos proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora del cliente es conocida de varias maneras: Procesador frontal (FEP) en PPTP, un Concentrador de acceso a L2TP (LAC) en L2TP o un gateway de seguridad IP en el IPSec. En este artículo, el término FEP se utilizará para describir esta funcionalidad, sin importar el protocolo de túnel.

Para realizar esta función, el FEP deberá tener instalado el protocolo apropiado de túnel y ser capaz de establecer el túnel cuando se conecte la computadora cliente.

En el ejemplo de Internet, la computadora cliente coloca una llamada de marcación al NAS activado por los túneles en el ISP; puede darse el caso de que una empresa haya contratado un ISP para instalar un conjunto nacional de FEP.

Esta configuración se conoce como "túnel obligatorio" debido a que el cliente está obligado a utilizar el túnel creado por FER Cuando se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel.

En los túneles obligatorios, la computadora cliente realiza una conexión única PPP, y cuando un cliente marca en el NAS se crea un túnel y todo el tráfico se enruta de manera automática a través de éste. Es posible configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel. De manera alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el FEP y servidor puede estar compartido entre varios clientes de marcación. Cuando un segundo cliente marca al servidor de acceso (FEP) a fin de alcanzar un destino no hay necesidad de crear una nueva instancia del túnel entre el FEP y el servidor del túnel.

Las VPNs proveen hoy ahorros de un 50 a un 75 por ciento en los costos de comunicaciones, y permiten mantener la arquitectura de las redes flexible para adaptarse a los nuevos mecanismos de negocio de las empresas.

Estudios de mercado asignan a las VPNs oportunidades de negocio por U$S 1.1 mil millones a nivel mundial para el año 2001, con un crecimiento anual del 72 por ciento.

Esto lo vemos reflejado en nuestro mercado local, dado que los principales vendedores comenzaron a ofrecer este tipo de servicio.

BIBLIOGRAFIA

www.3com.com/pressbox.

www.icsa.com

www.checkpoint.com

http://ds.internic.net/internet−drafts/drafts−ietf−pppext−pptp−02.txt

www.goto.com

www.gocsi.com

ANEXO

A.1 Artículo VPN inalámbricas

Las Redes Privadas Virtuales (VPN) ya son inalámbricas: 3Com® agrega tunelización a las redes de datos CDMA

SANTA CLARA, California − 3 de mayo de 1999 − 3Com Corporation (NASDAQ: COMS) anunció hoy que ha intensificado su equipo de infraestructura para redes de servicios múltiples a fin de posibilitar el despliegue de servicios de redes privadas virtuales (VPN) inalámbricas.

La Función de Interacción (IWF) dentro de la plataforma de acceso a servicios múltiples Total Control® de 3Com ahora soporta al Protocolo de Tunelización del Estrato 2 (L2TP) estándar de la IETF y el Protocolo de

Tunelización Punto a Punto (PPTP) de Microsoft®. El soporte por tunelización protegida en la IWF permite a los proveedores de servicios inalámbricos que usan redes de datos basadas en Acceso Múltiple por División de Códigos (CDMA) para ampliar el alcance de las VPN alámbricas de los clientes comerciales hacia sus empleados ambulantes que precisan del acceso a los datos cuando no hay un enchufe telefónico a la mano.

Por ejemplo, utilizando un auricular inalámbrico, el personal ambulante de ventas puede obtener acceso en forma directa y segura a la información de productos, precios e inventarios que hay en las intrarredes de sus empresas, enviar y recibir correo electrónico y utilizar los recursos del Internet público sin contraer cargos de larga distancia de las redes telefónicas de conmutación pública (PSTN). Asimismo, pueden enchufar el auricular en una computadora portátil plegable − usándola, de hecho, como módem − para obtener acceso a aplicaciones de cliente/servidor de su empresa, enviar por fax o sencillamente aprovechar la visualización más grande de la información en texto y gráficas.

"Las VPN inalámbricas permiten a las compañías de PCS ampliar sus carteras con servicios de datos intensificados que complementan sus productos populares para VPN alámbricas, mientras que crean nuevas fuentes de ingresos para su compañía", declaró Ben Cardwell, Director de Gestiones de Productos Inalámbricos de 3Com Carrier Systems.

La CDMA es una tecnología estándar de espectro distribuido usada en el despliegue de las redes de servicios de comunicaciones personales móviles (PCS). Permite que los proveedores de servicios integren los servicios de acceso de voz y datos a los abonados a precios más bajos que si usaran redes distintas. 3Com es el líder mundial en fabricación de equipos de CDMA para interacción con datos.

Dónde y cómo funcionan los protocolos de tunelización

En la nueva implementación de tunelización para CDMA de 3Com, los L2TP y PPTP encapsulan el tráfico de datos de un abonado en una conexión virtual protegida entre la red inalámbrica y la red "anfitriona" del cliente − el Internet o una red empresarial. Al usar L2TP o PPTP, la red anfitriona puede comprobar definitivamente si el usuario tiene privilegios de acceso a la red anfitriona.

No se precisa de modificaciones al dispositivo del cliente. Los usuarios finales son identificados como miembros de la VPN por el número de acceso telefónico que marcan. Mediante un túnel de L2TP o PPTP por el Internet, la IWF envía la llamada a la red anfitriona, la cual autentica al usuario en base al nombre y la contraseña de acceso de usuario.

El acceso inalámbrico elimina los problemas con las PSTN

La característica de Conexión Rápida a la Red del software de entrada de IWF conecta la red inalámbrica directamente al Internet, resultando en una conexión absolutamente digital que evita la PSTN y sus tiempos y costos de conexión relacionados. Al usar una solución inalámbrica de datos, el abonado ambulante disfruta de los beneficios de tiempos de conexión de llamadas de 3 a 5 segundos, en contraste con los tiempos de conexión de 20 a 30 segundos del módem alámbrico.

Acerca de la Corporación 3Com

Con más de 200 millones de clientes en el mundo entero, la Corporación 3Com comunica a más personas con la información en más formas que cualquier otra compañía de redes. 3Com proporciona productos innovadores de acceso a la información y soluciones de sistemas de redes a empresas grandes, medianas y pequeñas; portadores y proveedores de servicios de red; fabricantes de equipo original de PC y consumidores. 3Com−More connected!.

A.2 GLOSARIO

Datagramas: son paquetes de información.

Extranet. Una extranet es una red privada que usa los protocolos de Internet y el sistema público de telecomunicaciones para compartir, de modo seguro, parte de la información de un negocio o las operaciones con proveedores, vendedores, socios, clientes u otro tipo de negocios. Una extranet puede ser considerada como parte de la intranet de una compañía que se amplía a usuarios que están fuera de la empresa.

Intranet: Red TCP/IP de una empresa que utiliza los protocolos y normas abiertas que han surgido a partir de Internet .(Para fines de siglo ya habrá 4,6 millones de intranets y tan sólo 440.000 servidores de Internet (IDC))

Módem: (*modulador−demodulador*) modula las señales digitales que salen de un ordenador u otro dispositivo digital para convertirlas en señales analógicas para que puedan ser enviadas por una línea telefónica convencional de par entrelazado de cobre, y demodula la señal analógica para convertirla en una señal digital que pueda ser interpretada por el dispositivo.

PSI: Provedores Independientes de Servicio.

Red: Es una colección de estándares, basada en dispositivos que encadenan todo lo referente a la compañía, como computadoras de escritorio, anfitriones y recursos, sin sacrificar velocidad, costo o maniobrabilidad.

Tunel: Técnicas de encapsulado del tráfico**.**

A.3. CONCLUSIONES INDIVIDUALES

- **HERNÁNDEZ GARCÍA MÓNICA**

Como pudimos observar durante el desarrollo del presente trabajo, una red privada virtual conecta los componentes de una red con otra. Aparentemente las VPN parecen tener el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia.

Las VPN son de gran utilidad para los usuarios, porque les proporciona acceso remoto a recursos corporativos sobre Internet público y mantiene al mismo tiempo la privacidad de su información incluyendo la integridad de los datos al viajar a través de Internet. Además de que les brinda la certeza de que están trabajando en un canal seguro.

- **ESPINOSA JIMENEZ MA. MARGARITA**

Por lo anterior, entiendo que una VPN es una red privada que opera a través de una red pública, que bien ésta puede ser Internet. Toda la información que se envíe o reciba aparentemente estará operando a través de la red pública. Así toda la red que esté navegando, estará segura de cualquier ataque en la red, por navegadores, curiosos o inexpertos y principalmente de los hackers. Y además el acceso a este tipo de redes será exclusiva para las personas o grupos que estén suscritos a una VPN.

También es cierto que día con día crece la inseguridad en la red, es decir, uno no sabe, que nuestro nombre, domicilio, fecha de nacimiento, preferencias comerciales, entre otras cosas puede estar siendo pública en ese momento; y no privada como muchos lo creemos. Sin embargo también la tecnología avanza en la misma medida para bien, es decir, para estar al servicio y en protección de cualquier ataque que se le haga a nuestra privacía.

Las Redes Virtuales Privadas son una opción más para que las grandes (y pequeñas) empresas se mantengan a salvo de cualquier intento de ataque en contra de esa información tan valiosa. Asimismo pueden auxiliarse

de la amplia tecnología de vanguardia en cuanto a software y hardware se refiere.

Debemos tomar conciencia de que la tecnología de vanguardia muchas veces se aplica para mal (para violar información privada); pero que en muchas otras ocasiones ésta misma se encuentra en buenas manos y nos permite comunicar rápidamente y sobre todo ser transmitida de una forma segura y confiable.

- **JURADO QUINTANA NORMA IVETTE**

Considero importante conocer nuevas tecnologías que tal vez en un tiempo eran sólo sueños ó algo considerado como inalcanzable, las Redes Virtuales Privadas ofrecen posibilidades de expansión a los empresarios, ya que de muchas redes pequeñas se puede visualizar una red muy grande lo cual proporciona mayor cobertura, además de ser un medio de comunicación realmente seguro y que facilita que la información sea actualizada, oportuna y nuevamente menciono, son medio seguro.

La red privada virtual la podemos definir, en el alcance de este documento, como el conjunto de redes privadas que se interconexionan entre si mediante la explotación de los recursos de Internet. Tampoco cae fuera de esta definición aquella Intranet que tiene una serie de subredes físicamente distantes y consigue que los recursos remotos se puedan ver como locales utilizando a Internet como canal global de comunicaciones.

Una red virtual significa poseer los beneficios y características que ofrecen exclusivamente los enlaces privados de comunicación sin la necesidad de poseer la infraestructura requerida para ello. Una red virtual no requiere enlaces físicos, ya que se configura mediante software sobre la red inteligente del operador.

Cabe considerar la VPN de acceso remoto, en la cual se proporciona conectividad a la red corporativa a los usuarios remotos pero móviles, sin capacidad de disponer de una infraestructura de red estática.

Virtual Private Network

1